COMPUTATIONAL PROBLEMS IN ABSTRACT ALGEBRA.

Proceedings of a Conference held at Oxford under the auspices of the Science Research Council Atlas Computer Laboratory, 29th August to 2nd September 1967

EDITED BY

JOHN LEECH

Reader in Computing Science,
Stirling University

WITH A FOREWORD BY

DR. J. HOWLETT

Director, S.R.C. Atlas Computer Laboratory

THE QUEEN'S AWARD TO INDUSTRY 1966

PERGAMON PRESS

OXFORD · LONDON · EDINBURGH · NEW YORK
TORONTO . SYDNEY . PARIS . BRAUNSCHWEIG

Pergamon Press Ltd., Headington Hill Hall, Oxford
4 & 5 Fitzroy Square, London W.1
Pergamon Press (Scotland) Ltd., 2 & 3 Teviot Place, Edinburgh 1
Pergamon Press Inc., Maxwell House, Fairview Park, Elmsford,
New York 10523
Pergamon of Canada Ltd., 207 Queen's Quay West, Toronto 1
Pergamon Press (Aust.) Pty. Ltd., 19a Boundary Street, Rushcutters Bay,
N.S.W. 2011, Australia
Pergamon Press-S.A.R.L., 24 rue des Écoles, Paris 5e
Vieweg & Sohn GmbH, Burgplatz 1, Braunschweig

First edition 1970

Library of Congress Catalog Card No. 75-84072

Printed in Hungary

08 012975 7

Contents

Foreword

IF the electronic digital computer has not already virtually taken over the world's arithmetic it will have done so before long. This remarkable success story in the field of applied mathematics-much of it very simple mathematics, admittedly, such as cost calculations-contrasts strongly with the machine's very moderate impact so far on pure mathematics. Obvious economic considerations account for much of this difference: no one can be surprised that the need to optimize the design of a nuclear power reactor or to develop a stores holding and purchasing strategy for a large factory provides more economic drive than, say, the properties of the partition function. But this can hardly apply in a university environment, where the pure mathematicians have as much right to the central computing service as anyone else. The explanation must be the great difficulty of the problems; the machine offers great powers of logical processing, of which arithmetic is only a small and not very interesting part, but it is far from clear how these can be used in the service of anything that can be called genuine mathematics.

However, work has in fact been going on in various fields of pure mathematics ever since computers became available. Professor Douglas Munn, surveying the scene from the point of view of an algebraist, decided in 1966 that enough had been done on the application of computers to abstract algebra to warrant the holding of an international conference, to assess what had been achieved and to identify promising lines of future research. A frequent visitor to the Atlas Laboratory, he talked about this with me and my colleague Dr. Robert Churchhouse, and after very little discussion we found ourselves agreeing that the time was indeed right for such a conference, that Oxford would be an admirable location and that the Atlas Laboratory should organize it. We approached Professor Graham Higman who immediately and enthusiastically agreed to give his support; and with equal immediacy and enthusiasm had Professor Coulson's permission to hold the conference in Oxford's beautiful new Mathematics Institute.

The success of the meeting must be judged from the quality of the papers, reproduced in this volume. I want to record my gratitude to the Science Research Council, who allowed me to meet some of the expenses from Atlas Laboratory funds, and to I.C.T. Limited for generous financial support: jointly, they made it possible to hold the conference. The staff of the Mathematics Institute were as helpful and welcoming as anyone could ever be, Mr. C. L. Roberts and the staff of the Atlas Laboratory Administration Group ensured that the mechanics went without a hitch and the whole of the general organization was carried out with great efficiency by Miss Synolda Butler. I am most grateful to them all, and to Pergamon Press for undertaking the publication of the Proceedings: and finally, to Mr. John Leech for so willingly agreeing to be Editor.

J. HOWLETT

Preface

Dr. Howlett has described the genesis of the Conference; here I need only describe the compilation of this volume of Proceedings. Speakers at the Conference were invited to deliver manuscripts at or soon after the Conference, and this volume is based on these manuscripts, substantially as received. Most authors prepared their papers without reference to the papers of other authors. This has the result that their notation is not uniform and there are overlaps; no attempt has been made to coordinate papers in this respect. So each paper is a substantially independent account of its topics, and is capable of being read without reference to other papers. Readers may find it an advantage to have different authors' accounts where these overlap. A disadvantage, however, is that cross-references between papers in this volume are far from complete; the reader of a paper may check which other papers in the volume are also relevant.

The sequence of papers in this volume is based on that of the lectures at the Conference, with minor changes; the large body of papers on group theory are placed first, beginning with Dr. Neubüser's comprehensive survey, and subsequent papers are placed in roughly the order of distance of the subject from group theory. To complete the record of the Conference, I add that Mr. M. J. T. Guy and Professors D. G. Higman, W. 0. J. Moser, T. S. Motzkin and J. L. Selfridge also delivered lectures at the Conference, but did not submit manuscripts for publication; this accounts for a few allusions to topics absent from this volume. The correspondence between the subject matter of the other lectures and the present papers is not always close. Professor Mendelsohn's first paper is based on points made in discussion and not on a lecture of his own, while the paper by Professors Krause and Weston was not presented at the Conference. A bibliography on applications of computers to problems on algebra was prepared by Dr. Dénes and distributed at the Conference; this is not reproduced here as all relevant items have been included by Dr. Neubüser in the bibliography to his survey paper.

The editorial policy has been that the subject matter and style of papers are wholly the responsibility of the authors. Editing has been confined to points of typography, uniformity of style of references, divisions ofpapers, etc., and, at the request of certain authors whose native language is not English, some minor changes of wording. (This is a refined way of saying that I have done as little as I could get away with.)

I am indebted to the authors for their co-operation in producing this volume, to Dr. Howlett for contributing the Foreword, to the S.R.C. Atlas Computer Laboratory for a Research Fellowship during the tenure of which much of the work of editing was done, and to the University of Glasgow for leave of absence both to attend the Conference and to accept the Research Fellowship. It is also a pleasure to acknowledge the co-operation of the publishers, Pergamon Press, and it is through no fault of theirs that events such as the devaluation of British currency (which necessitated a change of printers) have conspired to delay the appearance of this volume.

JOHN LEECH

Investigations of groups on computers

J. NEUBÜSER

1. Introduction. In this paper a survey is given of methods used in and results obtained by programmes for the investigation of groups. Although the bibliographies [De **1**] and [Sa 1,2,3] have been used, among other sources, no claim for completeness can be made for two reasons, that some publications may have been overlooked, and that the conference itself has shown once more that there are many activities in this field which are not (yet) covered by regular publications.

1.1. Papers and programmes have not been included if their main objective is something different from the study of groups, even if groups play some role in them. Four particular cases of this kind may be mentioned.

1.1.1. Combinatorial problems dealing with things like generation of permutations, graphs, orthogonal latin squares, projective planes, block designs, difference sets, and Hadamard matrices. For most of these topics surveys are available, e.g. [Ha **1, 4;** Sw **1**].

13.2. Theorem-proving programmes. Most of these have been used to construct proofs for very elementary group-theoretical theorems. There seems to be only one [No **1**] specifically made to handle group-theoretical statements.

1.1.3. Programmes for the determination and study of homology and homotopy groups, where the main interest is in the topological relevance of the results. Such papers are [Li 4; Ma 1, 2; Pi 1] and part of [Ca 23.

1.1.4. Applications of groups in fields like coding theory [Pe 1] or the use of a computation in residue class groups for the improvement of a programme described in [Pa **1**].

1.2. Although the distinction is not always quite clear cut, it is practical for this survey to distinguish between special purpose and general purpose programmes. In spite of the fact that the first category is more likely to produce significant contributions to group theory, more space will be given in this report to the second kind, simply because this is the author's own field of work.

2. Special purpose **programmes.** By the first kind I mean programmes specially made for the investigation of a particular problem; when this

is solved, the programme may be put out of use. There are a number of problems tackled in this way, which we discuss in turn.

2.1. The construction of all groups of a particular kind,

2.1.1. A programme of this kind was first suggested as early as 1951 by M. H. A. Newman [Ne 4] for the investigation of the groups of order 256. P. Hall [Ha 7] had introduced the concept of isoclinism for the classification and construction of p-groups. Newman pointed out that the number of cases to be investigated for the determination of all groups of order 256 in a simple-minded use of Hall's ideas would be far too big for computers then (and would be even now). He gave an estimate to show that by a probabilistic approach it would be feasible to obtain the great majority of these groups in a reasonable time. It seems, however, that this suggestion has never been followed.

2.1.2. In this conference C. C. Sims [Si 3] gave an outline of a different procedure by which in principle each group of prime-power order would be obtained just once. In this a group G of order p^n is constructed as an extension of the last term $\Phi_k(G) \neq \langle 1 \rangle$ of its lower @-series, defined by $\Phi_1(G) = G$, $\Phi_{i+1}(G) = [G, \Phi_i(G)] \langle g^p \mid g \in \Phi_i(G) \rangle$. The non-isomorphic groups G with fixed $\Phi_k(G) \cong K$ and G/@,(G) $\cong$ ***H*** are in l-l correspondence with those orbits of $H^2(H, K)$ under the joint action of both automorphism groups *A(H)* and A(K), for which the extensions are groups with $\Phi_k(G) = K$. Sims has written a programme along these lines which determined the two-generator groups of order 32 in a very short time. According to him extrapolation from this experience would indicate quite bearable computation times ($\sim$ 10 hours) for the determination of most of the groups of order 128. Special methods are probably necessary for the case that ***His*** elementary abelian of order 32 and ***K*** elementary abelian of order 4.

2.1.3. Also in this conference J. Cannon [Ca 3] reported that R. James (Sydney) is determining the groups of order p^6 for arbitrary primes ***p*** using isoclinism. The calculations necessary in this set-up to find all non-isomorphic groups in a given isoclinism class were done by a computer for the first few primes and then generalized.

2.1.4. A listing of all primitive groups of low degrees is presently undertaken by C. C. Sims [Si 2,4]. Earlier hand calculations went up to degree 20. These groups have been redetermined and the previous results found correct. The calculations will be extended to higher degrees.

2.2. The Burnside problem. A recent survey of the problem is found in [Ha 3], to which the reader is referred for definitions used and theoretical results mentioned here. The finiteness of the Burnside groups ***B(n, r) of*** exponent ***n*** on ***r*** generators is known for ***n*** = 2, 3, 4, 6 and all ***r,*** but the order of ***B(n, r)*** is known only for ***n*** = 2, 3, 6, all ***r,*** and ***n = 4, r*** = 1, 2. In

1962 M. Hall jr. [Ha I] outlined a programme by which in particular the order of ***B(4,3)*** could be investigated. The idea was to use a Schreier technique to find generators and relations for a suitable subgroup of ***B(4,3)*** which could be handled. In 1964 M. Hall jr. and D. E. Knuth [Ha 2] announced that with a programme applicable to arbitrary nilpotent Burnside groups some results on ***B(4,*** 3) had been obtained, e.g. that the identity $(x, y, z, w, w, w) \equiv 1$ holds modulo the seventh term of the lower central series of this group. J. Leech [Le 2] has used Todd-Coxeterprogrammes (see § 3.1) to obtain and to improve systems of defining relations for ***B(3,*** 3) and ***B(4,2)*** and of groups of exponent 4 on three generators all or two of which are of order 2. An investigation along different lines of the groups ***B(4, k)*** is presently carried out by A. Tritter [Tr **1**]. He tries to prove that there is a bound for the classes of the derived groups of the groups ***B(4, k),*** which would be a consequence of a conjecture of G. Higman [Hi **1**]. For exponent 5 only the restricted Burnside problem has been solved. The biggest finite group ***B*(5,2)*** of exponent 5 on two generators was found to be of class at most 13 and order at most 5^{34}. Recently, E. F. Krause and K. Weston [Kr 3], starting from Kostrikin's calculations, used a computer to establish that these bounds are in fact attained.

Some of the programmes described in § 3.1 may also give some information on the restricted Burnside problem.

2.3. The search for simple groups. So far systematic searches with computers have established only the non-existence of simple groups of certain kinds.

2.3.1. In 1957 E. T. Parker and P. J. Nikolai [Pa **2**] tried to find analogues of the Mathieu groups M_{11} and M_{23}. Their computations showed that for $23 < p \leqslant 4079$ the cyclic and the alternating group are the only transitive permutation groups of degree $p = 2q + 1$, p and q primes.

2.3.2. In 1961, when the theorem that a group G of odd order is soluble had been proved by W. Feit and J. G. Thompson only under the additional assumption that all Sylow subgroups of G are abelian, a large-scale search for non-abelian simple groups of odd order was carried out by K. I. Appel, M. Hall jr. and J. G. Thompson [Ap **1**]. A number of restrictions for the orders of such groups were incorporated in a programme, which sorted about 400 "possible" orders out of all orders up to 10^8. These were eliminated by individual hand calculation, so that the non-existence of insoluble groups of odd order $\leqslant 10^8$ was established.

2.3.3. More recently K. I. Appel and E. T. Parker [Ap **2**] have made a computer search for insoluble groups of degrees $p = 4q + 1$, p and q primes, and have shown that there are no such groups of degrees 29, 53, 149, 173, 269,293 or 317 other than the alternating groups.

2.3.4. A systematic search is being currently made by M. Hall jr. [Ha 5] for simple groups of orders $\leqslant 10^6$.

2.3.5. Added in proof, July 1968. G. Higman and J. K. S. McKay [Hi 2] have used Todd-Coxeter and character-table programmes (see §§ 3.1,3.4.5 and 3.4.9) to prove the existence of a certain simple group described by Z. Janko [Ja 2].

2.4. Characters and representations of symmetric groups. A detailed description of the representation theory of the symmetric groups is given in [Ro 1]. As the methods for the computation of characters of symmetric groups are essentially combinatorial, they have been programmed rather early. The character tables of the symmetric groups of degree 15 and 16 were determined by R. L. Bivins ***et al.*** [Bi 1]. S. Comét wrote a series of papers on programmes for the determination of characters of the symmetric groups, in which in particular he developed techniques specially adapted to binary computers [Co 1,2,3,4]. He obtained lists of all absolutely irreducible characters for the symmetric groups of degree ≤ 20 [Co 5]. Other programmes have been developed by J. K. S. McKay [Mc 1] and R. E. Ingram, Dublin (unpublished).

Tables of irreducible unitary representations of symmetric groups (for applications in physics) have been computed by S. Katsura [Ka 1,2].

2.5. The Hp-problem. Let the prime p divide the order of a group G and let $Hp(G)$ be the subgroup of G generated by all elements of G not of order p. D. R. Hughes [Hu 1] has raised the question if $Hp(G)$ is always equal to $\langle 1 \rangle$, equal to G, or of index p in G. The question has been answered in the affirmative for $p = 2$ and $p = 3$, and for arbitrary p if G is finite and not a p-group [Hu 2] or a finite p-group of class $\leq p$ [Za 1]. G. E. Wall [Wa 2] showed that for a p-group the question can be investigated by a computation in a Lie-algebra over GF(p). By a laborious hand calculation he showed that the answer is negative forp-groups withp = 5. At present a programme is being developed by J. Cannon [Ca 3] for checking these calculations and extending them to greater p. ***Added in proof, July*** 1968 : The programme is now working and has confirmed the result for $p = 5$ and extended it to $p = 7$ (private communication).

2.6. Miscellaneous problems.

2.6.1. H. Brown (unpublished) has written a programme, following a method of H. Zassenhaus [Za 2], for the derivation of all space groups (in R_4) from given arithmetical (integral) crystal classes. The space groups are classified up to isomorphism by this programme. By a similar programme of G. Fast and T. W. Janssen [Fa 1] the space groups of R_4 are classified only up to equivalence as extensions of their translation subgroup by their arithmetical crystal class.

2.6.2. Let $\Gamma_0(n)$ be the group of all 2×2 integral matrices $A = \begin{pmatrix} a\, b \\ c\, d \end{pmatrix}$ with det $A = 1$ and $c \equiv 0 \pmod{n}$ and $\Gamma^*(n)$ the group generated by $\Gamma_0(n)$ and

$\begin{pmatrix}0 & -1\\ n & 0\end{pmatrix}$, H. Fell, M. Newman and E. Ordman [Fe 1] have tabulated the genera of the Riemann surfaces belonging to these groups for $n \leqslant 1000$ using classical formulae in the programme.

2.6.3. S. L. Altmann and C. J. Bradley [Al **1, 2**] have tabulated data for the irreducible representations of the rotation group of integral weight (see Gel'fand and Sapiro [Ge **1**]) up to weight 20.

2.6.4. Left normed commutators $[a, nb]$ are defined recursively by $[a, Ob] = a$, $[a, (i+ l)b] = [[a, ib], b]$. For a finite group G let $m(G) \neq 0$ be the smallest integer such that for all pairs $a, b \in$ G there is an integer n for which $[a, nb] = [a, (n+m(G))b]$. J. M. Campbell and W. J. Lamberth [Ca **2**] describe a programme for the determination of $m(G)$ for finite groups G given as permutation groups. For the alternating group A_6 of degree 6, for example, they obtained $m(A_6) = 120$.

2.6.5. Let Z_n be the ring of integers mod n and let π and π' be permutations of the elements of Z_n with $\pi(0)$ = n'(0) = 0. Let π and π' be called translation equivalent if there exists an element $d \in Z_n$ such that $\pi(i+ 1)$ -n(i) = $\pi'(i+ 1 + d) - \pi'(i+ d)$ for all $i \in$ Z,,. A group of permutations of the elements of Z_n is called translation invariant by E. S. Selmer [Se 2] if it consists of full equivalence classes under the defined translation equivalence. He has proved some permutation groups to be translation invariant and is presently also investigating others for this property with a computer.

2.6.6. M. E. White [Wh 1] announced a study of the possibility of presenting finite groups as groups of pairs of integers for which a suitable multiplication of a certain restricted kind is defined.

2.6.7. Programmes for the application of crystallographic groups to computations in quantum mechanics have been developed by S. Flodmark [Fl 1,2].

3. General purpose programmes. The'programmes to be mentioned here are not primarily made to answer a particular question but rather as a tool that can be used again and again. Some are based on algorithms previously designed for hand calculation, some are built up by using combinations of well-known theorems.

3.1. ***Todd-Coxeter and Schreier methods.*** The Todd-Coxeter algorithm [To **1**; Co 6] enumerates the cosets of a subgroup U of finite index in a group G, when G is given by finitely many abstract generators and defining relations and U by finitely many generators expressed as words in the generators of G. This algorithm seems to have been first programmed in 1953 by C. B. Haselgrove (unpublished). Since then many other programmes for this algorithm have been developed which sometimes differ in their strategy for choosing the next coset to be dealt with. J. Leech [Le 2] gave a very clear discussion of the different approaches, which is revised for these proceedings [Le **4**]. So it is sufficient here to give references (partially copied from [Le **2**]). A number of papers give details of programmes [Ba 1; El 1; Fe 2,3,4; Gu 1; Ma 3; Tr 2,3]. Applications are found in [Ca 1; Le 1,3; Me 3] and some of the papers mentioned before and hereafter.

The Todd-Coxeter procedure yields not only the number of cosets of U in G but also a permutation representation for the generators of G on the cosets of U. The kernel of this representation of G is $K = \bigcap_{g \in G} g^{-1} Ug$. Hence one can obtain G/K by a programme which generates a permutation group from given permutations or at least finds its order.

An interesting instance, where an observed periodicity of the output of a Todd-Coxeter programme led to a proof of the infiniteness of the group in question, is noted by C. C. Sims [Si **1**].

More recently the Todd-Coxeter technique has been combined with the Schreier technique, see e.g. [Ma **4**], to obtain generators for a subgroup U from generators of the whole group G and coset representatives of the cosets of U in G. The algorithms obtained solve the following problem: Let a group G be given by generators $g_1, \ldots, g_k$ and relations $r_1(g_1, \ldots, g_k) = \ldots = r_e(g_1, \ldots, g_k) = 1$ and let a subgroup U of finite index in G be generated by words $u_1, \ldots, u_s$ in the g_i. The Todd-Coxeter procedure yields coset representatives $c_1, \ldots, c_t$ of the cosets of U in G. For an element w, given as a word in the g_i, one has to find the expression $w = w^*c_j$, where c_j is one of the coset representatives and w^* is a word in the u_i. Some different methods for doing this have been discussed [Be 1; appendices to Le 1,3; Le 4; Me 1,2,3; Mo 1,2].

It would be most useful if these techniques could be extended further. Given generators and relations for a group G and coset representatives for the cosets of a subgroup U in G, the Schreier procedure gives generators and defining relations for U *(see* [Ma 4; Me 4]). However, their numbers increase with the index of U in G. If one had a method to reduce these numbers effectively in cases where this is theoretically possible, the Todd-Coxeter procedure could be applied again to the subgroup U and so on. No programme of this kind seems to exist yet.

Another application of the Todd-Coxeter technique was outlined by C. C. Sims [Si 3]. By systematically enumerating the words that could generate a subgroup and performing Todd-Coxeter computations for them, he finds all subgroups of index less than a prescribed bound in a finitely presented group.

3.2. ***Generation of groups, lattice of subgroups.*** A number of programmes have been developed to compute structural details for a finite group given by a set of generators. In all these programmes problems arise at three levels.

3.2.1. First, algorithms for the handling, i.e. comparison, multiplication, inversion, etc., of the group elements must be defined. These are rather obvious if the elements (and hence in particular the generators given as input to the programme) are permutations, matrices over some ring, affine transformations, etc. If, however, generators and defining relations are given, the insolubility of the word problem does not allow general handling of words in the generators unless the relations are of a restricted type. If this is not the case, the only way out is to try to get a faithful permutation representation of the group by the Todd-Coxeter procedure. If the generators are taken from the factors of a subnormal series of a soluble group, the relations can be brought into a simple form [Ju **1**]. Then by a kind of compiler the computer itself constructs optimal programmes for the handling of normal forms from these relations. Programmes of this kind are described in [Li 1, 2; Jü 1; Ne 2].

3.2.2. Next, algorithms for the generation of all elements of a finite group G from its generators $g_1, \ldots, g_n$ are needed. If the store of the machine is big enough to hold all elements of G, the following simple method [Ne 1; We **1**] can be used. Beginning with $U_0 = (I)$, form $U_{i+1} = \langle U_i, g_{i+1}\rangle$ by the following procedure, given in slightly simplified form here. Form $U_i^1 = U_i \cup U_i g_{i+1}$; beginning with $1 \in U_i$, multiply all elements in U_i^1 from the left by g_{i+1} until an element $g^* \notin U_i^1$ is obtained. Then replace U_i^1 by $U_i^2 = U_i^1 \cup U_i g^*$ and repeat the procedure. When left-multiplication of an U_i^j with g_{i+1} yields only elements in U_i^j, we have found ($U_i, g_{i+1}\rangle$. The condition, to keep all elements in a (fast-access) store, is a serious restriction. J. K. S. McKay [Mc **2**] mentions a variation of the method in which only the elements u of a subgroup U and coset representatives c of U in G are stored and all elements are expressed (uniquely) as products UC. This procedure saves store, but at the cost of computing time for the regeneration of elements by multiplication. In general no essentially better method seems to be known.

For permutation groups, however, a more effective and store-saving method exists [Si **3**]. Let G be a group of permutations of the integers $1, \ldots, n$ and let G_i be the stabilizer of $1, 2, \ldots, i$, $G_0 = G$. Then coset representatives are determined for all steps G_i, G_{i+1}. From the cycle-decomposition of the generators of G all images of 1 under G and hence coset representatives of G_1 in G are found. By the Schreier technique generators of G_1 can now be computed and the same process repeated for G_1. The problem is, to keep the number of generators small for all steps. This is done by working at all steps simultaneously and reducing the number of generators, obtained by the Schreier process for a subgroup U, by using the coset representatives of the subgroups of U which are already known at the time.

This method has been programmed by C. C. Sims [Si **3**], and in similar form by P. Swinnerton-Dyer (unpublished) in helping with M. Hall's computation [Ha **5**] of generating permutations for a simple group of Z Janko [Ja **2**]; another such programme is presently being worked out at Kiel. Sims' programme determined a permutation group of order about

5×10^8 in a very small time; he estimates that it can find the order of any permutation group of degree $\leqslant 200$ with a "small" number of generators.

3.2.3. When all elements of a finite group have been found, the next problem is to investigate its subgroups and their properties. A number of programmes have been developed for the determination of the lattice of subgroups together with conjugacy relations between the subgroups. W. D. Maurer [He 1; Ma **5, 6, 7, 8, 9**], and apparently similarly G. P. Spielman [Sp 1], have put their main interest in defining a simple language in which the user can give orders or ask questions to be checked against a file of examples. The programmes are mainly for demonstration, so the methods used are rather straightforward and hardly powerful enough to handle more complicated examples efficiently.

A more sophisticated combinatorial approach has been used by L. Gerhards and W. Lindenberg [Ge 3; Li **3**]. Basically their programme works as follows : A subgroup U of a finite group G is uniquely determined by the set of cyclic subgroups of prime power order contained in U. Hence U can be described by the characteristic function c_U, defined on the set S of all cyclic subgroups of prime power order in G, which is equal to 1 for the cyclic subgroups contained in U and equal to 0 for all others. Any characteristic function on S defines a generating system for some subgroup, hence all characteristic functions are considered in lexicographical order. Once a subgroup has been generated from a characteristic function, by a number of combinatorial tricks based on simple group theoretic arguments many other characteristic functions can be eliminated from being examined, as they define generating systems of subgroups already known.

Another mainly combinatorial method has been outlined by C. C. Sims [Si **3**]. The elements of G are ordered in a list L: $1 = g_1, g_2, \ldots, g_{|G|}$. Then for each subgroup U a canonical system of generators $x_1, \ldots, x_r$ is defined by the requirement that x_1 is the first element of U-(1) with respect to the order in L, x_{i+1} is the first element of $U - \langle x_1, x_2, \ldots, x_i \rangle$ with respect to this order. The task of finding all subgroups is thus equivalent to that of finding all canonical systems. If $\{x_1, \ldots, x_k\}$ is such a system, then so is $\{x_1, \ldots, x_{k-1}\}$. Hence, if all ordered systems of elements are ordered first by their length then, lexicographically, a system $\{x_1, \ldots, x_k\}$ can be discarded in the search for canonical systems if either $\{x_1, \ldots, x_{k-1}\}$ is not canonical or if in calculating the subgroup it generates an element not in $\langle x_1, \ldots . x_{k-1} \rangle$ is obtained that is earlier in L than x_k. This method has not been programmed yet, but it seems likely that it is rather efficient, in particular if there is some natural order of the elements which can be decided upon without searching in lists.

Added in proof, July 1968. Yet another combinatorial programme is at present being developed by W. Niegel at the Technische Hochschule, Miinchen.

A method involving more group theory has been used by J. Neubüser and V. Felsch [Fe 5,6; Ne 1,2] and in similar form by J. Cannon [Ca 3] and by D. R. Hayes and L. C. Biedenharn (unpublished). Subgroups are again represented by their characteristic functions on the set of all cyclic subgroups of prime power order (see above). Let the kth layer& of the lattice of subgroups consist of all subgroups whose order is the product of k primes. A subgroup $U \in \Sigma_i$ different from its derived group U' is obtained as a product of a group $V \in \Sigma_{i-1}$ by a cyclic subgroup $C \subseteq N_G(V)$ of prime power order. If the subgroups are constructed layerwise, starting from& one can ensure by simple calculation with characteristic functions (which can be handled nicely in a binary computer) that each subgroup is constructed only once. Perfect subgroups are taken care of by special subroutines for each of the very few isomorphism types of simple groups of composite order that can occur in the range of orders allowed by storage and speed restrictions of the computer presently used. These subroutines can be extended for bigger machines, as the list of all simple groups is known at least up to order 20,000. This means that the programme would work at least up to groups of order 40,000, which at present is definitely out of reach for any programme of the kinds discussed here that determines the full lattice of subgroups.

Although more combinatorial programmes have the advantage that there is no theoretical restriction for their applicability, comparison has shown the programmes described last to be more efficient than the existing combinatorial ones. With the present implementation groups up to order 1092 and with up to 2400 subgroups have been handled. Its range will be increased in a new implementation (in the final debugging state Oct. 1967) which on a bigger computer uses a 512 K backing store.

Added in proof, July 1968. This programme now works, and has produced the lattices of subgroups of groups including the alternating group A_7 (order 2520, with 3779 subgroups) and the largest of Dade's groups [Da 1] (order 1152, with 519 1 subgroups).

A special programme [Fe 9] for drawing a diagram of the lattice has been connected with the system of programmes in Kiel [Fe 5,6].

3.2.4. For many problems, such as the determination of crystal classes [Bü 1, 2], it is sufficient to determine only one representative from each class of conjugate subgroups in G. A certain variation of the method described in [Fe 5,6; Ne 1] is presently being programmed in Kiel. It will save a large amount of store at a (hopefully slight) cost of time. It seems that the more combinatorial algorithms cannot very easily be adapted to this purpose.

3.2.5. Together with the lattice of subgroups, some of these programmes [Fe 5,6; Ge 3; Li 3] compute properties of subgroups, etc. It is listed, e.g. by the Kiel programme [Fe 5,6], whether a subgroup U is cyclic, abelian, nilpotent, supersoluble, soluble or perfect and whether it is normal, subnormal or self-normalizing in G. The order, normalizer, centralizer and classes of conjugate elements of U are found. Also certain characteristic subgroups such as the upper and lower central series, commutator series Frattini and Fitting subgroups are determined.

3.2.6. Two sets of programmes developed by R. Yates [Ya **1**] and R. Segovia and H. V. McIntosh [Se **1**] determine the lattice of subgroups and some of these structural details for groups of special types.

3.2.7. Some more extensive applications of such programmes have been made. R. Biilow and J. Neubtiser [Bü **1, 2**] determined all integral classes of 4×4 integral matrix groups by analysing the 9 classes of maximal 4 **X** 4 integral groups, found by E. C. Dade [Da **1**]. A catalogue of the lattices of subgroups, etc., of the groups of order $\leqslant$ 100, omitting orders 64 and 96, has been compiled by J. Neubtiser [Ne **3**] using the Kiel programmes.

3.3. Automorphism groups. W. D. Maurer's system of programmes [Ma 8] also contains a programme which checks for the existence of an isomorphism between two given groups by constructing partial isomorphisms in a tree-of-trial-and-error procedure. Programmes for detecting isomorphisms of graphs [Be 2; Su I] may also be used in such a way.

The only programme known to me [Fe 5,7, 8] for the determination of the automorphism group $A(G)$ of a finite group G uses the structural data obtained by the subgroup lattice programme [Fe 5,6]. The basic idea is that an automorphism induces a lattice automorphism on the lattice of subgroups which preserves order, conjugacy, centralizers, etc. If a subgroup U is chosen it is usually rather easy by visual inspection of a diagram representing the lattice of subgroups to find all candidates for images of U under automorphisms of G. This vague idea has been made precise by introducing and studying certain equivalence relations on the set of all subgroups which are then used in the construction of $A(G)$.

For a soluble group which is not of prime power order L. Gerhards [Ge 2] gives an outline of a programme based on P. Hall's results [Ha 8] about Sylow systems. In this programme (which is not yet implemented) the automorphism group of G will be constructed from "extensible" automorphisms of the Sylow subgroups in a Sylow system and inner automorphisms.

3.4. Characters and representations.

3.4.1. There are a number of programmes for the determination of the absolutely irreducible characters of a finite group G. Most of these start from the class multiplication coefficients and lead to some kind of numerical computation. For the theoretical background to this procedure see e.g. [Cu 1].

Let Cl, ... C_r be the classes of conjugate elements in G, $C_1 = \{1\}$, h_i the number of elements in C_i, $\chi^1, \ldots, \chi^r$ the absolutely irreducible characters, d_j the dimension of χ^j, and χ_i^j the value of χ^j for an element of C_i. The class multiplication coefficients are defined by

$$C_i C_j = \sum_{k=1}^{r} c_{ijk} C_k.$$

Defining $w_i^s = \frac{h_i}{d_s} \chi_i^s$ one has $w_i^s w_j^s = \sum_{k=1}^{r} c_{ijk} w_k^s$. Henceforeachs, $1 \leqslant s \leqslant r$, the r values $w_l^s, 1 \leqslant l \leqslant r$, belonging to the sth character satisfy the r^2 equations

$$\sum_{k=1}^{r} (c_{ijk} - \delta_{ik} x_j) x_k = 0 \text{ for } 1 \leqslant i, \mathrm{j} \leqslant r. \qquad (*)$$

Considering for each $j_0, 1 \leqslant j_0 \leqslant r$, in turn the r equations obtained by fixing j = j_0, one sees that the vector $w^s = (w_1^s, \ldots, w_r^s)$ is an eigenvector of the matrix (c_{ij_0k}) belonging to the eigenvalue $w_{j_0}^s$, and further that these vectors w^s, $1 \leqslant s \leqslant r$, are (up to factors) the only common eigenvectors of all these matrices $(c_{ij_0k}), 1 \leqslant j_0 \leqslant r$.

3.4.2. [Cu 1]: If for a certain j_0 the matrix (c_{ij_0k}) has r different eigenvalues, the eigenvector spaces are one-dimensional and hence yield uniquely (up to scalar multiples) the vectors $w^s, 1 \leqslant s \leqslant r$. These factors are determined from $w_1^s = \frac{h_1}{d_s} \chi_1^s = 1$. From the orthogonality relations of the characters one has

$$d_j^2 \sum_{i=1}^{r} \frac{w_i^j \overline{w_i^j}}{h_i} = |G|.$$

From this $d_1, \ldots, d_r$ are found and then the characters. As there are simple examples in which none of the matrices (c_{ij_0k}) has r distinct eigenvalues, this method is not always applicable.

Essentially this method is applied for all matrices (c_{ij_0k}) in a programme by S. Flodmark and E. Blokker [F13] to obtain irreducible characters. These are then used to reduce the regular representation into representations $E_1, \ldots, E_r$ of degree $d_1^2, \ldots. d_r^2$ respectively. E_j contains the d_j copies of the jth absolutely irreducible representation that are contained in the regular representation. For further reduction of the E_j into irreducible representations, according to a private communication of S. Flodmark, a "numerical iteration procedure" is used. The author regrets that he cannot supply details about this, as he heard about the programme only when this article had already gone to press.

3.4.3. For hand computation W. Burnside [Bu I] gives the following method: Multiplying the equations (*) with a fixed j by an indeterminate y_j and summing over all j yields

$$\sum_{k=1}^{r} \left(\sum_{j=1}^{r} c_{ijk} y_j - \delta_{ik} \sum_{j=1}^{r} x_j y_j \right) x_k = 0.$$

For $1 \leqslant s \leqslant r$, w^s is an eigenvector of $\left(\sum_{j=1}^{r} c_{ijk}y_j\right)$ belonging to the eigenvalue ii.” $= \sum_{j=1}^{r} w_j^s y_j$. These eigenvalues λ^s are r different solutions, and hence are all the solutions, of the characteristic equation

$$\det\left(\sum_{j=1}^{r} c_{ijk}y_j - \delta_{ik}\lambda\right) = 0.$$

If one can factor this as a polynomial in λ with coefficients from the ring of polynomials in the indeterminates $y_1, \ldots, y_r$, one has found the w_j^s and hence the characters.

3.4.4. J. K. S. McKay [Mc **2**, 3] in his programme replaces the indeterminates y_j by random numbers a_j of uniform distribution in [0, 1] and proceeds for the matrix $(c_{ik}^*) = \left(\sum_{j=1}^{r} c_{ijk}a_j\right)$ as described in § 3.4.2 for a single (c_{ij_0k}). The set of r-tuples $(a_1, \ldots, a,)$ for which (c_{ik}^*) has multiple eigenvalues is of measure zero in the hypercube of all r-tuples, but numerical difficulties can occur if two eigenvalues are close together. Restrictions on the programme are given by the number of classes in G rather than by the order of G, as long as the c_{ijk} can be calculated. McKay has been able [Mc 3] to recalculate the character-table of Z. Janko’s first simple group [Ja **1**] from a matrix representation of it.

3.4.5. One can also use the property that the w’s are the only common eigenvectors of the matrices (c_{ij_0k}), $1 \leqslant j_0 \leqslant k$, in the following way. First the eigenvector spaces of (c_{i2k}) are determined. After n- 1 steps let $V_1, \ldots, V_s$ be the subspaces of common eigenvectors of the matrices $(c_{i2k}), \ldots, (c_{ink})$. Then each V_i of dimension $\geqslant 2$ is mapped by $(c_{i\,n+1\,k} - \delta_{ik}\lambda_j^{n+1})$, where λ_j^{n+1} runs through all eigenvalues of $(c_{i\,n+1\,k})$, and thus split into a direct sum of subspaces of common eigenvectors of $(c_{i2k}), \ldots, (c_{i\,n+1\,k})$.

In the programme of J. D. Dixon [Di 1] this procedure is further simplified and the calculation of eigenvalues is avoided in the following way. Let e be the exponent of G, ε a fixed primitive eth root of unity, and p a prime such that $e|p-1$. Then there is an integer z such that z has order e modulo p. The mapping $\Theta : f(\varepsilon) \to f(z)$, where f is any polynomial with integral coefficients, is a ring homomorphism of $Z(\varepsilon)$ onto the prime field Z_p, which can be used to translate the whole problem of finding common eigenvectors into the corresponding one over Z_p. This can be solved much more easily. By choosing p appropriately one can ensure that the characters in the complex field can be determined from the solutions found in Z_p.

3.4.6. D. R. Hayes [Ha **9**] has proposed to solve (*) by constructing successively partial solutions in a kind of tree-of-trial-and-error procedure. The method described by him has not yet been programmed.

3.4.7. A rather different approach has been used by C. Brott and J. Neubiiser [Br 1,2]. In their programme all monomial absolutely irreducible representations are found as induced representations of one-dimensional representations of certain subgroups and the corresponding characters as induced characters. For a big class of finite groups, including all p-groups, all absolutely irreducible representations are monomial; if this is not the case for a group G the remaining characters are found by one of the methods described above, taking advantage however of the characters already known.

For groups of order 2^n, another programme to find the absolutely irreducible representations by the process of induction has been written by P. G. Ruud and E. R. Keown [Ke 1; Ru 1,2].

Added in proof, July 1968, According to the summary printed in ***Mathematical Reviews,*** N. N. Aĭzenberg and A. A. Letičevskiĭ [Ai 1] "have developed algorithms for computing matrix representations and characters of an interesting class of finite groups".

3.4.8. All these programmes require that the group is completely known in some detail. However in many hand computations, e.g. [Fr 1; Ja 1, 2], character tables are found from rather poor information about the group, in fact the character table is used as a step in establishing the existence of a group with certain properties. It seems to be very worth while to build up a programme, possibly for on-line use and man-machine interaction from a remote console, which would incorporate the routine computations used in such work.

3.4.9. Added in proof, July 1968. In their proof of the existence of Janko's group of order 50 232 960, G. Higman and J. K. S. McKay [Hi 2] use some programmes which find rational and permutation characters from a given character table.

3.5. Miscellaneous programmes.

3.5.1. In [Ha 6] P. Hall introduced the so-called "commutator collecting process" for the study of an expansion

$$(gh)^n = g^n h^n [g, h]^{\varphi_1(n)} \dots$$

of the nth power of a product of two group elements into a product of certain commutators. He showed in particular that the functions $\varphi_i(n)$ are polynomials in n of degree not exceeding the weight of the commutator whose exponent they are. Hall's formula has been the object of a few programmes. A very straightforward simulation of the collection process was used by H. Felsch [Fe 2] to obtain the $\varphi_i(n)$ for the first few i. J. M. Campbell and W. J. Lamberth [Ca 2] have more recently written a more elaborate programme for the same purpose as a tool for the investigation of free nilpotent groups of finite exponent. E. F. Krause [Kr 1,2] has used some theoretical improvement of the collecting process to study groups of exponent 8. Together with K. Weston [Kr. 3,4] he studied a similar process in Lie rings and applied a programme for it in the study of Burnside groups of exponent 5. D. W. Walkup [Wa 1] announces that he has used a computer (in a way not further described) to show that a certain commutator identity is best possible.

3.5.2. H. J. Bernstein, 0. Moller and E. Strasser Rapaport [Be 3] describe a programme for finding factorizations of finite groups.

3.5.3. D. A. Smith [Sm 1] gives an algorithm for the determination of a basis of a finitely generated abelian group.

4. Acknowledgements. The author wishes to express his indebtedness to Mr. C. Brott, Mr. V. Bülow, Mr. V. Felsch and Mr. J. K. S. McKay for help in compiling and preparing the material for this article and to the editor of these proceedings who patiently waited for its completion.

REFERENCES

Ai 1. N. N. Aĭzenberg and A. A. Letičevskiĭ: On computing on "ECM" representations of wreath-products of finite groups. *Kibernetika (Kiev)* 1965, no. 3, 63-71; *Math. Rev. 35* (1968), 4315.

Al 1. S. L. Altmann and C. J. Bradley: A note on the calculation of the matrix elements of the rotation group. *Phil. Trans. Roy. Soc. London* (A) 255 (1962/63), 193-198.

Al 2. S. L. Altmann and C. J. Bradley: On the symmetries of spherical harmonics. *Phil. Trans. Roy. Soc. London* (A) 255 (1962/63), 199-215.

Ap 1. K. Appel, M. Hall jr. and J. Thompson: A search for simple groups of odd order. *Notices American Math. Soc. 8* (1961), 364.

Ap 2. K. I. Appel and E. T. Parker : On unsolvable groups of degree $p = 4q + 1$, p and q prime. *Canad. J. Math.* 19 (1967), 583-589.

Ba 1. P. A. Bandler: M.A. Thesis, Manchester, 1956.

Be 1. C. T. Benson and N. S. Mendelsohn: A calculus for a certain class of word problems in groups. *J. Combinatorial Theory* 1(1966), 202-208.

Be 2. R. Berger: A computer method for testing for isomorphism between finite groups. Mimeographed report for applied mathematics 220. Harvard Univ. (1962).

Be 3. H. J. Bernstein, 0. Moller and E. Strasser Rapaport: Machine factorization of groups. *Mathematical Algorithms* 1.3 (1966), 39-51.

Bi 1. R. L. Bivins, N. Metropolis, P. R. Stem and M. B. Wells: Characters of the symmetric groups of degree 15 and *16. Math. Tables and other Aids to Computation 8* (1954), 212-216.

Br 1. C. Brott: Ein Programm zur Bestimmung absolut irreduzibler Charaktere und Darstellungen endlicher Gruppen. Diplomarbeit, Kiel, 1966.

Br 2. C. Brott and J. Neubüser: A programme for the calculation of characters and representations of finite groups. These Proceedings, pp. 101-1 10.

Bu 1. W. Burnside: *Theory of Groups of Finite Order* (Cambridge Univ. Press, 1911).

Bü 1. R. Bülow and J. Neubüser: On some applications of group-theoretical programmes to the derivation of the crystal classes of *R*,. These Proceedings, pp. 131-135.

Bü 2. R. Bülow: Eine Ableitung der Kristallklassen im R_4 mit Hilfe gruppentheoretischer Programme. Diplomarbeit, Kiel, 1967.

Ca 1. C. M. Campbell: Some examples using coset enumeration. These Proceedings, pp. 37-41.

Ca 2. J. M. Campbell and W. J. Lamberth: Symbolic and numeric computation in group theory. ***Proc. 3rd Austral. Comp. Conf. 293-296,*** Canberra, May 1966.

Ca 3. J. Cannon: Some combinatorial and symbol manipulation programs in group theory. These Proceedings, pp. 199-203.

Co 1. S. Comét: On the machine calculations of characters of the symmetric group. ***Comptes Rendus, 12me Congres math. Scand.*** Lund, 1953 (1954), 18-23.

Co 2. S. Comét: Notations for partitions. ***Math. Tables and other Aids to Computation 9 (1955),*** 143-146.

Co 3. S. Comét: Über die Anwendung von Binärmodellen in der Theorie der Charaktere der symmetrischen Gruppen. ***Numer. Math.*** 1(1959), 90-109.

Co 4. S. Comét: Improved methods to calculate the characters of the symmetric group. ***Math. Comp.*** 14 (1960), 104-117.

Co 5. S. Comét: Character tables for $N\leqslant 20$ of the symmetric groups S_N. Kept in the library of Matematikmaskinnlmnden, P.O. Box 6131, Stockholm 6, Sweden.

Co 6. H. S. M. Coxeter and W. 0. J. Moser: ***Generators and Relations for Discrete Groups,*** 2nd ed. (Springer, Berlin, Göttingen, Heidelberg, 1965).

Cu 1. C. W. Curtis and J. Reiner: ***Representation Theory of Finite Groups and Associative Algebras*** (Interscience, New York, 1962).

Da 1. E. C. Dade: The maximal finite groups of 4 ×4 integral matrices. ***Illinois J. Math. 9*** (1965), 99-122.

De 1. J. Dénes: Bibliography on application of digital computers in abstract algebra. Mimeographed extract 1967 of: A bibliography on non-numerical applications of digital computers. ***Comput. Rev. 9*** (1968), 481-508.

Di 1. J. D. Dixon: High speed computation of group characters. ***Numer. Math.*** 10 (1967), 446-450.

El 1. H. Eltermann: Programmierung des Coxeter-Moser-Verfahrens zur Abzählung der Restklassen einer Gruppe nach Untergruppen auf Grund von definierenden Relationen. ***Mitt. Rh.- W. Inst. Znstr. Math. Bonn 2*** (1963), 105-108.

Fa 1. G. Fast and T. W. Janssen: Non-equivalent four-dimensional generalized magnetic space-time groups. Technical Report. Institute for Theoretical Physics, University of Nijmegen, 1967.

Fe 1. H. Fell, M. Newman and E. Ordman: Tables of genera of groups of linear fractional transformations. ***J. Res. Nat. Bur. Standards,*** Sect. B, 67B (1963), 61-68.

Fe 2. H. Felsch: Die Behandlung zweier gruppentheoretischer Verfahren auf elektronischen Rechemnaschinen. Diplomarbeit, Kiel, 1960.

Fe 3. H. Felsch: Programmierung der Restklassenabzählung einer Gruppe nach Untergruppen. ***NumerMath. 3*** (1961), 250-256.

Fe 4. H. Felsch, J. Neubüser and R. Rumberger: Gewinnung einer Permutationsdarstellung einer Gruppe aus definierenden Relationen. ***Mitt. Rh.- W. Inst. Znstr. .Math. Bonn 2 (1963),*** 75-104.

Fe 5. V. Felsch: Ein Programm zur Berechnung des Untergruppenverbandes und der Automorphismengruppe einer endlichen Gruppe. Diplomarbeit, Kiel, 1963.

Fe 6. V. Felsch and J. Neubüser: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. ***Mitt. Rh.- W. Inst. Znstr. Math. Bonn 2*** (1963), 39-74.

Fe 7. V. Felsch and J. Neubüser: Über ein Programm zur Berechnung der Automorphismengruppe einer endlichen Gruppe. ***Numer. Math.*** 11(1968), 277-292.

Fe 8. V. Felsch and J. Neubüser: On a programme for the determination of the automorphism group of a finite group. These Proceedings pp. 59-60

Fe 9. K. FERBER and H. JÜRGENSEN: A programme for the drawing of lattices. These Proceedings, pp. 83-87.

Fl 1. S. FLODMARK: Theory of symmetry projections in applied quantum mechanics. *Phys. Rev.* 132 (1963), 1343-1348.

Fl 2. S. FLODMARK: Symmetry projection program. Mimeographed notes, Stockholm, 1964.

Fl 3. S. FLODMARK and E. BLOKKER: A computer program for calculation of irreducible representations of finite groups. ***Znternat. J. Quantum Chem. Symposium*** 1 (1967), 703-711.

Fr 1. J.S. FRAME: The characters of the Weyl group E_8. These Proceedings, pp. 111-130.

Ge 1. I. M. GEL'FAND and Z. Y. ŠAPIRO: Representations of the group of rotations of 3-dimensional space and their applications. Uspehi ***Mat. Nauk (N.S.) 7 (47)*** (1952), 3-117; ***A.M.S. Transl. (2) 2*** (1956), 207-316.

Ge. 2. L. GERHARDS and E. ALTMANN: A computational method for the determination of the automorphism group of a finite solvable group. These Proceedings, pp. 61-74.

Ge 3. L. GERHARDS and W. LINDENBERG: Ein Verfahren zur Berechnung des vollständigen Untergmppenverbandes endlicher Gruppen auf Dualmaschinen. ***Numer. Math. 7*** (1965), 1-10.

Gu 1. M. J. T. GUY: Coset enumeration. Lecture delivered at the Conference on Computational Problems in Abstract Algebra, Oxford, 29 Aug.-2 Sept. 1967.

Ha 1. M. HALLJR.: Discrete variable problems, pp. 518-542 of J. Todd (ed.), ***A Survey of Numerical Analysis*** (McGraw Hill, New York, San Francisco, Toronto, London, 1962).

Ha 2. M. HALL JR. and D. E. KNUTH: Groups of exponent ***4. Notices American Math. Soc.*** 11 (1964), 120-121.

Ha 3. M. HALL JR.: Generators and relations in groups-The Burnside problem, pp. ***42-92*** of T. L. Saaty ***(ed.), Lectures on Modern Mathematics II (Wiley, New*** York, London, Sydney, 1964).

Ha 4. M. HALL JR. and D. E. KNUTH: Combinatorial analysis and computers. ***Amer. Math. Monthly 72*** II (1965), 21-28.

Ha 5. M. HALL JR.: A search for simple groups of order less than one million. These Proceedings, pp. 137-168.

Ha 6. P. HALL: A contribution to the theory of groups of prime power order. ***Proc. London Math. Soc. (2) 36*** (1933), 29-95.

Ha 7. P. HALL: The classification of prime power groups. ***J. reine angew. Math.*** 182 (1940), 130-141.

Ha 8. P. HALL: On the Sylow systems of soluble ***groups. Proc. London Math. Soc. (2)*** 43 (1937), 316-323.

Ha 9. D. R. HAYES: The calculation of the character-table of a given finite group. Mimeographed notes, 1963.

He 1. W. HENNEMAN: Note on "An algebraic substructure algorithm". ***Mathematical Algorithms 1.2 (1966), 40.***

Hi 1. G. HIGMAN: The orders of relatively free groups. ***Proc. Znternat. Conf. Theory of Groups. Austral. Nat. Univ. Canberra,*** August 1965,153-165.

Hi 2. G. HIGMAN and J. MCKAY: On Janko's simple group of order 50 232 960. ***Bull. London Math. Soc.*** 1 (1969), 89-94.

Hu 1. D. R. HUGHES: A problem in group theory. Research problem ***3. Bull. American Math. Soc. 63 (1957), 209.***

Hu 2. D. R. HUGHES and J. G. THOMPSON: The ***Hp***-problem and the structure of ***Hp***-groups. ***Pacific J Math.*** 9 (1959), 1097-1101.

Ja 1. Z. JANKO: A new finite group with abelian 2-Sylow subgroups. ***Proc. Nat. Acad.*** Sci. U.S.A. 53 (1965), 657-658.

Ja 2. Z. JANKO: Still one more new simple group of finite order. Mimeographed notes, Melbourne, 1967.

Jü 1. H. Jürgensen: Calculation with the elements of a group given by generators and defining relations. These Proceedings, pp. 47-57.

Ka 1. S. Katsura: Tables of representations of permutation groups for the many electron problem. Unbound report, Eugene, Oregon, 1962, available as: Document No 7567 AD1 Auxiliary Publications Project, Lib of Congr., Washington, D.C.

Ka 2. S. Katsura: Tables of representations of permutation groups for molecular integrals. J. *Chem. Phys. 38* (1963), 3033.

Ke 1. E. R. Keown: The ordinary representations of the groups of order 2^n, $1 \leq n \leq 6$. *Notices American Math. Soc.* 14 (1967), 116.

Kr 1. E. F. Krause: On the collection process. *Proc. American* Math. *Soc.* 15 (1964), 497-504.

Kr 2. E. F. Krause: Groups of exponent 8 satisfy the 14th Engel congruence. *Proc. American Math. Soc.* 15 (1964), 491-496.

Kr 3. E. F. Krause and K. Weston: The restricted Burnside group of exponent 5. *Notices American Math. Soc.* 14 (1967), 416-417.

Kr 4. E. F. Krause and K. Weston: An algorithm related to the restricted Burnside group of prime exponent. These Proceedings, pp. 185-187.

Le 1. J. Leech: Some definitions of Klein's simple group of order 168 and other groups [with Appendix]. *Proc. Glasgow Math. Assoc. 5 (1962),* 166-175.

Le 2. J. Leech: Coset enumeration on digital computers. *Proc. Cambridge Phil. Soc.* 59 (1963), 257-267; with supplementary notes and references, privately circulated 1967.

Le 3. J. Leech: Generators for certain normal subgroups of *(2,3,7). Proc. Cambridge Phil. Soc.* 61 (1965), 321-332.

Le 4. J. Leech: Coset enumeration. These Proceedings, pp. 21-35.

Li 1. W. Lindenberg: Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten. *Numer. Math.* 4 (1962), 151-153.

Li 2. W. Lindenberg: Die Struktur eines Übersetzungsprogramms zur Multiplikation von Gruppenelementen in digitalen Rechenautomaten. *Mitt. Rh.- W. Inst. Instr. Math. Bonn 2 (1963),* 1-38.

Li 3. W. Lindenberg and L. Gerhards: Combinatorial construction by a computer of the set of all subgroups of a finite group by composition of partial sets of its subgroups. These Proceedings, pp. 75-82.

Li 4. A. Liulevicius: Coalgebras, resolutions, and the computer I, II, III. *Mathematical Algorithms* 1.1 (1966) 4-12; 1.2 (1966) 2-10; 1.4 (1966) 1-68.

Ma 1. M. D. MacLaren: Notes on the machine computation of a spectral sequence. Argonne Nat. Lab. Working paper (1965), 26 pp.

Ma 2. M. D. MacLaren and M. E. Mahowald: Topological calculations by machine. Argonne Nat. Lab. Working paper (1966), 14 pp.

Ma 3. R. N. Maddison: Diploma Dissertation, Cambridge, 1958.

Ma 4. W. MAGNUS, A. Karrass and D. Solitar: *Combinatorial Group* Theory (Interscience, New York, London, Sydney 1966).

Ma 5. W. D. Maurer: Computer experiments in finite groups. Brown University (1965), 30 pp.

Ma 6. W. D. Maurer: Computer experiments in finite algebra. *Project MAC, M.Z.T. Memorandum MAC M 246* (1965), 17 pp.

Ma 7. W. D. Maurer: Computer experiments in finite algebra II. *Project MAC, M.I.T. Memorandum MAC M 282* (1965), 39 pp.

Ma 8. W. D. Maurer: Computer experiments in finite algebra. *Project MAC, M.Z.T. (1966), 19* pp. *Comm. Assoc. Comp. Mach. 9 (1966), 598-604.*

Ma 9. W. D. Maurer: An algebraic substructure algorithm. *Mathematical Algorithms* 1.1 (1966), 101-113.

Mc 1. J. K. S. McKay: Symmetric group characters. Algorithm 307. Comm. *Assoc. Comp. Mach.* 10 (1967), 451-452.

Mc 2. J. K. S. McKay: A method for computing the simple characters of a finite group. Mimeographed notes, 1966.

Mc 3. J. K. S. **McKay:** The construction of the character table of a finite group from generators and relations. These Proceedings, pp. 89-100.

Me 1. **N. S Mendelsohn:** An algorithm for the solution of a word problem. ***Notices American Math.*** *Soc.* 11 (1964), 137.

Me 2. **N. S. Mendelsohn:** An algorithmic solution for a word problem in group theory. *Canad.* J. Math. 16 (1964), 509-516; Review by W. 0. J. Moser, ***Math. Rev. 29*** (1965), 1248; Correction: *Canad.* J. *Math.* 17 (1965), 505; Corrected copy: University of Manitoba, Reprint series 1966/l, Winnipeg.

Me 3. **N. S. Mendelsohn:** Some examples of man-machine interaction in the solution of mathematical problems. These Proceedings, pp. 217-222.

Me 4. **N. S. Mendelsohn:** Defining relations for subgroups of finite index of groups with a finite presentation. These Proceedings, pp. 43–44.

Mo1. W. 0. J. **Moser:** Coset enumeration used to solve a word problem in groups. *Notices American Math. Soc.* 13 (1966), 245.

Mo 2. W. 0. J. **Moser:** On the Todd-Coxeter and Reidemeister-Schreier methods. Lecture delivered at the Conference on Computational Problems in Abstract Algebra Oxford, 29 Aug.-2 Sept. 1967.

Ne 1. J. Neubüser : Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine. ***Numer. Math. 2*** (1960), 280-292.

Ne 2. J. Neubüser: Bestimmung der Untergruppenverblnde endlicher p-Gruppen auf einer programmgesteuerten elektronischen Duahnaschine. ***Numer. Math. 3*** (1961), 271-278.

Ne 3. J. Neubüser: Die Untergruppenverblnde der Gruppen der Ordnungen $\leqslant$ 100 mit Ausnahme der Ordnungen 64 und 96. Habilitationsschrift, Kiel, 1967.

Ne 4. M. H. A. **Newman:** The influence of automatic computers on mathematical methods. ***Manchester University Computer Inaugural Conference (1951),*** 13.

No 1. L. M. **Norton:** ADEPT. A heuristic program for proving theorems of group theory. Ph.D. Thesis, MIT (1966), MAC TR 33.

Pa 1. G. **Pall** and E. **Seiden**: A problem in abelian groups, with application to the transposition of a matrix on an electronic computer. ***Math. Comp.*** 14 (1960), 189-192.

Pa 2. E. T. **Parker** and P. J. **Nikolai:** A search for analogues of the Mathieu groups. ***Math. Comp.*** 12 (1958), 3843.

Pe *1.* W. W. Peterson: ***Error-correcting Codes. New*** York, 1961.

Pi 1. T. B. Pinkerton: An algorithm for the automatic computation of integral homology groups I, II. ***Mathematical Afgorithms*** 1.1 (1966), 36-66; 1.2 (1966), *33-39.*

Ro 1. G. de B. **Robinson:** ***Representation Theory of the Symmetric Group*** (Univ. of Toronto Press, 1961).

Ru 1. P. G. Ruud and E. R. Keown: Representations of groups of order 32. ***Notices American Math.*** *Soc.* 14 (1967), 281.

Ru 2. P. G. **Ruud** and E. R. **Keown:** The computation of irreducible representations of finite groups of order 2^n, $n \leqslant 6$. These Proceedings, pp. 205-216.

Sa 1. J. E. Sammet: Survey of use of computers for doing non-numerical mathematics. IBM, TR-00.1428, Poughkeepsie, N.Y.

Sa 2. J. E. Sammet: An annotated descriptor-based bibliography on the use of computers for doing non-numerical mathematics. IBM, TR-00.1427, Poughkeepsie, N.Y.; and ***Comput. Rev. 7 (1966).***

Sa 3. J. E. Sammet: Modification No. 1 to "An annotated descriptor-based bibliography on the use of computers for doing non-numerical mathematics". Appendix to ***SZCSAM Bulletin*** *5* (1966).

se 1. R. SEGOVIA and H. V. MCINTOSH: *Computer Analysis of Finite Groups.* Inst. Politecnico Nacional, Mexico, 1966.

se 2. E. S. SELMER: Translation-invariant permutation groups. Mimeographed notes, Bergen, 1966.

Si 1. C. C. SIMS: On the group *(2, 3, 7; 9). Notices American Math. Soc.* 1 1 (1964), 687-688.

Si 2. C. C. SIMS: The primitive groups of degree not exceeding 20. Mimeographed notes, 1967.

Si 3. C. C. SIMS: Computational methods in the study of groups. Lecture delivered at the Conference on Computational Problems in Abstract Algebra, Oxford, 29 Aug.-2 Sept. 1967. (This lecture included material not in [Si **4**].)

Si 4. C. C. Sims: Computational methods in the study of permutation groups. These Proceedings, pp. 169-183.

Sm 1. D. A. SMITH: A basis algorithm for finitely generated abelian groups. *Mathematical Algorithms* 1.1 (1966), 14-35.

sp 1. G. P. SPIELMAN: Special interest form. *SZCSAM Bulletin 7* (1967), 19.

su 1. E. H. SUSSENGUTH JR.: Structure matching in information processing. Ph. D. Thesis, Harvard, 1964, Harvard Scientific Report ISR6.

SW 1. J. D. SWIFT : Isomorph rejection in exhaustive search techniques. *American Math. Soc. Proc. Symp. in Appl. Math.* 10 (1960), 195-200.

To 1. J. A. TODD and H. S. M. COXETER: A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc. (2) 5* (1936), 26-34.

Tr 1. A. L. TRITTER: A module-theoretic computation related to Bumside's problem. These Proceedings, pp. 189-1 98.

Tr 2. H. F. TROTTER: A machine program for coset enumeration. *Canad. Math. Bull.* 7 (1964), 357-368.

Tr 3. H. F. TROTTER: A program for the Coxeter-Todd algorithm for the enumeration of cosets in groups. *Mathematical Algorithms* 1.3 (1966), 12-18.

Wa 1. D. W. WALKUP: On a result of Heineken. *Notices American Math. Soc.* 10 (1963), 578.

Wa 2. G. E. WALL: On Hughes' *Hp* problem. *Proc. Znternat. Conf. Theory of Groups. Austral. Nat. Univ. Canberra,* August 1965,357-362.

We 1. M. WELLS: Enlargement of a group. Algorithm 136. *Comm. Assoc. Comp. Mach.* 5 (1962), 555.

Wh 1. M. E. WHITE: Modular arithmetic for finite groups. *Notices American Math. Soc.* 12 (1965), 52.

Ya 1. R. YATES: Group analysis programs. Quantum Theory Project, University of Florida, Gainesville, Florida, Program Note 5 (1963).

Za 1. G. ZAPPA: Contributo allo studio del problema di Hughes sui gruppi. *Ann. Mat. Pura Appl. (4) 57* (1962), 211-219.

Za 2. H. ZASSENHAUS: Über einen Algorithmus zur Bestimmung der Raumgruppen. *Comment. Math. Helv.* 21(1948), 117-141.

Coset enumeration

John Leech

1. Introduction. In 1936 Todd and Coxeter gave a method ([7], also described in [1], ch. 2) for establishing the order of a finite group defined by a set of relations satisfied by its generators. They enumerate systematically the cosets of a suitable subgroup whose order is evident from the defining relations for the whole group. (To be precise, what the method does is to establish the index, when finite, of a subgroup of a finitely presented group. The finiteness of the whole group is not necessary for the success of the method.) They describe the method as being "purely mechanical", and since that date the advent of electronic computers has led a number of people to programme the method for automatic execution. I have given an account [2] of such of this work as was known to me in 1962.

The present account is based in part on my former paper [2], but does not include the historical details there given. It includes also a discussion of the necessity for the termination of the process, and an application of it to the following word problem. If a coset enumeration shows that certain elements generate a subgroup of finite index in a finitely presented group, and that an element, given as a word in the generators of the group, is an element of the subgroup, it is required to express it as a word in the generators of the subgroup.

2. Hand calculation. The basic procedure when enumerating cosets by hand is to set out each relation *in extenso* at the head of a table. The lines of the table are filled with coset numbers so that the numbers fall in columns between the letters of the defining relation, the cosets in adjacent columns being related by the generator at the head of the space between the columns. If (as I assume hereafter) each relation equates a word in the generators of the group to the identity, then the first and last columns of the table for each relation will be identical. It is convenient to keep also a multiplication table showing the effect on each coset of each generator, and also of the inverse of each generator which is not involutory, as these are determined.

Initially entries are made so as to define the subgroup which is chosen as coset 1. As the work progresses, more cosets are defined and entered in the tables, and whenever a line of a relation table is completed, further entries are made in the multiplication and other tables. The enumeration is complete when the tables are full, leaving no space for the definition of further cosets, and exhibiting every coset in every significantly different position in each relation table. A worked example is given is § 11 below.

3. Coincidences. It may be found in the course of the work that two differently numbered cosets are in fact the same; this is commonly called a *coincidence* of the cosets. In such an event the greater of the numbers is replaced throughout by the smaller, and any consequent coincidences between other cosets are then dealt with similarly. If the tables are still incomplete after this, the enumeration continues as before. In hand work this replacement is inconvenient, and, with practice, skill is gained at defining cosets in such an order that coincidences are infrequent, and many enumerations can be carried out without the occurrence of coincidences. But there are many examples where coincidences are unavoidable. Thus if the defining relations are inconsistent, then the group consists of the identity element only, and any coset enumeration will reduce to only one coset. Usually it will have been necessary to define several cosets before the working shows that these are not distinct. The following two examples are of a non-trivial group (the simple group $LF(2, 7)$, Klein's group of order 168). Attempts to enumerate the 24 cosets of the subgroup generated by B in this group as defined by the relations

$$B^7 = (AB)^2 = (A^{-1}B)^3 = (A^2B^2)^4 = E$$

or

$$B^7 = (AB)^2 = (A^{-1}B)^3 = (A^3B^4)^3 = E$$

will result in the definition of many more than 24 cosets before the working shows that these are not all distinct.

4. Computer implementation. It is extremely inconvenient on a computer to store the incomplete lines of working in the relation tables and to locate places for insertion of new entries. It is much simpler to recompute the whole of a line in which a new entry is to be placed. In practice, therefore, the main working table stored in the machine is the coset multiplication table. Each line of the relation tables is then constructed as required from the entries in the multiplication table. It is in the nature of the working that access to this table is random and unpredictable, and it should be held in the immediately accessible part of the store. The number of cosets definable is then limited by the amount of such storage available, and if this limit is likely to be approached, the following steps should be taken to economize in its use.

First, as in hand working, no column should be used for the inverse of an involutory generator. A convenient implementation of this is to number the columns and to include with the data a short list showing which column is inverse to which; this will list the column for an involutory generator as being the column for its inverse. Whenever reference to the inverse of a generator is made, it is made through this list. No other part of the programme has then to take account of whether a generator is involutory, and problems in which none, some or all of the generators are involutory are handled uniformly.

Next, in computers with a fixed word length, it may be desirable to pack the multiplication table entries with several in each word, so that the whole of a line of the multiplication table may occupy only one or two words. If the word length is variable, a suitably short length can probably be chosen which will obviate further packing. In the author's experience, packing and unpacking do not add seriously to running times, and he has found that limitation on immediately accessible storage space has always been more important than running time.

The relations defining the group are conveniently stored as lists of integers, each of which denotes the column of the multiplication table corresponding to the generator or its inverse appearing at the corresponding point in the relation, suitably terminated (by a zero, perhaps) to indicate the end of the relation, with a count or other indication of whether it is the last relation. If storage space is extremely limited, it may be desirable to pack the relations with several letters in each computer word, but this is less likely to be important than packing the multiplication table.

Programmes for computer implementation of coset enumeration differ mainly in the choice of algorithm for determining the sequence in which new cosets are defined. It is not possible to implement the human judgement that can be applied to conduct enumerations without coincidences, as this often depends on examining the state of the relation tables, which the computer does not store. Most programmes follow, more or less closely, one of the two algorithms described in the following sections. The natural order for describing these is the reverse of the historical order adopted in [2], so the present "first and second algorithms" are the "second and first methods" of [2] respectively.

5. First algorithm. This follows rather closely the hand method as described in § 2. We examine each entry in the multiplication table, in the order in which they are made, in the following way. Suppose it has been found, by definition or deduction, that $aS_j = b$, where a and b are coset numbers and S_j is a generator. We have to examine each relation involving S_j or its inverse, for each significantly different occurrence of either, to find out whether insertion of $aS_j = b$ or $bS_j^{-1} = a$ at that point would complete a line of the relation table.

Suppose the relation is $R_1 R_2 \ldots R_n = E$, with $R_i = S_j$. Working in the backward direction, we extract the entries aR_{i-1}^{-1}, $aR_{i-1}^{-1}R_{i-2}^{-1}$, …, continuing until either an undefined coset is sought (i.e. a blank entry is found in the multiplication table) or the beginning of the relation is reached. In the latter event we continue by extracting $aR_{i-1}^{-1} R_{i-2}^{-1} \ldots R_1^{-1}R_n^{-1}$, $aR_{i-1}^{-1}R_{i-2}^{-1} \ldots R_1^{-1}R_n^{-1}R_{n-1}^{-1}$, …, continuing until either an undefined coset is sought or the entry $aR_{i-1}^{-1}R_{i-2}^{-1} \ldots R^{-1}\, R_n^{-1}R_{n-1}^{-1} \ldots R_{i+1}^{-1}$ is reached. This should be b; if it is not, a coincidence has been found. If an undefined coset has been reached, we make a similar examination in the forward direction, extracting the entries bR_{i+1}, $bR_{i+1}R_{i+2}$, $\ldots$, $bR_{i+1}R_{i+2}\ldots R_nR_1$, $\ldots$ until either an undefined coset is sought or the backward working is met. There are three possibilities. The forward and backward working may fail to meet, and no information can be deduced at this stage. Or they may just meet, so that the final cosets reached in the forward and backward working are related by a generator, and a new entry is made in the multiplication table. Or they may overlap, in which case different entries have been found for the same place in the relation table, and a coincidence has been found. (In this last case the coset numbers cannot have been the same in the two directions, otherwise the backward working would have completed a full cycle and no forward working would have been done.)

As new entries are made in the multiplication table, they are also placed in a list of unworked table entries. When the current entry has been examined in all significantly different positions in all relation tables as above, it is removed from the list and the next entry is examined similarly. When the list is empty, the multiplication table is examined. If this is complete, then the enumeration is finished, and the result is available. If not, then there are some blank entries in the multiplication table, and a new coset is defined by making an entry in one of these blanks and creating a new line of the table with an entry in the column inverse to that in which the blank was filled.

In hand calculation the choice of which blank to fill at each stage is a matter for human judgement; usually we fill a blank which leads to completion of one or more lines of relation tables if possible. On a computer, for a general-purpose programme, we have to adopt a simpler rule, such as always defining a new coset to fill the earliest blank in the multiplication table. For this reason we except to encounter coincidences more frequently than in hand work. Since coincidences are sometimes unavoidable, any programme should be able to deal with them, and it is no great disadvantage that it has to do so more often than in hand work.

6. Second algorithm. This is less similar to hand calculation than the first algorithm, and was devised to simplify the programme as much as possible. It was the first to be programmed, and this was for machines with very limited storage space, so that it was of importance to make the programmes as short as possible in order to maximize the space available for the multiplication table.

We construct the lines of the relation tables in a systematic order by taking each coset in turn and beginning a line of each relation table with it. We extract the entries aR_1, aR_1R_2, $\ldots$ successively, and if any of these is undefined, we define new cosets to complete the whole line of the table. The last entry in the line should be the same as the first; if it is not, as will always be the case when new cosets have been defined, then there is a coincidence between these cosets, and the programme deals with this and any consequent coincidences before continuing.

The programme for this algorithm is simpler than for the first algorithm as it has only to work through the relations in the forward direction, and there is no division into cases corresponding to that in the first algorithm where the workings may fail to meet, just meet or overlap. The coincidence procedure handles these cases uniformly. However, coincidences are much more frequent with this algorithm, occurring whenever new cosets are defined, which results in uneconomic use of space for the multiplication table. This is not only the space used for cosets defined to complete a line and eliminated at once by coincidence. Those surviving are defined in an inefficient order, which may result in the definition of many more of them. For example, in enumerations of the 448 cosets of the octahedral subgroup $\{A^2, A^{-1}B\}$ in the group of order 10752 defined by the relations

$$A^8 = B^7 = (AB)^2 = (A^{-1}B)^3 = E,$$

a programme using the first algorithm had a maximum of about 1300 cosets defined at one time, while one using the second algorithm had 2176 cosets defined at one time. The presentations of Klein's group given in § 3 would probably give more disparate figures, but these are not available. However, there is some reason to believe that examples of this kind are of infrequent occurrence in practice. (They may be recommended for use in programme checking.)

7. Computer handling of coincidences. This is the logically most complicated part of any coset enumeration programme. When it has been found that two cosets, numbered a, b say, with $b > a$, are the same, we have to replace occurrences of b in the multiplication table by a, and deal with any consequent coincidences similarly. We examine each entry in line b of the multiplication table. If any such entry is blank, we take no action and pass on to the next entry. If we find an entry $bR_i = b$, then we replace this by a. But if we find an entry $bR_i = c \neq b$, then we know that line c contains an entry $cR_i^{-1} = b$. In the first instance we delete this, rather than replacing it by a, to avoid having two occurrences of a in the same column. Then, whether $bR_i = b$ or not, we examine aR_i. If this was not defined, then we copy bR_i there. But if it was defined, then if $aR_i = b$ we replace it by a, and in any case we set up a new coincidence between bR_i and aR_i, and place it in a list of coincidences to be dealt with. In either case, if $(aR_i)R_i^{-1}$ is undefined, then we set it equal to a. In the first algorithm, if aR_i was undefined, the transferred entry $bR_i = c$, now $aR_i = c$, is placed in the list of unworked table entries.

When all the entries in line b have been dealt with, the line is deleted and becomes available for the definition of a new coset. In the first algorithm, any entry in the list of unworked table entries which involves b may be deleted. If aR_i had been undefined, the transferred entry $aR_i = c$ will produce all the corresponding working, while if it had been defined, this entry will have been dealt with in its own right or will be in the list awaiting working.

It is also necessary to ensure that there remains no occurrence of b in the list of coincidences to be dealt with, any such being replaced by a. A convenient way of avoiding such occurrences, and also avoiding storage of redundant information in this list, is the following. The list is kept as a list of pairs of numbers, the greater on the left, stored in decreasing order of left-hand number. At each stage we deal with the first entry in the list, which has the greatest left-hand number, so this number b cannot occur elsewhere in the list. When a new coincidence is to be placed in the list, a search is made for the place appropriate to its left-hand number. If a pair in the list has the same left-hand number, then the right-hand numbers of the old and new pair are paired, the greater on the left, and this pair replaces the original pair in the search for the place in the list. Eventually either a pair is found whose left-hand number is not equal to that of any pair in the list, which we then place in the list, or a pair is formed of two equal numbers, indicating that this coincidence did not give any new information, and no entry is made. In this way the list never contains redundant information.

When the coincidence between b and a has been fully dealt with as above, the next coincidence in the list is treated similarly, and we continue until this list is empty. We then return to normal working, beginning with the first algorithm, with the list of unworked multiplication table entries, and continue until the tables are complete or another coincidence occurs. An example which illustrates the handling of coincidences is given in § 12.

After a coincidence and its consequences have been dealt with, there will be a number of blank lines in the multiplication table, which are available for the definition of further cosets. It is not advisable to use these in their original position, however, except for those following the last undeleted coset, as the numerical sequence of cosets would depart from the logical sequence, and a sequence of operations based on the numerical sequence would become inefficient. The table can be closed up by transferring and renumbering the undeleted lines, retaining their original order. Experience suggests that it is uneconomic in time to do this every time a coincidence and its consequences have been dealt with, and that it is sufficient to do it when the enumeration is complete or when the storage limit is reached. (But with the second algorithm it is advisable to ensure that at each stage the next coset to be defined follows next after the last undeleted coset, using again any subsequent lines that have been used for cosets now deleted.)

8. Form of data. Essentially the data comprise only the relations defining the group and the elements generating the subgroup. In practice it is convenient to supply also a list of inverses, as suggested in § 4, or some other specification of the number of generators or the number of columns of the multiplication table. If the list of inverses is supplied, then it is unnecessary to include relations specifiying that generators are involutory with the defining relations, as these are implied by the list of inverses. It is convenient to supply the list of elements generating the subgroup next, as these are required for making the initial entries in the multiplication table and are not used again after the use of the defining relations has begun. With the second algorithm, these elements can be handled exactly like defining relations, the equivalent of a line of a relation table, beginning and ending with coset 1, being formed for each element. Then they are replaced by the defining relations, and the main working continues as described. A similar procedure can be used with the first algorithm.

9. Termination of the process. Proofs have been given by Mendelsohn [5] and Trotter [8] that algorithms approximating respectively to the first and second algorithms above terminate in any case of a subgroup of finite index, but I shall not reproduce these here. It must be emphasized that these proofs cannot give a bound for the number of cosets which it may be necessary to define, even in the case of an inconsistent set of relations leading to the trivial group, as it is known that there is no algorithm for deciding whether a given finitely presented group is trivial or finite or infinite [6]. If a bound could be obtained, as a function of the order and the defining relations, for the number of cosets which have to be defined for any group which is finite, this would provide such an algorithm. All that can be shown in this case is that if the index of the subgroup is finite, then the enumeration process cannot continue indefinitely.

10. A word problem. In addition to the basic purpose of exhibiting the index of a subgroup in a group, there are a number of uses to which the result of a coset enumeration can be put. For example, the columns of the multiplication table give a permutation representation for a group which will not infrequently be the whole group when this is finite. I shall not describe here applications such as this which make use only of the resulting tables. The problem which I discuss in the next two sections is the following.

Suppose that a coset enumeration has shown that a subgroup is of finite index in a given group, and that a certain word W in the generators of the group satisfies $1W = 1$, so that it is an element of the subgroup. The problem is to express this as a word in the generators of the subgroup. The final multiplication table does not enable us to find such an expression, but we can do so by keeping and using an explicit record of the steps taken in performing the enumeration. In its simplest form, the present algorithm is applicable only when the coset enumeration has not involved the definition of redundant cosets and their subsequent elimination by coincidences. An example of this is worked in detail in § 11. A modification of this algorithm is proposed which allows an extension to cases where coincidences are met in the course of the enumeration. An example of this is worked in detail in § 12.

Another problem which can be solved by this algorithm is that of expressing an arbitrary element of a group as the product of an element of the subgroup by a coset representative. The subgroup element can be found by multiplying the chosen element by the inverse of the coset representative and applying the algorithm to this product. A set of Schreier coset representatives can be obtained by using the definitions of the cosets which were used in the enumeration. Each coset is defined as the product of an earlier coset by a generator, and by repeated application of this we obtain a definition as a product of coset 1 by a word in the generators which is the required representative. Clearly every leading subword of this word is itself a coset representative.

11. A worked example. In this example I enumerate the six cosets of the subgroup $\{A\}$ in the octahedral group defined by the relations

$$A^4 = (AB)^2 = B^3 = E.$$

A systematic record is kept of the order in which the entries in the multiplication table are made and of the relations used in deducing them. First we insert the entry $1A = 1$, which defines coset 1 to be the subgroup $\{A\}$. Next we define $2 = 1B$ and $3 = 1B^{-1}$. On inserting these entries into the relation tables, we find that two lines are closed, allowing us to deduce $2A = 3$ from $(AB)^2 = E$ and $2B = 3$ from $B^3 = E$. Next we define $4 = 2A^{-1}$ and $5 = 3A$, and deduce $5A = 4$ from $A^4 = E$ and $5B = 4$ from $(AB)^2 = E$. Lastly we define $6 = 4B$ and deduce $6B = 5$ from $B^3 = E$ and then $6A = 6$ from $(AB)^2 = E$. The enumeration is now complete, and we have the multiplication and relation tables given below. The small figures in the relation tables denote the deductions made by the closures of these lines, numbered in the order in which they were made, and the same figures are affixed as subscripts to the entries in the multiplication table.

	A	A^{-1}	B	B^{-1}
1	1	1	2	3
2	3_1	4	3_2	1
3	5	2_1	1	2_2
4	2	5_3	6	5_4
5	4_3	3	4_4	6_5
6	6_6	6_6	5_5	4

	A		A		A		A	
1		1		1		1		1
2		3		5	$_3$	4		2
6		6		6		6		6

	A		B		A		B	
1		1		2	$_1$	3		1
3		5	$_4$	4		2		3
5		4		6	$_6$	6		5

	B		B		B	
1		2	$_2$	3		1
4		6	$_5$	5		4

In this example, the cosets have been defined in the sequence of the first algorithm above, the earliest blank in the multiplication table being filled at each stage, so, except for retaining the relation tables and annotating the deduced entries, we have done the work exactly according to the first algorithm. In this simple example no coincidences are encountered.

We are now in a position to deal with word problems such as the following. The word $(BA^{-1}B)^{-1}A(BA^{-1}B)$ is an element of the subgroup $\{A\}$, as we see by writing it in full with the coset numbers beneath, beginning with coset 1, like a line of a relation table, thus:

$$\begin{array}{ccccccccccccccc} & B^{-1} & & A & & B^{-1} & & A & & B & & A^{-1} & & B & \\ 1 & & 3 & & 5 & {}_5 & 6 & {}_6 & 6 & {}_5 & 5 & & 3 & & 1, \end{array}$$

and noticing that it ends with coset 1. The small figures 5 and 6 indicate that the relations $5B^{-1} = 6$ and $6A = 6$ were obtained by deduction, the others, $1B^{-1} = 3$, etc., having been made by definition. We deal first with the later numbered deduction $6A = 6$, which was deduced from $(AB)^2 = E$. We replace this A by $B^{-1}A^{-1}B^{-1}$, cancel an adjacent pair $B^{-1}B$, and obtain

$$\begin{array}{ccccccccccccccc} & B^{-1} & & A & & B^{-1} & & B^{-1} & & A^{-1} & & A^{-1} & & B & \\ 1 & & 3 & & 5 & {}_5 & 6 & & 4 & {}_3 & 5 & & 3 & & 1. \end{array}$$

Again we have two entries made by deduction and we deal first with the later numbered deduction, namely $5B^{-1} = 6$, which was deduced from $B^3 = E$. We replace this B^{-1} by B^2, cancel an adjacent pair BB^{-1}, and obtain

$$\begin{array}{ccccccccccccc} & B^{-1} & & A & & B & & A^{-1} & & A^{-1} & & B & \\ 1 & & 3 & & 5 & {}_4 & 4 & {}_3 & 5 & & 3 & & 1. \end{array}$$

Continuing in this way, always replacing the letter corresponding to the latest numbered deduction with the remainder of the relation from which it was deduced, and cancelling any adjacent mutually inverse letters, we obtain successively

$$\begin{array}{ccccccccccccc} & B^{-1} & & B^{-1} & & A^{-1} & & A^{-1} & & A^{-1} & & B & \\ 1 & & 3 & {}_2 & 2 & & 4 & {}_3 & 5 & & 3 & & 1, \end{array}$$

$$\begin{array}{ccccccccc} & B^{-1} & & B^{-1} & & A & & B & \\ 1 & & 3 & {}_2 & 2 & {}_1 & 3 & & 1, \end{array}$$

$$\begin{array}{ccccccc} & B & & A & & B & \\ 1 & & 2 & {}_1 & 3 & & 1, \end{array}$$

$$\begin{array}{ccc} & A^{-1} & \\ 1 & & 1. \end{array}$$

The work is now complete, as all the deduced entries have been replaced, and we have shown that $(BA^{-1}B)^{-1}A(BA^{-1}B) = A^{-1}$. The procedure adopted has been that at each stage the replacement made is that which corresponds to the latest deduced entry in the multiplication table. If this entry occurs several times in the word, the replacement is made at all occurrences. After a finite number of stages (which cannot exceed the number of deduced entries in the multiplication table), all deduced entries have been eliminated, and we have a word containing only entries made by definition, these entries being just those made in defining the subgroup. So although this word is still in the generators of the original group, its expression in terms of the generators of the subgroup is immediate.

I have programmed this algorithm for use with a hand-calculated coset enumeration, and have made substantial use of it [3]. However, it is capable of improvement in the following two ways.

First, any two or more deductions which could have been made independently in any order, such as $2A = 3$ and $2B = 3$ in this example, can be given the same number and dealt with at the same stage, since the result of substituting for any one of them cannot be to leave a substitution for another of them to be done. (This was done implicitly above when giving the same number to both of a pair of inverse entries, such as $2A = 3$ and $3A^{-1} = 2$ above.) This reduces the total number of stages to be carried out.

The second modification may be convenient if several words are to be dealt with from the same enumeration. As the enumeration is being done, we form a list of substitution words corresponding to the deduced entries in the multiplication table, each embodying the results of previous substitution words, and we use these instead of making substitutions of the remainder of the relations as above. This avoids making the same, possibly long, sequence of substitutions several times over, as may happen if several words are to be dealt with. In the example above, we would have the following substitution words. As no further substitutions are done on these words, the coset numbers do not have to be recorded.

$$2 \overset{A}{{}_{1}} 3 = B^{-1}A^{-1}B^{-1}$$

$$2 \overset{B}{{}_{2}} 3 = B^{-2}$$

$$5 \overset{A}{{}_{3}} 4 = 5 \overset{A^{-1}}{\;} 3 \overset{A^{-1}}{{}_{1}} 2 \overset{A^{-1}}{\;} 4 = A^{-1}BABA^{-1}$$

$$5 \overset{B}{{}_{4}} 4 = 5 \overset{A^{-1}}{\;} 3 \overset{B^{-1}}{{}_{2}} 2 \overset{A^{-1}}{\;} 4 = A^{-1}B^{2}A^{-1}$$

$$6 \overset{B}{{}_{5}} 5 = 6 \overset{B^{-1}}{\;} 4 \overset{B^{-1}}{{}_{4}} 5 = B^{-1}AB^{-2}A$$

$$6 \overset{A}{{}_{6}} 6 = 6 \overset{B^{-1}}{\;} 4 \overset{A^{-1}}{{}_{3}} 5 \overset{B^{-1}}{{}_{5}} 6 = B^{-1}AB^{-1}A^{-1}BA^{-1}B$$

With such a list available, we need only one stage of substitution for each word being dealt with, simplifying this part of the work, which has to be done for each word, at the expense of complicating the preliminary work which has to be done once only. Thus with the example above we obtain

$$1 \overset{B^{-1}}{\;} 3 \overset{A}{\;} 5 \overset{B^{-1}}{{}_{5}} 6 \overset{A}{{}_{6}} 6 \overset{B}{{}_{5}} 5 \overset{A^{-1}}{\;} 3 \overset{B}{\;} 1$$
$$= B^{-1}.A.A^{-1}B^{2}A^{-1}B.B^{-1}AB^{-1}A^{-1}BA^{-1}B.B^{-1}AB^{-2}A.A^{-1}.B$$
$$= A^{-1}.$$

I have used the first modification above with my original programme, as its use with a hand-calculated coset enumeration involves only preparing the data, recording the hand work, slightly differently. The second modification would involve substantial fresh programming which I have not yet done. I hope to do so and to incorporate the extension to enumerations involving coincidences proposed in the next section. It could then be used with a computer coset enumeration programme, as there would then be no special need to avoid coincidences.

12. An example with coincidences. I have not found an example of a coset enumeration which involves coincidences unavoidably, which reduces to more than one coset, and which is sufficiently simple to allow full exhibition of the working in a reasonable compass. The example I give is borrowed from Mendelsohn [5], and is to enumerate the five cosets of $\{X\}$ in the group defined by the relations

$$X^4 = X^2AXA^{-2} = E.$$

Mendelsohn thought originally that coincidences were unavoidable in this example, but subsequently found that this was wrong. It would be difficult, however, to devise a computer procedure to find the sequence of definition which has to be adopted to avoid coincidences in cases such as this (in this example we must avoid defining $1A$; the definitions $2 = 1A^{-1}$, $3 = 2X$, $4 = 3X$ and $5 = 4X$ are suitable). I give the working as it would be done by the first algorithm (§ 5), dealing with coincidences as in § 7. In addition to the substitution words, obtained as in § 11, we obtain coincidence words, which are used rather similarly in the working.

The first part of the working, up to the discovery of the first coincidence, follows exactly the lines of the example of § 11, and need not be given in detail. Defining new cosets so as always to fill the earliest blank in the multiplication table, we define $1X = 1, 2 = 1A, 3 = 1A^{-1}, 4 = 2X, 5 = 2X^{-1}$, $6 = 3X, 7 = 3X^{-1}, 8 = 3A^{-1}$, and deduce $2A = 4$, $8X = 7$ and $6X = 8$. At this stage we have the tables and substitution words given below, omitting incomplete lines of relation tables.

	X	X^{-1}	A	A^{-1}
1	1	1	2	3
2	4	5	4_1	1
3	6	7	1	8
4		2		2_1
5	2			
6	8_3	3		
7	3	8_2		
8	7_2	6_3	3	

$$\begin{array}{ccccccccc} & X & & X & & X & & X & \\ 1 & & 1 & & 1 & & 1 & & 1 \\ 3 & & 6 & {}_3 & 8 & & 7 & & 3 \end{array}$$

$$\begin{array}{ccccccccccccc} & X & & X & & A & & X & & A^{-1} & & A^{-1} & \\ 1 & & 1 & & 1 & & 2 & & 4 & {}_1 & 2 & & 1 \\ 8 & {}_2 & 7 & & 3 & & 1 & & 1 & & 3 & & 8 \\ 3 & & 6 & & 8 & & * & & 2 & & 1 & & 3 \end{array}$$

$$\begin{array}{ccclcll} & A & & = A^{-1}X^2AX \\ 2 & {}_1 & 4 \end{array}$$

$$\begin{array}{ccclcll} & X & & = A^2X^{-1}A^{-1}X^{-1} \\ 8 & {}_2 & 7 \end{array}$$

$$\begin{array}{cccccccccc} & X & & = & X^{-1} & & X^{-1} & & X^{-1} & = X^{-1}AXA^{-2} \\ 6 & {}_3 & 8 & & 6 & & 3 & & 7 \; {}_2 \; 8 & \end{array}$$

We now find that the space in the relation table marked by an asterisk can be filled from either $8A = 3$ or $2X^{-1} = 5$, so we have a coincidence between cosets 5 and 3. We record this, and deduce from it a coincidence word in the same way as a substitution word, finding

$$\begin{array}{ccccccccccccccccc} & E & & & & X & & A^{-1} & & A^{-1} & & X & & X & & A & \\ 5 & {}_4 & 3 & = & 5 & & 2 & & 1 & & 3 & & 6 & {}_3 & 8 & & 3 \end{array}$$

$$= X.A^{-1}.A^{-1}.X.X^{-1}AXA^{-2}.A$$

$$= XA^{-1}XA^{-1}.$$

(This proves that the given relations imply $(XA^{-1})^2 = E$.) Next we deal with the coincidence as in § 7. In line 5 of the multiplication table we find the entry $5X = 2$, so we delete the entry $2X^{-1} = 5$ from line 2. Then we examine $3X$ and find $3X = 6$, so we have a coincidence between cosets 2 and 6. We record this, and construct the coincidence word

$$\begin{array}{ccccccccccccc} & E & & & & X^{-1} & & E & & X & & & A^{-1}XA^{-1}X. \\ 2 & {}_5 & 6 & = & 2 & & 5 & {}_4 & 3 & & 6 & = & \end{array}$$

This completes the working for line 5, as it has no other entry, so we delete line 5 and deal next with the coincidence between cosets 2 and 6.

In line 6 we find first the entry $6X = 8$, so we delete the entry $8X^{-1} = 6$ from line 8. Then we examine $2X$ and find $2X = 4$, so we have a coincidence between cosets 8 and 4, from which we construct the coincidence word

$$\begin{array}{ccccccccccc} & E & & & & X^{-1} & & E & & X & \\ 8 & {}_6 & 4 & = & 8 & {}_3 & 6 & {}_5 & 2 & & 4 \end{array}$$

$$= A^2X^{-1}A^{-1}X.X^{-1}AX^{-1}A.X$$

$$= A^2X^{-2}AX.$$

Continuing along line 6, we find the entry $6X^{-1} = 3$, so we delete the entry $3X = 6$ from line 3. Then we examine $2X^{-1}$ and find this to be undefined (the entry $2X^{-1} = 5$ was deleted when we dealt with line 5), so we insert the entries $2X^{-1} = 3$ and $3X = 2$, and construct the substitution word

$$\begin{array}{ccccccccccc} & X & & & & X & & E & & & \\ 3 & {}_7 & 2 & = & 3 & & 6 & {}_5 & 2 & = & AX^{-1}A. \end{array}$$

This completes the working for line 6, so we delete it and deal next with the coincidence between cosets 4 and 8.

In line 8 we find first the entry $8X = 7$, so we delete the entry $7X^{-1} = 8$ from line 7. Then we examine $4X$ and find this to be undefined, so we insert the entries $4X = 7$ and $7X^{-1} = 4$, and obtain the substitution word

$$\begin{array}{ccccccccc} & X & & & & E & & X & \\ 4 & {}_8 & 7 & = & 4 & {}_6 & 8 & {}_2 & 7 \end{array}$$

$$= X^{-1}A^{-1}X^2A^{-2}.A^2X^{-1}A^{-1}X^{-1}$$

$$= X^{-1}A^{-1}XA^{-1}X^{-1}.$$

Continuing along line 8, the entry $8X^{-1}$ having been deleted, we find $8A = 3$, so we delete $3A^{-1} = 8$ from line 3. Then we examine $4A$ and find this to be undefined, so we put $4A = 3$ and $3A^{-1} = 4$, and construct the substitution word

$$\begin{array}{ccccccccc} & A & & & & E & & A & \\ 4 & {}_9 & 3 & = & 4 & {}_6 & 8 & & 3 \end{array}$$

$$= X^{-1}A^{-1}X^2A^{-2}.A$$

$$= X^{-1}A^{-1}X^2A^{-1}.$$

This completes the working for line 8, so we delete it. There are no further coincidences to be dealt with, so we return to normal working.

At this stage we have the following multiplication table.

	X	X^{-1}	A	A^{-1}
1	1	1	2	3
2	4	3_7	4_1	1
3	2_7	7	1	4_9
4	7_8	2	3_9	2_1
7	3	4_8		

The list of unworked table entries contains the entries $3X = 2$, $4X = 7$ and $4A = 3$. (It would be possible at this stage to renumber coset 7 as coset 5 and to delete the superseded entries from the list of substitution words, including all the coincidence words, renumbering those remaining. To avoid confusion, I have not done this here.) In the course of normal working, we construct the line

$$\begin{array}{ccccccccccccc} & X & & X & & A & & X & & A^{-1} & & A^{-1} & , \\ 2 & & 4 & & 7 & {}_{10} & 7 & & 3 & & 4 & & 2 \end{array}$$

which gives $7A = 7$, from which we obtain the substitution word

$$\begin{array}{ccccccccccccccc} & A & & & & X^{-1} & & X^{-1} & & A & & A & & X^{-1} & \\ 7 & {}_{10} & 7 & = & 7 & {}_8 & 4 & & 2 & {}_1 & 4 & {}_9 & 3 & & 7 \end{array}$$

$$= XAX^{-1}AX.X^{-1}.A^{-1}X^2AX.X^{-1}A^{-1}X^2A^{-1}.X^{-1}$$

$$= XAX^3A^{-1}X^{-1}.$$

The multiplication table is now complete, and completion of the ordinary working shows that the relation tables can all be filled consistently without further coincidences. We also have a complete set of substitution words for the deduced entries in the multiplication table, so we can now put into effect the modified algorithm of § 11 for expressing elements of the subgroup as words in its generators. For example

$$\begin{array}{ccccccccc} & A & & A & & A & & A & \\ 1 & & 2 & {}_1 & 4 & {}_9 & 3 & & 1 \end{array} = A.A^{-1}X^2AX.X^{-1}A^{-1}X^2A^{-1}.A$$

$$= X^4.$$

This example illustrates that the algorithm does not necessarily obtain the shortest word in the subgroup generators, and it may be possible to simplify it by use of the relations for the subgroup. In this example we have $X^4 = E$, so we have proved the relation $A^4 = E$ for this group.

In this algorithm, coincidence words are obtained in three ways. When a coincidence is met in normal working, the relation from which it was deduced gives the coincidence word, as with cosets 5 and 3 above. When a coincidence is deduced from another, as when we found above that both $5X$ and $3X$ were defined, we construct the coincidence word

$$2 \overset{E}{\quad} 6 = 2 \overset{X^{-1}}{\quad} 5 \overset{E}{\quad} 3 \overset{X}{\quad} 6$$

by adjoining $5X$ and $3X$ to the previous coincidence word. The third way did not occur in the example. Suppose we deduce a coincidence between cosets b and a, with $b > a$, obtaining the corresponding coincidence word, and find when placing this coincidence in the list of coincidences to be dealt with that the list contains a coincidence between cosets b and c, with $b > c$, whose coincidence word is available already. We replace our coincidence between b and a by one between c and a in our search for the place in the list, and construct the coincidence word

$$c \overset{E}{\quad} a = c \overset{E}{\quad} b \overset{E}{\quad} a.$$

This operation may be repeated as the search continues.

Substitution words are obtained from entries in normal working as previously. They are obtained from entries transferred by coincidences as the product of the former substitution word and the coincidence word, as was done above when we obtained the substitution word

$$3 \overset{X}{\quad} 2 = 3 \overset{X}{\quad} 6 \overset{E}{\quad} 2.$$

A programme to implement this algorithm would need substantially more storage space than a programme to implement only the coset enumeration, because of the need to store the substitution words. These could be packed with several letters to each computer word, but there would be complications as the length of these substitution words seems to be practically unlimited. Some economy can be effected by deleting the words corresponding to superseded entries and coincidences. The coincidence words could be listed separately, as it is known that they will all be superseded.

Such a programme could be used for proving relations in groups, either by discovering them (as with $(XA^{-1})^2 = E$ above) or by proving suspected relations (such as $A^4 = E$ above). In either case a formal proof could be printed out from the substitutions made in the course of the working. It would be of interest to apply such a programme to a problem such as the following. The relations

$$A^8 = B^7 = (AB)^2 = (A^{-1}B)^3 = E$$

imply $(A^2B^4)^6 = E$, but the only known proof is of surprising length. A proof could be obtained from the enumeration of 448 cosets of the octahedral subgroup $\{A^2, A^{-1}B\}$, which is believed to involve coincidences unavoidably (cf. § 6), and this could be compared with the published proof **[4]**.

13. Acknowledgement. The early part of this account reproduces almost exactly the corresponding part of my former paper **[2]**. I am indebted to the Council of the Cambridge Philosophical Society for permission to reproduce this.

REFERENCES

1. H. S. M. Coxeter and W. O. J. Moser: *Generators and Relations for Discrete Groups*. Ergebnisse der Mathematik NF 14 (Springer, Berlin 1965).

2. J. Leech: Coset enumeration on digital computers. *Proc. Cambridge Phil. Soc.* **59** (1963), 257–267.

3. J. Leech: Generators for certain normal subgroups of (2, 3, 7). *Proc. Cambridge Phil. Soc.* **61** (1965), 321–332.

4. J. Leech and J. Mennicke: Note on a conjecture of Coxeter. *Proc. Glasgow Math. Assoc.* **5** (1961), 25–29.

5. N. S. Mendelsohn: An algorithmic solution to a problem in group theory. *Canadian J. Maths.* **16** (1964), 509–516. (Correction, *Canadian J. Maths.* **17** (1965), 505.)

6. M. O. Rabin: Recursive unsolvability of group theoretic problems. *Annals of Maths.* **67** (1958), 172–194.

7. J. A. Todd and H. S. M. Coxeter: A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc.* (2) **5** (1936), 26–34.

8. H. F. Trotter: A machine program for coset enumeration. *Canadian Math. Bull.* **7** (1964), 357–368.

Some examples using coset enumeration

C.M. Campbell

Introduction. A modification of the Todd-Coxeter coset enumeration process [1] has been described by Campbell [2], Moser [3], and Benson and Mendelsohn [4]. In this note we give some examples that illustrate the way in which this modification is used.

Let G be an abstract group with a finite number of generators and relations, and let H be a subgroup of G. Assume further that the index $[G : H]$ of H in G is finite. Let E denote the identity and let $(^{-})$ denote the inverse of an element.

Theorem. *If from the relation $R = E$, where E is the identity and*

$$R = a_1 \dots a_r \dots a_s \dots a_p, \quad 1 \leqslant r \leqslant s \leqslant p,$$

we win the new information

$$\alpha . a_r a_{r+1} \dots a_s = \beta,$$

where each a_i is a generator g_j or its inverse and a, β are integers denoting cosets, then

$$\alpha . a_r \dots a_s = W./l,$$

where

$$w = W_{r-1} W_{r-2} \dots W_1 W_p \dots W_{s+1}$$

is a word in the subgroup and a, β are now thought of as coset representatives.

Proof. Express the relation $R = E$ in the form

$$a_r \dots a_s = \bar{a}_{r-1}\bar{a}_{r-2} \dots \bar{a}_1\bar{a}_p \dots a_{s+1}.$$

Then

$$\alpha . a_r \dots a_s = \alpha . \bar{a}_{r-1}\bar{a}_{r-2} \dots \bar{a}_1\bar{a}_p \dots a_{s+1}.$$

From previous information in the tables we find $\alpha \cdot \bar{a}_{r-1}$ expressed in the form $W_{r-1} \cdot \gamma$ (a and γ are now thought of as coset representatives and W_{r-1} is a word in the subgroup H):

$$\alpha . a_r \dots a_s = W_{r-1}\gamma . \bar{a}_{r-2} \dots \bar{a}_1\bar{a}_p \dots \bar{a}_{s+1}.$$

Now, again from the tables, $\gamma \cdot \bar{a}_{r-2} = W_{r-2} \cdot \delta$.

Therefore

$$\alpha . a_r \dots a_s = W_{r-1}W_{r-2}\delta . \bar{a}_{r-3} \dots \bar{a}_1\bar{a}_p \dots \bar{a}_{s+1}.$$

Repeating the process,

$$\alpha.a_r \ldots a, = W_{r-1}W_{r-2} \ldots W_1W_p \ldots W_s\mu.\bar{a}_{s+1}.$$

Finally, from the tables,

$$\mu.\bar{a}_{s+1} = W_{s+1}.\beta.$$

Therefore

$$\alpha.a_r \ldots a, = W_{r-1}W_{r-2} \ldots W_1W_p \ldots W_{s+1},$$

and hence

$$\alpha.a_r \ldots a_s = W.\beta.$$

The Todd-Coxeter process leads to an enumeration table and from the modification and our theorem (withp = 1) we obtain a table carrying additional information (see Example 1).

Examples. In [2] an algorithmic proof is given to show that the two relations

$$RS^2 = S^3R, \; SR^2 = R^3S$$

imply that $R = S = E$, where Eis the identity. This has been generalized by Benson and Mendelsohn [4] who show that the two relations

$$RS^{n-1} = S^nR, \; SR^{n-1} = R^nS$$

again imply that $R = S = E$.

We consider two examples that arise from the previous two.

Example 1. Let $G = \{R, S, T, U\}$ be subject to the relations $RS = S^2T$, $ST = T^2U$, $TU = U^2R$, $UR = R^2S$. Then G is cyclic of order 5.

Proof. $RS = S^2T$ (1)

$ST = T^2U$ (2)

$TU = U^2R$ (3)

$UR = R^2S$ (4)

$ST^2U = RS$ (5) from (1), (2)

$STU = \bar{R}$ (6) from (3), (4), (5)

where, as before, (⁻) denotes the inverse

$SU = \bar{R}ST$ (7) from (3), (6)

$S^3T = E$ (8) from (1), (2), (6)

$SRS = E$ (9) from (1), (8)

$U^2 = R$ (10) from (4), (9)

$ST = \bar{R}^2U$ (11) from (6), (10)

$S = \bar{R}^3$ (12) from (7), (11)

$U = \bar{R}^2$ (13) from (4), (12)

$T = \bar{R}$ (14) from (11), (12), (13)

$R^5 = E$ (15) from (10)

This algebraic proof follows algorithmically from the modified Todd–Coxeter process with the following enumeration and information tables. New information is found from the underlined positions in the tables in the order numbered.

	R	S	$\bar{T}$	$\bar{S}$	$\bar{S}$
1	1	2(2)3		2	1
2	(7)	1		3	2
3					3
4	2	3			4
5					5

	S	T	$\bar{U}$	$\bar{T}$	$\bar{T}$
1	2	5			1
2	3	2	(3)	5	2
3	(6)	1	5·	2	3
4					4
5					5

	T	U	$\bar{R}$	$\bar{U}$	$\bar{U}$
1				4	1
2	5	1	1	5(5)2	
3	2				3
4					4
5		2	4	1(4)5	

	U	R	$\bar{S}$	$\bar{R}$	$\bar{R}$
1	4(1)2		1	1	1
2	5				2
3					3
4(8)1		1		2	4
5	1	1			5

Coset	Representative	R	S	T	U
$1 = \{R\}$	$1 = E$	$1.R = R.1$	$1.S = E.2$		$1.U = E.4$
$2 = 1.S$	$2 = S$		$2.S = E3$	$2.T = E.5$	$2.u = R.5$
$3 = 2.s$	$3 = S^2$			$3.T = R.2$	
$4 = 1.u$	$4 = U$	$4.R = R^2.2$			$4.U = R.1$
$5 = 2.T$	$5 = ST$				$5.u = a.1$

From the positions numbered 3, 6, 7 we have, using our theorem, the additional information

$$5.TU = R.2,$$

$$3.ST = E.1,$$

$$2.RS = E.1.$$

In the above tables 4. $U = R.1$ and 5. $U = \bar{R}.1$, which implies that 4 and 5 are the same coset, and in terms of coset representatives $5 = \bar{R}^2.4$. Replacing 5 by $\bar{R}^2.4$ in the information tables gives

R	S	T	U
$1.R = R.1$	$1.S = E.2$		$1.u = E.4$
	$2.S = E3$	$2.T = \bar{R}^2.4$	$2.u = \bar{R}^3.4$
		$3.T = R.2$	
$4.R = R^2.2$			$4.U = R.1$

From these tables 1. $U = E.4$ and 2. $U = \bar{R}^3.4$, and it now follows that 1 and 2 are the same coset. Repeating the process as before leads finally to complete collapse.

The new information $\mathbf{4.R} = 2$ and $\mathbf{3.T} = 2$ reduce to equations (1) and (4) but from the new information $5.TU = 2$ equation (5) is obtained. In the first of the two calculations below we work with the coset representative as an integer and in the second we think of the coset representatives as a word in the group.

$$\begin{array}{rlrll}
5.TU &= 5.\bar{T}ST & ST.TU &= ST.TST & \text{from (2)} \\
&= E2.ST & &= ES.ST & \\
&= EE3.T & &= EES^2.T & \\
&= EER.2 & &= EER.S & \\
5.TU &= R.2 & &= R.S & \text{from (1)}
\end{array}$$

This is equation (5). In a similar manner we obtain equations (6)–(10). Equation (11) comes from the first coincidence when cosets 4 and 5 are identified.

$$\begin{array}{rlll}
5 &= \bar{R}1.\bar{U} & \text{from} & 5.u = \bar{R}.1 \\
&= \bar{R}\bar{R}4.U\bar{U} & \text{from} & 4.U = R.l \\
&= \bar{R}^2.4, & &
\end{array}$$

or, in terms of coset representatives,

$$\begin{array}{rll}
ST &= \bar{R}E.\bar{U} & \text{from (6)} \\
&= \bar{R}\bar{R}UU\bar{U} & \text{from (10)} \\
&= \bar{R}^2U, &
\end{array}$$

and this is equation (11). From the other coincidences we obtain equations (12)–(14).

EXAMPLE 2. The relations $SR^2 = RSRS$ and $RS^2 = SRSR$ imply that $R = S = E$.

Proof. The proof is again obtained algorithmically as in Example 1.

$$\begin{array}{rll}
SR^2 &= RSRS & (1) \\
RS^2 &= SRSR & (2) \\
SR^3 &= R^2S^2 & (3) \text{ from (1), (2)} \\
S^2RSR &= \bar{R}SR^2S & (4) \text{ from (1), (2)} \\
S^3 &= \bar{R}S^2R^2 & (5) \text{ from (1), (3)} \\
SR^2SRS &= RS^2R & (6) \text{ from (1), (3)} \\
S^2R^2S &= S^2R^2 & (7) \text{ from (2), (3), (5), (6)}
\end{array}$$

whence $S = E$ and $R = E$.

The following question now arises. Given $SR^n = R^{n-1}SRS$ and $RS^n = S^{n-1}RSR$, do these relations imply $R = S = E$? (True for $n = 1, 2$.) One further example is the following: show that the group generated by five generators a, b, c, d, e subject only to the relations $ab = c$, $bc = d$, $cd = e$, $de = a$, $ea = b$, is cyclic of order 11. This problem was discussed in the *American Mathematical Monthly* [5].

REFERENCES

1. H. S. M. COXETER and W. 0. J. MOSER: *Generators and Relations for Discrete Groups.* (Springer, Berlin, 1965).
2. C. M. CAMPBELL: Dissertation, McGill University, 1965.
3. W. O. J. MOSER: The Todd-Coxeter and Reidemeister-Schreier methods. Lecture delivered at the Conference on Computational Problems in Abstract Algebra held at Oxford, 1967.
4. ✓ C. T. BENSON and N. S. MENDELSOHN: A calculus for a certain class of word problems in groups, *J. Combinatorial Theory* 1 (1966), 202-208.
5. Problem *5327. American Math. Monthly 74* (1967), 91-93.

Defining relations for subgroups of finite index of groups with a finite presentation

N. S. MENDELSOHN

THIS note solves the following problem. Let G be a group with a finite presentation. Let ***H*** be a subgroup of G which is generated by a finite set of words in the generators of G and which is known to be of finite index. Find a set of defining relations for ***H.***

To solve this problem we need the following lemma.

LEMMA. ***Let G be a group with presentation***

$$G = \{x_1, x_2, \ldots x_r : R_1(x_1, \ldots x_r) = \ldots = R_u(x_1, \ldots x_r) = 1\}.$$

Suppose also that G is generated by $t_1, t_2, \ldots, t_m$ and that each t is expressed as a word in the x's and that each x is expressed as a word in the t's. Then a set of defining relations expressed entirely in terms of the t's can be found.

Proof. Let $x_i = W_i(t_1, t_2, \ldots, t_m)$ $i = 1, 2, \ldots, r$ and let $t_j = w_j(x_1, x_2, \ldots, x_r)$ $j = 1, 2, \ldots) m$. We abbreviate these as $x_i = W_i(t)$ and $t_j = = w_j(x)$. We now carry out Tietze transformations as follows. To the presentation $G = \{x_i : R_n = 1\}$ adjoin the generators t_j and the relations $t_j\{ w (x)\}^{-1} = 1$, obtaining

$$G = \{x_i, t_j : R_n(x_1, \ldots, x_r) = t_j\{w_j(x_1, \ldots, x_r)\}^{-1} = 1 \}.$$

Now replace each x_i by $W_i(t)$ and delete the generators x_i. We then obtain the required presentation with generating relations

$$R_n(W_1(t), W_2(t), \ldots, W_r(t)) = t_j\{w_j(W_1(t), \ldots, W_r(t))\}^{-1} = 1.$$

We note, in passing, that it is not generally true that the "inherited" relations $R_n(W_1(t), W_2(t), \ldots, W_r(t)) = 1$ are an adequate set of defining relations. We give later an example where the "extra" relations $t_j\{w_j(W_1(t), \ldots, W_r(t))\}^{-1} = 1$ cannot be deleted.

We now return to the solution of the main problem. Since the subgroup His defined by a finite set of words and is of finite index, the Todd-Coxeter coset enumeration process must close (see Mendelsohn [3]). Also by Mendelsohn [3], a set of Schreier-Reidemeister generators for *H* can be obtained and a rule for determining in which coset of ***Ha*** word in G lies. With this information we can write down a set of defining relations for ***H*** (as given, for example, in [2] pp. 86-95). Also by Benson and Mendelsohn [1] the Schreier-Reidemeister generators can be expressed as words in the originally given generators of H. We now start a second coset enumeration using the Schreier-Reidemeister generators as the defining generators for H. This enables us to write the originally given generators of H as words in the Schreier-Reidemeister generators. Now, by the use of the lemma, we are in a position to write defining relations for H in terms of its originally given generators.

Remark. It appears that we have given an extremely roundabout procedure for obtaining defining relations for H in terms of its given generators. Why introduce the Schreier-Reidemeister generators at all?

The following appears to be a plausible direct procedure. Every relation in G can be written as a product of conjugates of the given relations $R_i = 1$. Hence, the group H inherits as relators the conjugates of R_i when expressed as words in the generators of H.

It would appear that it is sufficient to take as conjugating elements one from each coset of H. Hence H inherits the relators $\sigma_j^{-1} R_i\sigma_j$ where R_i ranges over the defining relators of G, σ_j ranges over a set of coset representatives and $\sigma_j^{-1}R_i\sigma_j$ is expressed as a word in H.

The following counter example shows that these inherited relators are not necessarily a set of defining relators for H. The group was studied by Baumslag and Solitar.

Let G = $\{A, X : X^{-1}A^2X = A^3\}$. Let H be the subgroup generated by X and A^8. By Benson-Mendelsohn [1], H = G and in fact

$$A = A^8X^{-1}A^{-8}XA^8X^{-2}A^{-8}X^{-1}A^8XA^{-8}XA^8X^{-1}A^{-8}XA^8X.$$

Calling the right side of this equation Wit is seen that in terms of Xand A^8, the group G inherits the relation $X^{-2}W^2X = W^3$. Also, since G has only one coset and one defining relation no more than one relation can be obtained from coset enumeration. However, G. Higman has shown that in terms of X and A^8 the group G requires two defining relations. Hence the extra relation (in this case $A^8\ W^{-8} = 1$) cannot be deleted.

REFERENCES

1. C. T. Benson and N. S. Mendelsohn: A calculus for a certain class of word problems in groups. ***J. Combinatorial Theory*** **1** (1966), 202–208.
2. W. Magnus, A. Karrass and D. Solitar: ***Combinatorial Group Theory*** (Interscience Publishers, New York, 1966).
3. N. S. Mendelsohn: An algorithmic solution for a word problem in group theory. ***Canad. J. Math.*** 16 (1964), 509-516; correction 17 (1965), 505.

Nielsen transformations

M. J. DUNWOODY

LET G be a group with n generators. Let Σ be the set of ordered sets of n generators of G.

If π is a permutation of the set $\{1, 2, \dots, n\}$ then a, will denote the permutation of Σ such that

$$(g_1, \dots, g_n)\alpha_\pi = (g_{1\pi}, g_{2\pi}, \dots, g_{n\pi}).$$

If $i, j \in \{1, 2, \dots, n\}$, $i \neq$ j, then α_{-i}, $a_{i:j}$ will denote the permutations of Σ such that

$$(g_1, \dots, g_n)\alpha_{-i} = (g_1, g_2, \dots, g_{i-1}, g_i^{-1}, g_{i+1}, \dots, g_n),$$

$$(g_1, \dots \quad g_n)\alpha_{i:j} = (g_1, ., g_{j-1}, g_i g_j, g_{j+1}, \dots, g_n).$$

Let A be the group of permutations of Σ generated by all the above.

It is sometimes useful in group theory to know the transitivity classes of Σ under A. Let F be the free group on generators $x_1, x_2, \dots, x_n$. If $(g_1, g_2, \dots, g_n)$, $(h_1, h_2, \dots, h,)$ belong to Σ and R, S are the kernels of the respective homomorphisms θ, ϕ of ,F onto G such that $x_i\theta = g_i$, $x_i\phi = h_i$, i= 1, ... n, then there is an automorphism γ of F such that $Ry = S$ if $(g_1, g_2, \dots, g_n)$, $(h_1, h_2, \dots, h,)$ belong to the same transitivity class of Σ under A. When such an automorphism of F exists there is for instance an isomorphism induced between $F/[R, R]$ and $F/[S,$ S]; these groups need not be isomorphic if $(g_1, g_2, \dots, g_n)$, $(h_1, h_2, \dots, h,)$ belong to different transitivity classes under A.

The problem I consider is the following:

If G has n- 1 generators, then in every transitivity class of Σ under A is there a set of generators one of which is the unit element?

The answer to this question is yes if G is finite and soluble; in fact one has the following :

THEOREM. *If G is a finite soluble group with n-* 1 *generators, then A is transitive on Σ.*

Proof. The proof is by induction on the length c of a chief series of G. If c = 0, the theorem is trivial. Assume then that $c > 0$, and that the result is true for c- 1.

Suppose now that

$$E = M_0 < M_1 < M_2 < \dots < M_c = G$$

is a chief series for G. Let $h_1, \ldots, h_{n-1}$ be a set of $\boldsymbol{n}$- 1 generators for G. Let $(g_1, \ldots. g_n) \in \Sigma$, by the induction hypothesis on G/M_1 there exists $\boldsymbol{a} \in$ A such that

$$(g_1, \ldots, g_n)\alpha = (m, m_1h_1, m_2h_2, \ldots, m_{n-1}h_{n-1})$$

where $\boldsymbol{m}, m_1, m_2, \ldots, m_{n-1} \in M_1$. If $\boldsymbol{m} =$ e, then $m_1h_1, m_2h_2, \ldots, m_{n-1}h_{n-1}$ generate G and by using a product of the $\alpha_{i:1}$'s and their inverses we obtain a set of generators in which the first element belongs to M_1 and is not e. Therefore it can be assumed that $\boldsymbol{m} \neq \boldsymbol{e}$.

Now, since M_1 is abelian, if

$$g = w(h_1, h_2, \ldots . h_{n-1}) \in G$$

then

$$\begin{aligned} g^{-1}mg &= w(h_1, \ldots, h_{n-1})^{-1}mw(h_1, \ldots, h_{n-1}) \\ &= w(m_1h_1, , \ldots, m_{n-1}h_{n-1})^{-1}mw(m_1h_1, \ldots, m_{n-1}h_{n-1}). \end{aligned}$$

It follows that there is an element a' in A such that

$$(g_1, \ldots, g_n)\alpha' = (m^g, m_1h_1, \ldots, m_{n-1}h_{n-1}).$$

Now using $\alpha_{1;i+1}$ or its inverse the $(i+1)$th term can be changed to $m^g m_i h_i$ or $m^{-g}m_ih_i$. However, since M_1 is minimal normal, each m_i is a product of conjugates of $\boldsymbol{m}$ or its inverse. Hence by repeating the above process enough times it can be seen that there exists a" in A such that

$$(g_1, \ldots, g_n)\alpha'' = (m, h_1, h_2, \ldots, h_{n-1}).$$

However $h_1, \ldots, h_{n-1}$ generate G and so by using a product of the $\alpha_{i:1}$'s and their inverses we see that $(g_1, \ldots,$ g,) belongs to the same transitivity class under A as (e, $h_1, h_2, \ldots, h_n$), which proves the theorem.

To find a counter-example for the non-soluble case a computer might be employed. If G is the alternating group on five symbols and Σ is the set of sets of three elements which generate G, then Σ has 120× 1668 elements [**1**]. These are partitioned into 1668 transitivity classes under the action of automorphisms of G, and $\boldsymbol{A}$ can be regarded as acting on these classes rather than on the elements of Σ. If $\boldsymbol{A}$ is not 19-ply transitive on these classes, then the direct product of 19 copies of G, which can be generated by two elements, would have a set of three elements which generate it but which could not be reduced to two elements by Nielsen transformations.

REFERENCE

1. P. HALL: The Eulerian functions of a group. ***Quart.*** *J. Maths.* (Oxford Series) 7 (1936), 134–151.

Calculation with the elements of a finite group given by generators and defining relations

H. JÜRGENSEN

1. Preliminary remarks. The system of group theoretical programmes working at Kiel [4] consists of programmes which are independent of, and others which depend on, the special way in which the elements of the group to be calculated are represented. The latter are, roughly speaking, concerned with reading the input data and printing, multiplication of, and inverting elements.

I shall give an outline of some difficulties which arise with multiplication and inverting programmes, when the elements are represented by words of abstract generators, and of some ways to overcome or avoid them.

In 1961 Neubüser [3] described a programme by which these problems were, to a certain extent, solve8 for finite p-groups. In 1962 and 1963 Lindenberg published ideas [1] and a detailed description of a programme [2] for solving them for finite soluble groups.

Thus in a certain sense no theoretical difficulties were left; but, as experience proved, the practical problem of "minimizing" the time needed for computing the product of two elements, when just the necessary input data would be given, was not yet solved sufficiently. Hence some further refinements had to be introduced.

2. Input data. Let G be a finite group and e the identity element of G. An AG-system of G is a system of ***n*** generators $\boldsymbol{a_n}$, $a_{n-1}, \ldots, a_1$ of G and of $\boldsymbol{n(n+}1)/2$ words g_{ij} ($i = 1(1)j$; $j = 1(1)n$), for which the following conditions hold :

$$g_{ij} \in U_{j-1} = \mathrm{gp}(e, a1, a_2, \ldots, a_{j-1}) \subseteq G; \quad 1 \leqslant i \leqslant j \leqslant n \tag{R1}$$

$$a_j^{\psi_j} = g_{jj}; \quad 1 \leqslant j \leqslant n \tag{R2}$$

$$[a_i, a_j] = g_{ij}; \quad 1 \leqslant i < j \leqslant n \tag{R3}$$

$$\psi_j > 1 \text{ integer}; \; a_j^\tau \notin U_{j-1}; \; I \leqslant \tau < \psi_j; \quad 1 \leqslant j \leqslant n \tag{R4}$$

For a group G there exists an AG-system defining G, if and only if G is a finite soluble group.

Proof. Let an AG-system defining G be given. According to (R3) and (R1) a_j ($1 \leqslant j \leqslant n$) is an element of the normalizer $N_{U_{j-1}}$ of U_{j-1}, i.e. $U_{j-1} \lhd U_j$.

Because of (R1), (R2), and (R4) U_j/U_{j-1} is a finite cyclic group of order greater than 1; hence G is a finite soluble group.

Now let G be a finite soluble group. If G is cyclic, it will be defined by the generator a_1 with $g_{11} = e$ and $\psi_1 = |G|$. If G is not cyclic, there exists a finite chain of subgroups $U_0, U_1, \ldots, U_n$ of G with: $U_0 =$ gp(e); $U_n = G$; $U_{j-1} \lhd U_j$; U_j/U_{j-1} is cyclic and finite of order $Uj : U_{j-1} > 1$ $(1 \leqslant j \leqslant n)$. For $j = 1(1)n$ a_j is selected in such a way that gp($U_{j-1}, a_j) = U_j$; ψ_j will be defined as $U_j : U_{j-1}$ ((R4) holds). Then the words g_{ij} can be found such that (R1), (R2), and (R3) hold. For the proof that G is defined by an *AG*-system chosen like this we define:

A word $a_{\nu_m}^{\varepsilon_{\nu_m}} a_{\nu_{m-1}}^{\varepsilon_{\nu_{m-1}}} \ldots a_{\nu_1}^{\varepsilon_{\nu_1}} \in G\,(1 \leqslant \nu_i \leqslant n;$ ε_{ν_i} integer; $\boldsymbol{i} = 1(1)n)$, for which the following conditions hold, is called a normed word:

$$\nu_i < \nu_{i+1}; \qquad 1 \leqslant i < m \tag{N1}$$

$$\boldsymbol{0} \leqslant \varepsilon_{\nu_i}; \qquad 1 \leqslant i \leqslant m \tag{N2}$$

$$\varepsilon_{\nu_i} < \psi_{r_i}; \qquad 1 \leqslant i \leqslant m \tag{N3}$$

If only (N1) and (N2) hold, the word is called seminormed.

As $a_j \notin U_{j-1}$ and $a_j \in N_{U_{j-1}}$ $(1 \leqslant j \leqslant n)$, U_j can be decomposed into cosets:

$$U_j = U_{j-1} + a_j U_{j-1} + a_j^2 U_{j-1} + \ldots + a_j^{\psi_j - 1} U_{j-1}$$

Hence for every word in G there exists a normed word, which is equivalent to it. Since $|G| = \prod_{j=1}^{n} \psi_j$, the set of words of G can be represented uniquely by the set G^* of normed words in G, and G is defined by the AG-system.

As a secondary result of this proof we have : Let an AG-system defining G be given; the words g_{ij} can be written as normed ones.

3. Multiplication algorithm. In the following text the symbol U_j^* will denote the set of normed words in U_j. According to the proof from above, (R1) may and for practical purposes will now be replaced by the stronger condition:

$$g_{ij} = a_{j-1}^{\sigma_{j-1}^{(i,j)}} \; a_{j-2}^{\sigma_{j-2}^{(i,j)}} \cdot \cdot \cdot \; a_{1}^{\sigma_{1}^{(i,j)}} \in U_{j-1}^* \subseteq G; \quad 1 \leqslant i \leqslant j \leqslant n \tag{R1$'$}$$

As far as finite groups defined by AG-systems are concerned, the word problem is no obstacle.

There exists a well-defined finite algorithm by which the product $\boldsymbol{bc} \in \boldsymbol{G^*}$ is obtained for any two words $\boldsymbol{b}, c \in$ G, where $\boldsymbol{b}$ is seminormed, c is normed, and G is a finite group defined by an AG-system.

Proof. Use induction on t with $\boldsymbol{b}$, c $\in U_t$. The algorithm itself will be defined by the proof.

(1) $t = 1$: $\boldsymbol{b}$, c $\in U_1$ have the forms $\boldsymbol{b} = a_1^{\varepsilon_1}$ (seminormed), c $= a_1^{\delta_1}$ (normed). The normed product $bc \in U_1^*$ is defined by

$$bc = a_1^{\varepsilon_1 + \delta_1 - \psi_1 \text{ entier } ((\varepsilon_1 + \delta_1)/\psi_1)}$$

The proposition holds.

(2) Let the proposition be proved for $1 \leq t < k \leq n$.

(3) $t = k$: $b, c \in U_t = U_k$ have the forms

$b = a_k^{\varepsilon_k} a_{k-1}^{\varepsilon_{k-1}} \cdots a_1^{\varepsilon_1}$ (seminormed)

$c = a_k^{\delta_k} a_{k-1}^{\delta_{k-1}} \cdots a_1^{\delta_1}$ (normed).

$bc \in U_k^*$ is obtained by norming the words $w_1, w_2, \ldots, w_k$ of the sequence $a_1^{\varepsilon_1}c = a_1^{\varepsilon_1}w_0 = w_1$, $a_2^{\varepsilon_2}w_1 = w_2, \ldots, a_k^{\varepsilon_k}w_{k-1} = w_k = bc$.

To obtain $a_i^{\varepsilon_i}w_{i-1} \in U_k^*$ $(1 \leq i \leq k)$ ε_i times products of the form

$$a_i a_k^{\eta_k} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1}$$

with

$$a_k^{\eta_k} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1} \in U_k^*$$

have to be normed.

(3.1) $i = k$: We define

$$a_k a_k^{\eta_k} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1} = \begin{cases} a_k^{\eta_k+1} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1} \in U_k^*; & \eta_k + 1 < \psi_k \\ g_{kk} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1}; & \eta_k + 1 = \psi_k. \end{cases}$$

For $\eta_k + 1 = \psi_k$ the proposition follows from assumption (2).

(3.2) $i < k$: Proof by induction on η_k.

(3.2.1) $\eta_k = 0$: The proposition follows from assumption (2).

(3.2.2) Suppose the proposition has been proved for $0 \leq \eta_k < \lambda < \psi_k$.

(3.2.3) $\eta_k = \lambda$: The word to be normed has the form

$$a_i a_k^{\lambda} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1},$$

which is equivalent to

$$a_k a_i g_{ik} a_k^{\lambda-1} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1}.$$

According to assumption (3.2.2) the proposition holds for

$$s = g_{ik} a_k^{\lambda-1} a_{k-1}^{\eta_{k-1}} \cdots a_1^{\eta_1},$$

which will be normed to a word

$$a_k^{\zeta_k} a_{k-1}^{\zeta_{k-1}} \cdots a_1^{\zeta_1},$$

where $\zeta_k = \lambda - 1$, since $s \in U_{k-1}^* a_k^{\lambda-1} U_{k-1}^* = a_k^{\lambda-1} U_{k-1}^*$.
According to assumption (3.2.2) it holds for

$$a_i a_k^{\lambda-1} a_{k-1}^{\zeta_{k-1}} \cdots a_1^{\zeta_1},$$

and hence the proposition is proved.

4. Multiplication programme. A machine programme which strictly follows this algorithm will be rather slow; the reasons are that it is recursive, and that the input data, i.e. the words g_{ij} and the integers ψ_j and $\boldsymbol{n}$, which are constants throughout all calculations with the elements of a given group, have to be looked up for every multiplication again and again.

We could naturally save some computing machine time if a special multiplication programme was written for every AG-system. For a trained programmer this might take less time than doing all the group calculation by hand.

As had been realized for groups whose orders are powers of 2 by Neubüser, and with a different sort of defining systems for finite soluble groups by Lindenberg, a compromise would be to write a programming programme C, which will generate the multiplication programme M needed according to the special AG-system given.

I shall give a rough sketch of C in terms of M. C has been running at Kiel since 1965.

M is generated in two steps. First a multiplication programme M^* and an inverting programme INV are generated, for which just the input data, i.e. the AG-system given, are used. Then M itself is generated as an improved version of M^* in such a way that parts of M^* are replaced by new ones according to further relations which will be computed by M^*.

M and M^* both consist of a main programme H, the structure of which is the same in M and M^*, and a set of subroutines $P\langle i, j, \boldsymbol{k}\rangle$.

4.1. ***The programme H*** (see flow chart). The normed elements $a_n^{\varepsilon_n} a_{n-1}^{\varepsilon_{n-1}} \dots a_1^{\varepsilon_1} \in G^*$ are uniquely represented by the integers

$$\varepsilon_1 + \sum_{i=2}^{n} \left(\varepsilon_i \cdot \prod_{j=1}^{i-1} 2^{1+\text{entier } (\log_2(\psi_j - 1))} \right)$$

With 27 binary digits per machine word of the electronic computer used by us (Electrologica Xl) the group elements can normally be stored in one word each, when this representation is used.†

In the beginning of $\boldsymbol{H}$ the exponents ε_i of $\boldsymbol{b}$ and δ_i of c $(\boldsymbol{i} = 1(1)n)$ are isolated and stored to separate machine words.

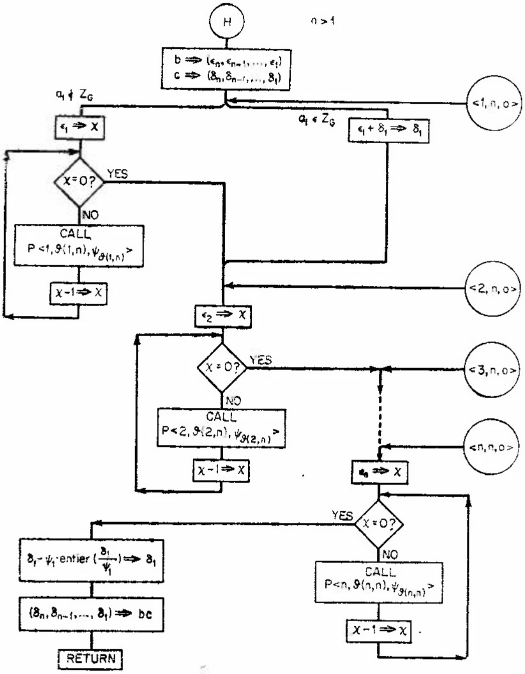
†The number of binary digits needed for the elements of a group G is

$$n + \sum_{i=1}^{n} \text{entier } (\log_2(\psi_i - 1)) < n + \sum_{i=1}^{n} \text{entier } (\log, \psi_i) \leqslant n + \text{entier } (\log, \prod_{i=1}^{n} \psi_i)$$
$$= n + \text{entier } (\log, |G|).$$

The representation which will need the fewest binary digits is

$$\varepsilon_1 + \sum_{i=2}^{n} \left(\varepsilon_i \cdot \prod_{j=1}^{i-1} \psi_j \right);$$

for a binary machine; however, isolating the ε_i will generally take more time, because divisions instead of shifting operations will be needed for the elements stored like this.



Then for $\boldsymbol{i} = 1(1)n$ the element $w_i = a_i a_n^{\delta_n} a_{n-1}^{\delta_{n-1}} \ldots a_1^{\delta_1}$ is normed ε_i times in such a way that the machine words, where the exponents δ_i are stored, will afterwards contain the exponents of the result.

For $\boldsymbol{i} = 1(1)k$ and $\boldsymbol{k} = 1(1)n$ we define the natural number $\theta(i, \boldsymbol{k})$ by:

$$g_{i,\,\theta(i,\,k)+t} = e \quad \text{if} \quad \theta(i, k) < t+\theta(i, k) \leqslant k \tag{1}$$

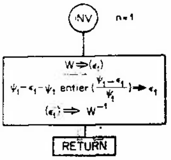
$$g_{i,\,\theta(i,k)} \neq e \ \text{ or } \ i = \theta(i, k). \tag{2}$$

Since from $g_{ij} = \mathrm{e}$ $(i<j)$ follows $a_i a_j^{\delta_j} = a_j^{\delta_j} a_i$, norming w_i is equivalent to norming $w_i' = a_i a_{\theta(i,\,n)}^{\delta_{\theta(i,\,n)}} a_{\theta(i,\,n)-1}^{\delta_{\theta(i,\,n)-1}} \ldots a_1^{\delta_1}$ and leaving $\delta_n, \delta_{n-1}, \ldots, \delta_{\theta(i\ n)+1}$ unchanged.

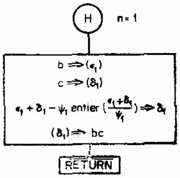
What ***H*** actually does for norming w_i is to call the subroutine $P\langle i, \theta(i, n), \psi_{\theta(i,\,n)}\rangle$.

Since $g_{11} = \mathrm{e}$ in any AG-system, the generator a_1 is treated in a special way throughout M^* and ***M:*** It is not necessary to reduce δ_1 modulo ψ_1 whenever $\delta_1 \geqslant \psi_1$; but this is done once at the end of ***H*** only. Furthermore if a_1 is an element of the centre of G, i.e. $\theta(1, \boldsymbol{n}) = 1$, calling $P\langle 1, \theta(1, n), \psi_{\theta(1,\,n)}\rangle$ ε_1 times is replaced by adding ε_1 to δ_1.

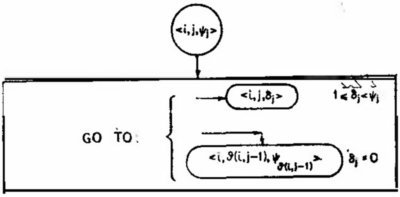
Before ***His*** returned from, the exponents δ_i will be "compressed" and stored to one machine word again as representation of the normed product bc.



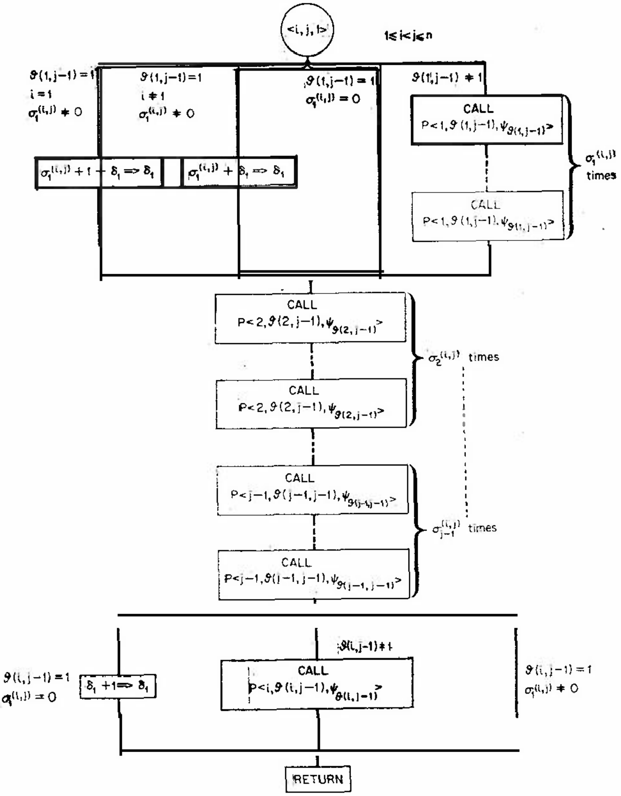
NV
$n=1$
$W \Rightarrow (\epsilon_1)$
$\psi_1 - \epsilon_1 - \psi_1$ entier $(\frac{\psi_1 - \epsilon_1}{\psi_1}) \Rightarrow \epsilon_1$
$(\epsilon_1) \Rightarrow W^{-1}$
RETURN



H
$n=1$
$b \Rightarrow (\epsilon_1)$
$c \Rightarrow (\delta_1)$
$\epsilon_1 + \delta_1 - \psi_1$ entier $(\frac{\epsilon_1 + \delta_1}{\psi_1}) \Rightarrow \delta_1$
$(\delta_1) \Rightarrow bc$
RETURN



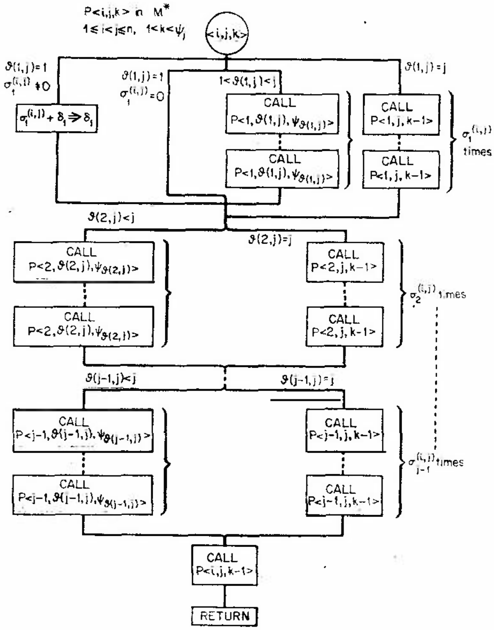
$<i,j,\psi_j>$
GO TO
$<i,j,\delta_j>$
$1 \leq \delta_j < \psi_j$
$<i,\vartheta(i,j-1),\psi_{\vartheta(i,j-1)}>$
$\delta_j = 0$



$<i,j,1>$
$1 \leq i < j \leq n$
$\vartheta(1,j-1)=1$
$i=1$
$\sigma_1^{(i,j)} \neq 0$
$\vartheta(1,j-1)=1$
$i \neq 1$
$\sigma_1^{(i,j)} \neq 0$
$\vartheta(1,j-1)=1$
$\sigma_1^{(i,j)} = 0$
$\vartheta(1,j-1) \neq 1$
$\sigma_1^{(i,j)} + 1 + \delta_1 \Rightarrow \delta_1$
$\sigma_1^{(i,j)} + \delta_1 \Rightarrow \delta_1$
CALL
$P<1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}>$
CALL
$P<1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}>$
$\sigma_1^{(i,j)}$ times
CALL
$P<2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}>$
CALL
$P<2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}>$
$\sigma_2^{(i,j)}$ times
CALL
$P<j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}>$
CALL
$P<j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}>$
$\sigma_{j-1}^{(i,j)}$ times
$\vartheta(i,j-1)=1$
$\sigma_i^{(i,j)} = 0$
$\delta_1 + 1 \Rightarrow \delta_1$
$\vartheta(i,j-1) \neq 1$
CALL
$P<i,\vartheta(i,j-1),\psi_{\vartheta(i,j-1)}>$
$\vartheta(i,j-1)=1$
$\sigma_i^{(i,j)} \neq 0$
RETURN

4.2. The subroutines $P\langle i, j, \psi_j\rangle$ $(1 \leq i < j \leq n)$. These subroutines just consist of a "go-to-instruction", which will lead to the subroutine $P\langle i, j, \delta_j\rangle$ for $\delta_j > 0$ and to $P\langle i, \theta(i, j-1), \psi_{\theta(i, j-1)}\rangle$ for $\delta_j = 0$, according to the actual value of δ_j (see flow chart).

4.3. The subroutines $P\langle i, j, k)$ $(1 \leq i < j \leq n;\ 1 \leq k < \psi_j)$. The element $a_i a_j^k a_{j-1}^{\delta_{j-1}} \dots a_1^{\delta_1}$ will be normed. $P\langle i, j, k)$ will (in most cases) call further subroutines according to g_{ij} (see flow charts).



4.4. The subroutines P $(j, j, \psi_j\rangle$ $(1 \leq j \leq n)$. The element $a_j a_j^{\delta_j} a_{j-1}^{\delta_{j-1}} \dots a_1^{\delta_1}$ will be normed. $P(j, j, \psi_j\rangle$ will call further subroutines according to g_{jj}, if $\delta_j + 1 = \psi_j$ (see flow chart).?

4.5. The inverting programme (see flow chart). When M^* is finished an inverting programme INV will be generated.

The word $w = a_n^{\varepsilon_n} a_{n-1}^{\varepsilon_{n-1}} \dots a_1^{\varepsilon_1} \in G^*$ is inverted by successively norming the following words :

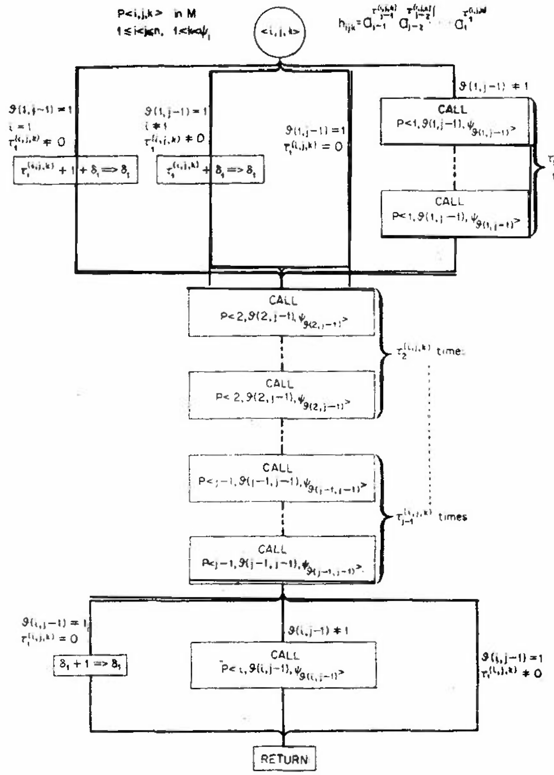
$$a_n^{|a_n| - \varepsilon_n} e = w_1$$

$$a_n^0 a_{n-1}^{|a_{n-1}| - \varepsilon_{n-1}} w_1 = w_2$$

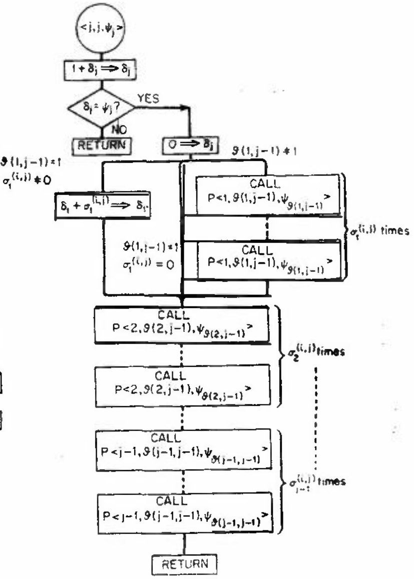
$$\vdots$$

$$a_n^0 a_{n-1}^0 \dots a_2^0 a_1^{|a_1| - \varepsilon_1} w_{n-1} = w_n = w^{-1}$$

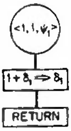
† All those subroutines $P\langle i, j, k\rangle$ will be generated for M^*, for which (a) $1 < i = j \leq n$ and $k = \psi_j$, or (b) $1 \leq i < j \leq n$ and $1 \leq k \leq \psi_j$ and $g_{ij} \neq e$, or (c) $i = j = 1$ and $\theta(1, n) \neq 1$ and $k = \psi_1$.

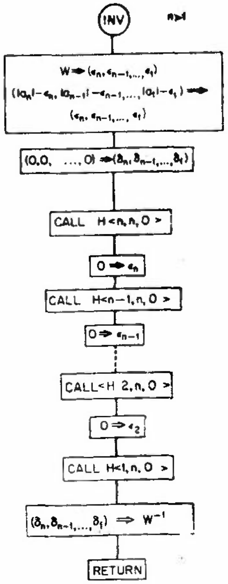

$P\langle i,j,k\rangle$ in M
$1 \leq i < j \leq n,\ 1 < k < \psi_i$
$\langle i,j,k\rangle$
$h_{ijk} = a_{j-1}^{\tau_{j-1}^{(i,j,k)}} a_{j-2}^{\tau_{j-2}^{(i,j,k)}} \cdots a_1^{\tau_1^{(i,j,k)}}$
$\vartheta(1,j-1) = 1$
$i = 1$
$\tau_1^{(i,j,k)} \neq 0$
$\tau_1^{(i,j,k)} + 1 + \delta_1 \Rightarrow \delta_1$
$\vartheta(1,j-1) = 1$
$i \neq 1$
$\tau_1^{(i,j,k)} \neq 0$
$\tau_1^{(i,j,k)} + \delta_1 \Rightarrow \delta_1$
$\vartheta(1,j-1) = 1$
$\tau_1^{(i,j,k)} = 0$
$\vartheta(1,j-1) \neq 1$
CALL
$P\langle 1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}\rangle$
CALL
$P\langle 1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}\rangle$
$\tau_1^{(i,j,k)}$ times
CALL
$P\langle 2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}\rangle$
CALL
$P\langle 2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}\rangle$
$\tau_2^{(i,j,k)}$ times
CALL
$P\langle j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}\rangle$
CALL
$P\langle j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}\rangle$
$\tau_{j-1}^{(i,j,k)}$ times
$\vartheta(i,j-1) = 1$
$\tau_i^{(i,j,k)} = 0$
$\delta_i + 1 \Rightarrow \delta_i$
$\vartheta(i,j-1) \neq 1$
CALL
$P\langle i,\vartheta(i,j-1),\psi_{\vartheta(i,j-1)}\rangle$
$\vartheta(i,j-1) = 1$
$\tau_i^{(i,j,k)} \neq 0$
RETURN

(1) $1 < j \leq n$


$\langle j,j,\psi_j\rangle$
$1 + \delta_j \Rightarrow \delta_j$
$\delta_j = \psi_j$?
YES
NO
RETURN
$0 \Rightarrow \delta_j$
$\vartheta(1,j-1) = 1$
$\sigma_1^{(i,j)} \neq 0$
$\delta_1 + \sigma_1^{(i,j)} \Rightarrow \delta_1$
$\vartheta(1,j-1) \neq 1$
CALL
$P\langle 1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}\rangle$
CALL
$P\langle 1,\vartheta(1,j-1),\psi_{\vartheta(1,j-1)}\rangle$
$\sigma_1^{(i,j)}$ times
$\vartheta(1,j-1) = 1$
$\sigma_1^{(i,j)} = 0$
CALL
$P\langle 2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}\rangle$
CALL
$P\langle 2,\vartheta(2,j-1),\psi_{\vartheta(2,j-1)}\rangle$
$\sigma_2^{(i,j)}$ times
CALL
$P\langle j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}\rangle$
CALL
$P\langle j-1,\vartheta(j-1,j-1),\psi_{\vartheta(j-1,j-1)}\rangle$
$\sigma_{j-1}^{(i,j)}$ times
RETURN

(2) $j = 1$


$\langle 1,1,\psi_1\rangle$
$1 + \delta_1 \Rightarrow \delta_1$
RETURN


INV
$n > 1$
$W \Rightarrow (\epsilon_n, \epsilon_{n-1}, \ldots, \epsilon_1)$
$(|a_n| - \epsilon_n, |a_{n-1}| - \epsilon_{n-1}, \ldots, |a_1| - \epsilon_1) \Rightarrow$
$(\epsilon_n, \epsilon_{n-1}, \ldots, \epsilon_1)$
$(0, 0, \ldots, 0) \Rightarrow (\delta_n, \delta_{n-1}, \ldots, \delta_1)$
CALL $H\langle n,n,0\rangle$
$0 \Rightarrow \epsilon_n$
CALL $H\langle n-1,n,0\rangle$
$0 \Rightarrow \epsilon_{n-1}$
CALL $\langle H\ 2,n,0\rangle$
$0 \Rightarrow \epsilon_2$
CALL $H\langle 1,n,0\rangle$
$(\delta_n, \delta_{n-1}, \ldots, \delta_1) \Rightarrow W^{-1}$
RETURN

It is important here that the multiplication algorithm is defined for seminormed words as left factors. For computing $|a_i|$ $(i = 1(1)n)$ M^* is used.

4.6. M developedfrom M.* What proved to be most time-consuming is that with an AG-system given the number of steps to be taken for norming the word $a_ia_j^{\delta_j}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1}$ will in general increase rather fast, when δ_j is increased.

As a remedy further normed words $h_{ijk} = [a_i, a_j^k]$ $(1 \leqslant i < j \leqslant n;$ $2 \leqslant k < \psi_j)$ are introduced, if there exist i and j $(1 \leqslant i<j\leqslant n)$ such that $\psi_j \neq 2$ and $g_{ij} \neq$ e. For computing these normed words M^* is used.

In M^* norming $a_ia_j^{\delta_j}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1}$ for $i<j$ and $\delta_j>1$ is based on the equation

$$a_ia_j^{\delta_j}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1} = a_ja_ig_{ij}a_j^{\delta_j-1}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1}.$$

The subroutines $P\langle i$, j, $k)$ of M^* for $i<j$ and $1 <k<\psi_j$, which norm the words $a_ia_j^ka_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1}$ can be replaced by others, which use the equation

$$a_ia_j^{\delta_j}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1} = a_j^{\delta_j}a_ih_{ij\,\delta_j}a_{j-1}^{\delta_{j-1}}\dots a_1^{\delta_1},$$

when the words h_{ijk} have been computed; in this way M is generated.[†]

When Neubüser and Lindenberg wrote their programming programmes, the problem of introducing further relations, which are not part of the input data, did not occur. The programme of Neubüser worked only for groups whose order is a power of 2, and $\psi_j = 2$ for j $= 1(1)n$; hence no words h_{ijk} existed. Lindenberg, on the other hand, uses defining systems as input data, which contain not only those words which correspond to the words g_{ij} in an AG-system, but also those which correspond to the words h_{ijk} and hence can for soluble groups be deduced from the rest.

5. Some extensions planned.

(a) For C it has been assumed that in an AG-system the words g_{ij} are normed ones. It is easy to prove that there exists a well-defined finite algorithm, by which the normed equivalents of the words g_{ij} in any *AG*-system will be obtained, if they are of finite "length". Programming this will make the preparation of input data less troublesome.

(b) In defining systems conjugates of the generators instead of commutators may be used (K-system).

(c) Although there does not exist an AG-system defining the alternating group of order 60, for example, there exists a system with products instead

[†] All those subroutines $P\langle i$, j, k) will be generated for ***M***, for which (a) $1 < i = j \leqslant n$ and $k = \psi_j$ or (b) $1 \leqslant i < j \leqslant n$ and $k = 1, \psi_j$ and $g_{ij} \neq e$ or (c) $1 \leqslant i < j \leqslant n$ and $1<k<\psi_j$ and $h_{ijk} \neq e$ or (d) $i = j = 1$ and $\theta(1, n) \neq 1$ and $k = \psi_1$.

Defining systems:

	AG	*K*	*P*	extended *P*	
(R1)	$g_{ij} \in \mathrm{gp}(e, a_1, a_2, \dots, a_{j-1})$		$g_{ij} \in \begin{cases} a_j^{\sigma(i,j)}\,\mathrm{gp}(e, a_1, \dots, a_{j-1}) & i<j \\ \mathrm{gp}(e, a_1, \dots, a_{j-1}) & i = j \end{cases}$	$g_{jik} \in \begin{cases} a_j^{\sigma(i,j,k)}\,\mathrm{gp}(e, a_1, \dots, a_{j-1}) & i < j;\ k = 1(1)\psi_j - 1 \\ \mathrm{gp}(e, a_1, \dots, a_{j-1}) & i = j;\ k = 1 \end{cases}$	$i = 1(1)j$ $j = 1(1)n$
(R2)	$a_j^{\psi_j} = g_{jj}$			$a_j^{\psi_j} = g_{jj1}$	$j = 1(1)n$
(R3)	$[a, a_j] = g_{ij}$	$a_j^{-1}a_ia_j = g_{ij}$	$a_ia_j = g_{ij}$	$a_ia_j^k = g_{ijk}$ $k = 1(1)\psi_j - 1$	$i = 1(1)j-1$ $j = 2(1)n$
(R4)	$\psi_j > 1;\ a_j^\tau \notin \mathrm{gp}(e, a_1, a_2, \dots, a_{j-1});\ \tau = 1(1)\psi_j - 1$				$j = 1(1)n$
	finite soluble groups		soluble and some non-soluble finite groups		

of commutators by which it may be defined.? Such systems (P-systems) exist as defining ones for every finite soluble group and even for some finite groups which are not soluble. If $\sigma_j^{(i,j)} = 1$ ($\boldsymbol{i} = 1(1)j-1$; $j = 2(1)n$), i.e. the group is soluble, there exists a well-defined finite multiplication algorithm.

(d) Some non-soluble finite groups may be calculated, when an "extended P-system" is given. As far as P-systems are concerned, the extended ones seem to be the "weakest" with a well-defined finite multiplication algorithm existing.

A new version of the programming programme, which is just being written, will allow the input data, i.e. the defining system, to be a mixture of ***AG*-**, *K*-, ***P*-**, and extended P-systems, and the words to be not necessarily normed ones.

REFERENCES

1. W. Lindenberg: Über eine Darstelhmg von Gruppenelementen in digitalen Rechenautomaten. *Num. Math.* 4 (1962), 151-153.
2. W. Lindenberg: Die Struktur eines Übersetzungsprogrammes zur Multiplikation von Gruppenelementen in digitalen Rechenautomaten. *Mitt. Rh- W. Inst. Znstr. Math.* Bonn 2 (1963), 1-38.
3. J. Neubüser: Bestimmung der Untergruppenverblnde endlicher p-Gruppen auf einer programmgesteuerten elektronischen Dualmaschine. *Num. Math. 3* (1961), 271-278.
4. See the papers by C. Brott, R. Bülow, K. Ferber, V. Felsch and J. Neubüser in these Proceedings.

† $a_1^2 = a_2^2 = a_3^3 = a_4^5 = e$, $a_1a_2 = a_2a_1$, $a_1a_3 = a_3a_2$, $a_1a_4 = a_4^2a_3a_2a_1$, $a_2a_3 = a_3a_2a_1$, $a_2a_4 = a_4^4a_2$, $a_3a_4 = a_4a_3^2a_2a_1$.

On a programme for the determination of the automorphism group of a finite group

V. FELSCH and J. NEUBÜSER

THE programme A for the determination of the automorphism group A(G) of a finite group G is part of a system of programmes for the investigation of finite groups implemented on an Electrologica Xl at the "Rechenzentrum der Universität Kiel". A detailed description [3] of A has been published in ***Numerische Mathematik.*** Therefore here we give only a short summary. Notations are as in [1].

The programme A makes use of information about the lattice of subgroups of the group G, provided by a programme Φ described in [2]. The programme A works as follows.

1. A system of generators and defining relations of G is determined. It is used later to decide whether a mapping from G onto G is a homomorphism. There are three cases:

1.1. If G is soluble, a system of generators $a_0 = 1, a_1, \dots, a$, is chosen such that the subgroups $U_i = (a_0, \dots, a_i \rangle$ form a subnormal series. For $i = 1(1)r$, let α_i be the least positive integer with $a_i^{\alpha_i} \in U_{i-1}$. Then

$$a_1^{\alpha_1} = 1, \qquad a_i^{\alpha_i} = a_1^{\nu_{i,1}} \cdots a_{i-1}^{\nu_{i,i-1}}, \qquad i = 2(1)r,$$

and

$$a_k a_i = a_1^{\mu_{k,i,1}} \dots a_{k-1}^{\mu_{k,i,k-1}} a_k, \qquad 1 \leq i < k \leq r,$$

are defining relations of G.

1.2. If G is nonsoluble, A searches for generators $a_0 = 1, a_1, \dots, a$, of G with the property: For $i = 1(1)r$ there exist integers $\alpha_i > 1$ such that each $g \in U_i = \langle a_1, \dots . a_i \rangle$ is obtained exactly once as g = $a_1^{\varepsilon_1} \dots a_i^{\varepsilon_i}$ with $0 \leq \varepsilon_j < \alpha_j$ forj = 1(1)i. Defining relations of the form

$$a_1^{\alpha_1} = 1, \qquad a_i^{\alpha_i} = a_1^{\nu_{i,1}} \cdots a_{i-1}^{\nu_{i,i-1}}, \qquad \mathrm{i} = 2(1)r,$$

and

$$a_k^{\beta} a_i = a_1^{\mu_{k,\beta,i,1}} \dots a_k^{\mu_{k,\beta,i,k}}, \qquad 1 \leq i < k \leq r, \quad 1 \leq \beta < \alpha_k,$$

are then determined.

1.3. If G does not possess such generators, then generators and defining relations must be provided as input by the user of the programme.

2. The coarsest equivalence relation, $\sim$ say, on the set of all subgroups of G, with the following properties is constructed:

(1) Each group of the lower and upper central series and of the commutator series of G forms a complete --class.

(2) $U \sim V$ implies: $|U| = |V|$; $N_G(U) \sim N_G(V)$; $C_G(U) \sim C_G(V)$; Uand V are both or *are* both not cyclic, abelian, nilpotent, supersoluble, soluble, perfect, normal in G, subnormal in G, or selfnormalizing ; for each $\sim$ -class $\mathfrak{K}$, U and V contain, are contained by, and normalize the same number of subgroups belonging to $\mathfrak{K}$ respectively.

3. For each element g $\in$ G the set H(g) of all $h \in$ G with (h)-(g) is determined. H(g) contains the set $J(g)$ of all images of g under A(G) and can be shown to be a "good approximation" of $J(g)$.

4. Generators $b_1, \ldots, b_s$ of G with minimal $d = \prod_{j=1}^{s} |H(b_j)|$ are selected. Then a list L of d bits is set up in 1 – l correspondence to the d different systems $b_1', \ldots, b_s'$ with $b_j' \in H(b_j)$. Systems $b_1', \ldots, b_s'$ not generating G are marked in L.

5. Generators $\varphi_1, \ldots, \varphi_m$ of the subgroup $I(G) \leqslant A(G)$ of inner automorphisms are determined from G/Z(G). For each $\varphi \in$ I(G) the system $b_1\varphi, \ldots. b_s\varphi$ is marked in L.

6. Let A, = I(G), $A_i \geqslant A$,,, the subgroup of $A(G)$ already calculated, and $b_1', \ldots, b_s'$ the first system not marked in L. Using the relations determined in § 1, it is checked if $b_j \rightarrow b_j'$ defines an endomorphism of G. If so this is an automorphism $\varphi_{i+1} \notin A_i$. Hence $A_{i+1} = \langle A_i, \varphi_{i+1} \rangle$ is constructed, and all systems $b_1\varphi, \ldots, b_s\varphi$ with $\varphi \in A_{i+1} - A_i$ are marked in L. Otherwise no automorphism of G maps, for any $\varphi \in A_i$, all b_j onto $b_j'\varphi$, and hence all systems $b_1'\varphi, \ldots, b_s'\varphi$ with $\varphi \in A_i$ are marked in L. All elements of $A(G)$ are obtained as soon as the number of unmarked bits in L is less than the order of the greatest known subgroup $A_i \leqslant A(G)$.

7. The order of and generators for $A(G)$ are printed. A typical running time for the combined programmes Φ and A is 8.5 minutes for a group of order 72 with automorphism group of order 3456.

REFERENCES

1. C. Brott and J. Neubüser: A programme for the calculation of characters and representations of finite groups. These Proceedings, pp. 101-1 10.

2. V. Felsch and J. Neubüser: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. ***Mitt. Rh.-W. Inst. f. Znstr. Math., Bonn 2*** (1963), 39-74.

3. V. Felsch and J. Neubüser: Über ein Programm zur Berechnung der Automorphismengruppe einer endlichen Gruppe. Numer. ***Math.*** 11 (1968), 277-292.

A computational method for determining the automorphism group of a finite solvable group

L. Gerhards and E. Altmann

Many problems in the theory of finite groups (especially of the extension theory) depend on the knowledge of the structure of the automorphism group $A(G)$ of a finite group G. In [2] a computer program for determining $A(G)$ of a finite group G has been given. With a view to the computational construction of $A(G)$ it seems to be profitable to develop systematically methods for determining $A(G)$ by "composition" of "allowable automorphisms" of special subgroups of G.

The main result of the present paper is a method for constructing the group $A(G)$ of a finite *solvable* group G of order $|G| = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$ by composition of special inner automorphisms of G and allowable automorphisms of $P_i (i = 1, \ldots, r)$, where the P_i are the Sylow subgroups of a complete Sylow basis of G.

The paper consists of three parts. In the first part (A, § 1), using the investigations of [1], ch. II, § 1, based on results of the theory of Sylow systems ([4], [5]) and general products ([1], [8], [9]), we explain a theoretical algorithm for constructing $A(G)$ by composition of $A(P_i)$ $(i = 1, \ldots, r)$ (A, § 2).

In the second part (B, § 5), using results obtained by the determination of the lattice $V(G)$ of all subgroups of G ([3], [6]), a computational method for constructing $A(G)$ will be developed by realization of the theoretical investigations of part A. In B, § 4, questions about computational representation of automorphisms are also discussed.

Finally in the third part (C, §§ 6, 7) possibilities for rationalization and extension of the program system to not necessarily solvable groups will be explained.

A. BASIC RESULTS FOR THE DETERMINATION OF A(G) FROM THE AUTOMORPHISM GROUPS $A(P_i)$ OF A SYLOW BASIS $P_1, \ldots, P_r$ OF G

1. Some results of the theory of Sylow systems and general products.

(a) *Sylow systems and Sylow system normalizers* ([4], [5]). Let G be a solvable group of order $|G| = q_1^{\alpha_1} \cdot \ldots \cdot q_r^{\alpha_r}$ (q_i primes). Then G contains for every q_i a q_i-Sylow-complement K_i ($i = 1, \ldots$, r) of order $K_i| = \prod_{\substack{j=1\\ j\neq i}}^{r} q_j^{\alpha_j}$, and every complete system $\mathfrak{K} = K_1, \ldots, K_r$ of q_i-Sylow-complements generates a complete Sylow system $\mathfrak{S}$ consisting of 2' subgroups $K_\varrho = \bigcap_{i \in e} K_i$, K_ϕ = G, defined by all subsets ϱ of the set of integers $\{1, \ldots, r\}$. If ϱ' denotes the complemented set of ϱ relative $(1, \ldots, r\}$, then $|K_\varrho| = \prod_{j \in e'} q_j^{\alpha_j}$ and for $\varrho, \sigma \subseteq \{1, \ldots, r\}$ we obtain the relations

$$(\alpha)\ K_{\varrho \cup \sigma} = K_\varrho \cap K_\sigma \tag{1.1}$$

$$(\beta)\ K_{\varrho \cap \sigma} = K_\varrho K_\sigma = K_\sigma K_\varrho.$$

Every two Sylow systems $\mathfrak{S}$, $\mathfrak{S}^*$ of G defined by $\mathfrak{K}$, $\mathfrak{K}^*$ are conjugate in G, and every Sylow system $\mathfrak{S}$ of G contains a complete Sylow ***basis***, i.e. a system $P_1, \ldots, P_r$ of Sylow subgroups of G such that G = $P_1 \cdot \ldots \cdot P_r$, $P_iP_k = P_kP_i$ $(i, k = 1, \ldots. r;\ i \neq k)$. Additionally we obtain $K_\varrho = \prod_{i \in \varrho} P_i$ $(\varrho \subseteq \{1, \ldots, r\})$ for all $K_\varrho \in \mathfrak{S}$.

The system normalizer $\mathfrak{N}(\mathfrak{S})$ defined by $\mathfrak{N}(\mathfrak{S}) = \{x \in G/x^{-1}K_\varrho x = K_\varrho$, for all $K_\varrho \in \mathfrak{S}\}$ can be represented as the intersection of the normalizers $N(K_i \subseteq G)$ or $N(P_i \subseteq G)$:

$$\mathfrak{N}(\mathfrak{S}) = \bigcap_{i=1}^{r} N(K_i \subseteq G) = \bigcap_{i=1}^{r} N(P_i \subseteq G). \tag{1.2}$$

$\mathfrak{N}(\mathfrak{S})$ is the direct product of its Sylow subgroups $P_i \cap N(K_i \subseteq G)$ $(i = 1, \ldots, r)$:

$$\mathfrak{N}(\mathfrak{S}) = P_1 \cap N(K_1 \subseteq G) \times \ldots \times P_r \cap N(K_r \subseteq G). \tag{1.3}$$

An automorphism a $\in A(G)$ of G maps the Sylow basis $P_1, \ldots, P_r$ of G on a conjugate one $P_1^*, \ldots, P_r^*$, that means there exists an element g $\in$ G such that

$$\alpha P_i = P_i^* = \tau(g)P_i \quad (i = 1, \ldots, r; \quad \tau(g) \in I(G)).^{\dagger} \tag{1.4}$$

The automorphism $\beta = \tau(g^{-1})$ o a $\in A(G)$ maps P_i onto P_i (i = 1, . . . , r), and the restriction of β on P_i yields an automorphism $\pi_i \in A(P_i)$ of P_i.

(b) ***General products*** ([8], [9], [1], ch. I). A group G is called a ***general product*** of the given abstract groups H_i (i = 1, 2) (or ***factored*** by ***Hi***) if and only if G contains two subgroups H_i^* such that $H_i^* \cong H_i$ and G = $H_1^*H_2^* = H_2^*H_1^*$, $H_1^* \cap H_2^* = \{e_G\}$.

Let G be factored by H_i ($i = 1, 2$), then to each $h_i \in H_i$ there corresponds a mapping $h_i\ k$ from H_i into H_i defined by:

$$h_1{}^2\ h_2 = H_1h_2h_1 \cap H_2 \qquad \text{for all } h_2 \in H_2, \tag{1.5}$$

$$h_2{}^1\ h_1 = h_2h_1H_2 \cap H_1 \qquad \text{for all } h_1 \in H_1. \tag{1.6}$$

† We denote by z(g) the automorphism of the inner automorphism group Z(G) of G induced by transformation by g $\in$ G.

The mappings $h_i{}^k$ $(i, k = 1, 2;\ i \neq k)$ together with the defining relations of H_i $(i = 1, 2)$ determine the structure of G; for multiplying the relation $(h_1^{-1}h_2H_1 \cap H_2)\cdot h_1{}^2\, h_2 = e_G$ with h_2h_1 from the left we obtain the following law for changing the components of an element of the general product G:

$$h_2h_1 = h_2{}^1\, h_1\cdot h_1{}^2\, h_2. \tag{1.7}$$

By (1.7) multiplication in G is completely determined.

Conversely, if H_1, H_2 are given groups and if according to (1.5), (1.6) each $h_i \in H_i$ $(i = 1, 2)$ is associated with a mapping $h_i{}^k$ $(i, k = 1, 2;\ i \neq k)$ from H_k into H_k, then the set $G = \{(\langle h_1, h_2\rangle / h_i \in H_i, (i = 1, 2))$ of all pairs $\langle h_1, h_2\rangle$ of elements $h_i \in H_i$ with the multiplication law

$$\langle h_1, h_2\rangle\cdot\langle h_1', h_2'\rangle = \langle h_1\cdot h_2'{}^1\, h_1,\ h_1'{}^2\, h_2\cdot h_2'\rangle \tag{1.8}$$

forms a group if and only if the following relations are valid :

$$\begin{array}{ll|l}
(a) & e_1{}^2h_2 = h_2 & e_2{}^1\, h_1 = h_1 \\
(\beta) & h_1{}^2\, e_2 = e_2 & h_2{}^1\, e_1 = e_1 \\
(\gamma) & (h_1\cdot h_1')\,{}^2\, h_2 = h_1'{}^2\,(h_1{}^2\, h_2) & (h_2\cdot h_2')\ I\, h_1 = h_2{}^1\,(h_2'{}^1\, h_1) \\
(6) & h_1{}^2\,(h_2\cdot h_2') = (h_2'{}^1h_1)\,{}^2\,h_2\cdot h_1{}^2\, h_2' & h_2{}^1\,(h_1\cdot h_1') = h_2{}^1\,h_1\cdot(h_1{}^2h_2)\,{}^1\, h;
\end{array} \tag{1.9}$$

The correspondence $h_1 \leftrightarrow \langle h_1, e_2\rangle$, $h_2 \leftrightarrow \langle e_1, h_2\rangle$ determines the isomorphism $H_1 \cong H_1^* = \{\langle h_1, e_2\rangle / h_1 \in H_1\}$, $H_2 \cong H_2^* = \{\langle e_1, h_2\rangle / h_2 \in H_2\}$ respectively. Because of $G = H_1^*H_2^*$, $H_1^* \cap H_2^* = \{\langle e_1, e_2\rangle\} = \{e_G\}$, $h_i^*{}^k\, h_k^* = (h_i{}^k\, h_k)^*$, G is a general product and conversely every general product can be represented in this way.

From (1.9 a, γ) it follows that the mappings $h_i{}^k$ form a permutation subgroup $\Pi_{i,k} \subseteq S_{|H_k|}$ of the symmetric group $S_{|H_k|}$ of degree $|H_k|$. The maximal invariant subgroup $N_i = \{h_i \in H_i / h_i{}^k\, h_k = h_k$, for all $h_k \in H_k\}$ of G contained in H_i determines the homomorphism $\tau_{i,\,k} : H_i \rightarrow \Pi_{i,\,k}$ from H_i onto $\Pi_{i,\,k}$. Hence :

$$H_i/N_i \cong \Pi_{i,\,k}, \tag{1.10}$$

and the mappings $(h_in_i)\,{}^k$ with $n_i \in N_i$ define the same permutation on H_k. Another important subgroup of the general product G is the "fix group" F_i of $\Pi_{k,\,i}$ defined by $F_i = \{h_i \in H_i / h_k{}^i\, h_i = h_i$, for all $h_k \in H_k\}$, containing all elements h_i of the component H_i, which are invariant against all mappings $h_k{}^i$ related to all elements $h_k \in H_k$. For F_i we obtain:

$$F_i = N(H_k \subseteq G) \cap Hi; \qquad N(H_k \subseteq G) = F_iH_k = H_kF_i. \tag{1.11}$$

If G is a solvable group with Sylow basis $P_1, \ldots, P_r$, the theory of general products is applicable to the subgroups $G_{k,\,i} = P_kP_i = P_iP_k$ of G. Important for the construction of the automorphism group $A(G)$ are the maximal invariant subgroups $N_k^{(i)}$ of $G_{k,\,i}$ contained in P_k and the fix groups

$F_k^{(i)}$ of $\Pi_{i,k}$. From (1.11) we obtain:

$$Fk = \bigcap_{\substack{i=1\\ i \neq k}}^{r} F_k^{(i)} = N(P_1 \cdot \ldots \cdot P_{k-1} P_{k+1} \cdot \ldots \cdot P_r \subseteq G) \cap P_k$$

and according to (1.3) $\boldsymbol{F} = F_1 \times \ldots \times F_k$ is the Sylow system normalizer related to the Sylow basis $P_1, \ldots, P_r$ of G.

2. Determination of *A(G)* by composition of allowable automorphisms. Let the composed mapping a = $\pi_1 \cdot \ldots$ ● Z, with $\pi_i \in A(P_i)$ ($i = 1, \ldots, r$) be defined by

$$\alpha(p_1 \cdot \ldots \cdot p_r) = \pi_1 p_1 \cdot \ldots \cdot \pi_r p_r \qquad (p_i \in P_i).$$

Then (cf. [1], ch. II, § 1):

THEOREM 2.1. a $\in$ *A(G) if and only if*

$$\pi_k \circ p_i\, k \circ \pi_k^{-1} = (\pi_i p_i)\, k \quad \bigwedge_{\substack{i,\, k = 1, \ldots, r\\ i \neq k}} . \tag{2.1}$$

Proof Since $P_i P_k = P_k P_i$ we obtain $\boldsymbol{a} \in \boldsymbol{A(G)}$ if and only if for $i < \boldsymbol{k}$:

$$\alpha(p_k p_i) \overset{(1.7)}{=} \alpha(p_k\, {}^i p_i \cdot p_i\, {}_{kpk)} = \alpha(p_k\, {}^i p_i) \cdot \alpha(p_i\, {}^k p_k) = (\alpha p_k) \cdot (\alpha p_i)$$
$$\overset{(1.7)}{=} (\alpha p_k)\, \iota\, (\alpha p_i) \cdot (\alpha p_i)\, {}_k\, (\alpha p_k),$$

hence : $\quad \alpha(p_k\, {}^i p_i) = (\alpha p_k)\, {}^i(\alpha p_i)$ and $\alpha(p_i\, {}^k p_k) = (\alpha p_i)\, {}^k (\dot{\alpha} p_k)$.

Because of the definition of a, these relations however are equivalent to (2.1).

From the point of view of computation it seems to be profitable to reduce the number of the relations (2.1), for which we have to decide the equality. The following theorem is fundamental for this reduction, and therefore for the construction of *A(G)*:

THEOREM **2.2.** ***The sign of equality is valid for all relations (2.1) if and only if for all generators*** $p_i^{(\nu)}$ ***of a generating system*** $\{p_i^{(\nu)}\}$ ***Of*** P_i ***the images of the mappings*** $\pi_k \circ p_i\, k \circ \pi_k^{-1}$ ***applied on the elements*** $p_k^{(\mu)}$ ***and*** $\pi_k p_k^{(\mu)}$ *of* ***a generating system*** $\{p_k^{(\mu)}\}$ *of* P_k ***are the same as for the mappings*** $(\pi_i p_i)\, k$ ***(i, k*** $= 1, \ldots, r$; $i \neq k$***).***

Proof. It is sufficient to prove the relations :

$$\pi_k \circ (p_i^{(1)} \cdot p_i^{(2)})\, k \circ \pi_k^{-1} = (\pi_i\, (p_i^{(1)} \cdot p_i^{(2)}))\, k \qquad (p_i^{(1)},\ p_i^{(2)} \in \{PI''\}), \tag{2.2}$$
$$\pi_k \circ p_i\, k \circ \pi_k^{-1} (p_k^{(1)} \cdot p_k^{(2)}) = (\pi_i p_i)\, k\, (p_k^{(1)} \cdot p_k^{(2)}) \qquad (p_k^{(1)},\ p_k^{(2)} \in \{p_k^{(\mu)}\}). \tag{2.3}$$

Then it is easy to give a complete proof of Theorem (2.2) by induction on the powers of the generators $p_i^{(\nu)}$ and $p_k^{(\mu)}$ of $\{p_i^{(\nu)}\}$ and $\{p_k^{(\mu)}\}$ respectively, and by induction on the length of the words in those generators representing the elements of P_i and P_k respectively. By the realization of this proof the same calculation as below will show that (2.1) is valid on $\pi_k(p_k^{(1)}\cdot p_k^{(2)})$. We obtain for $\boldsymbol{k} < i$:[†]

$$\pi_k \circ \left(p_i^{(1)}\cdot p_i^{(2)}\right) {\scriptstyle k} \circ \pi_k^{-1} \overset{(1.9,\gamma)}{=} \pi_k \circ p_i^{(1)} {\scriptstyle k} \circ p_i^{(2)} {\scriptstyle k} \circ \pi_k^{-1}$$

$$= \pi_k \circ p_i^{(1)} {\scriptstyle k} \circ \pi_k^{-1} \circ \pi_k \circ p_i^{(2)} {\scriptstyle k} \circ \pi_k^{-1}$$

since $p_i^{(1)}, p_i^{(2)} \in \{p_i^{(\nu)}\}$

$$= (\pi_i p_i^{(1)}) \, {\scriptstyle k} \circ (\pi_i p_i^{(2)}) \, k$$

$$\overset{(1.9,\gamma)}{=} \left((\pi_i p_i^{(1)})(\pi_i p_i^{(2)})\right) {\scriptstyle k}$$

$$= \left(\pi_i(p_i^{(1)} \cdot p^{(2)})\right) k\,,$$

proving (2.2), and because of

$$\begin{aligned}
\pi_k \circ p_i \, {\scriptstyle k} \circ \pi_k^{-1}(p_k^{(1)}\cdot p_k^{(2)}) &= \pi_k \circ p_i \, {\scriptstyle k} \circ \left[\pi_k^{-1}(p_k^{(1)}\cdot p_k^{(2)})\right] \\
&= \pi_k \circ p_i \, {\scriptstyle k} \circ \left[(\pi_k^{-1} p_k^{(1)})\cdot(\pi_k^{-1} p_k^{(2)})\right] \\
&\overset{(1.9,\delta)}{=} \pi_k \circ \left[p_i \, {\scriptstyle k} \circ (\pi_k^{-1} p_k^{(1)})\cdot\left\{(\pi_k^{-1} p_k^{(1)}) \, {\scriptstyle i} \, p_i\right\} {\scriptstyle k} \, (\pi_k^{-1} p_k^{(2)})\right] \\
&= \pi_k \circ p_i \, {\scriptstyle k} \circ \pi_k^{-1} p_k^{(1)} \cdot \pi_k\left[(\pi_k^{-1} p_k^{(1)}) \, {\scriptstyle i} \, p_i\right] {\scriptstyle k} \, (\pi_k^{-1} p_k^{(2)}) \\
&\overset{(2.2)}{=} \pi_k \circ p_i \, {\scriptstyle k} \circ \pi_k^{-1} p_k^{(1)} \cdot \left[\pi_i \circ (\pi_k^{-1} p_k^{(1)}) \, {\scriptstyle i} \, p_i\right] {\scriptstyle k} \, p_k^{(2)} \\
&= \pi_k \circ p_i \, {\scriptstyle k} \circ \pi_k^{-1} p_k^{(1)} \cdot \left[\pi_i \circ (\pi_k^{-1} p_k^{(1)}) \, {\scriptstyle i} \circ \pi_i^{-1} \circ (\pi_i p_i)\right] {\scriptstyle k} \, p_k^{(2)} \\
&= (\pi_i p_i) \, {\scriptstyle k} \, p_k^{(1)} \cdot (p_k^{(1)} \, {\scriptstyle i} \, (\pi_i p_i)) \, {\scriptstyle k} \, p_k^{(2)} \\
&\overset{(1.9,\delta)}{=} (\pi_i p_i) \, {\scriptstyle k} \, (p_k^{(1)} \cdot p_k^{(2)}),
\end{aligned}$$

proving the relations (2.3).

Let $\Gamma = \{\alpha \in A(G)/\alpha = \pi_1\cdot \ldots \cdot\pi_r, \pi_i \in A(P_i), (i = 1, \ldots, r)\}$ be the set of all automorphisms of G composed by automorphisms of the Sylow subgroups P_i. Then according to the relation (cf. A, § 1) g $\in F \leftrightarrow \tau(g)P_i = P_i$ (***i*** = 1, . . ., ***r***, -c(g) $\in I(G)$) there corresponds to every coset decomposition $G = g_1F + \ldots + g_tF$ of G by Fa coset decomposition $\boldsymbol{A(G)} = \tau(g_1)\Gamma + \ldots + {} + \tau(g_t)\Gamma$ ***of*** $A(G)$ by Γ.

Definition 2.1. ***An automorphism*** $\pi_i \in A(P_i)$ ***(i =*** 1, . . . , ***r) is called allowable*** *if* ***and only if there exists for every k ≠ i an automorphism*** $\pi_k \in A(P_k)$ ***such that a*** $= \pi_1\cdot \ldots \cdot\pi_i\cdot \ldots \cdot\pi_r \in$ **A(G).**

If $\pi_i \in A(P_i)$ is allowable, then

$$\pi_i F_i^{(k)} = F_i^{(k)} \tag{2.4}$$

$$\pi_i N_i^{(k)} = N_i^{(k)} \tag{2.5}$$

$$\pi_i \in N(\Pi_{i,\,k} \subseteq S_{|P_i|}) \tag{2.6}$$

$$\pi_i(N^* \cap P_i) = N^* \cap P_i,\ \boldsymbol{N^*} \text{ char } G. \tag{2.7}$$

By every allowable automorphism π_i an automorphism of the factor group $P_i/N_i^{(k)} \cong \Pi_{k,\,i}$ will be induced, and fixing the index ***i*** and assuming $\pi_i = {} = e_{A(P_i)}$ we obtain by (2.1) for an allowable automorphism $\pi_k \in A(P_k)$ ***(k ≠ i)*** the relations :

$$\pi_k \circ p_i \, {\scriptstyle k} \circ \pi_k^{-1} = {\scriptstyle pi\ k}\ ; \quad (\pi_k p_k) \, {\scriptstyle i} \, p_i = {\scriptstyle pk\ i} \, p_i\,, \tag{2.8}$$

[†] In consequence of (1.9), similar results are valid for $k > i$.

equivalent to :

$$\pi_k \in Z_k^{(i)} = Z(\Pi_{i,k} \subseteq S_{|P_k|});^{\dagger} \quad \pi_k p_k \in p_k N_k^{(i)} \tag{2.8}$$

If we denote by $\Pi_k^{(i)}$ the set of all $\pi_k \in A(P_k)$ inducing the identical automorphism on $P_k/N_k^{(i)}$, then

$$J_k^{(j)} = \bigcap_{\substack{i=1\\ i \neq k}}^{j} (Z_k^{(i)} \cap \Pi_k^{(i)}) \quad (j = 2, \ldots, r) \tag{2.9}$$

defines a system of groups of allowable automorphisms. This system is fundamental for the method of constructing *A(G)* from $A(P_i)$ described in B, § 5, because from a = $\pi_1 \cdot \ldots \cdot \pi_r \in$ *A(G)* and $\pi_i \in Z_i^{(k)} \cap \Pi_i^{(k)}$ ($k \neq i$) *we* obtain $\pi_k \in Z_k^{(i)} \cap \Pi_k^{(i)}$, and from $\pi_1 \cdot \ldots \cdot \pi_r \in$ *A(G)*, $\varepsilon_i \in J_i^{(r)}$ ($i = 1, \ldots, r$) we obtain cc' $= (\pi_1 \circ \varepsilon_1) \cdot \ldots \cdot (\pi_r \circ \varepsilon_r) \in A(G)$.

B. COMPUTATIONAL METHOD FOR THE CONSTRUCTION OF A(G)

3. Preliminaries for the construction of *A(G)*.

(a) ***Basic programs.*** The construction of *A(G)* is based on :

(a) the program for determination of the complete lattice V(G) of all subgroups of G described in [3], §§ 2, 3, and extended by the "composition method" of [6],

(β) the program for the determination of $A(P_i)$ ($i = 1, \ldots, r$) executed by the program system [2].

The program system (β) as well as (α) uses the method of representing the subgroups $U \subseteq$ G of G by a one-to-one correspondence to "characteristic numbers" $K[U] \leftrightarrow U$ described briefly in the following section.

(b) ***Special generating systems and characteristic numbers.*** In G a one-to-one correspondence exists between the subgroups US G of G and the systems S(U) of all cyclic subgroups of G contained in *U*. A system of generators of all elements of ***S(U)*** forms a "special generating system" ***E(U)*** of ***U.*** The elements of ***E(G)*** shall be listed. Assuming $\{h_{i_1}, \ldots, h_{i_e}\}$ is a complete generating system ***E(U)*** of *U* with $\{i_1, \ldots, i_e\} \subseteq \{1, \ldots, |E(G)|\}$, the characteristic number $K[$ ***U***$]$ of $U \subseteq$ G is represented by

$$K[U] = \sum_{j=1}^{e} 2^{i_j - 1}. \tag{3.1}$$

(c) Boolean operations for characteristic numbers. The Boolean operations of intersection "A " and disjunction " $\vee$ " are useful for a time-saving

† $Z(U \subseteq$ G) is the centralizer of UC G in G.

calculation with characteristic numbers :

$$K[U]\wedge K[V] = K[U\cap V] \tag{3.2}$$

$$UC\ V\leftrightarrow K[U]\wedge K[V] = K[U] \qquad (U,\ V,\ W\subseteq G) \tag{3.3}$$

$$\{U,\ V\}\subseteq W\leftrightarrow (K[U]\vee K[V])\wedge K(W) = K[U]\vee K[V]. \tag{3.4}$$ [†]

(d) ***Lists.*** For the determination of ***A(G)*** the following lists obtained by the construction of V(G) are used:

(a) CL-list, containing the characteristic numbers $K[U]$ of all subgroups $U\subseteq G$ of G.

(β) OL-list, containing the orders $U|$ of $U\subseteq$ G corresponding to $K[U]$. (The OL-list is a parallel list to the CL-list.)

(γ) NL-list, containing information, which enables us to find out $K[N(R\subseteq G)]$ for a representative R of a conjugate class of G. Since $N(\tau(g)R\subseteq G) = \tau(g)N(R\subseteq G)$ (r(g) $\in Z(G)$) it is easy to calculate $N(U\subseteq G)$ for all $U\subseteq G$.

(6) RL-list, containing 1 or0 at special bits, if $U\leftrightarrow K[U]$ has one of the following properties or not:

(Pl) U is cyclic.

(P2) U is abelian.

(P3) U is selfnormalizing in G.

(P4) U is normal in G.

(P5) U is a characteristic subgroup of G computed by the program for determination of V(G).

4. Representation of automorphisms in a computer. Let $x_1, \ldots, x_n$ be a system of generators of the group G and $R_j(x_i) = e_G$ ($j = 1, \ldots, m$) a system of defining relations for G. A mapping a of G into itself is an automorphism of G if and only if

$$G = \{\alpha x_1, \ldots, \alpha x_n\} \tag{4.1}$$

$$R_j(\alpha x_j) = e_G \quad (j = 1, \ldots, m). \tag{4.2}$$

The mappings a $\in$ ***A(G)*** will be stored in the computer by the images of a suitable system of generators. For the multiplication of al, $\alpha_2 \in$ ***A(G) we*** obtain the rule :

$$(\alpha_2\circ\alpha_1)x_i = \alpha_2\circ(\alpha_1 x_i) = \alpha_2 x_i^* = \alpha_2(w_i^*(x_k)) = w_i^*(\alpha_2 x_k), \tag{4.3}$$

where $x_i^* = w_i^*(x_k)$ is the representation of x_i^* as a word of the generators x_k of G. The knowledge of the word function w_i^* is therefore important for the multiplication of automorphisms. The time for testing a to be an automorphism and also for the multiplication of automorphisms depends on the structure of the system (4.2). Therefore it is profitable for computation to use a "special generating system" for G (cf. [3], [7]):

[†] $\{U, V\}$ means the subgroup generated by $U, V\subseteq G$.

A system $x_1, \ldots, x_n$ is called a ***special generating system*** of G if and only if for every $g \in G$ we obtain a representation $g = w(x_i) = x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$ with $0 \leq \varepsilon_k \leq \gamma_k$ (k = 1, . . ., ***n*)**, where γ_k is the least power of x_k such that

$$x_k^{\gamma_k} = x_1^{\varrho_{k,1}} \cdot \ldots \cdot x_{k-1}^{\varrho_{k,k-1}}.$$

If G is solvable, we can obtain a special generating system $x_1, \ldots, x_n$ of G using a subinvariant series

$$G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = \{e_G\} \tag{4.4}$$

such that $\{x_1, \ldots, x_i\} = G_i$ and $x_i \in N(\{x_1, \ldots, x_{i-1}\} \subseteq G)$. The defining relations of this system of generators are:

$$\begin{aligned} x_i^{\gamma_i} &= x_1^{\varrho_{i,1}} \cdot \ldots \cdot x_{i-1}^{\varrho_{i,i-1}} \qquad (\boldsymbol{i} = 1, \ldots, n) \\ x_k x_i &= x_1^{\sigma_1^{(k,i)}} \cdot \ldots \cdot x_{k-1}^{\sigma_{k-1}^{(k,i)}} x_k \qquad (1 \leq \boldsymbol{i} \leq \boldsymbol{k} \leq \boldsymbol{n}). \end{aligned} \tag{4.5}$$

Sometimes it is necessary to compute the automorphism $\alpha \in A(G)$--stored by the images $\alpha x_1, \ldots, \alpha x_n$ of the generators $x_1, \ldots, x_n$ of G-as images of another system $y_1, \ldots, y_t$ of generators of G. Assuming the relations $y_j = w_{y_j}(x_i)$ we obtain $\alpha_{y_j} = w_{y_j}(\alpha x_i)$.

5. The computational method for the composition of *A(G)*.

(a)[†] ***Determination of a complete*** *Sylow* ***basis*** $P_1, \ldots, P_r$ ***of G.*** For all $K_i \in \mathfrak{K}$ $(i = 1, \ldots, \boldsymbol{r})$ (cf. A, § 1, (a)) we obtain $|K_i| = \prod_{\substack{j=1 \\ j \neq i}}^{r} q_j^{\alpha_j}$. In the OL-list we search for the order $|K_i|$ (cf. B, § 3, (d), (β)), and we find in the corresponding place in the CL-list (cf. B, § 3 (d), (α)) the characteristic number $K[K_i] \leftrightarrow K_i$ ***(i*** = 1, ... *r*). Since $P_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{r} K_j$ $(\boldsymbol{i} = 1, \ldots, r)$ we get by (3.2):

$$P_i \leftrightarrow K[P_i] = \bigwedge_{\substack{j=1 \\ j \neq i}}^{r} K[K_j] \qquad (\boldsymbol{i} = 1, \ldots, \boldsymbol{r}). \tag{5.1}$$

(b) ***Determination of the system normalizer*** *F*. Using (1.2) and (3.2) we obtain $K[F] = \bigwedge_{i=1}^{r} K[N(K_i \subseteq G)]$. $K[N(K_i \subseteq G)]$ $(\boldsymbol{i} = 1, \ldots, \boldsymbol{r})$ is known from the NL-list (cf. B, § 3 (d), (y)).

(c) The coset decomposition *of* G ***by*** UC G and the ***determination*** *of a system* ***of representatives*** $\mathfrak{R} = \{r_1, \ldots, r_t\}$ of the decomposition are basic programs of the program system mentioned in B, § 3 (a), (α).

(d) ***Some remarks about determination of*** $V(P_i)$ ***and*** $A(P_i)$ $(\boldsymbol{i} = 1, \ldots, \boldsymbol{r})$. There is $G \supset U \in V(P_i) \leftrightarrow K[U] \wedge K[P_i] = K[U]$. For the determination of the

[†] The notations (a), (b), . . . , of § 5 correspond to the marks on the flow chart (cf. p. 71).

classes of conjugate subgroups of P_i we mention : If $U \lhd$ G, UC P_i(cf. B,§3 (d), (δ)), then $U \lhd P_i$. If P_i contains a complete class S of subgroups of G, which are conjugate in G, and if $|S| = [P_i:N(R \subseteq P_i)]$ for some representative $\boldsymbol{R}$ of the class S, then all $U \in S$ are also conjugate in P_i. If $|S| \neq [P_i : N(R \subseteq Pi)] = 1$, then $\boldsymbol{R} \lhd P_i$. If $|S| \neq [Pi : N(R \subseteq P_i)] \neq 1$ we decompose P_i in cosets by $N(R \subseteq Pi)$ and transform $\boldsymbol{R}$ by the elements of a system of representatives of this coset decomposition, using the relation

$$K[N(R \subseteq Pi)] = K[N(R \subseteq G) \cap P_i] = K[N(R \subseteq G)] \wedge K[P_i].$$

The determination of $A(P_i)$ can be executed by the method developed in the program system [**2**].

(e) Determination of the permutation groups $\Pi_{i,k}$ ***(i, k*** $= 1, \ldots, r; i \neq k$***).*** The elements of P_i ($i = 1, \ldots . r$) are numbered in the same sequence as they are generated by the generating program of P_i. Generating the subgroups $G_{i,k} = P_iP_k = P_kP_i$ Of G ($i, k = 1, \ldots, r; i < k$) on the one hand as a product of P_i, P_k and on the other hand as a product of P_k, P_i ***we*** obtain by comparing the products:

$$p_i^{(e)} p_k^{(s)} = p_k^{(s_\nu)} p_i^{(e_\varrho)} = p_i^{(e)} {}^k p_k^{(s)} \cdot p_k^{(s)} {}^i p_i^{(e)} \, (s = 1, \ldots, |P_k|;\ 1 \leqslant e \leqslant |P_i|). \quad \textbf{(5.2)}$$

From these relations we obtain the permutation $p_i^{(e)}\,{}^k$ of P_k related to the element $p_i^{(e)} \in P_i : p_i^{(e)} \to p_i^{(e)}\,{}^k = \binom{s}{s_\nu}$. If e runs from 1 to $|P_i|$, we get $\Pi_{i,k}$. Fixing s ($1 \leqslant s \leqslant |P_k|$) we can similarly determine for variable e (e = 1, . . . , $|P_i|$) the permutation $p_k^{(s)}\,{}^i = \binom{e}{e_\varrho}$ related to the element $p_k^{(s)} \in P_k$, and if s runs from 1 to $|P_k|$ we get $\Pi_{k,i}$. In view of Theorem 2.2 we have only to store the permutations $p_i^{(e)}\,{}^k$, $p_k^{(s)}\,{}^i$ of $\Pi_{i\ k},\Pi_{k,\ i}$, which are related to the generators of P_i, P_k respectively. The order of $|\Pi_{i,\ k}|$ and $|\Pi_{k,\ i}|$ are also stored in the computer.

(f) Determination of $F_i^{(k)}$ ***and*** $N_i^{(k)}$ ***(i, k*** $= 1, \ldots, r; i \neq k$***).***

(α) Since $N(P_k \subseteq G_{i,\ k}) = N(P_k \subseteq \text{G}) \cap G_{i,\ k}$, it follows from (1.11) and ***(3.2):***

$$\begin{aligned} K[F_i^{(k)}] &= K[N(P_k \subseteq G_{i,k}) \cap P_i] = K[N(P_k \subseteq G) \cap P_i)] \\ &= K[N(P_k \subseteq G) \wedge K[P_i] \qquad (i, k = 1, \ldots . r; \quad i \neq k). \end{aligned}$$

(β) $N_i^{(k)}$ is uniquely determined by $N_i^{(k)} \subseteq P_i$, $N_i^{(k)} \lhd P_iP_k$, $|N_i^{(k)}| = |P_i|/|\Pi_{i,\ k}|$ ($\boldsymbol{i,k} = 1, \ldots, r; i \neq k$). If $P_i^* \subseteq P_i$, $|P_i^*| = |P_i|/|\Pi_{i,k}|$, $P_i^* \lhd G$, then $N_i^{(k)} = P_i^*$. If we cannot find such a subgroup P_i^*, which is invariant in G, we look for asubgroup $\tilde{P}_i \subseteq P_i$ such that $|\tilde{P}_i| = |P_i|/|\Pi_{i,k}|$ and $|N(\tilde{P}_i \subseteq G_{i,k})| = |N(\tilde{P}_i \subseteq G) \cap G_{i,\ k}| = |G_{i,k}| = q_i^{\alpha_i} \cdot q_k^{\alpha_k}$. Since $N_i^{(k)}$ is uniquely determined, we have $N_i^{(k)} = \tilde{P}_i$.

(g) Determination *of* $A^*(P_i)$ ($i = 1, \ldots, r$) (cf. flow chart). There are two possibilities for the determination of $A^*(P_i)$ ($1 \leqslant i \leqslant r$)***:***

(a) Let F_i^{λ} $(\lambda = 1, \ldots) \lambda_i)$ be the different fix groups of $\Pi_{i,\ k}$ (i, $\boldsymbol{k} = 1, \ldots, r, i \neq k)$ and let $N^{(\nu)} \cap P_i (\nu = 1, \ldots, \nu_i)$. be the different characteristic subgroups of P_i induced by the $N^{(\nu)}$ char G and also different from all characteristic subgroups of P_i used by the determination of $A(P_i)$. Each group $F_i^{(\lambda)}$, $N^{(\nu)} \cap P_i$ determines a partition† $\mathfrak{Z}_i^{(\lambda)} = [F_i^{(\lambda)}, P_i - F_i^{(\lambda)}]$, $\overline{\mathfrak{Z}}_i^{(\nu)} = [N^{(\nu)} \cap P_i$, $P_i - (N^{(\nu)} \cap$ ***Pi)]*** of P_i respectively. To the partition $\left(\bigwedge_{\lambda=1}^{\lambda_i} \mathfrak{Z}_i^{(\lambda)}\right) \curlywedge \left(\bigwedge_{\nu=1}^{\nu_i} \overline{\mathfrak{Z}}_i^{(\nu)}\right)$ there corresponds a well-defined partition of the set $\{1, \ldots, |P_i|\}$:

$$(j_1, \ldots, j_e), (j_{e_1+1}, \ldots, j_{e_1+e_2}), \ldots, (j_{e_1+\cdots+e_{h-1}+1}, \ldots, j_{e_1+\cdots+e_h})$$

$$\left(\sum_{\tau=1}^{h} e_\tau = |P_i|\right) \tag{5.3}$$

Now we calculate the permutation ϱ_{π_i} of the set $\{1, \ldots, |P_i|\}$ related to the automorphism $\pi_i \in A(P_i)$ given by the images $\pi_i p_i^{(\nu)}$ of a generating system $\{p_i^{(\nu)}\}$ of P_i (cf. B, § 4). Then $\pi_i \in A^*(P_i)$ if and only if ϱ_{π_i} maps the classes of the partition (5.3) complexwise into themselves.

(β) If $f_{i,1}^{(\lambda)} = w_{i,1}^{(\lambda)}(p_i^{(\varphi)}), f_{i,2}^{(\lambda)} = w_{i,2}^{(\lambda)}(p_i^{(\varphi)}), \ldots, f_{i,h_i}^{(\lambda)} = w_{i,h_i}^{(\lambda)}(p_i^{(\varphi)})$,

$$\bar{f}_{i,1}^{(\nu)} = \bar{w}_{i,1}^{(\nu)}(p_i^{(\varphi)}), \bar{f}_{i,2}^{(\nu)} = \bar{w}_{i,2}^{(\nu)}(p_i^{(\varphi)}), \ldots, \bar{f}_{i,h_i}^{(\nu)} = \bar{w}_{i,h_i}^{(\nu)}(p_i^{(\varphi)})$$

is a generating system of $F_i^{(\lambda)}$, $N^{(\nu)} \cap P_i$ respectively — represented as words of the elements $p_i^{(\varphi)}$ of a generating system $\{p_i^{(\varphi)}\}$ of P_i — then $\pi_i \in A^*(P_i)$ if and only if both

$$\pi_i f_{i,j}^{(\lambda)} = w_{i,j}^{(\lambda)}(\pi_i p_i^{(\varphi)}) \in F_i^{(\lambda)} \text{ for } \lambda = 1, \ldots, \lambda_i;\ j = 1, \ldots, h_i$$

and $\pi_i \bar{f}_{i,j}^{(\nu)} = \bar{w}_{i,j}^{(\nu)}(\pi_i p_i^{(\varphi)}) \in N^{(\nu)} \cap P_i$ for v = 1, . . ., ν_i; j = 1, . . ., h_i.

(h) ***Determination*** *of* $I_i^{(j)}$ ($\boldsymbol{i} = 1, \ldots, \boldsymbol{r}; \boldsymbol{j} = \boldsymbol{2}, \ldots, \boldsymbol{r}$; $i \neq k$) (cf. ***flow*** chart).

(α) ***Determination*** *of* $I_i^{(j)}$ $(1 \leqslant i \leqslant r;\ 2 \leqslant j \leqslant \boldsymbol{r})$. Let $\mathfrak{Z}_i^{(k)}$ $(\boldsymbol{k} = 1, \ldots, j;\ \boldsymbol{i \neq k})$ be the coset decomposition of P_i by $N_i^{(k)}$, then, similarly to (g) (5.3), the greatest common refinement $\bigwedge_{\substack{k=1 \\ k \neq i}}^{j} \mathfrak{Z}_i^{(k)} = p_i^{(1)} \bigcap_{\substack{k=1 \\ k \neq i}}^{j} N_i^{(k)} + \ldots + p_i^{(\sigma)} \bigcap_{\substack{k=1 \\ k \neq i}}^{j} N_i^{(k)}$ corresponds to a well-defined partition of the set $\{1, \ldots, |P_i|\}$, which can easily be determined. Those $\pi_i \in A^*(P_i)$, the corresponding permutations ϱ_{π_i} of which map the class of the partition of $\{1, \ldots, |P_i|\}$ related to $\bigcap_{\substack{k=1 \\ k \neq i}}^{j} N_i^{(k)}$ into itself

† A non-empty system $\mathfrak{Z}$ of non-empty subsets $N \subseteq M$ of a set $M \neq 0$ is called a partition of M if and only if each element of M is contained in only one set N $\in \mathfrak{Z}$. The subsets NE $\boldsymbol{M}$ are called the classes of the partition $\mathfrak{Z}$. The greatest common refinement of the partitions $\mathfrak{Z}_1, \mathfrak{Z}_2$ of M formed by all non-empty intersections of the classes of $\mathfrak{Z}_1, \mathfrak{Z}_2$ is denoted by $\mathfrak{Z}_1 \curlywedge \mathfrak{Z}_2$.

and a representative z of every other class into an element $\bar{z}$ of the same class, belong to the group $I_i^{(j)}$ if and only if for all $p_k^{(\mu)} \in \{p_k^{(\mu)}\}$ of P_k (cf. Theorem 2.2) :

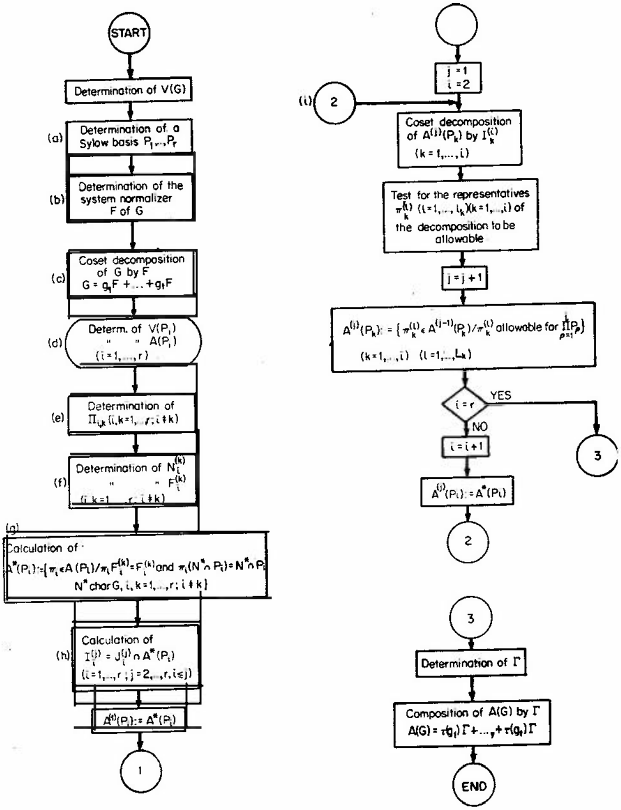
$$\pi_i \circ p_k{}^i \circ \pi_i^{-1} = p_k{}^t \bigwedge_{\substack{k=1,\dots,j\\ k\neq i}} . \tag{5.4}$$

The test of e quality for the relations (5.4) however is equivalent to comparing multiplication of permutations in an abbreviated form (cf. Theorem **2.2)**:

$$\varrho_{\pi_i} p_k{}^i \cdot \varrho_{\pi}{}_{\pi}^{-1} = p_k{}^i \bigwedge_{\substack{k=1,\dots,j\\ k\neq i}} , \tag{5.5}$$

for the test of (5.4) is restricted on the generating systems $\{p_i^{(\nu)}\}$ and $\{\pi_i p_i^{(\nu)}\}$ of P_i.

(β) ***Determination** of $I_i^{(j+1)}$using $I_i^{(j)}$*. By use of the coset decomposition $\mathfrak{Z}_i^{(j+1)}$ of P_i by $N_i^{(j+1)}$, the partition of $\{1, \dots, |P_i|\}$ related to the partition $\bigwedge_{\substack{k=1\\ k\neq i}}^{j} \mathfrak{Z}_i^{(k)}$, which has been needed by the construction of $I_i^{(j)}$, can be easily refined.


START
Determination of V(G)
(a) Determination of a Sylow basis P1,...,Pr
(b) Determination of the system normalizer F of G
(c) Coset decomposition of G by F G = g1F + ... + gtF
(d) Determ. of V(Pi) " " A(Pi) (i = 1,...,r)
(e) Determination of Πi,k (i,k = 1,...,r; i ≠ k)
(f) Determination of Ni(k) " " Fi(k) (i,k = 1,...,r; i ≠ k)
(g) Calculation of A*(Pi) := {πi ∈ A(Pi) / πi Fi(k) = Fi(k) and πi(N* ∩ Pi) = N* ∩ Pi N* char G, i, k = 1,...,r; i ≠ k}
(h) Calculation of Ii(j) = Ji(j) ∩ A*(Pi) (i = 1,...,r; j = 2,...,r, i ≤ j)
A(1)(Pi) := A*(Pi)
1
j = 1
i = 2
(i) 2
Coset decomposition of A(j)(Pk) by Ik(i) (k = 1,...,i)
Test for the representatives πk(l) (l = 1,...,lk)(k = 1,...,i) of the decomposition to be allowable
j = j + 1
A(j)(Pk) := {πk(l) ∈ A(j−1)(Pk) / πk(l) allowable for ∏ρ=1 Pρ} (k = 1,...,i) (l = 1,...,Lk)
i = r
YES
NO
3
i = i + 1
A(j)(Pi) := A*(Pi)
2
3
Determination of Γ
Composition of A(G) by Γ A(G) = τ(g1)Γ + ... + τ(gt)Γ
END

$\pi_i \in I_i^{(j)}$ belongs to $I_i^{(j+1)}$ if and only if $\varrho_{\pi_i} \leftrightarrow \pi_i$ maps the class of the above partition of $\{1, \ldots, |P_i|\}$ related to $\bigcap_{\substack{k=1\\k\neq i}}^{j+1} N_i^{(k)}$ into itself and an element z of every other class into an element $\bar{z}$ of the same class, and in addition for all $p_{j+1}^{(\mu)} \in \{p_{j+1}^{(\mu)}\}$ of P_{j+1} the appropriate relations (5.5) are satisfied.

(i) ***Determination*** of ***the group*** Γ. It is sufficient to describe the iterative process for determining Γ in the first two steps:

The groups $A^{(1)}(P_i)$ ($\boldsymbol{i} = 1, 2$) (cf. flow chart) are decomposed by $I_i^{(2)}$:

$$\begin{aligned} A^{(1)}(P_1) &= \pi_1^{(1)} I_1^{(2)} + \ldots + \pi_1^{(s_1)} I_1^{(2)} \\ A^{(1)}(P_2) &= \pi_2^{(1)} I_2^{(2)} + \ldots + \pi_2^{(s_2)} I_2^{(2)}. \end{aligned} \tag{5.6}$$

Then $\pi_2^{(e_2)} \cdot \pi_1^{(e_1)} \in A(P_1P_2)$ $(1 \leqslant e_1 \leqslant s_1;\ 1 \leqslant e_2 \leqslant s_2)$ if and only if for all $p_k^{(\nu_k)} \in \{p_k^{(\nu_k)}\}$ of P_k the mappings $\pi_i^{(e_i)} \boldsymbol{o} \boldsymbol{p}_k^{(\nu_k)} \circ (\pi_i^{(e_i)})^{-1}$ and $(\pi_k^{(e_k)} p_k^{(\nu_k)})^{i}$ applied to $\{p_i^{(\nu_i)}\}$ and $\{\pi_i p_i^{(\nu_i)}\}$ of P_i produce the same image:

$$\pi_i^{(e_i)} \circ p_k^{(\nu_k)\,i} \circ (\pi_i^{(e_i)})^{-1} = (\pi_k^{(e_k)} p_k)^{i} \quad (i, k = 1, 2; \quad i \neq k). \tag{5.7}$$

The test of (5.7) will be executed similarly as in (h). For the further investigation there remain the following groups:

$$A^{(2)}(P_i) = \pi_i^{(1)} I_i^{(2)} + \ldots + \pi_i^{(k_i)} I_i^{(2)} \quad (i = 1, 2).$$

Decomposing $I_i^{(2)}$ by $I_i^{(3)}$ ($\boldsymbol{i} = 1, 2$) we obtain a decomposition of $A^{(2)}(P_i)$ by $I_i^{(3)}$. Now we decompose $A^{(2)}(P_3) = A^*(P_3)$ by $I_3^{(3)}$. The test of the representatives of these decompositions to be allowable automorphisms is now the same for the pairs of groups $A^{(2)}(P_1)$, $A^{(2)}(P_3)$ and $A^{(2)}(P_2)$, $A^{(2)}(P_3)$ as described for the groups $A^{(1)}(P_1)$, $A^{(1)}(P_2)$ in the first step. Continuing this method for $\boldsymbol{r}$ steps we construct the group Γ.

Since $G = P_1 \cdot \ldots \cdot P_r$, each element of G can be represented as a word in the special generators needed for the determination of $A(P_i)$ ($\boldsymbol{i} = 1, \ldots, \boldsymbol{r}$). With respect to these generators it is easy to construct the inner automorphisms $\tau(g_t) \in$ I(G) generated by the representatives of the coset decomposition of G by the system normalizer of G; and therefore the composition of ***A(G)*** by Γ according to $\boldsymbol{A(G)} = \tau(g_1)\Gamma + \ldots + \tau(g_1)\Gamma$ is obvious.

C. OPTIMIZATION AND EXTENSION OF THE PROGRAM SYSTEM

6. Some aspects of optimization of the program system. Let G be a solvable group and $P_1, \ldots . P_r$ a Sylow basis of G. If $G = Q_1 \times \ldots \times Q_r$ is a direct product of direct indecomposable factors $Q_i = P_{i,1} \cdot \ldots \cdot P_{i,r_i}$ ($\boldsymbol{i} = \boldsymbol{1}, \ldots . s$; $\sum_{i=1}^{s} r_i = r$), where the $P_{i,k}$ belong to the Sylow basis of G, it can easily be proved that the direct product is uniquely determined.

The relations $K[P_{i_1} \cdot \ldots \cdot P_{i_r}] = K[P_{i_1}] \vee \ldots \vee K[P_{i_r}]$ ($\{i_1, \ldots, i_r\} \subseteq \subseteq (1, \ldots, r\}$) and the knowledge that both $K_\varrho = P_{i_1} \cdot \ldots \cdot P_{i_r}$ with $|K_\varrho| = \prod_{e=1}^{r} q_{i_e}^{\alpha_{i_e}}$ and the complemented group $K_{\varrho'} = P_{j_1} \cdot \ldots \cdot P_{j_r}$ with $|K_{\varrho'}| = \prod_{e=1}^{t} q_{j_e}^{\alpha_{j_e}}$ ($|K_\varrho| \cdot |K_{\varrho'}| = |G|$) are invariant in G and characterized in B, § 3 (d), (δ), enable us to develop a time-saving method for the determination of the direct product G = $Q_1 \times \ldots$ XQ, of G. Since the automorphism group *A(G)* is the composition of all automorphisms of Q_i ($i = 1, \ldots, s$), we have only to apply the method described in § 5 to the components Q_i ($i = 1, \ldots, s$).

From A, § 2 it seems to be profitable to alter the sequence of the groups $P_{i,l}$ ($l = 1, \ldots . r_i$) of the Sylow basis of Q_i ($i = 1, \ldots$, s), such that the index $[H_l^{(i)}: \mathfrak{N}(\mathfrak{S}_{Q_i})]$ of the system normalizer of Q_i in $H_l^{(i)} = P_{i,j_1} \cdot \ldots \cdot P_{i,j_l} \subseteq Q_i$ ($l = 2, \ldots, r_i$) is maximal, where the P_{i,j_ν} ($\nu = 1, \ldots, l$) are groups of the Sylow basis of Q_i. Then the order $|\Gamma_{H_l^{(i)}}|$ of the group $\Gamma_{H_l^{(i)}} \subseteq A(Q_i)$ generated by composition of allowable automorphisms **Of** P_{i,j_k} ($k = 1, \ldots, l$) will be minimal, and therefore in general the iterative process for the determination of Γ_{Q_i} will be optimized.

7. Some aspects for the extension of the program system to groups with a normal chain of Hall groups. For the determination of *A(G)* of a **finite** solvable group G we used only the following assumptions for the Sylow basis of G: (a) $G = P_1 \cdot \ldots \cdot P_r$, $P_iP_k = P_kP_i$, $(|P_i|, |P_k|) = 1$ ($i, k = 1, \ldots r$; $i \neq k$), (b) each Sylow system of G is conjugate in G. Therefore the methods of B, § 5 for constructing *A(G)* can be extended to all groups G containing a system of subgroups H_k ($k = 1, \ldots$, s) such that G = $H_1 \cdot \ldots \cdot H_s$, $H_iH_k = H_kH_i$, $(|H_i|, |H_k|) = 1$ ($i, k = 1, \ldots$, s; $i \neq k$) and such that all systems of that kind are conjugate in G.

In the case that G contains a normal chain of Hall groups :

$$G = N_s \supseteq \ldots \supseteq N_i \supseteq \ldots \supseteq N_1 \supset \{e_G\}$$

there exists a system of subgroups H_i ($i = 1, \ldots$, s) in G such that $H_i \lhd H_iH_k$ for $i < k$, $N_i = H_1 \cdot \ldots \cdot H_i$, $H_iH_k = H_kH_i$ and such that all systems of that kind are conjugate in G (cf. **[1]**, ch. II, § 2). The program developed in B, § 5 therefore can be extended to all ***not necessarily solvable*** groups containing a normal chain of Hall groups. If $s = 2$ we obtain the case that G is a group extension of N by *T* with $(|N|, |T|) = 1$:

$$G = NT, \text{ Na } G, \quad T \cong G/N, \; N \cap T = \{e_G\}, \; (|N|, \; |T|) = 1.$$

The automorphism group *A(G)* can be constructed in this case by composition of allowable automorphisms of N and *T*.

REFERENCES

1. E. Altmann : Anwendungen der Theorie der Faktorisierungen, Forschungsbericht des Landes Nordrhein Westfalen, Heft 1902. *Zugleich Schriften des Rhein – Westf. Inst. für Znstr. Math., Bonn,* Ser. A, No. 20.
2. V. Felsch and J. Neübuser: Über ein Programm zur Berechnung der Automorphismengruppe einer endlichen Gruppe. *Num. Math* 11 (1968), 277-292.
3. L. Gerhards and W. LINDENBERG: Ein Verfahren zur Berechnung des vollständigen Untergruppenverbandes endlicher Gruppen auf Dualmaschienen. Num. *Math. 7* (1965), 1-10.
4. P. Hall: On the *Sylow* systems of a soluble group. *Proc. London Math. Soc. (2) 43* (1937), 316-323.
5. P. Hall: On the Sylow normalizers of a soluble group. *Proc. London Math. Soc.* (2) 43 (1937), 507-528.
6. W. Lindenberg and L. GERHARDS: Combinatorial construction by computer of the set of all subgroups of a finite group by composition of partial sets of its subgroups. These Proceedings, pp. 75-82.
7. W. Lindenberg: Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten. *Num. Math. 4* (1962), 151-153.
8. L. Redei: Die Anwendung des schiefen Produktes in der Gruppentheorie. *JournaC reine angew. Math.* 188 (1950), 201-228.
9. J. SZEP: Über die als Produkte zweier Untergruppen darstellbaren endlichen Gruppen. *Corn. Math. Helv. 22* (1949), 31-33.

Combinatorial construction by computer of the set of all subgroups of a finite group by composition of partial sets of its subgroups

W. LINDENBERG and L. GERHARDS

THE following paper contains a description of the main parts of a program for computational determination of the lattice of all subgroups of a finite group $\mathfrak{G}$. The program has been developed by the authors and has been realized for the computer IBM 7090, It is of combinatorial type and does not require further assumptions for $\mathfrak{G}$.

1. Preliminaries. Let $\mathfrak{G} = \{x_1, \ldots, x_n\}$ be a finite group generated by an ordered system $(x_1, \ldots,$ x,) of independent? elements (e.g. permutations, matrices or abstract elements together with the connecting relations of multiplication [1], [3]). Generating $\mathfrak{G}$ successively by $x_1, x_2, \ldots, x_n$ we obtain a chain $(e) \subset \mathfrak{G}_1 \subset \ldots \subset \mathfrak{G}_n = \mathfrak{G}$ Of subgroups Of $\mathfrak{G}$ ($\mathfrak{G}_i = \{x_1, \ldots, x_i\}$, $i = 1, . ..) n$). The order of $\mathfrak{G}_i$ will be denoted by $|\mathfrak{G}_i|$. If $\mathfrak{M}_i$ is the set of all cyclic subgroups of $\mathfrak{G}_i$ of prime-power order, Z_i shall be some set of generators of *all* elements of $\mathfrak{M}_i$ such that $Z_i \cap Z_k = Z_i$ for all $k \geqslant i$ ($i, k = 1, \ldots,$ n). Let $|Z_i|$ be the number of elements of Z_i. We shall list all the elements of Z_i ($i = 1, \ldots, n$) in such a way that the sequence of the elements in the list of Z_i is the same as in the list of all elements of Z_k ($k \geqslant$ i), i.e. the part of the first $|Z_i|$ elements of the list of all elements of Z_k is identical with the list of Z_i.

For characterizing any subgroups $\mathfrak{A}$ of $\mathfrak{G}_i$ [4] we note that $Z^{(i)}_{\mathfrak{A}} = \mathfrak{A} \cap Z_i$ is uniquely determined by $\mathfrak{A}$. Now, if the ϱth element of Z_i ($1 \leqslant \varrho \leqslant |Z_i|$) is associated with the binary number $2^{\varrho-1}$, and any subset $\mathfrak{S}$ of Z_i with the sum $B(\mathfrak{S})$ of those binary numbers associated with all the elements of $\mathfrak{S}$, we have that $\mathfrak{A}$ corresponds uniquely with $B(Z^{(i)}_{\mathfrak{A}})$. For standardization, however, we complete this number by apposition of $|Z_n| - |Z_i|$ zeros to the higher digits of a number $B(\mathfrak{A})$ of $|Z_n$ digits. $B(\mathfrak{A})$ shall be used for representing the subgroup $\mathfrak{A}$ c $\mathfrak{G}$.‡ If $B(\mathfrak{A}) = \sum_{j=1}^{|Z_n|} a_j \cdot 2^{j-1}$ and $B(\mathfrak{B}) = \sum_{j=1}^{|Z_n|} b_j \cdot 2^{j-1}$

† This is no loss of generality.

‡ For the following discussions it will be useful to remember that, for any subgroup $\mathfrak{A} \subset \mathfrak{G}_i$ ($\mathfrak{A} \not\subset \mathfrak{G}_{i+1}$), $B(\mathfrak{A})$ may contain ones only in its $|Z_i|$ lower digits.

($\mathfrak{A}$, $\mathfrak{B}$ C $\mathfrak{G}$), we define

$$B(\mathfrak{A}) \vee B(\mathfrak{B}) = \sum_{j=1}^{|Z_n|} (a_j \vee b_j)\cdot 2^{j-1},$$
$$B(\mathfrak{A}) \wedge B(\mathfrak{B}) = \sum_{j=1}^{|Z_n|} (a_j \wedge b_j)\cdot 2^{j-1}, \tag{1.1}$$

where $a \vee b$ resp. $a \wedge b$ are the usual boolean operators. In particular we have [4]:

$$B(\mathfrak{A} \cap \mathfrak{B}) = B(\mathfrak{A}) \mathbf{A} B(\mathfrak{B}) \tag{1.2}$$

$$B(\{\mathfrak{A} \text{ u } \mathfrak{B}\}) \geqslant B(\mathfrak{A}) \vee B(\mathfrak{B})^{\dagger} \tag{1.3}$$

$$\mathfrak{A} \subseteq \mathfrak{B} \quad \Leftrightarrow B(\mathfrak{A}) \wedge B(\mathfrak{B}) = B(\mathfrak{A}). \tag{1.4}$$

2. The generation of the partial set of subgroups. In § 1, the set of the wanted subgroups of $\mathfrak{G}$ was represented by a set of certain numbers of $|Z_n|$ digits. Let S be the normal sequence of the first $2^{|Z_n|}$ binary numbers. To each element of S belongs-as discussed above-a well-defined partial set $\mathfrak{S}$ of Z_n. By $\mathfrak{S}$ there is also defined a subgroup $\mathfrak{A} = \{\mathfrak{S}\}$ of $\mathfrak{G}_i$, which is generated by all elements of $\mathfrak{S}$; it is $\mathfrak{S} \subseteq \mathfrak{A} \cap Z_n$. Thus theoretically we can obtain the wanted set of all subgroups of $\mathfrak{G}$ by taking all elements of *S*, constructing the corresponding subsets of Z_n, generating the groups defined by these subsets and finally storing their characteristic numbers, if they have not yet been determined. But a method of this kind cannot be used because of the large number $2^{|Z_n|}$ of operations to be done.

Therefore in [2] a method has been described for systematically reducing the above set S of binary numbers used for the determination of the desired set of all subgroups of $\mathfrak{G}$. Beyond this, however, it is practicable to divide the listed elements of Z_n into s sections C_i $(i = 1, \dots, \text{s})$ of length $l \leqslant |Z_n|$ and one further section C_{s+1} of length r (with $|Z_n| = s\cdot l + r\,(r < l)$; $c_{s+1} = \emptyset$, if $r = 0)$ with outpermuting the sequence of elements of Z_n, i.e.

$$Z_n = [z_1, \dots, z_{|Z_n|}]$$
$$= [z_1, \dots, z_l, \dots, z_{il+1}, \dots, z_{(i+1)l}, \dots, z_{(s-1)l+1}, \dots,$$
$$z_{sl}, z_{sl+1}, \dots, z_{sl+r}]^{\ddagger}$$

If now the method of [2] is used for each of these sections C_i $(i = 1, \dots, s+1)$ we obtain for each C_i a set G_i of subgroups of 8. Generally any two of these sets will not necessarily be disjoint, i.e. the characteristic number may occur more than once, but by eliminating those multiple elements, we obtain the disjoint sets G_i. Naturally in general $\bigcup_i G_i$ is not yet the wanted set of all subgroups of $\mathfrak{G}$. In § 3 we give a detailed description of the method of combining the characteristic numbers.

[†] The equality does not hold, because generally $\mathfrak{A} \cup \mathfrak{B} \subset \{\mathfrak{A} \cup \mathfrak{B}\}$.

[‡] Empirically it seems useful to choose $6 \leqslant l \leqslant 9$.

3. The **method of constructing the set of all subgroups of** $\mathfrak{G}$. First we give some definitions and notations :

Definition 1. The determination of the characteristic numbers of the group $\mathfrak{C} = \{\mathfrak{A}, \mathfrak{B}\}$ by the characteristic numbers $B(\mathfrak{A})$ and $B(\mathfrak{B})$ is called *composition;* the characteristic number of $\mathfrak{C}$ is denoted by $c(B(\mathfrak{A}), B(\mathfrak{B}))$, the order of $\mathfrak{C}$ by $|c(B(\mathfrak{A}), B(\mathfrak{B}))|$.[†]

Definition 2. Let Sbe a set of characteristic numbers; Sis said to be *closed* (relative to composition) if $c(B_1, B_2) \in S$ for arbitrary elements $B_1, B_2 \in S$.

Definition 3. Let S be a (not necessarily closed) set of characteristic numbers. The closed set $C(S) \supseteq S$ is called the *closure of S.*

We shall denote by

E_i the set of characteristic numbers of all subgroups of G_i $(i = 1, \ldots, s+1)$ (see § 2),

$|E_i|$ the number of elements of E_i,

$K_{1,2,\ldots,i} = C(E_1 \cup \ldots \cup E_i) - (E_1 \cup \ldots \cup E_i)$

$E_{1,2,\ldots,i,} = C(E_1 \cup \ldots \cup E_i)$

$|E_{1,2,\ldots,i}|$ is the number of elements of $E_{1,2,\ldots,i}$

$K_i = \{c(B,B') \notin E_i \cup E_{1,2,\ldots,i-1} | B \in E_i, B' \in E_{1,2,\ldots,i-1}$ arbitrary $(i = 2, \ldots, s+1)\}$.

Clearly we have:

$$c(c(B_1, B_2), c(B_1', B_2')) = c(c(B_1 \vee B_1'), c(B_2 \vee B_2')), \tag{3.1}$$

$E_i' = C(E_i')$ $(i = 1, \ldots . s+1)$, but in a way we may also assume $E_i = C(E_i)$. (3.2)

Now we prove

3.1. *If* $B_\lambda \in K_i$ $(\lambda = 1, 2; 2 \leqslant i \leqslant s+1)$, *then there always exist* $B_1^* \in E_i$ *and* $B_2^* \in E_{1,2,\ldots,i-1}$ *such that* $c(B_1, B_2) = c(B_1^*, B_2^*)$.

Proof. $B_\lambda \in K_i$ implies by definition $B_\lambda = c(B_\lambda', B_\lambda'')$, $B_\lambda' \in E_i$, $B_\lambda'' \in E_{1,2,\ldots,i-1}$ $(\lambda = 1, 2)$. Hence using (3.1): $c(B_1, B_2) = c(c(B_1', B_2''), c(B_2', B_2'')) = c(c(B_1' \vee B_2'), c(B_1'' \vee B_2''))$. According to (3.2) we obtain: $c(B_1' \vee B_2') = B_1^* \in E_i$, according to the definition of $E_{1,2,\ldots,i-1}$: $c(B_1'' \vee B_2'') = B_2^* \in E_{1,2,\ldots,i-1}$. Thus $c(B_1, B_2) = c(B_1^*, B_2^*)$, as required.

Using 3.1 we immediately obtain:

3.2. $K_i \cup E_i \cup E_{1,2,\ldots,i-1}$ *is the closure of* $E_1 \cup \ldots \cup E_i$ $(i = 2, \ldots, s+1)$.

Now we are able to describe the method of constructing the set of all subgroups of $\mathfrak{G}$. From (3.2) we have $C(E_1) = E_1$. Suppose $C(E_1 \cup \ldots \cup E_i) = K_{1,2,\ldots,i} \cup E_1 \cup \ldots \cup E_i = E_{1,2,\ldots,i}$ has already been determined.

[†] For abbreviation we shall often write $B_1, B_2, \ldots, B', B'', \ldots$, etc., instead of $B(\mathfrak{A}), B(\mathfrak{b}), \ldots$.

By successive composition of all elements $B \in E_{i+1}$ $(B \notin K_{1,\ldots,i})$[†] with all elements $B' \in E_{1,\ldots,i}$ we obtain from 3.2 the closure $C(E_1 \cup \ldots \cup E_{i+1}) = K_{i+1} \cup E_{i+1} \cup E_{1,2,\ldots,i}$ of $E_1 \cup \ldots \cup E_{i+1}$. This method is repeated until finally we obtain $C(E_1 \cup \ldots \cup E_{s+1})$. This, however, is the complete set of the characteristic numbers of all subgroups of $\mathfrak{G}$.

The composition is mainly a method of generating a group by a set of generators (defined by the characteristic numbers of the two components). A large number of the executed compositions, however, will yield characteristic numbers which have already been computed. As the computation of a group by a set of generating elements is a time-consuming process, all efforts have to be made for reducing the number of such computations. We now explain how this can be realized, discussing the most important points.

Obviously it is sufficient to discuss the method cf composition of only two characteristic numbers. We assume the set $E_{1,2,\ldots,i}$ to have been computed already and listed (list L_1). Another corresponding list L_2 contains the orders of those groups which are associated with the elements of L_1.[‡] Furthermore let L_1^* be the list of all characteristic numbers $B^*(\mathfrak{A})$ of all the other subgroups of $\mathfrak{G}_\omega$ already determined by the methods of § 2. L_2^* is the corresponding list of orders.

Let $B \in E_{i+1}$ $(B \notin K_{1,\ldots\ldots,i})$, $B' \in E_{1,2,\ldots,i}$, $B \vee B' = \sum_{i=1}^{|Z_n|} a_i \cdot 2^{i-1}$ $(a_\varkappa = 1;$ $a_\lambda = 0$ for all $\lambda > \varkappa)$; $\mathfrak{B}, \mathfrak{B}'$ $(\mathfrak{B} \not\subset \mathfrak{B}', \mathfrak{B}' \not\subset \mathfrak{B})$ are the corresponding groups to *B, B'*.

3.3. As explained in § 1 there exists an integer $\omega \leqslant n$ such that $|Z_{\omega-1}| < x \leqslant |Z_\omega|$. If p_ω is the least prime number dividing $\mathfrak{G}_\omega|$, $\frac{|\mathfrak{G}_\omega|}{p_\omega}$ may be regarded as a boundary for *{B$\vee$ B'}*, i.e. as soon as more than $\frac{|\mathfrak{G}_\omega|}{p_\omega} + 1$ elements have been computed, the process of generating the group *{B$\vee$ B'}* may be stopped at once, since the result would be $\mathfrak{G}_\omega$, which has the characteristic number $\sum_{i=1}^{|Z_\omega|} 2^{i-1}$. The boundary $\Omega_\omega = \frac{\mathrm{I}\mathfrak{G}_\omega|}{p_\omega}$ is valid for all binary numbers $2^{|Z_{\omega-1}|} \leqslant B \vee B' < 2^{|Z_\omega|}$ $(\omega = 1, \ldots, n)$. We note[††]

[†] This condition is necessary, if, before storing a new composed number ***B, we*** have verified only $B \notin \overline{K}_{i+1} \cup E_{i+1} \cup E_{1,2;\ldots,i}$ but not $B \notin \overline{K}_{i+1} \cup E_{i+1} \cup E_{1,\ldots,i} \cup E_{i+2} \cup \ldots \cup E_{s+1}$ ($\overline{K}_{i+1}$ subset of K_{i+1} already computed).

[‡] *(B}* | resp. | *{B'}* | may be presumed to be known; for they appear as a by-product of the determination of ***B*** resp. ***B'*** (by the process of generating the associated groups). The number $|L_1|$ of elements of L_1 is equal to the number $|L_2$ of elements L_2 and the order of thejth element of L_1 is identical with that of the jth element of L_2.

[††] Note $|Z_0| =_{df} 0$; $\mathfrak{B}, \mathfrak{B}' \subset \mathfrak{G}_\omega$. In the following we assume the characteristic number $\mathfrak{G}_\omega$ has been determined already.

3.3.0. Every process of generating $\{B(\mathfrak{B}) \vee B'(\mathfrak{B}')\}$ $(\mathfrak{B}, \mathfrak{B}' \subset \mathfrak{G}_\omega)$ may be bounded by $\frac{|\mathfrak{G}_\omega|}{p_\omega}$ $(1 \leqslant \omega \leqslant n)$.

3.4. Suppose all elements of $\{B \vee B'\}$ have been listed. The characteristic number $c(B, B')$ of $\{B \vee B'\}$ is generally defined by $Z_n \cap \{B \vee B'\}$; by the assumption, however, we have $Z_n \cap \{B \vee B'\} = Z_\omega \cap \{B \vee B'\}$. Thus we have

3.4.0. Z_ω $(1 \leqslant \omega \leqslant n)$ (instead of Z_n) may be used for computing $c(B, B')$.

3.5. Furthermore the computation of $B \vee B'$, $B \wedge B'$ or the test of equality $B = B'$ of the above mentioned /Z&digital numbers may be bounded by the lowest $|Z_\omega|$ digits of B and B' (for the other digits are equal to zero). Hence

3.5.0. Operations amongst the ($|Z_n|$-digital) numbers B, B' may be bounded to operations amongst B, B' by considering only $Z_\omega|$ digits ($|Z_\omega| \leqslant |Z_n|$).

3.6. The validity of $B(\mathfrak{B}) \in L_1$ can be tested first by looking for those elements $b_i \in L_2$ $(1 \leqslant i \leqslant |L_1|)$ with the property $b_i = |\mathfrak{B}|$ and afterwards by testing $B = B_i$ ($B_i \in L_1$ corresponding to b_i). This method will save time and may be combined with the method of 3.5.0. Analogous statements are valid for L_1^* respectively L_2^*:

3.6.0. For testing $B \in L_1$ resp. L_1^* the elements of L_2 resp. L_2^* may be used.

3.7. If $\mathfrak{B} \subset \mathfrak{B}'$ resp. $\mathfrak{B}' \subset \mathfrak{B}$—this can be decided directly by (1.4)—we obtain $c(B, B') = B$ resp. B', i.e.

3.7.0. The composition $c(B, B)$ may be omitted if $B \wedge B' = B$ or B'.

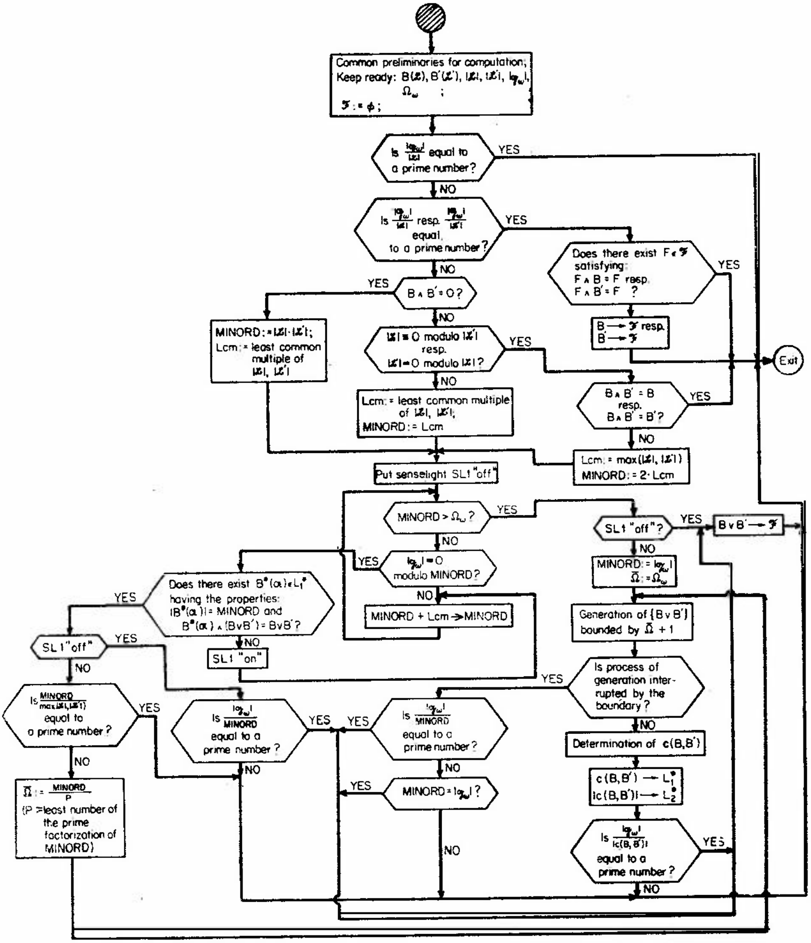
3.8. If $\left|\frac{\mathfrak{G}_\omega}{\mathfrak{B}}\right|$ resp. $\left|\frac{\mathfrak{G}_\omega}{\mathfrak{B}'}\right|$ are prime numbers (i.e. $\mathfrak{B}$ resp. $\mathfrak{B}'$ are maximal subgroups of $\mathfrak{G}_\omega$), a composition would be unnecessary, since the result would be $\mathfrak{G}_\omega$:

3.8.0. The composition may be omitted, if $\mathfrak{B}(\subset \mathfrak{G}_\omega)$ resp. $\mathfrak{B}'$(c $\mathfrak{G}_\omega$) are maximal subgroups of 8,.

3.9. As soon as for any two binary numbers $\tilde{B}$, $\tilde{B}'$ we have found (by computing or by using 3.8.0. for instance) that $\{\tilde{B} \vee \tilde{B}'\}$ is equal to $\mathfrak{G}_\omega$ or to any maximal subgroup of $\mathfrak{G}_\omega$, $\tilde{B} \vee \tilde{B}'$ is called a *jilter* and is listed. If there exists a filter F having the property $(B \vee B') \wedge F = F$, the result of the composition $c(B, B')$ is already known and therefore the composition may be omitted.

3.9.0. The composition $c(B, B')$ may be omitted if $(B \vee B') \wedge F = F$ for any element F of the list of filters.

3.10. Remembering the well-known formula $\{c(B(\mathfrak{B}), B'(\mathfrak{B}'))\} \geqslant \frac{|\mathfrak{B}| \cdot |\mathfrak{B}'|}{|\mathfrak{B} \cap \mathfrak{B}'|}$ we can estimate the order of the group being obtained by com-


Common preliminaries for computation; Keep ready: $B(\mathfrak{L})$, $B'(\mathfrak{L}')$, $|\mathfrak{L}|$, $|\mathfrak{L}'|$, $|\mathfrak{G}_\omega|$, Ω_ω ; $\mathfrak{F} := \phi$;
Is $\frac{|\mathfrak{G}_\omega|}{|\mathfrak{L}|}$ equal to a prime number?
YES
NO
Is $\frac{|\mathfrak{G}_\omega|}{|\mathfrak{L}|}$ resp. $\frac{|\mathfrak{G}_\omega|}{|\mathfrak{L}'|}$ equal to a prime number?
YES
Does there exist $F \in \mathfrak{F}$ satisfying: $F \wedge B = F$ resp. $F \wedge B' = F$?
YES
$B \rightarrow \mathfrak{F}$ resp. $B' \rightarrow \mathfrak{F}$
Exit
NO
YES
$B \wedge B' = 0$?
MINORD: $= |\mathfrak{L}| \cdot |\mathfrak{L}'|$; Lcm: = least common multiple of $|\mathfrak{L}|$, $|\mathfrak{L}'|$
NO
$|\mathfrak{L}| \equiv 0$ modulo $|\mathfrak{L}'|$ resp. $|\mathfrak{L}'| \equiv 0$ modulo $|\mathfrak{L}|$?
YES
NO
Lcm: = least common multiple of $|\mathfrak{L}|$, $|\mathfrak{L}'|$; MINORD: = Lcm
$B \wedge B' = B$ resp. $B \wedge B' = B'$?
YES
NO
Lcm: = max($|\mathfrak{L}|$, $|\mathfrak{L}'|$) MINORD: = 2·Lcm
Put senselight SL1 "off"
MINORD > Ω_ω ?
YES
NO
SL1 "off"?
YES
$B \vee B' \rightarrow \mathfrak{F}$
NO
MINORD: = $|\mathfrak{G}_\omega|$ $\bar{\Omega} := \Omega_\omega$
YES
$|\mathfrak{G}_\omega| \equiv 0$ modulo MINORD?
NO
MINORD + Lcm → MINORD
Does there exist $B^*(\alpha) \in L_1^*$ having the properties: $|B^*(\alpha)|$ = MINORD and $B^*(\alpha) \wedge (B \vee B') = B \vee B'$?
YES
NO
SL1 "on"
SL1 "off"
YES
NO
Generation of $\{B \vee B'\}$ bounded by $\bar{\Omega} + 1$
Is process of generation interrupted by the boundary?
YES
NO
Determination of $c(B,B')$
$c(B,B') \rightarrow L_1^*$ $|c(B,B')| \rightarrow L_2^*$
Is $\frac{\text{MINORD}}{\max(|\mathfrak{L}|,|\mathfrak{L}'|)}$ equal to a prime number?
YES
NO
$\bar{\Omega} := \frac{\text{MINORD}}{P}$ (P = least number of the prime factorization of MINORD)
Is $\frac{|\mathfrak{G}_\omega|}{\text{MINORD}}$ equal to a prime number?
YES
NO
YES
Is $\frac{|\mathfrak{G}_\omega|}{\text{MINORD}}$ equal to a prime number?
NO
YES
MINORD = $|\mathfrak{G}_\omega|$?
NO
Is $\frac{|\mathfrak{G}_\omega|}{|c(B,B')|}$ equal to a prime number?
YES
NO

position. The order $|\mathfrak{B} \cap \mathfrak{B}'|$ is equal to or less than the greatest common divisor of the orders of $\mathfrak{B}$ and $\mathfrak{B}'$. Thus assuming $B \wedge B' \neq \boldsymbol{B}$ resp. B' the order $\{c(B, B')\}|$ of the compound $\{B \vee B'\}$ will be bounded in the following way by a number called MINORD:

$$|\{\mathfrak{B} \cup \mathfrak{B}'\}| \geqslant \text{MINORD} = \begin{cases} |\mathfrak{B}| \cdot |\mathfrak{B}'|, \text{ if } B \wedge B' = \boldsymbol{0} \\ 2 \cdot \max(|\mathfrak{B}|, |\mathfrak{B}'|), \text{ if } |\mathfrak{B}| \equiv \text{Omod } |\mathfrak{B}'| \\ \qquad\qquad\qquad \text{resp. } \mathfrak{B}'| \equiv 0 \text{ mod } |\mathfrak{B}| \\ \text{least common multiple of } \mathfrak{B}|, |\mathfrak{B}'| \\ \text{for all other cases} \end{cases} \qquad (3.10.0)$$

If MINORD, computed by (3.10.0), is not yet a divisor of $|\mathfrak{G}_\omega|$, MINORD is repeatedly increased by the least common multiple until $|\mathfrak{G}_\omega|$ is divisible by MINORD. If there exists a characteristic number $B''(\mathfrak{B}'') \in L_1 \cup L_1^*$ ($|\mathfrak{B}''| =$ MINORD)-this may be tested by using 3.6.0—satisfying $(B \vee B') \wedge B'' = B \vee B'$ the composition may be omitted, for $c(B, B')$ would be equal to B''; otherwise we are looking for an element $B''(\mathfrak{B}'') \in L_1 \cup L_1^*$ satisfying $(B \vee B') \wedge B'' = B \vee B'$ and $|\mathfrak{B}''| >$ MINORD. Similarly to 3.3.0, $|\mathfrak{B}''|$ may be used for bounding the generation $\{B \vee B'\}$. Summarizing, we note

3.10.0. ***By computing the boundary*** MINORD *of* $\{\mathfrak{B} \cup \mathfrak{B}'\}$, ***the process of generating may be either omitted or bounded.***

The method by which the remarks 3.3.0. to 3.10.0. are used for composition is given in the flow-chart for computing $c(B(\mathfrak{B}), B'(\mathfrak{B}'))$ by $B(\mathfrak{B})$ and $B'(\mathfrak{B}')$.

4. Conclusion. By means of the computed set L_1 we are able to compute the full lattice $V(\mathfrak{G})$ of all subgroups of $\mathfrak{G}$. The method of computing $V(\mathfrak{G})$ is above all a method of iterative reduction of the set of all characteristic numbers by selecting-mainly by using (1.4)-those characteristic numbers corresponding to maximal subgroups. Since this method has been described in [2], it need not be further discussed here.

Finally the following table contains some examples of computed groups together with some further information. The computing time includes not only the time for computation of the lattice but also for computation of conjugate subgroups, the normalizers and centralizers of the representatives of these classes, and special characteristic subgroups, such as ascending and descending central-chains, Fitting and Frattini groups and others.

Group	Order	Mode of generation	Number of all cyclic subgroups of prime power order	Number of all proper subgroups	Number of classes of conjugated proper subgroups	Computing time
$\mathfrak{A}_5$	60	Permutations of degree 5	31	57	7	14·4 sec
$\mathfrak{S}_5$	120	Permutations of degree 5	56	154	17	1 min 12.6 sec
LF(2,7)	168	Permutations of degree 7	78	177	13	3 min 15·3 sec
$\mathfrak{G}_{192}^{(1)}$	192	Permutations of degree 8	61	349	56	4 min 40·0 sec
$\mathfrak{G}_{192}^{(2)}$	192	Permutations of degree 8	89	467	76	20 min 0·2 sec
$\mathfrak{G}_{216}$	216	Permutations of degree 9	76	180	18	5 min 28·5 sec
$\mathfrak{G}_{900}$	900	2 abstract elements	41	382	110	18 min 27·0 sec

REFERENCES

1. V. FELSCH and J. NEUBÜSER: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. *Mitt. d. Rhein. Westf. Inst. f. Znstr. Mathematik, Bonn, 2 (1963), 39-74.*
2. L. GERHARDS and W. LINDENBERG: Ein Verfahren zur Berechnung des vollständigen Untergruppenverbandes endlicher Gruppen auf Dualmaschinen. *Num. Math. 7* (1965), 1-10.
3. W. LINDENBERG: Über eine Darstelhmg von Gruppenelementen in digitalen Rechenautomaten. *Num. Math.* 4 (1962), 151-153.
4. J. NEUBÜSER: Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programm-gesteuerten elektronischen Dualmaschine. *Num. Math. 2* (1960), 280-292.

A programme for the drawing of lattices

K. Ferber and H. Jürgensen

The programme A described here was developed by the second author in 1965/66. It was established when a number of lattices of subgroups had to be drawn for [2], but it was organized in such a way that it is equally efficient for drawing a diagram representing any finite semi-order for which the relations of reflexiveness, transitivity, and antisymmetry hold. However, for this report we shall use the terms occurring with a lattice of subgroups, such as "subgroup", "order", "conjugate", "class of conjugate subgroups", etc.

For the programme A all subgroups of a group G are numbered in a list L_0: (1) = $U_0, U_1, \ldots, U_n$ = G in a fixed way. We shall refer to $\boldsymbol{i}$ as the list-number of U_i. In the diagram to be drawn, the subgroups are represented by circles or squares containing the list-number of the subgroup in the numbering mentioned above. If circles (squares) are connected horizontally, the corresponding subgroups are conjugate, if they are connected vertically, the lower one is a maximal subgroup of the higher one (see Fig. 1).

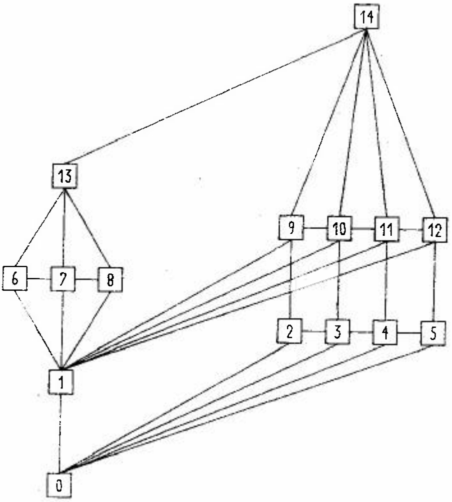


FIG. 1

The input for the programme Λ is a paper tape with the following information about the lattice L(G) of subgroups of G:

(1) the number k of classes of subgroups conjugate in G,
(2) the number n of subgroups of G,
(3) for each class K_i of conjugate subgroups $U_{i_1}, \ldots, U_{i_{n_t}}$ of G:
 (a) the order of these subgroups,
 (b) the list-numbers $i_1, \ldots, i_{n_t}$,
 (c) for each $U_{i_s} \in K_i$ the list-numbers of its maximal subgroups in the numbering mentioned above.

A paper tape with this information is provided, for example [1], by a programme Φ implemented on an Electrologica XI, which determines the lattice of subgroups of a group G from generators of G. The programme Λ which has been implemented on a Zuse Z22 reads this tape and punches a data tape for the plotter Zuse 264. For this the programme Λ needs some additional information about the size and shape of the diagram wanted.

The following data for the drawing may be prescribed :

(1) the radius r of the circles representing subgroups (or half the side of the squares),
(2) a (common) ordinate for the centres of circles representing a class K_i of conjugate subgroups,
(3) an abscissa of these centres for each subgroup.

If these data are not prescribed, the programme Λ puts $r = 3$ mm and tries to find suitable ordinates and abscissas. This is done in the following way.

An ordinate is calculated as a function which depends linearly on the radius r and logarithmically on the order of the subgroups in K_i. The abscissas are calculated by the programme only under special conditions : G must be a p-group or a group of order $p^m q$, where p and q are primes and $p < q$; moreover, when U, V are subgroups of G, U maximal in V, $|U| = p^r q$, $|V| = p^s q$, it is not allowed that there exists a subgroup W of G with $|W| = p^t q$ and $r < t < s$. Geometrically this means that the diagram of the lattice of G must consist of at most two "branches".

For groups satisfying these requirements the set of all subgroups of order p^j, $0 \leq j \leq m$, is called the first branch B^1, the set of all subgroups of order $p^j q$ is called the second branch B^2 of L(G); the set of all subgroups whose order is the product of i primes is called the ith layer L_i of $L(G)$. $L_i \cap B^j$ is called the row R_i^j.

In order to calculate the abscissas for B^1, the row R_a^1, containing the greatest number of subgroups is determined, and the abscissas for these subgroups are defined from left to right according to the sequence in which they occur on the data tape. All other rows are arranged in such a way that their geometrical centre has the same abscissa as the one of R_a^1.

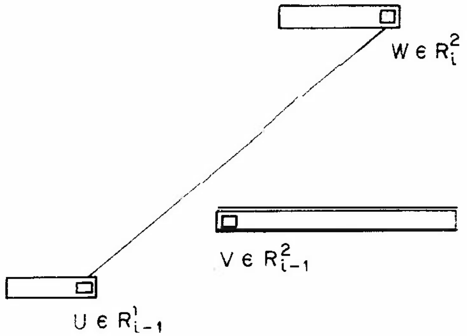


FIG. 2

The abscissas for the subgroups in B^2 are determined in two main steps.

First, consecutive rows of the first branch are considered. Let U be the first subgroup in the row R_{i-1}^1, V be the last subgroup in R_i^1, W be the first subgroup in R_i^2. Then the abscissa x_w for W is determined in such a way that V is left of the line connecting U and W and has a certain distance from it (see Fig. 2). From x_w the abscissa x_{ci} of the centre of R_i^2 is found. This calculation is done for all i, $1 \leqslant i \leqslant m$, and the maximum x of the x_{ci} found. Then all rows R_i^2 are moved to the right until the abscissas of their centres coincide with x.

Second, a similar procedure is performed for consecutive rows of the second branch. Let U be the last subgroup of R_{i-1}^1, V be the first subgroup of R_{i-1}^2 and W be the last subgroup of R_i^2 (see Fig. 3). It is tested if V is to the right of the line connecting U and *Wand* has a proper distance from it. If not, the second branch is again moved to the right until this is the case. This procedure is performed for all i, $1 < i \leqslant m + 1$.

From the maximal abscissas and ordinates the size of the diagram to be drawn is obtained. If this is too large, the radius r chosen for the circles is

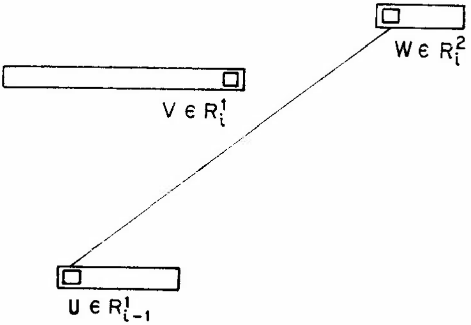


FIG. 3

reduced by 1 mm and the coordinates are calculated again, until either the size is small enough for the plotter or the radius is reduced to 1 mm. The size of the diagram is then printed or the calculation is interrupted with a note on the printer.

The programme A next forms a list L_1 which contains for every class K_i and every subgroup $U_{i_j} \in K_i$:

(1) the list-number i_j of U_{i_j},

(2) the number $m(U_{i_j})$ of maximal subgroups of U_{i_j},

(3) the list-numbers of these maximal subgroups in the list $\boldsymbol{Lo}$.

As we shall describe later, in the course of the programme all these numbers are inverted when the information they carry has been used for the construction of the data tape for the plotter. Hence in the following description some of these numbers may be negative. In this description we shall say that A draws the lattice instead of saying more correctly that A punches the tape for the plotter which draws the diagram representing the lattice.

The programme A contains the following two main subroutines working on the list L_1. Given a class $\boldsymbol{K}$ the subroutine "maxclass" searches for the subgroup $U \in \boldsymbol{K}$ whose list-number has greatest absolute value among those subgroups which have positive list-number or have a maximal subgroup with positive list-number.

Given a subgroup $U \in \boldsymbol{K}$ the subroutine "classconj" has the following effect :

(1) if the list-number of U is still positive, "classconj" draws U and all its conjugates with greater abscissas and positive list-numbers and then inverts all these list-numbers; the conjugate subgroups just drawn are connected by horizontal lines;

(2) let the subgroup drawn last be V. Then a subgroup $W \in \boldsymbol{K}$ is determined: If V is the last subgroup of $\boldsymbol{K}$ then $W = V$, otherwise $\boldsymbol{W}$ is the next subgroup of K right to V. If no subgroup, is drawn by "classconj" $\boldsymbol{W} = \boldsymbol{U}$.

Using these two subroutines the programme A works through the list of all classes beginning with the last one, i.e. the group G itself. For a class $\boldsymbol{K}$ first the subroutine "maxclass" is called and searches for a subgroup $U \in \boldsymbol{K}$ with the properties described above. If there is none, "maxclass" is called again for the next class until the list of all classes is finished.

(*) Otherwise for this subgroup U "classconj" is called which finally determines a subgroup $W \in \boldsymbol{K}$. Then A searches for a maximal subgroup U' of $\boldsymbol{W}$ with maximal positive list-number. If no such subgroup exists, A starts "maxclass" again for the same class $\boldsymbol{K}$. Otherwise a line is drawn from $\boldsymbol{W}$ to U' and the list-number of U' is inverted among the entries for the maximal subgroups of $\boldsymbol{W}$. If none of the entries for the maximal subgroups of *Wis* positive, also *m(W)* is inverted and "classconj" is started with the class K' to which U' belongs, and determines a subgroup $W' \in K'$. Then Λ searches for the subgroup U'' with maximal list-number among those containing W' and having a positive entry for W'. If there is none, "max-class" is started again with still the same class K. Otherwise W' and U'' are connected by a line and the entry for W' as a maximal subgroup of U'' is inverted. If U'' has no further positive entry in the list of its maximal subgroups, $m(U'')$ is inverted. In any case Λ then starts again at (*) with U'' instead of U. The programme stops when the class $K_0$is reached and all lines are drawn.

It may be mentioned that there is also a subroutine which inverts all list-numbers of non-normal subgroups in L_1, sо that, if required, only the lattice of normal subgroups is drawn.

The following improvement is planned for the programme. Whenever there is no subgroup U'' which contains W' as a maximal one, the programme starts "maxclass" again with the previous class K. For the drawing of the lattice it would save time to continue instead with a "neighbouring" subgroup W^* of W', which is still denoted as being maximal in some subgroup.

REFERENCES

1. V. FELSCH and J. NEUBÜSER: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. *Mitt. Rh.-W. Inst. f. Znstr. Math. Bonn 2* (1963), 39-74.
2. J. NEUBÜSER: Die Untergruppenverbände der Gruppen der Ordnungen ≤ 100 mit Ausnahme der Ordnungen 64 und 96. Habilitationsschrift, Kiel, 1967.

The construction of the character table of a finite group from generators and relations

JOHN MCKAY

Introduction. There are six problems in determining the character table from the generators and defining relations for a finite group. They are

(a) derivation of a faithful representation,
(b) generation of the group elements,
(c) determination of the mapping of an element into its conjugacy class,
(d) derivation of the structure constants of the class algebra,
(e) determination of the numerical values of the characters from the structure constants, and
(f) derivation of the algebraic from the numerical values.

Use of the methods is illustrated by the construction of the character table of the simple group J_1, of order 175,560, which is given in the Appendix in the form output by the computer.

G denotes a finite group of order g having r conjugacy classes C_i of order h_i, $i = 1, \ldots . r$. $C_{i'}$ is the class inverse to C_i. $A(G, C)$ denotes the group algebra of G over the complex field C.

Derivation of a faithful representation. Enumeration of the cosets of a subgroup H of G gives rise to a permutation representation on the generators and their inverses. The representation so formed is a faithful representation of the factor group G/N, where $N = \bigcap_{x \in G} x^{-1}Hx$, known as the "core" of H in G. The representation will be a faithful representation of G whenever H contains no non-trivial normal subgroup of G. There are three requirements in particular for representations to be useful for computing purposes. Firstly, the representation of an element should be unique; secondly, it should be representable within the computer sufficiently economically to cause no storage problem; and thirdly, it should be such that the product of two elements can be derived quickly. For the smaller groups these requirements may be relaxed, but for large groups they are essential.

Both permutation representations and faithful irreducible representations of minimal degree are suitable for computer work. Multiplication of permutations is fast but it is often easier to find a matrix representation more economical in space. Frame's work [1] on extracting the common irreducible constituents of two permutation representations appears to be promising as a basis of a method for doing this.

Generation of the group elements. One method for generating all elements of a group G is to compute the Cayley table. This method is quite satisfactory for groups of very small order but it is clearly of little use when working with large groups because the computation increases, at best, with g^2. A method with computation time linear in g is called for.

Let

$$G (= H_0) \supset H_1 \supset H_2 \supset \ldots \supset H_t \text{ be a chain of subgroups,}$$

and let

$$H_i = H_{i+1}x_1 \cup H_{i+1}x_2 \cup \ldots \cup H_{i+1}x_n$$

be a coset decomposition of H_i.

H_i can be generated systematically from H_{i+1} provided a faithful representation on the coset representatives and the generators of H_i is known and H_{i+1} itself can be generated systematically using this representation. Repeated coset enumeration will give G from the subgroup H_t. A solution to the following problem is required, see [2]:

given $\quad H_i$: $r_k(g_1, g_2, \ldots, g_s) = 1, \quad k = 1, 2, \ldots, m_i,$

and $\quad H_{i+1}$: $\{w_j(g_1, g_2, \ldots, g_s)\}$, $j = 1, 2, \ldots, n_i$,

derive a presentation of H_{i+1}: $r'_k(g_1, g_2, \ldots, g_s) = 1$, $k = 1, 2, \ldots, m_{i+1}$. There are two special cases of this technique which prove very useful. By taking just the identity subgroup of G, we may enumerate the cosets of the identity which are just the elements of G. This is a satisfactory method for generating all the elements of a group of moderate order. The other special case is when G $\supset$ ***H*** and the elements of ***H*** can be generated directly as matrices compatible with the representing matrices of G. This last case is illustrated by the generation of J_1 by taking $H \cong PSL(2, 11)$ (see Appendix).

To find the coset representatives, we use

Lemma. *There exists for each index* i $(\neq 1)$ *a coset* Hx_k *with* $k < i$ *such that either* (i) $Hx_i = Hx_k g_j^{-1}$ *or* (ii) $Hx_i = Hx_k g_j$ *for some generator* g_j *of* G.

All new cosets, except the first, are introduced in the middle of a relation. There is therefore a coset of lower index adjacent to the new one. Coset collapse will affect these adjacent cosets by possibly reducing their index. A coset of lower index to the right gives rise to situation (i) and to the left yields (ii).

We can generate the representing matrices on the coset representatives from those on the generators of G by seeking the coset Hx_k for increasing $i = 2, 3, \ldots, n$ and forming $\phi_i = \phi_k g_j^{-1}$ or $\phi_i = \phi_k g_j$ where ϕ_k is a coset representative of Hx_k.

The mapping of an element into its conjugacy class. A function f on G is a class function if

$$f(x) = f(y^{-1}xy), \quad x, \text{Y} \in G.$$

f induces an equivalence relation on the elements of G. We seek a function f such that the equivalence classes induced by f are the conjugacy classes of G. In order to avoid searching, we seek a local property of x such as the trace, determinant, or period. There are several groups with representations for which this local property is easily obtained. By taking the natural permutation representation of degree n of the symmetric group of n symbols we see that two elements are conjugate if and only if the partitions of their disjoint cycle lengths coincide. The general linear group of all invertible $n \times n$ matrices with entries over a field Kpresents no difficulties since two elements are conjugate if and only if their representing matrices are similar. We know that ths transforming matrix belongs to the group since it is the group of ***all*** invertible n **X** n matrices.

From a practical view point, a good set of local invariants that may be computed easily is the set of coefficients of the characteristic (or minimal) polynomial. The computation time is $O(n^3)$ for a matrix of order n.

If the number of conjugacy classes of G is known, it may be adequate to examine the characteristic polynomials of a random sample of the group to attempt to find a representative element of each class and to see which classes can be separated by their traces alone. The likelihood of success of the search is dependent on the size of the smallest non-trivial conjugacy classes. The characteristic polynomial of an element x also gives (by reversing the coefficients) the characteristic polynomial of x^{-1}.

It is a necessary condition that a representative element of period p shall have been found for each prime factor p of g. For sufficiency, let $Z(x)$ be the centralizer of x in G, then a representative of every class has been found if

$$g = \sum_{x} g/|Z(x)|, \ x \in C_i',$$

where the summation is over the representatives of all putative conjugacy classes C_i' of G.

If so, we shall have obtained a representative for each conjugacy class. For groups of small order, when it is feasible to store all the elements, one may alternatively compute the conjugacy class of x directly, forming all elements $y^{-1}xy$, y $\in$ G. Proceeding in this fashion, the elements may be arranged so that conjugacy classes are stored as sets of adjacent elements. The function f then consists of a subroutine which searches for the element whose class is determined by its position.

Derivation of the centre of the group algebra. Throughout the rest of this paper, c denotes summation from 1 to r unless stated to the contrary. The relations

$$c_i c_j = \sum_{k} \alpha_{ijk} c_k, \quad 1 \leq i, j \leq r, \tag{1}$$

defining multiplication of the class sums, $c_i = \Sigma\, x$, summed over all $x \in C_i$, are sufficient to determine the centre of the group algebra since the class sums form a basis for the centre.

The structure constants α_{ijk} may be interpreted in two ways: first, in the manner in which they occur in (1), and second, α_{ijk} may be regarded as the number of ways z may be formed as a product such that

$$xy = z, \quad x \in C_i, \quad y \in C_j$$

with z a fixed element of C_k.

The latter interpretation is the one used for the computation of the α_{ijk}.

For each element y representative of C_j, and for all $x \in C_i$, the number k such that $xy \in C_k$ is found. Let the number of products xy in C_k be β_{ijk}; then $\alpha_{ijk} = \dfrac{h_j}{h_k}\,\beta_{ijk}$.

The r^3 α_{ijk} satisfy symmetry relations most succinctly expressed by the relations satisfied by $\gamma_{ijk} = (h_i h_j)^{-1}\alpha_{ijk'}$. The γ_{ijk} are invariant under any permutation of the suffixes and also under the simultaneous inversion of all three suffixes.

Construction of the normal subgroup lattice. We define, for each conjugacy class, a basic normal subgroup B_i of G to be the normal closure of an element belonging to C_i. Such a basic normal subgroup is obtainable from the class algebra by forming the union of successive powers of C_i until no new class is introduced.

The minimal normal subgroups of G are included among the basic normal subgroups. We use the fact that the lattice of normal subgroups is modular and therefore satisfies the Jordan-Dedekind chain condition which enables us to build the lattice level by level. The first (and bottom) level is the identity subgroup and the last is the whole group. The number of levels is the length of a principal series for G. We shall denote the ith level of normal subgroups by L_i. The identity subgroup is taken as L_0.

Let n_i denote a normal subgroup. The computation follows the inductive scheme :

$$M_i = \{n_{i1}, \ldots , n_{it}\};$$

$$n_{ij} \in E_{i+1} \leftrightarrow n_{ij} \supset n_{ik} \text{ for some } k, \qquad \text{otherwise} \quad n_{ij} \in L_i;$$

$$M_{i+1} = \{n_{ij}n_{ik} \mid n_{ij}, n_{ik} \in L_i\} \cup E_{i+1};$$

and proceeds until $M_s = \{G\}$. To start we take $M_1 = \{B_2, \ldots , B_r\}$.

The numerical characters from the structure constants. Let R^s be an irreducible matrix representation of the group algebra $A(G, C)$. From (1) we find

$$R^s(c_i c_j) = R^s(c_i)R^s(c_j) = \sum_k \alpha_{ijk} R^s(c_k), \quad 1 \leqslant i, j \leqslant r. \tag{2}$$

Now $R^s(c_i)$ commutes with every $R^s(x)$, $x \in A(G, C)$, and since R^s is irreducible we may use Schur's lemma, hence

$$R^s(c_i) = m_i^s I_d, \tag{3}$$

where d $(= d_s)$ is the dimension of R^s, and m_i^s is a scalar.

Substituting (3) in (2) and comparing the coefficients of both sides, we obtain

$$m_i^s m_j^s = \sum_k \alpha_{ijk} m_k^s, \quad 1 \leq i, j \leq r, \tag{4}$$

which may be written

$$A^i \boldsymbol{m}^s = m_i^s \boldsymbol{m}^s, \; [A^i]_{jk} = \alpha_{ijk}, \quad 1 \leq i, j, k \leq r. \tag{5}$$

This collection of r sets of matrix equations is fundamental to the computation of the characters. We shall show that the matrices A', $1 \leq i \leq r$, have a unique common set of r eigenvectors.

First we find the eigenvalues of A'. Recall that R^s is a homomorphism of G into a group of $d \times d$ matrices. The identity of G maps into the identity matrix I_d. From (3) we deduce $m_1^s = 1$. But m_1^s is the first component of the vector $\boldsymbol{m}^s$ and so (5) has a non-trivial solution. Therefore

$$\det\,(A^i - m_i^s I) = 0, \quad 1 \leq i \leq r. \tag{6}$$

This is true for all $s = 1, 2, \ldots, r$, hence the eigenvalues of A^i are m_i^s, $1 \leq s \leq r$.

We use the row orthogonality properties of the characters to prove the $\boldsymbol{m}^s$, $1 \leq s \leq r$, to be a linearly independent set of vectors. First, we need the relation between the components of these vectors and the characters.

Take traces of both sides of (3) to derive

$$h_i \chi_i^s = m_i^s d_s,$$

hence

$$m_i^s = \frac{h_i \chi_i^s}{d_s}. \tag{7}$$

The row orthogonality relations are :

$$\sum_i h_i \chi_i^s \bar{\chi}_i^t = g\, \delta_{st}, \quad 1 \leq s, t \leq r. \tag{8}$$

Defining the $r \times r$ matrices M and X by

$$M_{st} = m_t^s, \; X_{st} = \chi_t^s, \text{ then } MX^* = \operatorname{diag}\left\{\frac{g}{d_1}, \frac{g}{d_2}, \ldots, \frac{g}{d_r}\right\}$$

where * denotes complex conjugate transpose. The diagonal entries g/d_i are all non-zero, hence the rank of M is r.

Let $\boldsymbol{x}$ be a vector such that $A^i \boldsymbol{x} = m_i^s \boldsymbol{x}$ for all $i = 1, 2, \ldots, r$, then $\boldsymbol{x} = \sum_t a_t \boldsymbol{m}^t$. Suppose $a_t \neq 0$. Then

$$\sum_t a_t m_i^t \boldsymbol{m}^t = \sum_t a_t m_i^s \boldsymbol{m}^t, \quad i = 1, 2, \ldots, r,$$

hence

$$\sum_t a_t m^t = \sum_t a_t m^s,$$

and so

$$x = a_s m_s .$$

We have the following situation.

The entries in the ith column of M are the eigenvalues of A^i and the rows of M correspond to the common eigenvectors normalized so that $m^s_1 = 1$. If the entries in the column of M corresponding to the eigenvalues of A' are all distinct then the whole matrix M can be determined from the matrix A' alone. This, however, is not usually the case. An extreme case occurs when G = $Z_2 \times Z_2 \times \ldots \times Z_2$, the direct product of n copies. of the cyclic group Z_2. Here each column of M (except the first) has entries ± 1 each sign occurring 2^{n-1} times.

A method is described to overcome the difficulty inherent in multiple eigenvalues.

The idea of the method is that if a matrix has distinct eigenvalues, then the eigenvectors are determinate (each to within a scalar multiple).

Let u_i, $i = 1, 2, \ldots, r$, be indeterminates and consider the matrix

$$\Phi = \sum_i u_i A^i \text{ which has eigenvalues } \sum_i u_i m^s_i, \quad 1 \leqslant s \leqslant r.$$

By choosing suitable values for the indeterminates we can arrange that the eigenvalues are distinct; if so, the eigenvectors of Φ are just m^s, $1 \leqslant s \leqslant r$.

For computational purposes we replace the indeterminates by random numbers. We may then associate a probability to the numerical separability of the eigenvalues.

We require that for each $p \neq q$ (= 1, 2, . . . , r) the eigenvalues corresponding to m^p and m^q should be separable, i.e.

$$\Big| \sum_i \theta_i m^p_i - \sum_i \theta_i m^q_i > \varepsilon(t) \quad \text{for all } p \neq q = 1, 2, \ldots, r,$$

where the θ_i are chosen from some suitable normalized distribution and $\varepsilon(t)$ is a small number dependent on the accuracy of the computer.

The largest eigenvalue of A' is 1. We introduce a normalizing factor of r^{-1} and choose θ_i to be the coordinates of a point on an n-dimensional hyperellipsoid of semi-axes $h_i^{-1/2}$ so that $\theta_i \, h_i^{1/2}$ are points distributed on the hypersurface of an n-dimensional sphere.

A detailed error analysis is hindered because of lack of adequate prior knowledge of the m^p.

The numerical method for solving the eigenvalue problem is the accelerated *QR* method [3]. The eigenvectors are found by inverse iteration.

Derivation of the algebraic form from the numerical. By normalizing the solution vectors of Φ so that the first component is unity, we have the numerical values of m^s_i. To find the dimension of the representation we

.use the relation, derivable from the row orthogonality relations

$$\frac{1}{g}\sum_i \frac{1}{h_i}\,|m_i^s|^2 = \frac{1}{d_s^2}.$$

By multiplying m_i^s by d_s and dividing by h_i we find the numerical characters. As decimal numbers, these are of little interest; we would prefer them in an algebraic form.

For a representation of degree d over the complex field and an element of period p,

$$\chi(x) = \sum_{i=1}^{d} \omega^{t_i}, \quad 0 \leqslant t_i \leqslant p-1,$$

where ω is a primitive pth root of unity. Let $\chi_N(x)$ be a numerical approximation to $\chi(x)$. We may rearrange the terms so that $t_1 \leqslant t_2 \leqslant \ldots \leqslant t_d$. There are $\binom{d+p-1}{d}$ such sequences. We could generate the sequence systematically starting at 0, 0, . . . , 0 and ending atp - 1, p- 1, . . . , p - 1, and examine the value of the cyclic sum each yields. We can improve on this. The problem may be visualized geometrically in the complex plane as follows :

Each root of unity may be represented by a unit vector which lies at an angle which is a multiple of $2\pi/p$ to the horizontal. We form a sum of these vectors by joining them up, end to end. We seek such a sum starting from the origin and reaching to $\chi(x)$. We generate the sequences described above but check to see whether, after fixing the first s vectors, the distance from the sum of first s terms to $\chi_N(x)$ is less than ***d-s;*** if not, we alter t_s.

Even with the above improvement, the algebraic form of the character of an element of period p in a representation of degree d such that $p, d > 10$ would be very time-consuming to determine, and in cases such as presented by the representations of J_1, this is out of the question. The following **fact** may be used: among the terms of the sequences computed may be some whose sum contribution to the total is nil. Each such subsequence may be decomposed into disjoint subsequences each containing a prime number of terms. These correspond to regular p_i-gons for prime p_i. From a computational viewpoint this implies that, provided $u \geqslant 0$, we can attempt to fit $\chi_N(x)$ with only $u = d- \sum_{i=1}^{k} c_i p_i$ $(c_i \geqslant 0)$ terms where p_i are **prime** divisors of p. We now compute the values that $\sum_i c_i p_i$ can take.

If p has only one prime factor, the values assumed are multiples of that factor.

Let p_1, p_2 be the smallest two distinct prime factors of p. All integers not less than $(p_1-1)(p_2-1)$ are representable as $c_1p_1+c_2p_2$ $(c_1, c_2 \geqslant 0)$. In cases when $(p_1-1)(p_2-1) > d$, values not greater than u are computed directly.

All integer valued characters are extracted before attempting to match terms because certain values, e.g. -1, are time-consuming to fit.

The above discussion has not taken into account that only an approximation to the numerical value of $\chi(x)$ is the starting point. If two distinct values of sums of roots of unity differ by less than ε in modulus, where ε is the accuracy of computation of the value of $\chi_N(x)$, then the results of the above algorithm will not necessarily be correct. A lower bound is required for the non-zero values of

$$P(\omega) = \left|\sum_{i=1}^{d}\omega^{k_i}-\sum_{i=1}^{d}\omega^{m_i}\right| \qquad 0 \leqslant k_i,\, m_i \leqslant p-1.$$

By forming the product of the conjugates of $P(o)$ we obtain a lower bound :

$$/P(w) \geqslant (2d)^{2-p}.$$

Results. Character tables have been computed for all non-abelian groups of order less than 32 from definitions in Coxeter and Moser [4] and for the non-abelian groups of order 2^n ($n \leqslant 6$) from definitions in Hall and Senior [5]. The character table of J_1 has been computed as described in the Appendix.

Appendix

A brief description of the determination of the character table of Janko's first new simple group J_1, of order $11(11^3-1)(11+1) = 175,560$, is given, see [6]. The work has been carried out on a KDF 9 computer with 16K words of fast store, of which 4K were used to contain the program.

Throughout, the capital letters A, B, C, D denote matrices representing a, b, c, d respectively.

We take as a definition, due to G. Higman, of J_1:

$$a^2 = (ab)^2 = b^5 = 1, \quad b^{-1}cbc^2 = (ac)^3 = c^{11} = 1,$$
$$d^2 = dbdb^{-1} = (cd)^2 = (ad)^6 = (ac^2d)^5 = 1.$$

We note that $\{a, b, c\}$ generate a subgroup H isomorphic to $PSL(2, 11)$, which is the group of 2 X2 matrices of unit determinant over $GF(11)$ with the centre factored out, i.e. each matrix is identified with its negative. The 660 matrices of $PSL(2, 11)$ are generated systematically.

This representation is extended to a tensor representation of dimension 7 by treating the transformations x $\leftarrow ax+by$ and y $\leftarrow cx+dy$ as acting in the space of homogeneous polynomials of degree 6 in x and y. In this space $x^{6-r}y^r \leftarrow (ax+by)^{6-r}(cx+dy)^r$. This representation extends to a faithful representation of J_1.

By choosing matrices of simple form for A and C $\in$ ***PSL (2,1*** 1), we find correspondingly simple forms for B (= $C^4AC^3AC^4A$) and D.

We-take $A = \begin{bmatrix} 0 & 1 \\ 10 & 0 \end{bmatrix}$, C $= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, deriving $B = \begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}$. In the tensor representation these extend to

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 6 & 4 & 9 & 4 & 6 & 1 \\ 0 & 1 & 5 & 10 & 10 & 5 & 1 \\ 0 & 0 & 1 & 4 & 6 & 4 & 1 \\ 0 & 0 & 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We now need the representing matrix for d. d commutes with b, hence $d_{ij} = 0$ except when $i = j$ or $b_i = b_{jj}$ (i ‡ j). This simplifies the possible form of D to that of a diagonal matrix augmented by non-zero entries in the (1, 6), (6, 1), (2, 7), (7, 2) positions. We compare CD and DC^{-1}. C^{-1} has entries $(-1)^{j-i}c_{ij}$. From the first row and entries (2, 2) and (3, 7) we derive the form

$$D = \begin{bmatrix} x & 0 & 0 & 0 & 0 & -6w & 0 \\ 0 & -x & 0 & 0 & 0 & 0 & w \\ 0 & 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -x & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}$$

but $d^2 = 1$,hencex $= \pm 1$.

Comparing $(AD)^3$ and $(DA)^3 = (AD)^{-3}$, we obtain from the (2, 1) entry $-wx^2 = 2w^3$, hence $w = 0$ or $2w^2 = -1$ giving $w = 0, 4$, or 7.

Finally checking $(AC^2D)^5 = 1$ gives the unique solution $w = 7$, $x = -1$. These matrices were manipulated using a matrix multiplication program for use with an on-line console to a PDP 8 computer.

The cosets of H in J_1 are enumerated and the 266 coset representatives found. By examining the characteristic polynomials of a random sample of the group representation (elements of the form h_ix_j where $h_i \in$ ***Hand*** x_j is a coset representative) we can distinguish 15 conjugacy classes. Of these, 7 may be distinguished by their traces and 6 by the first two coefficients. The two remaining classes include the identity and so may be separated by examination. The trace of the square of the matrix is computed instead of the second coefficient.

The rest of the computation follows the method described in the paper. Approximately 1,800,000 matrix multiplications are required, each matrix being of degree 7 over GF (11). The computation of the class algebra took eight hours and the construction of the final character table from the class algebra took less than two minutes.

Character Table

Class		1	2	3	4	5	6	7	8
Order			1463	5852	5852	5852	9240	9240	9240
Period			2	3	5	5	19	19	19
	1:	1	1	1	1	1			1
	2:	56	0	2	2+4c2	2+4cl	- 1	- 1	- 1
	3:	56	0	2	2+4cl	2+4c2	- 1	- 1	- 1
	4:	76	4		1	1	0	0	0
	5:	76	- 4	1	1		0	0	0
	6:	77	5	- 1	2	2			1
	7:	77	- 3	2	2cl	2c2	1		1
	8:	77	- 3	2	2c2	2cl	1	1	1
	9:	120	0	0	0	0	2c2 + 2c3 + 2c5	2c4 + 2c6 + 2c9	2c1+2c7+2c8
	10:	120	0	0	0	0	2c1+2c7+2c8	2c2+2c3+2c5	2c4+2c6+2c9
	11:	120	0	0	0	0	2c4+2c6+2c9	2c1+2c7+2c8	2c2 + 2c3 + 2c5
	12:	133	5	1	- 2	- 2	0	0	0
	13:	133	- 3	- 2	1+2c2	1+2c1	0	0	0
	14:	133	- 3	- 2	1+2c1	1+2c2	0	0	0
	15:	209	1	- 1	- 1	- 1	0	0	0

Character Table

Class		9	10	11	12	13	14	15
Order		11704	11704	15960	17556	17556	25080	29260
Period		15	15	11	10	10	7	6
	1:	1	1	1	1	1	1	1
	2:	2c3	2c6	1	0	0	0	0
	3:	2c6	2c3	1	0	0	0	0
	4:		1	- 1	- 1	- 1	- 1	
	5:	1	1	-1	1	1	- 1	- 1
	6:	-1	-1	0	0	0	0	- 1
	7:	2c3	2c6	0	2c2	2c4	0	0
	8:	2c6	2c3	0	2c4	2c2	0	0
	9:	0	0	- 1	0	0	1	0
	10:	0	0	- 1	0	0		0
	11:	0	0	- 1	0	0	1	0
	12:	1		1	0	0	0	- 1
	13:	1+2c6	1+2c3	1	2c2	2c4	0	0
	14:	1+2c3	1+2c6	1	2c4	2c2	0	0
	15:	- 1	-1	0	1	1	-1	1

In the table, c indicates the cosine of a multiple of 2π/period. For example, $2+4c2$, occurring in the second row of the table as the character of an element of period 5 in the fourth conjugacy class, is an abbreviation for $2+4\cos(2\times 2\pi/5)$.

REFERENCES

1. J. S. FRAME: The constructive reduction of finite group representations. *Proc. Symp. Pure Maths. (AMS) 6* (1962), 89-99.
2. N. S. MENDELSOHN: Defining relations for subgroups of finite index of groups with a finite presentation. These Proceedings, pp. 43-44.
3. J. G. F. FRANCIS: The QR transformation. *Pts.* 1 & *2. Computer Journal 4* (1961-1962), 265-271, 332-345.
4. H. S. M. COXETER and W. *0.* J. MOSER: *Generators and Relations for Discrete Groups.* Ergebnisse der Mathematik NF 14 (Springer, Berlin 1965).
5. M. HALL and J. K. SENIOR: *Groups of Order* 2^n ($n \leqslant 6$) (MacMillan, New York, 1964).
6. Z. JANKO: A new finite simple group with Abelian Sylow 2-subgroups and its characterization. *J. of Algebra, 3* (1966), 147-186.

A programme for the calculation of characters and representations of finite groups

C. Brottand J. Neubüser

1. **Introduction.** The programme described in this paper is part of a system of programmes for the investigation of finite groups. Other parts of this system are described in [3], [4].

The programme avoids numerical calculations as far as possible. Instead properties of the given group which are available from other programmes have been used to construct characters and representations by the process of induction. Only when this process does not yield all the required information does the programme use numerical methods.

The programme has been started as a "Diplomarbeit" [1]. We are grateful to the Deutsche Forschungsgemeinschaft for financial support and to Prof. K. H. Weise for opportunities given to us at the "Rechenzentrum der Universität Kiel". We would like to thank Mr. V. Felsch for valuable -help in connecting this programme with the one described in [3].

1.1. ***Notations.*** All groups considered are finite, they are denoted by G, $H, \dots$; $\langle g_1, \dots . g_e \rangle$ is the subgroup generated by the elements $g_1, \dots, g_e \in$ G; G' = $\langle x^{-1}y^{-1}xy \mid x, y \in$ G) is the commutator subgroup of G; $C_1, \dots . C_r$ are the classes of elements conjugate in G; $C_1 = \{I\}$, h_i is the number of elements in C_i. The structure constants c_{ijk} are defined by

$$C_iC_j = \sum_{k=1} c_{ijk}C_k. \tag{1.1.1}$$

$\mathbf{Z}$ is the ring of integers, $\boldsymbol{Z_p}$ the field of integers modulo a prime $\boldsymbol{p}$, $\boldsymbol{C}$ the complex field, $M_1, \dots, M_r$ the set of all absolutely irreducible CG-modules with dimensions $d_1, \dots, d_r$. $\chi^{(j)}$ is the character belonging to M_j, $\chi_i^{(j)}$ its value on C_i. All representations considered are C-representations, so irreducible always means absolutely irreducible.

2. **Available programmes for the investigation of finite** groups. Our programme X for the calculation of characters and representations of a given finite group G makes use of the data determined by a programme Φ for the investigation of the lattice of subgroups and of certain other properties of G. The input for the system of programmes consisting of Φ and X is a set of generators of G given in one of the following ways:

(2.1) (a) as permutations,
(b) as matrices over the rational field $\boldsymbol{R}$,
(c) as matrices over $\boldsymbol{Z}_p$,
(d) as matrices over $\boldsymbol{R(5)}$ where ζ is a fixed root of unity,
(e) as three-dimensional affine transformations considered modulo certain translations,
(f) for soluble groups as abstract generators with a special kind of defining relations **[8]**.

From these generators the programme Φ determines G. For all subgroups of G their characteristic numbers (as described in [3]) are stored: all cyclic subgroups of prime-power order are numbered $Z_1, \ldots, Z_n$. Then each subgroup $U \leqslant$ G is uniquely represented by the n-bit binary number k(U) whose ith bit is 1 if and only if $Z_i \leqslant U$.

Some of the lists obtained by Φ are preserved for further calculations. The programme Xmakes use of a list L_1 of all elements in the same form as the given generators, a list L_2 of all subgroups, and a list L_3 of all classes of subgroups conjugate in G.

L_2 contains :
(2.2) for each subgroup $U \leqslant G$:
(a) the characteristic number k(U),
(b) the number of an element in L_1 which transformes U into a fixed representative $\bar{U}$ of the class of subgroups conjugate to Uin G;
(2.3) for each cyclic subgroup $U \leqslant$ G the number in L_1 of a fixed generating element $u \in U$.

L3 contains :
(2.4) for each subgroup $\bar{U}$ chosen as representative of its class of conjugate subgroups :
(a) its order $|\bar{U}|$,
(b) the number in L_2 of its normalizer $N_G(\bar{U})$,
(c) the number in L_2 of its centralizer $C_G(\bar{U})$,
(d) one bit each to characterize if $\bar{U}$ is cyclic, abelian, nilpotent, supersoluble, soluble, perfect, normal, subnormal or selfnormalizing.

Of the characteristic subgroups determined by Φ only G' is needed by X. Only for the use in X two further lists are computed. They contain:
(2.5) for each class C_i, $1 \leqslant i \leqslant r$;
(a) the number of a fixed representative g_i in L_1,
(b) the number of elements in C_i,
(c) the order of the elements in C_i;
(2.6) for each element g $\in$ G the number of the class containing g.

The class of all elements conjugate to g $\in$ G is obtained by transforming g with representatives of the cosets of $C_G(g) = C_G(\langle g \rangle)$ in G. Since $x^{-1}g^ix = (x^{-1}gx)^i$, it is sufficient to do this for the elements chosen in (2.3).

3. One-dimensional representations.

3.1. For a one-dimensional representation τ of G we have G' $\leqslant$ ker τ. Hence τ induces a mapping τ' : G/G'-C given by

$$\tau'(G'g) = \mathrm{z(g)} \text{ for all } \mathrm{g} \in \mathrm{G}. \tag{3.1.1}$$

Let $\boldsymbol{H} = G/G'$ be of order $\boldsymbol{H} = p_1^{e_1} \ldots p_t^{e_t}$; then $\boldsymbol{H}$ is the direct product of its Sylow subgroups $S_{p_1}, \ldots, S_{p_t}$ of orders $p_i^{e_i}$, $1 \leqslant \boldsymbol{i} \leqslant t$. S_{p_i} is a direct product of cyclic groups of orders ***pf'***, . . . , $p_i^{e_{is_i}}$ with $e_{i1} + \ldots + e_{is_i} = e_i$. Let $\boldsymbol{m} = s_1 + \ldots + s_t$ and let $x_1, \ldots, x_m$ be generators of the cyclic direct factors of $\boldsymbol{H}$ thus obtained. For each τ' the values $\tau'(x_j)$ form an m-tuple $(w_1, \ldots, w_m)$ with $w_j \in$ C and $w_j^{|x_j|} = 1$. Conversely all the $\boldsymbol{H}|$ such m-tuples are different one-dimensional representations of $\boldsymbol{H}$ in C.

3.2. Let G' be in the layer (cf. [3]) Σ_r, let $S_{p_i}^*/G'$ be the p_i-Sylow subgroup of G/G'. Then $S_{p_i}^*$ is found in Σ_{e_i+r} by searching for a subgroup which contains G' and is of order $p_i^{e_i}|G'|$. The programme finds a decomposition of $S_{p_i}^*/G'$ into cyclic direct factors in the following way :

If $S_{p_i}^*/G'$ is not cyclic, a normal subgroup U with G' $\leqslant U \leqslant S_{p_i}^*$ and ***U/G'*** cyclic is searched for in Σ_{r+1} which has an $S_{p_i}^*$-complement $\boldsymbol{V}$ modulo G' in Σ_{r+e_i-1}. If no such normal subgroup U is found in Σ_{r+1} the search for U is continued in Σ_{r+2} with $\boldsymbol{V}$ in Σ_{r+e_i-2}.

If U and $\boldsymbol{V}$ have been found, U is stored away as a direct factor of $S_{p_i}^*/G'$, $S_{p_i}^*$ is replaced by $\boldsymbol{V}$ and the same process is continued. If G is abelian, L_3 yields the information whether U = ***U/G'*** is cyclic, otherwise we use that ***U/G'*** is a cyclic p-group if and only if there is exactly one maximal subgroup of U containing G'. All these decisions require only calculations with characteristic numbers, so this part of X is very fast.

3.3. Let ε be a fixed primitive nth root of unity. Let the classes of a cyclic group U = (x) of order n be $C_i = \{x^{i-1}\}$; then the one-dimensional representations can be numbered in such a way that

$$\tau_j(C_i) = \varepsilon^{(i-1)\cdot(j-1)}, \quad 1 \leqslant i, j \leqslant n. \tag{3.3.1}$$

Let the elements of the direct product ***UX V*** of two abelian groups U and $\boldsymbol{V}$ with elements $u_1 = 1, u_2, \ldots, u_n$ and $v_1 = 1, v_2, \ldots, v_m$ resp. be ordered into the sequence $u_1v_1, u_2v_1, \ldots, u_nv_m$. Then a table for U ***X V*** corresponding to (3.3.1) is obtained as the Kronecker product of the tables for U and ***V.*** Such a "normed table" of one-dimensional representations is first determined by the programme X from the direct decomposition of G/G'. Then G is decomposed into cosets modulo G', and for each class C_i of elements conjugate in G the coset g_kG' containing C_i is found. The kth row of the "normed table" of G/G' then is assigned to C_i.

4. Irreducible representations of higher dimensions.

4.1. Factor groups with faithful irreducible representations. A representation $\boldsymbol{T}$ of G is faithful on $G/$ker ***(T).*** Those factor groups of G with faithful irreducible representations can be found by applying a theorem of Gaschütz [5]. For this we give two definitions:

(4.1.1) The *socle* S(H) of a group His the product of ail minimal normal subgroups of H;

(4.1.2) a normal subgroup of a group H is called ***monogenic***, if it is generated by one class of elements conjugate in ***H***

(4.1.3) THEOREM. ***A finite group H has a faithful irreducible representation if and only if its socle S(H) is monogenic.***

In the programme this theorem is used in the following way: If Ng is transformed into ***Nh*** by Nx $\in G/N$, then $x^{-1}gxh^{-1} \in N$. Hence to check if $S(G/N)$ is monogenic means checking if the subgroup S $\trianglelefteq$ G with S/N = $S(G/N)$ is generated by N and one class of elements conjugate in G. In preparation for this all monogenic normal subgroups M_i, $1 \leqslant i \leqslant s \leqslant r$, of G are determined. Then for all N $\triangleleft$ G, N $\in \Sigma_i$, $0 \leqslant i \leqslant t-2$, where Σ_t = {G}, the minimal normal subgroups K_j/N of G/N are found by searching for normal subgroups $K_j \geqslant$ N minimal with respect to this property. $S(G/N)$ is then equal to S/N where S is the product of all these K_j. $S(G/N)$ is monogenic if for some M_i ***we*** have S = NM_i.

4.2. Induced representations. Let $U \leqslant$ G and ***M*** be a C&right-module of dimension s, ***T*** be the matrix representation afforded (uniquely up to equivalence) by ***M*** and let ψ be its character. The tensor product

$$M^G = M \otimes_{CU} CG \tag{4.2.1}$$

is a CG-right-module called the module induced from ***M.*** Let T^G be the matrix representation afforded by M^G, ψ^G its character, $(\psi^G)_U$ the restriction of ψ^G to U. T^G can be described as follows. Let

$$\mathrm{G} = Ug_1 \cup Ug_2 \cup \,.\,.\cup Ug_t,\ t = G:U \text{ and } g_1 = 1, \tag{4.2.2}$$

be a decomposition of G into cosets of ***U.*** Then, for a suitable choice of the basis of M^G, T”(g) is a $t\, X\, t$ matrix of $s \times s$ blocks for all g $\in$ G. The block (i, j) is equal to $T^*(g_igg_j^{-1})$ where

$$T^*(x) = \begin{cases} T(x) \text{ for } x \in U \\ 0 \text{ otherwise.} \end{cases} \tag{4.2.3}$$

If ***T*** is one-dimensional, T^G is monomial and

$$T^G_{ij}(g) = T^*(g_igg_j^{-1}). \tag{4.2.4}$$

Then

$$\psi^G(g) = \sum_{i=1}^{t} T^G_{ii}(g) = \sum_{i=1}^{t} T^*(g_igg_i^{-1}) \tag{4.2.5}$$

As a character is a class function, it is sufficient to calculate (4.2.5) for representatives g $\in$ G of the classes of elements conjugate in G.

4.3. *M-groups.*

(4.3.1) A finite group is called an ***M-group*** if all its irreducible representations are monomial.

As each irreducible monomial representation is induced ([2] Cor. 50.4), all irreducible representations of such groups are obtained as induced representations. In order to find M-groups among the factor groups we use a sufficient criterion of Huppert [6]:

(4.3.2) THEOREM. ***Let H have a soluble normal subgroup K with all Sylow subgroups** abelian **such that** H/K **is supersoluble, then His an M-group.***

We also use the following remark from [6] :

***(4.3.3) A finite group H has a uniquely determined normal subgroup U(H) which is minimal with respect to the property that its factor-group is supersoluble. For K ◁ G we have** $U(H/K) = U(H)K/K$.*

The programme first determines *U(G).* If G is supersoluble then *U(G)* = (1). Otherwise we use another theorem of Huppert [7]:

(4.3.4) THEOREM. *A finite **group H is supersoluble if and only** if all **its maximal subgroups have prime index.***

So *U(G)* is found by searching through all layers Σ_i, $i = 0(1)t-1$, for the first normal subgroup such that all maximal subgroups of G containing it have prime index. For a factor group G/N, which has a faithful irreducible representation, $U(G)N$ is formed. In order to decide whether G/N is an M-group $U(G)N/N$ has to be checked for the following properties :

(1) Is $U(G)N/N$ soluble?

As $U(G)N/N \cong U(G)/U(G) \cap$ N this can be decided in the following way:

(a) If *U(G)* is soluble, the same holds for $U(G)N/N$. Solubility of a subgroup of G is marked in L_3.

(b) If *U(G)* is insoluble, but N soluble, $U(G)N/N$ is insoluble.

(c) Only if *U(G)* and N are both insoluble, the programme has to check if the derived series of $U(G)N$ terminates below N.

(2) Are all Sylow subgroups of $U(G)N/N$ abelian?

If all Sylow subgroups of *U(G)* are marked as abelian in L_3, this is the case. Otherwise the programme described in § 3.2 is used to find the Sylow subgroups of $U(G)N/N$ and it is checked if their commutator subgroups are contained in N.

As the property of being an M-group is inherited by factor groups, the checking of (1) and (2) is started with Σ_0.

4.4. Induced monomial representations. We now describe how a subgroup *V* can be found whose one-dimensional representations yield irreducible representations of a fixed factor group G/N by the process of induction. The choice of U is restricted by a theorem of It8 ([2] Cor. 53.18):

(4.4.1) THEOREM. ***The dimension of an irreducible representation of a group H is a divisor of the index of each** abelian **normal subgroup A of H.***

We call the greatest common divisor of the indices of the maximal abelian normal subgroups of ***H*** the It&index ***i(H).*** By (4.4.1) we have to find a subgroup $U \geqslant$ N such that G: $U \mid i(G/N)$. In order to determine $i(G/N)$ we search for K_i a G with N a K_i, K_i/N abelian, and maximal with respect to these properties. Then $i(G/N)$ is calculated from the orders of the K_i listed in L_3.

We also use $\sum_{i=1} d_i^2 = |\,G\,|$. As there are $|G/G'|$ one-dimensional representations, only ***r*** $-$ $|G/G'|$ representations of dimensions $\geqslant 2$ are missing. For their dimensions we have:

$$\sum_{i=|G/G'|+1}^{r} d_i^2 = |\,G\,| - |\,G/G'\,|.$$

Hence $2 \leqslant G : U \leqslant \sqrt{|G| - |G/G'| - 4(r - |G/G'| - 1)}$ is a restriction for the index of U.

Finally we can restrict the search for U to representatives of the classes of subgroups conjugate under G, as conjugate subgroups yield equivalent representations.

The kernel ***V*** a U of the one-dimensional representation ***T*** of U used for the induction process must satisfy the requirements

$$U/V \text{ cyclic,} \tag{4.4.2}$$

$$\text{N} = \ker\ T^G = \bigcap_{g \in G} V^g. \tag{4.4.3}$$

The programme X deals with all factor groups G/N with faithful irreducible representations in turn. If G/N cannot be recognized as an M-group by (4.3.2), the user of the programme is informed that possibly not all irreducible representations of G/N will be found. In spite of this, the programme tries to find irreducible monomial representations of G/N.

First, the programme searches for subgroups $U \in \Sigma_s$, $s \leqslant t-1$, such that N a U and G : U is a dimension allowed by the restrictions. Then subgroups $V \in \Sigma_i$, $i \leqslant$ s- 1, ***V*** a U are searched for, which satisfy (4.4.2) and (4.4.3). This is done in the following way: if ***V*** a G then also ***V*** a ***U.*** Otherwise the normalizer $N_G(V)$ is determined from L_2 and L_3. If $U \leqslant$ ***No(V) we*** have ***V*** a ***U. U/V*** is cyclic if and only if for each prime $p \mid$ ***U/V*** there is exactly one maximal subgroup of index ***p*** in U, containing ***V.*** If ***V*** a **G we must** have ***V*** = N, otherwise the intersection of all conjugates of ***V*** in G is formed and this must be equal to N. If ***V*** is found, meeting all requirements, N, U and ***V*** are listed.

For the determination of faithful one-dimensional representations of U/V we have to find an element x $\in U$ with (x, ***V)*** = ***U.*** This is found as a generator of a cyclic subgroup Z of G meeting the following requirements :

$Z \leq U$, $Z \not\leq V$ and $ZV \not\leq M_i$ for all maximal subgroups M_i of U containing V.

The whole process described in § 4.4 needs only calculations with characteristic numbers and hence is rather fast.

4.5. A test for irreducibility. We use the inner product of characters

$$(\psi, \chi) = \frac{1}{|G|} \sum_{g \in G} \psi(g)\overline{\chi}(g) \qquad (4.5.1)$$

to check the irreducibility of T^G. By a special case of Frobenius' reciprocity theorem ([2], 38.8), for any character ψ of a subgroup $U \leq G$ ***we have:***

$$((\psi^G)_U, \psi) = (\psi^G, \psi^G). \qquad (4.5.2)$$

Since a character χ of a representation of G is irreducible if and only if $(\chi, \chi) = 1$, we have:

ψ^G ***is irreducible if and only*** *if*

$$((\psi^G)_U, \psi) = \frac{1}{|U|} \sum_{u \in U} \psi^G(u)\overline{\psi}(u) = 1. \qquad (4.5.3)$$

Let e be the exponent of G. Then the values of ψ^G, and hence $|U| \cdot ((\psi^G)_U, y)$, are sums of eth roots of unity, i.e. sums of powers of a fixed primitive eth root of unity, ε say.

For the calculation of the sum (4.5.2) we count in a list ***L*** the number n_j of times ε^j, $0 \leq j \leq$ e $-$ 1, occurs as a summand of $|U| \cdot ((\psi^G)_U$, y). We then use the fact that a sum of nth roots of unity is equal to zero if and only if it can be decomposed into sums over cosets of nontrivial subgroups of the group of al lnth roots of unity ([9], p. 240). Because of this theorem the programme proceeds as follows : for each divisor ***d*** of e and each ***i, 0*** $\leq$ ***i*** $\leq$ ***d-*** 1, the smallest of the numbers n_i, n_{d+i}, n_{2d+i}, . . . is subtracted from all these numbers. ψ^G is irreducible if and only if, after doing this, $n_0 =$ U| and n_i = Oforalli, $1 \leq i \leq e-1$.

4.6. The calculation of induced representations. The programme deals in turn with the triplets *N*, *U*, *V* previously found. First G is decomposed into cosets of ***U***, then for each faithful one-dimensional representation T_i of ***U/V*** the calculation is performed in four steps:

(1) T_i is calculated in the **same** way as described in § 3.3 for the one-dimensional representations of G.

(2) The character-values $\chi_i^{(j)}$ of the induced representations T_j^G are calculated for representatives of the classes of elements conjugate in G.

(3) The irreducibility of T_j^G is tested by the method described in § 4.5.

(4) If T_j^G passes the test, the values of $\chi_i^{(j)}$ are brought into a normal form by a method analogous to that described in § 4.5, and are compared with the list of irreducible characters previously obtained in order to decide if T_j^G is a new irreducible representation.

If required the kernel of T_j^G, the matrices representing generators or all elements of G in T_j^G, are computed and printed. The programme stops as soon as r irreducible representations have been found. This often happens long before all triplets N, U, V have been investigated.

4.7. In debugging the programme we have used the special version (2.1 d) of the programme Φ to generate a matrix group from the images of the generators of G under an irreducible representation $\boldsymbol{T}$. This must be isomorphic to $G/\ker \boldsymbol{T}$.

5. The numerical part of the programme.

5.1. The part of the programme described so far finds only the monomial irreducible representations and characters. For low orders there are very few groups having non-monomial irreducible representations. Up to order 96 there are one of order 24, four of order 48, one of order 60 and two of order 72. No method is included yet in our programme for the determination of non-monomial irreducible representations, but at least an attempt is made to complete the character table by a more numerical part of the programme. For its description we define:

$$w_i^{(s)} = \frac{h_i}{d_s}\chi_i^{(s)}, \quad 1 \leqslant i, s \leqslant r. \tag{5.1.1}$$

Then from [2], p. 235,

$$w_i^{(s)}w_j^{(s)} = \sum_{k=1}^{r} c_{ijk}w_k^{(s)}, \quad 1 \leqslant i, j, s \leqslant r, \tag{5.1.2}$$

we have

$$\sum_{k=1}^{r} (c_{ijk} - \delta_{ik}w_j^{(s)})w_k^{(s)} = 0, \tag{5.1.3}$$

i.e. for each s the r values $w_I^{(s)}$, $1 \leqslant I \leqslant r$; belonging to the sth character satisfy the r^2 equations

$$\sum_{k=1}^{r} (c_{ijk} - \delta_{ik}x_j)x_k = 0, \quad 1 \leqslant \boldsymbol{i}, \boldsymbol{j} \leqslant \boldsymbol{r}. \tag{5.1.4}$$

To solve this system we choose a fixed j = j_0 and consider only the r equations

$$\sum_{k=1}^{r} (c_{ij_0k} - \delta_{ik}x_{j_0})x_k = 0, \quad 1 \leqslant \boldsymbol{i} \leqslant r. \tag{5.1.5}$$

Then for each s, $1 \leqslant s \leqslant r$; the vector $(w_1^{(s)}, \ldots, w_r^{(s)})$ is an eigenvector of the matrix (c_{ij_0k}) belonging to the eigenvalue $w_{j_0}^{(s)}$. If for some j_0 this matrix has r different eigenvalues, the eigenvectors are essentially uniquely determined and hence must coincide up to a factor with the vectors $(w_1^{(s)}, \ldots, w_r^{(s)})$, $1 \leqslant s \leqslant r$. This factor is calculated from

$$w_1^{(s)} = \frac{h_1}{d_s}\chi_1^{(s)} = 1.$$

From [2], 31.18,

$$d_s^2 \sum_{i=1}^{r} \frac{w_i^{(s)} w_i^{(s)}}{h_i} = |G|, \tag{5.1.6}$$

we obtain the dimensions $d_1, \ldots, d_r$ and hence the values $\chi_i^{(s)}$.

In our programme we use the characters already obtained by the process of induction to reduce the task of finding the eigenvalues of the (c_{ijk}) as roots of the characteristic polynomials.

5.2. For the numerical programme we first compute the structure constants c_{ijk}. Let $x_1, \ldots, x_r$ be representatives of the r classes of elements conjugate in G. Then for all $k = 1(1)r$ and all $b \in C_i$ the number of solutions of $bx = x_k$ in C_j is counted.

For each matrix (c_{ijk}), $2 \leqslant j \leqslant r$, its characteristic polynomial is computed by the Hessenberg procedure [12]. Zeros of this polynomial belonging to known characters are split off and the zeros of the remaining polynomial are computed by the Bairstow procedure. For a simple root of this polynomial a character is found as an eigenvector.

The numerical method described above does not work if there is a non-monomial character $\chi^{(s)}$ such that for each j there exists s' $\neq s$ with $\chi_j^{(s)} = \chi_j^{(s')}$. This case has not yet been covered in our programme, but we intend to replace the numerical part by a method proposed by John D. Dixon† which makes use of the fact that the vectors $\mathbf{w}^{(s)}$, $1 \leqslant s \leqslant r$, are essentially uniquely determined as common eigenvectors of all matrices (c_{ijk}), $1 \leqslant j \leqslant r$. An outline of this method in included in the survey [10].

6. Experience **with the programme.** The programme has been run for all groups contained in [11] and for several other examples, e.g. it has been used in the investigation of finite groups of 4×4 integral matrices. Typical running times for the programmeX(which is implemented on an Electrologica Xl with 20K core-store of 27 bits each and an addition-time of 64 μsec) are the following:

For the symmetric group on 4 symbols 6 sec, for a certain group of order 72 with 24 classes 2 min 10 sec, for another group of order 72 with 6 classes 37 sec, for a group of order 88 with 55 classes 1 min 45 sec.

REFERENCES

1. C. Brott: Ein Programm zur Bestimmung absolut irreduzibler Charaktere und Darstellungen endlicher Gruppen. Diplomarbeit, Kiel, 1966.
2. C. W. Curtis and I. Reiner: *Representation Theory of Finite Groups and Associative Algebras (New* York, 1962).
3. V. Felsch and J. Neubüser: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. *Mitt. Rh.- W. Inst. f. Znstr. Math., Bonn 2* (1963), 39-74.

† High-speed computation of characters. Mimeographed manuscript, Sydney, 1967.

4. V. FELSCH and J. NEUBÜSER : Über ein Programm zur Berechnung der Automorphismengruppe einer endlichen Gruppe. *Numer. Math.* 11 (1968), 277-292.
5. W. GASCHÜTZ: Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen. *Math. Nachr.* 11 (1954), 129-133.
6. B. HUPPERT: Monomiale Darstellungen endlicher Gruppen. *Nagoya* Math. *J.* 6 (1953), 93-94.
7. B. HUPPERT: Normalteiler und maximale Untergruppen endlicher Gruppen. Math. *Zeit. 60* (1954), 409-434.
8. W. LINDENBERG: Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten. *Numer. Math. 4 (1962),* 151-153.
9. G. A. MILLER, H. F. BLICHFELDT and L. E. DICKSON: ***Theory and Applications of Finite Groups*** *(New* York, 1938).
10. J. NEUBÜSER: The investigation of finite groups on computers. These Proceedings, pp. 1-19.
11. J. NEUBÜSER: Die Untergruppenverbände der Gruppen der Ordnungen $\leqslant 100$ mit Ausnahme der Ordnungen 64 und 96. Habilitationsschrift, Kiel, 1967.
12. J. H. WILKINSON: Stability of the reduction of a matrix to almost triangular and triangular forms by elementary similarity transformations. J. ***Assoc. Comp. Much.*** 6 (1959), 336-359.

The characters of the Weyl group E_8

J. S. Frame

1. Introduction. The group F of order $192 \cdot 10! = 2^{14}3^5 5^2 7 = 696{,}729{,}600$ whose 112 absolutely irreducible characters (all rational) are described in this paper is isomorphic to the Weyl group *Es*. The group F itself is described by Coxeter **[1]** as the &dimensional group $3^{[4,2,1]}$ of symmetries of Gosset's semi-regular polytope 4_{21}, and it is the largest of the irreducible finite groups generated by reflections. Its factor group A = F/C with respect to its center C = $\{I, -I\}$ is the orthogonal group of half the order investigated by Hamill [7] as a collineation group and by Edge [2] as the group A of automorphisms of the non-singular quadric consisting of 135 points of a finite projective space [7]. The simple group denoted $FH(8, 2)$ by Dickson is a subgroup $A+$ of index 2 in $A = F/C$.

The 8-dimensional orthogonal representation of F, called 8, below, contains a monomial subgroup M of order $2^7 8$!, consisting of the products of 8 ! permutation matrices by 2^7 involutory diagonal matrices of determinant 1. There are 64 right cosets of M in the double coset *MRM* of *M* generated by the involution *R:*

$$R = \begin{bmatrix} I_4 - E & - \quad E \\ - \quad E & I_4 - E \end{bmatrix} \quad \text{where } E = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = E^2 \qquad (1.1)$$

Here I_4 is the 4×4 identity matrix. Each matrix in *MRM* has 7 entries $\pm 1/4$, and one entry $\pm 3/4$ in each row and column, and the product of the entries in any row or column is negative. The remaining 70 right cosets of M in F lie in the double coset *MQM* where

$$Q = RR' = \begin{bmatrix} I-E & -E \\ -E & I-E \end{bmatrix} \begin{bmatrix} I-E & E \\ E & I-E \end{bmatrix} = \begin{bmatrix} I-2E & 0 \\ 0 & I-2E \end{bmatrix} \quad (1.2)$$

For each row or column of a matrix in *MQM* there are four entries 0 and four entries $\pm$ 1/2 and the product of the four signs has a common value for the eight rows, and a common value for the eight columns.

If the signs in row 8 and then in column 8 of all the 8 ! permutation matrices of Mare changed, the resulting group isomorphic with S_8 can be combined with the matrix R of (1. 1), acting in the role of the transposition (8 9), to produce a subgroup S of F of index 1920 isomorphic to the symmetric group S_9.

We denote the 112 irreducible characters of F by their degrees marked with a subscript x, y, z, or w to indicate one of four types. The symbols 700, and 700_{xx} denote two different characters of degree 700 and type x. The 67 characters of F that are irreducible characters of F/C include 27 associated pairs classified as type x, and 13 self-associated characters classified as type y. The remaining 45 faithful characters of F include 20 associated pairs classified as type z and 5 self-associated characters of type w. Pairs of associated characters are equal for elements of the even subgroups F^+ of $For A+$ of A, and have opposite signs in the odd coset of F^+ of $A+$, while self-associated characters vanish in these odd cosets.

We also classify the classes into four types a, b, c, d as follows. Of the 40 classes of elements of A in A^+, the 25 classes C_a of type a split into pairs of classes C_a and $-C_a$ in Fin which an element of F^+ is not conjugate to its negative, whereas 15 classes C_b of type b do not split in F. Of the remaining 27 classes of A in the odd coset of A^+, 20 classes C_c split into pairs C_c and $-C_c$ in F with elements not conjugate to their negatives, and 7 classes C_d of A do not split in F. This classification enables us to partition the 112 x 112 character table as follows.

(1.3)

Character blocks of A			No.
X_a	X_a	Y_a	25
X_b	X_b	Y_b	15
X_c	$-X_e$	0	20
X_d	$-X_d$	0	7

$27 + 27 + 13 = 67$

Class type	No.	Character blocks of F					
C_a	25	**25**	X_a	X_a	Y_a	Z_a	Z_a	W_a
$-C_a$	255	X_a	X_a	Y_a	I-z.	$-Z_a$	$-W_a$
C_b	15	X_b	X_b	Y_b	0	0	0
C_c	20	X_c	$-X_c$	0	$\boxed{Z_c}$	$-Z_c$	0
$-C_c$	200	X_c	$-X_{--}$	0	$-Z_c$	Z_c	0
C_d	7	X_d	$-X_d$	0	0	0	0

$112 = 27 + 27 + 13 + 20 + 20 + 5$

All the 112 x 112 entries of the character table may thus be displayed in four square blocks totaling $40^2 + 27^2 + 25^2 + 20^2 = 3354$ entries, of which the first two blocks describe characters of type x or y of A in its even and odd classes, and the last two describe the faithful characters of F of types z and w in its even and odd classes. To check orthogonality by rows in these subtables all products involving x's or Z's must be doubled in forming scalar products.

All the faithful irreducible characters of F of type z and w are found among the irreducible constituents of the odd Kronecker powers of the fundamental character 8_z, whereas the characters of F/C of types x and y are constituents of even Kronecker powers. To each partition (λ) of m corresponds a Schur character $\{\lambda\}$ which is irreducible for the general linear group *GL* (8, C) containing a Murnaghan character $[\lambda]$ which is irreducible for the infinite g-dimensional real orthogonal group G **[9]**. For m = 1, 2, 3, 4, all these characters except [4] are also irreducible for the finite subgroup *F* of G, but for $m > 4$ many are reducible for *F* and must be split by other means.

2. The classes. The class symbol $1^\alpha\, 2^\beta\, 3^\gamma \dots$, where $8 = \alpha + 2\beta + 3\gamma + \dots$, is commonly used to describe a class of permutations having a 1-cycles, β 2-cycles, γ 3-cycles, etc. We extend it to other classes of the monomial group M by denoting by $\bar{k}$ or $k^{-1}(2k)$ a k-cycle with an odd number of minus signs, whose eigenvalues are those (2k)th roots of unity which are not kth roots of unity. Similarly the symbol $1^\alpha\, 2^\beta\, 3^\gamma \dots$, where $8 = \alpha + 2\beta + 3\gamma + \dots$, in which one or more of the exponents is negative, denotes a class of matrices in 8, whose eigenvalues consist of a 1's, plus β pairs 1 and − 1, plus γ complete sets of cube roots of unity, etc., and a symbol $\bar{k}$ is equivalent to $k^{-1}(2k)$. Thus 10/2, or 2 $4^{-1}(10)^{-1}(20)$, denotes a class of elements of order 20 whose eigenvalues are the eight primitive 20th roots of unity that are not 10th roots nor 4th roots of unity.

For a matrix in the representation 8, some power of which is an involution of trace 0 and type 2^4, these symbols do not specify the class uniquely. One class, denoted 2^4v, contains diagonal monomial matrices of type $1^4\,\bar{1}^4$ and also permutation matrices of M with four 2-cycles and no negative signs. These each commute with $2^{13}3^3$ elements of A, and correspond to class 3 (called $1^{-1}2^4v$) in H_0. This class is not represented in the symmetric subgroup S_9. Another class, denoted 2^4u or $\bar{2}\, 2^3$, contains elements of type $1\, 2^4$ in S_9, but these are represented in M by four 2-cycles one of which has both its signs changed. Type $1^2\, \bar{1}^2 2^2$ of M also contributes to class 2^4u in A. Each element commutes with $2^{11}3$ elements of A. The letters v or u follow the class symbols for matrices some power of which is in class 2^4v or 2^4u. We also use v and u to distinguish the class $2^2 4v$ that contains permutations in M from the class $2^2 4u$ which represents permutations of S_9 whose image in M has two minus signs in one 2-cycle. Thus the classes containing the squares, cubes, or other powers of any element of $\boldsymbol{F}$ can be read directly from the class symbol.

We obtain the 67 classes of $A = F/C$ directly by using the classes of two important subgroups of index 120 and 135 and then finding 8-dimensional matrices that represent the missing nine classes, rather than by using the geometrical arguments of Hamill [7] and Edge [2]. Of the 67 classes of *A*, 25 even classes (type *a)* and 20 odd classes (type c) split in *F* to produce two classes each, whereas 15 even classes (type b) and 7 odd classes (type d) represent single classes of *F*.

(1) A subgroup *H* of index 120 in *A* is isomorphic to the Weyl group of type E_7, which is the direct product of its center C = {*I*, -Z} and the group

H_0 of order $2^9 3^4 5 \cdot 7$ whose 30 classes and characters were described by Frame [4]. The 60 classes of H are labeled $1, 1', 2, 2', \ldots, 30, 30'$, so that class k' contains the product by $-I$ of an element of class k. There are 46 classes of A containing elements of H. For the 12 classes of A that split in H the corresponding classes of *Hand* the values of the induced permutation character 120, are:

(2.1)

A	H	120, I	A	H	120,	A	H	120,
$1^4 2^2$	2, 16	30+2	$1^6 2$	1′, 16′	1+63	$1^2 \bar{1} 2 \bar{3}$	7′, 8′	1-i-3
$1^2 2\ 4$	5, 18, 19	6+1+1	$1^2 2^3$	2′, 3′, 17′	3+1+12	$2\ 3^2$	9′, 22′	1+3
$1\ 2^2 3$	8, 21	6+2	$1^2 2\ 2^{-2}$	4′, 28′	1+3	$1^2 6$	10′, 23′	1+3
1223	24, 27	1+1	132 3	6′, 21′	1+15	125	15′, 25′	1+3

(2) Twelve additional classes of A that are not represented in H but are represented in the monomial subgroup $M' = M/C$ of $A = F/C$ are denoted by the symbols

$$1\ \bar{2}^2\ 3,\ 4^2 u,\ \bar{2}^4,\ \bar{4}^2,\ 1\ \mathrm{i}\ 3\ \bar{3}v,\ \bar{2}\ \bar{6}v,\ 1\ 3\ 4,\ 1\ \bar{2}\ \bar{5},\ \bar{2}\ 3\ \bar{3}v,\ \bar{2}^2 4,\ 1\ \mathrm{i}\ 6,\ 8u. \tag{2.2}$$

(3) Five of the remaining nine classes of A contain 8 X 8 real orthogonal symplectic matrices that commute with a skew matrix of type $\bar{2}^4$ and order 4 that we call "i". By appropriate choice of "i" the 8 X 8 orthogonal matrices are equivalent to 4×4 unitary matrices $A+ iB$ under the correspondence

$$i - \begin{bmatrix} 0 & z \\ -z & 0 \end{bmatrix}_1, \quad A+iB \rightarrow \begin{bmatrix} A & B \\ -B & 1 \end{bmatrix} \tag{2.3}$$

The $2^{10} 3^2 5$ matrices of this type form the normalizer N_i of i, which has a monomial subgroup M_i of order $2^7 4!$ and index 15. In six cosets of M_i the matrices have exactly 2 zero entries per row or column. In the other eight cosets there are no zero entries.

The classes of type $12/4$, its square $\bar{6}^2/\bar{2}^2$, and fourth power $\bar{3}^4/\bar{1}^4$ are represented by the following unitary matrices of orders 24, 12, 6 in F, or 12, 6 and 3 in A. Roman numerals indicate Hamill's class symbols [7].

$$\frac{1}{2}\begin{bmatrix} 1-i & 0 & 0 & 1-i \\ -1+i & 0 & 0 & 1-i \\ 0 & 1-i & -1+i & 0 \\ 0 & 1-\ddot{i} & 1-i & 0 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} -i & -i & -i & -i \\ i & -i & -i & i \\ i & i & -i & -i \\ i & -i & i & -i \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}$$

Type $12/\bar{4}$ (LXVII) — Type $\bar{6}^2/\bar{2}^2$ (LXVI) — Type $\bar{3}^4/\bar{1}^4$ (LVI)

(2.4)

Type $\bar{10}/\bar{2}$ and its square $\bar{5}^2/\bar{1}^2$ belong to classes of elements of orders 20 and 10 in F, or 10 and 5 in $A = F/C$. Representative 4×4 unitary matrices $A + iB$ for these classes are

$$\frac{1}{2}\begin{bmatrix} 0 & 1+i & 0 & 1-i \\ 1-i & 0 & 1+i & 0 \\ -1+i & 0 & 1+i & 0 \\ 0 & 1+i & 0 & -1+i \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} 1 & 1 & i & i \\ -1 & 1 & i & -i \\ -1 & -1 & i & i \\ 1 & -1 & i & -i \end{bmatrix}. \tag{2.5}$$

Type $\bar{1}0/\bar{2}$ (LXIV) Type $\bar{5}^2/\bar{1}^2$ (LX)

(4) The four remaining classes are Miss Hamill's classes LVII, LVIII, LIX, and LXV [7], here denoted $6^2/2^2v$, $9/1$, $\bar{3}^2\ 6/1^2\ 2$, and $1\ 3^{-1}\ 5^{-1}\ 15$ respectively, and represented by the orthogonal matrices

$$\frac{1}{4}\begin{bmatrix} 1 & -1 & 3 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 3 & -1 & -1 & -1 \\ -1 & 1 & I & 3 & 1 & 1 & 1 & 1 \\ -3 & -1 & -1 & 1 & -1 & -1 & -1 & -1 \\ -1 & -3 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 3 \\ 1 & -1 & -1 & 1 & -1 & 3 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 3 & -1 \end{bmatrix}, \quad \frac{1}{4}\begin{bmatrix} -1 & -3 & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & -3 & I & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -3 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -3 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 & -3 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 & & -3 & -1 \\ -1 & 1 & 1 & 1 & 1 & 1 & 1 & 3 \\ 3 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \end{bmatrix}, \tag{2.6}$$

Type $6^2/2^2v$ (LVII) Type $9/1$ (LVIII)

$$\frac{1}{4}\begin{bmatrix} 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ -1 & -1 & -1 & 3 & -1 & -1 & -1 & -1 \\ 3 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -2 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & o & -1 & -1 & -1 & 0 & 1 \\ 1 & -1 & -1 & 0 & 0 & o & -1 & 0 \\ 0 & 0 & O & -1 & -1 & 1 & o & -1 \\ 0 & 0 & 0 & 1 & -1 & -1 & o & -1 \\ 0 & 0 & o & -1 & 1 & -1 & o & -1 \\ 1 & -1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Type $\bar{3}^2\ \bar{6}/\bar{1}^2\ \bar{2}$ (LIX) Type $1\ 3^{-1}\ 5^{-1}\ 15$ (LXV)

Type $\bar{9}/\bar{1}$ is the negative of a 9-cycle of S_9, represented in F by the negative of the product of R in (1 .1) by an 8-cycle permutation matrix of M in which the signs are changed to negative in the last row and column. The negative of a matrix of type $13^{-1}\ 5^{-1}\ 15$ represents an element of order 30 in F whose 5th power is of type $\bar{3}^4/\bar{1}^4$.

3. The decomposition of Kronecker powers. If the cycle symbols $\bar{k}$ in a class symbol are replaced by $k^{-1}(2k)$, then the first, second, third, fourth, . . . powers of an element in class 1" $2^{\beta}\, 3^{\gamma}\, 4^{\delta}$. . . have the character values

$$\text{a}, \alpha+2\beta, \alpha+3\gamma, \alpha+2\beta+4\delta, \ldots \tag{3.1}$$

in the 8-dimensional orthogonal representation 8, of ***F***. Using the formulas worked out by Murnaghan [9], the character 8_z^m of the mth Kronecker powers of 8, may be split into characters $[\lambda]$, one for each partition (λ) of ***m***, which are irreducible for the full S-dimensional orthogonal group O_8. This is a substantial refinement of the Schur decomposition which yields characters irreducible for the full linear group. Constituents of odd powers of 8_z, including the first power 8, itself, will be classified as type z (pairs of associated characters) or type w (self-associated characters which vanish in the odd coset of A $^+$ or ***F*** $^+$). For ***m*** = 0, 1, 2, 3, 4, all but one of these Murnaghan characters are irreducible for the subgroup ***F*** of O_8. We denote them by their degrees with subscripts, and express their values in terms of a, β, γ, 6,. . . asfollows

$$[0] = 1, = \text{I} \tag{3.2}$$

$$[1] = 8, = \text{a}$$

$$[1^2] = 28, =_{0}\overset{\alpha}{2} -\beta$$

$$[2] = 35, = (\alpha+2)(\alpha-1)/2+\beta$$

$$[1^3] = 56, \underset{\boldsymbol{0}}{=}\overset{\alpha}{3}-\alpha\beta+\gamma$$

$$[2\ 1]= 160, = (\alpha+2)\ \alpha(\alpha-2)/3-\gamma$$

$$[3] = 112_z = (\alpha+4)\ \boldsymbol{a(a\text{-}}\ 1)/6+\alpha\beta+\gamma$$

$$[1^4] = 70_y = \binom{\alpha}{4}-\binom{\alpha}{2}\beta+\binom{\beta}{2}+\alpha\gamma-\delta$$

$$[2\ 1^2]= 350, = (\alpha+2)\ \alpha(\alpha-1)(\alpha-3)/8-(\alpha+2)(\alpha-1)\beta/2\binom{\beta}{2}+\delta$$

$$[2^2] = \boldsymbol{300,} = (\alpha+2)(\alpha+1)\ \alpha(\alpha-3)/12+\beta(\beta-1)-\alpha\gamma+\alpha\beta$$

$$[3\ 1] = 567, = (\alpha+4)(\alpha+1)(\alpha-1)(\alpha-2)/8 + \binom{\alpha}{2}\beta-\binom{\beta+1}{2}-\delta$$

$$[4] = 210_x+84_x = (\alpha+6)(\alpha+1)\ \alpha(\alpha-1)/24+\binom{\alpha+1}{2}\beta+\binom{\beta}{2}+\alpha\gamma+\delta$$

The first eleven of these characters are found to be irreducible for ***F*** by summing their squares over the group. It is clear that [4] cannot be irreducible for ***F***, since its degree 294 = 2.3.7^2 does not divide the group order

$|F|$. We shall see presently how to split this character by using permutation characters induced from the subgroups $\boldsymbol{H}$ and M.

It is probably simpler not to use all these formulas explicitly, but to calculate 8_z, 28, and 160, by these formulas, and then express the rest by Kronecker products as follows.

$$\begin{aligned}
&\text{In } [2]: && 35, = 8_z^2 - 1_x - 28_x \\
&\text{In } [1^3]: && 56, = 8_z(28_x - 1_x) - 160, \\
&\text{In } [3]: && 112, = 8_z(35_x - 1_x) - 160, \\
&\text{In } [2\ 1^2]: && 350, = 28_x^{[1^2]} - 28_x \\
&\text{In } [1^4]: && 70, = 8_z(56_z) \quad 350, \quad 28, \\
&\text{In } [2^2]: && 300, = 8_z(160_z) - 28_x(35_x) \\
&\text{In } [3\ 1]: && 567, = 35_x(28_x - 1_x) - 28_x - 350_x \\
&\text{In } [4]: && 210_x + 84_x = 8_z(112_z) - 35_x - 567_x
\end{aligned} \tag{3.3}$$

Several irreducible components of the Kronecker 5th power of 8, can be split off in like manner as follows. Here the irreducible character $56_z'$ **is** the associate of 56_z, with values of opposite sign in the odd classes of types c and *d.*

$$\begin{aligned}
&\text{In } [1^5]: && 56_z' \text{ is associate of } 56, \\
&\text{In } [2\ 1^3]: && 448, = 8_z(70_y) - 56_z - 56_z' \\
&\text{In } [2^2 1]: && 840, = 56_z(28_x + 1_x) - 8_z(28_x + 70_y) \\
&\text{In } [3\ 1^2]: && 1296_z = 160_z(28_x) - 8_z(35_x + 300_x + 70_y) + 56_z' \\
&\text{In } [3\ 2]: && 1400, = 8_z(300_x) - 160_z - 840, \\
&\text{In } [4\ 1]: && 1008, = 8_z(210_x - 84_x) \\
&\text{In } [5]: && 560, = 8_z(84_x) - 112,
\end{aligned} \tag{3.4}$$

Before the characters [4], [4 1], and [5] of O_8 can be split in F, it is necessary to obtain the character 84_x. Note first that the difference of the symmetrized Kronecker squares of the characters 56, and 28, splits into two characters, one the associate $350_x'$ of the known character 350_x, and the other a new character of degree 840:

$$840, = 56_z^{[2]} - 28_x^{[2]} - 350_x'. \tag{3.5}$$

4. **Induced permutation characters.** Three permutation characters of A, denoted 120_p, 135_p, and 960, respectively, are induced by the subgroups of A index 120, 135, and 960, called H, M, and S above. Both $\boldsymbol{H}$ and $\boldsymbol{M}$ have exactly three double cosets in $\boldsymbol{A}$, containing $1 + 56 + 63$ cosets of $\boldsymbol{H}$, or $1 + 64 + 70$ cosets of $\boldsymbol{M}$ respectively. Hence by a theorem of Frame [3] these permutation characters each split into the 1-character 1_x and a

pair of characters of degrees f_1, f_2 or f_3, f_4 such that

$$120(56)(63)/f_1f_2 \text{ is a square, and } f_1+f_2 = 119, \qquad \textbf{(4.1)}$$

$$135(64)(70)/f_3f_4 \text{ is a square, and } f_3+f_4 = 134.$$

The unique positive integral solutions of these equations are

$$f_1,\ f_2 = 35 \text{ and } 84 \text{ in } 120_p, \qquad (4.2)$$

$$f_3,\ f_4 = 50 \text{ and } 84 \text{ in } 135,. \qquad (4.3)$$

It is easily verified that 120, contains the character 35, already computed, so

$$84, = 120_p - 1_x - 35_x, \qquad (4.4)$$

$$50, = 135_p - 120_p + 35,. \qquad (4.5)$$

It can be checked that 84, is also a constituent of the character 960, induced by the symmetric subgroup S = S_9. Hence the character $960_p - 1_x -$ 84, of degree 875 splits into two irreducible constituents whose degrees divide $2^{13}\ 3^5\ 5^2\ 7$. The splitting into 175, and 700, is verified when it is found that this character has a constituent in common with the Murnaghan character [6] of degree 1386 for the orthogonal group O_8, which splits as follows into three known constituents and one new constituent 700,:

$$[6] = 700_x + 567_x + 84_x + 35_x. \qquad (4.6)$$

The other constituent 175, of 960, is

$$175, = 960_p - 1_x - 84_x - 700_x. \qquad (4.7)$$

To check this character 175_x, we note that it splits in H into the sum of the two characters $105_b + 70'_a$. Thus its values for the 46 classes of A in ***H*** can be computed directly from these subgroup characters without evaluating [6]. Both degrees 175 and 700 are divisible by 5^2 and 7, so the characters 175, and 700, both vanish for the 11 classes of elements whose orders are divisible by 5 or 7. Thus it may be easier to determine 175, first for most classes, and then find 700, from (4.7) rather than from (4.6).

Having the additional characters 84_x, 50_x, 175, and 700_x, we can now compute several more characters of types x and y quite simply as follows:

$$1400, = 28_x(50_x) \qquad (4.8)$$

$$1050, = 35_x(50_x) - 700,$$

$$1575, = 28_x(84_x) - 567_x - 210_x = 8_z(560_z) - 35_x(84_x - 1_x)$$

$$1344, = 35_x(84_x) - 8_z(112_z) - 700_x$$

$$2100, = 28_x(210_x - 84_x) - 84_x - 1344,$$

$$2268, = 35_x(210_x - 84_x) - 567_x - 1575,$$

$$525, = 84_x^{[1^2]} - 567_x - 1050_x - 1344,$$

$$700_{xx} = 50_x^{[1^2]} - 525_x$$

$$4200, = 28_x(\ 175,) - 700_{xx}.$$

The symbol 700_{xx} denotes a second character of type x and degree 700, distinct from 700,. Other new characters are defined by

$$\begin{aligned} 972, &= 50_x(84_x) - 50_x - 84_x - 1050, - 1344, - 700_{xx} \qquad (4.9)\\ 4096, &= (35_x - 1_x)(300_x - 28_x) - 840_x - 700_x - 1344_x - 2268_x. \end{aligned}$$

The character 972, of degree $2^2 3^5$ is of highest type modulo 3, so it must vanish in all 3-singular classes.

By decomposing Kronecker products involving characters of relatively small degree such as 70_y, 50_x, 84_x, 28, and 35, we can now solve for ten more of the 13 self-associated characters of type y as follows :

$$\begin{aligned} 1134_y &= 70_y(28_x) - 70, - (28, + 28'_x) - (350, + 350'_x) \qquad (4.10)\\ 1680, &= 70_y(35_x) - 70_y - (350_x + 350'_x)\\ &= 70_y(84_x) - (2100_x + 2100'_x)\\ 168, &= 50_x^{[2]} - 50_x \quad 84_x - 972_x\\ 420_y &= 70_y(70_y + 1_x) - 28_x(28_x + 28'_x) - (840_x + 840'_x) - 1134_y - 168_y\\ 3150, &= 28_x(168_y) - 1134_y - 420_y\\ 4200, &= 35_x(\,168,) - (840_x + 840;)\\ 2688, &= 28_x(420_y - 168,) \quad 168, \quad 4200,\\ 2100_y &= 50_x(168_y - 1_x - 1'_x) - (700_{xx} + 700'_{xx}) - (972_x + 972'_x) - 168_y - 2688_y\\ 1400, &= 50_x(70_x) - 2100,\\ 4536, &= 28_x(525_x) - 300_x - 700_x - 1400_x - 2268_x - 4096_x - 1400,. \end{aligned}$$

5. **Kronecker products with the character** 8_z. Products of the character 8, with any constituent of an even (odd) Kronecker power will split into constituents of powers of the opposite parity. By splitting products of 8, with the even-power constituents of types x and y already found we can complete the list of irreducible characters of types z and w as follows. We start with a second character 1400, of type z and degree 1400, not to be confused with 1400, already obtained.

$$\begin{aligned} 1400_{zz} &= 8_z(175_x) \qquad (5.1)\\ 4200, &= 8_z(700_{xx} - 175,)\\ 400, &= 8_z(50_x)\\ 3240, &= 8_z(700_x - 50_x) - 1400, - 560,\\ 4536, &= 8_z(972_x) \quad 3240,\\ 2400, &= 56_z(84_x) - 1296, - 1008,\\ 3360, &= 8_z(1400_x - 525_x - 50_x) - 3240_z\\ 2800, &= 56_z(50_x)\\ 4096, &= 8_z(\,1575,) - 56_z(84_x) - 560, - 3240,\\ 5600, &= 8_z(2268_x - 525_x) - 1008_z - 3240_z - 2800_z\\ 448, &= 8_z(1344_x - 1575_x) + 1296_z - 1400_z + 2400_z \end{aligned}$$

TABLE *1. Three permutation characters in*

Class symbols		$A \vert / \vert C_k \vert$	$120_,$	$135_,$	$960_,$
		Type *a* classes			
I	1^8	$2^{13}3^5 5^2 7$	120	135	960
III	$1^4 2^2$	$2^{11}3^2 5$	32	31	96
XI	$1^2 2\ 4$	$2^7 3$	8	7	8
x v	$1^4 \bar{2}^2$	$2^{10}3^2$	12	3	—
XXXVII	$1^2 \bar{2}\ \bar{4}$	2^6	2	1	—
IV	153	$2^7 3^5 5$	36	27	72
XIV	$1^4 \bar{1}\ \bar{3}v$	$2^7 3^3$	12	3	—
IX	$1\ 2^2 3$	$2^6 3^2$	8	7	12
XXVII	1223	$2^4 3$	2	1	2
XXXII	$I\ \bar{2}^2 3v$	$2^5 3^2$	—	3	—
X	$1^2 3^2$	$2^4 3^4$	6	9	12
XXVI	$1^2 \bar{3}^2$	$2^4 3^2$	2	1	—
XL	$1^2 9/3$	2 33	3	—	—
LVIII	$9/\bar{1}$	33	—	—	3
XXXVIII	$\bar{3}^3/\bar{1}$	$2^4 3^5$	3	—	24
XL1	$1\ 3\ \bar{3}^2/\bar{1}^2$	$2^4 3^3$	3	—	—
XLII	$1\ 3\ \bar{6}/\bar{2}$	$2^3 3^2$	3	—	—
LVI	$\bar{3}^4/\bar{1}^4$	$2^6 3^5 5$	—	—	—
LIX	$\bar{3}^2 \bar{6}/\bar{1}^2 \bar{2}$	$2^4 3^2$	—	—	—
XII	$1^3 5$	$2^3 3 5^2$	10	5	5
XXIX	$1^2\ \bar{1}\ \bar{5}$	23 5	2	1	1
XXX	3 5	2 3 5	1	2	2
LX	$\bar{5}^2/\bar{1}^2$	$2^2 3 5^2$	—	—	—
LXV	1·15/3·5	3 5	—	—	—
XXXIV	1 7	2 7	1	2	1
		Type *d* classes			
XXIII	$2^2 4v$	$2^9 3^2$	12	19	—
XVIII	$2^2 4u$	2^8	4	3	8
LIII	$\bar{2}^2 4$	$2^8 3$		7	—
XLVI	$\bar{2}\ 3\ 3v$	$2^3 3^2$	—	1	—
LIV	$1\ \bar{1}\ \bar{6}$	$2^3 3$	—	1	—
LV	$8v$	2^6	2	5	—
XLVIII	$8u$	2 4	—	1	2

$$
\begin{aligned}
448, &= 8_z(70_x) - 56_z - 56: \\
1344, &= 8_z(840_x) - 840_z - 4536_z \\
5600_w &= 8_z(1134_y) - 840_z - 840'_z - 448_w - 1344_w \\
2016, &= 8_z(420_y) - 1344, \\
7168, &= 8_z(2688_x) - 3360_z - 3360'_z - 5600_w - 2016_w
\end{aligned} \tag{5.2}
$$

***the 67 classes of A** = F/C*

		Type *b* classes			
Class	symbols	$\|A\|/\|C_k\|$	120,	135,	960,
XIII	24v	$2^{13}3^3$	24	39	—
XXXVI	4^2v	2^{10}	4	11	—
VIII	2^4u	$2^{11}3$	8	7	16
XXVIII	4%	27	—	3	4
xxxv	1124	2^6	2	1	—
LXI	$\bar{2}^4$	$2^{10}3^25$	—	15	—
LXII	$\bar{4}^2$	2^63	—	3	—
XXXI	$1\ \bar{1}\ 3\ \bar{3}$	2^33^3	—	3	—
xXx1x	$2\ 6v$	2^43^3	6	9	—
XXXIII	$2\ 6u$	2^43	2	1	4
LXIII	26	2^33^2	—	3	—
LVII	$6^2/2^2v$	2^63^3	—	—	—
LXVI	$\bar{6}^2/\bar{2}^2$	2^53^2	—	—	
LXVII	$(\overline{12})/\bar{4}$	2^33	—	—	—
LXIV	$(\overline{10})/\bar{2}$	2” 5		—	—
		Type c classes			
II	1^62	$2^{10}3^457$	64	63	288
V	1^22^3	$2^{10}3^2$	16	15	32
XXI	$1^22\ \bar{2}^2$	2^83	4	3	—
VII	144	$2^93\ 5$	20	11	16
xxv	$1^3\bar{1}\ 4$	2^63	6	1	—
VI	132 3	2^53^35	16	15	30
XVI	$1^2\bar{1}\ 2\ 3$	2^53^2	4	3	2
XXIV	$1^3\bar{2}\ 3$	2^53^2	6	1	—
XXIX	1 3 4	2^53	2	5	4
XLVII	1 3 4	2^33	—	1	—
XVII	$2\ 3^2$	2^33^3	4	3	6
XXII	1^26	2^33^2	4	3	2
LI	$2\ 9/3$	$2\ 3^2$	1	—	—
XLIX	$2\ \bar{3}^3/\bar{1}^3$	2^43^4	1	—	—
L	$6\ \bar{3}/\bar{1}$	2^43^2	1	—	8
LII	$2\ 3\ \bar{6}/\bar{1}\ 2$	2^33	1	—	—
xx	1 2 5	$2^23\ 5$	4	3	3
XLIV	$1\ \bar{2}\ \bar{5}$	2^25	—	1	1
XLIII	$2\ 3\ \bar{5}/\bar{1}^2$	23 5	1	—	—
XLV	$2\ \bar{7}/\bar{1}$	2 7	1	—	1

6. Blocks of defect one. The Brauer theory of modular characters, used to determine several of the characters of the subgroup H_0 of $\boldsymbol{A}[4]$, can be applied in like manner to find some new characters and check some of those already computed. In a block of defect one (mod ***p*)**, where p^a but not p^{a+1} divides the group order, the characters have degrees divisible by p^{a-1} but not by p^a. Since all characters of $\boldsymbol{A}$ and $\boldsymbol{F}$ are rational, there

Table 2. ***The $X_{ab}Y_{ab}$ block for even classes of A^+***

1^8	$2^{13}3^5 5^2 7$	1,	28,	35,	84,	50_x	350.	300,	567,	210,	840_x
$1^4 2^2$	$2^{11}3^2 5$	1	4	11	20	10	-10	20	39	26	24
$1^4 24$	$2^7 3$	1	0	3	4	2	-2	0	-1	2	0
$1^4\bar{2}^2$	$2^{10}3^2$	1	8	7	4	-2	26	8	15	6	16
$1^2\bar{2}\bar{4}$	2^6	1	2	1	0	0	0	-2	-1	0	0
153	$2^7 3^5 5$	1	10	14	21	5	35	30	81	39	-24
$1^2\bar{1}\bar{3}v$	$2^7 3^3$	1	2	6	5	-3	-5	6	9	7	8
$12^2 3$	$2^6 3^2$	1	-2	2	5	1	-1	2	-3	-1	0
1223	$2^4 3$	1	0	0	1	-1		1	0	-1-1	0
$1\bar{2}^2 3v$	$2^5 3^2$	1	2	-2	1	1	-1	2	-3	3	4
$1^2 3^2$	$2^4 3^4$	1	1	2	3	5	-1	-6	0	3	3
123”	$2^4 3^2$	1	1	2	-1	1	-1	2	0	-1	3
$1^2 9/3$	2 33	1	1	2	0	-1	-1	0	0	0	0
$\bar{9}/\bar{1}$	33	1	1	-1	0	-1	-1	0	0	0	0
$\bar{3}^3/\bar{1}$	$2^4 3^5$	1	1	-1	3	-4	-1	3	0	-6	3
$13\bar{3}^2/\bar{1}^2$	$2^4 3^3$	1	5	3	-1	0	7	3	0	-2	-1
$13\bar{6}/\bar{2}$	$2^3 3^2$	1	-1	1	1	-2	-1	-1	0	0	1
$\bar{3}^4/\bar{1}^4$	$2^6 3^5 5$	1	10	5	-6	5	35	30	0	-15	30
$\bar{3}^2\bar{6}/\bar{1}^2\bar{2}$	$2^4 3^2$	1	2	1	-2	1	-1	2	0	-3	-2
135	$2^3 3 5^2$	13	5		4	0	0	0		7	5-5
$1^2\bar{1}\bar{5}$	23 5	1	-1	1	0	0	0	0	-1	1	-1
3 5	2 35	1	0	-1	1		0	0	0	1-1	1
$\bar{5}^2/\bar{1}^2$	$2^2 3 5^2$	1	3	0	-1	0	0	0	-3	0	0
1·15/3·5	3 5	10		o-1	0	0	0		0	0	0
1 7	2 7	10		0	0	1	o-1		0	0	0
2%	$2^{13}3^3$	1	-4	3	20	18	-2	12	-9	-14	8
$4^2 v$	2^{10}	1	o	-1	4	6	2	0	-1	-2	0
$2^4 u$	$2^{11}3$	1	-4	3	4	2	-2	12	-9	2	8
$4^2 u$	2^7	1	0	-1	0	2	2	0	-1	2	0
$1\bar{1}2\bar{4}$	2^6	1	-2	1	0	0	0	2	-1	0	0
$\bar{2}^4$	$2^{10}3^2 5$	1	4	-5	4	10	-10	20	-9	10	-40
$\bar{4}^2$	$2^6 3$	1	0	-1	0	2	-2	0	3	-2	0
$1\bar{1}3\bar{3}v$	$2^3 3^3$	1	-1	0	-1	3	1	0	0	1	-1
26v	$2^4 3^3$	1	-1	0	5	3	1	0	0	-5	-1
$26u$	$2^4 3$	1	-1	0	1	-1	1	0	0	-1	-1
26	$2^3 3^2$	1	1	-2	1	1	-1	2	0	1	-1
$6^2/2^2 v$	$2^6 3^3$	1	2	-3	2	-3	-5	6	0	1	-10
$\bar{6}^2/\bar{2}^2$	$2^5 3^2$	1	-2	1	-2	1	-1	2	0	1	2
$(1\bar{2})/\bar{4}$	$2^3 3$	1	0	-1	0	-1	1	0	0	1	0
$(\overline{10})/\bar{2}$	2^2 5	1	-1	0	-1	0	0	0	1	0	0

TABLE 2 *(continued)*

700,	175,	1400,	1050,	1575,	1344,	2100,	2268,	525,	700,	I
60	15	40	50	15	***64***	-60	12	5	20	III
4	-1	0	2	-1	***0***	-4	-4	-3	0	XI
-4	-1	-16	-10	11	***0***	12	-12	-7	0	xv
0	-1	0	0	1	***0***	0	0	-1	-2	XXXVII
55	-5	50	15	90	84	75	81	30	-20	IV
−1	-5	-6	-17	-6	4	-5	9	6	-4	XIV
3	3	-2	-1	-6	4	3	-3	2	-4	IX
1	-1	0	-1	2	0	-1	-1	0	cl	XXVII
-1	-1	2	-1	2	0	3	-3	2	0	XXXII
4	4	5	6	0	-6	3	0	3	7	x
0	0	1	2	0	-2	3	0	-1	-1	XXVI
-2	1	-1	0	0	0	0	0	0	1	XL
1	1	-1	0	0	0	0	0	0	1	LVIII
7	13	-4	-3	9	−6	-6	0	12	-2	XXXVIII
-1	1	0	1	-3	-2	-2	0	0	2	XL1
-1	-1	2	-1	-1	0	0	0	2	0	XL11
10	-5	50	15	-45	-24	-60	0	30	-20	LVI
2	-1	2	-1	-1	0	0	0	2	0	LIX
0	0	0	0	0	-1	0	-2	0	0	XII
0	0	0	0	0	-1	0	2	0	0	XXIX
0	0	0	0	0	-1	0	1	0	0	xxx
0	0	0	0	0	4	0	3	0	0	LX
0	0	0	0	0	1	0	0	0	0	LXV
0	0	0	0	0	0	0	0	0	0	XXXIV
-4	-17	-72	58	-57	64	52	-36	45	92	XIII
-4-1		0	-2	3	0	-4	4	1	8	XXXVI
12	-1	-8	-6	-9	0	4	12	-19	-4	VIII
0	3	0	-2	-1	0	0	0	1	0	XXVIII
0	-1	0	0	1	0	0	0	-1	2	xxxv
-20	15	40	-30	15	0	20	-36	5	20	LX1
0	-1	0	-2	-1	0	0	0	-3	0	LX11
2	-2	-3	-2	0	-2	1	0	3	−1	xxx1
-4	-2	-3	4	0	4	1	0	3	-1	xXx1x
0	2	1	0	0	0	1	0	-1	−1	XXXIII
−2	0	1	0	0	0	-1	0	-1	−1	LX111
2	-5	-6	7	3	-8	4	0	6	-4	LVII
-2	3	-2	3	3	0	-4	0	2	-4	LXVI
0	-1	0	1	-1	0	0	0	0	0	LXVII
0	0	0	0	0	0	0	-1	0	0	LXIV

[continued on pp. 124, 125]

Table 2 (continued)

1^8	$2^{13}3^55^27$	972,	4096,	4200,	2240,	2835,	6075,	3200,	70_y	1134,	1680_y
1^42^2	$2^{11}3^25$	36	0	40	64	51	-45	0	-10	-18	-80
1^224	2^73	0	0	0	0	-5	3	0	-2	6	0
$1^4\bar{2}^2$	$2^{10}3^2$	0	0	-8	0	3	-9	0	14	30	32
$1^2\bar{2}\bar{4}$	2^6	2	0	0	0	-1	1	0	2	-2	0
1^53	2^73^55	0	64	-30	-4	-81	0	-40	10	0	60
$1^4\bar{1}\bar{3}v$	2^73^3	0	0	-6	-4	-9	0	8	-6	0	-20
12^23	2^63^2	0	0	-2	4	3	0	0	2	0	4
1225	2^43	0	0	0	0	1	0	0	-2	0	0
$1\bar{2}^23v$	2^53^2	0	0	-2	0	3	0	0	2	0	-4
1^23^2	2^43^4	0	-8	-3	2	0	0	-4	4	0	6
$1^2\bar{3}^2$	2^43^2	0	0	1	-2	0	0	0	-4	0	−2
$1^29/3$	2 33	0	1	0	2	0	0	-1	-2	0	0
$\bar{9}/\bar{1}$	33	0	1	0	-1	0	0	-1	1	0	0
$\bar{3}^3/\bar{1}$	2^43^5	0	-8	15	−10	0	0	14	-2	0	6
$13\bar{3}^2/\bar{1}^2$	2^43^3	0	0	3	2	0	0	2	6	0	-2
$13\bar{6}/\bar{2}$	2^33^2	0	0	1	0	0	0	0	2	0	2
$\bar{3}^4/\bar{1}^4$	2^63^55	0	64	-30	-40	0	0	-40	19	81	6
$\bar{3}^2\bar{6}/\bar{1}^2\bar{2}$	2^43^2	0	0	-2	0	0	0	0	-1	-3	2
1^35	2^335^2	-3	-4	0	-5	5	0	0	0	-6	0
$3\bar{5}$	23 5	1	0	0	-1	1	0	0	0	2	0
$\bar{5}^2/\bar{1}^2$	2^235[illegible]	0	-1	0	1	-1	0	0	0	0	0
		-3	-4	0	0	0	0	0	5	4	-5
$1\cdot15/3\cdot5$	3 5	0	-1	0	0	0	0	0	-1	1	1
1 7	2 7	-1	1	0	0	0	-1	1	0	0	0
2^4v	$2^{13}3^3$	108	0	-24	-64	-45	27	128	6	-18	16
4%	2^{10}	8	0	-8	0	3	-1	0	-2	-2	0
2^4u	$2^{11}3$	12	0	8	0	3-21		0	6	-18	16
4^2u	2 7	0	0	0	0	-1	3	0	-2	-2	0
$1\bar{1}2\bar{4}$	2^6	-2	0	0	0	-1	1	0	2	-2	0
$\bar{2}^4$	$2^{10}3^25$	36	0	40	0	-45	-45	0	6	30	-16
$\bar{4}^2$	2^63	0	0	0	0	3	3	0	2	2	0
$1\bar{1}3\bar{3}v$	2^33^3	0	0	3	2	0	0	-4	0	0	-2
26v	2^43^3	0	0	3	-4	0	0	-4	0	0	-2
$26u$	2^43	0	0	-1	0	0	0	0	0	0	-2
26	2^33^2	0	0	1	0	0	0	0	0	0	2
$6^2/2^2v$	2^63^3	0	0	-6	8	0	0	8	3	9	-2
$\bar{6}^2/\bar{2}^2$	2^53^2	0	0	-2	0	0	0	0	3	-3	2
$(\bar{1}\bar{2})/\bar{4}$	2^33	0	0	0	0	0	0	0	-1	−1	0
$(1\bar{0})/\bar{2}$	2^2 5	1	0	0	0	0	0	0	1	0	−1

TABLE 2 *(continued)*

168,	420,	3150,	4200,	2688,	2100,	1400,	4536,	5670,	4480,	I
8	20	30	40	0	-60	-40	-72	-90	0	III
0	-4	-2	0	0	-4	0	0	6	0	XI
8	12	22	24	0	-20	-8	-24	6	0	xv
0	0	2	0	0	0	0	0	-2	0	XXXVII
-12	-30	-90	-120	-48	30	20	0	0	-80	IV
4	2	6	8	-16	14	4	0	0	16	XIV
-4	2	6	-8	0	6	-4	0	0	0	IX
0	2	-2	0	0	2	0	0	0	0	XXVII
-4	-6	-2	0	0	-2	4	0	0	0	xxx11
6	6	0	6	-12	12	8	0	0	4	x
2	2	0	-2	0	0	-4	0	0	0	XXVI
0	0	0	0	0	0	2	0	0	-2	XL
0	0	0	0	0	0	-1	0	0	1	LVIII
6	-12	18	-12	-12	-6	14	0	0	–20	XXXVIII
-2	-4	-6	-4	-4	2	-2	0	0	4	XL1
2	0	-2	0	0	-2	-2	0	0	0	XL11
15	24	45	15	60	30	65	81	-81	-44	LVI
-1	0	1	3	0	-2	1	-3	3	0	LIX
-2	0	0	0	8	0	0	6	0	0	XII
-2	0	0	0	0	0	0	-2	0	0	XXIX
-2	0	0	0	2	0	0	0	0	0	xxx
3	5	0	0	3	0	0	1	5	-5	LX
0	-1	0	0	0	0	0	1	-1	1	LXV
0	0	0	0	0	0	0	0	0	0	XXXIV
40	-28	-114	104	128	116	-8	-72	-90	128	XIII
8	-4	6	-8	0	-4	-8	8	6	0	XXXVI
8	4	-18	8	0	-12	24	24	6	0	VIII
0	4	-2	0	0	-4	0	0	-2	0	XXVIII
0	0	2	0	0	0	0	0	-2	0	xxxv
24	36	30	-40	64	20	40	-24	6	64	LX1
4	0	-2	-4	0	0	4	-4	-2	0	LXII
, 4	-4	0	2	2	2	-2	0	0	-2	xxx1
-2	2	0	2	-4	-4	4	0	0	4	XXXIX
2	-2	0	2	0	0	0	0	0	0	XXX111
0	0	0	2	-2	2	-2	0	0	-2	LX111
7	8	-3	-1	-4	-10	1	9	-9	4	LVII
3	0	-3	-1	4	2	1	-3	3	4	LXVI
1	0	1	-1	0	0	1	-1	1	0	LXVII
-1	1	0	0	-1	0	0	1	1	-1	LXIV

TABLE 3. *The X_{cd} character block for odd classes of A not in A^+*

1^8	1,	28,	35,	84_x	50_x	350_x	300_x	567_x	210_x	840_x	700_x	175_x	1400_x	1050_x	1575_x	1344_x	2100_x	2268_x	525_x	700_{xx}	972_x	4096_x	4200_x	2240_x	2835_x	6075_x	3200_x
$1^6 2$	1	14	21	42	20	70	90	189	84	84	210	35	280	210	315	336	210	378	105	70	162	512	420	336	189	405	160
$1^2 2^3$	1	-2	5	10	4	-10	10	-3	4	20	18	3	-8	2	-21	16	-14	-6	-7	-10	18	0	4	16	-3	-27	32
$1^2 2\ 2'$	1	2	1	2	0	2	-2	-3	0	4	2	-5	o	-2	7	0	-6	-6	-3	-6	6	0	-4	0	-3	9	0
144	1	6	9	10	0	10	10	29	16	-4	10	-5	0	-10	15	16	10	10	5	-10	-6	0	-20	-16	-19	-15	0
$1^3 \bar{1}\ 4$	1	0	3	2	-2	-4	0	1	2	0	-2	-1	0	-4	-3	O	-2	2	3	0	0	0	0	0	1	3	0
132 3	1	2	6	9	5	-5	0	9	9	-6	15	5	10	15	0	6	-15	-9	0	10	0	-16	0	6	9	0	-20
$1^2 \bar{1}\ 2\ \bar{3}$	1	-2	2	1	1	-1	4	-3	1	2	3	-3	-2	-1	o	-2	1	3	-4	2	0	0	4	-2	-3	0	-4
$1^3 \bar{2}\ 3$	1	4	4	1	-1	5	2	3	1	2	-3	1	-4	-1	0	-2	1	-3	-2	2	0	0	2	2	3	0	0
134	1	0	0	1	3	1	-2	-1	1	2	1	1	0	-1	o	-2	1	1	2	2	0	0	-2	2	-1	0	0
134	1	0	o	-1	1	-1	0	1	-1	0	1	-1	o	-1	0	0	1	-1	0	0	0	0	0	0	1	0	0
$2\ 3^2$	1	-1	0	3	-1	1	0	0	-3	3	0	2	1	0	0	0	3	0	3	-5	0	-4	3	0	0	o	-2
$1^2 6$	1	1	2	1	1	-1	-2	0	1	-1	0	0	1	2	o	-2	1	0	-1	-1	0	0	1	-2	0	0	2
$2\ 9/3$	1	-1	0	o	-1	1	0	0	0	0	0	-1	1	0	0	0	0	0	0	1	0	-1	0	0	0	0	1
$2\ \bar{3}^3/\bar{1}^3$	1	5	3	-3	2	7	9	O	-6	3	3	-1	10	3	-9	-6	-6	0	6	-2	0	8	-3	-6	0	0	-2
$6\ \bar{3}/\bar{1}$	1	1	-1	1	-2	-1	1	o	-2	-1	3	3	-2	-1	3	-2	-2	0	2	2	0	0	1	-2	0	0	2
$2\ \bar{3}\ \bar{6}/\bar{1}\ \bar{2}$	1	-1	1	-1	0	-1	1	0	0	1	-1	1	0	1	1	0	0	0	0	0	0	o	-1	0	0	0	0
125	1	-1	1	2	0	0	0	-1	-1	-1	0	0	0	0	0	1	o	-2	0	o	-1	2	0	1	-1	0	0
125	1	1	-1	0	0	0	o	-1	1	1	0	0	0	0	0	1	0	0	0	o	-1	0	o	-1	1	0	0
$2\ 3\ \bar{5}/\bar{1}^2$	1	2	1	-1	0	0	o	-1	-1	-1	0	0	0	0	0	1	0	1	0	0	0	-1	0	1	-1	0	0
$2\ \bar{7}/\bar{1}$	1	0	0	o	-1	o	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	-1	-1
$2^2 4v$	1	-2	1	10	8	2	2	-3	-8	-4	-6	-5	-16	14	-9	16	10	-6	13	14	18	0	-4	-16	-3	9	0
$2^2 4u$	1	-2	1	2	0	2	2	-3	0	-4	2	3	0	-2	-1	0	2	2	-3	-2	2	o	-4	0	5	1	0
$\bar{2}^2 4$	1	2	-3	2	4	-2	6	-3	4	-4	-6	3	8	-6	3	0	2	-6	1	2	6	0	4	0	-3	-3	0
$\bar{2}\ 3\ \bar{3}v$	1	1	-2	1	-1	-1	2	0	1	-1	0	-2	-1	2	o	-2	1	0	1	-1	0	o	-1	2	0	0	0
$1\ \bar{1}\ \bar{6}$	1	-1	o	-1	1	1	0	0	1	-1	0	0	-1	0	0	o	-1	0	1	-1	0	0	1	0	0	0	0
$8v$	1	0	-1	2	2	0	0	1	-2	o	-2	-1	0	0	1	0	-2	2	-1	0	0	0	0	0	1	-1	0
$8u$	1	0	-1	0	0	0	0	1	0	0	0	1	0	0	-1	0	0	o	-1	0	0	0	0	o	-1	1	0

TABLE 4. *The Z_a W_a character block for even classes of F^+.*

8	56	160	112	840	1296	1400	1008	560_z	1400_{zz}	4200	400	3240_z	4536_z	2400_z	3360	2800	4096	5600	448	448_w	1344_w	5600_w	2016_w	7168_w
4	-4	16	24	4	-24	60	24	56	60	20	40	84	60	-80	16	-40	0	-80	32	-32	32	-80	48	0
2	-2	0	4	2	-4	-2	-4	4	-2	2	4	2	-2	0	0	-4	0	0	0	0	0	8	-8	0
4	12	16	8	20	24	-4	8	8	-4	4	-8	-12	12	16	-16	-24	0	-16	0	32	32	16	16	0
2	2	0	o	-2	o	-2	0	o	-2	-2	0	2	2	0	0	0	0	0	0	0	0	0	0	0
5	11	34	31	21	81	95	90	74	– 25	-75	25	81	-81	60	-6	55	64	20	16	28	-60	-10	-90	-128
3	-3	6	9	3	-9	9	6	6	-15	3	-9	-9	9	-12	-18	9	0	12	0	-12	12	-6	-6	0
1	-1	-2	3	1	-3	3	-6	2	3	-7	1	-3	3	4	-2	-1	0	4	8	4	-4	-2	6	0
1	-1	0	-1	1	1	-1	-2	2	-1	1	-1	1	-1	0	0	1	0	0	0	0	o	-2	2	0
1	3	-2	-1	5	-3	-1	2	2	-1	1	1	-3	3	4	2	3	0	-4	0	-4	-4	-2	-2	0
2	2	-2	4	-6	O	-4	0	2	8	6	10	0	0	6	-6	10	-8	2	-2	4	12	-4	0	-8
2	-2	2	0	2	0	0	0	-2	0	-2	2	0	0	2	2	-2	0	2	-2	-4	4	-4	0	0
2	-1	1	1	0	0	-1	0	-1	2	o	-2	0	0	0	0	1	1	-1	1	-2	0	2	0	-2
1	1	-1	-1	0	0	1	0	1	1	o	-1	0	0	0	0	-1	-1	1	-1	-1	0	1	0	-1
1	-2	2	-4	-3	0	4	-9	7	13	-15	-4	0	0	3	-12	8	8	-11	-16	2	6	-2	-18	32
3	6	6	0	3	0	0	-3	-3	3	3	0	0	o	-3	0	0	0	3	0	6	-6	-6	-6	0
1	o	-2	2	-1	0	2	-1	-1	-1	1	-2	0	0	1	2	0	o	-1	0	2	2	-2	-2	0
4	16	20	-4	60	0	40	-36	-20	-20	-60	20	0	0	-60	60	80	-64	-20	– 16	44	60	100	36	-16
2	0	2	-2	-2	0	4	-2	-2	-2	2	2	0	0	2	-2	0	0	-2	0	-2	-2	2	2	0
3	1	5	7	-5	1	0	3	5	0	0	0	-5	-4	0	5	0	-4	0	-2	-2	-6	0	6	8
1	-1	-1	1	1	-1	0	1	-1	0	0	0	1	0	o	-1	0	0	0	-2	2	-2	0	2	0
0	1	-1	1	1	1	0	O	-1	0	0	0	1	-1	0	-1	o	-1	0	1	-2	0	0	0	2
2	4	O	-2	O	-6	0	2	0	0	0	0	O	-6	0	0	0	4	0	2	2	6	0	4	2
1	-1	O	-1	0	0	0	1	0	0	0	0	0	0	0	0	o	-1	0	1	1	0	o	-1	1
1	o	-1	0	0	1	0	0	0	0	0	1	-1	o	-1	0	0	1	0	0	0	0	0	0	0

TABLE 5. ***The Z_c character block for odd classes of F not in F^+.***

1^8	$2^{13}3^55^27$	8,	56,	160,	112,	840,	1296,	1400,	1008,	560,	1400_{sz}	4200,	400,	3240,	4536,	2400,	3360,	2800,	4096,	5600,	448,
1^62	$2^{10}3^45\ 7$	6	14	64	56	126	216	350	252	196	210	210	120	594	378	120	336	280	512	280	112
1^22^3	$2^{10}3^2$	2	-6	0	8	10	-24	10	-12	12	6	-26	8	6	30	-24	-16	-24	0	8	16
$1^22\ \bar{2}^2$	2^83	2	2	0	0	2	0	-6	-4	4	-10	-2	0	6	6	8	0	0	O	-8	0
144	$2^93\ 5$	4	4	16	16	4	16	20	24	24	-20	-20	0	- 4	- 2 0	O	-16	0	0	0	0
$1^3\bar{1}\ \bar{4}$	2^63	2	-2	0	4	-2	-4	2	0	0	2	2	-4	-2	2	0	0	4	0	0	0
$1^32\ 3$	2^53^35	3	-1	4	11	-9	-9	5	0	16	15	15	15	9	-9	0	6	−5	−16	−20	4
$1^2\bar{1}\ 2\ 3$	2^53^2	1	-3	0	1	5	-3	-1	0	0	-3	5	1	3	-3	0	-2	3	0	4	-4
$1^3\bar{2}\ 3$	2^53^2	3	3	6	3	3	3	-3	0	0	3	3	-3	-3	3	0	o	-3	0	0	0
1 3 4	2^53	1	1	-2	1	1	1	-1	0	0	1	1	3	-1	1	0	-4	3	0	0	0
1 3 4	2^83	1	-1	0	-1	-1	1	1	0	0	-1	1	1	-1	1	0	o	-1	0	0	0
$2\ 3^2$	2^33^3	0	2	-2	2	0	0	2	o	-2	0	0	0	0	0	6	0	-2	-4	4	4
1^26	2^33^2	2	0	0	2	-2	0	-2	0	0	0	-2	2	0	0	0	2	0	0	2	-2
$2\ 9/3$	$2\ 3^2$	0	-1	1	-1	0	o	-1	0		10	0	0	0	0	0	0	1	-1	1	1
$2\ \bar{3}^3/\bar{1}^3$	2^43^4	3	4	8	-2	9	0	10	-9	−7	-3	-3	6	0	0	-3	6	8	-8	-1	-4
6 3/i	2^43^2	1	0	0	-2	-1	0	2	-3	3	3	-1	-2	0	0	3	-2	0	0	1	-4
2 3 b/I $\bar{2}$	2^33	1	-2	0	0	1	0	0	1	-1	1	-1	0	0	0	1	0	0	o	-1	0
1 2 5	$2^23\ 5$	1	-1	-1	1	1	1	0	-3	1	0	0	0	-1	-2	0	1	0	2	0	2
1 2 5	$2^2\ 5$	1	1	-1	-1	1	-1	0	1	1	0	0	0	-1	0	0	1	0	0	0	0
$2\ 3\ \bar{5}/\bar{1}^2$	2 3 5	2	1	1	-1	-1	-1	0	0	-1	0	0	0	1	- 1	0	-1	0	1	0	1
$2\ \bar{7}/\bar{1}$	2 7	1	o	-1	0	0		10	0	0	0	o	- 1	1	0	-1	0	0	-1	0	0

will be exactly p characters in a block of defect one (mod p). In our case, where the associated graph is a simple chain, consecutive characters share one common modular irreducible character, and combine to form a singular modular indecomposable character that vanishes in the so-called p-singular classes of elements whose orders are divisible by p. The sum of the p characters, taken with alternate signs, vanishes in the p-regular classes.

The group A has order $|A| = 2^{13}\, 3^5\, 5^2\, 7 = \frac{1}{2}|F|$, so the pertinent primes are 2, 3, 5, 7. For the prime 2, the pairs of associated characters 4096_x and $4096'_x$ form an indecomposable for A, so the characters vanish for all elements of even order in the even subgroup. A similar observation applies to the characters 4096_z and $4096'_z$. For the prime 3 we can calculate two new characters 2835_x and 5670_y whose degrees are divisible by $3^4 = 81$. Since the two characters 567_x and 2268_x agree in 3-singular classes of the even subgroup A^+, but have opposite signs in such classes of the odd coset, the associated character $567'_x$ belongs in the block with 2268_x. Their sum (in p-regular classes) defines a character 2835_x such that $567'_x+2835_x$ and 2835_x+2268_x vanish in the 3-singular classes. Similarly the characters 1134_y and 4536_y combine to produce 5670_y. We write

$$567'_x - \mathit{2835}_x + 2268_x \pmod 3 \tag{6.1}$$

$$1134_y - \mathit{5670}_y + 4536_y \pmod 3 \tag{6.2}$$

$$1296'_z - 4536_z + 3240_z \pmod 3 \tag{6.3}$$

to indicate the 3-blocks of defect one, using the last only as a check. Similarly for the prime 5, we find two new characters 2240_x and 4480_y and check others from the chains

$$35'_x - 840'_x + 2835_x - \mathit{2240}_x + 210_x \pmod 5 \tag{6.4}$$

$$70_y - 1680_y + 5670_y - \mathit{4480}_y + 420_y \pmod 5 \tag{6.5}$$

$$160'_z - 840'_z + 3360_z - 3240_z + 560_z \pmod 5. \tag{6.6}$$

Two Kronecker products with the character 175_x serve as checks:

$$35_x(175_x) = 1050_x + 2240_x + 2835_x \tag{6.7}$$

$$50_x(175_x) = 210_x + 1400_x + 2240_x + 420_y + 4480_y. \tag{6.8}$$

We calculate 6075_x from a Kronecker product:

$$6075_x = 8_z(2400_z) - 1575_x - 2100_x - 2100'_x - 1680_y - 5670_y \tag{6.9}$$

noting that its degree is $3^5 5^2$, so it must vanish in all the 3-singular and 5-singular classes. Finally we use it in a 7-chain to compute the last character 3200_x, and display a second 7-chain to check certain characters of type z.

$$1'_x - 300'_x + 4096'_x - 6075'_x + \mathit{3200}_x - 972_x + 50_x \pmod 7 \tag{6.10}$$

$$8'_z - 160'_z + 1296'_z - 2400'_z + 4096_z - 3240_z + 400_z \pmod 7 \tag{6.11}$$

Counting the associates of characters already computed, the list of 112 characters of the largest of the five Weyl groups G_2, F_4, E_6, E_7, and E_8 is now complete. In Table 1 we list symbols for the 67 classes of A, together with the orders of centralizers of an element, the class numeral used by Hamill [7], and Edge [2], and the characters of this class for the permutation representations induced by the subgroups H of index 120, A4 of index 135, and S of index 960. In F the centralizer orders must be doubled for classes of type a or c, and each odd cycle symbol k or $\bar{k}$ replaced by $\bar{k}$ or k to obtain the additional 45 classes of F. As explained above in (1.3) the information for the complete 112 x 112 character table is conveyed by four square blocks of dimensions 40 for $[X_{ab}, Y_{ab}]$, 27 for $[X_{cd}]$ which include the 67 characters of A, and 25 for $[Z_a, W_a]$, 20 for $[Z_c]$ which include the characters of faithful representations of F.

Reference should also be made to Dye's papers (10, **11**], which appeared after this paper was submitted.

REFERENCES

1. H. S. M. Coxeter: *Regular Polytopes* (Macmillan, 1963).
2. W. L. Edge: An orthogonal group of order $2^{13}.3^5.5^2.7$. *Annali di Matematica (4)* 61 (1963), 1-96.
3. J. S. Frame: The degrees of the irreducible representation s of simply transitive permutation groups. *Duke Math. Journal 3* (1937), 8-17.
4. J. S. Frame: The classes and representations of the groups of 27 lines and 28 bitangents. *Annali di Matematica (4) 32* (1951), 83-169.
5. J. S. Frame: An irreducible representation extracted from two permutation groups. *Annals of Math. 55* (1952), 85–100.
6. J. S. Frame: The constructive reduction of finite group representations. *Proc. of Symposia in Pure Math. (Amer. Math. Soc.) 6* (1962), 89-99.
7. C. M. Hamill: A collineation group of order $2^{13}.3^5.5^2.7$. *Proc. London Math. Soc.* (3) 3 (1953), 54-79.
8. T. Kondo:\ The characters of the Weyl group of type F_4. *J. Fac. Sci. Univ. Tokyo* 1 (1965), 145-153.
9. F. D. Murnaghan: *The Orthogonal and Symplectic Groups.* Comm. of the Dublin Inst. for Adv. Study, Ser. A, No. 13 (Dublin, 1958).
10. R. H. Dye: The simple group FH (8,2) of order 2^{12} 3^5 5^2 7 and the associated geometry of triality. *Proc. London Math. Soc. (3)* 18 (1968), 521-562.
11. R. H. Dye: The characters of a collineation group in seven dimensions. *J. London Math. Soc. 44* (1969), 169-174.

On some applications of group-theoretical programmes to the derivation of the crystal classes of R_4

R. BÜLOW AND J. NEUBÜSER

1. In mathematical crystallography symmetry properties of crystals are described by group-theoretical means [1, 7]. One considers groups of motions fixing a (point-)lattice. These groups can therefore be represented as groups of linear or affine transformations over the ring Z of integers. For such groups certain equivalence relations are introduced.

In particular two subgroups $\mathfrak{G}$ and $\mathfrak{H}$ of $GL_n(\mathbf{Z})$ are called geometrically equivalent, if there exists an integral nonsingular matrix X, such that $X^{-1}\mathfrak{G}X = \mathfrak{H}$. If, moreover, such X can be found with det $X = \pm 1$ (i.e. with X^{-1} integral, too), $\mathfrak{G}$ and $\mathfrak{H}$ are called arithmetically equivalent. The equivalence classes are called geometrical and arithmetical crystal classes respectively.

The lists of both geometrical and arithmetical crystal classes for dimensions $n = 1, 2, 3$ have been known for some time. In 1951 A. C. Hurley [5] published a list of the geometrical crystal classes for $n = 4$, which has since been slightly corrected [6].

2. In 1965 E. C. Dade [2] gave a complete list of representatives of the "maximal" arithmetical crystal classes, a problem which had also been considered by C. Hermann [4]. Dade's list consists of 9 groups:

group	order
Q_4	1152
Cu_4	384
$Sx_2 \otimes Cu_2$	96
$Sx_3 \otimes Cu_1$	96
Sx_4	240
$Sx_2^{(2)}$	288
$Py_3 \otimes Cu_1$	96
Py_4	240
$Sx_2^{\otimes 2}$	144

All crystal classes can be found by classifying the subgroups of these nine groups. Obviously subgroups conjugate in one of these groups are arithmetically and hence geometrically equivalent. Therefore it suffices to take one representative from each of the classes of conjugate subgroups of the nine groups and classify the set of subgroups of $GL_n(\mathbf{Z})$ thus obtained.

This has been done using a programme Φ [3] developed at the "Rechenzentrum der Universität Kiel" for the investigation of given finite groups by a computer.. This programme determines, for a finite subgroup $\mathfrak{G}$ of $GL_n(\mathbf{Z})$ given by a set of generating matrices, among other things the following :

1. a list of all elements of $\mathfrak{G}$,
2. the classes of elements conjugate in $\mathfrak{G}$,
3. the lattice of subgroups of $\mathfrak{G}$, where for a representative $\mathfrak{U}$ of each class of subgroups conjugate in $\mathfrak{G}$ the following information is given:

(a) generating elements of $\mathfrak{U}$,
(b) all maximal subgroups of $\mathfrak{U}$,
(c) for each class $\mathfrak{C}$ of elements conjugate in $\mathfrak{U}$ the number of elements in $\mathfrak{C}$ and their order, trace, and determinant.

The lattice of subgroups of the group Q_4 exceeded the capacity of the store of the machine at our disposal. For this group we first computed the classes of conjugate elements with the programme Φ. From these it is easily seen that the element $-E$ (where E = unit element) is contained in the intersection of the centre and the derived group and hence in the Frattini subgroup of Q_4. Hence -E is contained in all maximal subgroups of Q_4 and we found these by computing the lattice of subgroups of $Q_4/\langle - E)$ which could be handled in our machine. There are three maximal subgroups of order 576 normal in Q_4, two classes of three conjugate maximal subgroups each, of order 384 and one class of sixteen conjugate maximal subgroups of order 72. One representative of each of these six classes of maximal subgroups of Q_4 and the other eight Dade groups were then investigated with the programme Φ, giving a total of 1869 representatives of classes of conjugate subgroups of these groups, which had to be classified into crystal classes. This has been done in the following way:

Let us call two subgroups $\mathfrak{G}$, $\mathfrak{H}$ of $GL_n(\mathbf{Z})$ similar, if there is a 1-1 correspondence between the classes of conjugate elements in $\mathfrak{G}$ and those in $\mathfrak{H}$, such that corresponding classes contain the same number of elements and these have the same order, trace, and determinant. Obviously this similarity is an equivalence relation, implied by both geometrical and arithmetical equivalence.

The 1869 groups mentioned above were first sorted into similarity classes using the information provided by the programme. 227 such classes were thus obtained, consisting of 1 up to 43 groups. Geometrical and arithmetical equivalence then had to be decided only within these classes.

3. To some extent geometrical and arithmetical equivalence were treated simultaneously. We therefore speak just of equivalence, if a distinction

is not relevant. By definition two subgroups $\mathfrak{G}$ and $\mathfrak{H}$ of $GL_n(\mathbf{Z})$ are equivalent (geometrically or arithmetically), if there is an isomorphism φ of $\mathfrak{G}$ onto $\mathfrak{H}$ and an integral matrix X (with det $X \neq 0$ or det $X = \pm 1$ resp.) such that

$$XG = (G\varphi)X \text{ for all } G \in \mathfrak{G}. \tag{3.1}$$

The work involved in checking this for the groups in each similarity class has been substantially reduced by the following arguments:

1. An equivalence established between groups $\mathfrak{G}$ and $\mathfrak{H}$ implies equivalence between the corresponding subgroups of $\mathfrak{G}$ and $\mathfrak{H}$. We therefore started deciding the equivalence of big groups and used the information gained for smaller groups.

2. On the other hand, if a group $\mathfrak{G}$ contains a class of conjugate subgroups $\mathfrak{U}_i$ distinguished from all other subgroups of $\mathfrak{G}$ by their isomorphism-type and the invariants of their elements, then a group $\mathfrak{G}^*$ equivalent to $\mathfrak{G}$ must have again a unique class of subgroups $\mathfrak{U}_i^*$ with the same properties, and the $\mathfrak{U}_i$'s must be equivalent to the $\mathfrak{U}_i^*$'s. This remark often allows us to deduce nonequivalence of groups from nonequivalence of certain subgroups.

3. In order to prove nonequivalence of $\mathfrak{G}$ and $\mathfrak{H}$ it suffices to show that for some set of elements $G_1, \ldots, G_k \in \mathfrak{G}$ there is no set of elements $H_1, \ldots, H_k \in \mathfrak{H}$ such that $XG_i = H_iX$ holds for some X (with det $X \neq 0$ or det $X = \pm 1$ resp.). For this purpose preferably $G_1, \ldots, G_k$ were chosen as a class $\mathfrak{C}$ of conjugate elements, which is distinguished from all other classes of $\mathfrak{G}$ by the invariants determined by the programme Φ (number of elements in $\mathfrak{C}$, order, trace, determinant). A group $\mathfrak{G}^*$ similar to $\mathfrak{G}$ then contains just one class $\mathfrak{C}^*$ with the same properties. If $\mathfrak{C}^*$ is small enough, a programme has been used to try all $|\mathfrak{C}^*|$! permutations of the elements of $\mathfrak{C}^*$ as possible images of the elements of $\mathfrak{C}$ in a fixed order. A similar procedure was sometimes applied for two classes with either different or equal properties.

4. In order to prove equivalence, one has to show that for some system of generators $G_1, \ldots, G_s$ of $\mathfrak{G}$ there is a system $H_1, \ldots, H_s$ of generators of $\mathfrak{H}$ such that $XG_i = H_iX$ $(i = 1, \ldots, s)$ for some matrix X. This was done in the following way: A subgroup $\mathfrak{U}$ of order as low as possible and an element B of order as high as possible were chosen such that $\mathfrak{U}$ and B together generate $\mathfrak{G}$ and that both the classes of conjugates of $\mathfrak{U}$ and of B are unique in $\mathfrak{G}$ with respect to isomorphism-type and invariants. If $\mathfrak{G}^*$ is equivalent to $\mathfrak{G}$ there is a subgroup $\mathfrak{U}^*$ and an element B^* of $\mathfrak{G}^*$ having the same properties as $\mathfrak{U}$ and B in $\mathfrak{G}$. It then suffices to fix $\mathfrak{U}^*$ as image of $\mathfrak{U}$ and to try all conjugates of B^* as images of B.

4. All the choices described so far lead to some sets of elements $G_1, \ldots, G_s$ of $\mathfrak{G}$ and $H_1, \ldots. H_s$ of $\mathfrak{H}$ for which we have to decide if there is an integral

matrix $X = (x_{jk})$ such that

$$XG_i = H_iX \text{ for } i= 1, \ldots, s. \tag{4.1}$$

This is a homogeneous system of linear equations for the x_{jk} with coefficients in Z. A programme has been written which reduces (4.1) by integral row-operations to row-reduced echelon form. From this it determines the x_{jk} as integral linear combinations of some $x_1, \ldots, x_r$ of them, chosen as parameters. Then it computes det X as a polynomial $p(x_1, \ldots, x_r)$ in these parameters. Three cases can occur:

1. If $p(x_1, \ldots,$ x,) $\equiv 0$ the mapping $G_i \to H_i$ is not induced by transformation with any matrix from $GL_n(Q)$ (where Q is the rational field).

2. If $p(x_1, \ldots,$ x,) $\not\equiv 0$ and the (integral) coefficients of all monomials in it have a greatest common divisor > 1, then no X with det $X = \pm 1$ can exist as the parameters can only be substituted by integers. In this case, however, $G_i \to H_i$ can be induced by transformation with some matrix X with det $X \neq 0$ and hence $\mathfrak{G}$ and $\mathfrak{H}$ are geometrically equivalent.

3. If $p(x_1, \ldots . x_r) \not\equiv 0$ and the greatest common divisor of the coefficients of all monomials is 1, one has to try to find values of the parameters $x_1, \ldots, x_r$ such that the matrix X obtained by substituting these values for the parameters has det $X = 1$. If one does find such values for the $x_1, \ldots, x_r$, $\mathfrak{G}$ and $\mathfrak{H}$ are arithmetically equivalent; if one does not find such values, only geometrical equivalence has been proved, but no conclusion about arithmetical equivalence has been reached.

In all examples treated by us in which the third case occurred, it was always possible to find such values; so in fact the study of the greatest common divisor of the coefficients of the monomials of $p(x_1, \ldots,$ x,) was sufficient to prove nonequivalence. However, we owe to W. Gaschütz an example of two groups (in GL_{22} (Z)) for which the greatest common divisor of these coefficients is 1, but which are not arithmetically equivalent.

5. By the procedures described, we were able to classify the 1869 groups into both geometrical and arithmetical crystal classes. It turned out that the geometrical classes coincided with the similarity classes introduced here; this incidentally is also true for $n = 1, 2, 3$. Although it is unlikely that this is always the case, we do not know of an example of similar but not geometrically equivalent groups for any $n \geqslant 5$.

710 arithmetical classes were obtained, but as some hand-work was involved in the sorting, etc., this number has to be checked before it can be regarded as certain. Independent derivations of the arithmetical classes have been undertaken by H. Zassenhaus and D. Falk [**10**] by slightly different algebraic methods and by H. Wondratschek by more geometrical means. It has been agreed that the results of all these calculations will be collated before they are published jointly.

As a by-product of this investigation one gets a complete list of Bravais lattices in 4 dimensions which will correct an incomplete (and partially incorrect) list previously obtained [8] by heuristic considerations.

The list of arithmetical classes will also be used to determine the list of all space-groups in 4 dimensions. A programme for this, following ideas of H. Zassenhaus [9], has already been written and used on partial lists of crystal classes by H. Brown.

We would like to thank Professor H. Wondratschek, who first aroused our interest in the subject, for many valuable discussions and suggestions.

REFERENCES

1. J. J. Burkhardt: ***Die Bewegungsgruppen der Kristallographie,*** 2nd ed. (Birkhäuser Verlag, Basel, Stuttgart, 1966).
2. E. C. Dade: The maximal finite groups of 4X 4 integral matrices. ***Illinois J. Math.*** 9 (1965), 99-122.
3. V. Felsch and J. Neubüser: Ein Programm zur Berechnung des Untergruppenverbandes einer endlichen Gruppe. ***Mitt. Rhein-Westf. Inst. f. Znstr. Math. Bonn*** 2 (1963), 39-74.
4. C. Hermann: Translationsgruppen in *n* Dimensionen. ***Zur Struktur und Materie der Festkörper,*** 24-33 (Springer Verlag, Berlin, Göttingen, Heidelberg, 1951).
5. A. C. Hurley: Finite rotation groups and crystal classes in four dimensions. ***Proc. Camb. Phil. Soc. 47*** (1951), 650-661.
6. A. C. Hurley, J. Neubüser and H. Wondratschek: Crystal classes of four-dimensional space R4. ***Acta Cryst. 22*** (1967), 605.
7. J. S. Lomont: ***Applications of Finite Groups*** (Academic Press, New York, London, 1959).
8. A. I. Mackay and G. S. Pawley: Bravais lattices in four-dimensional space. ***Acta Cryst.*** 16 (1963), 11-19.
9. H. Zassenhaus : Über einen Algorithmus zur Bestimmung der Raumgruppen. Comm. ***Math. Helv.*** 21 (1948), 117-141.
10. H. Zassenhaus: On the classification of finite integral groups of degree 4. Mimeographed notes, Columbus, 1966.

A search for simple groups of order less than one million[†]

MARSHALL HALL Jr.

1. Introduction. In 1900 L. E. Dickson [17] listed 53 known simple groups of composite order less than one million. Three more groups have been added to this list since that time. A group of order 29,120 was discovered by M. Suzuki [31] in 1960, the first of an infinite class, and one of order 175,560 was discovered by Z. Janko [25] in 1965 which appears to be isolated. Very recently Z. Janko announced that a simple group with certain properties would have order 604,800 and have a specific character table. The construction of a simple group of order 604,800 is given for the first time in this paper.

The search for simple groups described here is not as yet complete. Approximately 100 further orders, all of the form $2^a3^b5^c7^d$, remain to be examined.

A number of people have helped me with this search. Dr. Leonard Baumert has helped with advice and computing. Dr. Leonard Scott sent me the proof of a formula on modular characters. But my main sources of help have come from Mr. Richard Lane and Professor Richard Brauer. For more than a year Mr. Richard Lane has carried out a large number of complicated computations on the IBM 7094 at the California Institute of Technology's computing center. Professor Richard Brauer has been generous with help in references, correspondence, and conversations.

The construction of the simple group of order 604,800 was carried out in August 1967 at the University of Warwick and at Cambridge University. Mr. Peter Swinnerton-Dyer was extremely helpful in writing on short notice a program for the Titan computer at Cambridge which finally confirmed the correctness of the construction.

2. Notation. List of known simple groups in the range. The notation for the classical simple groups used here will be essentially that used in Artin [1]. Here let $GF(q)$ be the finite field with q elements where $q = p^r, p$ a prime.

[†] This research was supported in part by NSF grant GP3909 and in part by ONR contract N00014-67-A-0094-0010.

$PSL_n(q)$ is the projective special linear group of dimension n over $GF(q)$. Here $PSL_n(q)$ is the group of n-dimensional matrices of determinant 1 over $GF(q)$ modulo its center. $PSL_2(q)$ is of order $\frac{1}{2}q(q^2-1)$ for q odd and of order $q(q^2-1)$ for $q = 2^r$. $PSL_3(q)$ is of order $q^3(q^3-1)(q^2-1)/z$ where z is 1 unless there is an element of order 3 in $GF(q)$ in which case z = 3.

$Sp_{2n}(q)$ is the symplectic group of order $q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$.

$U_n(q)$ is the unitary group of order $\frac{q^{n(n-1)/2}}{t}\prod_{i=2}^{n}(q^i-(-1)^i)$, $t = (n,q+1)$.

A, is the alternating group of n letters.

The simple Mathieu groups M_{11}, M_{12}, and M_{22} come within the range of this search. The Suzuki groups $Su(q)$ with $q = 2^{2n+1} \geqslant 8$ are of order $q^2(q^2+1)(q-1)$. Here $Su(8)$ of order 29,120 is the only Suzuki group in the range. The Janko group of order 175,560 is still an isolated group and will be called merely the Janko group. No simple groups of the Chevalley types [15] or Rimhak Ree's [27,28] occur in the range examined.

The known 56 simple groups of order less than one million are: 28 groups $PSL_2(p)$, p a prime, $p = 5, 7, \ldots, 113$. The other 28, listed by their order are:

Group type	*Order*
$PSL_2(9) = A_6$	$360 = 8\cdot 9\cdot 5$
$PSL_2(8)$	$504 = 8\cdot 9\cdot 7$
A_7	$2520 = 8\cdot 9\cdot 5\cdot 7$
$PSL_2(16)$	$4080 = 16\cdot 3\cdot 5\cdot 17$
$PSL_3(3)$	$5616 = 16\cdot 27\cdot 13$
$U_3(3)$	$6048 = 32\cdot 27\cdot 7$
$PSL_2(25)$	$7800 = 8\cdot 3\cdot 25\cdot 13$
M_{11}	$7920 = 16\cdot 9\cdot 5\cdot 11$
$PSL_2(27)$	$9828 = 4\cdot 27\cdot 7\cdot 13$
$PSL_4(2) = A_8$	$20\ 160 = 64\cdot 9\cdot 5\cdot 7$
$PSL_3(4)$	$20\ 160 = 64\cdot 9\cdot 5\cdot 7$
$Sp_4(3) = U_4(2)$	$25920 = 64\cdot 81\cdot 5$
$Su(8)$	$29120 = 64\cdot 5\cdot 7\cdot 13$
$PSL_2(32)$	$32736 = 32\cdot 5\cdot 7\cdot 31$
$PSL_2(49)$	$58\ 800 = 16\cdot 3\cdot 25\cdot 49$
$U_3(4)$	$62\ 400 = 64\cdot 3\cdot 25\cdot 13$
M_{12}	$95\ 040 = 64\cdot 27\cdot 5\cdot 11$
$U_3(5)$	$126000 = 16\cdot 9\cdot 125\cdot 7$

Group type	*Order*
Janko group	$175560 = 8\cdot3\cdot5\cdot7\cdot11\cdot19$
A_9	$181\,440 = 64\cdot81\cdot5\cdot7$
$PSL_2(64)$	$262\,080 = 64\cdot9\cdot5\cdot7\cdot13$
$PSL_2(81)$	$265680 = 16\cdot81\cdot5\cdot41$
$PSL_3(5)$	$372000 = 32\cdot3\cdot125\cdot31$
M_{22}	$443\,520 = 128\cdot9\cdot5\cdot7\cdot11$
New group	$604800 = 128\cdot27\cdot25\cdot7$
$PSL_2(121)$	$885\,720 = 8\cdot3\cdot5\cdot121\cdot61$
$PSL_2(125)$	$976\,500 = 4\cdot9\cdot125\cdot7\cdot31$
$Sp_4(4)$	$979200 = 256\cdot9\cdot25\cdot17$

3. Known results **used.** The known results used will be numbered for references later in the paper.

(1) A paper, as yet unpublished, by John Thompson [33] determines the minimal simple groups. These are among

$$\begin{array}{ll} PSL_2(p), & p \text{ prime}, p \geqslant 5 \\ PSL_2(2^p) & p \text{ prime} \\ PSL_2(3^p) & p \text{ prime} \\ PSL_3(3) & \\ Su(2^p) & p \text{ an odd prime.} \end{array}$$

Not all of these are minimal. In particular any one of these whose order is a multiple of 60 contains $PSL_2(5) = A_5$ of order 60.

(2) Daniel Gorenstein and John Walter [22] have shown that a simple group with a dihedral Sylow 2-subgroup is necessarily a group $PSL_2(q)$, q odd, or the group A_7. In particular if the order of the group is not divisible by 8 then it is divisible by 4 and is a group $PSL_2(q)$ with $q \equiv 3$ or 5 (mod 8).

(3) Daniel Gorenstein [21] has shown that if a Sylow 2-subgroup of the simple group G is Abelian, and if the centralizer of every involution is solvable, then G is one of $PSL_2(q)$ where $q \equiv 3$ or 5 (mod 8), $q > 5$ or $q = 2^n$, $n \geqslant 2$.

(4) Richard Brauer and Michio Suzuki **[11]** have shown that a Sylow 2-subgroup of a simple group cannot be a quaternion group or generalized quaternion group.

(5) It has been shown by J. S. Brodkey [13] that if a Sylow subgroup P of a group G is Abelian then there exist two Sylow subgroups whose intersection is the intersection of all of them. In particular if any two Sylow p-subgroups have a non-trivial intersection, then the intersection of all of them is a non-trivial group, necessarily a normal subgroup of G. Hence if a simple

group has an Abelian Sylow p-subgroup S(p) = P_0 there must be a conjugate P_1 with $P_0 \cap P_1 = 1$.

The Brauer theory of modular characters has played a major role in this search, in particular the theory for groups whose order is divisible by exactly the first power of a prime. Let p be a prime and suppose that g, the order of the group G, is divisible by exactly the first power of p. We write

$$g = pqw(1+rp), \quad \text{p-1} = qt. \tag{3.1}$$

Here G has $1+rp$ Sylow p-subgroups $S(p)$ and the order of the normalizer $N(p)$ of a Sylow p-subgroup is $|N(p)| = pqw$. The centralizer C(p) of $S(p)$ is of order pw and C(p) = $S(p) \times V$ where $V = V(p)$ is of order w. $N(p)/C(p)$ is cyclic of order q where $q|p - 1$ is the order of the group of automorphisms of $S(p)$ induced by $N(p)$. By a classical theorem of Burnside's ([**14**], p. 203) if we had $q = 1$, G would have a normal p-complement and so we have $q > 1$ for a simple group.

(6) Brauer [3]. The principal block of characters $B_0(p)$ contains q ordinary characters $\chi_1, \chi_2, \ldots, \chi_q$ where χ_1 is the trivial character of degree $f_1 = 1$ and $\chi_i(1) = f_i$, $i = 2, \ldots, q$, and a family of $t = (p-1)/q$ exceptional characters χ_0^j which are p-conjugate and are all of the same degree $\chi_0^j(1) = f_0$, j= 1, ..., t. For the ordinary characters there is a sign $\delta_i = \pm 1$ such that $\delta_i f_i \equiv 1 \pmod{p}$ and for the exceptional character there is a sign $\delta_0 = \pm 1$ such that $\delta_0 f_0 \equiv -q \pmod{p}$. If $q = p - 1$ the single exceptional character is not distinguishable from the ordinary character. Also the degrees satisfy the relations

$$1+\delta_2 f_2 + \ldots + \delta_q f_q + \delta_0 f_0 = 0, \tag{3.2a}$$
$$f_i \,|q(1+rp). \quad u = 0, 1, \ldots, q.$$

If u is a generator of $S(p)$ then

$$\chi_i(u) = \delta_i, \; i = 1, \ldots, q, \tag{3.2b}$$
$$\chi_0^j(u) = -\delta_0(\varepsilon^v + \varepsilon^{sv} + \ldots + \varepsilon^{s^{q-1}v}), \quad v = v(j),$$

where ε is a primitive ith root of unity, s is a primitive solution of $s^q \equiv 1 \pmod{p}$ and v = v(j) ranges over t values such that vs^i gives a full set of a non-zero residues modulo p. These values of the exceptional characters are the Gauss periods of cyclotomy. If w = 1 then $B_0(p)$ is the only block containing characters of degrees not divisible by p. If w > 1 there are further non-principal blocks of characters of degrees not divisible by p and Brauer gives relations similar to (3.2a, b) for these blocks. A character χ of degree divisible by p is a block by itself and vanishes for everyp-singular element (an element of order divisible by p). No simple group of order divisible by p has an (irreducible) character (except the trivial one) of degree less than $\frac{1}{2}(p-1)$ and if it does have an irreducible character of degree $\frac{1}{2}(p-1)$ then it is isomorphic to $PSL_2(p)$. This has been shown to be true by Feit and Thompson [20] even if a higher power of p than the first divides the order of the group. More recently Feit [18] has extended this to show the same conclusion if G has a character of degree less than $\boldsymbol{p}-1$. Everett Dade [16] has extended Brauer's work to cover the case in which a Sylow subgroup is cyclic.

(7) It was shown by Brauer [3] that, for groups divisible by only the first power of a primep, the characters of a block may be associated with a tree. Each ordinary character is a vertex and each modular character is an arc. An ordinary character (treating a family of p-conjugate exceptional characters as a single character) decomposes as the sum of the modular characters which are arcs with an end at the vertex for the ordinary character. A modular character appears as a constituent of exactly two ordinary characters and in each of these with multiplicity one. If χ_i and χ_k are the two ends of an arc then $\chi_i+\chi_k$ is a modular indecomposable and vanishes for everyp-singular element, and so in particular if δ_i and δ_k are the corresponding signs $\delta_i+\delta_k=0$. H. F. Tuan [34] has refined this for the principal block and has shown that the real characters (characters real for every element) in the tree form a stem which may be drawn in a straight line, and the tree is symmetric with respect to this stem with complex conjugacy interchanging the remaining vertices and arcs.

(8) Brauer and Tuan ([12], Lemma 1) showed that for χ a character in the principal $\boldsymbol{p}$ block $B_0(p)$, in the notation of (5), then the restriction of χ to V, $\chi| V$, has the form

$$\chi \quad V = m\varrho_0+p\theta \tag{3.3}$$

where ϱ_0 is the identity character of V and θ is some character of V possibly reducible. In private communication to me, Leonard Scott has generalized this to characters χ of a non-principal block $B_j(p)$. In this case the formula becomes

$$\chi \mid V = m\sum_{i=1}^{s}\zeta^{N_i}+p\theta \tag{3.4}$$

where ζ^{N_i}, $\boldsymbol{i}=1,\ldots,$ s, are the irreducible characters of V conjugate in $N(p)$ associated with the block $B_j(p)$. In case the character χ has degree divisible by $\boldsymbol{p}$, a simple consequence of the fact that χ vanishes for p-singular elements yields

$$\chi \mid V = p\theta. \tag{3.5}$$

The formula (3.4) gives for an $x\in V$ the determinantal relation $\det(\chi(x)) = \det(\theta(x))^p$, so that if θ is of degree 1 and G is simple then $\det\theta(x)=1$, whence $\theta(x)=1$ and $\chi(x)=\chi(1)$ is the identity matrix, a situation impossible for a simple group. In particular with $g = pqw(1+\boldsymbol{rp})$ for a simple group G, if $B_0(p)$ contains a character of degree less than $2p$, then $w=1$. This is also proved and used by Stanton [30] in his study of the Mathieu groups. To avoid confusion with other references to Brauer and Tuan we shall call this the Stanton condition.

(9) Burnside has shown that groups of orders p^aq^b, p and q primes, are solvable. A proof of this may be found on page 291 of the writer's book [23].

(10) It was shown by Burnside that if a Sylow p-subgroup 5'(p) of a group G is in the center of its normalizer $N(p)$, then G has a normal p-complement ([23], p. 203). Here the normal p-complement K is a normal subgroup of G such that $G/K \cong S(p)$. An easy consequence of the Burnside result ([23], p. 204) is that the order of a simple group is divisible by 12 or by the cube of the smallest prime dividing its order. Further results depending on the theory of the transfer ([23], ch. 14) assure the existence of normal subgroups with p-factor groups. A recent theorem of John Thompson's [32] gives an elegant condition for the existence of normal p-complements.

(11) Brauer and Reynolds [10] have shown that a simple group G whose order g is divisible by a prime $p > q^{1/3}$ is isomorphic to $PSL_2(p)$ where $p > 3$ or to $PSL_2(2^n)$ where $p = 2^n + 1$ is a Fermat prime. Thus these groups are the unique simple groups of their orders.

In a more refined form they show that if $p^2 \nmid g$ and we write g = $pqw(1+rp)$ as in (3.1), if it should happen that

$$(p-1)(1+rp) = (vp-1)(up+1) \tag{3.6}$$

has only $vp-1 = p- 1$ and $up+1 = 1+rp$ as a solution in integers, then with S the largest normal subgroup of G of order prime top *we* have one of

$$\begin{aligned}
&\text{(a) G/S} \cong PSL_2(p) \text{ and } r = 1,\\
&\text{(b) G/S} \cong PSL_2(2^n) \text{ where } p = 2^n+1,\ r = \tfrac{1}{2}(p-3),\\
&\text{(c) G/S is the metacyclic group of order } pq.
\end{aligned} \tag{3.7}$$

This argument depends on the fact that the degrees f_i, $i = 1, \ldots, q$, and f_0 in the principal block $B_0(p)$ divide $(p-1)(1+rp)$ and if there is no second representation in (3.6) then f_i and tf_0 can only take the values 1, ***p-l***, $1+rp$, and $(p-1)(1+rp)$. These restrictions together with the relation (3.2) restrict the degrees so heavily that they are able to reach the strong conclusions listed in (3.7).

(12) Suppose there is a factorization in (3.6) above so that $(p-1)(rp+1) =$ $= (vp- 1)(up+1)$. Here $vp-1 > p-1$ so that v > 1 and consequently $up+1 < rp+1$ and so $u<r$. Multiply out the equation, add 1 to both sides and divide by p. This gives

$$rp - r + l = uvp + v - u. \tag{3.8}$$

This leads to the identity

$$(r-u)(u+1) = (up+1)(r-uv) \tag{3.9}$$

which we may obtain by multiplying out the right-hand side and replacing u^2vp by u times the value of uvp from (3.8). Since $r > u$ the left-hand side is positive and so we may put $r-uv = h$ where h is a positive integer. Writing

$$(r-u)(u+1) = h(up+1) \tag{3.10}$$

and solving for r, we have

$$r = (hup+h+u^2+u)/(u+1) = F(p, u, h). \tag{3.11}$$

Thus the existence of further factorizations (3.6) is equivalent to expressing r in the form (3.11) with positive h and u. We see that $r > hpu/(u+1) > \frac{1}{2} hp$, so that for a given $r, h < 2r/p$. For a given h, since $u+1 \mid h(p-1)$ there are only a finite number of trials to be made. As $g = pqw(1+rp)$ and $q \geqslant 2$ it follows that $2rp^2 < g$, $2r < g/p^2$ whence $h < g/p^3$.

(13) The general theory of modular characters of G, when g is divisible by a power p^s of a prime p higher than the first, has been used only in a limited way. For reference see Brauer [6]. Suppose g = $p^s g'$ where g' $\not\equiv 0$ (mod p). Any element x of the finite group G has a unique expression x = yz = zy where the order of y is a power ofp and the order z is relatively prime to p. We call y the p-part of x. Here if the order of x is prime to p, then y = 1. If the p-part of x is not 1 we call x p-singular, and if the p-part of x is 1 we call x p-regular. An irreducible character χ of G of degree divisible by p^s is said to be of highest type and is a p-block by itself and vanishes for every p-singular element. An irreducible character of degree divisible by p^{s-1} is of defect 1 and all characters of its block have degrees exactly divisible by p^{s-1}.

The orthogonality relation holds :

$$\sum_{\chi \in B(p)} \chi(x)\chi(y) = 0, \text{ p-parts of x and y not conjugate.} \tag{3.12}$$

A refinement of this, which also appears in both the Brauer-Tuan paper [12] and the Stanton paper [30], is the following: Let p and q be different primes and suppose that G contains no element of order pq. We quote Lemma 2 of Stanton [30]. If G contains no elements of order pq, where g = $p^a q^b g'$, (g', pq) = 1, and if

$$\sum_{i=1}^{k} a_i \zeta_i(x) = 0$$

for all p-regular elements x, then

$$\Sigma\ a_i \zeta_i(x) = 0, \quad \zeta_i \in \text{B(q) a } q \text{ block,}$$

for all q-singular elements x. Furthermore

$$\Sigma\ a_i \zeta_i(1) \equiv 0 \pmod{q^b},\ \zeta_i \in B(q).$$

We refer to this as the principle of "block separation". An application is given in Example 2 of § 5.

In Brauer-Tuan [12] it has been shown that a character of degree p^s, $s \geqslant 1$, is not in the principal block $B_0(p)$ for a simple group G.

A useful fact is that an algebraic conjugate of a character in the principal block $B_0(p)$ is also in the principal block. Thus if in $B_0(p)$ there is only a single character of a particular degree, then it is necessarily rational. For a rational character of degree n representing a group G of order g faithfully it has been shown by Schur [29] that the highest power of a prime p that can divide g is p^s where

$$s = \left[\frac{n}{p-1}\right] + \left[\frac{n}{p(p-1)}\right] + \dots + \left[\frac{n}{p^i(p-1)}\right] \cdot \tag{3.13}$$

Here the square bracket [x] denotes the integral part of x.

(14) The writer [24] has shown that if a group G has a Sylow p-subgroup P and a normal subgroup K, then the number n_p of Sylow p-subgroups in G is of the form $n_p = a_pb_pc_p$ where a_p is the number of Sylow p-subgroups in G/K, b_p is the number of Sylow p-subgroups in K, and c_p is the number of Sylow p-subgroups in $N_{PK}(P \cap K)/P \cap K$. From this it is shown that n_p is the product of factors of the following two kinds: (1) the number s_p of Sylow p-subgroups in a simple group X; and (2) a prime power q^t where $q^t \equiv 1 \pmod{p}$.

The Brauer-Reynolds results (3.7) combined with these results show that certain numbers of the form $1 + kp$ cannot be the n_p of any finite group: For example 15 cannot be n_7 in any group nor can 21 be n_5 in any group.

(15) A method attributed to Richard Brauer is quoted in the thesis of E. L. Michaels [26]. This applies to cases in which a Sylow p-subgroup is of order p^r, $r > 1$. Let K be of order p^{r-1} and the intersection of two Sylow p-subgroups P_0 and P_1. Then $P_0 \cup P_1 \subseteq$ No(K) $= H$ and so H contains more than one Sylow p-subgroup, say $1 + b_Kp$ Sylow p-subgroups, and of course every Sylow p-subgroup P_i intersecting P_0 in K normalizes K. Let G contain [G : $N(P)$] $= 1 + mp$ $S(p)$'s and suppose that P_0 contains r_K conjugates of K. Counting incidences of conjugates of Kin Sylow p-subgroups we obtain

$$[G : N(P)]r_K = (1 + b_Kp)[G : H]. \tag{3.14}$$

Here the left-hand side says that each of $1 + mp = [G : N(P)]$ $S(p)$'s contains r_K conjugates of K, while the right-hand side says that each of [G : H] conjugates of Kis contained in $1 + b_Kp$ $S(p)$'s. Also

$$mp = P \sum_K r_K b_K + ap^2, \tag{3.15}$$

where under conjugation by P_0 the remaining $S(p)$'s are counted, first those whose intersection with P_0 is of index p, and the rest ap^2 those whose intersection with P_0 is of index p^2 or higher. This method is particularly useful if the order of an $S(p)$ is exactly p^2, as the two relations (3.14) and (3.15) are then highly restrictive.

(16) If in G there are r classes of conjugates, $K_1, K_2, \ldots, K_r$, then in the group ring R(G) over the complex field the class sums $C_i = \Sigma$ x, $x \in K_i$, play a special role in character theory. Here

$$C_iC_j = C_jC_i = \sum_{k=1} c_{ijk}C_k, \tag{3.16}$$

where the c_{ijk} are non-negative integers. The coefficients c_{ijk} can be expressed in terms of the characters ([14], p 316). We have

$$c_{ijk} = \frac{g}{c(x_i)c(x_j)} \sum_{a=1}^{r} \left(\frac{\chi_i^a \chi_j^a \overline{\chi_k^a}}{n_a} \right). \tag{3.17}$$

Here χ_i^a is the value of the irreducible character χ^a for an element x_i of the ith class K_i and $n_a = \chi^a(1)$ is the degree of this character. $c(x_i)$, $c(x_j)$ are respectively the orders of the centralizers $C_G(x_i)$, $C_G(x_j)$.

A particular case of (3.17) is that in which $x_i = x_j = \tau$ is an involution. If x_k is of order $\boldsymbol{p}$ then, as shown in Brauer-Fowler ([**8**], Lemma 2A), c_{ijk} is the number of involutions conjugate to τ transforming x_k into x_k^{-1}. In case x_k is of order $\boldsymbol{p}$ and (x) is its own centralizer and $q|p-1$ is even this number is exactly $\boldsymbol{p}$. As $\chi(x)$ vanishes for characters not in $B_0(p)$ the equation (3.17) determines $c(\tau)$ in terms of the values of $\chi(\tau)$ and $\chi(x)$ for χ in $B_0(p)$. In case q is odd there is no involution in $N(p)$ and so this number c_{ijk} must be zero. We also have $c_{ijk} = 0$ if q is even but τ is not conjugate to the involution in $N(p)$.

4. General outline of the **search.** The major result of Feit and Thompson [19] is that simple groups are of even order. Starting from the earlier results in (9) of § 3 it is not too difficult to show directly that there is no simple group of odd order less than one million, and in fact a search of odd orders less than one hundred million was completed at almost the same time that the Feit-Thompson result was announced.

The results (2) of Gorenstein and Walter show that if g, the order of the simple group G, is divisible by 4 but not by 8, then G is a group $PSL_2(q)$. Next suppose that g is divisible by 8 but not by 16. A Sylow 2-subgroup S(2) is one of the five non-isomorphic groups of order 8. If S(2) is cyclic or is the Abelian group with a basis [4,2] then S(2) is necessarily in the center of N(2) and G has a normal 2-complement by (9). If S(2) is the quaternion group then by the result (4) of Brauer and Suzuki G is not simple. If S(2) is the dihedral group of order 8, then from Gorenstein and Walter (2) G is a known group, namely $PSL_2(q)$ or A_7. There remains the possibility that S(2) is the elementary Abelian group of order 8. As S(2) is Abelian G is trivially 2-normal and the theorem of Grün ([23], p. 215) applies, so that G has a 2-factor group isomorphic to the 2-factor group of N(2). The automorphism group of S(2) is of order (2^3-1)(2^3- 2) **x** (2^3-2^2) = 168 and as N(2)/C(2) is of odd order, its order must divide 21.

It is easy to find that if N(2)/C(2) is of order 3 then N(2) has a factor group of order 2, and so by Grün's theorem G has a normal subgroup of index 2. Hence if g is divisible by 8 but not by 16, we may restrict our search to orders which are also multiples of 7. We have incidentally proved the uniqueness of the groups $PSL_2(q)$ as the only simple groups of their order when g is divisible by 8 but not 16 or 7. In our list then there is a unique simple group of each of the orders 360, 7800, 885 720, as well as orders multiples of 4 but not 8, namely 9828 and 976 500, in each case the appropriate $PSL_2(q)$.

A simple group G which is not minimal will contain some proper subgroup which is not solvable and so has a simple group as a composition factor. Hence G has a subgroup $\boldsymbol{H}$ and $\boldsymbol{H}$ has a normal subgroup $\boldsymbol{K}$ (possibly $\boldsymbol{K} = 1$) such that $\boldsymbol{H/K}$ is a simple group. We call a factor group of a subgroup a ***section.*** Hence by John Thompson (1) we may confine our search to groups which have one of the simple groups listed as a section. Here if $[G : H] = t$ and $[\boldsymbol{K}: 1] = k$, and $H/K = s$ we have $g = tsk$. If the simple group $\boldsymbol{H/K}$ is $PSL_2(p)$ for $\boldsymbol{p} \geqslant 41$ then as g $\leqslant$ 1,000,000, $s \geqslant |PSL_2(41)| = 34\ 440$ it follows that $\boldsymbol{tk} < 30$. Then $[\mathrm{G} : H] = t < 30$ and so G has a permutation representation on t letters. But as $\boldsymbol{p} \geqslant \boldsymbol{41}$ **G** cannot represent an element of order $\boldsymbol{p}$ faithfully on less than 30 letters. Thus we may exclude as a section $PSL_2(p)$ with $\boldsymbol{p} \geqslant 41$. If $PSL_2(37)$ of order 25,308 is a section, then $\boldsymbol{tk} \leqslant 39$, and since G is represented as a permutation group on t letters and contains an element of order 37, then $\boldsymbol{k} = 1$, $t \leqslant 39$. Here $\boldsymbol{H} = G_1$ is the subgroup of G fixing a letter and, as $PSL_2(37)$ does not (from its character table) have a permutation representation on less than 38 letters, it follows that $t = 39$. Then the order of G is $25\ 308 \cdot 39 = 987012$ and by Gorenstein and Walter must be $PSL_2(q)$ with $q \equiv 3, 5 \pmod 8$ which it is not. If the Suzuki group $Su(8)$ of order 29 120 is a section of G, then $\boldsymbol{tk} \leqslant 34$. Now $Su(8)$ has as rational characters the identical character, one of degree 64 and another of degree 91. It has two algebraically conjugate characters of degree 14 both of which take the value -1 on elements of order 5, three algebraic conjugates of degree 35, and three algebraic conjugates of degree 65. From this it easily follows that $Su(8)$ has no subgroup of index less than 65, and this of course corresponds to its representation as a doubly transitive group on 65 letters. Since $Su(8)$ has an element of order 13 we must have $t \geqslant 14$, and as $\boldsymbol{tk} \leqslant \boldsymbol{34}$ then $\boldsymbol{k} = 1$ or 2. With $\boldsymbol{tk} \leqslant 34$ and either $\boldsymbol{k} = 1$ or $\boldsymbol{k} = 2$, the representation of G on 34 or fewer letters with G either $Su(8)$ or the extension of $Su(8)$ by a center of order 2 corresponds to a subgroup of $Su(8)$ of index less than 65, which is a conflict. Hence no simple G has $Su(8)$ as a section. $PSL_2(32)$ is of order $32\ 736 = 32.3 \cdot 11 \cdot 31$. If $PSL_2(32)$ is a section of G then $\boldsymbol{tk} \leqslant 30$, clearly a conflict as we cannot represent an element of order 31 on 30 or fewer letters.

Having eliminated the groups above as sections of G, and having shown easily that a section of a section is again a section, we have from John Thompson's results in (1) that one of the following minimal simple groups is a section of G.

Group	*Order*
$PSL_2(5)$	$60 = 4\cdot 3\cdot 5$
$PSL_2(7)$	$168 = 8\cdot 3\cdot 7$
$PSL_2(8)$	$504 = 8\cdot 9\cdot 7$
$PSL_2(12)$	$1092 = 4\cdot 3\cdot 7\cdot 13$
$PSL_2(17)$	$2448 = 16\cdot 9\cdot 17$
$PSL_3(3)$	$5616 = 16\cdot 27\cdot 13$
$PSL_2(23)$	$6072 = 8\cdot 3\cdot 11\cdot 23$
$PSL_2(27)$	$9828 = 4\cdot 27\cdot 7\cdot 13$

From Gorenstein's result (3) it follows that if the order of G is a multiple of 8 but not 16, then the centralizer of an involution τ is not solvable and so $H = C_G(\tau)/\langle\tau\rangle$ is a non-solvable group of order a multiple of 4 but not 8. Hence H contains as a section one of the groups $PSL_2(5)$, $PSL_2(13)$ or $PSL_2(27)$ and so the order of G is a multiple of $8\cdot 3\cdot 5\cdot 7 = 840$ or of $8\cdot 3\cdot 7\cdot 13 = 2184$.

On the basis of the above information we may divide the orders to be examined into seven lists, the orders being multiples of particular numbers.

	Form of g	*Number of orders*
A	$16\cdot 3\cdot 5m = 240m$	4166
B	$16\cdot 3\cdot 7m = 336m,\ m \not\equiv O(5)$	2381
C	$8\cdot 3\cdot 5\cdot 7m = 840m,\ m$ odd	595
D	$8\cdot 3\cdot 7\cdot 13m = 2184m, m$ odd, $\not\equiv O(5)$	183
E	$16\cdot 9\cdot 17m = 2448m,\ m \not\equiv 0(5),\ \not\equiv O(7)$	280
F	$16\cdot 27\cdot 13m = 5616m,\ m \not\equiv 0(5),\ \not\equiv O(7)$	124
G	$16\cdot 3\cdot 11\cdot 23m = 12144m,\ m \not\equiv 0(5),\ \not\equiv O(7)$	57
	Total number of orders	7786

As we have already remarked, if g is divisible by 8 but not 16 then g is also divisible by 7 and from the Gorenstein result (3) G contains $PSL_2(5)$, $PSL_2(13)$ or $PSL_2(27)$ as a section and so g is divisible by 5 or 13, giving lists C and D. For multiples of 16, g is certainly a multiple of 3. If g is a multiple of 5 or 7 it is included in lists A or B. If g is not a multiple of 5 or 7 it contains $PSL_2(17)$, $PSL_3(3)$ or $PSL_2(23)$ as a section and so is listed in list E, F, or G. There are a few duplications between lists E, F, and G, but otherwise no duplications in the lists. If we did not use John Thompson's unpublished results (1), apart from lists C and D we would also have to consider all 62,500 multiples of 16. This would add a large number of orders to be examined, but probably not very many difficult ones, since in practice the orders with only high powers of small primes seem to be the most difficult to eliminate.

From the result (11) of Brauer and Reynolds, if g is divisible by a prime $p > 100$ then as $g < 1{,}000{,}000$, $p < g^{1/3}$ and so G is necessarily $PSL_2(p)$ or $PSL_2(2^n)$ where $p = 2^n + 1$ is a Fermat prime. Hence we may assume that g is divisible by no prime greater than 97.

At this stage we can divide our search into two parts. For the first part g is divisible by a prime p in the range $37 \leqslant p \leqslant 97$. For the second part every prime dividing g is at most 31. The first part is far easier. We have a prime p dividing g where $p^4 > g$, since $37^4 = 1{,}874{,}161 > g$. Suppose first $p^3|g$. Then G has $1 + kp$ Sylow subgroups S(p) and $(1+kp)p^3|g < p^4$, whence $k = 0$ and so $S(p) \lhd G$ and G is not simple. Next suppose that $p^2|g$, and that G has $1 + kp$ $S(p)$'s. Then $(1 + kp)p^2|g < p^4$ and so $1 + kp < p^2$. Here an $S(p)$ of order p^2 is necessarily Abelian. As $1 + kp < p^2$, two $S(p)$'s have an intersection of order p. For if $P_0 \cap P_1 = 1$, where P_0 and P_1 are two distinct $S(p)$'s, then P_1 would have p^2 distinct conjugates under P_0 and G would have at least $1 + p^2 > 1 + kp$ Sylow subgroups S(P), a conflict. But then by Brodkey's result (5) all $S(p)$'s intersect in a subgroup of order p which is normal in G, and so G is not simple. It follows therefore from our assumption that if g is divisible by a prime p such that $p^4 > g$, then only the first power of p divides g.

For the primes p with $37 \leqslant p \leqslant 97$ we rely on the Brauer-Reynolds results of (11) and (12). The number $1 + rp$ of admissible $S(p)$'s was calculated by (3.1 1), and degrees satisfying (3.2) were found. In $g = (1 + rp)pqw$ the values of g and w were determined so that g would be divisible by 168 or 48, following Gorenstein and Walter's results (2) and (3). The details of these calculations for $p = 59$ are given in Example 1 of § 5.

The Stanton condition of (8) and the principle of block separation are applicable. An illustration of block separation is given in Example 2 of § 5. All orders multiples of primes p, $37 \leqslant p \leqslant 97$, were eliminated in this way except for $g = 265\,680 = 16 \cdot 81 \cdot 5 \cdot 41$, which is the order of the simple group $PSL_2(81)$. The value $g = 885\,720$ which is the order of $PSL_2(121)$ is a multiple of 61 but did not come into consideration since here g is divisible by exactly 8 but not by 7 and so its Sylow 2-group must be dihedral and thus the Gorenstein-Walter results apply.

The remaining numbers in the lists A through G were calculated by multiplying out products of the primes 2 through 31 in all possible ways for each list giving all values of g in the lists not exceeding one million. This saved the trouble of factorization and automatically eliminated all orders divisible by primes exceeding 3 1.

The number of orders in the lists at this stage was as follows:

	Form of g	*Number of orders*	*Reduced number*
A	$240m$	1064	684
B	$336m$	563	208
C	$840m$	181	135
D	$2184m$	68	32
E	$2448m$	125	29
F	$5616m$	72	52
G	$12144m$	44	6
	Totals	2117	1146

At this stage the computer calculated for every order the possible number of $S(p)$'s for $p = 7, \ldots, 31$. Sylow numbers $1 + rp$ which arose were then listed by the primes, and, assuming g to be divisible by exactly the first power of p, further factorizations of the form $(p-1)(1+rp) = (up+1)(vp-1)$ were found. Here a given $(p-1)(1+rp)$ was tested for divisibility by all numbers $up+1$ or $vp-1$ less than 1000, since in every case $1{,}000{,}000 > g > p(1+rp) > (p-1)(1+rp)$. If one or more further factorizations for $(p-1)(1+rp)$ were found, then for each value of q dividing $p-1$ which actually arose for some order the degrees satisfying (3.2) for $1+rp$ $S(p)$'s were listed. Note that the existence of a second factorization does not guarantee the existence of degrees greater than $\frac{1}{2}(p-1)$ satisfying (3.2). For example with 320 $S(11)$'s, $10\cdot 320 = 100\cdot 32$ but no degrees are found for $q = 2$, 5, or 10.

Suppose g is divisible by exactly the first power of the prime p. For $n_p = 1 + rp$ Sylow p-subgroups, and $q \mid (p-1)$, the order of the automorphisms induced in $S(p)$ by $N(p)$, if there is no set of degrees satisfying (3.2) this is a combination to be excluded and as such a "bad" combination. If g is divisible by p^2 or a higher power and if $1 + rp < p^2$, then in the representation of G on $1+rp$ letters every orbit is a p-cycle and so $S(p)$ is Abelian of exponent p. But then any two $S(p)$'s have a non-trivial intersection and by Brodkey's result (5) all $S(p)$'s intersect in a non-trivial subgroup of G which is necessarily normal. Hence if $p^2 \mid g$, $1 + rp < p^2$ $S(p)$'s is not possible in a simple group.

The computer took the 2117 orders each with its list of Sylow numbers $1+rp$ and order of $N(p)$ $g/(1+rp)$ and marked it "Fails Brauer test on $p = s$" in case for the prime s dividing g to the first power, no pair $1+rs$, $q \mid s-1$, $sq(1+rs) \mid g$ was a good pair and marked it "Fails Sp" test" if $p^n \mid g$, $n-2$ and all $1+rp < p^2$. This reduced the number of orders to be considered from 2117 to 1146. Note that the tests used so far depend essentially on a Sylow number $1+rp$ and, if only the first power of p

divides g, then also on $q|(p-1)$. These tests involving table look-ups were easy to put on the machine.

The remaining 1146 orders were examined individually. The Stanton principle, that if every set of characters for $B_0(p)$ (p dividing g to the first power) contains a character of degree less than $2p$, *we* must have w = 1, could have been mechanized. But this test, illustrated in Example 3 of § 5, was not difficult to apply by hand.

Certain orders were eliminated by consideration of Sylow groups of order p^2 or higher. Example 4 of § 5 illustrates a relatively easy case.

The interplay between a Sylow p-group and a Sylow q-group provided information in many cases. Since a group of order 35 is necessarily cyclic it follows that if an S(5) is of order 5 and an S(7) is of order 7, then if 7 divides the order of N(5) then also 5 divides the order of N(7) and conversely.

Since an overwhelming fraction of the orders were divisible by a prime p to exactly the first power, most investigations relied on the Brauer theory (6) of modular characters for these. For the most part the computations relied on the principal block $B_0(p)$. Here $C(p) = S(p) \times V(p)$. If $V(p) \neq 1$ the restriction formulae (3.3), (3.4) and (3.5) were very valuable. Example 5 eliminating the order g = 25200 = $16\cdot 9 \cdot 25 \cdot 7$ illustrates several of these principles, including the use of the Brauer-Fowler formula.

Example 6 shows how this theory is useful in constructing the simple groups when they exist. For g = 29120 = $64\cdot 5\cdot 7\cdot 13$, there is a unique simple group, the Suzuki group $Su(8)$. The Brauer theory makes the construction of the complete character table easy. From this table we are then able to deduce that G has a doubly transitive permutation representation on 65 letters. We can then construct this permutation representation and thus prove the existence and uniqueness of a simple group of this order. Z. Janko **[25]** has shown how to use the character table of his group to construct it as a matrix group of dimension 7 over $GF(11)$.

5. Examples of application of the general theory.

EXAMPLE 1. ***g is a multiple of p = 59.*** Here g = $59(1+59r)qw$, $q \geqslant 2$. Thus $r \leqslant 143$. In the formula (3.11) $h \leqslant 4$. r = $F(59, u, h)$. There are 9 combinations (h, u, r) satisfying (3.11).

(h, u, r)	$(p-1)(1+rp)$	$= (1+up)(vp-1)$,	$g = (1+rp)pqw$
(1, 1, 31)	58.1830	= 60.1769,	g = 107,970qw
(1, 28, 85)	58.5016	= 1653.176,	g = 295,944qw
(1, 57, 115)	58.6786	= 3364.117,	g = 400,374qw
(2, 1, 61)	58.3600	= 60.3480,	g = 212,400qw
(2, 3, 92)	58·5429	= 178.1769,	g = 320,311qw
(2, 28, 142)	58.8379	= 1653.294,	g = 494,361qw

$$\begin{array}{llll} (3,1,91) & 58.5370 & = 60.5191, & g = 316{,}830qw \\ (3,2,\ 121) & 58.7140 & = 119.3480, & g = 421{,}260qw \\ (4,\ 1,\ 121) & 58.7140 & = 60.6902, & g = 421{,}260qw \end{array}$$

The last two give the same value of r so that we are dealing with a triple factorization

$$58.7140 = 60.6902 = 119.3480.$$

In every case then we have $qw \leqslant 9$ and so necessarily $q = 2$. We have shown that we need consider only values of g which are multiples of 168 or 48. We consider the factorization of $1+rp$.

$$\begin{aligned} 1830 &= 2\cdot3\cdot5\cdot61 \\ 5016 &= 8\cdot3\cdot11\cdot19 \\ 6786 &= 2\cdot81\cdot43 \\ 3600 &= 16\cdot9\cdot25 \\ 5429 &= 61\cdot89 \\ 8379 &= 9\cdot49\cdot19 \\ 5370 &= 2\cdot3\cdot5\cdot179 \\ 7140 &= 4\cdot3\cdot5\cdot7\cdot17 \end{aligned}$$

In order that g be a multiple of 168 or 48, with the possible values of qw making $g < 1{,}000{,}000$, we need consider only $1+rp = 1830$, $q = 2$, $w = 4$; $1+rp = 5016$, $q = 2$, $w = 1$; $1+rp = 3600$, $q = z$, $w = 1$ or 2; $1+rp = 7140$, $q = 2w = 1$.

The basic relations (3.2) on the degrees of $B_0(59)$ reduce here to

$$1+\delta_0 f_0+\delta_1 f_1 = 0, \quad \delta_1 f_1 \equiv 1, \delta_0 f_0 \equiv -2(59),$$
$$f_0 \mid 2(1+rp), \quad f_1 \mid 2(1+rp), \quad f_0, f_1 > 29. \tag{5.1}$$

For the four possible values for $1+rp$ we find degrees satisfying (5.1) only in the first and last cases.

$$\begin{array}{ll} 1830\ S(59)\text{'s} & 1-61+60 = 0 \\ 7140\ S(59)\text{'s} & 1-120+119 = 0 \end{array} \tag{5.2}$$

For 1830 $S(59)$'s, since the degree 60 is less than $2p = 118$, the Stanton condition (8) requires $w = 1$, but this is in conflict with the condition that g be a multiple of 4. Hence we may exclude 1830 $S(59)$'s. The only case remaining is that of 7140 $S(59)$'s, $q = 2$, $w = 1$ and we have

$$g = 7140\cdot59\cdot2 = 842{,}520 = 8\cdot3\cdot5\cdot7\cdot17\cdot59,$$
$$|N(59)| = 118 = 2.59, \quad q = 2, \; w = 1. \tag{5.3}$$

Degrees in $B_0(59)$: $1-120+119 = 0$.

Here a group of order $17\cdot59$ is necessarily Abelian and so since $17 \nmid |N(59)|$ it follows that $59 \nmid |N(17)|$. The only possible numbers of $S(17)$'s are easily found to be

$$15.59 = 885 \ S(17)\text{'s with } |N(17)| = 8\cdot 7\cdot 17$$
$$168.59 = 9912 \ S(17)\text{'s with } |N(17)| = 5\cdot 17.$$

If $|N(17)| = 5.17$, then S(17) is in the center of its normalizer and by the Burnside condition (9) $\boldsymbol{b}$ has a normal 17 complement. We may exclude this. An S(2) of order 8 is necessarily the elementary Abelian group because of (2) and (4) and so with $N(17)| = 8\cdot 7\cdot 17$ we must have $q = 2$, w = 28 for $N(17)$. Thus the relations (3.2) reduce to

$$1+\delta_0 f_0+\delta_1 f_1 = 0, \quad \delta_0 f_0 \equiv -2(17), \quad \delta_1 f_1 \equiv 1(17) \qquad (5.4)$$

and f_0, f_1 divide $2\cdot 885 = 2\cdot 3\cdot 5\cdot 59$, $f_i < 8$. No such divisors exist and so we may exclude 885 $S(17)$'s. We conclude that no simple group of this order exists. This completes the elimination of all orders which are multiples of 59.

Example **2. *Block separation.***

$$g = 783216 = 16\cdot 27\cdot 49\cdot 37, \ 5292 \ S(37)\text{'s}, \ q = 4, \ w = 1.$$

Degrees in $B_0(37)$: 1-189+2(112)-36 = 0.

Here $\delta_0 f_0$ = − 189, $\delta_1 f_1 = \delta_2 f_2 = 1\ 12$, $\delta_3 f_3$ = -36.

Here there are $(37-1)/4 = 9$ 37-conjugate characters of degree 189, and in $B_0(37)$ two characters of degree 112 and one of degree 36. The characters of degree 189 and 112 are of 7-defect 1. For any 37-regular element x we have by (3.12)

$$1 - \chi_{189}(x) + \chi_{112}^{(1)}(x) + \chi_{112}^{(2)}(x) - \chi_{36}(x) = 0. \qquad (5.5)$$

The characters of degrees 189 and 112 belong to 7-blocks of defect 1, those of degree 1 and 36 to 7-blocks of defect 2. Hence by block separation as given in Lemma 2 in (11) of § 3 we must have

$$1-\chi_{36}(1) = 1\text{-}36 = -35 \equiv 0 \pmod{49}$$

But this is a conflict and so there is [no simple group of order g. (All other possibilities were eliminated by more elementary arguments.)

Example **3. *The Stanton condition***

$$g = 92400 = 16\cdot 3\cdot 25\cdot 7\cdot 11.$$

For $p = 11$ the only number of $S(11)$'s for which degrees satisfying (3.2) exist is 210 $S(11)$'s. Here $|N(11) = 440 = 8\cdot 5\cdot 11$.

For $q = 2$ the degrees $1 + \delta_0 f_0 + \delta_2 f_2 = 0$ are $1+20-21 = 0$.

For $q = 5$ degrees are $1 + \delta_0 f_0 + \delta_2 f_2 + \delta_3 f_3 + \delta_4 f_4 + \delta_5 f_5 = 0$, where $\delta_0 f_0$ = 6, 50, or 105 and $\delta_i f_i$ = 210, -175, 100 -21, 12, -10.

For $q = 10$ degrees are $1 + \sum_{i=1}^{10} \delta_i f_i = 0$

with $\delta_i f_i$ = 210, -175, 100, -21, 12, -10.

For $q = 5$ or $q = 10$ there is in every instance a degree 10 or 12.

By the Stanton principle quoted in (8) since there is in every instance a character in $B_0($ 11) of degree less than $2p = 22$ in $g = p(1+rp)qw$ we must have w = 1. But here $qw = 40$ and so for $q = 2$, $w = 20$; $q = 5$, w = 8 ; $q = 10$, w = 4. Hence the condition is violated and there is no simple group of order g = 92400.

Example 4. ***The Brauer method for groups divisible by*** p^2.

$$g = 202800 = 16\cdot 3\cdot 25\cdot 169$$

Numbers of the form $1 + 13k$ dividing g are 1, 40, 300. By the Brodkey argument (5) as 40< 169 we cannot have 40 S(13)'s. Suppose we have 300 S(13)'s and $|N(13)| = 676 = 4\cdot 169$. As $300 = 1+23\cdot 13$, and $23 \not\equiv 0$ (13), if P_0 is an S(13) there must be a P_1 with $[P_0 : P_0 \cap P_1] = 13$. Write $P_0 \cap P_1 = K$. In the notation of (3.14)

$$300r_K = (1+ 13b_K)[G : No(K)]. \tag{5.6}$$

As $1 < 1 + 13b_K < 300$ and as $(1 + 13b_K)/g$ its only possible value is $40 = 1+3\cdot 13$. Hence

$$300r_K = 40[G : N_G(K)] \tag{5.7}$$
$$15r_K = 2[G : \mathrm{No(K)}].$$

Here (3.15) takes the form

$$299 = 13 \sum_K r_K b_K + a\cdot 169 \tag{5.8}$$
$$23 = \sum_K r_K b_K + 13a.$$

But $1+b_K 13 = 40$ and so $b_K = 3$ in every case and from (5.7) it follows that r_K is even. Thus in (5.8) a is odd and 13a < 23 and so $a = 1$ giving $23 = \sum_K 3r_K + 13$ whence $3 \mid 23 - 13 = 10$ which is false. We have reached a conflict and conclude that there is no simple group of order 202 800.

An alternate argument applicable here rests on showing that no group contains exactly 40 S(13)'s. From the writer's result (14), since 40 is not a prime power and 40 has no proper factorization $40 = (1 + 13r)(1+13s)$, it follows that if there is a group with 40 S(13)'s then there is a simple group with 40 S(13)'s. Since 40 < 169 there is no simple group G with 40 S(13)'s if $13^2 | g$, by the Brodkey argument (5). If g = $40\cdot 13qw$, since $12\cdot 40$ does not have a further factorization $(13u+ 1)(13v- 1)$, the Brauer-Reynolds argument (11) shows that there is no simple group of such an order, as $13-1$ is not a power of 2 and $PSL_2(13)$ has 13 + 1 = 14 S(13)'s. Hence no group has 40 S(13)'s. Thus it is impossible that $H_1(K)$ has 40 S(13)'s in the above argument.

Example 5. $g = 25200 = 16\cdot 9\cdot 25\cdot 7.$

For $p = 7$ the admissible Sylow numbers and orders of N(7) are as follows :

$$\begin{aligned}
&36\ S(7)\text{'s}, && |N(7)| = 700 = 4\cdot 25\cdot 7\\
&50\ S(7)\text{'s}, && |N(7) \ = 504 = 8\cdot 9\cdot 7\\
&120\ S(7)\text{'s}, && |N(7)| = 210 = 2\cdot 3\cdot 5\cdot 7\\
&225\ S(7)\text{'s}, && |N(7)| = 112 = 16.7\\
&400\ S(7)\text{'s}, && |\mathrm{N}(7)| = 63 = 9\ \cdot 7\\
&1800\ S(7)\text{'s}, && |N(7)| = 14 = 2.7
\end{aligned}$$

We shall handle these separately. Except for 1800 $S(7)$'s we have $w > 1$. In $B_0(7)$ for 36 or 50 $S(7)$'s we have a character of degree 6 or 8 in every case. By the Stanton condition in (8) we may exclude 36 or 50 $S(7)$'s. For 120 $S(7)$'s, $|N(7) = 2\cdot 3\cdot 5\cdot 7$ and there are characters of degree 6 or 8 to be excluded by the Stanton condition except for

$q = 2$, $w = 15$, degrees $1-16+15 = 0 \quad (1+\delta_0 f_0+\delta_2 f_2 = 0)$;
$\boldsymbol{q = 6}$, $\boldsymbol{w = 5}$, degrees

$$\begin{aligned}
&1-48+2(36)+2(-20)+15 = 0,\\
&\text{if } 120+2(-48)+2(-20)+15 = 0.
\end{aligned}$$

In all three cases we have a single character of degree 15, which is therefore necessarily rational. Hence on restriction to V(7) (writing χ_{15} for a character of degree 15)

$$\chi_{15} \mid V(7) = \sigma_0 + 7\ \mu_2. \tag{5.9}$$

Here σ_0 is the identity character for V(7) and μ_2 a character of degree 2, necessarily rational since χ_{15} is. But by the Schur result (3.13) a rational character of degree 2 can represent a group whose g order is divisible by at most $2^3\cdot 3 = 24$ and by no prime $\boldsymbol{p} \geq 5$. But w = 15 or 5 and this conflicts with the Schur result if V(7) is to be faithfully represented, as it must be if G is simple.

For 225 $S(7)$'s $|N(7)| = 112 = 16\cdot 7$ we must have $\boldsymbol{q} = 2$, $w = 8$ and as the only degrees possible are if $5 - 6 = 0$ the Stanton condition excludes this. Again for 400 $S(7)$'s, $|N(7)| = 63 = 9.7$, we must have $\boldsymbol{q = 3}$, $w = 3$ and the degrees are all excluded by the Stanton condition.

For 1800 $S(7)$'s $|N(7)| = 14 = 2.7$ we have $\boldsymbol{q} = 2$, $w = 1$. The possible degrees $1 + \delta_0 f_0 + \delta_2 f_2 = 0$ are:

$$\begin{aligned}
1+5-6 &= 0,\\
1-16+15 &= 0,\\
1-\ 9+\ 8 &= 0.
\end{aligned} \tag{5.10}$$

The first case may be excluded by Schur's result since the rational character χ_6 cannot faithfully represent a group whose order is divisible by 25.

Here N(7) has the following defining relations: $a^7 = 1$, $b^2 = 1$, $\boldsymbol{bab} = a^{-1}$. The table of characters for N(7) is as follows:

$c(x)$	14	7	7	7	2
$h(x)$	1	2	2	2	7
x	1	a	a^2	a^3	b
λ_0	1	1	1	1	1
Al.	1	1	1	1	- 1
μ_1	2	η_1	η_2	η_3	0
μ_2	2	η_2	η_3	η_1	0
μ_3	2	η_3	η_1	η_2	0

(5.11)

x is an element, h(x) the number of conjugates of x, c(x) the order of C,(x). Here $\eta_1 = \varepsilon + \varepsilon^{-1}$, $\eta_2 = \varepsilon^2 + \varepsilon^{-2}$, $\eta_3 = \varepsilon^3 + \varepsilon^{-3}$, where ε is a primitive 7th root of unity, and $\eta_1 + \eta_2 + \eta_3 = -1$

From the Brauer results (3.3) the other degrees in (5.10) correspond to the following characters in G:

$c(x)$	g	7	7	7	
$h(x)$	1	3600	3600	3600	
x	1	a	a^2	a^3	b
ϱ_0	1	1	1	1	1
ϱ_1	15	1	1	1	
θ_1	16	η_1	η_2	η_3	
θ_2	16	η_2	η_3	η_1	
θ_3	16	η_3	η_1	η_2	

(5.12)

$c(x)$	g	7	7	7	
$h(x)$	1	3600	3600	3600	
x	1	a	a^2	a^3	b
ϱ_0	1	1	1	1	1
ϱ_1	8	1	1	1	
θ_1	9	η_1	η_2	η_3	
θ_2	9	η_2	η_3	η_1	
θ_3	9	η_3	η_1	η_2	

(5.13)

Since $g = 25200 = 16 \cdot 9 \cdot 25 \cdot 7$, the characters in (5.12) θ_1, θ_2, θ_3 are of highest type for $\boldsymbol{p} = 2$ and so vanish for $\boldsymbol{b}$, a 2-singular element. All further characters for G have degrees multiples of 7 and vanish for $\boldsymbol{a}$, a^2, and a^3.

Hence, by orthogonality between the a column and the b column in (5.12), $\varrho_1(b) = -1$. By the Brauer-Fowler formula in (3.17) we have $c_{ijk} = 7$ if $x_i = x_j = b$ and $x_k = a$. Here this gives

$$7 = \frac{25200}{c(b)^2}\left(1+\frac{1}{15}\right). \tag{5.14}$$

This gives $c(b)^2 = 3840$ which is a conflict since 3840 is not a square. Hence we may exclude the degrees in (5.12).

For the degrees in (5.13) if we restrict ϱ_1 to N(7) we see, from the values $\varrho_1(1) = 8$, $\varrho_1(a) = 1$, that we must have

$$\varrho_1 \,|\, N(7) = \lambda_i + \lambda_j + \mu_1 + \mu_2 + \mu_3, \tag{5.15}$$

where λ_i and λ_j are any combination of λ_0 and λ_1. We conclude that

$$\varrho_1(b) = 2, 0, -2. \tag{5.16}$$

The matrix $M(b)$ which has $\varrho_1(b)$ as its trace has 8 eigenvalues which are $+1$ or -1, say r (+ 1)‘s and t (– 1)’s, where $r + t = 8$. The determinant of $M(b)$ (which may be taken in diagonal form) is (– 1)‘. As the determinant of M is a one-dimensional representation of G, which is simple, it must be 1 for every element. Hence t is even and $\varrho_1(b) = r - t = 8 - 2t \equiv 0 \pmod 4$. Thus $\varrho_1(b) \equiv 0 \pmod 4$ and from (5.16) this makes $\varrho_1(b) = 0$. The 7-conjugate characters $\theta_1, \theta_2, \theta_3$ are equal for b and so, by orthogonality with the a-column, $\theta_1(b) = \theta_2(b) = \theta_3(b) = 1$. In this case with $x_i = x_j = b$, $x_k = a$ the Brauer-Fowler formula becomes

$$7 = \frac{25200}{c(b)^2} = \left(1-\frac{1}{9}\right), \tag{5.17}$$

giving $c(b)^3 = 3200$ which is not a square, and so the degrees (5.13) are also to be excluded.

Thus every possibility has been excluded and we conclude that there is no simple group of order 25200.

There are other cases, not illustrated here, in which the restrictions to $V(p)$ such as $\chi_{15} | V(7) = \sigma_0 + 7\psi_2$ are very useful. For example if there is an involution τ in V(7) we must have $\mu_2(\tau) = -2$ in order for the determinant to be $+1$. In this case τ is the only involution in V(7) and so in the center of N(7). Also $\chi_{15}(\tau) = -13$ and so $c(\tau) > 169$. If say $|N(7)| = 84$, then $H = C_G(\tau)$ properly contains N(7). This may force H to be G or to contain a number of $S(7)$'s such as 15, which is impossible by the writer's results in (14).

EXAMPLE 6. The Suzuki group.

$$g = 29120 = 64 \cdot 5 \cdot 7 \cdot 13.$$

Here the Suzuki group $Su(8)$ of order $29120 = 64\cdot 5\cdot 7 \cdot 13$ will be constructed directly from its order using the Brauer theory of modular characters.

The only divisors of g of the form $1 + 13k$ are 14, 40, and 560. By the Brauer-Reynolds results (1 1), 14 $S(13)$'s is possible only for $PSL_2(13)$. There is no further factorization $12\cdot 40+(13u+1)(13v-1)$ so that 40 $S(13)$'s is impossible. For 560 $S(13)$'s we have the factorizations $6720 = 12\cdot 560 = 14\cdot 480 = 40.168 = 105\cdot 64$. Here $|N(13)|=52=4\cdot 13$. For $q = 2$ there are no degrees $1 + \delta_0 f_0 + \delta_2 f_2 = 0$ with $f_i|2\cdot 560$, $\delta_0 f_0 \equiv - 2(13)$, $\delta_2 f_2 \equiv 1(13)$. For $q = 4$ we have $1+\delta_0 f_0+\delta_2 f_2+\delta_3 f_3+\delta_4 f_4 = 0$ with $f_i|4\cdot 560$ and $\delta_0 f_0 \equiv -4(13)$, $\delta_i f_i \equiv 1(13)$, $i = 2, 3, 4$. Here the possible values for $\delta_0 f_0$ are -4, -160, -56, 35 of which the 4 is too small since $4<\frac{1}{2}(13-1) = 6$. For $\delta_i f_i$ the possible values are 560, 14, 40, $-$ 64. Since one of thef's must be odd we must have $\delta_0 f_0 = 35$, and we find the only combination to be

$$1+35-64+2(14) = 0. \qquad (5.18)$$

As $7 \nmid |N(13)|$ it now follows that $13 \nmid |N(7)|$ and so the number of $S(7)$'s is a multiple of 13. For S(7) we must have $q = 2$ since 3 does not divide g. Here $1 + \delta_0 f_0 + \delta_2 f_2 = 0$ with $\delta_0 f_0 \equiv$ -2 (mod 7), $\delta_1 f_1 \equiv 1$ (mod 7). As degrees not in (5.18) are multiples of 13 this forces $\delta_2 f_2 = 64$, and so we have $\delta_0 f_0 = - 65$ and the S(7) degrees are

$$1-65+64 = 0. \qquad (5.19)$$

Since these degrees must divide $q(1 + rp) = 2(1 + 7r)$ the only possibility is $1 + 7r = 65 \cdot 32 = 2080$ $S(7)$'s, $N(7) = 14$, $q = 2$ $w = 1$. Since degrees not in (5.18) or (5.19) are multiples of both 7 and 13, and as g = 29120 is the sum of the squares of all degrees, there is exactly one further irreducible character and this is of degree 91.

At this stage we have a partial character table for G, where an $S(13) = (a)$ with $a^{13} = 1$ and $N(13)$ is defined by

$$a^{13} = 1, \quad b^4 = 1, \quad b\text{-}lab = a^5. \qquad (5.20)$$

There are three classes of elements of order 13 with representatives a, a^3, a^9 and as $c(a) = 13$ each of these contains 2240 elements. For an S(7) = (c) we have as defining relations for N(7)

$$c' = 1, \quad x^2 = 1, \quad xcx = c^{-1},! \qquad (5.21)$$

and each of the three classes with representatives c, c^2, c^3 contains 4160 elements. The partial table follows:

$c(x)$	g	13	13	13	7	7	7
$h(x)$	1	2240	2240	2240	4160	4160	4160
x	1	a	a^3	a^9	c	c^2	c^3
ϱ_0	1	1	1	1	1	1	1
ϱ_1	64	- 1	- 1	- 1	1	1	1
ϱ_2	14	1	1	1	0	0	0
ϱ_3	14	1	1	1	0	0	0
ϱ_4	35	$-u_1$	$-u_2$	$-u_3$	0	0	0
ϱ_5	35	$-u_2$	$-u_3$	$-u_1$	o	0	0
ϱ_6	35	$-u_3$	$-u_1$	$-u_2$	0	0	0
e7	65	0	0	0	v_1	v_2	v_3
ϱ_8	65	0	0	0	v_2	v_3	v_1
ϱ_9	65	0	0	0	v_3	v_1	v_2
ϱ_{10}	91	0	0	0	0	0	0

(5.22)

Here the u's are Gauss sums of 13th roots of unity, the v's of the 7throots ofunityand $u_1+u_2+u_3 = v_1+v_2+v_3 = -1$.

For an S(5) we have $q = 2$ or $q = 4$. If $q = 2$ the degrees are $1 + \delta_0 f_0 + + \delta_2 f_2 = 0$ with $\delta_2 f_2 \equiv 1 \pmod 5$ and $\delta_0 f_0 \equiv -2 \pmod 5$. There are no such degrees and so we have $q = 4$ and the degrees satisfy $\delta_i f_i \equiv 1 \pmod 5$. The only possibility is

$$1-64+2(-14)+91 = 0. \tag{5.23}$$

All other characters are of degrees multiples of 5. Hence for N(5) we have $q = 4$, $w = 1$,

$$d^5 = 1,\ y^4 = 1,\ y^{-1}dy = d^2. \tag{5.24}$$

The degrees in (5.23) serve as a partial confirmation that a group of the order may exist. As (5.23) is the relation ondegrees for $B_0(5)$ with $q = 4$, and necessarily $w = 1$ since all other degrees are of highest type for $q = 5$, we must have 1456 $S(5)$'s and so d has $c(d) = 5$ and then $h(d) = 5824$. Also $\varrho_0(d) = 1$, $\varrho_1(d) = -1$, $\varrho_2(d) = -1$ and $\varrho_{10}(d) = 1$, while $\varrho_i(d) = 0$ for the remaining characters.

There are 11 distinct irreducible characters for G, the two of degree 14 being complex conjugates from considerations of the tree for $B_0(13)$ as given by (5.18) or $B_0(5)$ as given by (5.23). Hence there are exactly 11 conjugate classes of elements in G with representatives 1, a, a^3, a^9, c, c^2, c^3, d for eight of these and three other classes of which b and b^2 from (5.20) must be two. As b^2 is of order two each of its characters is a sum of + 1's and − 1's and so real. All characters in (5.22) are real as are also the characters of d. If the characters of b were all real then by orthogonality all characters would be real, contrary to the fact that ϱ_2 and ϱ_3 are complex conjugates. Thus some character of b is complex and its complex conjugate is the character of b^{-1}. Hence b^2, b and b^{-1} are representatives of the three remaining classes. It remains to determine their characters. We shall first give the complete table and then say how (5.22) was completed. Here is the full table.

$$g = 29120 = 64\cdot5\cdot7\cdot13$$

$c(x)$	g	13	13	13	7	7	7	5	64	16	16
$h(x)$	1	2240	2240	2240	4160	4160	4160	5824	455	1820	1820
x	1	a	a^3	a^9	c	c^2	c^3	d	b^2	b	b^{-1}
ϱ_0	1	1	1	1	1	1	1	1	1	1	1
ϱ_1	64	-1	-1	-1	1	1	1	-1	0	0	0
ϱ_2	14	1	1	1	0	0	0	-1	-2	$2i$	$-2i$
ϱ_3	14	1	1	1	0	0	0	-1	-2	$-2i$	$2i$
ϱ_4	35	$-u_1$	$-u_2$	$-u_3$	0	0	0	0	3	-1	-1
ϱ_5	35	$-u_2$	$-u_3$	$-u_1$	0	0	0	0	3	-1	-1
ϱ_6	35	$-u_3$	$-u_1$	$-u_2$	0	0	0	0	3	-1	-1
$e7$	65	0	0	0	v_1	$v2$	v_3	0	1	1	1
ϱ_8	65	0	0	0	$v2$	$v3$	v_1	0	1	1	1
ϱ_9	65	0	0	0	v_3	v_1	$v2$	0	1	1	1
ϱ_{10}	91	0	0	0	0	0	0	0	-5	-1	-1

(5.25)

As there is only one class of involutions, namely $\tau = b^2$, we may apply the Brauer-Fowler formula three times, namely for $B_0(13)$, $B_0(7)$, and $B_0(5)$, to τ. As ϱ_1 of degree 64 is of highest type for $p = 2$, then $\varrho_1(\tau) = 0$ and so for $B_0(7)$ with degrees $1 - 65 + 64 = 0$ we find by orthogonality $\varrho_7(\tau) = \text{es(z)} = \varrho_9(\tau) = 1$ and the Brauer-Fowler formula becomes

$$7 = \frac{29120}{c(\tau)^2}\left(1-\frac{1}{65}\right), \tag{5.26}$$

yielding $$c(\tau)^2 = 4096, \quad c(\tau) = 64.$$

As σ_2 and σ_3 are complex conjugates but real for τ we put $\varrho_2(\tau) = \varrho_3(\tau) = x$. Also $\varrho_4(\tau) = \varrho_5(\tau) = y$ as these are algebraic conjugates but rational for τ. We already have $\varrho_7(\tau) = \varrho_8(\tau) = 1$ and $\varrho_{10}(\tau) = \text{z}$. Orthogonality with the columns for a and d and the order of $c(\tau)$ give

$$\begin{gathered} 1+2x+y = 0, \\ 1-2x+z = 0, \\ 1+2x^2+3y^2+3+z^2 = c(\tau) = 64. \end{gathered} \tag{5.27}$$

This leads to $18x^2+8x-56 = 0$ whose roots are x = -2 and x $= 14/9$. Since x is a rational integer it **is** $x = \varrho_2(\tau) = \varrho_3(\tau)$ = -2 and the characters for $b^2 = \tau$ are completely determined.

The remaining 3640 elements are equally divided between the classes for $\boldsymbol{b}$ and b^{-1} since $\boldsymbol{c(b)} = \boldsymbol{c}(b^{-1})$ whence there are 1820 in each and $\boldsymbol{c(b)} = c(b^{-1}) = 16$. As all characters except ϱ_2 and ϱ_3 are real we have $\varrho_i(b) = \varrho_i(b^{-1})$ in all other cases and row orthogonality determines all of these. Complex conjugacy and the fact that $\boldsymbol{c(b)} = 16$ determines ϱ_2 and ϱ_3 for $\boldsymbol{b}$ and b^{-1}.

From the table of characters we see that S(2) is non-Abelian since $c(b) = 16$, and so the center Z(2) of S(2) is of order 2, 4, or 8. An element of order 5 or 13 in N(2) would normalize and so centralize Z(2) contrary to the fact that C(5) = S(5) and C(13) = S(13). Hence the number of $S(2)$'s is a multiple of 65 and so is either 65 or 455. If the number were 455, since $455 \not\equiv 1 \pmod 4$ there would be two $S(2)$'s $P_0 \cap P_2 = K$ where Kis of order 32 and $N_G(K)$contains an odd number of $S(2)$'s. As $32-1 = 31$ is not a multiple of 5, 7, or 13 an element of odd order normalizing Kcentralizes some 2-element, contrary to the fact C(5) = S(5), C(7) = $S(7)$and C(13) = S(13). Hence the number of $S(2)$'s is not 455 but is 65 and N(2) is of order 64.7 and is a Frobenius group as C(7) = S(7). Thus S(2) has a center Z(2) of order 8 and $S(2)/Z(2)$ is also of order 8 and both are acted upon by S(7) without fixed points. Each of 65 $S(2)$'s has 63 elements besides the identity giving 4095 2-elements which must be distinct since G has 455 involutions and 3640 elements of order 4. Hence the S(2)'s have trivial intersection and in the representation of G on the 65 cosets of N(2), every 2-element fixes exactly one letter. G_1 = N(2) is a Frobenius group on the 64 letters it moves, being the regular representation of S(2) normalized by an element $\boldsymbol{c}$ of order 7.

An automorphism $\boldsymbol{m}$ of order 7 on an elementary Abelian group of order 8 satisfies either $x^{m^3+m+1} = 1$ or $x^{m^3+m^2+1}= 1$ for every element. The group S(2) of order 64 is determined up to isomorphism by the fact that it is non-Abelian and has a center Z(2) and factor group $S(2)/Z(2)$ both elementary of order 8 and having an automorphism of order 7 which is fixed point free. Here c, of order 7, induces the automorphism, and on $S(2)/Z(2)$, we have the relation $x^{c^3+c+1} = 1$ and on $Z(2)$ $x^{c^3+c^2+1} = 1$. If the same relation held in both places S(2) would be Abelian. Interchanging the relations amounts to replacing c by c^{-1}.

Take $b_1 = \boldsymbol{b}$ of order 4 and $b_1^2 = e_1$ is in Z(2). The automorphism induced by c $(x \to c^{-1}xc)$ is given by

$$\begin{array}{ll} b_1 \to b_2, & e_1 \to e_2, \\ b_2 \to b_3, & e_2 \to e_3, \\ b_3 \to b_1b_2, & e_3 \to e_1e_3. \end{array} \tag{5.28}$$

These give rise to relations

$$\begin{aligned} b_1^2 &= e_1 = (b_2, b_3), \\ b_2^2 &= e_2 = (b_1, b_3)(b_2, b_3), \qquad (5.29) \\ b_3^2 &= e_3 = (b_1, b_2)(b_1, b_3)(b_2, b_3), \end{aligned}$$

using the commutator notation $(x, y) = x^{-1}y^{-1}xy$.

We may now give the permutations on letters 0, . . . , 63 generating N(2).

c = (0)(1, 2, 3,4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14)(15, 16, 17, 18, 19, 20, 21) (22, 23, 24, 25, 26, 27,28)(29,30,31,32,33,34, 35)(36,37,38,39,40,41,42) (43,44,45,46, 47, 48, 49)(50 51,52,53,54,55,56)(57,58,59,60,61,62,63).

$b = b_1 =$ *(0, 8,* 1, 15)(2, 22, 6, 50)(3, 29,4, 36)(5, 43, 7, 57)(9, 39, 58, 25) (10,28, 52, 14)(11, 37,46, 51)(12, 62, 40, 27)(13, 33, 34, 19)(16, 60, 44, 18) (17,49, 24,42)(20,61, 41, 54)(21,45, 56, 31)(23, 53, 30, 32)(26,48, 47, 55) (35, 59, 63, 38).

(5.30)

The Suzuki group G will be obtained by adjoining **a** further letter ∞ and finding an involution τ (necessarily conjugate to b^2) interchanging ∞ and 0 and so normalizing the group (c). τ must also have the property that for any u $\in G_\infty$ = N(2) $\tau u \tau = x \tau y$ for appropriate x, $y \in$ N(2). With a certain amount of trial this determines τ (up to a conjugate by c) as

τ = (∞, 0)(1, 57)(2, 63)(3, 62)(4, 61)(5, 60)(6, 59)(7, 58)(8, 26)(9,25) (10,24)(11, 23)(12, 22)(13, 28)(14, 27)(15, 37)(16, 36)(17, 42)(18, 41) (19,40)(20, 39)(21, 38)(29, 52)(30, 51)(31, 50)(32, 56)(33, 55)(34, 54) (35, 53)(43)(44, 49)(45, 48)(46,47). (5.31)

6. **Construction of a new simple group of order** 604,800. In his announcement "Still one more new simple group of finite order" Zvonimir Janko gives a character table for a simple group of order 604,800 if such a group exists. In this group there are two classes of involutions, one with a centralizer of order 1920, the other with a centralizer of order 240. He gives the character table for such a group.

The group has 21 classes and three of the characters are as follows:

Order of an element	1	2	4	8	6	12	10	10	2	6	10	10
Order of centralizer	g	1920	96	8	24	12	10	10	240	12	20	20
ψ_1	1	1	1	1	1	1	1	1	1	1	1	1
ψ_8	36	4	40	1	1	−1	−1	0	0	0	0	
ψ_{10}	63	15	3	1	0	0	0	0	-1	-1	-1	-1
$\psi_1+\psi_8+\psi_{10} = \chi$	100	208222	0	0	0	0	0	0				

3	3	5	5	5	5	15	15	7
1080	36	300	300	50	50	15	15	7
1	1	1	1	1	1	1	1	1
9	0	-4	-4	1	1	-1	-1	1
0	3	3	3	-2	-2	0	0	0
10	3	0	0	0	0	0	0	2

(6.1)

Under the assumption that χ is the character of a group G of order 604,800 represented as a permutation group on 100 letters, the group G will be constructed and it will be shown that G is simple.

The stabilizer of a letter G_α is of order 6048. From the fact that an S(7) is its own centralizer it is not difficult to show that G_α must be the simple group $U_3(3)$. As χ is the sum of three irreducible characters of G it follows that G_α has precisely two orbits besides the fixed letter α, and in D. G. Higman's terminology, G is a rank three group.

In $GF(3^2)$ the mapping $x \rightarrow x^3 = \bar{x}$ is an involutory automorphism. The unitary group $U_3(3)$ consists of the linear transformations over $GF(3^2)$ on x, y, z leaving invariant for points A = (x, y, z) the metric

$$(\mathrm{A}, \mathrm{A}) = x\bar{x}+y\bar{y}+z\bar{z}. \qquad (6.2)$$

A natural representation for $H = U_3(3)$ is as a permutation group on the 28 points A for which (A, A) = 0 considering these as points in the projective plane PG(2, 33. These lie in sets of four on 63 lines and form a block design D with parameters $b = 63$, v = 28, $r = 9$, $k = 4$, A = 1. Number the points 1, . . ., 28 and the lines 37, . . . , 99 we have for the set of lines containing the point 1

L_{37}:	1, 2, 3, 4
L_{44}:	1, 5, 18, 28
L_{51}:	1, 6, 14, 23
L_{58}:	1, 7, 15, 22
L_{65}:	1, 8, 19, 25
L_{72}:	1, 9, 16, 27
L_{63}:	1, 10, 17, 24
L,:	1, 11, 20, 21
L_{41}:	1, 12, 13, 26

(6.3)

Here *His* generated by the permutations

$$\begin{aligned}a = {} & (1, 5, 7, 3, 12, 24, 11)(2, 23, 4, 27, 13, 14, 26)(6, 20, 18, 8, 25, 21, 28)\\ & (9, 10, 17, 15, 22, 16, 19),\\ b = {} & (1)(2)(3, 4)(5, 17, 7, 16, 8, 20, 6, 13)(9, 19, 11, 14, 12, 18, 10, 15)\\ & (21, 23, 26, 28, 24, 22, 27, 25).\end{aligned} \tag{6.4}$$

The Sylow 7-group (a) is normalized by the element c and $N(7) = (a, c)$ where

$$\begin{aligned}c = {} & (1)(2, 20, 10)(3, 11, 24)(4, 21, 17)(5, 7, 12)(6, 19, 27)(8, 16, 23)\\ & (9, 14, 25)(13, 18, 15)(22, 26, 28).\end{aligned} \tag{6.5}$$

Here (c) is normalized by the involution d where

$$\begin{aligned}d = {} & (1)(8)(19)(25)(2, 28)(3, 18)(4, 5)(6, 27)(7, 17)(9, 14)(10, 22)(11, 13)\\ & (12, 21)(15, 24)(16, 23)(20, 26).\end{aligned} \tag{6.6}$$

We shall construct G as a permutation group on the 100 symbols 00,01, . . . , 99 and H shall be the stabilizer G_{00}. From the character χ of (6.1) we see that a 7-element fixes exactly one of the 99 letters moved by H; thus of the two orbits of H on the 99 letters one is a multiple of 7 in length, the other of length congruent to one modulo 7. As both orbit lengths are divisors of 6048, the only possible lengths are 36 and 63. The 63 orbit for H will be on the blocks of D numbered from 37 to 99. The 36 orbit will be on cosets of the subgroup $(a, d\rangle$ of order 168 and isomorphic to $PSL_2(7)$, numbering the cosets from 01 to 36. The permutations representing the elements a, b, c, d are as follows:

a =

$$\begin{aligned}&(00)(01)(02, 03, 04, 05, 06, 07, 08)(09, 10, 11, 12, 13, 14, 15)\\ &\quad (16, 17, 18, 19, 20, 21, 22)(23, 24, 25, 26, 27, 28, 29)\\ &\quad (30, 31, 32, 33, 34, 35, 36)(37, 38, 39, 40, 41, 42, 43)\\ &\quad (44, 45, 46, 47, 48, 49, 50)(51, 52, 53, 54, 55, 56, 57)\\ &\quad (58, 59, 60, 61, 62, 63, 64)(65, 66, 67, 68, 69, 70, 71)\\ &\quad (72, 73, 74, 75, 76, 77, 78)(79, 80, 81, 82, 83, 84, 85)\\ &\quad (86, 87, 88, 89, 90, 91, 92)(93, 94, 95, 96, 97, 98, 99)\end{aligned}$$

b =

(00)(01, 02, 09, 16, 23, 20, 30, 17)(03, 35, 13, 29, 31, 24, 25, 11)
(04, 26, 27, 07)(05, 21, 14, 10)(06, 19, 32, 36)
(08, 18, 28, 22, 15, 12, 33, 34)(37)(38, 92, 67, 77, 99, 89,49, 84)
(39, 59, 82,46, 88, 54, 52, 68)(40, 55,47, 81,75, 95, 61, 78)
(41,44, 63, 58, 72, 65, 50, 51)(42, 76, 53, 93, 86, 80, 79, 57)
(43, 85,48, 70, 96, 83, 66, 94)(45, 97)(56, 87)
(60, 71, 91, 69, 90, 73, 64,74)(62, 98)

c =

(00)(01)(02, 28,21)(03,23, 18)(04,25, 22)(05,27, 19)(06, 29, 16)
(07,24, 20)(08,26, 17)(09, 13, 14)(10, 15, 11)(12)(30, 36, 34)(31)
(32, 33, 35)(37, 50, 63)(38,45, 60)(39,47, 64)(40, 49, 61)(41,44, 58)
(42,46, 62)(43,48, 59)(51, 65, 72)(52, 67, 76)(53, 69, 73)(54, 71, 77)
(55, 66,74)(56, 68, 78)(57, 70, 75)(79, 89,96)(80, 91, 93)(81, 86,97)
(82, 88,94)(83, 90, 98)(84, 92, 95)(85, 87, 99)

d =

(00)(01)(02)(03,05)(04,25)(06)(07, 20)(08, 17)(12)(13)(09,14)(10)(11,15)
(16,29)(18,27)(19, 23)(21,28)(22)(24)(26)(30)(31)(32,35)(33)(34,36)
(37, 44)(38, 88)(39, 64)(40, 90)(41, 50)(42, 95)(43, 97)(45, 82)(46, 92)
(47)(48, 86)(49, 83)(79, 89)(58, 63)(59, 81)(60,94)(61, 98)(62, 84)
(80, 85)(87, 93)(91, 99)(96)(51, 72)(52)(53, 68)(54, 71)(55, 66)(56, 69)
(57)(65)(67, 76)(70, 75)(73, 78)(74)(77)

(6.7)

In $H = G_{00}$ the normalizer of a 7-group is $N_H(7) = \langle \boldsymbol{a},$ c) of order 21. In G the normalizer $N_G(7)$ of a 'I-group is of order 42, and S(7) is its own centralizer in G. Thus in G there is an involution *t* such that $N_G(7) =$ $(\boldsymbol{a}$, c, $t\rangle$ and such that $\boldsymbol{tat} = \boldsymbol{a}^{-1}$. Of the two classes of involutions in G, one fixes 20 of the 100 letters, the other none. Since *(a)* has 2 fixed letters and 14 7-cycles, an involution *u* fixing 20 letters must fix two or more letters in one of the 7-cycles and for such an involution we cannot have $uau = a^{-1}$. Hence the involution *t* in $N_G(7)$ must move all letters. We may choose a conjugate of *t* in $N_G(7)$ so that ***ct*** = ***tc*** is of order 6. We shall determine this permutation ***t***.

Since $\boldsymbol{tat} = \boldsymbol{a}^{-1}$, and *t* moves all 100 letters, *t* interchanges the two letters 00 and 01 fixed by ***a***. Since *tc* = *ct* and *c* fixes exactly the four letters 00, 01, 12, and 31, it follows that *t* also interchanges 12 and 31. Hence, as

$tat = a^{-1}$,

$$\begin{aligned} a &= (09,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15)(30,\ 31,\ 32,\ 33,\ 34,\ 35,\ 36), \\ a\text{-}1 &= (34,\ 33,\ 32,\ 31,\ 30,\ 36,\ 35)(13,\ 12,\ 11,\ 10{,}09,\ 15,\ 14). \end{aligned} \tag{6.8}$$

Thus

$$t = (00{,}01)(09,\ 34)(10,\ 33)(11,\ 32)(12,\ 31)(13,\ 30)(14,\ 36)(15,\ 35). \tag{6.9}$$

At this stage an element of luck enters in. The element tb^2t has a relatively large number of its values determined:

$$tb^2t = \begin{pmatrix} 00, & 01, & 13, & 30, & 32, & 35, & 31, & \ldots \\ 34, & 01, & 00, & 12, & 15, & 10, & 09, & \ldots \end{pmatrix}. \tag{6.10}$$

We now form an element fixing 00:

$$tb^2a^4tb^2t = \begin{pmatrix} 00, & 01, & 13, & 30, & 31, & 32, & 35, & \ldots \\ 00, & 34, & 01, & 10, & 09, & 15, & 12 & , \ldots \end{pmatrix}. \tag{6.11}$$

This is sufficient to determine the permutation completely. It is $a^3b^6ada^3$. Thus t must satisfy

$$tb^2a^4tb^2t = a^3b^6ada^3. \tag{6.12}$$

In permutation form this begins

$$\begin{array}{rl}
t & \begin{pmatrix} 00, 01, & 02, 03, 04, 05, \ldots & \\ 01, 00 & A_i & \end{pmatrix}; \\
b^2a^4 & \begin{pmatrix} 01, 00 & A_i & \\ 13, 00 & A_j & \end{pmatrix}, \\
t & \begin{pmatrix} 13, 00 & A_j & \\ 30, 01 & 05 & \end{pmatrix}, \\
b^2 & \begin{pmatrix} 30, 01, 19, & 05 & 24 \\ 01, 09, 36, & 14 & 11 \end{pmatrix}, \\
t & \begin{pmatrix} & 14 & 11 \\ 00, 34, 14, 36, & 21, & 32 \end{pmatrix}.
\end{array} \tag{6.13}$$

The element t interchanging 00 and 01 normalizes the group $\langle a, d\rangle$ of order 168 fixing 00 and 01. Its orbits are

$$\begin{array}{l}
\{00\}, \\
\{01\}, \\
(09, \ldots, 15\}, \\
(30, \ldots, 36\}, \\
(02, \ldots, 08, 16, \ldots, 22, 23, \ldots, 29\}, \\
(51, \ldots, 57, 65, \ldots, 71, 72, \ldots, 78\}, \\
(37, \ldots, 43, 44, \ldots, 50, 58, \ldots, 64, 79, \ldots, 85, 86, \ldots, 92, 93, \ldots, 99).
\end{array} \tag{6.14}$$

Since t moves all letters it must interchange the orbits of odd length. In particular if $t = (03, A_i)$ then A_i is one of the numbers 51,. . . ,57,65,. . , ,71, 72,. . .,78. As $\boldsymbol{tat} = a^{-1}$,

$$\begin{matrix}(02,03,04,05,06,07,08)\\ (-, A_i, -, A_j, \ldots\ldots\ldots)\end{matrix} \qquad (6.15)$$

where $(-, A_i, -, A_j \ldots)$ is in some order (51, 57, 56, 55, 54, 53, 52), (65,71,70,69,68,67,66) or (72,78,77,76,75,74,73) and also $b^2a^4 =0^{A_i}_{A_j}$.

We have

$$\begin{aligned}b^2a^4 = {} & (00)(01, 13, 35,26,04, 24, 15, 30)(02, 20,21, 14)\\ & (03, 10, 18, 19, 33, 05, 11, 32)(06, 36, 16, 17)\\ & (07, 23, 34, 22,09,27,08, 25)(12, 31, 29,28)\\ & (37, 41, 60, 88, 56, 53, 90, 61)(38, 71, 66, 40, 44, 62, 59, 50)\\ & (39, 79)(42, 57, 73, 78, 52,43,45,49)(46, 51, 48,93, 84, 89, 81, 99)\\ & (47, 72)(54, 65, 55, 85, 67, 96, 70, 80)(58, 69, 77, 86, 83, 98, 95, 75)\\ & (63,76,97, 94, 82, 92, 74, 68)(64)(87,91)\end{aligned} \qquad (6.16)$$

Here $A_i = 73$, $A_j = 78$ is the only pair from the 21 orbit of $\boldsymbol{(a, d)}$ in the 63 orbit of $\boldsymbol{H}$ satisfying $b^2a^4 = {}^{A_i}_{0A_j}$ and $a^{-1} = (\ldots A_i, -, A_j \ldots)$. Hence from (6.13) we must have $t = (03, 73)$. The equation (6.13) and the relations $\boldsymbol{tat} = a^{-1}$, $\boldsymbol{tc} = \boldsymbol{ct}$ now completely determine $\boldsymbol{t}$:

$$\begin{aligned}t = {} & (00,01)(02, 74)(03, 73)(04, 72)(05, 78)(06, 77)(07, 76)(08, 75)(09, 34)\\ & (10, 33)(11, 32)(12, 31)(13, 30)(14, 36)(15, 35)(16, 71)(17,70)(18, 69)\\ & (19, 68)(20, 67)(21, 66)(22, 65)(23, 53)(24, 52)(25, 51)(26, 57)(27, 56)\\ & (28, 55)(29, 54)(37,91)(38, 90)(39, 89)(40, 88)(41, 87)(42, 86)(43, 92)\\ & (44,99)(45,98)(46,97)(47,96)(48,95)(49,94)(50,93)(58, 85)(59, 84)\\ & (60, 83)(61, 82)(62, 81)(63, 80)(64, 79).\end{aligned} \qquad (6.17)$$

We now have a permutation group G on 100 letters 00, 01,. . . ,99, $\boldsymbol{G = (a, b, t)}$ and a group $\boldsymbol{H = (a, b)}$ fixing 00 where it is known that $\boldsymbol{H}$ is the simple group of order 6048. Let $M = G_{00}$ be the subgroup of G fixing 00. It is well known that M is generated by the 300 elements

$$x_i a\ \overline{x_i a}^{-1},\ x_i b\ \overline{x_i b}^{-1},\ x_i t\ \overline{x_i t}^{-1}, \qquad (6.18)$$

where $x_i = \begin{pmatrix}00, \ldots\\ i, \ldots\end{pmatrix}$, $i = 00, \ldots,$ 99, are coset representatives of M in G and $\bar{y} = x_j$ is the coset representative of My $= Mx_j$. Here, with the help of Mr. Peter Swinnerton-Dyer and the Titan computer at the Cambridge University Mathematical Laboratory, it was shown that each of the 300 permutations in (6.18) lies in $H = (a,$ b). Thus $M \subseteq H$, and so $M = H$, whence $G_{00} = H$ and G is of order 604,800.

It remains *to* be shown that G is simple. In G the normafizer of the group *(a)* contains the element t interchanging 00 and 01. As these are the only letters fixed by *(a)* it follows that $[N_G(\langle a\rangle)] = 2$. As $|N_H(\langle a\rangle)| = 21$ it follows that $|N_G(\langle a\rangle)| = 42$ and *(a)* = S(7) is its own centralizer in G.

In a chief series for G one of the factors has order a multiple of 6048. If this is not a minimal normal subgroup, then a minimal normal subgroup K has order 2, 4, 5, or 25. But then an S(7) normalizing K must also centralize K, which is false since S(7) is its own centralizer. Hence a minimal normal subgroup K has order a multiple of 6048 and also 14,400 since it must contain all 14,400 $S(7)$'s. Thus either $[G:K] = 2$ or G = K and G is simple. If $[G:K] = 2$ then $N_K(7)$ is of order 21 and so $t \notin K$ but $H \subseteq K$. But mapping *G/K* onto the group + 1, − 1 we map $H \to +1$, $t \to -1$ and this conflicts with the relation (6.12). Hence G is simple.

As this is written some questions remain unanswered. The original character table given by Janko has been shown by Walter Feit to be in error. Janko has made corrections to his table. The character table of the group constructed here has not yet been calculated. And it has not been established that there is a unique simple group or order 604,800.

[Added in proof by the Editor: The uniqueness of the simple group of order 604,800 has since been established ; see Marshall Hall Jr. and David Wales: The simple group of order ***604 800, J. Algebra 9*** (1968), 417-450.]

REFERENCES

1. E. ARTIN: *Geometric Algebra* (Interscience, New York, 1957).
2. R. BRAUER: Investigations on group characters. *Ann. of Math. 42* (1941), 936-958.
3. R. BRAUER: On groups whose order contains a prime number to the first power, part I, *Am.* J. Math. 64 (1942), 401-420; part II, *Am. J. Math. 64* (1942), 421-440.
4. R. BRAUER: On the connections between the ordinary and the modular characters of groups of finite order. *Ann. of Math. 42* (1941). 926-935.
5. R. BRAUER: On permutation groups of prime'degree and related classes of groups. *Ann. of Math. 44* (1943), 57-79.
6. R. BRAUER: Zur Darstellungstheorie der Gruppen endlicher Ordnung, part I, *Math. Zeit.* 63 (1956), 406444; part II, *Math. Zeit. 72 (1959), 25-46.*
7. R. BRAUER: Some applications of the theory of blocks of characters of finite groups, *J. of Algebra,* part I, 1(1964), 152-167; part II, 1(1964), 307-334; part III, 3 (1966), 225-255.
8. R. BRAUER and K. A. FOWLER: On groups of even order. *Ann. of Math. 62* (1955), 5655.583.
9. R. BRAUER and C. NESBITT: On the modular characters of groups. *Ann. of Math. 42* (1941), 556-590.
10. R. BRAUER and W. F. REYNOLDS: On a problem of E. Artin. *Ann. of Math. 68* (1958). 713-720.

11. R. Brauer and M. Suzuki: On finite groups of even order whose 2-Sylow group is a quatemion group. *Proc. Nat. Acad. Sci. U.S.A. 45* (1959), 1757-1759.
12. R. Brauer and H. F. Tuan: On simple groups of finite order. *Bull. Amer. Math. Soc.* 51 (1945), 756-766.
13. J. S. Brodkey: A note on finite groups with an Abelian Sylow group. *Proc. Amer. Math. Soc.* 14 (1963), 132-133.
14. W. Burnside: *The Theory* of *Groups,* 2nd edition (Cambridge University Press, 1911).
15. C. Ciievalley: Sur certains groupes simples. *Tôhoku Math. J. (2) 7* (1955), 14-66.
16. Everett C. Dade: Blocks with cyclic defect groups. *Ann. of Math. 84* (1966), 20-48.
17. L. E. Dickson: *Linear Groups* (Reprinted by Dover, New York, 1958).
18. Walter Feit: On finite linear groups. *J. of Algebra 5* (1967). 378-400.
19. 'W. Feit and John Thompson: Solvability of groups of odd order. *Pacific J. Math.* 13 (1963), 775-1029.
20. W. Feit and John Thompson: Groups which have a faithful representation of degree less than $(p-1)/2$. *Pacific J. Math.* 11 (1961), 1257-1262.
21. D. Gorenstein: Finite groups in which Sylow 2-subgroups are Abelian and centralizers of involutions are solvable. *Canad. J. Math.* 17 (1965). 860-906.
22. D. Gorenstein and J. H. Walter: The characterization of finite groups with dihedral Sylow 2-subgroups. *J. of Algebra,* part I, 2 (1965), 85-151; part II, 2 (1965), 218-270; part III, 2 (1965), 354-393.
23. Marshall Hall Jr. : *The Theory of Groups* (Macmillan, New York, 1959).
24. Marshall Hall Jr. : On the number of Sylow subgroups in a finite group, to appear in *J. of Algebra.*
25. Zvonomir Janko: A new finite simple group with Abelian Sylow 2-subgroups and its characterization. *J. of Algebra 3* (1966), 147-186.
26. E. L. Michaels: A study of simple groups of even order. Ph.D. Thesis, Notre Dame University, 1963.
27. Rimhak Ree: A family of simple groups associated with the simple Lie algebra of type (G_2). *Amer. J. Math. 83* (1961), 432-462.
28. Rimhak Ree: A family of simple groups associated with the simple Lie algebra of type (F_4). *Amer. J. Math. 83* (1961). 401-431.
29. Issai Schur: Über eine Klasse von endlichen Gruppen linearer Substitutionen. *Sitz. der Preussischen Akad. Berlin (1905),* 77-91.
30. R. G. Stanton: The Mathieu groups. *Canad. J. Math. 3* (1951), 164-174.
31. Michio Suzuki: A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A. 46* (1960), 868-870.
32. John G. Thompson: Normalp-complements for finite groups. *J. of Algebra* 1 (1964), 43-46.
33. John G. Thompson: N-groups. To be published.
34. Hsio F. Tuan: On groups whose orders contain a prime number to the first power. *Ann. of Math. 45* (1944), 110-140.

Computational methods in the study of permutation groups†

CHARLES C. SIMS

1. **Introduction.** One of the oldest problems in the theory of permutation groups is the determination of the primitive groups of a given degree. During a period of several decades a great deal of effort was spent on constructing the permutation groups of low degree. For degrees 2 through 11 lists of all permutation groups appeared. For degrees 12 through 15 the lists were limited to the transitive groups, while only the primitive groups of degrees 16 through 20 were determined. A detailed account of the early work in this area can be found in the first article of [12] and references to later papers are given in **[1]** and in [2] p. 564. The only recent work of this type known to the author is that of Parker, Nikolai, and Appel **[13]**, **[14]**, and a series of papers by Ito. These authors have shown that for certain prime degrees any non-solvable transitive group contains the alternating group.

The basic assumption of this paper is that it would be useful to extend the determination of the primitive groups of low degree and that with recent advances in group theory and the availability of electronic computers for routine calculations it is feasible to carry out the determination as far as degree 30 and probably farther. Ideally one would wish to have an algorithm sufficiently mechanical and efficient to be carried out entirely on a computer. Such an algorithm does not yet exist. The procedure outlined in this paper combines the use of a computer with more conventional techniques.

Suppose we wish to find the primitive groups of a given degree n. It will be assumed that the primitive groups of degree less than n have already been determined. Since a minimal normal subgroup of a primitive group is transitive and is a direct product of isomorphic simple groups, the first step is to take each of the known simple groups H, including the groups of prime order, determine the transitive groups M of degree n isomorphic to the direct product of one or more copies of H, and then for each such group M find the primitive groups containing M as a normal subgroup. While this is by no means a trivial procedure, it is considerably

† This research was supported in part by the National Science Foundation.

easier than the second step, showing that there are no other primitive groups of degree n. The list of primitive groups so far constructed can fail to be complete only if there exists a primitive group G of degree n which is a new simple group and so cannot be represented faithfully on fewer than n points. Here it seems useful to distinguish three cases:

1. G is simply primitive, that is, primitive but not doubly transitive.
2. G is doubly transitive but not doubly primitive.
3. G is doubly primitive.

The first two cases will be dealt with in the next two sections. In the third case, G is a transitive extension of one of the primitive groups of degree n- 1 which contains only even permutations. The techniques of transitive extension are discussed at length in [S] and [11]. Thus it seems necessary only to point out that the non-existence of transitive extensions for several families of transitive groups is already known. See for example [9], [10], and [16] p. 22. It seems probable that a computer program could be written to construct up to isomorphism as permutation groups the transition extensions of a given transitive group. So far, the author has found that with the program presented in § 4 of this paper and a small amount of hand computation all transitive extensions can be determined easily.

The paper concludes with a short description of a computer program for finding the order and some of the structure of the group generated by a given set of permutations and with a list of the 129 primitive groups of degree not exceeding 20. This list was taken from the literature and checked by the methods described here. The notation and terminology for permutation groups is that of [16] with one important exception. The term "block" is used only in the context of block designs and the older terms "sets of imprimitivity" and "systems of imprimitivity" are used for what are called blocks and complete block systems in [16]. Throughout G will denote a primitive group on the finite set Ω with $|\Omega| = n$.

2. Simply primitive groups. In this section we discuss techniques for handling the first of the three cases described in the Introduction. For each $\alpha \in \Omega$ let $\Delta_1(\alpha) = \{\alpha\}, \Delta_2(\alpha), \ldots, \Delta_k(\alpha)$ be the orbits of G_α numbered in such a way that $\Delta_i(\alpha^g) = \Delta_i(\alpha)^g$ for all $g \in$ G. Let $n_i = |\Delta_i(\alpha)|$. We shall assume $1 = n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$ and $k \geqslant 3$. For $1 \leqslant i \leqslant k$ we denote by i' that integer such that $\Delta_{i'}(\alpha)$ is the orbit of G_α paired with $\Delta_i(\alpha)$. A necessary condition that $i' = i$ is that nn_i is even. The following theorem contains most of the known number-theoretic conditions satisfied by n and the n_i. These conditions follow easily from results in [16], in particular Theorems 11.7, 13.9, 17.4, 17.5, 17.7, 18.2, and 31.2.

THEOREM 2.1. *Let* $1 = n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$, $k \geqslant 3$, *be a sequence of positive integers. Let* π *be the smallest set of primes such that*

(a) *π contains all prime divisors of the* n_i,

(b) *if* $\frac{1}{2}n_i < p < n_i$ *for some i and some* $p \in \pi$, *then* π *contains the prime divisors of all integers m such that* $p < m < n_i$. *If in addition* $n_i - p \geqslant 3$, *then* π *contains all primes less than* n_i.

The following are necessary conditions for there to exist a primitive group G of degree $n = n_1 + \ldots + n_k$ *such that* G_α *has k orbits of lengths* $n_1, \ldots, n_k$:

(1) *If* $n_k > 1$, *then* $(n_i, n_k) \neq 1$, $2 \leqslant i \leqslant k$.

(2) $n_i \leqslant n_2 n_{i-1}$, $2 \leqslant i \leqslant k$. *If the number of* n_j *equal to* n_2 *is odd, then* $n_i \leqslant (n_2 - 1)n_{i-1}$, $3 \leqslant i \leqslant k$.

(3) *No element of* π *is greater than* n_2.

(4) *If* $\frac{1}{2}n_i < p < n_i$ *for some i and some* $p \in \pi$, *then there exists an* $n_j > n_i$ *such that* n_j *divides* $n_i(n_i - 1)$.

(5) *If* n_i *is a prime, then* n_i^2 *does not divide any* n_j.

(6) *If n is odd, then for each odd number t the number of* n_i *such that* $n_i = t$ *is even.*

(7) *If n is a prime, then* $n_2 = n_3 = \ldots = n_k$. (*In this case G is solvable.*)

(8) *If* $n_2 \leqslant 2$, *then n is a prime.*

(9) *If n is twice a prime, then* $k = 3$, $n = (2s+1)^2 + 1$, $n_2 = s(2s+1)$, *and* $n_3 = (s+1)(2s+1)$.

(10) *If* $3 \leqslant n_2 \leqslant 4$ *and n is not divisible by a prime greater than 3, then* $n = 2^a$ *or* $n = 3^a$ *and in either case* $a < n_2$.

In addition, we note that the primitive groups in which $n_2 = 3$ have been completely determined by Wong [17].

Once those partitions $n = n_1 + \ldots + n_k$ which satisfy the conditions of Theorem 2.1 have been found, we can apply the results of Higman [7] to reduce the possibilities still further. Given a primitive group G in which G_α has orbits $\Delta_1(\alpha), \ldots, \Delta_k(\alpha)$ as above, we may define $n \times n$ matrices B_i, $1 \leqslant i \leqslant k$, whose rows and columns are indexed by the elements of Ω, as follows :

$$B_i = [b^i_{\alpha\beta}]$$

where

$$b^i_{\alpha\beta} = \begin{cases} 1 & \text{if } \alpha \in \Delta_i(\beta), \\ 0 & \text{otherwise.} \end{cases}$$

We also define $k \times k$ matrices M_i, $1 \leqslant i \leqslant k$, by

$$M_i = [m^i_{jk}], \quad m^i_{jk} = \quad \Delta_j(\alpha) \cap \Delta_i(\beta) \;|, \; \beta \in \Delta_k(\alpha).$$

THEOREM 2.2. *The integers* m^i_{jk} *satisfy the following conditions:*

$$\sum_i m^i_{jk} = n_j, \quad \sum_j m^i_{jk} = n_i, \; m^i_{jk} = m^j_{ik'},$$

$$m^i_{j1} = \delta_{ij} n_i, \; m^i_{1k} = \delta_{ik'},$$

$$m^i_{jk} n_k = m^{i'}_{kj} n_j, \quad m^i_{j'k} n_k = m^k_{i'j} n_j = m^j_{k'i} n_i.$$

THEOREM 2.3. *The matrices $M_i, 1 \leqslant i \leqslant k$, form a basis* ***for a*** *subalgebra* ***of*** *the algebra* ***of*** *$k \times k$ matrices. In* ***fact,***

$$M_iM_j = \sum_{k} m^{j}_{i'k'} M_k.$$

An $r \times r$ matrix C will be called irreducible if there is no permutation σ of $1, \ldots, r$ such that when σ is applied to the rows and columns of C, the result is a direct sum of two matrices. Because of the primitivity of G we have

THEOREM 2.4. *Fix i, $2 \leqslant i \leqslant k$, and let $M = M_i$ and $A = B_i$. Then*

(1) M and A are irreducible.

(2) M and A have the same minimal polynomial ***f.***

(3) *If we define vectors U_q, $q \geqslant 0$, by $U_q = (u_{q1}, \ldots, u_{qk})$, $U_0 = (1, 0, 0, 0, \ldots, 0)$, $U_{q+1} = U_qM$, then the trace of A^q is nu_{q1}.*

(4) n_i is a root off and if $n_i = \theta_1, \theta_2, \ldots, \theta_r$ are the distinct roots off, then the multiplicity of θ_j as an eigenvalue of A is

$$e_j = \text{trace } f_j(A)/f_j(\theta_j),$$

where $f_j(x) = f(x)/(x-\theta_j)^{d_j}$ and d_j is the multiplicity of θ_j in f. Also $d_1 = e_1 = 1$.

In view of part (3) of Theorem 2.4 the e_j can be computed from a knowledge of M. The fact that the e_j must be positive integers imposes still further conditions on the matrices M_i and the integers n_i. Once matrices $M_1, \ldots, M_k$ satisfying the conditions of Theorems 2.2, 2.3, and 2.4 have been found, it is usually not particularly difficult to construct the possible matrices $B_1, \ldots, B_k$, if they exist. This is of course equivalent to finding the graphs $\mathcal{G}_i$ as defined in [15]. Once the B_i are known, G must be a subgroup of the group of permutation matrices commuting with each of the B_i.

3. Doubly transitive groups. In this section we take up the second of the three cases described in the Introduction. Throughout, G will be assumed to be doubly transitive on Ω. For any subset Δ of Ω, Δ^* will denote the set of 2-element subsets of Δ and G* will denote the permutation group on Ω^* induced by G. We shall not explicitly make the assumption that G is not doubly primitive, but many of the results are trivial for doubly primitive groups.

Of fundamental importance to the following discussion is the concept of a block design. A block design, or more correctly a balanced incomplete block design, with parameters v, b, k, r, λ is a set Ω of points together with a set B of blocks and an incidence relation between points and blocks such that

(1) $|\Omega| = v$,

(2) $|B| = b$,

(3) each block is incident with exactly k points,

(4) each point is incident with exactly ***r***blocks,

(5) any two distinct points are incident with exactly A blocks.

The parameters of a block design satisfy the conditions

$$bk = rv, \quad r(k- 1) = \lambda(v- 1).$$

A Steiner triple system is a block design with $\lambda = 1$ and $k = 3$. A projective plane is a block design with $\lambda = 1$ and b = v $\geqslant$ 4. We shall say a block design is trivial if for every k-element subset Δ of Ω there is a block Γ such that every point in Δ is incident with Γ. An automorphism of a block design consists of a permutation g of the points and a permutation h of the blocks such that a point a is incident with a block Γ if and only if α^g is incident with Γ^h. In many situations, in particular when $\lambda = 1$, two blocks are the same if they are incident with the same points. In this case h is determined by g and we may consider the automorphism to be the permutation g. For a more complete discussion of block designs the reader is referred to [**6**]. We note that for any subset Δ of Ω with $|\Delta \geqslant 2$ the double transitivity of G implies that (Ω, B) is a block design, where

$$B = \{\Delta^g \mid g \in G\}$$

and incidence is set membership.

The following is an analogue of Theorem 18.2 of [**16**] for doubly transitive groups.

THEOREM 3.1. *Let G be a doubly transitive group on Ω, let a and β be distinct points of Ω, and let Γ be an orbit of $G_{\alpha\beta}$ on $\Omega-\{\alpha, \beta\}$. Then at least one of the following holds:*

(I) Every composition factor of $G_{\alpha\beta}$ is a composition factor of some subgroup of $G^{\Gamma}_{\alpha\beta}$.

(2) G is a group of automorphisms of a non-trivial block design with point set Ω for which $\lambda = 1$.

Proof The following lemma is easily verified and we omit its proof.

LEMMA 3.2. *Let A be a subset of Ω with $|\Delta| \geqslant 2$. Then A* is a set of imprimitivity for G* if and only if (Ω, B) is a block design for which $\lambda = 1$, where*

$$B = \{\Delta^g \mid g \in G\}.$$

Now assume that conclusion (2) of the theorem does not hold.

LEMMA 3.3. *Let $V \neq 1$ be a subgroup of G fixing two points. There exists $g \in G$ such that $g^{-1}Vg = U \leqslant G_{\alpha\beta}$ and $U^{\Gamma} \neq 1$.*

Proof Let $\gamma \in \Gamma$ and let A be the fixed point set of V. $2 \leqslant |\Delta| < |\Omega|$. Consider

$$\psi = \bigcap_g \Delta^g,$$

the intersection being taken over all g in G such that $\{\alpha, \beta\} \subseteq \Delta^g$. Then

$$\psi^* = \bigcap_g (\Delta^*)^g$$

and ψ^* is a set of imprimitivity of G*. By Lemma 3.2 $|\psi| = 2$. Thus there is a g in G such that $\{a, \beta\} \subseteq \Delta^g$ and $\gamma \notin \Delta^g$. Then $U = g^{-1}Vg \subseteq G_{\alpha\beta}$ and $U^\Gamma \neq 1$.

The proof of Theorem 3.1 is completed as in the proof of Theorem 18.2 of [**16**].

We wish now to consider the consequences of the assumption that G^* is imprimitive. If we are assuming that G cannot be represented non-trivially on fewer than $n = |\Omega|$ points, then G* cannot have a set of imprimitivity with more than $(n-1)/2$ elements. Let $B = \{E_i \mid 1 \leqslant i \leqslant b\}$ be a non-trivial system of imprimitivity for G*. Let Δ_i denote the union of the elements in E_i and let $\mathfrak{G}_i$ be the undirected graph (Δ_i, E_i). (Ω, B) is a block design, where a point a is incident to E_i if and only if $a \in \Delta_i$. (It is possible to have $\Delta_i = \Delta_j$ with $i \neq$ j.) Let v, b, k, r, λ be the parameters of this block design. The graphs $\mathfrak{G}_i$ are all isomorphic and the automorphism group of any one of them is transitive on vertices and edges. Thus there is a positive integer d such that each vertex of $\mathfrak{G}_i$ is connected to exactly d other vertices. The integers v, b, k, r, I, d will be called the parameters of the system of imprimitivity B.

THEOREM 3.4. *The parameters of a system of imprimitivity B for G* satisfy the following conditions:*

(1) $bk = rv$,

(2) $r(k\text{-}1) = \lambda(v-1)$,

(3) *dk is even and* $bdk = v(v-1)$,

(4) $rd = w\text{-}l$,

(5) $d\lambda = k\text{-}l$.

Proof. Let $B = \{E_i \mid 1 \leqslant i \leqslant b\}$ and let $\mathfrak{G}_i$ be as defined above. (1) and (2) follow from the fact that (Ω, B) is a block design. Since $\mathfrak{G}_i$ has k vertices and each vertex is connected to d other vertices, $|E_i| = dk/2$. Therefore

$$|\,\Omega^* = v(v-1)/2 = b \mid E_i = bdk/2,$$

or

$$bdk = v(v-1).$$

(4) follows from (1) and (3). Finally (2) and (4) imply (5).

We now prove an analogue of Theorems 17.4 and 17.5 of [**16**].

THEOREM 3.5. *Let G be doubly transitive on Ω, let a and β be distinct points of Ω, and let the orbits of $G_{\alpha\beta}$ be* $\{a\} = \Delta_1$, $\{\beta\} = \Delta_2$, $\Delta_3, \ldots, A_t$. *Set* $n_i = |\Delta_i|$ *and suppose* $1 = n_1 = n_2 \leqslant n_3 \leqslant \ldots \leqslant n_t$. *Then at least one of the following holds:*

(1) ***if 3 $\leqslant i \leqslant t$, then $n_i \leqslant n_3 n_{i-1}$ and $(n_i, n,) \neq 1$,***

(2) there exists a non-trivial system of imprimitivity for G* for which $d > 1$,

(3) G is sharply doubly transitive.

Proof. If $n_t = 1$, then G is sharply doubly transitive. If $n_t > 1$ and $n_3 = 1$, then by Theorem 3.1 G is an automorphism group of a non-trivial block design with λ = 1. If $\psi_1, . . ., \psi_b$ are the blocks of this design, then $\{\psi_1^*, . . . , \psi_b^*\}$ is a non-trivial system of imprimitivity for G* for which $d = | \psi_i | - 1 \geqslant 2$. Thus we may assume $n_i \geqslant 2$ for $i \geqslant 3$. Suppose there exists an $i \geqslant 3$ such that $(n_i, n,) = 1$. For any two distinct points γ and δ of Ω let $\Gamma(\gamma, \delta)$ denote the union of those orbits of $G_{\gamma\delta}$ with length $n,$. Clearly $\Gamma(\gamma, \delta) = \Gamma(\delta, \gamma)$. No w choose $\gamma \in \Delta_i$. From the proof of Theorem 17.5 of [16] applied to G_α we see that $\Gamma(\alpha, \beta) = \Gamma(\alpha, \gamma)$. Thus we can obtain a non-trivial equivalence relation $\sim$ on Ω^* by defining $\{y, \delta\} \sim \{\varepsilon, \eta\}$ if and only if $\Gamma(\gamma, \delta) = \Gamma(\varepsilon, \eta)$. The equivalence classes of $\sim$ form a non-trivial system of imprimitivity for G* for which $d \geqslant n_i \geqslant 2$. If there is an $i \geqslant 3$ such that $n_i > n_3 n_{i-1}$, we define $\Gamma(\gamma, 6)$ to be the union of all orbits of $G_{\gamma\delta}$ with length at least n_i. If $\gamma \in \Delta_3$, then by the proof of Theorem 17.4 of **[16]** applied to G_α $\Gamma(\alpha, \beta) = \Gamma(\alpha, \gamma)$ and we can proceed as before.

THEOREM *3.6.* ***Let v, b, k, r, I, d be the parameters of a non-trivial system of imprimitivity of G*. Any one of the following implies that G is sharply doubly transitive or an automorphism group of a non-trivial block design for which λ =*** 1:

(1) ***d = 2,***

(2) *d* = 1 *and k* = *v*−1,

(3) d = 1, ***k $\leqslant$ 6, and v is odd.***

Proof. We shall show that if any one of the conditions (I), (2), or (3) holds, then, for any two distinct points a and β of Ω, $G_{\alpha\beta}$ fixes at least 3 points. It will follow by Theorem 3.1 that G is sharply doubly transitive or an automorphism group of a non-trivial block design with λ = 1. Let $B = \{E_i \mid 1 \leqslant i \leqslant b\}$ be the system of imprimitivity for G* and let the graphs $\mathfrak{G}_i$ be defined as before. Suppose first that $d = 2$. Given a $\neq \beta$ there exists a unique $\gamma \neq \beta$ such that $\{a, \beta\}$ and $\{a, \gamma\}$ are edges of the same $\mathfrak{G}_i$. Therefore $G_{\alpha\beta}$ fixes y. Suppose now that d = 1 and $k = v$- 1. Then $b = v$ and for each $a \in \Omega$ there is a unique $\mathfrak{G}_i$ such that a is not a vertex of $\mathfrak{G}_i$. Given $\beta \neq a$, $G_{\alpha\beta}$ must fix the unique point γ such that $\{\beta, \gamma\}$ is an edge of $\mathfrak{G}_i$. Finally, suppose d = 1 and $k \leqslant$ 6. Then $k = 4$ or 6. If k = 4, let E_1 = {{a, β}, {γ, S}}. $G_{\alpha\beta}$ maps $\{\gamma, \delta\}$ into itself and if G is not an automorphism group of a block design for which λ = 1, then $G_{\alpha\beta}$ is a 2-group. If in addition v is odd, then $G_{\alpha\beta}$ must fix a third point. A similar argument takes care of the case ***k = 6.***

THEOREM *3.7.* ***Let G be doubly transitive on Ω, let a and β be distinct points of Ω, and let H be the subgroup of G mapping {a, β} into itself. If G_α***

has a set of imprimitivity on $\Omega - \{\alpha\}$ of length $m \geqslant 2$, then H has an orbit of length less than or equal to $m - 1$ on $\Omega - \{\alpha, \beta\}$.

Proof. Let Δ be a set of imprimitivity of G_a with $|\Delta| = m$. Let

$$A = \{(\gamma, \{\delta, \varepsilon\}) \mid \delta \neq \varepsilon, \quad \exists\, g \in G \text{ such that } \gamma^g = a \text{ and } \{\delta, \varepsilon\}^g \subseteq \Delta\}.$$

A simple computation shows that

$$A = \tfrac{1}{2}n(n- i)(m- 1).$$

If we let $\Gamma = \{\gamma \mid (\gamma, \{a, \beta\}) \in A\}$, then $\Gamma = m- 1$ and Γ is mapped into itself by H.

If in Theorem 3.7 $m \leqslant 4$ and G* is primitive, then it follows from Theorem 2.1 and the remark following it that G is abstractly a "known" group.

The results of this section seem to indicate that at least for low degrees most doubly transitive groups which are not doubly primitive will be sharply doubly transitive or automorphism groups of block designs with $\lambda = 1$. The sharply doubly transitive groups are known. The question of which block designs with $\lambda = 1$ have doubly transitive .automorphism groups is still open. It is known that projective planes with doubly transitive groups are Desarguesian. Also, Hall [5] and Fischer [3] have made some progress in the case of Steiner triple systems.

4. A computer program. In this section we present a short description of a computer program for determining the order and some of the structure of the group generated by a given set of permutations. Before describing the program itself, however, it is necessary to discuss the method to be used for storing a permutation group G in the computer. There are three basic requirements which such a method should satisfy:

(1) it should be efficient with respect to storage,

(2) given a permutation h it should be easy to determine whether or not h is in G,

(3) it is should be possible to run through the elements of G one at a time without repetitions.

One method satisfying all of these conditions will now be presented.

Let G be a permutation group on $\Omega = \{1, \ldots, n\}$. Let $G^{(0)} = G$ and for $1 \leqslant i \leqslant n- 1$ let $G^{(i)}$ be the subgroup of G fixing $1, 2, \ldots, i$. Let U_i be a system of right coset representatives for $G^{(i)}$ in $G^{(i-1)}$, $1 \leqslant i \leqslant n- 1$. Define

$$n_i = |U_i| = |G^{(i-1)}: G^{(i)}|.$$

n_i is the length of the orbit Δ of $G^{(i-1)}$ containing i and for each $j \in \Delta$ there is a unique element in U_i taking i to j. Also

$$|G| = \prod_{i=1}^{n-1} n_i$$

and every element of G has a unique representation of the form

$$g_{n-1}g_{n-2} \dots g_1,$$

where $g_i \in U_i$. We shall store the group G by storing the permutations in each of the U_i. The total number of permutations stored is

$$\sum_{i=1}^{n-1} n_i < n(n+1)/2.$$

Thus the storage space required to store an arbitrary permutation group of degree n grows as n^3. By "packing" more than one integer into a computer word, one can easily store a group of degree 50 on any of the large computers available today. Because of the canonical form described above, it is easy to run through the elements of G one at a time. Also, suppose we are given a permutation h on Ω and we wish to find .out if h is in G. A necessary condition that $h \in$ G is that there exists $g_1 \in U_1$ such that hg_1^{-1} fixes 1. Similarly there must be a $g_2 \in U_2$ such that $hg_1^{-1}g_2^{-1}$ fixes 2. Continuing in this manner we either arrive at elements $g_i \in U_i$ such that

$$hg_1^{-1}g_2^{-1} \dots g_{n-1}^{-1} = 1$$

and so

$$h = g_{n-1}g_{n-2} \dots g_1 \in G,$$

or *his* not in G.

Permutation groups are not usually given by sets U_i and so we need a program that will construct sets U_i for the group G generated by a set X of permutations. Given X it is easy to construct U_1. If for any g $\in$ G we denote by $\phi(g)$ the representative in U_1 for the coset $G^{(1)}g$, then, by Lemmas 7.2.2 of [4], $G^{(1)}$ is generated by

$$X_1 = \{ux\phi(ux)^{-1} | u \in U_1,\ x \in X\}.$$

Continuing in this manner we can obtain generators for each of the subgroups $G^{(i)}$ and construct sets U_i of coset representatives. There is one difficulty which must be overcome. In general the set X_1 will be much larger than X. Unless some care is exercised, the sets of generators can grow so large as to be unmanageable. This can be avoided by not constructing all the generators of $G^{(i)}$ at one time, but rather as soon as a new generator for $G^{(i)}$ has been obtained, using it to construct new elements in U_{i+1} and new generators for $G^{(i+1)}$. Also, whenever one of the elements $ux\phi(ux)^{-1}$ is computed, the process described above should be used to determine if it can be expressed in terms of the coset representative already constructed and is therefore redundant.

A computer program of the type described has been written for the IBM 7040 at Rutgers. In its present form it can handle any group of degree 50 or less and can be of some use up to degree 127. Problem 5 on page 83 of [4] can be done in slightly over a minute.

5. The **primitive groups of degree not exceeding** 20. In this section we provide a list of the 129 primitive groups of degrees 2 to 20. The information

TABLE *1. The Primitive Groups of Degree not exceeding 20*

Degree	*No.*	Order	*t*	*N*	G_n	Generators	±	Comments
2	1	2	2	—			—	S_2
3	1	3		—				A_3
	2	6	3	3G1	2G1		—	S_3
4	1	12	2P	e.a.	3G1			A_4
	2	24	4	e.a.	3G2		—	S_4
5	1	5		—		a_5		
	2	10		5G1		a_5, b_5^2		
	3	20	2	5G1		a_5, b_5	—	
	4	60	3P	—	4G1			A_5
	5	120	5	5G4	4G2		—	S_5
6	1	60	2P	—	5G2	a_5, b_5^2, a_6		*PSL*(2, 5)
	2	120	3	6G1	5G3	a_5, b_5, a_6	—	*PGL*(2, 5)
	3	360	4p	—	5G4			A_6
	4	720	6	6G3	5G5		—	S_6
7	1	7		—		a_7		
	2	14		7G1		a_7, b_7^3	—	
	3	21		7G1		a_7, b_7^2		
	4	42	2	7G1		a_7, b_7	—	
	5	168	2	—		a_7, c_7		*PSL*(3, 2)
	6	2520	5p	—	6G3			A_7
	7	5040	7	7G6	6G4		—	S_7
8	1	56	2P	e.a.	7G1	a_7, a_8		
	2	168	2P	e.a.	7G3	a_7, b_7^2, a_8		
	3	168	2P	—	7G3	a_7, b_7^2, d_8		*PSL*(2, 7)
	4	336	3	8G3	7G4	a_7, b_7, d_8	—	*PGL*(2, 7)
	5	1344	3	e.a.	7G5	a_7, c_7, a_8		
	6	20160	6p	—	7G6			A_8
	7	40320	8	8G6	7G7		—	S_8
9	1	36		e.a.		a_9, c_9^2		
	2	72		e.a.		a_9, c_9^2, d_9	—	
	3	72	2	e.a.		a_9, c_9	—	
	4	72	2	e.a.		a_9, c_9^2, c_9d_9		
	5	144	2	e.a.		a_9, c_9, d_9	—	
	6	216	2	e.a.		a_9, c_9^2, e_9		
	7	432	2	e.a.		a_9, c_9, e_9	—	
	8	504	3P	—	8G1	a_7, a_8, f_9		*PSL*(2, 8)
	9	1512	3P	9G8	8G2	a_7, b_7^2, a_8, f_9		
	10	$\frac{1}{2}\cdot 9!$	7P	—	8G6			A_a
	11	9!	9	9G10	8G7		—	S_9
10	1	60		—		a_{10}^2, b_{10}	—	A_5
	2	120		10G1		a_{10}, b_{10}	—	S_5
	3	360	2P	—	9G1	a_9, c_9^2, c_{10}		*PSL*(2, 9)
	4	720	2p	10G3	9G2	a_9, c_9^2, d_9, c_{10}	—	S_6
	5	720	3	10G3	9G3	a_9, c_9, c_{10}		*PGL*(2, 9)
	6	720	3	10G3	9G4	a_9, c_9^2, c_9d_9, c_{10}		
	7	1440	3	10G3	9G5	a_9, c_9, d_9, c_{10}	—	

TABLE 1 *(continued)*

Degree	NO.	)rder	t	N	G_n	Generators	±	Comments
	8	·10!	$8p$	—	$9G10$			A_{10}
	9	10!	10	$10G8$	9611		—	S_{10}
11	1	11		—		a_{11}		
	2	22		$11G1$		a_{11}, b_{11}^5	—	
	3	55		$11G1$		a_{11}, b_{11}^2		
	4	110	2	$11G1$		a_{11}, b_{11}	—	
	5	660	$2P$	—	$10G1$	a_{10}^2, b_{10}, c_{11}		$PSL(2, 11)$
	6	7920	4	—	$10G6$	$a_9, c_9^2, c_9d_9, c_{10}, d_{11}$		M_{11}
	7	··11!	$9p$	—	$10G8$			A_{11}
	8	11!	11	11G7	$10G9$		—	S_{11}
12	1	660	$2P$	—	11G3	a_{11}, b_{11}^2, a_{12}		$PSL(2, 11)$
	2	1320	3	$12G1$	11G4	a_{11}, b_{11}, a_{12}	—	$PGL(2, 11)$
	3	7920	$3P$	—	11G5	$a_{10}^2, b_{10}, c_{11}, b_{12}$		M_{11}
	4	5040	5	—	$11G6$	$a_9, c_9^2, c_9d_9, c_{10},$ d_{11}, c_{12}		M_{12}
	5	·12!	$10p$	—	11G7			A_{12}
	6	12!	12	$12G5$	$11G8$		—	S_{12}
13	1	13		—		a_{13}		
	2	26		13G1		a_{13}, b_{13}^6		
	3	39		$13G1$		a_{13}, b_{13}^4		
	4	52		$13G1$		a_{13}, b_{13}^3	—	
	5	78		$13G1$		a_{13}, b_{13}^2		
	6	156	2	$13G1$		a_{13}, b_{13}	—	
	7	5616	2	—		a_{13}, c_{13}		$PSL(3, 3)$
	8	··13!	$11p$	—	$12G5$			A_{13}
	9	13!	13	$13G8$	$12G6$		—	S_{13}
14	1	1092	$2p$	—	$13G5$	a_{13}, b_{13}^2, a_{14}		$PSL(2, 13)$
	2	2184	3	$14G1$	$13G6$	a_{13}, b_{13}, a_{14}	—	$PGL(2, 13)$
	3	··14!	$12p$	—	$13G8$			A_{14}
	4	14!	14	$14G3$	$13G9$		—	S_{14}
15	1	360		—		a_{15}, b_{15}		-46
	2	720		$15G1$		a_{15}, c_{15}		S_6
	3	2520	2	—		b_{15}, d_{15}		A_7
	4	0160	2	—		d_{15}, e_{15}		$PSL(4, 2)$
	5	··15!	$13p$	—	$14G3$			A_{15}
	6	15!	15	$15G5$	$14G4$		—	S_{15}
16	1	80		e.a.		a_{15}, a_{16}		
	2	160		e.a.		a_{15}, a_{16}, e_{16}^2		
	3	240	2	e.a.		$a_{15}e_{15}, a_{16}$		
	4	288		e.a.		$b_{15}, a_{16}, f_{16}, g_{16}$		
	5	320		e.a.		a_{15}, a_{16}, e_{16}		
	6	480	2	e.a.		$a_{15}e_{15}, a_{16}, e_{16}^2$		
	7	576		e.a.		$b_{15}, a_{16}, f_{16}, g_{16}h_{16}$		

[continued on p. 180]

TABLE 1 (continued)

Degre	No.	Order	t	N	G_n	Generators	±	Comments
16	8	576		e.a.		b_{15}, a_{16}, f_{16}, g_{16}, $h_{16}g_{16}h_{16}$		
	9	960		e.a.		a_{15}, a_{16}, i_{16}		
	10	960	2	e.a.		$a_{15}e_{15}$, a_{16}, e_{16}		
	11	960	2	e.a.		a_{15}, a_{16},f_{16}		
	12	1152		e.a		b_{15}, a_{16}, f_{16}, g_{16}, h_{16}		
	13	1920		e.a.		a_{15}, a_{16}, j_{16}		
	14	1920	2	e.a.		a_{15}, a_{16}, k_{16}		
	15	2880	2	e.a.		$a_{15}e_{15}$, a_{16},f_{16}		
	16	5760	2	e.a.		$a_{15}e_{15}$, a_{16}, k_{16}		
	17	5760	$2p$	e.a.	15G1	a_{15}, b_{15}, a_{16}		
	18	11520	$2p$	e.a.	15*G*2	a_{15}, c_{15}, a_{16}		
	19	40320	3	e.a.	15*G*3	b_{15}, d_{15}, a_{16}		
	20	22560	3	e.a.	15*G*4	d_{15}, e_{15}; a_{16}		
	21	$\frac{1}{2}\cdot 16!$	$14p$	—	15*G*5			A_{16}
	22	16!	16	6*G*21	15*G*6		—	S_{16}
17	1	17		—		a_{17}		
	2	34		17*G*1		a_{17}, b_{17}^8		
	3	68		17*G*1		a_{17}, b_{17}^4		
	4	136		17*G*1		a_{17}, b_{17}^2		
	5	272	2	17*G*1		a_{17}, b_{17}	—	
	6	4080	3	—	16*G*3	$a_{15}e_{15}$, a_{16}, c_{17}		*PSL*(2, 16)
	7	8160	3	17*G*6	16*G*6	$a_{15}e_{15}$, a_{16}, e_{16}^2, c_{17}		
	8	16320	3	17*G*6	16*G*10	$a_{15}e_{15}$, a_{16}, e_{16}, c_{17}		
	9	$\frac{1}{2}\cdot 17!$	$15p$	—	16*G*21			A_{17}
	10	17!	17	17*G*9	16622		—	S_{17}
18	1	2448	$2p$	—	17*G*4	a_{17}, b_{17}^2, a_{18}		*PSL*(2, 17)
	2	4896	3	18*G*1	17*G*5	a_{17}, b_{17}, a_{18}	—	*PGL*(2, 17)
	3	$\frac{1}{2}\cdot 18!$	$16p$	—	17*G*9			A_{18}
	4	18!	18	18*G*3	17*G*10		—	S_{18}
19	1	19		—		a_{19}		
	2	38		19*G*1		a_{19}, b_{19}^9	—	
	3	57		19*G*1		a_{19}, b_{19}^6		
	4	114		19*G*1		a_{19}, b_{19}^3	—	
	5	171		19*G*1		a_{19}, b_{19}^2		
	6	342	2	19*G*1		a_{19}, b_{19}	—	
	7	$\frac{1}{2}\cdot 19!$	171	—	18*G*3			A_{19}
	8	19!	19	19*G*7	18*G*4		—	S_{19}
20	1	3420	$2p$	—	19*G*5	a_{19}, b_{19}^2 a_{20}		*PSL*(2,19)
	2	6840	3	20*G*1	19*G*6	a_{19}, b_{19}, a_{20}	—	*PGL*(2, 19)
	3	$\frac{1}{2}\cdot 20!$	$18p$	—	19*G*7			A_{20}
	4	20!	20	20*G*3	19*G*8		—	S_{20}

TABLE 2. *Generating Permutations*

Degree	Permutations
5	a = (1, 2, 3, 4, 5) *b* = (1) (2, 3, 5, 4)
6	*a* = (1, 6) (2) (3, 4) (5)
7	a = (1, 2, 3, 4, 5, 6, 7) *b* = (1) (2, 4, 3, 7, 5, 6) *c* = (1) (2, 3) (4, 7) (5) (6)
8	*a* = (1, 8) (2, 4) (3, 7) (5, 6) *b* = (1, 4) (2, 8) (3, 5) (6, 7) *c* = (1, 7) (2, 5) (3, 8) (4, 6) *d* = (1, 8) (2, 7) (3, 4) (5, 6)
9	*a* = (1, 2, 3) (4, 5, 6) (7, 8, 9) *b* = (1, 4, 7) (2, 5, 8) (3, 6, 9) *c* = (1) (2, 6, 4, 9, 3, 8, 7, 5) *d* = (1) (2) (3) (4, 7) (5, 8) (6, 9) *e* = (1) (2, 4, 9) (3, 7, 5) (6) (8) *f* = (1) (2, 7) (3, 6) (4, 5) (8, 9)
10	a = (1, 8) (2, 5, 6, 3) (4, 9, 7, 10) *b* = (1, 5, 7) (2, 9, 4) (3, 8, 10) (6) *c* = (1, 10) (2) (3) (4, 7) (5, 6) (8, 9)
11	a = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) *b* = (1) (2, 3, 5, 9, 6, 11, 10, 8, 4, 7) *c* = (1, 11) (2, 7) (3, 5) (4, 6) (8) (9) (10) *d* = (1) (2) (3) (4, 8) (5, 9) (6, 7) (10, 11)
12	*a* = (1, 12) (2, 11) (3, 6) (4, 8) (5, 9) (7, 10) *b* = (1) (2, 5) (3, 6) (4, 7) (8) (9) (10) (11, 12) *c* = (1) (2) (3) (4, 7) (5, 8) (6, 9) (10) (11, 12)
13	*a* = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13) *b* = (1) (2, 3, 5, 9, 4, 7, 13, 12, 10, 6, 11, 8) *c* = (1) (2, 3) (4) (5, 10) (6) (7, 11) (8) (9, 12) (13)
14	*a* = (1, 14) (2, 13) (3, 7) (4, 5) (6) (8, 12) (9) (10, 11)
15	*a* = (1, 15, 7, 5, 12) (2, 9, 13, 14, 8) (3, 6, 10, 11, 4) *b* = (1, 4, 5) (2, 8, 10) (3, 12, 15) (6, 13, 11) (7, 9, 14) *c* = (1, 7) (2, 11) (3, 12) (4, 13) (5, 10) (6) (8, 14) (9) (15) *d* = (1, 9, 5, 14, 13, 2, 6) (3, 15, 4, 7, 8, 12, 11) (10) *e* = (1, 3, 2) (4, 8, 12) (5, 11, 14) (6, 9, 15) (7, 10, 13)

[continued on p. 182]

TABLE 2 *(continued)*

Degree	Permutations

16	*a* = (1, 16) (2, 3) (4, 5) (6, 7) (8, 9) (10, 11) (12, 13) (14, 15)
	b = (1, 3) (2, 16) (4, 6) (5, 7) (8, 10) (9, 11) (12, 14) (13, 15)
	c = (1, 5) (2, 6) (3, 7) (4, 16) (8, 12) (9, 13) (10, 14) (11, 15)
	d = (1, 9) (2, 10) (3, 11) (4, 12) (5, 13) (6, 14) (7, 15) (8, 16)
	e = (1, 12, 7, 5) (2, 4, 13, 11) (3, 8, 10, 14) (6, 9) (15) (16)
	f = (1, 3, 2) (4, 12, 8) (5, 15, 10) (6, 13, 11) (7, 14, 9) (16)
	g = (1) (2, 3) (4) (5) (6, 7) (8, 12) (9, 13) (10, 15) (11, 14) (16)
	h = (1, 15) (2, 12) (3) (4, 10) (5) (6) (7, 9) (8) (11) (13) (14) (16)
	i = (1, 7) (2, 12) (3, 11) (4, 10) (5, 13) (6) (8) (9, 15) (14) (16)
	j = (1, 14) (2, 13) (3) (4, 11) (5) (6) (7, 8) (9) (10) (12) (15) (16)
	k = (1, 3) (2) (4, 8) (5, 11) (6, 10) (7, 9) (12) (13, 15) (14) (16)

17	a = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17)
	b = (1) (2, 4, 10, 11, 14, 6, 16, 12, 17, 15, 9, 8,5,13, 3, 7)
	c = (1) (2, 3) (4, 9) (5, 7) (6, 8) (10, 14) (11, 13) (12, 15) (16, 17)

18	a = (1, 18) (2) (3, 10) (4, 7) (5, 14) (6, 8) (9, 16) (11, 13) (12, 15) (17)

19	a = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19)
	b = (1) (2, 3, 5, 9, 17, 14, 8, 15, 10, 19, 18, 16, 12, 4, 7, 13, 6, 11)

20	a = (1, 20) (2, 19) (3, 10) (4, 7) (5, 15) (6, 16) (8, 9) (11, 18) (12, 13) (14, 17)

is given in the form of two tables. In Table 1 the groups are listed together with some facts about them. In Table 2 we give the generators for these groups which are referred to in Table 1. The groups in Table 1 are listed by degree and for a fixed degree by order. Beyond this the numbering is arbitrary. The order of the group is listed as is the transitivity t, whenever $t > 1$. If the group is t-fold primitive, this fact is indicated by the letter p following the transitivity. Generating permutations are given for all groups except the alternating and symmetric groups of each degree. The entries in this column refer to permutations in Table 2. For example, *a,* denotes the first permutation listed under degree 7 in Table 2. No attempt has been made to give generating sets with the fewest possible elements. Permutations in Table 2 should be considered defined on and fixing all integers greater than the degree under which they are listed. A minus sign (-) in the column headed ± indicates that the group contains odd permutations. Whenever the group G is doubly primitive so that the subgroup G_n fixing the last integer on which G acts is a primitive group of degree $n-1$, this subgroup G_n is given. The symbol $6G3$, for example, refers to the third group of degree 6. In all cases G_n is the actual group listed and not just permutation isomorphic to it. Any primitive group G of degree $n < 60$

has a unique minimal normal subgroup N. If $n \leqslant 20$, then N is simple and primitive or elementary abelian. If N is primitive, it is listed, with a dash (-) indicating that N = G. The letters e.a. mean that N is elementary abelian and imprimitive. We note that for groups 1, 2, and 5 of degree 8 N = $\langle a_8, b_8, c_8 \rangle$, for groups 1 to 7 of degree 9 N = $\langle a_9, b_9 \rangle$, and for groups 1 to 20 of degree 16 N = $\langle a_{16}, b_{16}, c_{16}, d_{16} \rangle$. Whenever the group is abstractly isomorphic to a member of one of the families of groups A,, S_n, *PSL(n, q), PGL (n, q),* this fact is noted in the last column. In those cases involving the groups $A_5 \cong PSL(2, 4) \cong PSL(2,5)$, $S_5 \cong PGL(2, 5)$, $PSL(2, 7) \cong PSL(3, 2)$, As $\cong PSL(2, 9)$ and $A_8 \cong PSL(4, 2)$, only one of the two or three possible designations is listed.

Great care has been taken to ensure the accuracy of these tables. However, the author would appreciate being informed of any errors that may be found.

REFERENCES

1. E R. Bennet: Primitive groups with a determination of the primitive groups of degree 20. *Amer. J. Math. 34* (1912), 1-20.
2. H. Burckhardt and H. Vogt: Sur les groupes discontinues: Groupes de substitutions. *Encyclopédie des sciences mathématiques pures et appliquées,* Edition Française. Algebre, Tome I, Vol. I (Arithmétique), Chapter I, § 8 (1909).
3. B. Fischer Eine Kennzeichnung der symmetrischen Gruppen vom Grade 6 and 7. *Math. Z. 95* (1967), 288-298.
4. M. Hall: *The Theory of Groups* (New York: The Macmillan Company, 1959).
5. M. Hall: Automorphisms of Steiner triple systems. *Proc. of the Symp. in Pure Math. 6* (1962), 47-66.
6. M. Hall: Block designs. *Applied Combinatorial Mathematics 369-405. (New* York: John Wiley & Sons, 1964).
7. D. G. Higman: Intersection matrices for finite permutation groups. *J. Algebra 6* (1967), 22-42.
8. T. C. Holyoke: On the structure of multiply transitive permutation groups. *Amer. J. Math. 74* (1952), 787-796.
9. D. R. Hughes: On t-designs and groups. *Amer. J. Math. 87* (1965), 761-778.
10. D. R Hughes: Extensions of designs and groups: projective, symplectic and certain affine groups. *Math. Z. 89* (1965), 199-205.
11. W. A. Manning: *Primitive Groups,* Part I *(Math. and Astron.,* Vol. I) (Stanford: Stanford Univ. Press, 1921).
12. G. A. Miller *Collected Works,* Vol. I (Urbana: University of Illinois Press, 1935).
13. E. T. Parker and P. J. Nikolai: A search for analogues of the Mathieu groups. *Math. Tables Aids Comput.* 12 (1958), 3843.
14. E T. Parker and K. I. Appel: On unsolvable groups of degree*p* = *4q*+ 1, *p* and *q* primes. *Canad. J. Math.* 19 (1967), 583-589.
15. C. C. Sims: Graphs and finite permutation groups. *Math. Z. 95 (1967), 76-86.*
16. H. Wielandt: *Finite Permutation Groups* (New York: Academic Press, 1964).
17. W. J Wong: Determination of a class of primitive permutation groups. *Math. Z.* 99 (1967), 235-246.

An algorithm related to the restricted Burnside group of prime exponent

E. KRAUSE and K. WESTON

Introduction. Denote the freest Lie ring of characteristic c on n generators satisfying the mth Engel condition by $L(c, n, m)$.

It is a long-standing conjecture, probably introduced by Sanov, that the Restricted Burnside Problem for prime exponentp is equivalent to the problem of nilpotency for $L(p, n, p-1)$. In this report we discuss a general algorithm for Lie rings which analogously to the collection process yields L(p, n, m) $(m<p)$ as the latter yields $R(p, n)$. This algorithm is not only more practical but can be readily used with a computer. For instance we applied the algorithm aided by a Univac 1107 computer for $p = 5$, $n = 2$, $m = 4$, and found $L(5, 2, 4)$ [1].

An associated matrix algebra of a Lie algebra. Suppose L is a Lie algebra over a field F spanned by elements $\beta = \{m_1, \dots, m_k\}$ and $M_{k\times 1}$ is the F-space of $k \times 1$ column matrices over F. Define the coordinate mapping f_β: $L \to M_{k+1}$ by $f_\beta(m)$ = column of coordinates of $m \in L$ with respect to some linear combination of β (i.e. if β is not a basis, $f_\beta(m)$ requires a choice between all of the linear combinations of β. In this case any fixed choice is sufficient for m). If Tis a linear operator of L let M,(T) designate the matrix whose ith column is $f_\beta(T(m_i))$. Also denote the inner derivation of $l \in L$ by $g(l)$. Then the associated F-algebra A_β of L consists of elements from $M_{k\times 1}$ under ordinary matrix addition and multiplication is defined by

$$c_1 \otimes c_2 = M_\beta(g(f_\beta^{-1}(c_2)) \times c_1, \quad c_1, c_2 \in A_\beta \tag{1}$$

(X denotes matrix multiplication).

The following theorems are easily verified.

THEOREM 1. *f_β is an isomorphism between L and A_β if and only if β is a basis.*

THEOREM 2. *If $L(p, n, m)/L^k(p, n, m)$ is spanned by $\beta = \{m_1, \dots, m_g\}$ modulo L^k (p,n,m) then A, is a Lie algebra over $GF(p)$ on n generators satisfying the m-th Engel condition if and only if*

$$A_\beta \cong L(p, n, m)/L^k(p, n, m).$$

The associated algebra of a finitely generated Lie algebra. If L *is* a Lie algebra with generators $x_1, \dots, x_n$, spanned by monomials $\beta = \{m_1, \dots,$

$m_k\}$, $m_i = m_i(x_1, \ldots, x_n)$, we show here an easy method to calculate A, from the matrices $M_\beta(g(x_1)), \ldots, M_\beta(g(x_n))$.

If $\lambda_1, \ldots . \lambda_k$ is the natural basis for A, then by (1)

$$\lambda_i \otimes \lambda_j = M_\beta(g(m_j))\, X\, \lambda_i$$

(i.e. $\lambda_i \otimes \lambda_j$ = the ith column of $M_\beta(g(m_j))$). Thus a multiplication table for A, is easily calculated by observing the columns of the matrices $M_\beta(g(m_1)), \ldots, M_\beta(g(m_k))$.

Because of our convention of writing operators on the left, the inner derivation g is a Lie anti-homomorphism of L into the algebra of linear operators :
$g(e \cdot m) = [g(m), g(e)] = -[g(e), g(m)]$, e, m EL, where $[T, S] = TS - ST$, S, T linear operators. Also $M_\beta(g(e \cdot m)) = [M_\beta(g(m)), M_\beta(g(e))]$ or more generally

$$M_\beta(g(e_1, \ldots, e_j)) = (-1)^{j+1}[M_\beta(g(e_1)), M_\beta(g(e_2)), \ldots, M_\beta(g(e_j))]. \quad (2)$$

Consequently (2) affords a simple formula for calculating $M_\beta(g(m_i))$, $i = 1, \ldots, k$ from the matrices $M_\beta(g(x_1)), \ldots, M_\beta(g(x_n))$.

Therefore, with restrictions on the size of k of course, one can use a computer to calculate and even print the multiplication table of A, given the matrices $M_\beta(g(x_1)), \ldots, M_\beta(g(x_n))$.

Algorithm for $L(p$, n, $m)$ $(m < p)$. Designate $L(p, n, m)$ *by* L; since $m<p$, $L(p, n, m)$ is nilpotent of class c [2]. We wish to use Theorems 1 and 2 to determine a basis β for L/L^k ($k = 1, 2, \ldots,$ c) from the bases of $L/L^2, \ldots, L^{k-2}/L^{k-1}$. Therefore A, $\cong L/L^k$ by Theorem 1.

Suppose L is generated by $x_1, \ldots, x_n$ and $L^\alpha/L^{\alpha+1}$ (a = 1, . . . , x- 1) has a basis consisting of monomials $\beta_\alpha = \{m_{\alpha,1} + L^{\alpha+1}, \ldots, m_{\alpha, j_\alpha} + L^{\alpha+1}\}$ $m_{\alpha, j_i} = m_{\alpha\, j_i}(x_1, \ldots, x_n)$. Next select any set of monomials

$$\beta_{k-1} = \{m_{k-1,1} + L^k, \ldots, m_{k-1, j_{k-1}} + L^k\}, m_{k-1, j_i} = m_{k-1, j_i}(x_1, \ldots, x_n)$$

which span L^{k-1}/L^k .For example β_{k-1} could consist of all of the monomials with k- 1 factors. Then L/L^k is spanned by

$$\beta = \{m_{1,1} + L^k, \ldots, m_{1, j_1} + L^k, \ldots, m_{k-1,1} + L^k, \ldots, m_{k-1, j_{k-1}} + L^k\}$$

and β constitutes a basis if and only if β_{k-1} is a basis. Thus if A, is a Lie algebra over $GF(p)$ on n generators satisfying the mth Engel condition, then $A_\beta \cong L/L^k$ by Theorem 2. Hence, by Theorem 1, β is a basis, which in turn implies that β_{k-1} is a basis. If A, fails to satisfy any of the above conditions, β_{k-1} must be a set of dependent vectors. Thus we have to select a proper subset spanning L^{k-1}/L^k and repeat the process.

This process of course only affords us a check whether a basis has been found for L^{k-1}/L^k and does not actually calculate one except by trial and error. The use of a computer to calculate A, has already been mentioned. A computer may be used also to scan the multiplication table of A, and determine which of the conditions of Theorem 2 are fulfilled by A,. A program for determining whether *A,* is a Lie algebra on ***n*** generators satisfying the mth Engel condition is on file in the Computing Science Library of the University of Notre Dame.

REFERENCES

1. E. KRAUSE and K. WESTON: The restricted Burnside group of exponent 5 (in preparation).
2. A. KOSTRIKIN: On locally nilpotent Lie rings satisfying an Engel condition. ***Doklady Akademii Nauk SSSR*** (1958), 1074-7.

A module-theoretic computation related to the Burnside problem

A. L. TRITTER

ALTHOUGH the Burnside conjecture is known to be true for exponent 4 (i.e. although it is known that finitely generated groups of exponent 4 are finite), we cannot usefully say that the Burnside problem is settled, even in this case. For instance, a sharp bound on the order of B(4, n) would be valuable, and there are perhaps other questions that arise in consideration of the Burnside problem whose answers would be of interest.

1. Introductory considerations. Defining the lower central series $\{G_i\}$ and the derived series $\{G^{(i)}\}$ of a group G in the usual way :

$$G_1 = G, \ G_{i+1} = [G_i, G],$$
$$G^{(0)} = G, \ G^{(i+1)} = [G^{(i)}, G^{(i)}],$$

where $[H, K]$ ($H \subseteq$ G, $K \subseteq$ G, G a group) is the least subgroup of G containing all commutators $h^{-1}k^{-1}hk$ ($h \in H$, $k \in K$), we know that, for every group G and for every natural number n, $G^{(n)} \subseteq G_{2^n}$. But we can deduce from a result of C. R. B. Wright [1] that, when G is of exponent 4, any inclusion $G^{(r)} \subseteq G_s$ not predicted from this elementary result (i.e. with $2^r < s$) must lead to a bound for the derived length of G. If we choose G = $B(4, 8)$ and n = 3, what we are saying is this:

(i) we know $G^{(3)} \subseteq G_8$ to be true ;

(ii) if we could show $G^{(3)} \subseteq G_9$ we could bound the derived length of every group of exponent 4.

The bound would be applicable to all groups of exponent 4 because of the natural homomorphisms to groups of exponent 4 on fewer than 8 generators and the fact that, for any group G, $G^{(3)}$ is generated modulo G_9 by commutators of the form

$$[[[a_0, a_1,], [a_2, a_3]], [[a_4, a_5], [a_6, a_7]]],$$

where the a, are among the generators of G, so that no more than 8 distinct generators of G could be present in any one of these commutators. We wish, therefore, to show that:

With G = B(4, 8) generated by go, $g_1, \ldots, g_7$, the commutator

$$[[[g_0, g_1], [g_2, g_3]], [[g_4\ g_5], [g_6, g_7]]]$$

lies in $G^{(3)}$ modulo commutators of order higher than 8.

It is sufficient to place this one commutator, since both $G^{(3)}$ and G_9 are plainly Se-modules (S_8 acting by permuting the g_i), and commutators of the same apparent form, but in which not all generators which appear are distinct, can be taken to be homomorphic images of commutators of this form with all generators distinct.

Professor G. Higman, to whom I am indebted for this problem, has shown [2] that this group-theoretic question is equivalent to the following module-theoretic question (which arises upon examination of the associated Lie ring of G):

> In the free Lie ring of characteristic 2 on 8 generators $x_0, x_1, x_2, \ldots, x_7$ we consider the element $\sum x_0\, x_{1\sigma}\, x_{2\sigma} \cdots x_{7\sigma}$ (multiplications to be performed from left to right;, where the σ are precisely those permutations (there are 1312 such) on the integers $1, 2, \ldots, 7$ for which $(i+1)\sigma < i\sigma$ for no more than two values of *i*.
>
> Letting S_8 act by permuting the integers $0, 1, 2, \ldots, 7$ occurring in the subscripts on the x_i, we generate an S_8-module from this one element, and we then close this S_8-module under addition (in the ring), yielding an additive S_8-module.
>
> Question-does the element $(((x_0x_1)(x_2x_3))((x_4x_5)(x_6x_7)))$ lie in this additive S_8-module ?

This paper is concerned with the use of the I.C. T. Atlas, located at Chilton, Berkshire, and sponsored by the Atlas Computer Laboratory of the U.K. Science Research Council, to answer this question.

2. General approach. To search for an element in a finite additive module (and this one has no more than 2^{81} elements) is a task most straightforwardly accomplished by representing the module as a finite-dimensional vector space, obtaining a basis, and seeing whether the "target" element is linearly dependent upon this basis. It is clear that all the ring elements which interest us, whether target or "data", are balanced homogeneous elements of weight 8; it is therefore true that the space they span lies within that generated by ***all*** the balanced homogeneous elements of weight 8, equivalently by the left normed monomials in which the x_i appear once each. The 5040 balanced left-normed Lie monomials of weight 8 with x_0 appearing first are known on Lie ring-theoretic grounds to be linearly independent and to generate (additively) all these monomials, and hence any element of that part of the ring on which our attention is focused has a unique expressionas a sum of terms drawn from among them; this expression may be found by repeated application of the second and third of the "Jacobi identities" appearing in the customary definition of a Lie ring :

(i) $aa = 0$ for all elements a

(ii) $ab+ba = 0$ for all elements a and b

(iii) $a(bc) + b(ca) + c(ab) = 0$ for all elements a, b and c.

Thus, our problem splits into two parts in a completely natural way. We must, first, represent the data by a matrix, 8! by 7!, over the field with 2 elements (each row giving the expression of a single data element in terms of the balanced left-normed Lie monomials of weight 8 with x_0 at the far left), and, second, triangularize this matrix, meanwhile searching for proof that the target vector is, or is not, representable as a sum of rows of the matrix.

We observe that, as representations are unique, no question can arise as to whether we shall recognize the target when we see it, and that the one ring element from which all other data elements are generated actually arises in the form desired, namely as a sum of (13 12) balanced left-normed Lie monomials of weight 8, with x_0 appearing first in each term. Henceforward, we reserve the word "term" for this rather special sort of term, a balanced left-normed Lie monomial of weight 8 on the letters $x_0, x_1, x_2, \ldots, x_7$, with x_0 appearing at the far left.

3. Generating the matrix. The module appearing in the question we are dealing with has been embedded in the vector space of dimension 7! over $GF(2)$ and is therefore of dimension no more than 7!, and the addition of the vector space is the ring-addition. But the second operation (upon terms) with which we are concerned is not the second ring operation, Lie multiplication, but is rather that operation upon terms induced by permuting the ring generators $x_0, x_1, x_2, \ldots,$ x7. Now it is self-evident that any permutation of the generators which fixes x_0 merely induces a permutation of terms, but a hand-calculation upon a few examples of the effect of a permutation of generators not fixing x_0 will easily convince the reader that the situation here is not so simple. We therefore choose an 8-cycle $\boldsymbol{R}$ from S_8 and represent every element of S_8 as the composition of some power of $\boldsymbol{R}$ with a permutation fixing 0 (remember, we think of S_8 as acting on the subscripts, not the generators).

The single generator of the &-module we are producing leads to a total (including itself) of 8 elements if we construct the R-module it generates, and these 8 elements generate as &-module the structure we want; here S_7 is the subgroup of S_8 which fixes 0. But the action of S_7 upon terms ***is*** merely to permute them in the obvious way, and it is therefore the case that, once we have 8 generators for an &-module instead of only one for an &-module, the two operations we need are simply the addition and multiplication of the group ring of S_7 over GF(2). It is furthermore true that the full significance for our structure of the Jacobi identities will have been expressed in the technique we use to apply the operation on terms induced by ***R***, in getting from one generator for an &-module to 8 generators for an ST-module.

To sum up, for reasons of computational simplicity we shall not look directly at the Ss-module generated by $\sum x_0x_{1\sigma}x_{2\sigma}\ldots x_{7\sigma}$, but we shall see it by looking at the S_7-module genera&d by

$$\Big\{\sum_{\sigma} x_{0R^i}x_{1\sigma R^i}x_{2\sigma R^i}\ldots x_{7\sigma R^i}\,\Big|\, 0 \leqslant i < 8\Big\}.$$

4. The **R-module.** There is a natural mapping from the group ring of S_8 over $GF(2)$ onto that part of our Lie ring we have already termed interesting, the balanced homogeneous elements of weight 8, induced by mapping

$$\begin{pmatrix}0 & 1 & 2 \ldots 7\\ \alpha_0 & al & a2 \;.\;.\;.\; \alpha_7\end{pmatrix}$$

onto the balanced left-normed monomial $x_{\alpha_0}x_{\alpha_1}x_{\alpha_2}\;.\;.\;.\;x_{\alpha_7}$, clearly of weight 8, and extending linearly. Also, there is a one-to-one mapping onto the group ring of S_7 (the subgroup of S_8 fixing 0) over $GF(2)$ from this same part of the Lie ring induced in exactly the same way, but requiring the element of the Lie ring to have been expressed in its unique form as a sum of left-normed monomials in which x_0 appears first. The composition of these two mappings is a mapping μ from the group ring of S_8 over GF(2) onto the group ring of S_7 over GF(2), fully expressing the effect of the Jacobi identities in this part of the Lie ring. It should be observed that the restriction of μ to the group ring of S_1 (the subgroup of S_8 fixing 0) over GF(2) is the identity mapping.

It should now be clear that to construct the mapping on terms induced by ***R***, we need only know how to multiply each element

$$\alpha = \begin{pmatrix}1 & 2 & ,,, & 7\\ \alpha_1 & \alpha_2 & ,\;,\;, & \alpha_7\end{pmatrix} \text{ of } S_7,$$

seen as an element

$$\begin{pmatrix}0 & 1 & 2 & . & ..7\\ 0 & \alpha_1 & \alpha_2 & .\;.\;. & \alpha_7\end{pmatrix} = \alpha$$

of the group ring of S_8 over ***GF(2)***, by ***R***, and obtain the image under μ in the result. This, in fact, is precisely what we do. The ***R*** we employ (it could have been any B-cycle) is

$$\begin{pmatrix}0 & 1 & 2 \ldots 7\\ 1 & 2 & 3 \ldots 0\end{pmatrix}; \quad \text{i.e.} \quad iR = \begin{cases} i f\,! & 0 \leqslant i < 7\\ 0 & i = 7\end{cases}.$$

The method is as follows. For every $x \in S_7$ there is a unique k, $0 < k < 8$, and a unique $z \in S_7$, such that $xR = R^kz$. We regard this relation as defining two functions k and z of x, and we tabulate these two functions. That is, we serially number the elements of S_7 so that for every $g \in S_7$ there is a unique $\bar{g}$, $0 \leqslant \bar{g} < 5040$, corresponding to it, and we construct two tables of 5040 entries so that as x varies over S_7 we have 2^{7-k} in the one, and $\bar{z}$ in the other, in the $\bar{x}$th entry. We also construct a table in which appear the $R^k\mu$; in fact, we must multiply $R^k\mu$ by z in calculating $xR\cdot \mu = R^kz\cdot \mu =$ $= R^k\cdot z\mu = R^k\cdot \mu z = R^k\mu\cdot z$ (since multiplication in the group ring is associative, and $z \in S_7$). As it can be shown that the number of terms occurring in $R^k\mu$ is 2^{7-k} for $0 < k < 8$, and as it is clear that $e\mu$ = e (where e is the identity of S_8), we give this table 128 entries:

in the Oth, we place $\bar{e}$
in the 1st, we place the serial number of the term $R^7\mu$,
in the 2nd-3rd, we place the serial numbers of the terms of $R^6\mu$,
in the 4th--7th, we place the serial numbers of the terms of $R^5\mu$,
in the 8th-15th, we place the serial numbers of the terms of $R^4\mu$,
in the 16th-31st, we place the serial numbers of the terms of $R^3\mu$,
in the 32nd-63rd, we place the serial numbers of the terms of $R^2\mu$,
in the 64th-127th, we place the serial numbers of the terms of $R\mu$.

It is now the case that the quantity 2^{7-k} (which must at first have appeared quite artificial) gives not only the length of the block in this table corresponding to R^k, but also where in the table to look for it: the serial numbers of the terms of $R^k\mu$ begin at the 2^{7-k}th entry and occupy 2^{7-k} entries.

It is necessary to explain that we have recorded $\bar{e}$ in this table in order to make considerably more efficient the operation of multiplying by z. The problem is that, as will be more fully explored below, we do not know how to right-multiply an element of the group ring (from now on, of S_7 over *GF(2)*, represented as a sequence of serial numbers unambiguously delimited) by an arbitrary element of S_7; what we *do* know how to do is to right-multiply by each element of S_7 in turn, without having any idea of which is which, nor of the order in which they appear (to be sure, without repetitions or omissions). We have, therefore, retained $\bar{e}$ so that, when the entries in this 128-entry table are modified so as to represent the effect of right-multiplying them all by a specific but unknown element of S_7, we can look at the Oth entry to find the effect of the multiplication upon the identity element of the group, and hence to find by what element we have multiplied; if we are applying the operation on terms induced by R to an element of the group ring in which the term x appears, and if $xR = R^kz$, and if the Oth entry is $\bar{z}$, then the block of entries starting at the 2^{7-k}th and going on for 2^{7-k} entries gives the serial numbers of the terms of $xR\mu$.

This method allows us to proceed from each generator of the &-module to the next, starting with the sole generator of our &-module. After seven applications of it, we have eight ring elements forming an R-module, and these generate as S_7-module the structure we want.

5. The **&-module.** Let the eight ring elements so far constructed be called $P_0, P_1, P_2, \ldots, P_7$, in the order in which they were obtained. Then P_0 is the generator originally given for the S_8-module and, if we regard the P_i for the moment as elements of the group ring of S_8 over ***GF(2), we*** have $P_i = P_{i-1}R\mu\,(0<i<8)$; the 8! rows of our data matrix are seen to be the elements ***Pig*** $(0 \leq i < 8,\ g \in S_7)$ of the group ring of S_7 over ***GF(2).*** What we have still to do to be able to construct this matrix is discover how to multiply an arbitrary element $\boldsymbol{P}$ of the group ring by an arbitrary element g of the group; equivalently, since $\boldsymbol{P}$ is represented as a sequence of the serial numbers of those elements of S_7 which appear in it (coefficient 1 rather than 0), we want to construct for each $g \in S_7$ a function that will get us from $\bar{x}$ to $\overline{xg}$ for every $x \in S_7$.

This function is, of course, the right regular representation of S_7, and it is most easily displayed as the Cayley table of that group; the table has $(7!)^2$ entries, more than 25 million. Let us look more closely at what we are actually obliged to do:

> For an element Pof the group ring, which we might as well regard as arbitrary (of course it is not, but it is about the structure of $\boldsymbol{P}$ that we hope to learn), we must be able to compute ***Pg*** for every $g \in S_7$, but we do not care in what order we compute these, nor yet which is which, just so long as our computation is exhaustive.

Our original thought was to enumerate S_7 in some way go, $g_1, g_2, \ldots, g_{5039}$ and produce successively $Pg_0, Pg_1, Pg_2, \ldots, Pg_{5039}$, but to right-multiply an arbitrary $\boldsymbol{P}$ by g_i requires the availability of the entire column of the Cayley table of S_7 which corresponds to the group element g_i, and this is unmanageable. Suppose, however, that the enumeration $\{g_i\}$ is such that $g_{i-1}^{-1}g_i$ takes only comparatively few distinct values ; then $Pg_i = Pg_{i-1} \times g_{i-1}^{-1}g_i$ can be derived at each step from Pg_{i-1} rather than from $\boldsymbol{P}$, and only comparatively few columns (***four*** will suffice) of the Cayley table need be available.

This enumeration is recognizable as one of the central problems of campanology (bell-ringing: ***vide infra***), and there is an extensive and centuries-old non-mathematical literature about it. There is also a developing mathematical literature on the subject [3].

The campanological approach we have actually taken to this problem uses a composition attributed [4] to John Vicars (most likely date: 1740) for a full peal of Grandsire Triples; more familiarly, we have taken from Vicars the specihcation of four elements ***ho,*** $h_1, h_2, h_3 \in S_7$ and a function k:5040→4 (a sequence $k_0, k_1, k_2, \ldots, k_{5039}$ all drawn from among 0, 1,2,3) such that if we put $g_0 = h_{k_0}$ and $g_i = g_{i-1}h_{k_i}$ $(0 < i < 5040)$, then go, g_1, $g_2, \ldots, g_{5039}$ constitutes an enumeration of S_7. The function $\boldsymbol{k}$ and the columns of the Cayley table of S_7 which correspond to h_0, h_1, h_2, h_3 are all computed and stored, making possible the right-multiplications which we need for this section; but, as explained above, this multiplication is also perfectly satisfactory for calculating the R-module beforehand.

Theoretically, then, we have solved the problem of generating the data matrix; practically, a program having the structure here specified has been written, debugged, and run on Atlas. It occupies approximately 500 words of store and takes about six minutes to run, but its tables fill the core store; the part of the program which computes ***k***, the campanological subroutine, takes 43 instructions and 9 words of tables (in machine code), and runs in a few milliseconds. The program writes the data matrix onto magnetic tape, and ends by wriiing out a "key block" containing such information as the target vector and how much of the triangularization (none, at this stage) has already been done.

6. **Bell-ringing.** To the reader entirely unfamiliar with campanology (as pursued in England) I can offer no better advice than to entertain himself reading Dorothy Sayers' delightful detective novel ***The Nine Tailors*** *[5]*, where he will find an enticing introduction to the subject and an adequate bibliography; when I recognized my problem as possibly campanological this was the sole source of my own familiarity. I then, however, approached D. Roaf, of Oxford University, for a tutorial session on mathematical campanology (something I was not then certain existed), and it is to him that I must express heartfelt thanks for a more detailed exposition of the subject.

Broadly, then, let us suppose that we are ringing n bells. We ring them all, one after the other, in some sequence; this is called a ***row*** of the composition. Then we ring another row; the place-permutation (not the letter-permutation) applied to the bells to get from one row to the next is called a change-hence the term change-ringing. The way in which a ringer memorizes his duty varies a little, but ordinarily he learns the changes and various sequences (called ***leads***) of $2n$ changes ; a ringer learning to conduct will certainly also learn the orbits, or parts of the orbits, of several bells, and will be able to give simple rules for the sequencing of leads in any composition with which he is familiar. But as every ringer must memorize all the changes employed, only a few group elements h_i can occur, and as the rules a conductor learns are simple, the function ***k*** must be easy to calculate.

As to nomenclature, the term Triples signifies that $\boldsymbol{n} = 7$, and a ***method*** on n bells is a set of h_i, so that in Grandsire Triples we have seven bells and four changes (1)(23)(45)(67), (12)(34)(56)(7), (12)(3)(45)(67), (1)(2)(3)(45)(67); a ***composition*** is a function ***k*** specifying a sequence for the h_i.

7. **Triangularizing the matrix.** At this stage, our problem is as follows: given 8! vectors of dimension 7! over ***GF(2),*** and one more such vector, is or is not the one a linear combination of the 40320? In general, such

a question is most straightforwardly answered by developing a triangular basis for the space spanned by the row vectors, and “pivoting” each basis vector in turn “out” of the target vector; if there appears no basis vector at all to correspond to some non-zero coordinate of the target vector then the answer is found to be “no”, if the target vector suddenly disappears then we know the answer is “yes”. Triangularizing a matrix is neither entertaining nor interesting.

When interest is aroused, it is by one or other of the effects that scale can have on this problem. Most usually, the interest lies in problems of loss of significance caused by limitations on the accuracy with which matrix elements can be retained. But our problem is not of this kind; as our matrix is over a finite field, we necessarily retain absolute accuracy. Indeed, as the field is GF(2), each exact matrix element occupies only one bit in memory, vector addition is represented by the “exclusive-or” operation, and multiplication does not arise. In our problem, the sheer immensity of the data leads to a class of questions concerning the distribution in time of machine errors.

Once we have said this, we have opened Pandora’s box. When a mathematical “proof” is based in part upon error-preventing, error-detecting, and error-correcting techniques whose reliability is statistical in character, the nature of proof is utterly unlike anything David Hilbert might have recognized as such. But this problem goes far beyond the scope of the present paper; we shall attempt to discuss it elsewhere. In this paper, we shall do no more than to look briefly at some of the methods actually employed in the computer program which makes the calculation.

If the answer to our question is “yes”, if the target vector is a linear combination of the data vectors, then it is found to be so in an explicit way, and detailed record-keeping along the way should make it possible to say something like :

> The target vector is the sum of such and such basis vectors and, for each of them, this basis vector is the sum of that data vector and those earlier basis vectors.

In this case we should have available an effective, and cheap, way of confirming that the answer is indeed “yes”.

But suppose the answer to be “no”. Then we are asserting that there are $2^{8!}$ linear combinations of the data vectors, and that the target vector is none of them. How can such an assertion be verified, except exhaustively (i.e. by doing it again)? Well, there *is* one thing available for us to try-if the matrix actually yielded 7! basis vectors, there has surely been an error. But if only a smaller number have appeared, we are on no surer ground than before.

Let us recapitulate. An affiative answer would be verified if we were to maintain records from which the “pedigree” of the target vector and every basis vector could be determined. A negative answer could be made marginally more convincing if we knew the rank of the data matrix. But, in general, to be justified in accepting a negative answer, we must repeat the entire calculation at least once.

Suppose we do so. And suppose the answer is now "yes". What do we do ? Or suppose the answer is again "no". How reliable is a single bit? Should we try again ? Or what?

What, in fact, we do is this. We do, of course, keep the pedigree records, and we always know how many basis vectors have been found. But, in addition, every operation (including the checking operations) is performed twice, and the results are compared, bit by bit. In a single magnetic tape pass, the data matrix is read in from two separate files assumed to hold identical data, and, for so long as that is true, the common value of the input data is accepted; as wide as possible a section of the data matrix is processed ***en passant*** and the result is written out as a data file. Then it is done again; the same two data files are read in and compared a second time, their common value processed a second time, and the result written out as a second file which should be identical to the first. These two data files are the input to the next tape pass, when they will be compared bit by bit (and each file consists of more than 200 million bits), ***twice,*** and so on. The basis vectors developed on the first run through a pass go onto an output tape, those from the second onto another, at the time; these are compared explicitly, twice (of course), after the second time through. If at any stage a discrepancy is discovered between tapes whose contents should be identical, elaborate signalling and recovery procedures are automatically put into operation; we shall say no more about these but that we have available, on a typical tape pass, three sets of tapes, called ***A, B,*** and C, such that if we are now reading data from ***B*** and writing it to ***C,*** then ***B*** was written on the previous pass and ***A*** was being read on that pass. That way, if we discover a discrepancy in the ***B*** tapes after having written upon the C tapes, the ***A*** tapes (from which ***B*** were made, and which have already satisfied two bit-by-bit comparisons) are still intact. When I say that the data matrix occupies a file taking up two reels of tape, you will see that this program keeps 14 tape drives busy – ***A, B, C,*** each 2 reels long, + 1 reel output for basis vectors, X2 copies of everything.

A magnetic tape pass takes about 18 minutes from beginning to end, of which the second half is a repetition of the first; the program can be interrupted under switch control, with effectively no wastage of machine time, at any such breakpoint. Another switch will cause the program to pause at the next breakpoint and await the instruction to interrupt or to proceed; yet another, inspected by the program three times per second of elapsed time, says to interrupt at once, discarding anything done since the last previous breakpoint. Other switches instruct the program whether to stop or to go on to get the rank of the data matrix in case the answer is found to be "yes", in case it is found to be "no", in which of two modes a continuously monitored visual display is to show progress, and finally something slightly peculiar. Suppose that an input discrepancy is found on, say, a ***B-C*** pass. A decision is taken to "back off" and run ***A*** → ***B*** again. Now, if this decision is implemented immediately, no new problem arises. But, suppose as well that we interrupt at this point; then, when we go back onto the machine to re-run ***A-B,*** there is no record anywhere except in our own minds that it is not possible to back off from this pass (as C is not the predecessor of ***A*** here-it has been altered on the abortive ***B-C*** pass). The last switch is used to inform the program that thejirst magnetic tape pass of the present machine run is one from which no back-off is possible; it is, of course, used on the very first run, as well as in the more complex situation described above.

One more word about the triangularization. It has been necessary, for efficiency's sake, to economize as much as possible on the total time for which the program occupies Atlas, and this has meant developing a new triangularization algorithm. This algorithm will be discussed elsewhere, rather than here. It is a natural modification of existing methods, simply taking maximal advantage of the fact that the matrix is over a finite field while, at the same time, using the space outside the upper right triangle of the matrix, as it is progressively vacated by the triangularization, as the place to record all the "pedigree" data (there is exactly the necessary amount of space).

8. **Present status.** The matrix-generating program is written, debugged, and run. The triangularization algorithm has been tested by hand, and is correct. The triangularization program is written and undergoing debugging.

REFERENCES

1. C. R. B. Wright: On the nilpotency class of a group of exponent four. ***Pac. J. Maths.*** 11 (1961), 387-394.
2. Unpublished private communication.
3. S. M. Johnson: Generation of permutations by adjacent transposition. ***Maths. Comp.*** 17 (1963), 282-285.
4. J. Armiger Trollope: ***Grandsire:*** The Jasper Snowdon Change-ringing Series, pp. 51, 122 (Whitehead & Miller, 1948).
5. Dorothy L. Sayers: ***The Nine Tailors*** (Victor Gollancz, 1934, many reprints).

Some combinatorial and symbol manipulation programs in group theory

JOHN J. CANNON

Introduction. Over the past two years computers have been used to carry out a number of large calculations, of both a numerical and non-numerical nature, arising out of research in group theory at Sydney. These problems include :

(i) construction of subgroup lattices;
(ii) investigation of positive quadratic forms;
(iii) determination of the groups of order $p^6, p > 2$;
(iv) construction of counter-examples to Hughes' conjecture in group theory.

Only (i), (iii) and (iv) will be discussed here.

All programs described here have been written in the English Electric KDF9 Assembly Language, USERCODE.

Subgroup lattices. A program has been written which determines the generators and relations of all the subgroups of a finite soluble group. The program finds the subgroups using the same method as Neubüser [I] with the difference that as a subgroup of order d is found the generators and relations of all possible groups of order d are checked through to find a set of generators and relations for the subgroup. As the program is restricted to groups of order less than 400 by machine considerations, one only needs to know all the possible groups of order less than 200, and most of these are known.

The program reads the generators and relations of the given group and, using coset enumeration, finds a faithful permutation representation (possibly the regular representation). The permutation representation is used to determine the elements of the group and to find its Cayley table, and is then discarded. At the same time as the group elements are being found as permutations they are also found as words in the original abstract generators. These n words are stored in an n-word stack so that instead of using either the abstract word or its permutation representation, one uses the number indicating the position of the group element in this stack. The Cayley table may then be stored compactly as a Latin square with several entries stored in a single machine word. In this manner the multiplication tables of groups of order up to 380 may be kept in-the core of a 32K machine. Only when group elements are being output is reference made to the stack of group words.

The user has the option of outputting either the generators and relations of each subgroup or the elements of the subgroup or both.

So far the program has been run successfully for a number of small groups (all of order less than 100). Before larger groups can be run more sets of generators and relations have to be checked and included in the program.

Investigation of groups of order $p^6, p > 2$. R. James has been enumerating the p-groups of order $p^6, p > 2$, checking the work of Easterfield, by the method of isoclinism.

Isoclinism [2, 3] splits the possible sets of generators and relations into classes so that all members of a class have the same commutator relations. The problem then is to find all the non-isomorphic groups within each isoclinism class.

We may suppose that isomorphism is an automorphism and apply a general automorphism to a general set of generators and relations (remembering that commutator relations are invariant within an isoclinism class). This will give rise to a set of relations on the integers mod n, for some n (obtained by equating indices of each generator before and after the automorphism). For p-groups, $n = p^r$ for some r. These relations can be expressed as an equivalence relation on a set of matrices over GF(p). The equivalence classes of these matrices give the non-isomorphic groups of this isoclinism class.

Difficulties arise in the determination of a set of equivalence class representatives for general p and it is to this problem that a computer has been applied. Using a computer it is simple to calculate the equivalence classes and to select a suitable equivalence class representative (an element which will give the corresponding generators and relations in the simplest possible form) for each class, for the first few primes. It is then usually easy to write down a set of equivalence class representatives for general p.

The groups of order p^5 $(p > 2)$ were checked by this method and the groups of order p^6 $(p > 2)$ are being found.

Hughes' conjecture and commutator calculations. Consider a group G of order p^a where p is a prime. Take the subgroup H of G generated by the elements of G having order greater than p. We suppose that G has some elements whose orders are greater than p. Then Hughes' conjecture is that **H** is of index 1 or p in C. It is true for $p = 2, 3$.

G. E. Wall has shown that the conjecture is false for p if a certain expression **E** is zero in a Lie algebra generated by two elements of nilpotency class $2p-1$, satisfying the (p - 1)th Engel condition, over $GF(p)$.

Hand calculations carried out by Wall show that the conjecture is false for $p = 5$. As the calculations are extremely long and tedious, it was decided to develop programs to verify the calculations for $p = 5$, and to carry them out for $p = 7$ and 11.

The problem will be considered in four parts:

(1) Determination of a basis for the two-generator free Lie algebra of nilpotency class $2p - 1$.

(2) Determination of a basis of the algebra in (1) with the $(p-1)$th Engel condition imposed.

(3) Calculation of the expression E

(4) Expression of E in terms of the basis elements found in (2).

These will now be considered in turn.

(1) Let ξ and η denote the two generators of the algebra. We define the weight of an arbitrary element of the algebra as follows: The elements ξ and η are of weight one. If A = $(P$, Q) is an element of the algebra, then

$$\text{weight A} = \text{weight P} + \text{weight Q}.$$

Basic commutators are next defined together with an ordering $(<)$ on them. The elements ξ and η are basic. Under the ordering all basic commutators of weight w come after those of weight $w-1$. Ordering is arbitrary among basic commutators of weight w, but once an ordering is chosen it must be adhered to. A commutator C = (A, B), A = $(P$, Q), where A and B are basic, is basic if A $> B$ and $B \geqslant Q$.

The elements of weight w form a subspace of the algebra and a basis of this subspace is provided by the basic commutators of weight w [4].

Given an element of the algebra, (A, B), where A $= \Sigma\lambda_i C_i$, $B = \Sigma\mu_j C_j$, C_i, C' basic, we describe a collection process [5].

(i) Put $(A, B) = \Sigma\lambda_i\mu_j\ (C_i, C_j)$.

(ii) If C_i and C_j are basic, put

(a) $(C_i, C_j) = 0$ if $C_i = C_j$,

(b) $(C_i, C_j) = -(C_j, C_i)$ if $C_i < C_j$,

(c) $(C_i, C_j) = (C_i, Cj)$ if $C_i > C_j$.

(iii) If $C_i > C_j$ are basic and $C_i = (P_i, Q_i)$, put

(a) $(C_i, C_j) = ((P_i, Q_i), C_j)$ if $C_j \geqslant Q_i$,

(b) $(C_i, C_j) = -((Q_i, C_j), P_i) + ((P_i, C_j), Q_i)$ if $C_j < Q_i$.

(iv) Return to (i) and repeat the process until (A, B) is expressed as a linear combination of basic commutators.

A program has been developed which calculates the basic commutators of weight w by combining all the basic commutators of weight w- 1 with ξ and μ in turn, and applying the collection process.

The basic commutators are placed in a stack as they are formed and so the order of occurrence of the commutators in this stack gives a suitable ordering of the basic commutators. Each basic commutator (P, Q) is stored in the stack as a number pair (p, q), where p is the integer giving the position of the basic commutator p in the stack and similarly for q.

For the collection process linear combinations of commutators are stored in a list structure. List elements consist of two consecutive words the first of which contains the coefficient of the present term and a pointer to the next term, while the second contains the commutator in the form $((p, q)$, r). New list elements may be obtained from a free space list.

When the Jacobi identity is applied to commutators of weight w, one requires A = $(P$, Q), P, Q basic, weight A less than w, to be expressed in terms of basic commutators. So to avoid much recalculation, after all the basic commutators of weight w have been found, all products of pairs of basic commutators giving linear combinations of basic commutators of weight w are calculated and entered in a table. It is possible to arrange the table so that no space is wasted and so that products can be looked up quickly. In the table commutators are again represented in a list structure, this time, however, using one word list elements. Each list element contains the coefficient of the present term, the number giving the position of the commutator in the stack of basic commutators, and a pointer giving the address of the next term.

On a KDF9 with a 16K store, the 2538 basic commutators of weights equal to or less than 14 were found in 5 minutes. When the store is increased to 32K, the machine will be able to find the 4720 basic commutators of weights equal to or less than 15. I hope also to express all terms of the Campbell-Baker-Hausdorff formula, of weights equal to or less than 15, in terms of basic commutators.

(2) The $(p-$ 1)th Engel condition states that

$$(- - - (A, \underbrace{B) - - - , B)}_{p-1} = 0$$

where B is an arbitrary element of the Lie algebra.

The basic commutators of weights less than p remain independent. For weights greater than p- 1 one first finds the basic commutators as in (I), and then derives all the relations between them generated by the Engel condition. These relations give rise to a homogeneous system of linear equations in the basic commutators over $GF(p)$, which upon solution gives a linearly independent set of basis elements, i.e. Engel basic commutators.

The programming is tedious but straightforward.

(3) The expression E is constructed as follows (all variables are non-commutative and the polynomials are over $GF(p)$ from (iv) on):

(i) $a(X, Y) = ((---\underbrace{(Y,X),X)\ ---\ )X}_{p-1\ X\text{'s}})$ where $(A, B) = AB - BA$.

(ii) $b(X, Y)$ = coefficient of $\lambda^{p-1}\,\mu$ in $(\lambda X+\mu Y)^p$.

(iii) $c(X, Y) = b(X, Y) - a(X, Y)$.

(iv) $d(X, Y) = \sum_{i=0}^{p-2} \frac{1}{(i+1)!} C^{(i)}(X, Y)$ where (i) denotes a certain ith derivative.

(v) $e(X, Y) = \sum_{i=0}^{p-2} (X+Y)^i\, d(X, Y)\, (X+Y)^{p-i-2}$.

(vi) $f(X, Y)$ = set of terms of $e(X, Y)$ involving $(p-1)$ X's and $(p-1)$ Y's. Now put $X = \bar{\xi}$, $Y = \bar{\mu}$ where $a\bar{b} = (a, b)$. (The Lie algebra product.)

(vii) $E = \bar{\xi} f(\bar{\xi}, \bar{\mu})$.

A powerful programming system was developed with the ability to handle non-commutative as well as commutative polynomials. It is hoped to publish a description of this system shortly.

As an illustration, the polynomial $f(X, Y)$ for $p = 7$ contains about 840 terms and took 3 minutes machine time for its construction.

(4) Straightforward.

The hand calculations for $p = 5$ were verified and a new counter-example found for $p = 7$. It is hoped to run $p = 11$.

Acknowledgments. I would like to thank Dr. Neubüser for valuable suggestions concerning the subgroup lattice programs and Professor Wall who provided the initial motivation for the development of the programs associated with Hughes' conjecture.

REFERENCES

1. J. Neubüser : Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten Dualmaschine. Num. Math. 2 (1960), 280-292.
2. P. Hall: Classification of prime power groups. J. reine angew. Math. 182 (1940), 130-141.
3. M. Hall and J. Senior: The *Groups* of *Order* 2” (n ≤ 6) (Macmillan, New York, 1964).
4. M. Hall: The Theory *of Groups* (Macmillan, New York, 1959).
5. M. Hall: A basis for free Lie rings and higher commutators in free groups. *Proc. Amer. Math. Soc.* 1 (1950), 575-581.

The computation of irreducible representations of finite groups of order 2^n, $n \leqslant 6$[†]

P. G. RUUD and R. KEOWN

1. Introduction. Most textbooks and monographs on group representation theory include the statement that the construction of the irreducible representations of a particular group or family of groups is an art rather than a science. This paper is a contribution to the art in the case of 2-groups of order 2^n, n $\leqslant$ 6. The construction is based on the definitions of these groups given in the monumental work of Hall and Senior [5]. The authors and their colleagues have computed a representative element from each one of the classes of equivalent irreducible representations in the case of each class of isomorphic 2-groups of order 2" ($n < 6$) and of numerous groups of order 64. An omission in the original program, whose correction is now believed understood, prevented the successful calculation of all of the representations of the groups of order 64.

This collection of 2-groups contains many abelian and metacyclic groups for which a general theory of their representations exists. However, there are many 2-groups in the collection of Hall and Senior for which such a theory is not currently available. This paper is a description of a method of computation rather than a theory of the representations of 2-groups. The calculation does not employ trial-and-error or iteration procedures.

A ***monomial representation*** of a finite group G is a matrix representation $\boldsymbol{T}$ of G such that each matrix $\boldsymbol{T(g)}$, g $\in$ G, contains exactly one non-zero entry in each row and column. An ***induced monomial representation*** of G is any induced representation U^G where U is a one-dimensional representation of some subgroup. It is known, see Curtis and Reiner ([3], pages 314 and 356), that every irreducible K-representation of a finite nilpotent group G is an induced monomial representation. Every finite 2-group is known to be nilpotent. The defining relations of Hall and Senior provide an ascending normal series of the form

$$\{1\} \subset H_1 \subset \ldots \subset H_r = G, \tag{1.1}$$

[†] This work was a collaboration between the authors and R. F. Hansen, E. R. McCarthy and D. L. Stambaugh.

in which each subgroup H_i is a subgroup of index two in H_{i+1}, $1 \leq i \leq r-1$, where G is a 2-group of order 2'. Our irreduci'ole representations are monomial representations constructed by induction on the normal series (1.1). Originally the authors believed that each self-conjugate representation of an H_i in this series would generate the two associated representations of H_{i+1} under multiplication by the appropriate scalar matrix. This idea proved false. Presently, it is conjectured (not proved) that a minor modification of the method and program will avoid this error.

The second section of the paper discusses the manner of obtaining the Cayley table of a 2-group from the defining relations of Hall and Senior. The third section explains the inductive construction of the irreducible representations from the Cayley table. The fourth section describes the programs used in the calculation. Until the early part of 1967, the present authors were unaware of the very significant work on representation theory in progress abroad, see Brott [2], Gerhards and Lindenberg [4], Lindenberg [8], and Neubiiser [10]. Excellent sources of information on the theorems quoted in this paper are the monographs of Boerner [l], Curtis and Reiner [3], and Lomont [7].

2. Development of the Cayley tables of 2-groups. The method of calculation of the irreducible representations of 2-groups described in this paper depends upon the availability within the computer of the Cayley table of the group under investigation. The work of Hall and Senior describes each group of order 2^n, $1 \leq n \leq 6$, in three ways: "(1) by generators and defining relations; (2) by generating permutations; and (3) by its lattice of normal subgroups, together with the identification of every such group and its factor group". The generation of the Cayley table from the permutation presentation of a group appeared to be the most expedient method, if not the most concise. R. F. Hansen [6] wrote the necessary program and assumed the burdensome task of preparing the necessary input for all 2-groups of order greater than 4 and less than 128. All Cayley tables were computed by this method and checked for accuracy. A very small number of typographical mistakes in the lists of permutation generators was apparently uncovered in the process. D. L. Stambaugh [12] attacked the problem of discovering a satisfactory method of obtaining the Cayley tables directly from the generators and the defining relations. An examination of a number of Cayley tables strongly suggests that a presentation of the generators as regular permutations with degrees equal to that of the group can be obtained in a direct manner. In order to describe the method discovered by Stambaugh, it is convenient to briefly discuss the definition of the groups by means of the Hall-Senior defining relations.

Each group G is described by a set B of generators $[b_1, \ldots, b_r]$ *where* the number r is the exponent of 2 in the order 2^r of the group. Every element g of G has a unique ***standard expansion,***

$$g = b_1^{e_1} \ldots b_r^{e_r}, \tag{2.1}$$

in terms of these generators where each e_i, $1 \leqslant i \leqslant r$; is either 0 or 1. The element g with corresponding exponents the set $[e_1, \ldots,$ e,] is numbered

$$e_r 2^{r-1} + \ldots + e_1 + 1. \qquad (2.2)$$

We adopt the notation H_j for the subgroup $(b_1, \ldots, b_j)$ generated by the first j generators. The ascending normal series,

$$\{1\} \subset H_1 \subset \ldots \subset H_r = G, \qquad (2.3)$$

is the basis of the present calculation of the irreducible representations of G. The Hall-Senior defining relations are given in terms of a subset $[a_1, \ldots, a_j]$ of **B**. The squares a_i^2, $1 \leqslant i \leqslant j$, of these are listed either in terms of central elements or ***a's*** with smaller subscripts. The collection of all commutators $[a_i, a,] = a_i^{-1} a_m^{-1} a_i a_m$, $1 \leqslant i < m \leqslant j$, is similarly described. The set $[a_1, \ldots, a_j]$ is a proper subset of $[b_1, \ldots,$ b,] when G is not a stem group. Stem 2-groups are those in which the center Z is contained in the derived group G' of G. Additional information is given for non-stem groups enabling one to extend the information from the set $[a_1, \ldots, a_j]$ to the set $[b_1, \ldots,$ b,]. The computational scheme of Stambaugh is based on a set of defining relations which gives all squares b_i^2, $1 \leqslant i \leqslant$ r, and all commutators $[b_i,$ b,], $1 \leqslant i < m \leqslant r$, in terms of generators with smaller subscripts. Stambaugh writes the commutators in the form

$$b_i b_m = b_m b_i x, \quad 1 \leqslant i < m \leqslant r; \qquad (2.4)$$

where x is obtained at an earlier stage in an inductive computational scheme. We refer to the description of each group in terms of the ***b's*** as the ***Hall-Senior defining relations*** although, strictly speaking, these correspond exactly to those of their monograph only for stem groups.

The set $[y_1, \ldots, y_r]$ of regular permutations corresponding to the set $[b_1, \ldots,$ b,] of generators of the group G has a number of properties conveniently discussed together. Each permutation y_i is associated with three sets, B_i, E_i, and S_i, which are defined as follows: B_i consists of the set $[1, \ldots, 2^{i-1}]$ of the first 2^{i-1} integers; E_i consists of the set $[2^{i-1}+1, \ldots, 2^i]$ of the next 2^{i-1} integers; while S_i, the union of B_i and E_i, consists of the first 2' integers. Each y_i is determined by a permutation p_i defined on the set S_i where it maps B_i in a one-one fashion on E_i and conversely. Consequently, its inverse p_i^{-1} has the same domain, but the opposite effects on B_i and E_i. Each permutation p_i is extended to the set of the first 2 integers by means of a family of permutations $[c_1, \ldots, c_{r-1}]$. The permutation c_i is defined on the set S_{i+1} in the following fashion:

$$\left.\begin{aligned} c_i(k) &= k + 2^i, k \in B_{i+1}, \\ c_i(k) &= k - 2^i, k \in E_{i+1}, \end{aligned}\right. \quad 1 \leqslant i \leqslant r-1. \qquad (2.5)$$

The ith permutation p_i, defined on the set S_i, is extended by successive products and conjugations to obtain

$$\begin{aligned} y_i = {} & p_i[c_ip_ic_i^{-1}]\ [c_{i+1}p_ic_ip_i(c_{i+1}c_i)^{-1}]\times \ldots \\ & X\ \ [c_{r-1}p_ic_{r-2} \ldots c_ip_i(c_{r-1} \ldots c_i)^{-1}]. \end{aligned} \tag{2.6}$$

The permutation p_1 is associated with the sets B_1, E_1, and S_1 corresponding to [1], [2], and [1, 2] respectively; it is defined to be the transposition $\begin{pmatrix} & 2 \\ 2 & 1 \end{pmatrix}$. It is easily checked that p_1 fulfills the above requirements. The permutation y_1 corresponding to b_1 is obtained by means of equation *(2.6)*.

The construction of the remaining p's and y's is carried out by induction. Suppose that the definition of the set $[y_1, \ldots, y_{k-1}]$ of the first k- 1 permutations has been completed. We consider the construction of p_k. We are given the following conditions:

$$\begin{aligned} &(1) && p_k(1) = 2^{k-1}+1, \\ &(2) && y_1p_k = p_ky_1q_1, \\ & && \quad\ldots \\ &(k) && y_{k-1}p_k = p_ky_{k-1}q_{k-1}, \\ &(k+1) && p_kp_k = q_k, \end{aligned} \tag{2.7)}$$

which are required to hold on S_k where the set of permutations $[y_1, \ldots, y_{k-1}, q_1, \ldots, q_k]$ are known.

The preceding $k+$ 1 conditions are written in the form employed in the program of Stambaugh; however, a description of his method appears somewhat clearer if the commutation relations are rewritten in the form

$$p_k = (y_i^{-1}p_iy_i)q_i, \quad 1 \leqslant i \leqslant k-1. \tag{2.8}$$

One begins the construction with the knowledge of $p_k(1)$, always defined by (2.71). At the beginning of the ith stage, employing $(2.7(i+1))$, p_k has been defined on the set B_i of the first 2^{i-1} integers with p_k taking values in E_k. The problem is to extend the domain of definition of p_k to the set E_i of the next 2^{i-1} integers with p_k taking values in E_k. The right factor q_i of the product $(y_i^{-1}p_ky_i)q_i$ maps the set E_i onto itself in a 1-1 manner. The next right-most factor y_i maps E_i onto B_i where p_k is already defined. The mapping p_k itself maps B_i into the set E_k which is carried into itself by the last mapping y_i^{-1} in the product. It follows that the definition of p_k has now been extended to the set B_{i+1}. After condition $(2.7k)$ is employed, p_k is defined on B_k with p_k taking values in E_k. This implies that p_k^{-1} is defined on E_k and takes its values in B_k. The $(k+1)$th relation of (2.7) can be rewritten in the form

$$p_k = q_kp_k^{-1}, \tag{2.9}$$

where the permutation on the right is well-defined on the set E_k and assumes values in B_k. This completes the definition of p_k on the set S_k. The definition of y_k follows from equation (2.6). This method of construction is effective for all groups of order 32 and for those groups of order 64 for which it has been employed.

A modification of the method is under consideration in which the back solutions of (2.7) are used to extend the permutations rather than (2.6). These equations can be rewritten in the form

$$\begin{array}{rrcl} (1) & p_k(1) & = & 2^{k-1}+1, \\ (2) & p_1 p_k & = & p_k r_1, \\ & & . \; . \; . & \\ (k) & p_{k-1} p_k & = & p_k r_{k-1}, \\ (k+1) & p_k & = & r_k p_k^{-1}, \end{array} \tag{2.10}$$

denoting p_i and its extensions by the same symbol, where the set $[p_1, \ldots, p_{k-1}, r_1, \ldots, r_{k-1}]$ of permutations is known on the set S_{k-1} before the kth stage of construction. One finds from (2.10) permutations representing the $2^{k-1}-1$ elements of G following b_k in the Cayley table. These appear in the form

$$\begin{array}{rl} (1) & p_1 p_k = p_k r_1, \\ (2) & p_2 p_k = p_k r_2, \\ & . \; . \; . \\ (12 \ldots (k-1)) & p_1 p_2 \ldots p_k = p_k r_1 r_2 \ldots r_{k-1}. \end{array} \tag{2.11}$$

Assume, as an induction hypothesis, that all of the known permutations agree on S_{k-1} with the presentations of their corresponding elements in the left regular presentation of G. The values of the left members of (2.11) are known for the left regular presentation on the number 1, which implies that p_k, the permutation representing b_k in the left regular presentation, is known on the set S_{k-1}. Using equation (2.9), one determines the values of the left regular presentation of b_k on the remainder of the set S_k of the first 2^k integers. Solving for the 2^{k-1} permutations preceding p_k in the form

$$p_1 \ldots p_j = p_k r_1 \ldots r_j p_k^{-1} \tag{2.12}$$

permits their evaluation on the set E_k and, consequently, on the set S_k. The determination of the left regular presentations of the $2^{k-1}-1$ elements following b_k on the set S_k can then be completed. This finishes the kth stage of the construction. Since the induction hypothesis is surely fulfilled for $k=1$, it follows that this method determines the left regular presentation of the group G. It appears that this method will generate the Cayley table in substantially less time than the first. It has not yet been programmed.

3. The calculation of the irreducible representations of 2-groups. This section discusses a systematic method of calculation of the irreducible representations of 2-groups. Some basic definitions and results are given to make the material more intelligible to the non-specialist.

Let t be an r-dimensional matrix representation of the subgroup H of index $\boldsymbol{k}$ in the finite group G. Denote by $[g_1H, \ldots, g_kH]$ the collection of all distinct left cosets of $\boldsymbol{H}$ in G. The function $\boldsymbol{T}$ which makes correspond to each x of G the block matrix

$$T(x) = \left\| \begin{matrix} t'(g_1^{-1}xg_1) & \ldots & t'(g_1^{-1}xg_k) \\ & \ldots & \\ t'(g_k^{-1}xg_1) & \ldots & t'(g_k^{-1}xg_k) \end{matrix} \right\|, \qquad (3.1)$$

where each $t'(g_i^{-1}xg_j)$ is an $r \boldsymbol{X} r$ matrix, $1 \leqslant i, j \leqslant \boldsymbol{k},$

with

$$t'(g_i^{-1}xg_j) = 0, \qquad g_i^{-1}xg_j \notin H,$$

and

$$t'(g_i^{-1}xg_j) = t(g_i^{-1}xg_j), \; g_i^{-1}xg_j \in H,$$

is an ***(rk* X** rk)-dimensional representation of G which is said to be ***induced*** by the representation t of $\boldsymbol{H}$. Only under special circumstances is $\boldsymbol{T}$ an irreducible representation of G even though $\boldsymbol{t}$ is an irreducible representation of $\boldsymbol{H}$. Given a representation $\boldsymbol{T}$ of G, there exists a representation $\boldsymbol{t}$ of $\boldsymbol{H}$ whose values are given by

$$t(h) = T(h), \quad h \in H. \qquad (3.2)$$

The representation $\boldsymbol{t}$ is said to be ***subduced*** by the representation $\boldsymbol{T}$. As in the case of induced representations, the subduced representation t of $\boldsymbol{H}$ need not be irreducible even though the subducing representation $\boldsymbol{T}$ of G is.

The following remarks are valid in the case where $\boldsymbol{H}$ is a normal subgroup of G, but not always in the general case. Let t be a representation of ***Hand*** g any element of G. The mapping t_g defined by

$$t_g(h) = t(g^{-1}hg), \qquad h \in H, \qquad (3.3)$$

is a representation of $\boldsymbol{H}$ which is said to be a ***conjugate*** of $\boldsymbol{t}$. The representation t_g is said to be obtained through ***conjugation*** of t by g. The representation t may or may not be equivalent to its conjugate t_g. The set $\boldsymbol{K}$ of all g such that t_g is equivalent to t is a group called the ***little group*** of $\boldsymbol{t}$. A representation t which is equivalent to each of its conjugates is said to be ***self-conjugate.***

Let t be a representation of $\boldsymbol{H}$ subduced by the irreducible representation $\boldsymbol{T}$ of G. The representation t is the direct sum

$$t = n_1t_1 \dot{+} \ldots \dot{+} n_kt_k \qquad (3.4)$$

of irreducible representations of ***H.*** The set $[t_{i_1}, \ldots, t_{i_j}]$ of irreducible representations which appear with non-zero coefficients in (3.4) is called the ***orbit*** of ***T.*** The number of elements in an orbit is called its ***order.*** According to a result of Clifford, the elements of an orbit are mutually conjugate and every conjugate appears. Furthermore, each conjugate occurs the same number of times in equation (3.4) which can be written

$$t = n(t_{i_1} \dotplus \ldots \dotplus t_{i_j}). \tag{3.5}$$

The number ***n*** is referred to as the ***multiplicity*** of the orbit. It is known that every irreducible representation t of ***H*** belongs to the orbit of at least one irreducible representation ***T*** of G.

Two irreducible representations T and T' of G are said to be ***associates*** if their orbits have an irreducible representation t of ***H*** in common, which implies that their orbits coincide. An irreducible representation ***T*** of G is said to be ***self-associate*** if its orbit is disjoint from that of every other non-equivalent irreducible representation of G. When ***His*** a subgroup of index two in G, the orbit of an irreducible representation ***T*** of G is either a single, self-conjugate irreducible representation t or a pair, t and ***t',*** of mutually conjugate irreducible representations of ***H.*** In either case, the multiplicity of the orbit is always one. In the second case, the representation ***R*** of G induced by t is an irreducible representation of G equivalent to ***T.*** In the first, the representation ***R*** induced by t is equivalent to the direct sum, $T+$ ***T',*** where T' is the only other associate of ***T.***

These results suggest that the irreducible representations of 2-groups can be computed by induction if a convenient algorithm can be developed for reducing the induced representations arising from self-conjugate representations of a subgroup of index two. The remainder of this section is devoted to the development of such an algorithm and the description of a practical scheme of induction. We begin with an observation concerning the one-dimensional representations of any 2-group given by the Hall-Senior defining relations.

THEOREM. ***Let*** $[b_1, \ldots,$ ***b,] be the Hall-Senior generators of a 2-group G of order*** 2^n, $1 \leqslant n \leqslant 6$. ***Let C be the set*** $[c_1, \ldots, c_d]$ ***of those generators, defined inductively, which either appear as a commutator in the defining relations or as one factor of a commutator given by the defining relations in which the other factors are already in C. Each set K of complex numbers*** $[k_1, \ldots, k_n]$ ***which satisfy the defining relations,*** k_i ***having the value*** 1 ***for each element*** c_i ***of C, determines a one-dimensional representation of G which is specified by its values on the generators, namely,***

$$T_K(b_i) = k_i, \quad 1 \leqslant i \leqslant n. \tag{3.6}$$

Each one-dimensional, irreducible representation T of G corresponds to exactly one such K. The derived group G' of G is generated by the elements of the set C. Each maximal subgroup M ***of G is the kernel of a representation***

T_K where each of the elements of K is either 1 or - 1. The Frattini subgroup of G is the intersection of the kernelsof all irreducible representations obtained from such K's.

Proof It is clear that each K, as defined above, defines a one-dimensional representation of G, and that distinct pairs, K and K', define distinct irreducible representations. Conversely, every one-dimensional representation T of G determines a unique K. Thus every one-dimensional representation of a 2-group G can be obtained immediately from its Hall-Senior defining relations. Each K, containing at least one - 1, whose elements are either 1 or - 1, determines an irreducible representation T one-half of whose values are 1 and the other one-half are - 1. The kernel of the corresponding T_K is clearly a maximal subgroup M of G. Conversely, each maximal subgroup A4 generates a one-dimensional representation corresponding to a K of this type. The Frattini subgroup is the common part of these kernels. The subgroup (C) generated by C is contained in the derived group G'. To see that (C)coincides with G', let b_j be any generator coming later in the sequence of generators than the elements of C. We construct a K to show that no element of G having b_j in its standard expansion is an element of G'. Let k_j have the value - 1 and let k_m have the value 1 for m different from j except when b_m^2 equals b_j. In this exceptional case, which can occur for at most one b,, let k_m have the value i. Let T_K be the corresponding one-dimensional representation and note that any element of G whose standard expansion contains b_j does not belong to the kernel of T_K. It follows that the elements of C generate G'.

We turn to the calculation of the higher dimensional irreducible representations of G. Note that a 2-group of order 16 or less cannot have an irreducible representation of dimension greater than two and that a 2-group of order 32 or 64 cannot have an irreducible representation of dimension greater than four. Let the central series of G determined by the Hall-Senior defining relations be given by

$$\{1\} \subset H_1 \subset . . . \subset H_n = G.$$

Recall that $H_r, 1 \leqslant$ r $\leqslant n$, denotes the subgroup (b_1, . . . , b,) determined by the first r generators. The irreducible representations of H_r can be determined by induction from the irreducible representations of H_{r-1} and its subgroups. Some, perhaps all, of the two-dimensional representations of H_r can be calculated immediately by induction from the pairs of conjugate one-dimensional representations of H_{r-1}. However, the two-dimensional self-conjugate representations of H_{r-1}, if any exist, give rise to a more troublesome problem. Each of these, say t,is the orbit of a pair, T and T', of associated two-dimensional irreducible representations of Hr. The representation R induced by $t$is the direct sum of the associated pair, Tand T'. To avoid the reduction problem, we note that each self-conjugate two-dimensional irreducible representation t of H_{r-1} is an induced representation from either member of a pair, s and s', of conjugate representations of some normal subgroup Kof H_{r-1}. The subgroup Kcan be readily identified from the representation t since it consists of those elements of H_{r-1} which are mapped into diagonal matrices by t. Furthermore, the pair, s and s', of conjugate representations of Kcan be read off from the entries of these diagonal matrices. Observe that each of the associated representations, T and T', of H_r subduce the representation t on H_{r-1} and, consequently, give rise to the same matrices for K as t. Moreover, either of T and T', say T, must be an induced monomial representation obtained by induction from a one-dimensional representation of some normal subgroup H, containing K, of index two in H_r. The set of normal subgroups, containing K, of index two in H_r can be determined immediately from the one-dimensional representations of H_r. Each of these is of the form $(K,$ g) for an easily determined element g of H_r. Such a subgroup $(K,$ g) is a suitable H for our purposes only if the irreducible representations of ***Kis*** carried into itself under conjugation by g, a property easily checked from the data available.

When a suitable H has been determined, one computes the pair, q and r, of associated one-dimensional representations of H, each of which subduces the representations on K. The representation q of Hinduces one of the pair, T and T', of associated representations of H_r each of which has $[t]$ for its orbit. The representation r induces the other. This completes the construction of the irreducible, two-dimensional representations of H_r. When the order of H_r exceeds 16, there may exist four-dimensional irreducible representations of H,. These arise from conjugate pairs of two-dimensional or from self-conjugate four-dimensional irreducible representations of H_{r-1}. The construction of the self-associated four-dimensional representations of H_r from the conjugate pairs of two-dimensional representations of H_{r-1} is straightforward. The construction of the associated four-dimensional representations, T and T', of H_r from a self-conjugate four-dimensional irreducible representation t of H_{r-1} is very much as before. Select the subgroup K of index four in H_{r-1} whose elements correspond to diagonal matrices under the representation t. A set $[s_1, s_2, s_3, s_4]$ of four mutually conjugate representations of K can be determined from the diagonal matrices which are images of K under the representation t. The subgroups of index four of H_r which contain K are of the form $(K,$ g) and can be determined from the available data. Such a subgroup H of H_r is suitable for our purposes only if the representation s_1 of K is carried into itself by conjugation under g. This being the case, s_1 is a self-conjugate representation of Kconsidered as a subgroup of index two in H. Consequently, s_1 induces a pair, q and r, of associated one-dimensional representations of H. The representation q of H induces one of the associates with orbit t and the representation r induces the other.

This concludes the outline of the method of calculation. The next section is concerned with the programs for the calculation.

4. Current computer programs. During the study and analysis of finite groups at Texas A &M University, several computer programs have been written. These programs are all written in FORTRAN IV language and are operational on the IBM 7094 digital computer. The following paragraphs are devoted to a discussion of the capabilities of available programs the extent to which each has been used and the relative merits or demerits of each.

(1) A program has been written to test whether a Cayley table presentation is in fact a group by appealing to the group axioms. This program is completely general and the size of the group that can be tested is limited only by the machine storage capacity. The highest order group tested on this program to date is a group of order 64. Should the set being tested fail to satisfy the requirements of a group, the program indicates which axioms were violated and which elements of the set failed to comply.

(2) Given the Cayley table of a finite group, a program was written to determine how many conjugacy classes the group has and to provide a listing of the elements in each class.

(3) A program was written to determine the order of each element of the group.

(4) A program was written which first determines all subgroups of a given group when provided with the Cayley table of the group in question. This is accomplished by using the test program to verify which combinations of elements are in fact groups. It then determines which subgroups are normal. Finally, using the normal subgroups, the corresponding factor groups are computed. The total output from this program for a given group includes all proper subgroups, indicates which subgroups are normal and gives the Cayley table of the corresponding factor group.

This program has been run for groups only as high as order 16. It is not efficient in the sense of computer time for groups of higher order.

(5) As noted in § 2, a program was written to construct the corresponding group Cayley table from the generating permutations for the group. This program has been used to construct the Cayley tables of all groups of order 2^n, $n \leqslant 6$, using the permutations provided in the work of Hall and Senior [5].

(6) The procedure discussed in § 2 for computing Cayley tables of 2-groups from the generators and commutator relations was programmed. This program has been used to generate the Cayley tables for all groups of order 2^n, $n \leqslant 5$, and some of the groups of order 2^6.

(7) In the analysis of a particular group, it is beneficial if the student can examine different Cayley table presentations of the same group. Some of the variations studied were rearrangements of the table according to element order, conjugacy classes or by positioning a particular normal subgroup of index four or less in the first part of the table. A program was written to produce the transformed Cayley table from the original by providing the computer with the desired isomorphism and the original Cayley table.

(8) An algorithm similar to the one discussed in § 3 for computing irreducible representations was programmed. This algorithm differed only in that the programmed version did not permit the calculation of two or four-dimensional representations which arose from self-conjugate two-dimensional representations of the subgroup of index two. Consequently, this program cannot be used for those groups of order sixty-four where the above situation arises. The program does calculate one element from each class of equivalent irreducible representations for groups of order 2^n, $n \leqslant 5$. The program is contingent only upon having a suitable Cayley table presentation of the group available. This poses no restriction in 2^n since any group may be appropriately transformed using the program in paragraph (7) above. The logic of the procedure is to use the known irreducible representations of the group of order 2^1 to obtain those of the group of order 2^2, then use these representations of 2^2 just determined to obtain those of the next subgroup and so on to the group of order 2". The output from the program consists of the matrix representations evaluated at each element of the group. All groups of order 2^n, $n \leqslant 5$, have been subjected to this program with appropriate results obtained. Approximately $3\frac{1}{2}$ minutes of computer time were used. The same program has been used to calculate the irreducible representations of some of the groups of order 64.

In actual practice, many of these programs are used simultaneously with results from one conveyed to others as necessary. For example, the $3\frac{1}{2}$ minutes of computer time above included generating the Cayley tables from the generating permutations, verifying that the result was in fact a group satisfying the generating relations, and determining the conjugacy class structure and the irreducible representations.

As this study of finite groups, and in particular 2-groups, continues, several new problems are being contemplated. Clearly a modification of the representation program to carry out the complete algorithm of § 3 is immediate. The method of § 2 for generating Cayley tables looks promising in considering the step towards 2-groups of order 128. Now that irreducible representations are available for other 2-groups, a study of their subgroup structure and other properties is simplified. The question of whether the representation algorithm would apply with reasonable modification to groups of order p^n, p a prime, also merits consideration.

Readers who might be interested in programs or results of the foregoing are invited to contact the authors at Texas A&M University, College Station, Texas, or at the University of Arkansas, Fayetteville, Arkansas.

REFERENCES

1. H. BOERNER: ***Representations of Groups*** (John Wiley & Sons, New York, 1963).
2. C. BROTT: Diplomarbeit, Kiel, 1966, unpublished.
3. C. W. CURTIS and I. REINER: ***Representation Theory of Finite Groups and Associative Algebras*** (John Wiley & Sons, New York, 1963).

4. L. GERHARDS and W. LINDENBERG: Em Verfahren zur Berechnung des vollständiger Untergruppenverbandes endlicher Gruppen auf Dualmaschinen. ***Numer. Math.* 7** (1965), 1-10.
5. MARSHALL HALL JR. and JAMES K. SENIOR: ***The Groups of Order*** 2^n ***(n*** $\leqslant$ ***6)*** (The Macmillan Co., New York; Collier-Macmillan, Ltd., London, 1964).
6. R. F. HANSEN: M.A. Thesis, Texas A & M University, 1967, unpublished.
7. J. S. LOMONT: ***Applications ofFinite Groups*** (Academic Press, New York, London, 1959).
8. W. LINDENBERG: Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten. ***Numer. Math.*** 4 (1962), 151-153.
9. E. R. MCCARTHY: M.A. Thesis, Texas A & M University, 1966, unpublished.
10. J. NEUBÜSER: Bestimmung der Untergruppenverbinde endlicher p-Gruppen auf einer programmgesteuerten elektronischen Dualmachine. ***Numer. Math.* 3** (1961), ***271-278.***
11. P. G. RUUD: M.A. Thesis, Texas A & M University, 1967, unpublished.
12. D. L. STAMBAUGH: M.A. Thesis, Texas A & M University, 1967, unpublished.

Some examples of man-machine interaction in the solution of mathematical problems

N. S. MENDELSOHN

Summary. Three illustrative examples are given of how the enormous speed and capacity of computing machines can be used to aid the mathematician in the solution of problems he might not otherwise be willing to undertake. The ways in which man and machine can interact are many and varied. The examples given indicate three distinct directions in which such interplay can take place.

Example 1. The Sandler group. The collineation group of the free plane generated by four points was studied by R. G. Sandler in [3]. The group has its own intrinsic interest but there were two directions in which it appeared that interesting information might be obtained. Two natural analogies suggested themselves.

In the first case, by analogy with the situation in classical projective planes, there was the possibility that this group, or at least a very large subgroup, might yield a new simple group of very large order, and if this were so one might expect an infinite class of such groups based on the collineation groups of the free planes which are finitely generated.

Secondly, an analogy with group theory is possible. In group theory, every group on k generators is a homomorphic image of the free group with k generators. It might then be possible to show that the collineation group of every projective plane generated by k points is a homomorphic image of the collineation group of the free plane generated by four points.

We show here that the second possibility is closer to the true situation.

Sandler's group has the presentation

$$G= \{A, B, C \quad A^2 = B^4 = C^2 = (AB)^3 = \big((B^2A)^2C\big)^3 = CBAB^2ACB^2 = I\}.$$

It can be shown that the element AC has infinite order. To study this group it is convenient to look at homomorphic images in which AC is of finite order. Accordingly, let G_n be the group obtained from Sandler's group by adjoining the relation $(AC)" = I$. It is not hard to see that A and B generate the symmetric group S_4 on four symbols, and that in any homomorphic image of G the image of the subgroup generated by A and B must be the full group S_4 or the identity. Coset enumeration is used for the first few values of n. Here are *some* of the results.

$$G_1 = I;\ G_2 = I;$$

$G_3 = LF(2, 7)$, with a faithful representation

$$A \rightarrow (26)\ (34),$$
$$B \rightarrow (23)\ (4567),$$
$$c \rightarrow (12)\ (45).$$

It is to be noted that G_3 is the collineation group of the Fano projective plane which contains seven points.

$G_4 = LF(2, 7)$ with a faithful representation (using subscripted letters)

$$A_1 \rightarrow (26)\ (34),$$
$$B_1 \rightarrow (23)\ (4567),$$
$$C_1 \rightarrow (12)\ (67).$$

An isomorphism between G_4 and G_3 is given by the mapping $A_1 \leftrightarrow A$, $B_1 \leftrightarrow B$, $C_1 \leftrightarrow B^{-2}CB^2$.

G_5 is a group of order 1080. A faithful representation of degree 45 which is equivalent to the representation given by the permutation of the subsets of the subgroup generated by A and B under right multiplication is given by

$A \rightarrow$ (1) (5) (7) (12) (35) (36) (41) (44) (45) (2, 6) (3, 4) (8, 9) (10, 11)
(13, 14) (15, 24) (16, 23) (17, 18) (19, 34) (20, 21) (22, 25) (26, 30)
(27, 28) (29, 33) (31, 32) (37,43) (38, 39) (40,42),

$B \rightarrow$ (1) (44) (45) (2, 3) (32, 43) (39, 40) (4, 5, 6, 7) (8, 16, 17, 22)
(9, 29, 14, 15) (10, 13, 28, 21) (11, 34, 23, 24) (12, 38,41,42)
(18, 19, 20, 30) (25, 26, 27, 33) (31, 36, 37, 35),

$C \rightarrow$ (3) (9) (13) (16) (19) (24) (25) (32) (40) (1, 2) (4, 10) (5, 17)
(6, 8) (7, 28) (11, 12) (14, 30) (15, 37) (18, 31)(20, 35)(21,22)(23,38)
(26, 41) (27, 34) (29, 36) (33, 42) (39, 45) (43, 44).

Marshall Hall pointed out to the author that this representation is imprimitive with 1,44, 45 a set of imprimitivity. By considering the representation obtained by permuting the sets of imprimitivity one obtains a factor group of G_5 of order 360, and hence G_5 has a normal subgroup of order 3. A faithful representation of this factor group by permutations on 15 symbols is given by

$A \rightarrow$ (1) (5) (7) (2, 6) (3,4) (8, 9) (10, 11) (12, 15) (13, 14),
$B \rightarrow$ (1) (2, 3) (4, 5, 6, 7) (8, 9, 11, 14) (10, 13, 12, 15),
$\mathbf{C} \rightarrow$ (3) (9) (13) (1, 2) (4, 10) (5, 11) (6, 8) (7, 12) (14, 15).

This factor group is not A_5 since it has S_4 as a subgroup while A_5 contains no elements of order 4.

G,. The group G_6 is of infinite order. In this case we find a homomorphism of G_6 onto $SL(3, Z)$, where the latter is understood to be the set of all non-singular matrices of order 3 and determinant 1 and whose entries are integers.

The following mapping exhibits the homomorphism explicitly :

$$A \to \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

$$B \to \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

$$C \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}.$$

A direct verification shows that the defining relations are satisfied by these matrices. On the other hand the three matrices generate $SL(3, Z)$ as is seen by the mappings

$$X = C(AC)^3B^2AB^2C \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$AXA \to \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$B^2AB^2AXB^2AB^2A \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$B^2AB^2XAB^2AB^2A \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$AB^2AB^2AXB^2AB^2 \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$AB^2AB^2XAB^2AB^2 \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

where it is known that the six matrices appearing on the right generate $SL(3, Z)$.

The following geometrical corollary then follows. The group generated by all relations of a finite Desarguesian plane which is generated by four points is a homomorphic image of the collineation group of the free plane generated by four points.

Example 2. Complete latin squares. A complete latin square of order n is an array in which every row and every column is a permutation of n symbols and such that every ordered pair of symbols appears as a consecutive pair exactly once in the rows and once in the columns. For example

$$\begin{array}{cccc} A & B & C & D \\ C & A & D & B \\ B & D & A & C \\ D & C & B & A \end{array}$$

is a complete latin square of order 4.

In [2] B. Gordon has shown that complete latin squares exist for every even order and in [1] E. N. Gilbert has given a number of special constructions all for even order. It is known that for $n = 3, 5, 7, 9$ no complete latin square exists and it had been conjectured that none exists for any odd order. An exhaustive search by machine is quite impractical for $n \geqslant 11$ so that a specialized search based on an incomplete mathematical theory may be of use.

Following Gordon we look for a solution in which the square is the multiplication table for a group. The problem is then reduced to the following. Let $g_1, g_2, \ldots, g_n$ be the distinct elements of a group. Is it possible to arrange them so that the elements $g_1, g_1^{-1}g_2, g_2^{-1}g_3, \ldots, g_{n-1}^{-1}g_n$ are all distinct?

If the group is of odd order and Abelian it is known to be impossible for such an arrangement to exist. Hence we look to groups which are non-abelian. The **smallest** order of a non-abelian group of odd order is 21. However, a search through the 21! permutations of the elements of the group is still impractical. The compromise used was to start the arrangement of the elements of the group by hand until one gets stuck (usually after 16 to 18 elements). When this is finished the arrangement was put into the machine with a back-tracking program to try to alter and complete the arrangement. This proved eminently successful. On p. 221 is an example of one of the latin squares of order 21.

Example 3. Commutators. There are a number of combinatorial problems in which it is important to know whether or not an element of a commutator subgroup is a commutator. More generally the following question is of interest. Given an element A of the commutator subgroup, *An example of a latin square of order* 21 *without repeated digraphs (both rows and columns)*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*
K	*A*	*P*	*I*	*S*	*M*	*T*	*R*	*Q*	*F*	*B*	*E*	*J*	*H*	*C*	*O*	*D*	*N*	*L*	*U*	*G*
O	*M*	*L*	*K*	*B*	*R*	*F*	*D*	*S*	*Q*	*H*	*N*	*E*	*C*	*T*	*J*	*P*	*G*	*U*	*A*	*I*
P	*F*	*S*	*A*	*K*	*H*	*J*	*Q*	*E*	*I*	*N*	*R*	*L*	*O*	*G*	*M*	*C*	*U*	*T*	*B*	*D*
E	*D*	*A*	*J*	*C*	*P*	*S*	*L*	*H*	*B*	*T*	*I*	*G*	*F*	*Q*	*N*	*U*	*K*	*M*	*R*	*O*
R	*C*	*F*	*L*	*G*	*S*	*K*	*T*	*O*	*N*	*J*	*A*	*D*	*I*	*E*	*U*	*B*	*P*	*H*	*Q*	*M*
C	*J*	*E*	*B*	*A*	*N*	*M*	*I*	*L*	*D*	*R*	*H*	*S*	*P*	*U*	*F*	*O*	*T*	*G*	*K*	*Q*
F	*N*	*G*	*C*	*R*	*I*	*D*	*O*	*A*	*L*	*P*	*T*	*H*	*U*	*M*	*S*	*E*	*Q*	*K*	*J*	*B*
L	*Q*	*B*	*M*	*O*	*C*	*E*	*S*	*N*	*K*	*G*	*D*	*U*	*J*	*I*	*R*	*T*	*A*	*F*	*H*	*P*
M	*H*	*T*	*P*	*N*	*Q*	*I*	*C*	*K*	*E*	*O*	*U*	*R*	*G*	*J*	*L*	*S*	*D*	*B*	*F*	*A*
S	*I*	*K*	*F*	*P*	*O*	*L*	*E*	*R*	*A*	*U*	*Q*	*T*	*M*	*D*	*H*	*G*	*B*	*J*	*N*	*C*
Q	*G*	*I*	*T*	*D*	*K*	*P*	*J*	*M*	*U*	*L*	*F*	*C*	*A*	*R*	*B*	*N*	*S*	*O*	*E*	*H*
T	*E*	*N*	*H*	*M*	*G*	*R*	*K*	*U*	*P*	*D*	*C*	*B*	*L*	*A*	*Q*	*J*	*F*	*I*	*O*	*S*
N	*P*	*M*	*E*	*T*	*L*	*B*	*U*	*C*	*H*	*F*	*K*	*I*	*Q*	*S*	*G*	*A*	*O*	*R*	*D*	*J*
B	*K*	*O*	*Q*	*L*	*J*	*U*	*N*	*D*	*M*	*A*	*S*	*F*	*R*	*P*	*C*	*I*	*H*	*E*	*G*	*T*
G	*L*	*R*	*N*	*F*	*U*	*H*	*A*	*T*	*C*	*Q*	*O*	*K*	*S*	*B*	*I*	*M*	*J*	*D*	*P*	*E*
H	*O*	*J*	*S*	*U*	*E*	*A*	*G*	*P*	*R*	*M*	*B*	*Q*	*D*	*L*	*T*	*K*	*C*	*N*	*I*	*F*
D	*T*	*Q*	*U*	*I*	*B*	*O*	*F*	*J*	*G*	*E*	*M*	*P*	*K*	*N*	*A*	*H*	*L*	*C*	*S*	*R*
J	*R*	*U*	*O*	*H*	*D*	*Q*	*P*	*B*	*S*	*C*	*G*	*N*	*T*	*F*	*E*	*L*	*I*	*A*	*M*	*K*
I	*U*	*D*	*G*	*Q*	*A*	*C*	*M*	*F*	*T*	*S*	*J*	*O*	*B*	*H*	*K*	*R*	*E*	*P*	*L*	*N*
U	*S*	*H*	*R*	*J*	*T*	*N*	*B*	*G*	*O*	*I*	*P*	*A*	*E*	*K*	*D*	*F*	*M*	*Q*	*C*	*L*

find the minimum value k such that A is expressible as a product of k commutators.

This problem, in general, is known to be unsolvable. However, for free groups it is solvable but the solution is by no means trivial. The author has studied the problem of a machine program for making the computations. To test the possible efficiency of the program the author carried out hand calculations which would imitate the machine's behaviour. Naturally, relations were generated in a random order, but a number of them proved to be very interesting and one of these led to an interesting theorem. Here are some of the results turned out at random, all referring to free groups.

(a) In a free group a word of length six or less which lies in the commutator subgroup is a commutator, e.g.

$$a^{-1}b^{-1}c^{-1}abc = (ba,\ bc).$$

(b) The cube of a commutator can be expressed as a product of two commutators, e.g.

$$(a, b)^3 = (\text{a-1b-1a-1ba}, a^{-1}b^{-2}a)(aba^{-1}b^{-1}a, b).$$

(c) Each of the products (a, b) (c, a) and (a, b) (b, c) can be expressed as a single commutator.

(d) $c^{-3}(cx)^3x^{-3} = (xc^2, c^{-1}x^{-2})$.

This last relation leads to a very interesting theorem of group theory.

THEOREM. ***Let G be a group for which every commutator has order* 1 *or 3. Then G' is periodic.***

Remark. This theorem was proved by a colleague of mine, N. D. Gupta. He used a more complicated lemma than that used in the proof below.

Proof. From the identity $c^{-3}(cx)^3x^{-3} = (xc^2, c^{-1}x^{-2})$ it follows that $(cx)^3 = c^*x^3$ where c and c^* are commutators. Hence if $c_1, c_2, c_3, \ldots, c_m$ are commutators $(c_1c_2 \ldots c_m)^3 = c_1{}^*c_2{}^* \ldots c^*_{m-1}$. By iteration $(c_1c_2 \ldots c_m)^{3^m} = 1$.

Concluding remarks. The above examples indicate that there can be a fruitful symbiosis between machine and mathematician. The author would also point out that it is well worth while for him to scan the output of a computer even though it may appear random and disconnected. There is the possibility of real discovery.

REFERENCES

1. E. N. Gilbert: Latin squares which contain no repeated digrams. SIAM Rev. 7 (1965), 189-198.
2. B. Gordon: Sequences in groups with distinct partial products. *Pacific J. Math. 2* (1961), 1309-1313.
3. R. G. Sandler: The collineation groups of free planes II: A presentation for the group *G,. Proc. Amer. Math. Soc. 16 (1965),* 181-186.

Construction and analysis of non-equivalent finite semigroups

ROBERT J. PLEMMONS

1. Introduction. In searching for examples of finite algebraic systems that satisfy certain identities or have specific properties, it is often convenient to have available a listing of all non-equivalent (i.e., non-isomorphic or anti-isomorphic) systems of given types and orders, together with information concerning their properties. This paper is concerned with the development of algorithms used to design computer programs for the purpose of constructing and analyzing certain systems such as groupoids and semigroups, having small orders. Of course, the basic problem in such projects is to develop an efficient algorithm to construct one representative system from each class of those that are either isomorphic or anti-isomorphic.

Digital computers were first applied to the construction of non-equivalent finite semigroups by G. E. Forsythe in 1954 [3], when he constructed all semigroups of order 4 by use of the computer SWAC, at Los Angeles. Hand computations [10] had previously yielded those of order $N \leq 3$. In 1955, T. S. Motzkin and J. L. Selfridge obtained all semigroups of order 5, also by using SWAC, and about the same time similar results were obtained in Japan by hand computations [11]. It was not until 1966 that the results for $N = 6$ were obtained at Auburn University [8].

In § 2 we develop an algorithm to construct all non-equivalent semigroups of order $N \leq 6$, the results for $N = 6$ being new. The analysis of these semigroups is discussed in § 3. In addition, some applications to the development of certain theorems about finite semigroups are mentioned, along with the formulation of an associated conjecture. All notation and definitions follow [1] and [2].

2. The construction algorithm. As we have mentioned, the problem of constructing all non-equivalent finite algebraic systems of given type and order is essentially the problem of efficiently choosing a representative system from each class of those that are either isomorphic or anti-isomorphic. It is trivial to construct an algorithm to do this. One needs only to compute all possible systems of that type, to determine which are isomorphic or anti-isomorphic and then to choose one system from each such class [3]. However, the computation time is then proportional to the total number of such systems. The algorithm presented in this paper constructs only those groupoids that are neither isomorphic nor anti-isomorphic; and, after adding a routine to ensure associativity, it makes feasible the construction of all semigroups of order N $\leqslant$ 6, on most modern digital computers.

The algorithm will be given for the most general binary system, the groupoid, since routines to restrict the binary operations can readily be added. Let N be a positive integer and let S be the set of all positive integers less than or equal to N. We choose this as the set of elements for our groupoids of order N, since they are readily used as subscripts in FORTRAN. Let R_N denote the set of all **NXN** matrix arrays

$$\mathrm{A} = (a_{ij})$$

where each $a_{ij} \in$ S. Then each array (a_{ij}) represents a groupoid of order N with binary operation o defined by

$$i o j = a_{ij}.$$

Conversely, each groupoid of order N has such a representation.

Let P_N denote the permutation group on S and let A^T denote the transpose of $A \in R_N$. For each $\alpha \in P_N$ and each $A = (a_{ij}) \in R_N$ *we* define

$$A\alpha = B = (b_{ij})$$

where

$$b_{ij} = \alpha[a_{\alpha^{-1}(i)\alpha^{-1}(j)}], \quad i, j \in S.$$

Then two groupoids of order N, represented by A and B in R_N, are isomorphic if and only if

$$A\alpha = B$$

for some a $\in P_N$, and are anti-isomorphic if and only if

$$A^T\beta = B$$

for some $\beta \in P_N$.

Now the set R_N is ordered by the relation $\leqslant$, defined by the rule that if $A, B \in R_N$ then

$$A \leqslant B$$

if and only if $a_{ij} = b_{ij}$ for each $i, j \in S$, or else there is a pair $m, k \in S$ such that

$$a_{mk} < b_{mk}$$

and $a_{ij} = b_{ij}$ for all i, j $\in$ S where

$$\mathrm{j+(i\text{-}1)N} < k+(m\text{-}l)N.$$

In other words the ordering is row-wise.

Now for each $A \in R_N$ we let I_A denote the set of all $A\alpha$, as a ranges over P_N. Then either $I_A = I_{A^T}$ or else $I_A \cap I_{A^T} = \emptyset$, and moreover $I, = I_{A^T}$ if and only if $A\alpha = A^T$ for some $a \in P_N$.

In order to construct only those groupoids that are non-equivalent, we construct only the minimal matrix (with respect to the ordering) in the set $I_A \cup I_{A^T}$. This can be accomplished in the following way, using the familiar backtrack method of exhaustive search. Starting with all ones (the null groupoid), we initiate a process of backing up and going forward, row-wise, in defining terms in the table, beginning with the last position, Now whenever the process backs up in the table, the previous position is zeroed and we consider the product there as undefined. In general, suppose the process is at position (i, j). The term a_{ij} is replaced by $a_{ij}+ 1$. Then:

1. If $a_{ij} > N$, we set $a_{ij} = 0$ and back up in the table. If $i = j = 1$, the process is complete and we have all the desired systems; if not, the process goes to position $(i, j- 1)$ if $j \neq 1$ or $(i- 1, N)$ if $j = 1$.

2. If $a_{ij} \leq N$, we first check to see if the binary operation defined by the partial table constructed thus far satisfies the necessary restrictions. If it does not, we once again increment a_{ij} by one. If it does, we next check to see if the partial table would come first in the ordered set $I_A \cup I_{A^T}$. To do this we consider permutations a $\in P_N$ and check to see if

$$a_{ij} \leq \alpha[a_{\alpha^{-1}(i)\alpha^{-1}(j)}]$$

and

$$a_{ij} \leq \alpha[a_{\alpha^{-1}(j)\alpha^{-1}(i)}],$$

whenever $a_{\alpha^{-1}(i)\alpha^{-1}(j)}$ and $a_{\alpha^{-1}(j)\alpha^{-1}(i)}$ are defined. If either of the inequalities does not hold we once again increment a_{ij} by one. Otherwise we go forward in the table. Now if $i = j = N$, we have a desired system. If not we go to position $(i, j+ 1)$ if $j \neq N$or $(i+ 1, 1)$ if $j = N$, and continue.

Using this algorithm, we may construct all the non-equivalent groupoids of order N, each of which is minimal in its class. The method enables us to exclude consideration of many tables at one time. In fact, if we have a failure at position (i, j) and if all possibilities are exhausted below (i, j) in the row ordering, we may exclude from consideration a total of N^k tables where

$$k = N^2 - [j+(i- 1)N].$$

Also, the process can often be augmented by devices to reduce the work factor. For example, we usually need to consider only certain permutations of S in P_N, depending on the type system we are constructing and on the form of the partial table, constructed at that stage in the process. One method for accomplishing this is the following. Let $D = (a_{ii})$ be the diagonal of $A = (a_{ij}) \in R_N$. Consider these diagonals ordered in the usual sense from the (1,l) to the (N, N) positions, and for each diagonal D and each $a \in P_N$ let $D\alpha$ denote the diagonal of $A\alpha$, where D is the diagonal of **A.** Now suppose that

$$\{D_1, \ldots, D_m\}$$

is the set of all distinct diagonals with the property that $D_i \leqslant D_i\alpha$ for each $\alpha \in P_N$. Let

$$L_{D_i}$$

denote the set of all non-equivalent groupoids with diagonal D_i. Then

$$\bigcup_{i=1}^{m} L_{D_i}$$

is the set of all non-equivalent groupoids of order N. Thus to construct these groupoids we need only construct each diagonal D_i, lowest in the ordering, determine the subgroup of P_N leaving D_i fixed, and then construct all non-equivalent groupoids with diagonal D_i by using this subgroup in the equivalence checks. This procedure reduces the work factor considerably. In addition to this, terms can often be defined ahead in the table to ensure that the binary operation in the partial table has the desired properties.

This algorithm has been coded into FORTRAN and the program has been run, in one form or another, on several computers, including those at Auburn University, the University of Tennessee and the National Security Agency. Programs resulting from the algorithm have been applied to the construction of various types of systems, such as groupoids, semigroups and loops; with the construction of the Cayley tables for all semigroups of order $N \leqslant 6$ being one of the more noteworthy results. A monograph listing these tables, along with other information, can be obtained from the Department of Mathematics at Auburn University, Auburn, Alabama [8].

3. Some analysis results. These finite semigroups, constructed by use of the algorithm described in § 2, have been classified according to several properties, such as being regular, inverse or subdirectly irreducible. Such classification is accomplished by adding appropriate subroutines to the construction program. A table giving the number of (regular, inverse) semigroups of order $N \leqslant 6$ is given at the end of the paper (p. 228). Also included is the number of semigroups containing k idempotents for $k = 1, \ldots, N$.

Perhaps the most interesting use of the algorithm has been in the construction of specific finite systems of order N that satisfy certain identities or have certain properties, or else proving that no such systems exist for that order. For example, one such application has solved the problem of finding the smallest order semigroup whose system of identities has no finite basis [5], [6], [7].

THEOREM. ***There is a semigroup of order 5 whose system of identities has no finite basis, and, moreover, the system of identities for each semigroup of order $N < 5$ has a finite basis.***

Other analysis results were obtained by constructing all the congruence relations on each semigroup of order $N \leqslant 5$ and on selected semigroups of order 6. The algorithm to construct these relations first determines the equivalences on the set and then tests for compatibility with the binary operations of the non-equivalent semigroups of that order. The resulting examples are useful in the study of semigroup decompositions and in the study of homomorphisms, since the consideration of homomorphisms can be limited to the consideration of congruences. These computations have suggested the next result.

THEOREM. ***The following four conditions concerning a semigroup S of order $N > 2$ are equivalent.***

(A) ***Each reflexive relation on S is left compatible.***

(B) ***Each equivalence relation on S is a left congruence.***

(C) ***For each x, y and z in S either $xy = xz$ or $xy = y$ and $xz = z$.***

(D) ***$S = A \cup B$, where $A \cap B = \emptyset$ and where, for some idempotent function f from A to A, the binary operation for S is given by***

$$xy = \begin{cases} f(x) & \text{if } x \in A. \\ y & \text{if } x \in B. \end{cases}$$

This theorem, together with its dual, shows that each equivalence relation on a semigroup S is also a congruence relation if and only if S is a [left, right] zero semigroup.

The examination of these examples has also led to the following conjecture :

> If a finite semigroup of order $N > 3$ has exactly one proper congruence relation, then it is a group or a simple group with zero.

In conclusion we mention that the construction of all non-equivalent semigroups of order 7 would be rather difficult, both from the standpoint of running time on any particular computer and from the standpoint of output volume. Although there is no known rule giving the number of non-equivalent finite semigroups as a function of the order, a good estimate for the number of order 7 is around 200,000. However, the construction and analysis of special types for $N \geqslant 7$ is sometimes feasible and could be useful in the formulation and testing of conjectures.

REFERENCES

1. A. H. CLIFFORD and G. P. PRESTON: ***The Algebraic Theory of Semigroups,*** Amer. Math. Soc., Math. Surveys, Vol. I (Providence, 1961).
2. A. H. CLIFFORD and G. P. PRESTON: ***The Algebraic Theory of Semigroups,*** Amer. Math. Soc., Math. Surveys, Vol. II (Providence, 1967).
3. G. E. FORSYTHE: SWAC computes 126 distinct semigroups of order 4. ***Proc. Amer. Math. Soc.* 6** (1955), 443-445.

Totals

Semigroups of order	2	3	4	5	6
Total no. non-equivalent	4	18	126	1160	35,973
No. commutative	3	12	58	325	2143
No. regular	3	9	42	206	1352
No. inverse	2	5	16	52	208
No. with 1 idempotent	2	5	19	132	3107
No. with 2 idempotents	2	7	37	216	1780
No. with 3 idempotents		6	44	351	3093
No. with 4 idempotents			26	326	4157
No. with 5 idempotents				135	2961
No. with 6 idempotents					875

4. M. Hall Jr. and D. E. Knuth: Combinatorial analysis and computers. Amer. *Math. Monthly, 72* (1965), 21-28.
5. R. C. Lyndon: Identities in finite algebras. *Proc. Amer. Math. Soc. 5* (1954) 8-9.
6. V. L. Murskii: The existence in three valued logic. of a closed class with finite'basis not having a finite complete system of identities. Soviet *Math. Dok!. 6* (1965), 1020-1024.
7. P. Perkins: *Bases for Equational Theories of Semigroups,* Ph.D. Dissertation, University of California, Berkeley, 1966.
8. R. J. Plemmons: *Cayley Tablesfor all Semigroups of Order* N $\leqslant$ 6, Monograph, Auburn University, Auburn, Alabama, 1966.
9. B. M. Schein: Homomorphisms and subdirect decompositions of semigroups. *Pacific.J of Math.* 17(1966). 529-547.
10. T. Tamura: Some remarks on semigroups and all types of orders **2,3. *J Gakugei,*** *Takashima University,* 3 (1953), 1-11.
11. K. T. Tetsuya, T. Hashimoto, T. Akazawa, R. Shibota, T. Inui, T. Tamura: All semigroups of order at most *5. J. Gakugei, Tukushima University, 6 (1955),* 19-39.

Some contributions of computation to semigroups and groupoids’

TAKAYUKI TAMURA

REVIEWING the contribution of computers to the theory of semigroups, we note that G. E. Forsythe computed all semigroups of order 4 [2] in 1954, and T. S. Motzkin and J. L. Selfridge obtained all semigroups of order 5 [4] in 1955. For the ten years from 1955 through 1965, nobody treated the computation of all semigroups of order 6. However, R. Plemmons did all semigroups of order 6 by IBM 7040 in 1965 [5]. On the other hand the author and his students obtained the semigroups of order 3 in 1953 [8], of order 4 in 1954 [9] and of order 5 in 1955 [1c0] by hand, independently of those mentioned above. Beside these, certain special types of semigroups and groupoids of order 3, which are distributive to given semigroups of order 3, were computed by hand [12], [13], [14]. In 1965 we obtained the number of non-isomorphic, non-anti-isomorphic groupoids of order $\leqslant 4$ which have a given permutation group as the automorphism group (§§ 1.4, 1.5). Although the result was presented at the meeting of the American Mathematical Society at Reno, 1965, it has not been published. Afterwards R. Plemmons checked the total number by computing machine and wrote to the author that our number was correct; the author wishes to thank Dr. Plemmons. Recently R. Dickinson analyzed the behavior of some operations on the binary relations by machine [17].

In this paper we announce the result concerning the automorphism groups and the total number of groupoids and additionally we introduce the significance of a new concept "general product", which ***uses*** a machine to get a suggestion for an important problem on the extension of semigroups, and further we show the result in a special case which easily computed without using a machine. The detailed proof of some theorems will be omitted because of pressure on space in these Proceedings, and the complete proof will be published elsewhere.

[†] This research was supported by NSF GP-5988 and GP-7608.

PART I. GROUPOIDS AND THEIR AUTOMORPHISM GROUPS

1.1. Introduction. A groupoid G is a set S with a binary operation θ in which the product z of x and y of S is denoted by

$$z = xey.$$

G is often denoted by $G = G(S, \theta)$. An automorphism α of G is a permutation of S (i.e. a one-to-one transformation of S onto S) such that

$$(x\theta y)\alpha = (x\alpha)\theta(y\alpha) \text{ for all } x, \ y \in S.$$

The group of all automorphisms of G is called the automorphism group of G and denoted by $\mathfrak{A}(G)$ or $\mathfrak{A}(S, \theta)$. It is a subgroup of the symmetric group $\mathfrak{S}(S)$ over S. The following problem is raised:

Problem. Let S be a fixed set. Under what condition on S |, for every subgroup $\mathfrak{H}$ of $\mathfrak{S}(S)$, does there exist G = G(S, θ) such that $\mathfrak{A}(G) = \mathfrak{H}$? This problem is a step towards the following problem.

Let $\mathfrak{H}$ be a subgroup of $\mathfrak{S}(S)$. Under what condition on $\mathfrak{H}$ does there exist a groupoid G such that $\mathfrak{A}(G) = \mathfrak{H}$?

However, we will consider only the first problem in this paper.

The answer to the problem is:

THEOREM 1.1. ***For every subgroup $\mathfrak{H}$ of $\mathfrak{S}(S)$ there is at least a groupoid G defined on S such that $\mathfrak{A}(G) = \mathfrak{H}$ if and only if $|S| \leqslant 4$.***

In the next section we will sketch the outline of the proof. From now on we shall not distinguish in symbols S from G, that is, G shall denote a set as well as a groupoid defined on it. The groupoids with operations $\theta, \xi, \cdots$ are denoted by $(G, \theta), (G, \xi), \cdots$. The automorphism group $\mathfrak{A}(G, \theta)$ will be denoted by $\mathfrak{A}(G)$ or $\mathfrak{A}(\theta)$ if there is no fear of confusion as far as a set G is fixed. $\mathfrak{S}(G)$ is the symmetric group over a set G.

1.2. Outline of the proof of Theorem 1.1. The following theorem was given in 1963 [**16**].

THEOREM 1.2 ***Every permutation of a set G is an automorphism of a groupoid G if and only if G is either isomorphic or*** *anti-isomorphic*[†] ***onto one of the following***

(1 .1) ***A right zero semigroup: $xy = y$ for all x, y.***

(1.2) ***The idempotent quasigroup of order 3.***

(1.3) ***The groupoid {1, 2) of order 2 such that***

$$x \cdot 1 = 2, \qquad x \cdot 2 = 1 \qquad (x = 1, 2).$$

The following theorem partially contains Theorem 1.2.

THEOREM 1.3. ***Let $|G \geqslant 5$. The following statements are equivalent.***

[†] We will use "dually isomorphic" as synonymous to "anti-isomorphic".

(1.4) ***A groupoid G is isomorphic onto either a right zero semigroup or a left zero semigroup.***

(1.5) $\mathfrak{A}(G) = \mathfrak{S}(G)$.

(1.6) ***Every even permutation of G is contained in*** $\mathfrak{A}(G)$.

(1.7) $\mathfrak{A}(G)$ ***is triply transitive (i.e.*** *3-ply* ***transitive*** (cf. [3])).

(1.8) $\mathfrak{A}(G)$ ***is doubly transitive and there is an element*** $\varphi \in \mathfrak{A}(G)$ ***such that*** $a\varphi = a$, $b\varphi = b$ *for some* a, $b \in G$, $a \neq b$, *but* $x\varphi \neq x$ *for all* $x \neq a$, $x \neq b$.

Proof. The proof will be done in the following direction:

$$\begin{tikzcd}
(1\cdot7) \arrow[r] & (1\cdot4) \arrow[d] & \\
& & (1\cdot8) \arrow[ul] \\
(1\cdot6) \arrow[uu] & (1\cdot5) \arrow[l] \arrow[ur] &
\end{tikzcd}$$

(1.4) → (1.5) is given by Theorem 1.2; (1.5) → (1.6), (1.5) → (1.8) are obvious ; (1.6) → (1.7) is easily proved by the fact that the alternating group is triply transitive if $|G| \geqslant 5$. We need to prove only (1.7) → (1.4) and (1.8) → (1.4). The detailed proof is in [20].

Remark. We do not assume finiteness of G. The definitions of double and triple transitivity and even permutation are still effective.

Let $\mathfrak{H}$ be a proper subgroup of $\mathfrak{S}(G)$, $|(G)| \geqslant 5$. If $\mathfrak{H}$ can be an automorphism group of a groupoid (G, θ) for some θ, then $\mathfrak{H}$ is neither triply transitive, nor the alternating group on a set G.

Theorem 1.4. ***Every permutation group on a set G,*** $|G| \leqslant 4$, ***is the*** *automorphism group of* ***a groupoid (G,*** θ) *for some* θ.

The proof of Theorem 1.4 is the main purpose of §§ 1.4, 1.5 below. In order to count the number of groupoids for each permutation group, we will experimentally verify the existence for each case.

§ 1.3 is the introduction of the basic concept for the preparation of §§ 1.4, 1.5.

1.3. Preparation. Let $\mathfrak{G}$ denote the set of all binary operations θ, ξ, · . defined on a set G. Let a, β, · · · be elements of $\mathfrak{S}(G)$, i. e. permutations of G. To each a a unary operation $\bar{\alpha}$ on $\mathfrak{G}$, $\theta \to \theta^{\bar{\alpha}}$, corresponds in the following way :

$$x\theta^{\bar{\alpha}}y = \{(x\alpha^{-1})\theta(y\alpha^{-1})\}\alpha, \ x, \ y \ \in G.$$

The groupoids (G, θ) and (G, $\theta^{\bar{\alpha}}$) are isomorphic since $(x\theta^{\bar{\alpha}}y)\alpha^{-1} = (x\alpha^{-1})\theta(y\alpha^{-1})$. Clearly a is an automorphism of (G, θ) if and only if $\theta^{\bar{\alpha}} = \theta$. The product $\bar{\alpha}\bar{\beta}$ of $\bar{\alpha}$ and $\bar{\beta}$ is defined in the usual way:

$$\theta^{\bar{\alpha}\bar{\beta}} = (\theta^{\bar{\alpha}})^{\bar{\beta}} \text{ for all } \theta \in \mathfrak{G}.$$

It is easy to see that

$$\theta^{\bar{\alpha}\bar{\beta}} = \theta^{\overline{\alpha\beta}} \text{ for all } \theta \in \mathfrak{G}.$$

$\theta^{\bar{\alpha}} = \theta^{\bar{\beta}}$ if and only if $\alpha\beta^{-1} \in \mathfrak{A}(\theta)$. Let $\bar{\mathfrak{S}} = \{\bar{\alpha};\ \alpha \in \mathfrak{S}(G)\}$. Then $\bar{\mathfrak{S}}$ is isomorphic onto $\mathfrak{S}(G)$ under $\alpha \to \bar{\alpha}$. Suppose $\bar{\alpha} = \beta$. $\alpha\beta^{-1}$ is in $\mathfrak{A}(G, \theta)$ for all $\theta \in \mathfrak{G}$. On the other hand, there is $\theta_0 \in \mathfrak{G}$ such that $\mathfrak{A}(G, \theta_0)$ consists of the identical mapping ε alone (cf. **[20]**). Hence $\alpha\beta^{-1} = \varepsilon$ and so $\alpha = \beta$.

Define another unary operation $\theta \to \theta'$ on $\mathfrak{G}$ as follows:

$$x\theta' y = y\theta x.$$

Then clearly $(\theta')' = \theta$ and (G, θ) is anti-isomorphic onto (G, θ'); $\theta' = \theta$ if and only if (G, θ) is commutative. Also $(\theta')^{\bar{\alpha}} = (\theta^{\bar{\alpha}})'$ for all $\theta \in \mathfrak{G}$.

We denote $(\theta')^{\bar{\alpha}}$ by $\theta^{\bar{\alpha}'}$. Then a is an anti-automorphism of (G, θ) if and only if $\theta^{\bar{\alpha}'} = \theta$. We can easily prove

$$(\theta^{\bar{\alpha}})^{\bar{\beta}'} = \theta^{\overline{\alpha\beta}}$$
$$(\theta^{\bar{\alpha}'})^{\bar{\beta}} = \theta^{\overline{\alpha\beta}'}$$
$$(\theta^{\bar{\alpha}'})^{\bar{\beta}'} = \theta^{\overline{\alpha\beta}}.$$

As defined in § 1 .1, $\mathfrak{A}(\theta)$ is the automorphism group of (G, θ) while $\mathfrak{A}'(\theta)$ denotes the set of all anti-automorphisms of (G, θ).

We define

$$\mathfrak{B}(\theta) = \mathfrak{A}(\theta) \text{ u } \mathfrak{A}'(\theta).$$

Then $\mathfrak{B}(\theta)$ is a subgroup of $\mathfrak{S}(G, \theta)$ and the index of $\mathfrak{A}(\theta)$ to B(8) is 2.

Let $\beta \in \mathfrak{S}(G)$. Then

$$\mathfrak{A}(\theta^{\bar{\beta}}) = \beta^{-1} \cdot \mathfrak{A}(\theta) \cdot \beta, \qquad \mathfrak{A}'(\theta^{\bar{\beta}}) = \beta^{-1} \cdot \mathfrak{A}'(\boldsymbol{\theta}) \cdot \beta.$$

Let $\mathfrak{H} = \mathfrak{A}(G, \theta)$ and let $\alpha \in \mathfrak{S}(G)$. Then $\mathfrak{H} = \mathfrak{A}(\theta^{\bar{\alpha}})$ if and only if α is in the normalizer $\mathfrak{N}(\mathfrak{H})$ of $\mathfrak{H}$ in $\mathfrak{S}(G)$. Therefore $\theta^{\bar{\alpha}} = \theta^{\bar{\beta}}$ and $\mathfrak{A}(\theta^{\bar{\alpha}}) = \mathfrak{A}(\theta^{\bar{\beta}}) = \mathfrak{A}(\theta) = \mathfrak{H}$ if and only if $\alpha, \beta \in \mathfrak{N}(\mathfrak{H})$ and $\alpha \equiv \beta$ (mod $\mathfrak{H}$).

Let $\mathfrak{H}$ be a permutation group over a set G and suppose that $\mathfrak{H}$ is generated by a subset $\mathfrak{K} = \{\alpha_\lambda;\ \lambda \in X\}$ of $\mathfrak{H}$.

Let

$$G \times G = \{(x, y);\ x, y \in G\}.$$

A binary operation on G is understood to be a mapping θ of GX G into G. $\mathfrak{H}$ is contained in the automorphism group $\mathfrak{A}(G)$ of a groupoid G defined by θ if and only if, for $x, y \in$ G,

$$[(\text{x}, y)\theta]\alpha = (\text{xa}, y\alpha)\theta \text{ for all } \alpha \in \mathfrak{H}.$$

We define an equivalence relation $\mathfrak{V}$ on GX G as follows:

(x, y) $\mathfrak{V}$ (z, u) if and only if z = ***xa***, u **=** ***ya*** for some $\alpha \in \mathfrak{H}$. Clearly $\mathfrak{V}$ is the transitive closure of a relation $\mathfrak{V}_1$, defined by

(x, y) $\mathfrak{V}_1$ (z, u) if and only if z = ***xa***, u **=** $y\alpha$ for some a $\in \mathfrak{K}$.

If we let c = ***(a***, $b)\theta$ and if (x, y) ***%(a***, b), then (x, $y)\theta$ is automatically determined by

$$(\boldsymbol{x}, y)\theta = [(\boldsymbol{a}, b)\theta]\alpha \text{ for some } \boldsymbol{a} \in \mathfrak{H}.$$

Let ***{(a***, b_ξ); $\xi \in \Xi\}$ be a representative system from the equivalence classes modulo $\mathfrak{V}$. We may determine only $\{(a_\xi, b_\xi)\theta;\ \xi \in \Xi\}$. However, there is some restriction for choosing $(a_\xi, b_\xi)\theta$:

$$[(a_\xi, b_\xi)\theta]\alpha = (a_\xi\alpha, b_\xi\alpha)\theta.$$

For (a_ξ, b_ξ) define an equivalence relation $\underset{\xi}{\sim}$ on the set union $\mathfrak{K}\cup\mathfrak{K}^{-1}$ as follows :

$$\alpha \underset{\xi}{\sim} \beta \text{ ifandonly if } (a_\xi\alpha, b_\xi\alpha) = (a_\xi\beta, b_\xi\beta).$$

For (a_ξ, b_ξ) we select an element c_ξ of G such that the following condition is satisfied :

$$a \underset{\xi}{\sim} \beta \text{ implies } c_\xi\alpha = c_\xi\beta.$$

1.4. **Groupoids of order** ≤ 3. First of all we explain the notation and the abbreviations appearing below :

$\mathfrak{H}$	Automorphism group $\mathfrak{H}$.
S_i	The symmetric group of degree ***i.***
c	The number of conjugates of $\mathfrak{H}$, i.e. $c = \dfrac{\lvert S_i\rvert}{\lvert \text{Normalizer} \rvert}$,
n	The index of $\mathfrak{H}$ to its normalizer, $n = \dfrac{\lvert \text{Normalizer} \rvert}{\lvert\mathfrak{H}\rvert}$,
up to isO	Up to isomorphism.
up to dual	Up to dual-isomorphism (i.e. anti-isomorphism).
self-dual	Anti-isomorphic to itself.
comm	Commutative.

First we have the following table for groupoids of order 2. Since the case is simple, we omit the explanation.

TABLE 1. ***Groupoids of Order 2***

$\mathfrak{H}$	c	n	Comm, up to iso	Self-dual, non-comm, up to iso	Non-self-dual, up to iso, up to dual	Total up to iso, up to dual	Total up to iso	Semi-groups up to iso, up to dual
S_2	1	1	0	0	2	2	4	1
$\{e\}$	1	2	4	0	1	5	6	3
Total			4	0	3	7	10	4

For S_2 $\begin{array}{|cc|}1 & 1\\ 2 & 2\end{array}$ † $\begin{array}{|cc|}2 & 1\\ 2 & 1\end{array}$

For $\{e\}$ $\begin{array}{|cc|}1 & 1\\ 1 & 1\end{array}$ $\begin{array}{|cc|}1 & 1\\ 1 & 2\end{array}$ $\begin{array}{|cc|}1 & 2\\ 2 & 1\end{array}$ $\begin{array}{|cc|}2 & 1\\ 1 & 1\end{array}$ $\begin{array}{|cc|}1 & 1\\ 2 & 1\end{array}$

In the following table [(I, 2, 3)] is the permutation group generated by a 3-cycle (1, 2, 3). [(I, 2)] is one generated by a 2-cycle or substitution (1, 2).

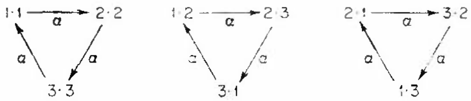
TABLE 2. *Groupoids of Order 3*

$\mathfrak{H}$	c	n	Comm, up to iso	Self-dual non-comm, up to iso	Non-self-dual, up to iso, up to dual	Total up to is0', up to dual	Total up to is0	Semi-groups up to iso, up to dual
S_3	1	1	1	0	1	2	3	1
[(1, 2, 3)]	1	2	4	0	4	8	12	0
[(1, 2)]	3	1	8	0	35	43	78	5
$\{e\}$	1	6	116	9	1556	1681	3237	12
Total			129	9	1596	1734	3330	18

By Theorem 1, if $\mathfrak{H} = S_3$, we have two isomorphically, dual-isomorphically distinct groupoids :

$\begin{array}{|ccc|}1 & 2 & 3\\ 1 & 2 & 3\\ 1 & 2 & 3\end{array}$ $\begin{array}{|ccc|}1 & 3 & 2\\ 3 & 2 & 1\\ 2 & 1 & 3\end{array}$

Case $\mathfrak{H}$ = [(1, 2, 3)]. Let α = (1, 2, 3). %-classes :



† $\begin{array}{|cc}1 & 1\\ 2 & 2\end{array}$ denotes the multiplication table $\begin{array}{c|cc|} & 1 & 2\\ \hline 1 & 1 & 1\\ 2 & 2 & 2\end{array}$

Since there is no restriction to choosing $((1\ .\ 1)\theta, (1\cdot 2)\theta, (2\cdot 1)\theta\}$, we have 27 groupoids G such that

$$[\alpha] \subseteq \mathfrak{A}(G).$$

However, the set of the 27 groupoids contains the 3 groupoids in which S_3 is the automorphism group; the number of isomorphically distinct groupoids G for $\mathfrak{H} = [\alpha]$ is

$$\tfrac{1}{2}(27-3) = 12 \text{ where } n = 2 \text{ in Table 2.}$$

If G has dual-automorphisms, $\beta = (1, 2)$ must be a dual-automorphism. In this case, since

$$(3\cdot 3)\beta = 3.3, \ (1\cdot 2)\beta = 1\cdot 2, \ (2\cdot 1)\beta = 2\cdot 1,$$

we must have $(3\cdot 3)\theta = (1\cdot 2)\theta = (2\cdot 1)\theta = 3$. Therefore if $\mathfrak{H} \subseteq \mathfrak{A}(G)$ and if (1, 2) is a dual-automorphism of G, then G is

1	3	2
3	2	1
2	1	3

while this G is already obtained for $\mathfrak{H} = S_3$, and (1, 2) is an automorphism. In the present case there is no self-dual, non-commutative groupoid. There are formally 9 commutative groupoids; but excluding one we have non-isomorphic commutative groupoids :

$$\tfrac{1}{2}(9-1) = 4$$

and $12\text{-}4 = 8$ non-self-dual G's,

$8 \div 2 = 4$ isomorphically distinct non-self-dual G's.

Therefore we have $4+4 = 8$ non-isomorphic, non-dual-isomorphic G's.

Case $\mathfrak{H} = [(1, 2)]$. Let $\alpha = (1, 2)$. There are 5 &classes among which a class consists of only $3\cdot 3$. Clearly $(3.3)\ \theta = 3$. The number of non-isomorphic G's is

$$81\text{-}3 = 78.$$

If G is commutative then $(1\cdot 2)\alpha = 1.2$, hence $(1\cdot 2)\theta = 3$. The number of non-isomorphic commutative G's is

$$9\text{-}1 = 8.$$

The number of non-self-dual G's is 78-8 = 70, and hence the number of those, up to isomorphism, is

$$70 \div 2 = 35.$$

Therefore the number of non-isomorphic, non-dual-isomorphic G's is

$$35+8 = 43.$$

We remark that there is no non-commutative self-dual groupoid for $\mathfrak{H}$ because S_3 has no subgroup of order 4.

Case $\mathfrak{H} = \{e\}$. First, we find the number of self-dual, non-commutative groupoids G for $\{e\}$. Let $\beta = (1, 2)$ be a dual-automorphism of G. Then we can easily see that

$$(1\cdot 2)\beta = (1\cdot 2),\ (2\cdot 1)\beta = (2\cdot 1),\ (3\cdot 3)\beta = (3.3)$$
$$(1\cdot 1)\beta = (2\cdot 2),\ (1\cdot 3)\beta = (3\cdot 2),\ (3\cdot 1)\beta = (2\cdot 3),$$

and hence

$$(1\cdot 2)\theta = (2\cdot 1)\theta = (3\cdot 3)\theta = 3.$$

The 27 G's contain the 9 G's which appeared in the previous cases. We have that the number of isomorphically distinct G's is

$$\tfrac{1}{2}(27-9) = \mathbf{9}$$

since we recall that the normalizer of $[(I, 2)]$ is itself.

The number $y = 116$ of all non-isomorphic commutative groupoids whose automorphism group is $\{e\}$ is the solution of

$$6y+4\times 2+8\times 3+1 = 3^{6}.$$

The number $x = 3237$ of all non-isomorphic groupoids corresponding to $\{e\}$ is the solution of

$$6x+78\times 3+12\times 2+3 = 3^{9}.$$

The number of non-self-dual G's, up to isomorphism and dual-isomorphism, is

$$\tfrac{1}{2}(3237-(116+9)) = 1556.$$

The total number of G's up to isomorphism and dual-isomorphism is the sum

$$116+9+1556 = 1681.$$

For $[(1, 2, 3)]$, let $\alpha = (1, 2, 3)$:

x	y	z
$z\alpha$	$x\alpha$	$y\alpha$
$y\alpha^2$	$z\alpha^2$	$x\alpha^2$

where (x, y, z) is

(1, 2, 1), (2, 2, I), (2, 3, 2), (2, 1, 3) commutative,

(1, 1, 2), (2, 1, 1), (2, 1, 2), (2, 3, 1) non-self-dual.

For [(1, 2)], let $\beta = (1, 2)$:

commutative

x	3	z
3	$x\beta$	$z\beta$
z	$z\beta$	3

where (x, z) is

(1, 1), (1, 3), (2, 1), (2, 2),
(2, 3), (3, 1), (3, 2), (3, 3).

Non-self-dual :

x	y	z
$y\beta$	$x\beta$	$z\beta$
u	$u\beta$	3

where (x, y, z, u) is

(1,1,1,1),(1,1,3,1),(1,3,2,3),(2,1,2,2),(2,3,1,2),(3,1,1,3),(3,1,3,2),
(1,1,1,2),(1,1,3,2),(2,1,1,1),(2,1,2,3),(2,3,1,3),(3,1,2,1),(3,1,3,3),
(1,1,2,1),(1,1,3,3),(2,1,1,2),(2,1,3,1),(2,3,2,3),(3,1,2,2),(3,3,1,2),
(1,1,2,2),(1,3,1,2),(2,1,1,3),(2,1,3,2),(3,1,1,1),(3,1,2,3),(3,3,1,3),
(1,1,2,3),(1,3,1,3),(2,1,2,1),(2,1,3,3),(3,1,1,2),(3,1,3,1),(3,3,2,3).

For {e}:

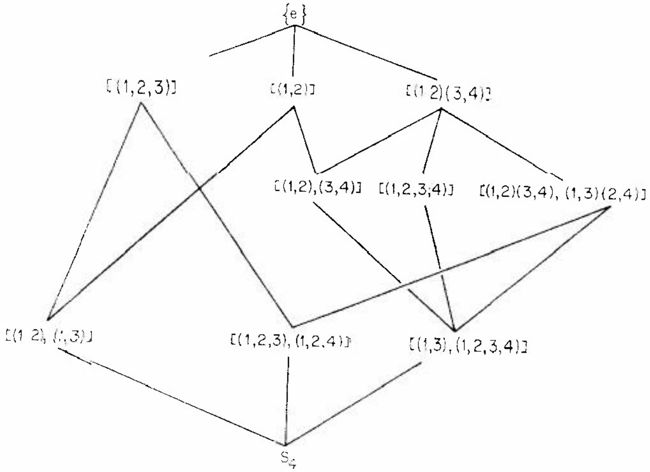
x	3	Y
3	$x\beta$	$z\beta$
z	$y\beta$	3

where (x, y, z) is

(1, 1, 2), (2, 1, 2), (3, 1, 2),
(1, 1, 3), (2, 1, 3), (3, 1, 3),
(1, 2, 3), (2, 2, 3), (3, 2, 3).

1.5. Groupoids of order 4.

TABLE 3. *Subgroups of S_4*

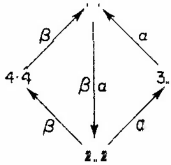


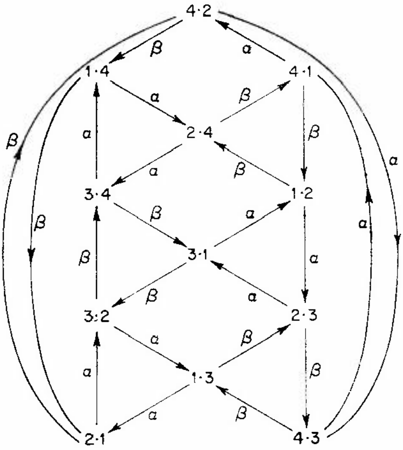
This diagram shows that A is lower than B and is connected with B by a segment if and only if some conjugate of A contains some conjugate of B.

If $\mathfrak{H} = S_4$, G is isomorphic to either a right zero or a left zero semigroup, by Theorem 1.1.

(1) $\mathfrak{H} = [(1, 2, 3), (1, 2, 4)]$ (alternating group).

Let a = (1, 2, 3), β = (1, 2, 4). We have the !&classes :





$(3 \cdot 3)\beta = 3 \cdot 3$ implies $3 \cdot 3 = 3$, hence G has to be idempotent. G is a right zero semigroup if $4 \cdot 2 = 2$; a left zero semigroup if $4 \cdot 2 = 4$. Let G_i be a groupoid determined by $4 \cdot 2 = i$ $(i = 1, 2)$. G_1 is isomorphic to G_2 under a transposition (1, 2) and also G_1 is anti-isomorphic to G_2.

G_1	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

$\cong$

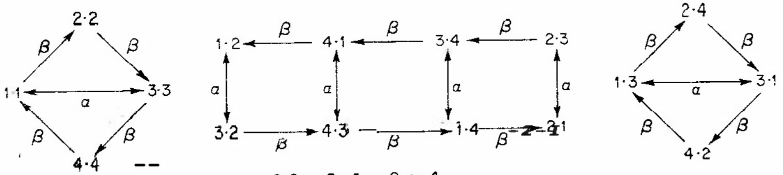
G_2	1	2	3	4
1	1	4	2	3
2	3	2	4	1
3	4	1	3	2
4	2	3	1	4

G_1 is characterized by the groupoid, which is neither a left nor a right zero semigroup, such that any permutation is either an automorphism or an anti-automorphism.

(2) $\mathfrak{H} = [(1, 3), (1, 2, 3, 4)]$.

The normalizer of $\mathfrak{H}$ is $\mathfrak{H}$ itself, $|\mathfrak{H}| = 8$, $n = 1$, c $= 24/8 = 3$.

Let a = (1, 3), $\beta = (1, 2, 3, 4)$. We have the 'B-classes :

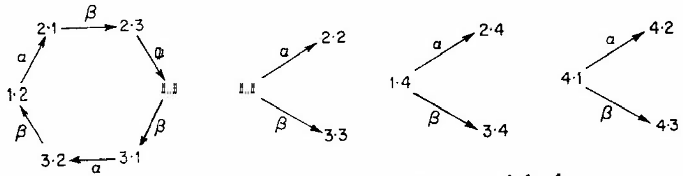


2·2, 2·4 = 2 or 4

The calculation $2^2 \times 4 = 16$, $16 - 2 = 14$ gives the number of non-isomorphic G's. Suppose the groupoids have a dual automorphism. Since no subgroup is of order 16, every element of $\mathfrak{H}$ is a dual automorphism. For a dual automorphism a, $(1 \cdot 3)\alpha = 1 \cdot 3$, hence $1 \cdot 3 = 2$ or 4. For an automorphism β, $(1 \cdot 3)\beta = 2 \cdot 4 = 2$ or 4 because $(2 \cdot 4)\alpha = 2 \cdot 4$. However, this is a contradiction to $2\beta = 3, 4\beta = 1$. Hence there are no self-dual G's. The number of non-isomorphic, non-anti-isomorphic G's is $14 \div 2 = 7$.

(3) $\mathfrak{H} = [(1, 2), (1, 3)]$.

$|\mathfrak{H}| = 6$, $n = 1$, c $= 24/6 = 4$. We have the B-classes :



1·1, 1·4, 4·1 = 1 or 4, 4·4 = 4

The calculation $4 \times 2^3 = 32$, $32 - 2 = 30$ gives the number of non-isomorphic G's. If a dual automorphism exists, then it is in $\mathfrak{H}$. Accordingly if G is self-dual, it must be commutative.

We find the commutative G's:

$$(1\cdot 2)\alpha = 2\cdot 1 = 1\cdot 2,\ 1\cdot 2 = 3 \text{ or } 4.$$

We have 8 non-isomorphic commutative G's, and the calculation $30 - 8 = 22$, $22 \div 2 = 11$ gives the number of non-self-dual G's, and we have a total of $8 + 11 = 19$ non-isomorphic and non-anti-isomorphic G's.

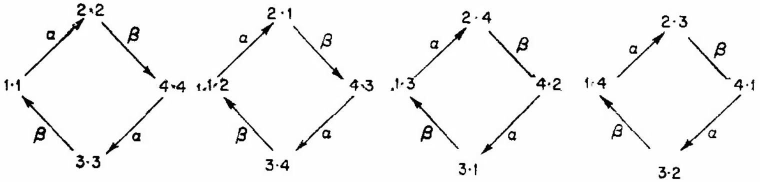
(4) $\mathfrak{H} = [(1, 2)(3, 4), (1, 3)(2, 4)]$.

$|\mathfrak{H} = 4$, $\mathfrak{H}$ is normal, $n = 24/4 = 6$, $c = 1$,

The number of groupoids G with $\mathfrak{H} \subset \mathfrak{A}(G)$ which appeared in the previous cases is

$$14X3+2+2 = 46.$$

Let $\alpha = (1, 2)(3, 4)$, $\beta = (1, 3)(2, 4)$. We have the 'B-classes:

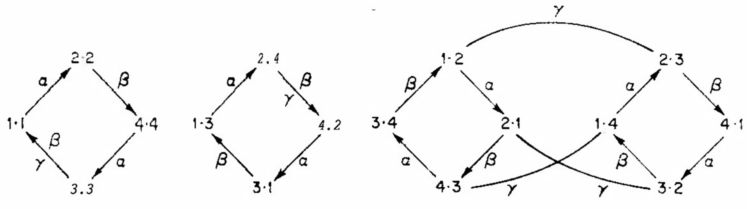


The calculation $4^4 - 46 = 210$, $210 \div 6 = 35$ gives the number of non-isomorphic G's. There is no commutative G in the 35 G's, because

$$(1\cdot 2)\alpha = 1.2$$

and we have no value $1\cdot 2$.

Suppose $\gamma = (1, 3)$ is a dual automorphism. We then have the 'B-classes:



2·2, 2·4 = 2 or 4

The class of $2^2 \times 4 = 16$ groupoids contains 2 of those corresponding to $[(1, 2, 3), (1, 2, 4)]$, and so we calculate $16 - 2 = 14$, $14 \div 2 = 7$, for the number of self-dual, non-commutative G's. Since the normalizer of $[(1, 3), (1, 2, 3, 4)]$ is itself, $8 \div 4 = 2$, and we calculate $35 - 7 = 28$, $28 \div 2 = 14$ non-self-dual G's, giving $14 + 7 = 21$ for the total up to isomorphism and dual-isomorphism.

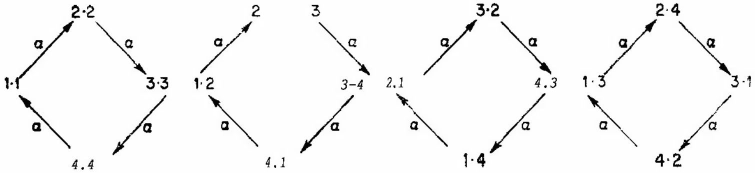
(5) $\mathfrak{H} = [(1, 2, 3, 4)]$.

$|\mathfrak{H}| = 4$. The normalizer of $\mathfrak{H}$ is $[(1, 3), (1, 2, 3, 4)]$ of order 8, $\boldsymbol{n} = 8/4 = \mathbf{2}$, $c = 24/8 = 3$.

The number of the groupoids corresponding to the groups which contain $\mathfrak{H}$ is

$$14+2 = 16.$$

Let $\alpha = (1, 2, 3, 4)$. We have the 'B-classes:



We calculate $4^4 - 16 = 240$, $240 \div 2 = 120$ for the number of non-isomorphic G's. We have $[(1, 2, 3, 4)] \subset [(1, 3), (1, 2, 3, 4)]$. Suppose $\gamma = (1, 3)$ is a dual-automorphism. Then $(1\cdot 2)\alpha = (1\cdot 2)\gamma$, but there is no value $1\cdot 2$ which satisfies this. Suppose some G is commutative. Then $(1\cdot 3)\alpha^2 = 3\cdot 1 = 1\cdot 3$, but there is no $1\cdot 3$ fixed by α^2. Consequently there is no self-dual G in this case, and we have only the

$$120 \text{ a } 2 = 60 \text{ non-self-dual G's.}$$

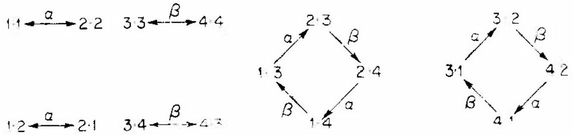
(6) $\mathfrak{H} = [(1, 2), (3, 4)]$.

$|\mathfrak{H}| = 4$. Its normalizer is $[(1, 2), (1, 3, 2, 4)]$ of order 8, $n = 8/4 = 2$, $c = 24/8 = 3$.

The number of the groupoids corresponding to the groups $\supset \mathfrak{H}$ is

$$14+2 = 16.$$

Let $\boldsymbol{a} = (1, 2)$, $\beta = (3, 4)$. We have the %-classes:



1·1, 1·2 = 1 or 2   3·3, 3·4 = 3 or 4

We calculate $2^4 \times 4^2 = 256$, $256 - 16 = 240$, $240 \div 2 = 120$ for the number of non-isomorphic G's. We can prove that there is no self-dual G, so we have

$$120 \div 2 = 60 \text{ non-self-dual G's.}$$

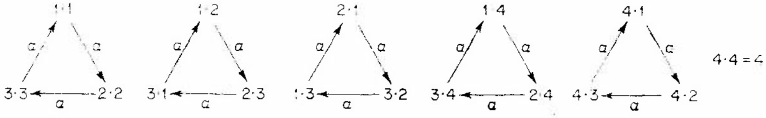
(7) $\mathfrak{H} = [(1, 2, 3)]$.

$\mathfrak{H} = 3$. The normalizer is $[(1, 2), (1, 3)]$ of order 6, $n = 6/3 = 2$, $c = 24/6 = 4$.

The number of groupoids corresponding to the groups bigger than $\mathfrak{H}$ is

$$30+2+2 = \mathbf{34.}$$

Let $\alpha = (1, 2, 3)$.



$$4{\cdot}4 = 4$$

We calculate $4^5 = 1024$, $1024 - 34 = 990$, $990 \div 2 = 495$ for the number of non-isomorphic G's.

The number of the groupoids which have $\beta = (1, 2)$ as a dual automorphism is

$$2^3 \times 4 = \mathbf{32}$$

since $1{\cdot}1 = 1$ or4, $2{\cdot}3 = 1$ or4, $3{\cdot}2 = 1$ or4.

Among the 1024 groupoids, there are 64 commutative ones. Eight of the 64 correspond to [(I, 2), (1, 3)], and so $32 - 8 = 24$ is the number of non-commutative G's which have (1, 2) as a dual-automorphism. **Two of** these 24 G's correspond to [(I, 2, 3), (1, 2, 4)], leaving

$$\mathbf{24-2 = 22.}$$

The number of commutative G's is $(64 - 8) \div 2 = 28$ (up to isomorphism). The number of non-commutative self-dual G's is

$$22 \div 2 = 11 \text{ (up to isomorphism).}$$

To count the total number up to isomorphism and dual-isomorphism, we calculate

$495 - (28 + 11) = 456$, $456 \div 2 = 228$, $228 + 39 = 267$ for this number.

(8) $\mathfrak{H} = [(1, 2)(3, 4)]$.

$\mathfrak{H} = 2$, the normalizer is [(1, 2), (I, 3, 2, 4)] of order 8, $n = 8/2 = \mathbf{4}$, $\mathbf{c} = 24/8 = \mathbf{3}$.

The number of G's with $\mathfrak{A}(G) \supset \mathfrak{H}$ is

$$240+240+210+42+2+2 = 736.$$

Under $\alpha = (1, 2)(3, 4)$, we have the %-classes:

$$1{\cdot}1 \xleftrightarrow{\alpha} 2\ 2 \qquad \mathbf{3}\ 3 \xleftrightarrow{\alpha} 44 \qquad 1{\cdot}2 \xleftrightarrow{\alpha} 2' \qquad 3\ 4 \xleftrightarrow{\alpha} 4\ 3$$

$$1{\cdot}4 \xleftrightarrow{\alpha} 2{\cdot}3 \qquad 4{\cdot}1 \xleftrightarrow{\alpha} 3{\cdot}2 \qquad 3 \xleftrightarrow{\alpha} 2\mathbf{4} \qquad 3{\cdot}1 \xleftrightarrow{\alpha} 4\ 2$$

The calculation $4^8 - 736 = 64{,}800$, $64{,}800 \div 4 = 16{,}200$ gives the number of non-isomorphic G's.

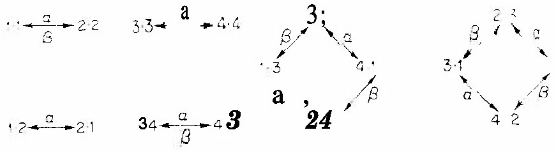
Considering the self-dual G'S, we have

$$[(1, 2)(3, 4)] \subset [(1, 2), (3, 4)],$$

$$[(1, 2)(3, 4)] \subset [(1, \mathbf{3}, \mathbf{2}, 4)],$$

$$[(1, 2)(3, 4)] \subset [(1, 2)(3, 4), (1, 3)(2, 4)].$$

If β = (1, 2) is a dual-automorphism, we have the &classes:

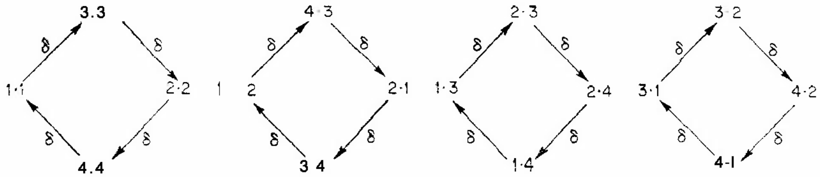


1·2, 3·3 = 3 or 4 3·4 = 1 or 2 1·1 ≡ 1 or 2

Here we have $2^4 \times 4^2 = 256$ non-isomorphic G's.

If γ = (1, 3)(2, 4), is a dual-automorphism, $(1{\cdot}3)\gamma = 1{\cdot}3$, but no element is fixed by γ. This case is impossible, therefore we see that there is no commutative G.

If $\delta = (1, 3, 2, 4)$ is a dual-automorphism, under δ, we have the B-classes:



We have 44 = 256 non-isomorphic G's in this case. The two cases contain 16 groupoids in common among which 14 correspond to [(1,2)(3,4), (1, 3)(2,4)] and 2 to [(1, 2, 3), (1, 2, 4)], and we calculate 256 − 16 = 240,240 **X** 2 = 480, 480÷4 = 120 self-dual non-commutative G's, and further calculation gives 16,200 − 120 = 16,080, 16,080 ÷ 2 = 8040, 8040 + 120 = 8160 for the number up to isomorphism and dual-isomorphism.

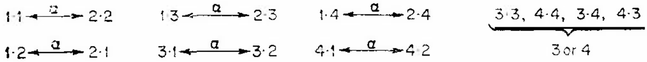
(9) $\mathfrak{H}$ = [(1, 2)].

$|\mathfrak{H}|$ = 2, the normalizer is [(1, 2), (3, 4)] of order 4, ***n*** **=** 4/2 **= *2,*** ***c*** **=** 24/4 **= *6*.**

The number of G's with $\mathfrak{A}(G) \supset \mathfrak{H}$ is

$$60 + 240 + 14 + 2 = 316.$$

Under ***a*** **=** (1, 2) we have the %-classes:



We calculate 4^6 x $2^4 = 65{,}536$, $65{,}536 - 316 = 65{,}220$, $65{,}220 \div 2 = 32{,}610$, for the number of non-isomorphic G's.

$$[(1,\ 2)] \subset [(1,\ 2),\ (3,4)].$$

Suppose $\beta = (3,\ 4)$ is a dual-automorphism. Then

$$(3\cdot 4)\alpha = (3\cdot 4)\beta = 3.4.$$

This is impossible since no element is fixed by both a and β. Therefore there is no self-dual non-commutative G. To find all commutative G's, we have the B-classes :

$$1\cdot1 \xleftrightarrow{\alpha} 2\cdot2 \qquad 1\cdot2 \xleftrightarrow{\alpha} 2\cdot1 \qquad 1\cdot3 \xleftrightarrow{\alpha} 2\cdot3 \qquad 1\cdot4 \xleftrightarrow{\alpha} 2\cdot4, \qquad 3.4 = 4.3$$

$$1.2,\ 3.3,\ 3\text{-}4.\ 44 = 3 \text{ or } 4,$$

and we find $4^3 \times 2^4 = 1024$ non-isomorphic G's.

The 32 commutative groupoids correspond to [(I, 2), (1, 3)]. Of these, 16 are contained in the 1024 groupoids, and we calculate :

$1024 - 16 = 1008$,

1008s $2 = 504$ (commutative, up to isomorphism),

$32{,}610 - 504 = 32{,}106$,

$32{,}106 \div 2 = 16{,}053$ (non-commutative, up to isomorphism),

$504 + 16{,}053 = 16{,}557$ (total, up to isomorphism and dual isomorphism).

(10) $\mathfrak{H} = \{e\}$.

$n = 24$, $c = 1$.

We consider G's. with dual-automorphisms. We may assume that (1, 2) is the only dual-automorphism.

The %-classes are:

$$\begin{array}{lll} 1\cdot1 \longleftrightarrow 2\cdot2 & 1\cdot4 \longleftrightarrow 4\cdot2 & 3.3;\ 4\cdot4,\ 1\cdot2,\ 2\cdot1 = 3 \text{ or} 4 \\ 1\cdot3 \longleftrightarrow 3\cdot2 & 4\cdot1 \longleftrightarrow 2\cdot4 & \\ 3\cdot1 \longleftrightarrow 2\cdot3 & 3\cdot4 \longleftrightarrow 4\cdot3 & \end{array}$$

We find 4^6 x $2^4 = 65{,}536$ non-isomorphic self-dual G's.

Among them there are $4^3 \times 2^4 = 1024$ commutative G's, leaving $65{,}536 - 1024 = 64{,}512$ non-commutative self-dual G's.

The number of self-dual, non-commutative G's with dual-automorphism (1, 2) already counted is :

for [(1, 2, 3), (1, 2, 4)]	$1 \times 2 = 2$
for [(1, 2)(3, 4), (1, 3)(2, 4)]	$7 \times 2 = 1\ 4$
for[(1, **2**, 3)]	11x$4 = 44$
for [(1, 2)(3, 4)]	$120 \times 2 = 240$
totalling	300
leaving	$64{,}512 - 300 = 64{,}212$.

The self-dual non-commutative G's number $64{,}212 \div 4 = 16{,}053$.

Next we count the number of commutative G's, comprising the already counted commutative G's:

$$8 \times 4 = 32$$

$$28 \mathrm{X}\ 8 = 224$$

$$504 \times 12 = 6048$$

totalling $6304.$

Solving 24x+ 6304 = 4^{10} = 1,048,576, we obtain

$$x = 43{,}428.$$

To count the total number y of non-isomorphic G's, we may subtract the following sum from 4^{16}:

$$2\times 1+1\times 2+14\times 3+30\times 4+35\times 6+120\times 6$$

$$+120\times 6+495\times 8+16{,}200\times 12+32{,}610\times 12;$$

then we have y = 178,932,325.

To count the number z of non-self-dual G's, we have:

$$2z+43{,}428+16{,}053 = 178{,}932{,}325,$$

$$z = 89{,}436{,}422.$$

The number w of non-isomorphic, non-anti-isomorphic G's is

$$w = 43{,}428+16{,}053+89{,}436{,}422 = 89{,}495{,}903.$$

Table 4 shows the summary.

Addendum. We would like to mention the following propositions.

THEOREM 1.5. *Let G be a finite set. For every permutation group $\mathfrak{H}$ on G (i.e. $\mathfrak{H} \subseteq \mathfrak{S}(G)$), there is at least a groupoid G with $\mathfrak{H} \subseteq \mathfrak{A}(G)$.*

Let $N(\mathfrak{H})$ denote the number of all groupoids G with $\mathfrak{H} \subseteq \mathfrak{A}(G)$ and $M(\mathfrak{H})$ the number of all groupoids G with $\mathfrak{H} = \mathfrak{A}(G)$. $N(\mathfrak{H})$ and $M(\mathfrak{H})$ are the numbers which count seemingly distinct G(containing isomorphic or anti-isomorphic G's).

The following theorem is obvious.

THEOREM 1.6. *Let $\mathfrak{H}$ be a proper subgroup of $\mathfrak{S}(G)$. There exists a groupoid G with $\mathfrak{H} = \mathfrak{A}(G)$ if and only if*

$$N(\mathfrak{H}) > \sum_{\mathfrak{H}\subset\mathfrak{K}} M(\mathfrak{K}).$$

Problem. Let $|G| = 5$. Under what condition on the properties (for example transitivity) on $\mathfrak{H}$, do there exist groupoids G, $|G| = 5$, such that $\mathfrak{H} = \mathfrak{A}(G)$?

TABLE 4. *Groupoids of Order 4 and their Automorphism Groups*

$\mathfrak{H}$	c	n	Comm, up to iso	Self-dual, non-comm, up to iso	Non-self-dual, up to iso	Total up to iso, up to dual iso	Total up to iso	Semigroups up to iso, up to dual iso
S_4	1	1	0	0	1		2	1
[(1, 2, 3), (1, 2, 4)]	1	2	0	1	0	1	1	0
[(1, 3), (1, 2, 3, 4)]	3	1	0	0	7	7	14	0
[(1, 2), (1, 3)]	4	1	8	0	11	19	30	5
[(1, 2)(3, 4), (1,3)(2, 4)]	1	6	0	7	14	21	35	1
[(1, 2, 3, 4)]	3	2	0	0	60	60	120	0
[(1, 2), (3, 4)]	3	2	0	0	60	60	120	2
[(1, 2, 3)]	4	2	28	11	228	267	495	0
[(1, 2) (3, 4)]	3	4	0	120	8040	8160	16,200	4
[(1, 2)]	6	2	504	0	16,053	16,557	32,610	40
[e]	1	24	43,428	16,053	89,436,422	89,495,903	178,932,325	73
Total			43,968	16,192	89,460,896	89,512,864	178,981,952	126

PART II. SYSTEM OF OPERATIONS AND EXTENSION THEORY

2.1. Introduction. Let T be a right zero semigroup, i.e. $\alpha\beta = \beta$ for all a, $\beta \in T$, and $\{D_\alpha; a \in T\}$ be a system of semigroups with same cardinality $|D_\alpha| = m$. The problem at the present time is to construct a semigroup D such that D is a set union of $D_{,}$, $a \in T$, and

$$D_\alpha D_\beta \subseteq D_\beta \text{ for all } a, \beta \in T.$$

D does not necessarily exist for an arbitrary system of semigroups. For example, let

D,: right zero semigroup of order 2.

	a	*b*
a	*a*	*b*
b	*a*	*b*

D_2: a group of order 2.

	c	*d*
c	*c*	*d*
d	*d*	*c*

Here $D_1 \cap D_2 = \emptyset$. Then there is no semigroup D satisfying

$$D = D_1 \cup D_2, \qquad D_1 D_2 \subseteq D_2, \qquad D_2 D_1 \subseteq D_1.$$

So our question is this:

Under what condition on $\{D_{,}; \alpha \in T\}$ does there exist such a semigroup D?

How can we determine all D for given T and $\{D_{,}; a \in T\}$?

The problem in some special cases was studied by R. Yoshida [18], [19] in which he did not assume the same cardinality of $D_{,}$. In this paper we look at the problem from the more general point of view; we will introduce the concept of a general product of a set by a semigroup using the system of groupoids. Finally we will show the computing results on a certain special case. The detailed proof will be published elsewhere.

2.2. The system of operations.+ Let E be a set and $\mathfrak{B}_E$ be the set of all binary operations (not necessarily associative) defined on E. Let x, y $\in E$, $\theta \in \mathfrak{B}_E$ and let $x\theta y$ denote the product of x and y by θ. A groupoid with θ defined on E is denoted by $E(\theta)$. The equality of elements of $\mathfrak{B}_E$ is defined in the natural sense:

$$\theta = \eta \text{ if and only if } x\theta y = x\eta y \text{ for all x, } y \in E.$$

Let $a \in E$ be fixed. For a we define two binary operations ${}_a\!*$ and $*_a$ as follows :

$$x(\theta\ {}_a\!*\ \eta)y = (x\theta a)\eta y, \tag{2.1}$$

$$x(\theta\ *_a\ \eta)y = x\theta(a\eta y). \tag{2.2}$$

† The system of semigroup operation was studied in [7].

Immediately we have :

PROPOSITION **2.1.** ***$\mathfrak{B}_E$ is a semigroup with respect to $_a \ast$ and $\ast_a$ for all $a \in E$.***

The semigroups $\mathfrak{B}_E$ with $_a\ast$ and $\ast_a$ are denoted by $\mathfrak{B}_E\ ({}_a\ast)$ and $\mathfrak{B}_E\ (\ast_a)$ respectively.

$E(\theta)$ is associative if and only if $\theta\ {}_a\ast\ \theta = \theta \ast_a\ \theta$ for all $a \in E$

Let φ be a permutation of E. For $\theta \in \mathfrak{B}_E$, $\theta\varphi$ is defined by

$$x(\theta\varphi)y = [(x\varphi^{-1})\theta(y\varphi^{-1})]\varphi. \tag{2.3}$$

Thus φ induces a permutation of $\mathfrak{B}_E$. For $\theta \in \mathfrak{B}_E$ another operation θ' is defined by

$$x\theta' y = y\theta x.$$

LEMMA.
$$\begin{aligned}(\theta\ {}_a\ast\ \eta)\varphi &= (\theta\varphi)\ {}_{a\varphi}\ast\ (\eta\varphi),\\ (\theta \ast_a \eta)\varphi &= (\theta\varphi) \ast_{a\varphi} (\eta\varphi),\\ (\theta\ {}_a\ast\ \eta)' &= \eta' \ast_a \theta',\\ (\theta \ast_a \eta)' &= \eta'\ {}_a\ast\ \theta'.\end{aligned}$$

PROPOSITION **2.2.** ***$\mathfrak{B}_E({}_a\ast)$ is isomorphic with $\mathfrak{B}_E({}_b\ast)$ and is anti-isomorphic with $\mathfrak{B}_E(\ast_b)$ for all a, $b \in E$***

2.3. General product. Let S be a set and T be a semigroup. Suppose that a mapping Θ of $T X T$ into $\mathfrak{B}_S$, $(a, \beta)\Theta = \theta_{\alpha,\beta}$, satisfies

$$\theta_{\alpha,\beta}\ {}_a\ast\ \theta_{\alpha\beta,\gamma} = \theta_{\alpha,\beta\gamma} \ast_a \theta_{\beta,\gamma} \quad \text{for all } a, \beta, \gamma \in T \text{ and all } a \in S \tag{2.4}$$

Consider the product set

$$S X T = \{(x, \alpha);\ x \in S, \alpha \in T\}$$

in which $(x, a) = (y, \beta)$ if and only if $x = y$, $a = \beta$.

Given S, T, Θ, a binary operation is defined on SX T as follows :

$$(x, \alpha)\ (y, \beta) = (x\theta_{\alpha,\beta}y, \alpha\beta). \tag{2.5}$$

PROPOSITION **2.3.** ***$S{\times}T$ is a semigroup with respect to the operation*** (2.5), ***and it is homomorphic onto T under the projection $(x, a) \rightarrow \alpha$.***

Definition. The semigroup, SXT with (2.5), is called a ***generalproduct*** of a set S by a semigroup T with respect to Θ, and is denoted by

$$S \overline{\times}_\Theta T.$$

If it is not necessary to specify Θ it is denoted by

$$S R T.$$

PROPOSITION **2.4.** ***Suppose that T is isomorphic with T' under a mapping ψ and $|S| = |S'|$; let φ be a bijection $S \text{-} S$. Then***

$$S \overline{\times}_\Theta T \cong S' \overline{\times}_{\Theta'} T'$$

where $\quad \Theta = \{\theta_{\alpha,\beta};\ (\alpha, \beta) \in T{\times}T\},\ \Theta' = \{\theta'_{\alpha\psi,\beta\psi};\ (\alpha\psi, \beta\psi) \in T'{\times}T'\}$

and $\quad x\theta'_{\alpha\psi,\beta\psi}y = [(x\varphi^{-1})\theta_{\alpha,\beta}(y\varphi^{-1})]\varphi,\ x, \mathrm{Y} \in S'.$

In this case we say that Θ in S is equivalent to Θ' in S'.

We understand that $S \times_{\Theta} T$ is determined by $\boldsymbol{T}$, $|S|$ and the equivalence of Θ in the above sense.

Definition. If a semigroup $\boldsymbol{D}$ is isomorphic onto some $S \times_{\Theta} T$, then $\boldsymbol{D}$ is called ***general product decomposable (gp-decomposable).*** If $|S| > 1$ and $|T| > 1$, then $\boldsymbol{D}$ is called ***properly gp-decomposable.***

Definition. Let g be a homomorphism of a semigroup $\boldsymbol{D}$ onto a semigroup $\boldsymbol{T}$: $\boldsymbol{D} = \bigcup_{\alpha \in T} D_{\alpha}$, $D_{\alpha}g = \boldsymbol{\alpha}$. If $|D_{\alpha}| = |D_{\beta}|$ for all $\boldsymbol{\alpha}, \beta \in T$, then g is called a ***homogeneous homomorphism (h-homomorphism)*** of $\boldsymbol{D}$, or $\boldsymbol{D}$ is said to be ***h-homomorphic*** onto $\boldsymbol{T}$. If $|D_{\alpha}| > 1$ and $|T| > 1$, then g is called a ***proper h-homomorphism.***

THEOREM **2.1.** ***A semigroup D is gp-decomposable if and only if D has an h-homomorphism.***

In other words, $\boldsymbol{D} \cong S \overline{\times}_{\Theta} T$, $|S| > 1$, $|T| > 1$, ***for some*** Θ ***if and only if D is properly h-homomorphic onto T.***

Proof. Suppose that $\boldsymbol{D}$ is h-homomorphic onto $\boldsymbol{T}$ under g.

$$\boldsymbol{D} = \bigcup_{\alpha \in T} D_{\alpha}, \quad D_{\alpha}g = \boldsymbol{\alpha}.$$

Let S be a set with $|S| = |D_{\alpha}|$ for all $\boldsymbol{\alpha} \in \boldsymbol{T}$, and let f_{α} be a bijection of D_{α} to S. Fixing $\{ f_{\alpha}$; a $\in \boldsymbol{T}\}$, for each $(\boldsymbol{\alpha}, \beta) \in \boldsymbol{T} \boldsymbol{X} \boldsymbol{T}$ we define a binary operation $\theta_{\alpha,\beta}$ on S as follows. Let x, y $\in$ S:

$$x\theta_{\alpha,\,\beta}y = [(xf_{\alpha}^{-1})(xf_{\beta}^{-1})]f_{\alpha\beta}.$$

Let $\boldsymbol{a}$ be any element of $\boldsymbol{D}$, hence $\boldsymbol{a} \in D_{\alpha}$ for some $\boldsymbol{a} \in \boldsymbol{T}$. We define a mapping ψ of $\boldsymbol{D}$ onto **SX** $\boldsymbol{T}$ as follows :

$$a \overset{\psi}{\rightarrow} (af_{\alpha}, \alpha).$$

Then ψ is an isomorphism of $\boldsymbol{D}$ onto $S \overline{\times}_{\Theta} T$. The proof of the converse **is** easy.

Even if $\boldsymbol{D}$, S, ***Tare*** given, Θ depends on the choice of $\{f_{\alpha}$; a $\in \boldsymbol{T}\}$. However, Θ is unique in some sense. To explain this situation we shall define a terminology.

Definition. Let gand g' be homomorphisms of semigroups $\boldsymbol{A}$ and B onto a semigroup C respectively. An isomorphism $\boldsymbol{h}$ of $\boldsymbol{A}$ into (onto) $\boldsymbol{B}$ is called a ***restricted isomorphism*** of $\boldsymbol{A}$ into (onto) $\boldsymbol{B}$ with respect to g and g' or we say $\boldsymbol{A}$ is ***restrictedly isomorphic*** into (onto) $\boldsymbol{B}$ with respect to g and g' if there is an automorphism $\boldsymbol{k}$ of C such that $\boldsymbol{h} \cdot g' = g \cdot \boldsymbol{k}$:

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "h"'] & C \arrow[d, "k"] \\ B \arrow[r, "g'"'] & C \end{tikzcd}$$

Dejinition. Let G(0) and $G'(\theta')$ be groupoids with binary operations θ, θ' respectively. If there are three bijections ***h,*** q, r of G(8) to $G'(\theta')$ such that

$$(x\theta y)r = (xh)\theta'(yq) \text{ for all } x, \text{y} \in \text{G } (\theta),$$

then we say that ***G(8)*** is ***isotopic*** to $G'(\theta')$. If it is necessary to specify ***h, q, r, we*** say ***G(8)*** is ***(h,*** *q, r)-isotopic* to $G'(\theta')$. We denote it by

$$G(\theta) \underset{(h,q,r)}{\approx} G'(\theta') \text{ or } \text{G}(8) \approx G'(\theta').$$

Theorem 2.2. Let S and T be a fixed set and a semigroup respectively. Let $(\alpha,\beta)\Theta = \theta_{\alpha,\beta}$, $(\alpha,\beta)\Theta' = \theta'_{\alpha,\beta}$, ***a,*** $\beta \in$ ***T.*** $S\overline{\times}_\Theta T$ ***is restrictedly isomorphic onto*** $S\overline{\times}_{\Theta'} T$ ***with respect to the projections of*** $S\overline{\times}\ _\Theta T$ ***and*** $S\overline{\times}_{\Theta'}T$ ***to T if and only*** *if* ***there is an automorphism a*** $\to \alpha'$ ***of T and a system*** $\{f_\alpha;$ ***a*** $\in T\}$ ***of permutations of S such that a groupoid*** $S(\theta_{\alpha,\beta})$ ***is*** $(f_\alpha, f_\beta, f_{\alpha\beta})$*-isotopic to* $S(\theta'_{\alpha',\beta'})$ ***for all*** $\alpha, \beta \in T$.

Let ϱ and σ be relations on a semigroup ***D.*** As usual the product $\varrho\cdot\sigma$ of ϱ and σ is defined by

$$\varrho\cdot\sigma = \{(x, y);\ (x, z) \in \varrho,\quad (\text{z, y}) \in \sigma \text{ for some } \text{z} \in \boldsymbol{D}\}.$$

Let $\omega = D\times D$, $\iota = \{(x, x);\ x \in D\}$.

Theorem ***2.3. A semigroup D is gp-decomposable if and only*** *if* ***there is a congruence*** ϱ ***on D and an equivalence*** σ ***on D such that***

$$\varrho\cdot\sigma = \omega, \tag{2.6}$$

$$\varrho \cap \sigma = \iota, \tag{2.7}$$

in which (2.6) can be replaced by

$$\sigma\cdot\varrho = \omega. \tag{2.6'}$$

Then D $\cong (D/\sigma)\overline{\times}(D/\varrho)$ ***where*** D/ϱ ***is the factor semigroup of D*** *modulo* ϱ ***and*** D/σ ***is the factor set of D*** *modulo* σ.

We know many examples of general products: Direct product, semidirect product [3], **[6]**, group extension [3], Rees' regular representation of completely simple semigroups **[1]**, the representation of commutative archimedean cancellative semigroups without idempotent **[11]**, Q-semigroups **[15]**, and so on.

2.4. Left general product. As a special case of a general product, we make the

Definition. A general product $S\overline{\times}_\Theta T$ is called a ***left general product*** of S by ***T*** if and only if

$$(\alpha, \beta)\Theta = (\alpha, \gamma)\Theta \quad \text{for all} \quad \text{a}, \beta, \gamma \in \boldsymbol{T}. \tag{2.8}$$

$S\overline{\times}_\Theta T$ is called a ***right general product*** of S by ***T*** if and only if

$$(\alpha, \beta)\Theta = (\gamma, \beta)\Theta \quad \text{for all} \quad \alpha, \beta, \gamma \in \boldsymbol{T}. \tag{2.8'}$$

In case (2.8), $\theta_{\alpha,\,\beta}$ depends on only a, so $\theta_{\alpha,\,\beta}$ is denoted by $\theta_{\alpha\cdot}$. Then (2.4) is rewritten :

$$\theta_{\alpha\cdot} \;{}_{a}\!\ast\; \theta_{\alpha\beta\cdot} = \theta_{\alpha\cdot} \;\ast_{a}\; \theta_{\beta\cdot} \quad \text{for all a, } \beta \in \boldsymbol{T}\text{, all } \boldsymbol{a} \in \boldsymbol{S} \qquad \textbf{\textit{(2.9)}}$$

In case (2.8′), $\theta_{\alpha,\,\beta}$ is independent of α, and $\theta_{\alpha,\,\beta}$ is denoted by $\theta_{\cdot\beta}$ and (2.4) is

$$\theta_{\cdot\alpha} \;{}_{a}\!\ast\; \theta_{\cdot\beta} = \theta_{\cdot\alpha\beta} \;\ast\;{}_{a}\; \theta_{\cdot\beta} \quad \text{for all } \boldsymbol{a}, \beta \in \boldsymbol{T}\text{, all } \boldsymbol{a} \in \boldsymbol{S} \qquad \textbf{\textit{(2.9')}}$$

A left congruence is a left compatible equivalence, namely an equivalence σ satisfying

$$x\,\sigma\,y \Rightarrow zx\,\sigma\,zy \quad \text{for all z.}$$

THEOREM ***2.4. Let D be a semigroup. D is isomorphic onto a left general product of a set S by a semigroup T if and only if there is a congruence ϱ on D and a left congruence σ on D such that***

$$D/\varrho \cong T, \qquad D/\sigma = \boldsymbol{S} \,|$$

and

$$\varrho\cdot\sigma = \omega \ (\textbf{\textit{equivalently}}\ \ \sigma\cdot\varrho = \omega),$$

$$\varrho \cap \sigma = \iota.$$

EXAMPLE. Let $\boldsymbol{T}$ be a semigroup, $\boldsymbol{F}$ a set, and let x denote a mapping of $\boldsymbol{F}$ into $\boldsymbol{T}$:

$$\lambda x = \alpha_{\lambda} \text{ where } \lambda \in F,\ \alpha_{\lambda} \in \boldsymbol{T}.$$

The set of all mappings x of $\boldsymbol{F}$ into $\boldsymbol{T}$ is denoted by S. For $\beta \in \boldsymbol{T}$ and x $\in$ S we define an element $\beta\cdot x$ as follows:

$$\lambda x = \alpha_{\lambda} \Rightarrow \lambda(\beta\cdot x) = \beta\alpha_{\lambda}.$$

Then

$$(\beta\gamma)\cdot x = \beta\cdot(\gamma\cdot x).$$

A binary operation is defined on G = SX $\boldsymbol{T}$ as follows:

$$(x, \alpha)(y, \beta) = (\alpha\cdot y, \alpha\beta). \qquad (2.10)$$

Then G is a semigroup with respect to (2.10) and it is a left general product of S by $\boldsymbol{T}$. Further the semigroup G with (2.10) is completely determined by a semigroup $\boldsymbol{T}$ and a cardinal number $\boldsymbol{m} = |F|$, and G is denoted by

$$\mathrm{G} = \mathfrak{S}\mathfrak{D}_m(T).$$

We can describe the structure of $\mathfrak{B}_E({}_a\ast)$ in terms of the semigroup of this kind.

THEOREM ***2.5. Let $m = |E| - 1$ and Se be the full transformation semigroup over E*** (*cf.* [1]). ***$\mathfrak{B}_E({}_a\ast)$ is isomorphic onto $\mathfrak{S}\mathfrak{D}_m(\mathfrak{T}_E)$.***

2.5. Sub-generalproduct. In § 2.3 we found that the two concepts, h-homomorphism and general product, are equivalent. What relationship does there exist between general products and homomorphisms?

Let U be a subset of $S\overline{\times}T$, and define

$$P_{rj_T}(U) = \{\alpha \in T;\ (x, \alpha) \in U\}.$$

Dejinition. If U is a subsemigroup of $S\overline{\times}_{\Theta}T$ and if $p_{rj_T}(U) = T$, then U is called a ***sub-general product*** of $S\overline{\times}_{\Theta}T$.

In the following theorem, the latter statement makes the theorem have sense.

THEOREM 2.6. ***If a semigroup D is homomorphic onto a semigroup T under a mapping g, then D is restrictedly isomorphic into*** $S\overline{\times}_{\Theta}T$ ***with respect to g and the projection of*** $S\overline{\times}_{\Theta}T$ ***to Tfor some*** S. ***Furthermore there exists an*** S_0 ***among the above S such that*** S_0 ***is either the minimum of*** $S|$ ***or possibly the minimum plus one.***

Proof. Let $\boldsymbol{D} = \bigcup_{\alpha\in T} \boldsymbol{D}$,, $D_\alpha g =$ a, Clearly $D_\alpha| \leqslant |\boldsymbol{D}$ for all a $\in \boldsymbol{T}$. The set $\{|D_\alpha|;\ \boldsymbol{a} \in \boldsymbol{T}\}$ has a least upper bound. (For this the well-ordered principle is used.) Let

$$\boldsymbol{m} = 1 + \text{l.u.b. } \{|D_\alpha|;\quad \boldsymbol{a} \in \boldsymbol{T}\}$$

and take a system of sets S_α of symbols such that

$$|S_\alpha| = \boldsymbol{m} \quad \text{for all} \quad \boldsymbol{a} \in \boldsymbol{T}$$

and a set S_0 with $|S_0 = \boldsymbol{m}$. Further we assume that $D_\alpha \subseteq S_\alpha$ and S_α contains a special symbol 0,,

$$0_\alpha \notin D_\alpha,$$

and S_0 contains a special symbol 0. Now let f_α be a bijection of S to S_α such that

$$\boldsymbol{Of, = 0,.}$$

We define a binary operation on G = **SX** $\boldsymbol{T}$ as follows:

$$(x, \alpha)(y, \beta) = \begin{cases} ((xf_\alpha \cdot yf_\beta)f_{\alpha\beta}^{-1}, \alpha\beta) & xf_\alpha \in D_\alpha,\ yf_\beta \in D_\beta \\ (0, \alpha\beta) & \text{otherwise.} \end{cases}$$

Then we can prove that G $= S\overline{\times}_{\Theta}T$ where

$$x\theta_{\alpha,\beta}y = \begin{cases} ((xf_\alpha)(yf_\beta))f_{\alpha\beta}^{-1}, & xf_\alpha \in D_\beta,\ yf_\beta \in D_\beta \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

Let $\boldsymbol{D'} = \{$(x, ***a);*** $xf_\alpha \in D_\alpha$, **a** $\in T\}$. Then P_{rj_T} ***(D')*** $=$ ***T*** and ***D'*** $\cong$ ***D*** under $(x, \alpha) \to xf_\alpha$, $\alpha \in T$.

2.6. Construction of some general products. As a simplest interesting example of general product, we will construct all general left products of a set S by a right zero semigroup ***T.***

Let $T = \{\alpha, \beta\}$,

$$\begin{array}{ccc} & \alpha & \beta \\ \boldsymbol{a} & \mathbf{r} & \beta \\ \beta & \alpha & \beta \end{array}$$

The equations (2.9) are

$$\left.\begin{aligned} \theta_{\alpha\cdot}\ {}_a{*}\ \theta_{\beta\cdot} &= \theta_{\alpha\cdot}\ {*}_a\ \theta_{\beta\cdot} \\ \theta_{\beta\cdot}\ {}_a{*}\ \theta_{\alpha\cdot} &= \theta_{\beta\cdot}\ {*}_a\ \theta_{\alpha\cdot} \\ \theta_{\alpha\cdot}\ {}_a{*}\ \theta_{\alpha\cdot} &= \theta_{\alpha\cdot}\ {*}_a\ \theta_{\alpha\cdot} \\ \theta_{\beta\cdot}\ {}_a{*}\ \theta_{\beta\cdot} &= \theta_{\beta\cdot}\ {*}_a\ \theta_{\beta\cdot} \end{aligned}\right| \qquad (2.11)$$

$\theta_{\alpha\cdot}$ and $\theta_{\beta\cdot}$ are semigroup operations. In order to construct all left general products $G = S\overline{\times}_\Theta T$ *we* may find all ordered pairs of semigroup operations on S:

$$(\theta_{\alpha\cdot}, \theta_{\beta\cdot})$$

which corresponds to

$$G = G_\alpha(\theta_{\alpha\cdot}) \cup G_\beta(\theta_{\beta\cdot}), \qquad G_\alpha | = | G_\beta |.$$

For fixed ***T*** and S, G is denoted by $G(\theta_{\alpha\cdot}, \theta_{\beta\cdot})$. Clearly

$$G(\theta_{\alpha\cdot}, \theta_{\beta\cdot}) \cong G(\theta_{\beta\cdot}, \theta_{\alpha\cdot}).$$

Instead of ordered pairs it is sufficient to find pairs $(\theta_{\alpha\cdot}, \theta_{\beta\cdot})$ regardless of order.

Let $\mathfrak{S}_S$ denote the set of all semigroup operations defined on S. ($\mathfrak{S}_S$ contains isomorphic ones.) We define a relation $\sim$ on $\mathfrak{S}_S$ as follows:

$\theta \sim \eta$ if and only if $\theta\ {}_a{*}\eta = \theta {*}_a \eta$ and $\eta\ {}_a{*}\theta = \eta\ {*}_a \theta$ for all $a \in S$.

The relation $\sim$ is reflexive symmetric.

Let φ_x^θ, ψ_x^θ be transformations of S defined by

$$z\varphi_x^\theta = z\theta x, \quad z\psi_x^\theta = x\theta z$$

respectively. Then

$$\theta\ {}_a{*}\eta = \theta {*}_a\ \eta \text{ for all } a \in S, \text{ if and only if}$$
$$\psi_x^\theta\varphi_y^\eta = \varphi_y^\eta\psi_x^\theta \text{ for all } x, y \in S.$$

As special cases we will determine the relation $\sim$ on $\mathfrak{S}_S$ in the case $|S| \leqq 3$.

*I. Left **generalproduct** of **S**, $|S|$ **= 2, by right zero semigroup T.***

Let S = *{a, b}*. $\begin{array}{|cc|} x & y \\ z & u \end{array}$, x, y, z, u = a or *b*, is the table $\begin{array}{c|cc} & a & b \\ \hline a & x & y \\ b & z & u \end{array}$

Explanation of the notations which will be used later: For example

4 denotes the semigroup $\left|\begin{array}{cc} a & b \\ b & a \end{array}\right|$, i.e. $40 = 4$

4_1 denotes $\left|\begin{array}{cc} b & a \\ a & b \end{array}\right|$ which is the isomorphic image of 4 under 1 $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$.

TABLE **5. *Semigroups of Order 2***

	$0\begin{pmatrix} a & b \\ a & b \end{pmatrix}$	$1\begin{pmatrix} a & b \\ b & a \end{pmatrix}$
1	$\boxed{\begin{matrix} a & b \\ a & b \end{matrix}}$	0
2	$\boxed{\begin{matrix} a & a \\ a & a \end{matrix}}$	$\boxed{\begin{matrix} b & b \\ b & b \end{matrix}}$
3	$\boxed{\begin{matrix} a & a \\ a & b \end{matrix}}$	$\boxed{\begin{matrix} a & b \\ b & b \end{matrix}}$
4	$\boxed{\begin{matrix} a & b \\ b & a \end{matrix}}$	$\boxed{\begin{matrix} b & a \\ a & b \end{matrix}}$

11 is exactly the same as 1, i.e. $1_0 = 11$.

1' denotes $\boxed{\begin{matrix} a & a \\ b & b \end{matrix}}$, omitted from Table 5.

Table 6 shows all η such that $\theta_0 \sim \eta$. We may pick θ_0 from all non-isomorphic semigroups, but must select η from all semigroups. Generally the following holds :

$\theta \sim \eta$ implies $\theta\varphi \sim \eta\varphi$ for all permutations φ of S (see § 2.2), (2.12)

e $\sim \eta$ implies $\eta' \sim \theta'$. (2.13)

TABLE 6

$\theta_0 \sim \eta$

θ_0	η
1	1
1'	1'
2	2, 3
3	2, 3
4	4, 4,

From the table we also have

$$\theta_0 = 2_1, \quad \eta = 21, 31,$$
$$\theta_0 = 3_1, \quad \eta = 21, 31,$$
$$\theta_0 = 4_1, \quad \eta = 4, \ 41.$$

Table 7 shows all non-isomorphic left general products ***D*** of S, $|S| = 2$, by a right zero semigroup of order 2.

TABLE 7

θ_{α}.	θ_{β}.
1	1
1'	1'
2	2
2	3
3	3
4	4

As an application of the above results, we have

THEOREM 2.7. ***Let Sbeaset,*** $|S| = 2$, ***andTbe a right zerosemigroup of order n. A left general product D of*** S ***by T is isomorphic onto either the direct product of a semigroup*** S ***of order 2 and a right zero semigroup T of order n***

$$D \cong S \times T, \quad |S| = 2, \quad |T| = n$$

or the union of the two direct products

$$D = (S_1 \times T_1) \cup (S_2 \times T_2),$$

where T_1 ***and*** T_2 ***are right zero semigroups,*** $T_1| + T_2| = n$ ***and*** S_1 ***is a null semigroup of order 2 and*** S_2 ***is a semilattice of order 2.***

II. ***Left generalproduct of*** S, $|S| = 3$, ***by right zero semigroup.***

Let $\boldsymbol{T} = \{\alpha, \beta\}$, $\begin{array}{c|cc} & \alpha & \beta \\ \hline \alpha & \alpha & \beta \\ \beta & \alpha & \beta \end{array}$.

The method is the same as in case I, and we use the same notation. Let $\mathfrak{S}_3$ denote the set of all semigroups defined on S, $S| = 3$. Table 8 shows $\mathfrak{S}_3$ except the dual forms. Those were copied from **[8]**, **[10]**. Table 9 shows all η for given θ_0 such that $\theta_0 \sim \eta$.

This table shows, for example, that $2 = 20 = 21$, $2_2 = 2_3$, $2_4 = 2_5$.

In the following family $\mathfrak{T}$ of ten subsets of $\mathfrak{S}_3$, each set satisfies the property: Any two elements of each set are --equivalent, and each set is a maximal set with this property.

$$\mathfrak{T}\begin{cases} \{1\}, \{2, 3, 15\}, \{4, 5_2, 16\}, 6, 6_2, 6_4\}, \{7, 7_2, 1\ 1\}, \\ (7, 12_2\}, \{2, 8, 14', 14'_1\}, \{2, 9, 18\}, \{2, 10, 10_1\}, \{2, 13, 13_1\ 17\}. \end{cases}$$

Let $\mathfrak{T}'$ denote the family obtained from $\mathfrak{T}$ by replacing $(6, 6_2, 6_4,\}$ by $\{6\}$ and $(2, 10, 101)$ by $(2, 10\}$ and leaving the remaining sets unchanged.

TABLE 8. *All Semigroups of Order 3 up to Isomorphism and Dual-isomorphism*

	0 $\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$	1 $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$	2 $\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$	3 $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$	4 $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$	5 $\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$
1	a b c abc abc	0	0	0	0	0
2	a a a a a a aaa	0	b b b b b b b b b	2	c c c ccc ccc	4
3	a a a a a a a a b	a a a aca aaa	b b b b b b b b a	c b b b b b b b b	ccc c a c ccc	b c c c c c c c c
4	a b a b a b a b a	a a c a a c cca	b a a a b b a b b	b b c b b c c c b	c a a a c c a c c	c b c b c b c b c
5	a b b b a a b a a	a c c c a a caa	b a b a b a b a b	b c b c b c b c b	c c a cca a a c	c c b c c b b b c
6	a b c b c a c a b	0	c a b a b c b c a	2	b c a c a b a b c	4
7	a b a a b a a b a	a a c a a c a a c	a b b a b b a b b	b b c b b c b b c	a c c a c c a c c	c b c c b c c b c
8	a a a a b c a b c	0	a b c b b b a b c	2	a b c a b c c c c	4
9	a a a a b b a b b	a a a a c c acc	a b a b b b a b a	c b c b b b c b c	a a c a a c ccc	bbc bbc , ccc
10	a a a a b c a c b	a a a a c b a b c	a b c b b b c b a	cbu bbb abc	a b c b a c cce	b a c a b c cc

TABLE 8 *(continued)*

	$0\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix}$	$1\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix}$	$2\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}$	$3\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}$	$4\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix}$	$5\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}$
11	a b a a b b a b c	a a c a b c a c c	0	a b c b b c c b c	1	3
12	a b b a b b a b c	a c c a b c a c c	a b a a b a a b c	a b c c b c c b c	a a c a b c a a c	a b c b b c b b c
13	a a a a a a a a c	a a a a b a a a a	b b b bbbj b b c	a b b b b b b b b	c c c c b c c c c	a c c c c c c c c
14	a a a a a b a a c	a a a a b a a c a	bba b b b b b c	a b b b b b c b b	c a c c b c c c c	a c c b c c c c c
15	a a a a a b a b c	a a a a b c a c a	b b a b b b a b c	a b c b b b c b b	c a c a b c c c c	a b c b c c c c c
16	a b a b a b a b c	a a c a b c c c a	b a a a b b a b c	a b c b b c c c b	c a a a b c a c c	a b c b c b c b c
17	aaa uba a a c	0	a b b bbb’ b b c	2	a c c c b c c c c	4
18	a a a a b b a b c	a a a abc a c c	a b a b b b a b c	a b c b b b c b c	a a c abc ccc	a b c b b c c c c

We have the following theorem, in which we do not assume T is finite:

THEOREM 2.8. *A left general product D of S, $|S| = 3$, by a right zero semigroup T is determined by a mapping π of the set T into one of the sets belonging to $\mathfrak{T}'$ in such a way that $\theta_{\alpha}. = n(a)$, $\alpha \in T$. Every left general product D of S, $|S| = 3$, by T is isomorphic or anti-isomorphic onto one of those thus obtained. Accordingly D is the disjoint union of at most four*

distinct (but not necessarily isomorphically distinct) direct products, i.e.

$$\boldsymbol{D} = \bigcup_{i=1}^{m} (S(\theta_i)\times T_i),\ \boldsymbol{m} \leqslant \boldsymbol{4},$$

where $\boldsymbol{T} = \bigcup_{i=1}^{m} T_i, . T_i' s$ ***are right zero semigroups and either*** $\theta_i = \pi(T_i)$ ***(i***$=$ 1, ... $\boldsymbol{m}$***) or*** $\theta'_i = \pi(T_i)$ ***(i = 1, . . ., m).***

III. ***Right generalproduct of*** S ***by right zero semigroup.***

First let $\boldsymbol{T} = \{\boldsymbol{a}, \ \beta\}$, $\begin{array}{ccc} & \alpha & \beta \\ \alpha & \boldsymbol{a} & \beta \\ \beta & \alpha & \beta \end{array}$.

The equations (2.9') are

$$\left.\begin{array}{l} e_{\cdot\alpha}\ {}_a{*}\ \theta_{\cdot\beta} = \theta_{\cdot\beta}\ {*}_a\ \theta_{\cdot\beta} \\ \theta_{\cdot\beta}\ {}_a{*}\ \theta_{\cdot\alpha} = \theta_{\cdot\alpha}\ {*}_a\ \theta_{\cdot\alpha} \\ \theta_{\cdot\alpha}\ {}_a{*}\ \theta_{\cdot\alpha} = \theta_{\cdot\alpha}\ {*}_a\ \theta_{\cdot\alpha} \\ \theta_{\cdot\beta}\ {}_a{*}\ \theta_{\cdot\beta} = \theta_{\cdot\beta}\ {*}_a\ \theta_{\cdot\beta} \end{array}\right\} \qquad (2.14)$$

A relation $\approx$ is defined on $\mathfrak{S}_S$ as follows:

$\theta \approx \eta$ if and only if

$$\begin{array}{l} \theta\ {}_a{*}\ \eta = \eta\ {*}_a\ \eta \\ \eta\ {}_a{*}\ \theta = \theta\ {*}_a\ \theta \end{array} \qquad \text{for all } \boldsymbol{a} \in \mathbf{S}$$

Recall that

$$z\varphi^{\theta}_x = z\theta x,\ z\psi^{\theta}_x = x\theta z.$$

Using these notations,

$\theta\ {}_a{*}\ \eta = \eta\ {*}_a\ \eta$ for all $a \in S$ if and only if $\psi^{n}_{x\theta y} = \psi^{\eta}_{y}\psi^{\eta}_{x}$ for all $x, y \in S$.

Therefore $x \to \psi^{\eta}_x$ is an anti-homomorphism of a semigroup $S(\theta)$ into the left regular representation of a semigroup $S(\eta)$.

We have obtained all non-isomorphic right general products of S, $|S| \leqslant 3$, by a right zero semigroup of order 2. The results will be published elsewhere.

IV. ***General product of*** S by ***a right zero semigroup T of order 2.***

Let $T = \{\alpha, \beta\}$, $\begin{array}{ccc} & \alpha & \beta \\ \boldsymbol{a} & \alpha & \beta \\ \beta & \alpha & \beta \end{array}$.

TABLE 9†

$\theta_0 \sim \eta$

θ_0	η
1	1
2	2, 3, 3_1, 8, 8′, 9, 9_1, 10, 10_1, 13, 13_1, 14, 14_1, 14′, $14'_1$, 15, 15,. 17, 18, 18,
3	2, 3, 15
4	4, 5_2, 16
5	4_2, 5, 16_2
6	6, 6_2, 6_4
7	7, 7_2, 11, 12_2
8	2, 8, 14′. 14;
9	2, 9, 18
10	2, 10, 10,
11	7, 7_2, 11
12	7_2, 12
13	2, 13, 13_1, 17
14	2, 8′, 14, 14,
15	2, 3, 15
16	4, 5_2, 16
17	2, 13, 13_1, 17
18	2, 9, 18

† These were computed by P. Dubois, J. Youngs, T. Okamoto, R. Kaneiwa, and A. Ohta under the author's direction.

To find $(\theta_{\alpha,\alpha}, \theta_{\alpha,\beta}, \theta_{\beta,\alpha}, \theta_{\beta,\beta})$ we may solve the following equations:

$$\left.\begin{array}{ll}
\theta_{\alpha,\alpha}\ {}_a\!\ast\ \theta_{\alpha,\beta} = \theta_{\alpha,\beta} \ast_a \theta_{\alpha,\beta}, & \theta_{\beta,\beta}\ {}_a\!\ast\ \theta_{\beta,\alpha} = \theta_{\beta,\alpha} \ast_a \theta_{\beta,\alpha}, \\
\theta_{\alpha,\beta}\ {}_a\!\ast\ \theta_{\beta,\alpha} = \theta_{\alpha,\alpha} \ast_a \theta_{\beta,\alpha}, & \theta_{\beta,\alpha}\ {}_a\!\ast\ \theta_{\alpha,\beta} = \theta_{\beta,\beta} \ast_a \theta_{\alpha,\beta}, \\
\theta_{\alpha,\beta}\ {}_a\!\ast\ \theta_{\beta,\beta} = \theta_{\alpha,\beta} \ast_a \theta_{\beta,\beta}, & \theta_{\beta,\alpha}\ {}_a\!\ast\ \theta_{\alpha,\alpha} = \theta_{\beta,\alpha} \ast_a \theta_{\alpha,\alpha}, \\
\theta_{\alpha,\alpha}\ {}_a\!\ast\ \theta_{\alpha,\alpha} = \theta_{\alpha,\alpha} \ast_a \theta_{\alpha,\alpha}, & \theta_{\beta,\beta}\ {}_a\!\ast\ \theta_{\beta,\beta} = \theta_{\beta,\beta} \ast_a \theta_{\beta,\beta}.
\end{array}\right\} \quad (2.15)$$

These are equivalent to:

$$\left.\begin{array}{ll}
\psi_x^{\alpha,\alpha}\varphi_y^{\alpha,\beta}=\varphi_y^{\alpha,\beta}\psi_x^{\alpha,\beta}, & \psi_x^{\beta,\beta}\varphi_y^{\beta,\alpha}=\varphi_y^{\beta,\alpha}\psi_x^{\beta,\alpha} \\
\psi_x^{\alpha,\beta}\varphi_y^{\beta,\alpha}=\varphi_y^{\beta,\alpha}\psi_x^{\alpha,\alpha}, & \psi_x^{\beta,\alpha}\varphi_y^{\alpha,\beta}=\varphi_y^{\alpha,\beta}\psi_x^{\beta,\beta} \\
\psi_x^{\alpha,\beta}\varphi_y^{\beta,\beta}=\varphi_y^{\beta,\beta}\psi_x^{\alpha,\beta}, & \psi_x^{\beta,\alpha}\varphi_y^{\alpha,\alpha}=\varphi_y^{\alpha,\alpha}\psi_x^{\beta,\alpha} \\
\theta_{\alpha,\alpha} \text{ and } \theta_{\beta,\beta} \text{ are semigroups.} &
\end{array}\right\} \tag{2.16}$$

The author and R. Dickinson have computed all non-isomorphic general products of S, $|S| \leqslant 3$, by a right zero semigroup of order 2 using a CDC 6600. The results will be published elsewhere.

Acknowledgements. The author is grateful to the following people for their assistance in the computation by hand or by machine:

Mr. Richard Biggs for Part I,

Mr. Robert Dickinson, Professor Morio Sasaki and his students for Part II.

The author also wishes to thank the Editor, Mr. John Leech, for his thoughtful elaboration of the manuscript.

REFERENCES

1. A. H. CLIFFORD and G. B. PRESTON: *The Algebraic Theory of Semigroups, vol.* 1, Amer. Math. Soc. Survey 7 (Providence, 1961).
2. G. E. FORSYTHE: SWAC computes 126 distinct semigroups of order 4. *Proc. Amer. Math. Soc.* ***6*** (1955), 443-445.
3. M. HALL: *The Theory of Groups* (Macmillan Co., New York, 1959).
4. T. S. MOTZKIN and J. L. SELFRIDGE: Semigroups of order five. (Presented in Amer. Math. Soc. Los Angeles Meeting on November 12,1955).
5. R. J. PLEMMONS: Cayley tables for all semigroups of order $\leqslant$ 6. (Distributed by Department of Mathematics, Auburn University, Alabama 1965.)
6. E. SHENKMAN: *Group Theory* (Van Nostrand, Princeton, 1965).
7. T. TAMURA: On the system of semigroup operations defined in a set. *J. Gakugei, Tokushima Univ. 2 (1952),* 1-18.
8. T. TAMURA: Some remarks on semigroups and all types of semigroups of order 2,3. *J. Gakugei, Tokushima Univ.* ***3*** (1953), 1-11.
9. T. TAMURA, Notes on finite semigroups and determination of semigroups of order 4. *J. Gakugei, Tokushima Univ.* ***5*** (1954), 17-27.
10. T. TAMURA *et al.:* All semigroups of order at most 5. *J. Gakugei, Tokushima Univ.* 6 (1955), 19-39.
11. T. TAMURA: Commutative nonpotent archimedean semigroup with cancellation law 1. *J. Gakugei, Tokushima Univ.* ***8*** (1957), 5-11.
12. T. TAMURA: Distributive multiplications to semigroup operations. *J. Gakugei, Tokushima Univ.* 8 (1957), 91-101.
13. T. TAMURA *et al.:* Semigroups of order < 10 whose greatest c-homomorphic images are groups. *J. Gakugei, Tokushima Univ.* 10 (1959), 43-64.
14. T. TAMURA: Semigroups of order 5, 6, 7, 8 whose greatest c-homomorphic images are unipotent semigroups with groups. *J. Gakugei, Tokushima Univ.* 11 (1960), 53-66.

15. T. TAMURA: Note on finite semigroups which satisfy certain grouplike condition. ***Proc. Jap. Acad.* *36*** (1960), 62-64.
16. T. TAMURA: Some special groupoids. ***Math. Jap.* *8*** (1963), 23-31.
17. T. TAMURA and R. DICKINSON: Semigroups connected with equivalence and congruence relations. ***Proc. Jap. Acad.* *42*** (1966), 688-692.
18. R. YOSHIDA: I-compositions of semigroups I. ***Memoirs of the Research Inst. of Sci. and Eng., Ritsumeikan Univ.*** 14 (1965), 1-12.
19. *R.* YOSHIDA: Z-compositions of semigroups II. ***Memoirs of the Research Inst. of Sci. and Eng., Ritsumeikan Univ.*** 15 (1966), 1-5.
20. T. TAMURA: Note on automorphism group of groupoids. ***Proc. Jap. Acad.* *43*** (1967), 843-846.

Simple Word Problems in Universal Algebras'

DONALD E. KNUTH and PETER B. BENDIX

Summary. An algorithm is described which is capable of solving certain word problems: i.e. of deciding whether or not two words composed of variables and operators can be proved equal as a consequence of a given set of identities satisfied by the operators. Although the general word problem is well known to be unsolvable, this algorithm provides results in many interesting cases. For example in elementary group theory if we are given the binary operator . , the unary operator -, and the nullary operator e, the algorithm is capable of deducing from the three identities $a\cdot(b\cdot c) =$ (a.b).c, $a\cdot a^{-} =$ e, $a\cdot e =$ a, the laws $a^{-}\cdot a =$ e, e.a = a, a- = a, etc.; and furthermore it can show that $a\cdot b = b\cdot a^{-}$ is not a consequence of the given axioms.

The method is based on a well-ordering of the set of all words, such that each identity can be construed as a "reduction", in the sense that the right-hand side of the identity represents a word smaller in the ordering than the left-hand side. A set of reduction identities is said to be "complete" when two words are equal as a consequence of the identities if and only if they reduce to the same word by a series of reductions. The method used in this algorithm is essentially to test whether a given set of identities is complete; if it is not complete the algorithm in many cases finds a new consequence of the identities which can be added to the list. The process is repeated until either a complete set is achieved or until an anomalous situation occurs which cannot at present be handled.

Results of several computational experiments using the algorithm are given.

Introduction. The purpose of this paper is to examine a general technique for solving certain algebraic problems which are traditionally treated in an ***ad hoc*,** trial-and-error manner. The technique is precise enough that it can be done by computer, but it is also simple enough that it is useful for hand calculation as an aid to working with unfamiliar types of algebraic axioms.

Given a set of operators and some identities satisfied by these operators, the general problem treated here is to examine the consequences of the given identities, i.e. to determine which formulas are equal because of the identities. The general approach suggested here may be described in very informal terms as follows: Let us regard an identity of the form $\alpha = \beta$ as a "reduction," where we choose one side of the identity, say β, as being "simpler" than the other side **α,** and we agree to simplify any formula

† The work reported in this paper was supported in part by the U.S. Office of Naval Research.

having the form of α to the form of β. For example, the axiom $a^{-1}(ab) = \boldsymbol{b}$ can be considered as a reduction rule in which we are to replace any formula of the form $a^{-1}(ab)$ by $\boldsymbol{b}$. (The associative law for multiplication is not necessarily being assumed here.) It is demonstrated in this paper that the most fruitful way to obtain new consequences of reductions is to take pairs of reductions $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$ and to find a formula which has the form of α_1 and in which one of the subformulas corresponding to an operator of α_1 also has the form of α_2. If the latter subformula is replaced by β_2, and the resulting formula is equated to β_1, a useful new identity often results. For example, let $\mathrm{a}_1 = \alpha_2 = a^{-1}(ab)$, and let $\beta_1 = \beta_2 = b$; then the formula $(x^{-1})^{-1}$ $(x^{-1}(xy))$ has the form of α_1 while its subformula $(x^{-1}(xy))$ corresponding to the multiplication of $\boldsymbol{a}$ by $\boldsymbol{b}$ in α_1 has the form of α_2; so we can equate $(x^{-1})^{-1}$ (x-'(xy)) both to xy and to $(x^{-1})^{-1}y$.

The general procedure which has been described so vaguely in the preceding paragraph is formalized rigorously in §§ 1-6 of this paper. § 7 presents over a dozen examples of how the method has given successful results for many different axiom systems of interest. The success of this technique seems to indicate that it might be worth while teaching its general principles to students in introductory algebra courses.

The formal development in §§ 1-6 of this paper is primarily a precise statement of what hundreds of mathematicians have been doing for many decades, so no great claims of originality are intended for most of the concepts or methods used. However, the overall viewpoint of this paper appears to be novel, and so it seems desirable to present here a self-contained treatment of the underlying theory. The main new contribution of this paper is intended to be an extension of some methods used by Trevor Evans [4]; we allow operators to be of arbitrary degree, and we make use of a well-ordering of words which allows us to treat axioms such as the associative law. Furthermore some of the techniques and results of the examples in § 7 appear to be of independent interest.

1. **Words.** In the following sections we will deal with four fixed sequences of quantities :

(a) An infinite sequence of ***variables*** vi, v_2, v_3, . . . , which are distinguishable symbols from an infinite alphabet.

(b) A finite sequence of ***operators*** f_1, f_2, f_3, • . . , f_N, which are distinguishable symbols from some alphabet, disjoint from the variables.

(c) A finite sequence of ***degrees*** $d_1, d_2, d_3, \ldots$, d_N, which are nonnegative integers. We say d_j is the degree of operator f_j.

(d) A finite sequence of ***weights*** w_1, w_2, w_3, . . ., w_N, which are nonnegative integers. We say w_j is the weight of operator f_j.

An operator whose degree is 0, 1, 2, 3,. . . , will be called a nullary, unary, binary, ternary, . . . , operator, respectively. Nullary operators take the place in this discussion of what are traditionally called "constants" or "generators". We will assume there is at least one nullary operator.

Two special conditions are placed on the sequences defined above:

(1) ***Each nullary operator has positive weight.*** Thus if $d_j = 0$, $w_j > 0$.

(2) Each unary operator has positive weight, with the possible exception of f_N. Thus if $d_j = 1$ and j $< N$, $w_j > 0$.

The reason for these two restrictions will become clear in the proof of Theorem 1.

Certain sequences of variable and operator symbols are called ***words*** ("well-formed formulas"), which are defined inductively as follows : A variable v_j standing alone is a word; and

$$f_j\alpha_1 \ldots \text{ad} \tag{1.1}$$

is a word if $\alpha_1, \ldots, \alpha_d$ are words and $\boldsymbol{d} = d_j$. Note that if f_j is a nullary operator, the symbol f_j standing alone is a word.

The *subwords* of a word ***a*** are defined to be (i) the entire word ***a*** itself, and (ii) the subwords of al, . . . , α_d, if ***a*** has the form (1.1). Clearly the number of subwords of ***a*** is the number of symbols in a, and in fact each symbol of ***a*** is the initial symbol of a unique subword. Furthermore, assuming that ***a*** and β are words, β is a subword of ***a*** if and only if β is a substring of ***a***, i.e. a = $\varphi\beta\psi$ for some strings of symbols φ and ψ.

Let us say a ***nontrivial*** *subword* is a subword which contains at least one operator symbol; i.e. a subword which is not simply of the trivial form "v_j" for some variable v_j. The number of nontrivial subwords of a word a is clearly the number of operator symbols in ***a***.

This definition of words and subwords is, of course, just one of many ways to define what is essentially an "ordered tree structure", and we may make use of the well-known properties of tree structure.

Let us write $n(x, \boldsymbol{a})$ for the number of occurrences of the symbol x in the word ***a***. A ***pure word a*** is one containing no variables at all; i.e. a is pure if $n(v_j, \boldsymbol{a}) = 0$ for all ***j***. The ***weight*** of a pure word is

$$w(\alpha) = \sum_j w_j n(f_j, \alpha); \tag{1.2}$$

i.e. the sum of the weights of its individual symbols. Since every nullary operator has positive weight, every pure word has positive weight.

The set of all pure words can be ordered by the following relation: ***a*** $> \beta$ if and only if either

(1) $w(\alpha) > w(\beta)$; or

(2) $\boldsymbol{w(a)} = w(\beta)$ and $\boldsymbol{a} = f_j\alpha_1 \ldots \alpha_{d_j}$, $\beta = f_k\beta_1 \ldots \beta_{d_k}$, and either

(2a)j $>$ ***k***; or

(2b) $j = k$ and $\alpha_1 = \beta_1, \ldots . \alpha_{t-1} = \beta_{t-1}, \boldsymbol{a}_t > \beta_t$ for some t, $1 \leqslant t \leqslant d_j$.

It is not difficult to design an algorithm which decides whether or not $a > \beta$, given two pure words a and β; details will be omitted here.

THEOREM 1. *The set of all pure words is well-ordered by the relation* "$>$".

Proof. First it is necessary to prove that $a > \beta > \gamma$ implies $a > \gamma$; and that for any pure words a and β, exactly one of the three possibilities $a > \beta$, $a = \beta$, $a < \beta$ holds. These properties are readily verified by a somewhat tedious case analysis, so it is clear that we have at least a linear ordering.

We must now prove there is no infinite sequence of pure words with

$$\alpha_1 > \alpha_2 > \alpha_3 > \ldots . \tag{1.3}$$

Since the words are ordered first on weight, we need only show there is no infinite sequence (1.3) of pure words *having the same weight w.*

Now let a be a pure word with n_j symbols of degree d_j. It is easy to prove inductively that

$$n_0+n_1+n_2+\ldots = 1+0\cdot n_0+1\cdot n_1+2\cdot n_2+\ldots,$$

i.e. $n_0 = 1+n_2+2n_3+\ldots$. Since each nullary operator has positive weight, we have $w \geqslant n_0$; so there are only a finite number of choices for $n_0, n_2, n_3, \ldots$, if we are to have a word of weight w. Furthermore if each unary operator has positive weight, we have $w \geqslant n_1$, so there would be only finitely many pure words of weight w. Therefore (1.3) is impossible unless f_N is a unary operator of weight zero.

Therefore let $w_N = 0$, $d_N = 1$, and define the function $h(a)$ to be the word obtained from a by erasing all occurrences of f_N. Clearly if a is a word of weight w, so is $h(a)$. And by the argument in the preceding paragraph only finitely many words $h(\alpha)$ exist of weight w. To complete the proof of the theorem, we will show there is no infinite sequence (1.3) such that $h(\alpha_1) = h(\alpha_2) = h(\alpha_3) = \ldots$.

Let $h(a) = s_1 s_2 \ldots s_n$; then a has the form $f_N^{r_1} s_1 f_N^{r_2} s_2 \ldots f_N^{r_n} s_n$, where $r_1, \ldots, r_n$ are nonnegative integers. Define $r(a) = (r_1, \ldots, r_n)$, an n-tuple of nonnegative integers. It is now easy to verify that, if $h(\alpha) = h(\beta)$, *we* have $a > \beta$ if and only if $r(a) > r(\beta)$ in lexicographic order. Since it is well known that lexicographic order is a well-ordering, the proof of Theorem 1 is complete.

Note that if f_j were a unary operator of weight zero and $j < N$, we would not have a well-ordering, since there would be a sequence of pure words of the form $f_N\alpha > f_j f_N\alpha > f_j f_j f_N\alpha > \ldots$. And if we have nullary operators of weight zero, other counterexamples arise; for example if f_1 is nullary and f_2 is binary, both of weight zero, then

$$f_2f_2f_1f_1f_1 > f_2f_1f_2f_2f_1f_1f_1 > f_2f_1f_2f_1f_2f_2f_1f_1f_1 > \ldots .$$

This accounts for the restrictions we have imposed on the degrees and the weights.

2. Substitutions. Most of § 1 was concerned with pure words, and it is now time to consider the variables which can enter. If ***a*** is a string of symbols containing variables, we let ***v(a)*** be the largest subscript of any variable occurring in ***a***. If ***a*** involves no variables, we let $v(\alpha) = \boldsymbol{0}$.

If ***a***, $\theta_1, \theta_2, \ldots, \theta_n$ are strings of symbols, where n $\geqslant$ *v(a)*, we will write

$$S(\theta_1, \theta_2, \ldots, \theta_n; \alpha) \tag{2.1}$$

for the string obtained from a by substituting θ_j for each occurrence of v_j, $1 \leqslant j \leqslant n$. For example if *v(a)* = 2, $S(v_2, v_1;$ ***a)*** is obtained from ***a*** by interchanging the variables v_1 and v_2.

We say a word β ***has the form of*** a word ***a*** if β can be obtained by substitution from a; i.e. if there exist words $\theta_1, \theta_2, \ldots, \theta_n$ such that $\beta =$ $\mathsf{S} = (\theta_1, \theta_2, \ldots, \theta_n; \boldsymbol{a})$.

It is not difficult to prove that two substitutions can always be replaced by one, in the sense that

$$\begin{aligned} &S(\varphi_1, \ldots, \varphi_m; S(\theta_1, \ldots, \theta_n; \alpha)) \\ &\quad = S(S(\varphi_1, \ldots, \varphi_m; \theta_1), \ldots, S(\varphi_1, \ldots, \varphi_m; \theta_n); \alpha). \end{aligned} \tag{2.2}$$

So if γ has the form of β and β has the form of ***a***, γ also has the form of ***a***.

It is comparatively easy to design an algorithm which decides whether or not β has the form of ***a***, given two words β and a. Briefly, let ***a*** = $\lambda_1 \lambda_2 \ldots \lambda_m$, where each λ_j is a variable or an operator. Then β must have the form $\beta = \beta_1\beta_2 \ldots \beta_m$ where, if y_j is an operator, $y_j = \beta_j$; and if $y_j = y_k$ is a variable, then $\beta_j = \beta_k$ is a word, for 1 $\leqslant$ j $\leqslant$ ***k*** $\leqslant$ ***m.***

Let w_0 be the minimum weight of a pure word; thus w_0 is the minimum weight of a nullary operator. We define the weight ***w(a)*** of an arbitrary word to be the minimum weight of all pure words which have the form of ***a:***

$$w(\alpha) = w_0 \sum_{j \geqslant 1} n(v_j, \boldsymbol{a}) + \sum_{j \geqslant 1} w_j n(f_j, \boldsymbol{a}). \tag{2.3}$$

We now extend the "$>$" relation, which was defined only for pure words in § 1, to words involving variables. Let us say that ***a*** $> \beta$ if and only if either

(1) ***w(a)*** $> w(\beta)$ and $n(v_i,$ ***a)*** $\geqslant n(v_i, \beta)$ for all ***i*** $\geqslant 1$; or

(2) ***w(a)*** $= w(\beta)$ and $n(v_i,$ ***a)*** $= n(v_i, \beta)$ for all $i \geqslant 1$

and either ***a*** $= f_N^t v_k$, $\beta = v_k$ for some $t \geqslant 1$, or
$\alpha = f_j\alpha_1 \ldots \alpha_{d_j}$, $\beta = f_k\beta_1 \ldots \beta_{d_k}$ and either

(2a) j $>$ ***k;*** or

(2b) j = ***k*** and $\alpha_1 = \beta_1, \ldots, \alpha_{t-1} = \beta_{t-1}$, ***a***, $> \beta_t$ for some t, $1 \leqslant t \leqslant d_j$.

It is not difficult to design a relatively simple algorithm which determines, given words ***a*** and β, whether ***a*** $< \beta$, or a $= \beta$, or a $> \beta$, or whether ***a*** and β are unrelated. In the latter case we write "a $\#$ β". When a and β are' pure words, the situation ***a*** $\#$ β is impossible; but when variables are involved, we can have unrelated words such as

$$f_5v_1v_1v_1v_1v_2 \;\#\; f_3v_2v_2v_1, \tag{2.4}$$

$$f_2v_1v_2 \;\#\; f_2v_2v_1, \tag{2.5}$$

where $f_2, f_3,$ f_5 are operators of degrees 2, 3, 5 respectively.

The principal motivation for the given definition of a $> \beta$ is the following fact:

THEOREM 2. *If* $\alpha > \beta$ ***then*** $S(\theta_1, \theta_2, \ldots, \theta_n; \alpha) > S(\theta_1, \theta_2, \ldots, \theta_n; \beta)$, *for* ***all words*** $\theta_1, \ldots, \theta_n$.

Proof Let $\alpha' = S(\theta_1, \theta_2, \ldots, \theta_n; \alpha)$ and $\beta' = S(\theta_1, \theta_2, \ldots, \theta_n; \beta)$. If condition (1) holds for α and β, then it must hold also for a' and β'. For in the first place, every word has weight $\geqslant w_0$, so

$$\begin{aligned} w(\alpha') &= w(\alpha) + \sum_{j\geqslant 1} n(v_j, \alpha)\big(w(\theta_j) - w_0\big) \\ &> w(\beta) + \sum_{j\geqslant 1} n(v_j, \beta)\big(w(\theta_j) - w_0\big) = w(\beta'). \end{aligned}$$

Secondly, $n(v_i, \alpha') = \sum_{j\geqslant 1} n(v_j, \alpha)n(v_i, \theta_j) \geqslant \sum_{j\geqslant 1} n(v_j, \beta)n(v_i, \theta_j) = n(v_i, \beta')$.

If condition (2) holds for α and β, then similarly we find $w(\alpha') = w(\beta')$ and $n(v_i,$ a'$) = n(v_i, \beta')$ for all i, and $\alpha' = f_j\alpha'_1 \ldots \alpha'_{d_j}$, $\beta' = f_k\beta'_1 \ldots \beta'_{d_k}$ where $\alpha'_r = S(\theta_1, \ldots, \theta_n;$ a,) and $\beta'_r = S(\theta_1, \ldots, \theta_n; \beta_r)$ for all **r**. Hence either j > **k**, or an inductive argument based on the length of a will complete the proof.

Corollary. There is no infinite sequence of words such that a, $> \alpha_2 >$ $> \alpha_3 > \ldots$. For if there were such a sequence, we could substitute a nullary operator f for each variable v_j, $j \geqslant 1$; Theorem 2 implies that this would give an infinite descending sequence of pure words, contradicting Theorem 1.

It should be emphasized that Theorem 2 is a key result in the method which will be explained in detail in subsequent sections; and the fact that $\alpha \# \beta$ can occur for certain words a and β is a serious restriction on the present applicability of the method. The authors believe that further theory can be developed to lift these restrictions, but such research will have to be left for later investigations.

It may seem curious that $f_5\ v_1\ v_1v_1v_1v_2 \# f_3v_2v_2v_1$; surely $f_5v_1v_1v_1v_1v_2$ appears to be a much "bigger" word than $f_3v_2v_2v_1$. But if we substitute a short formula for v_1 and a long formula for v_2, we will find $f_3v_2v_2v_1$ is actually longer than $f_5v_1v_1v_1v_2$.

Theorem 2 is not quite "best possible"; there are words a and β for which $\alpha \# \beta$ yet $S(\theta_1, \theta_2, \ldots, \theta_n; \alpha) > S(\theta_1, \theta_2, \ldots, \theta_n; \beta)$ for all "pure" words $\theta_1, \ldots, \theta_n$. For example, consider

$$f_3v_1 \;\#\; f_2f_1 \tag{2.6}$$

where f_3 and f_2 are unary operators of weight one, and f_1 is a nullary operator of weight one. If we substitute for v_1 a pure word θ of weight 1, we have $f_3\theta \;\; > f_2 f_1$ by case (2a); but if we substitute for v_1 any word θ of weight greater than one, we get $f_3\theta > f_2 f_1$ by case (1). We could therefore have made the methods of this paper slightly more powerful if we had been able to define $f_3 v_1 \;\; > f_2 f_1$; but such an effort to make Theorem 2 "best possible" appears to lead to such a complicated definition of the relation $\alpha > \beta$ that the comparatively simple definition given here is preferable. So far in practice no situation such as (2.6) has occurred.

Let α and β be words with $v(\alpha) \leqslant \boldsymbol{n}$, $v(\beta) \leqslant \boldsymbol{n}$. In the following discussion we will be interested in the general solution of the equation

$$S(\theta_1, \ldots . \theta_n; \alpha) = S(\theta_1, \ldots, \theta_n; \beta) \tag{2.7}$$

in words $\theta_1, \ldots, \theta_n$. Such an equation can always be treated in a reasonably simple manner:

THEOREM ***3. Either (2.7) has no solution, or there is a number k, $0 \leqslant k \leqslant n$, and words $\sigma_1, \ldots, \sigma_n$ with $v(\sigma_j) \leqslant k$ for $1 \leqslant j \leqslant n$, where***

$$\{v_1, v_2, \ldots, v_k\} \subseteq \{\sigma_1, \ldots, \sigma_n\}, \tag{2.8}$$

such that all solutions of (2.7) have the form

$$\theta_j = S(\varphi_1, \ldots, \varphi_k; \sigma_j), \quad 1 \leqslant j \leqslant n. \tag{2.9}$$

Moreover, there is an algorithm which determines whether or not (2.7) is solvable, and which determines $\sigma_1, \ldots, \sigma_n$ when a solution exists.

(Note that this theorem provides the general solution of (2.7). The significance of relation (2.8) is that the simple words $v_1, v_2, \ldots, v_k$ are included among the o's, i.e. that some $\boldsymbol{k}$ of the θ's may be selected arbitrarily and the other $\boldsymbol{n}$-$\boldsymbol{k}$ θ's must have a specified relationship to these $\boldsymbol{k}$ "independent" variables. This result is equivalent to the "Unification Theorem" of J. A. Robinson [lo].)

Proof Theorem 3 can be proved by induction on n, and for fixed n by induction on the length of $\alpha\beta$, as follows.

Case 1. $\alpha = v_p$, $\beta = v_q$. If $\boldsymbol{p} = \boldsymbol{q}$, then obviously any words $\theta_1, \ldots, \theta_n$ will satisfy (2.7), so we may take $k = \boldsymbol{n}$, $\sigma_1 = v_1, \ldots, \sigma_n = v_n$. If $\boldsymbol{p} \neq \boldsymbol{q}$, the general solution is clearly obtained by taking $\boldsymbol{k} = \boldsymbol{n}\text{-}\ 1$,

$$\sigma_1 = v_1, \ldots, \sigma_{q-1} = v_{q-1}, \sigma_q = v_p, \quad \sigma_{q+1} = v_q, \ldots, \sigma_n = v_{n-1}.$$

Case 2. a = $f_p\alpha_1 \ldots \alpha_d$, $\beta = v_q$. Then if the variable v_q appears in α, the equation (2.7) has no solution since the length of $S(\theta_1, \ldots, \theta_n, \cdot\, \alpha)$ is greater than the length of $\theta_q = S(\theta_1, \ldots, \theta_n; \beta)$. On the other hand if v_q does not appear in α we clearly have $\boldsymbol{k} = \boldsymbol{n}\text{-}\ 1$, $\sigma_1 = v_1, \ldots, \sigma_{q-1} = v_{q-1}$, $\sigma_q = S(v_1, \ldots, v_{q-1}, v_{q-1}, \ldots, v_n; \text{a})$, $\sigma_{q+1} = v_q, \ldots, \sigma_n = v_{n-1}$ as the general solution.

Case 3. $\alpha = v_p$, $\beta = f_q\beta_1 \ldots \beta_d$. This is case 2 with α and β interchanged.

Case 4. ***a*** = $f_p\alpha_1 . . .\alpha_d, \beta = f_q\beta_1 . . . \beta_d$. Here there is no solution of (2.7) unless $p = q$, so we may assume $\boldsymbol{p} = q$ and $\boldsymbol{d} = d'$. ***Now (2.7)*** is equivalent to the system of $\boldsymbol{d}$ simultaneous equations

$$S(\theta_1, . . ., \theta_n; \alpha_j) \doteq S(\theta_1, . . ., \theta_n; \beta_j) \tag{2.10}$$

for $1 \leqslant j \leqslant \boldsymbol{d}$. If $\boldsymbol{d} = 0$, the general solution is of course to take $\boldsymbol{k = n}$, $\sigma_1 = v_1, . . ., \sigma_n = \boldsymbol{v}$,. Suppose we have obtained the general solution of the system (2.10) for $1 \leqslant j \leqslant \boldsymbol{r}$; where $0 \leqslant \boldsymbol{r} < \boldsymbol{d}$; ***we*** will show how to extend this to a solution of (2.10) for $1 \leqslant j \leqslant r + \boldsymbol{1}$: If (2.10), for $1 \leqslant j \leqslant \boldsymbol{r}$, has no solution, then (2.10) certainly has no solution for $1 \leqslant j \leqslant r + 1$. Otherwise let the general solution to (2.10), for $1 \leqslant j \leqslant \boldsymbol{r}$; be given by $\boldsymbol{k}, \sigma_1, . . ., \boldsymbol{a}$,. Now the general solution to (2.10) for $1 \leqslant j \leqslant r + 1$ is obtained by setting $\theta_j = S(\varphi_1, . . ., \varphi_k; \sigma_j), 1 \leqslant j \leqslant n$, and $S(\theta_1, . . ., \theta_n;$ a,+,) = $S(\theta_1, . . ., \theta_n; \beta_{r+1})$. By (2.2) this requires solving

$$S(\varphi_1, . . ., \varphi_k; S(\sigma_1, . . ., \sigma_n; \alpha_{r+1})) = \\ S(\varphi_1, . . ., \varphi_k; S(\sigma_1, . . ., \sigma_n; \beta_{r+1})). \tag{2.11}$$

The general solution of this equation can be obtained by induction, since either $k < n$ or $k = n$ and $\{\sigma_1, ... \sigma_n\} = \{v_1, ... v_n\}$ and $S(\sigma_1, ... \sigma_n; \alpha_{r+1})S(\sigma_1, . . ., \sigma_n; \beta_{r+1})$ is shorter than $\alpha\beta$. If (2.11) has the general solution $\boldsymbol{k'}, \sigma_1', . . ., \sigma_k'$, then (2.10) for $1 \leqslant j \leqslant \boldsymbol{r} + 1$ has the general solution k', $S(\sigma_1', . . ., \sigma_k'; \sigma_1), . . . S(\sigma_1', . . ., \sigma_k'; \sigma_n)$. The latter strings include $\{v_1, . . ., v_{k'}\}$ since $\{\sigma_1', . . ., \sigma_k'\} \supseteq \{v_1, . . ., v_{k'}\}$ and $\{\sigma_1, . . ., \sigma_n\} \supseteq \{v_1, . . ., v_k\}$. This inductive process ultimately allows us to solve (2.10) for $1 \leqslant j \leqslant d$, as required.

This completes the inductive proof that a general solution (2.8), (2.9) to the equation (2.7) can be obtained, and it is evident that the proof is equivalent to a recursive algorithm for obtaining the solution.

As an example of the process used in the proof of Theorem 3, let $n = 7$, $d_1 = 1$, $d_2 = 2$, and

$$\begin{aligned} \alpha &= f_2f_1f_2f_1v_4f_2v_3f_1f_2v_2v_2f_2v_1f_2v_3f_1v_1, \\ \beta &= f_2f_1f_2v_5f_2v_5v_6f_2v_7f_2f_1v_6f_1f_2v_5v_6. \end{aligned} \tag{2.12}$$

We wish to determine what formulas can be obtained by a common substitution in a and β, which is essentially saying we want to solve the equation $\alpha = \beta$ for $v_1, . . ., v_7$. This reduces, first, to solving the simultaneous equations

$$f\ 1\ \ f\ 1v_4\ 2v_3{}'4f{:}2v_2v_2 = f_1f_2v_5f_2v_5v_6, \tag{2.13}$$

$$f_2v_1f_2v_3f_1v_1 = f_2v_7f_2f_1v_6f_1f_2v_5v_6 \tag{2.14}$$

To solve (2.13), we first remove the common f_1 at the left, then solve the system $f_1v_4 = v_5$, $f_2v_3f_1f_2v_2v_2 = f_2v_5v_6$, etc., and we ultimately obtain the conditions

$$v_3 = v_5 = f_1v_4, \quad v_6 = f_1f_2v_2v_2. \tag{2.15}$$

Substituting these into (2.14) gives the equation

$$f_2v_1f_2f_1v_4f_1v_1 = f_2v_7f_2f_1f_1f_2v_2v_2f_1f_2f_1v_4f_1f_2v_2v_2,$$

and to make a long story short this equation in the variables v_1, v_2, v_4, v_7 ultimately implies that

$$v_4 = f_1f_2v_2v_2, \quad v_1 = v_7 = f_2f_1f_1f_2v_2v_2f_1f_2v_2v_2.$$

Finally, in connection with (2.15), we have found that every word obtainable by a common substitution of words into ***a*** and β is obtained by substituting some word for v_2 in

$$f_2f_1f_2f_1f_1f_2v_2v_2f_2f_1f_1f_2v_2v_2f_1f_2v_2v_2f_2f_2f_1f_1f_2v_2v_2f_1f_2v_2v_2$$
$$f_2f_1f_1f_2v_2v_2f_1f_2f_1f_1f_2v_2v_2f_1f_2v_2v_2.$$

Stating this in the more formal language of Theorem 3 and its proof, the general solution to (2.7), (2.12) is given by

$$k = 1, \quad \sigma_1 = \sigma_7 = f_2f_1f_1f_2v_1v_1f_1f_2v_1v_1\sigma_2 = v_1,$$
$$\sigma_3 = \sigma_5 = f_1f_1f_2v_1v_1, \quad \sigma_4 = \sigma_6 = f_1f_2v_1v_1.$$

3. The word problem. Given a set $\boldsymbol{R} = \{(\lambda_1, \varrho_1), \ldots, (\lambda_m, \varrho_m)\}$ of pairs of words, called "relations", we can define a corresponding equivalence relation (in fact, a congruence relation) between words in a natural manner, by regarding the relations as "axioms",

$$\lambda_k \equiv \varrho_k \; (\boldsymbol{R}), \quad 1 \leqslant \boldsymbol{k} \leqslant \boldsymbol{m}, \tag{3.1}$$

where the variables range over the set of all words. This " $\equiv$ " relation is to be extended to the smallest congruence relation containing (3.1).

For our purposes it is most convenient to define the congruence relations in the following more precise manner: Let β be a subword of α, so that ***a*** has the form $\varphi\beta\psi$ for some strings φ, ψ. Assume that there is a relation (λ, ϱ) in $\boldsymbol{R}$ such that β has the form of λ: $\beta = S(\theta_1, \ldots, \theta_n; \lambda)$ for some $\theta_1, \ldots. \theta_n$, where $n \geqslant v(\lambda)$, $v(\varrho)$. Let $\beta' = S(\theta_1, \ldots, \theta_n; \varrho)$, so that β and β' are obtained from λ and ϱ by means of the same substitutions. Let ***a'*** $= \varphi\beta'\gamma$ be the word a with its component β replaced by β'. Then we say ***a reduces to*** α' with respect to ***R***, and we write

$$\boldsymbol{a} \to \boldsymbol{a'} \; (\boldsymbol{R}). \tag{3.2}$$

Finally, we say that

$$\alpha \equiv \beta \, (R) \tag{3.3}$$

if there is a sequence of words $\alpha_0, \alpha_1, \ldots, \alpha_n$ for some $n \geqslant 0$ such that $\alpha = \alpha_0$, $\alpha_n = \beta$, and for $0 \leqslant j < n$ we have either $\alpha_j \to \alpha_{j+1}$ ***(R)*** or $\alpha_{j+1} \to \alpha_j$ ***(R)***. (Note: When the set ***R*** is understood from the context, the ***"(R)"*** may be omitted from notations (3.2) and (3.3).)

The ***wordproblem*** is the problem of deciding whether or not a $\equiv \beta$ ***(R),*** given two words a and β and a set of relations ***R***. Although the word problem is known to be quite difficult (indeed, unsolvable) in general, we present here a method for solving certain word problems which are general enough to be of wide interest.

The principal restriction is that we require all of the relations to be comparable in the sense of § 2: we require that

$$\lambda > \varrho \tag{3.4}$$

for each relation in ***R***. In such a case *we* say ***R*** is a set of ***reductions.*** It follows from Theorem 2 that

$$\boldsymbol{a} \to \chi' \text{ implies } \boldsymbol{a} > \boldsymbol{a'}. \tag{3.5}$$

4. **The completeness theorem.** Let ***R*** be a set of reductions. We say a word ***a*** is ***irreducible*** with respect to ***R*** if there is no ***a'*** such that ***a*** → ***a'***.

It is not difficult to design an algorithm which determines whether or not a given word is irreducible with respect to ***R***. If ***R*** = $\{(\lambda_1, \varrho_1), \ldots, (\lambda_m, \varrho_m)\}$, we must verify that no subword of ***a*** has the form of λ_1, or $\lambda_2, \ldots$, or λ_m.

If ***a*** is reducible with respect to ***R***, the algorithm just outlined can be extended so that it finds some ***a'*** for which a → ***a'***. Now the same procedure can be applied to α', and if it is reducible we can find a further word a", and so on. We have $\alpha \to \alpha' \to \alpha'' \to \ldots$; so by (3.5) and the corollary to Theorem 2, this process eventually terminates.

Thus, ***there is an algorithm which, given any word a and any set of reductions R, finds an irreducible word*** α_0 ***such that a*** $\equiv \alpha_0$, ***with respect to R.***

We have therefore shown that each word is equivalent to at least one irreducible word. It would be very pleasant if we could also show that each word is equivalent to ***at most*** one irreducible word; for then the algorithm above solves the word problem! Take any two words ***a*** and β, and use the given algorithm to find irreducible α_0 and β_0. If a $\equiv \beta$, then $\alpha_0 \equiv \beta_0$, so by hypothesis α_0 must be equal to β_0. If a $\not\equiv \beta$, then $\alpha_0 \not\equiv \beta_0$, so α_0 must be unequal to β_0. In effect, α_0 and β_0 are canonical representatives of the equivalence classes.

This pleasant state of affairs is of course not true for every set of reductions ***R***, but we will see that it is true for surprisingly many sets and therefore it is an important property worthy of a special name. Let us say ***R*** is a ***complete*** set of reductions if no two distinct irreducible words are equivalent, with respect to ***R***. We will show in the next section that there is an algorithm to determine whether or not a given set of reductions is complete. First we need to characterize the completeness condition in a more useful way.

Let "$\to^*$" denote the reflexive transitive completion of "$\to$", so that ***a*** $\to^* \beta$ means that there are words $\alpha_0, \alpha_1, \ldots$, ***a***$_n$ for some $n \geq 0$ such that ***a*** = α_0, $\alpha_j \to \alpha_{j+1}$ for $0 \leq j < n$, and $\alpha_n = \beta$.

Theorem 4. ***A set of reductions R is complete if and only if the following "lattice condition" is satisfied:***

If $\alpha \to \alpha'$ *and* $\alpha \to \alpha''$ ***there exists a word*** γ ***such that a'*** $\to^* \gamma$ ***and*** $\alpha'' \to^* \gamma$.

Proof. If x $\to$ $\mathbf{a'}$ and $\mathbf{a} \to \alpha''$, we can find irreducible words α'_0 and α''_0 such that $\alpha' \to^* \alpha'_0$ and $\alpha' \to^* \alpha''_0$. Since $\alpha'_0 \equiv \alpha''_0$, we may take $\gamma = \alpha'_0 = \alpha''_0$ if ***R*** is complete.

Conversely let us assume that the lattice condition holds; we will show that ***R*** is complete. First, we show that ***if a*** $\to^* \alpha_0$ ***and a*** $\to^* \alpha'_0$, *where* α_0 ***and*** α'_0 ***are irreducible, we must have*** $\alpha_0 = \alpha'_0$. For if not, the set of all x which violate this property has no infinite decreasing sequence so there must be a "smallest" $\mathbf{a}$ (with respect to the $>$ relation) such that $\mathbf{a} \to^* \alpha_0$, $\alpha \to^* \alpha'_0 \not\equiv \alpha_0$, where both α_0 and α'_0 are irreducible. Clearly $\mathbf{a}$ is not itself irreducible, since otherwise $\alpha_0 = x = \alpha'_0$. So we must have $\mathbf{a} \not\equiv \alpha_0, \mathbf{a} \not\equiv \alpha'_0$, and there must be elements α_1, α'_1 such that $\mathbf{a} \to \alpha_1 \to^* \alpha_0$, $\mathbf{a} \to \alpha'_1 \to^* \alpha'_0$. By the lattice condition there is a word γ such that $\alpha_1 \to^* \gamma$ and $\alpha'_1 \to {}^* \gamma$. Furthermore there is an irreducible word γ_0 such that $\gamma \to^* \gamma_0$. Now by (3.5), $\mathbf{a} >$ al, so (by the way we chose a) we must have $\alpha_0 = \gamma_0$. Similarly the fact that $\mathbf{a} > \alpha'_1$ implies that $\alpha'_0 = \gamma_0$. This contradicts the assumption that $\alpha_0 \not\equiv \alpha'_0$.

Now to show that ***R*** is complete, we will prove the following fact: *If* $\alpha \equiv \beta, \alpha \to^* \alpha_0$, *and* $\beta \to^* \beta_0$, ***where*** α_0 ***and*** β_0 ***are irreducible, then*** $\alpha_0 = \beta_0$. Let the derivation of the relation $\mathbf{a} \equiv \beta$ be $\mathbf{a} = \sigma_0 \leftrightarrow \sigma_1 \leftrightarrow \ldots \leftrightarrow \sigma_n = \beta$, where "$\leftrightarrow$" denotes "$\to$" or "$\leftarrow$". If $n = 0$, ***we*** have $\mathbf{a} = \beta$, hence $\alpha_0 = \beta_0$ by the proof in the preceding paragraph. If $n = 1$, we have either a $\to \beta$ or $\beta \to \alpha$, and again the result holds by the preceding paragraph. Finally if $\boldsymbol{n} > 1$, let $\sigma_1 \to^* \sigma'_1$, where σ'_1 is irreducible. By induction on ***n, we*** have $\sigma'_1 = \beta_0$, and also $\sigma'_1 = \alpha_0$. Therefore ***R*** and the proof are both complete.

5. The superposition process. Our immediate goal, in view of Theorem 4, is to design an algorithm which is capable of testing whether or not the "lattice condition" is satisfied for all words.

En terms of the definitions already given, the hypothesis that a $\to$ $\mathbf{a'}$ and $\mathbf{a} \to \alpha''$ has the following detailed meaning: There are subwords β_1 and β_2 of a, so that α has the form

$$\mathbf{a} = \varphi_1\beta_1\psi_1 = \varphi_2\beta_2\psi_2. \tag{5.1}$$

There are also relations (λ_1, ϱ_1), $(1.2, \varrho_2)$ in ***R,*** and words $\theta_1, \ldots, \theta_m$, $\sigma_1, \ldots, \sigma_n$ such that

$$\beta_1 = S(\theta_1, \ldots, \theta_m; \lambda_1), \quad \beta_2 = S(\sigma_1, \ldots, \sigma_n; 3.2) \tag{5.2}$$

and

$$\mathbf{a'} = \varphi_1 S(\theta_1, \ldots. \theta_m; \varrho_1)\psi_1, \quad \text{a"} = \varphi_2 S(\sigma_1, \ldots. \sigma_n; \varrho_2)\psi_2. \tag{5.3}$$

The lattice condition will hold if we can find a word γ such that $\mathbf{a'} \to^* \gamma$ and $\mathbf{a''} \to^* \gamma$.

Several possibilities arise, depending on the relative positions of β_1 and β_2 in (5.1). If β_1 and β_2 are disjoint (have no common symbols), then assuming φ_1 is shorter than φ_2 we have $\varphi_2 = \varphi_1\beta_1\varphi_3$ for some φ_3, and the lattice condition is trivially satisfied with

$$\gamma = \varphi_1 S(\theta_1, \ldots, \theta_m; \varrho_1)\varphi_3 S(\sigma_1, \ldots, \sigma_n; \varrho_2)\psi_2.$$

If β_1 and β_2 are not disjoint, then one must be a subword of the other, and by symmetry we may assume that β_1 is a subword of β_2. In fact we may even assume that cc = β_2, for the lattice condition must hold in this special case and it will hold for $\boldsymbol{a} = \varphi_2\beta_2\psi_2$ if it holds for $\boldsymbol{a} = \beta_2$. In view of (5.2), two cases can arise:

Case 1. β_1 is a subword of one of the occurrences of σ_j, for some j. In this case, note that there are $n(v_j, \lambda_2)$ occurrences of σ_j in ***a***, and a' has been obtained from ***a*** by replacing one of these occurrences of σ_j by the word σ'_j, where $\sigma_j \to \sigma'_j$. If we now replace σ_j by σ'_j in each of its remaining $n(v_j, \lambda_2) - 1$ occurrences in a, we obtain the word

$$\alpha_1 = S(\sigma_1, \ldots . \sigma_{j-1}, \sigma'_j, \sigma_{j+1}, \ldots . \text{a}, ; \lambda_2);$$

and it is clear that ***a'*** $\to^*$ α_1. Therefore the lattice condition is satisfied in this case if we take

$$\gamma = S(\sigma_1, \ldots, \sigma_{j-1}, \sigma'_j, \sigma_{j+1}, \ldots, \sigma_n; \varrho_2).$$

Case 2. The only remaining possibility is that

$$\beta_1 = S(\sigma_1, \ldots, \sigma_n; \mu) \tag{5.4}$$

where μ is a nontrivial subword of λ_2. (See the definition of "nontrivial subword" in § 1.) The observations above show that the lattice condition holds in all other cases, regardless of the set of reductions ***R, so*** an algorithm which tests ***R*** for completeness need only consider this case. It therefore behooves us to make a thorough investigation of this remaining possibility.

For convenience, let us write simply λ instead of λ_2. Since μ is a subword of λ we must have $\lambda = \varphi\mu\psi$, for some strings φ and ψ, and it follows from the assumptions above that

$$\varphi_1 = S(\sigma_1, \ldots, \sigma_n; \varphi), \quad \psi_1 = S(\sigma_1, \ldots, \sigma_n; \psi). \tag{5.5}$$

THEOREM ***5. Let*** μ ***be a subword*** *of* ***the word*** λ, ***where A =*** $\varphi\mu\psi$, ***and let*** $C(\lambda_1, \mu, \lambda)$ ***be the set*** *of* ***all words a which can be written in the form***

$$\text{a} = \varphi_1 S(\theta_1, \ldots, \theta_m; \lambda_1)\psi_1 = S(\sigma_1, \ldots, \text{a}, : \lambda) \tag{5.6}$$

for words $\sigma_1, \ldots, \sigma_n, \theta_1, \ldots, \theta_m$, ***where*** φ_1 ***and*** ψ_1 ***are defined by (5.5). Then either*** $C(\lambda_1, \mu, \lambda)$ ***is the empty set, or there is a word*** $\sigma(\lambda_1, \mu, \lambda)$, ***the*** "superposition ***of*** λ_1 ***on*** μ ***in I," such that*** $C(\lambda_1, \mu, \lambda)$ ***is the set*** *of* ***all words that have the form*** *of* $\sigma(\lambda_1, \mu, \lambda)$; i.e.

$$C(\lambda_1, \mu, \lambda) = \{S(\varphi_1, \ldots, \varphi_k; \sigma(\lambda_1, \mu, \lambda)) \ \varphi_1, \ldots, \varphi_k \text{ are words}\}. \tag{5.7}$$

Furthermore there is an algorithm which *finds* ***such a word*** $\sigma(\lambda_1, \mu, \lambda)$, ***or which determines that*** $\sigma(\lambda_1, \mu, \lambda)$ ***does not exist.***

Proof Let $\lambda' = S(v_{n+1}, \ldots, v_{n+m}; \lambda_1)$ be the word obtained by changing all the variables v_j in λ_1 to v_{n+j}; then λ' and λ have distinct variables. Let $\sigma_{n+1} = \theta_1, \ldots, \sigma_{n+m} = \theta_m,$ and let $\boldsymbol{r} = m+n$. Then the words al, ... σ_r are solutions to the equation

$$S(\sigma_1, \ldots, \text{a,; A}) = S(\sigma_1, \ldots, \text{a,;}\ \varphi)\ S(\sigma_1, \ldots, \sigma_r; \lambda')\ S(\sigma_1, \ldots, \text{a,; y}).$$

By Theorem 3, we can determine whether or not this equation has solutions; and when solutions exist, we can find a general solution $\boldsymbol{k}$, $\sigma_1', \ldots, \sigma_r'$. Theorem 5 follows if we now define $\sigma(\lambda_1, \mu, \lambda) = S(\sigma_1', \ldots, \sigma_r'; \lambda)$.

COROLLARY. ***Let R be a set** of **reductions; and let A be any algorithm which, given a word a, finds a word** α_0 **such that a** $\rightarrow^* \alpha_0$ **and** α_0 **is irreducible, with respect to R. Then R is complete** if **and only** if **the following condition holds** for **all pairs** of **reductions** $(\lambda_1, \varrho_1), (\lambda_2, \varrho_2)$ **in R and all nontrivial subwords** μ of λ_2 **such that the superposition** $\sigma(\lambda_1, \mu, \lambda_2)$ **exists:***

Let

$$\text{a} = \sigma(\lambda_1, \mu, \lambda_2) = \varphi_1 S(\theta_1, \ldots, \theta_m; \lambda_1)\psi_1 = S(\sigma_1, \ldots, \text{a,;}\ \lambda_2), \tag{5.8}$$

where φ_1 ***and*** ψ_1 ***are defined by (5.5). Let***

$$\sigma' = \varphi_1 S(\theta_1, \ldots, \theta_m; \varrho_1)\psi_1, \sigma'' = S(\sigma_1, \ldots, \sigma_n; \varrho_1), \tag{5.9}$$

and use algorithm A to find irreducible words σ_0' ***and*** σ_0'' ***such that a'*** $\rightarrow^* \sigma_0'$ ***and*** $\sigma_0'' \rightarrow^* \sigma_0''$. ***Then*** σ_0' must ***be identically equal to*** σ_0''.

Proof. Since a $\rightarrow$ a' and a $\rightarrow$ a", the condition that $\sigma_0' \equiv \sigma_0''$ is certainly necessary if $\boldsymbol{R}$ is complete. Conversely we must show that $\boldsymbol{R}$ is complete under the stated conditions.

The condition of Theorem 4 will be satisfied for all words $\boldsymbol{a}$ unless we can find reductions $(\lambda_1, \varrho_1), (\lambda_2, \varrho_2)$ and a nontrivial subword μ of λ_2 such that, in the notation of Theorem 4,

$$a = S(\varphi_1, \ldots, \varphi_k; \sigma), a' = S(\varphi_1, \ldots, \varphi_k; \sigma'), \alpha'' = S(\varphi_1, \ldots, \varphi_k; a'')$$

for some words $\varphi_1, \ldots, \varphi_k$. (This must happen because the discussion earlier in this section proves that we may assume a is a member of $C(\lambda_1, \mu, \lambda)$ if the condition of Theorem 4 is violated, and Theorem 5 states that a has this form.) But now we may take $\gamma = S(\varphi_1, \ldots, \varphi_k; \sigma_0') = S(\varphi_1, \ldots, \varphi_k; \sigma_0'')$, and the condition of Theorem 4 is satisfied.

Note that this corollary amounts to an algorithm for testing the completeness of any set of reductions. A computer implementation of this algorithm is facilitated by observing that the words $\sigma_1, \ldots,$ a,, $\theta_1, \ldots, \theta_m$ of (5.9) are precisely the words $\sigma_1', \ldots, \sigma_r'$ obtained during the construction of $\sigma(\lambda_1, \mu, \lambda_2)$ in the proof of Theorem 5.

As an example of this corollary, let us consider the case when $\boldsymbol{R}$ contains the single reduction

$$(\lambda, \varrho) = (f_2 f_2 v_1 v_2 v_3,\ f_2 v_1 f_2 v_2 v_3).$$

Here f_2 is a binary operator, and the relation $\lambda \to \varrho$ is the well-known associative law, $(v_1 \cdot v_2) \cdot v_3 \to v_1 \cdot (v_2 \cdot v_3)$, if we write $(v_1 \cdot v_2)$, for $f_2 v_1 v_2$. (Note that $\lambda > \varrho$, by the definition of § 2.)

Since $f_2 f_2 v_1 v_2 v_3$ has two nontrivial subwords, the corollary in this case requires us to test $\sigma(\lambda, \lambda, \lambda)$ and $\sigma(\lambda, f_2 v_1 v_2, \lambda)$. In the former case we obviously have a very uninteresting situation where $\sigma' =$ a”, so the condition is clearly fulfilled. In the latter case, we may take

$$\sigma = \sigma(\lambda, f_2 v_1 v_2, \lambda) = f_2 f_2 f_2 v_1 v_2 v_3 v_4,$$
$$\sigma' = f_2 f_2 v_1 f_2 v_2 v_3 v_4,\ \sigma'' = f_2 f_2 v_1 v_2 f_2 v_3 v_4.$$

Both of the latter reduce to $f_2 v_1 f_2 v_2 f_2 v_3 v_4$, so the associative law by itself is a "complete" reduction.

The argument just given amounts to the traditional theorem (found in the early pages of most algebra textbooks) that, as a consequence of the associative law, any two ways of parenthesizing a formula are equal when the variables appear in the same order from left to right.

We may observe that the testing procedure in the corollary may be simplified by omitting the case when $\lambda_1 = \lambda_2 = \mu$, since $\sigma' = \sigma''$. Furthermore we may omit the case when μ is simply a nullary operator f_q, since in that case we must have $\lambda_1 = f_q$, and both σ' and a” reduce to the common word γ obtained by replacing all occurrences off, in ϱ_2 by ϱ_1. (The argument is essentially the same as the argument of "Case 1" at the beginning of this section.)

6. Extension to a complete set. When a set of reductions is incomplete, we may be able to add further reductions to obtain a complete set. In this section we will show how the procedure of the corollary to Theorem 5 can be extended so that a complete set may be obtained in many cases.

First note that if $\boldsymbol{R}$ is a set of reductions and if $R_1 = \boldsymbol{R} \cup \{(\boldsymbol{I}, \varrho)\}$ where $\lambda \equiv \varrho$ **(R)**, then R_1 and $\boldsymbol{R}$ generate the same equivalence relation:

$$\boldsymbol{a} \equiv \beta \ (\boldsymbol{R}) \text{ if and only if a } \equiv \beta \ (R_1). \tag{6.1}$$

For if $\boldsymbol{a} \equiv \beta$ **(R)** we certainly have a $\equiv \beta$ (R_1); conversely if $\theta \to \varphi$ (R_1) using the relation (λ, ϱ), it follows from $\lambda \equiv \varrho$ **(R)** that $\theta \equiv \varphi$ **(R)**, and this suffices to prove (6.1) since all applications of the extra reduction (λ, ϱ) can be replaced by sequences of reductions using $\boldsymbol{R}$ alone.

Now if $R_1 = \boldsymbol{R} \cup \{(\lambda, \varrho)\}$ and $R_2 = \boldsymbol{R} \cup \{(\lambda', \varrho')\}$, where

$$\lambda \equiv \varrho \ (R_2) \text{ and } \lambda' \equiv \varrho' \ (R_1), \tag{6.2}$$

we can prove that R_1 and R_2 are ***equivalent*** sets of reductions, in the sense that

$$\text{a} \equiv \beta (R_1) \text{ if and only if } \alpha \equiv \beta \ (R_2). \tag{6.3}$$

For both of these relations are equivalent to the condition $\boldsymbol{a} \equiv \beta \ (R_1 \cup R_2)$ ***by*** (6.1).

Because of (6.3), we may assume that, for each reduction (λ, ϱ) in R, both λ and ϱ are irreducible with respect to the other reductions of $\boldsymbol{R}$.

The following procedure may now be used to attempt to complete a given set $\boldsymbol{R}$ of reductions.

Apply the tests of the corollary to Theorem 5, for all λ_1, λ_2, and μ. If in every case $\sigma_0' = \sigma_0''$, $\boldsymbol{R}$ is complete and the procedure terminates. If some choice of λ_1, λ_2, μ leads to $\sigma_0' \neq \sigma_0''$, then we have either $\sigma_0' > \sigma_0''$, $\sigma_0'' > \sigma_0'$, or $\sigma_0' \# \sigma_0''$. In the latter case, the process terminates unsuccessfully, having derived an equivalence $\sigma_0' \equiv \sigma_0''$ $(\boldsymbol{R})$ for which no reduction (as defined in this paper) can be used. In the former cases, we add a new reduction (σ_0', σ_0'') or (σ_0'', σ_0'), respectively, to $\boldsymbol{R}$, and begin the procedure again.

Whenever a new reduction (;I', ϱ') is added to $\boldsymbol{R}$, the entire new set $\boldsymbol{R}$ is checked to make sure it contains only irreducible words. This means, for each reduction (λ, ϱ) in $\boldsymbol{R}$ we find irreducible λ_0 and ϱ_0 such that $\lambda \to^* \lambda_0$ and $\varrho \to^* \varrho_0$, with respect to $\boldsymbol{R}$- $\{(\lambda, \varrho)\}$. Here it is possible that $\lambda_0 = \varrho_0$, in which case by (6.1) we may remove (λ, ϱ) from $\boldsymbol{R}$. Otherwise we might have $\lambda_0 > \varrho_0$ or $\varrho_0 > \lambda_0$, and $(1, \varrho)$ may be replaced by (λ_0, ϱ_0) or (ϱ_0, λ_0), respectively, by (6.3). We might also find that $\lambda_0 \# \varrho_0$, in which case the process terminates unsuccessfully as above.

Several examples of experiments with this procedure appear in the remainder of this paper. It was found to be most useful to test short reductions first (i.e. to consider first those λ_1 and λ_2 which have small weight or short length). Shorter words are more likely to lead to interesting consequences which cause the longer words to reduce and, perhaps, eventually to disappear.

In practice, when equivalent words cc and β are found so that $\alpha \# \beta$, it is often possible to continue the process by introducing a new operator into the system, as shown in the examples of the next section.

7. Computational experiments. In this section we will make free use of more familiar "infix" notations, such as $\alpha \cdot \beta$, in place of the prefix notation $f_j\alpha\beta$ which was more convenient for a formal development of the theory. Furthermore the word "axiom" will often be used instead of "reduction", and the letters $\boldsymbol{a}$, $\boldsymbol{b}$, c, $\boldsymbol{d}$ will be used in place of the variables v_1, v_2, v_3, v_4.

The computational procedure explained in § 6 was programmed in FORTRAN IV for an IBM 7094 computer, making use of standard techniques of tree structure manipulation. The running times quoted below could be improved somewhat, perhaps by an order of magnitude, (a) by recoding the most extensively used subroutines in assembly language, (b) by keeping more detailed records of which pairs (λ_1, λ_2) have already been tested against each other, and (c) by keeping more detailed records of those pairs (α, λ) of words for which we have already verified that a does not have the form of A. These three improvements have not been made at the time of writing, because of the experimental nature of the algorithm.

Example 1. Group theory I. The first example on which this method was tried was the traditional definition of an abstract group. Here we have three operators: a binary operator $f_2 = \cdot$ of weight zero, a unary operator $f_3 = {}^-$ of weight zero, and a nullary operator $f_1 =$ e of weight one, satisfying the following three axioms.

1. $e\cdot a \to$ a. ("There exists a left identity, e.")
2. $a^-\cdot a \to$ e. ("For every a, there exists a left inverse with respect to e.")
3. $(a.\ b)\cdot c \to a\cdot(b\cdot$ c). ("Multiplication is associative.“)

The procedure was first carried out by hand, to see if it would succeed in deriving the identities $a\cdot e = a$, $a^{--} = a$, etc., without making use of any more ingenuity than can normally be expected of a computer's brain. The success of this hand-computation experiment provided the initial incentive to create the computer program, so that experiments on other axiom systems could be performed.

When the computer program was finally completed, the machine treated the above three axioms as follows: First axioms 1 and 2 were found to be complete, by themselves; but when $\lambda_1 =$ **a-.** a of axiom 2 was superposed on $\mu = a\cdot b$ of $\lambda_2 = (a\cdot\ b)\cdot c$ of axiom 3, the resulting formula $(a^-\cdot\ a)\cdot b$ could be reduced in two ways as

$$(a^-\cdot a)\cdot b \to a^-\cdot(a\cdot b)$$

and

$$(a^-\cdot a)\cdot b \to e\cdot b \to b.$$

Therefore a new axiom was added,

4. $a^-\cdot(a\cdot b) \to b.$

Axiom 1 was superposed on the subword $a\cdot b$ of this new axiom, and another new axiom resulted:

5. $e^-\cdot a \to a.$

The computation continued as follows:

6. a---e $\to$ a from 2 and 4.

7. $a^{--}\cdot b \to a\cdot b$ from 6 and 3.

Now axiom 6 was no longer irreducible and it was replaced by

8. $a\cdot e \to a.$

Thus, the computer found a proof that e is a right identity; the proof is essentially the following, if reduced to applications of axioms 1, 2, and 3:

$$\begin{aligned} a\cdot e &\equiv (e\cdot a)\cdot e \equiv ((a^{--}\cdot a^-)\cdot a)\cdot e \equiv (a^{--}\cdot(a^-\cdot a))\cdot e \ \mathbf{3}\ (a^{--}\cdot e)\cdot e \\ &\equiv a^{--}\cdot(e\cdot e) \equiv a^{--}\cdot e \equiv a^{--}\cdot(a^-\cdot a) \equiv (a^{--}\cdot a^-)\cdot a \\ &\equiv e\text{-}a \equiv a. \end{aligned}$$

This ten-step proof is apparently the shortest possible one.

The computation continued further:

9. $e^- \to e$ from 2 and 8.

(Now axiom 5 disappeared.)

10 $a^{--} \to a$ from 7 and 8.

(Now axiom 7 disappeared).

11. $a \cdot a^- \to e$ from 10 and 2.

12. $a \cdot (b \cdot (a \cdot b)^-) \to e$ from 3 and 11.

13. $a \cdot (a^- \cdot b) \to b$ from 11 and 3.

So far, the computation was done almost as a professional mathematician would have performed things. The axioms present at this point were 1 2, 3, 4, 8, 9, 10, 11, 12, 13 ; these do not form a complete set, and the ensuing computation reflected the computer's groping for the right way to complete the set:

14. $(a \cdot b)^- \cdot (a \cdot (b \cdot c)) \to c$ from 3 and 4.

15. $b \cdot (c \cdot ((b \cdot c)^- \cdot a)) \to a$ from 13 and 3.

16. $b \cdot (c \cdot (a \cdot (b \cdot (c \cdot a))^-)) \to e$ from 12 and 3.

17. $a \cdot (b \cdot a)^- \to b^-$ from 12 and 4, using 8.

18. $b \cdot ((a \cdot b)^- \cdot c) \to a^- \cdot c$ from 17 and 3.

(Now axiom 15 disappeared.)

19. $b \cdot (c \cdot (a \cdot (b \cdot c))^-) \to a$ from 17 and 3.

(Now axiom 16 disappeared.)

20. $(a \cdot b)^- \to b^- \cdot a^-$ from 17 and 4.

At this point, axioms 12, 14, 18, and 19 disappeared, and the resulting complete set of axioms was:

1. $e \cdot a \to a$
2. $a^- \cdot a \to e$
3. $(a \cdot b) \cdot c \to a \cdot (b \cdot c)$
4. $a^- \cdot (a \cdot b) \to b$
8. $a \cdot e \to a$
9. $e^- \to e$
10. $a^{--} \to a$
11. $a \cdot a^- \to e$
13. $a \cdot (a^- \cdot b) \to b$
20. $(a \cdot b)^- \to b^- \cdot a^-$

A study of these ten reductions shows that they suffice to solve the word problem for free groups with no relations; two words formed with the operators $\cdot$, $^-$, and e can be proved equivalent as a consequence of axioms 1, 2, 3 if and only if they reduce to the same irreducible word, when the above ten reductions are applied in any order.

The computer took 30 seconds for this calculation. Note that, of the 17 axioms derived during the process, axioms 5, 14,15,16, 18, 19 never took part in the derivations of the final complete set; so we can give the machine an "efficiency rating" of 1 1/17 = 65%, if we consider how many of its attempts were along fruitful lines. This would seem to compare favorably with the behavior of most novice students of algebra, who do not have the benefit of the corollary to Theorem 5 to show them which combinations of axioms can possibly lead to new results.

Example 2. Group theory II In the previous example, the unary operator $^-$ was assigned weight zero. In § 1 we observed that a unary operator may be assigned weight zero only in exceptional circumstances (at least under the well-ordering we are considering), so it may be interesting to consider what would happen if we would attempt to complete the group theory axioms of Example 1, but if we made a "slight" change so that the $^-$ operator has positive weight.

From the description of Example 1, it is clear that the computation would proceed in exactly the same manner, regardless of the weight of $^-$, until we reach step 20; now the axiom would be reversed:

20. $b^-\cdot a^- \rightarrow (a\cdot b)^-$.

Thus, $(a\cdot b)^- = f_3f_2ab$ would be considered as a "reduction" of the word $b^-\cdot a^- = f_2f_3bf_3a$; and this is apparently quite a reasonable idea because $(a\cdot b)^-$ is in fact a shorter formula.

But if axiom 20 is written in this way, the computation will never terminate, and no complete set of axioms will ever be produced!

THEOREM ***6.*** *If* ***the operator*** $^-$ ***is assigned a positive weight, no finite complete set of reductions is equivalent to the group theory axioms***

$$(a\cdot b)\cdot c \rightarrow a\cdot(b\cdot c),\ e\cdot a \rightarrow \boldsymbol{a},\ a^-\cdot a \rightarrow \boldsymbol{e}.$$

Proof. Consider the two words

a, = $v_{n+1}\cdot(v_1\cdot(v_2 \ldots \cdot(v_n\cdot v_{n+1}) \ldots))^-$,

$\beta_n = (v_1\cdot(v_2 \ldots \cdot(v_{n-1}\cdot v_n) \ldots))^-$, n $\geqslant 2$.

It is obvious that β_n is not equivalent to any lesser word in the well-ordering, since all words equivalent to β_n have at least one occurrence of each variable $v_1, \ldots, v_n$, plus at least n- 1 multiplication operators, plus at least one $^-$ operator. Since ***a,*** is equivalent to β_n, any complete set ***R*** of reductions must include some (λ, ϱ) which reduces a,. Now no subword of α_n, except ***a,*** itself, can be reduced, since each of its smaller subwords is the least in its equivalence class. Therefore α_n itself must have the form of λ; we must have a, = $S(\theta_1, \ldots, \theta_m; \lambda)$ for some words $\theta_1, \ldots, \theta_m$. It is easy to see that this means there are only a few possibilities for the word λ. ***Now*** the word

a,: = $v_{n+2}\cdot(v_1\cdot(v_2 \ldots \cdot(v_n\cdot v_{n+1}) \ldots))^-$

is ***not*** equivalent to any lesser word in the well-ordering, so α_n' cannot have the form of λ. This implies finally that $\lambda \equiv \alpha_n$, except perhaps for permutation of variables; so $\boldsymbol{R}$ must contain infinitely many reductions.

Example 3. Group theory III. Suppose we start as in Example 1 but with left identity and left inverse replaced by right identity and right inverse :

1. $a\cdot e \rightarrow a$
2. $a\cdot a^- \rightarrow e$
3. $(a\cdot b)\cdot c \rightarrow a\cdot(b\cdot c)$.

It should be emphasized that the computational procedure is ***not*** symmetrical between right and left, due to the nature of the well-ordering, so that this is quite a different problem from Example 1. In this case, axiom 1 combined with axiom 3 generates "$a\cdot(e\cdot b) \rightarrow a\cdot b$", which has no analog in the system of Example 1.

The computer found this system slightly more difficult than the system of Example 1; 24 axioms were generated during the computation, of which 8 did not participate in the derivation of the final set of reductions. This gives an "efficiency rating" of 67%, roughly the same as in Example 1. The computation required 40 seconds, compared with 30 seconds in the former case. The same set of reductions was obtained as the answer.

Example 4. Inverse property. Suppose we have only two operators $\cdot$ and $^-$ as in the previous examples and suppose that only the single axiom

1. $a^-\cdot(a\cdot b) \rightarrow b$

is given. No associative law, etc., is assumed.

This example can be worked by hand : First we superpose $a^-\cdot(a\cdot b)$ onto its component $(a\cdot b)$, obtaining the word $a^{--}\cdot(a^-\cdot(a\cdot b))$ which can be reduced both to $a\cdot b$ and to $a^{--}\cdot b$. This gives us a second axiom

2. $a^{--}\cdot b \rightarrow a\cdot b$

as a consequence of axiom 1.

Now $a^-\cdot(a\cdot b)$ can be superposed onto $a^{--}\cdot b$; we obtain the word $a^{--}\cdot(a^-\cdot b)$ which reduces to b by axiom 1, and to $a\cdot(a^-\cdot b)$ by axiom 2. Thus, a third axiom

3. $a\cdot(a^-\cdot b) \rightarrow b$

is generated. It is interesting (and not well known) that axiom 3 follows from axiom 1 and no other hypotheses; this fact can be used to simplify several proofs which appear in the literature, for example in the algebraic structures associated with projective geometry.

A rather tedious further consideration of about ten more cases shows that axioms 1, 2, 3 form a complete set. Thus, we can show that $a^{--}\cdot b \equiv a\cdot b$

is a consequence of axiom 1, but we cannot prove that $a^{--} \equiv a$ without further assumptions.

A similar process shows that axioms 1 and 2 follow from axiom 3.

Example 5. Group theory IV. The axioms in example 1 are slightly stronger than the "classical" definition (e.g. Dickson [3]), which states that multiplication is associative, there is at least one left identity, and that ***for each left identity*** there exists a left inverse of each element. Our axioms of Example 1 just state that there is a left inverse for the left identity e.

Consider the five axioms

1. $(a \cdot b) \cdot c \to a \cdot (b \cdot c)$
2. $e \cdot a \to a$
3. $f \cdot a \to a$
4. $a^{-} \cdot a \to e$
5. $a^{\sim} \cdot a \to f$

where e, f are nullary operators; $^{-}$ and $^{\sim}$ are unary operators; and $\cdot$ is a binary operator. Here we are postulating two left identities, and a left inverse for each one. The computer, when presented with these axioms, found a complete set of reductions in 50 seconds, namely the two reductions

$$f - e$$
$$a - \to a^{-}$$

together with the ten reductions in Example 1. As a consequence, it is clear that the identity and inverse functions are unique.

The derivation off → e was achieved quickly in a rather simple way, by first deriving "a-. $(a \cdot b) \to b$" as in Example 1, then deriving "$f^{-} \cdot b \to b$" by setting $a = f$, and finally deriving "$f \to e$" by setting $b = f$.

Example 6. Central groupoids I. An interesting algebraic system has recently been described by Evans [5]. There is one binary operator . and one axiom

1. $(a \cdot b) \cdot (b \cdot c) \to b.$

Let us call this a "central groupoid", since the product $(a.\ b) \cdot (b \cdot c)$ reduces to its central element b. The computational procedure of § 6 can in this case be carried out easily by hand, and we obtain two further axioms

2. $a \cdot ((a \cdot b) \cdot c) \to a \cdot b$
3. $(a \cdot (b \cdot c)) \cdot c \to b \cdot c$

which complete the set.

Evans [5] has shown that every finite central groupoid has n^2 elements, for some nonnegative integer n. It is also possible to show [7] that every finite central groupoid with n^2 elements has exactly n idempotent elements, i.e. elements with $a \cdot a = a$. On the other hand, we can show (by virtue of the fact that the three axioms above form a complete set) that the ***free*** central groupoid on any number of generators has no idempotents at all. For if there is an idempotent, consider the least word a in the well-ordering such that $\alpha \equiv \alpha\cdot\alpha$. Clearly a is not a generator, and so a must have the form $\alpha = \beta\cdot\gamma$ where ***a***, β, and γ are irreducible. Thus $(\beta\cdot\gamma)\cdot(\beta\cdot\gamma)$ must be reducible; this is only possible if $\gamma = \beta$, and then $\beta\cdot\beta =$ a = a $\cdot\alpha = \beta$ is not irreducible after all. (This proof was communicated to the authors by Professor Evans in 1966.)

Example 7. A "random" axiom. Experiments on several axioms which were more or less selected at random show that the resulting systems often degenerate. For example, suppose we have a ternary operator denoted by (x, y, z), which satisfies the axiom

1. $(a, (b, c, a), d) \to c$.

Superposing the left-hand side onto (b, c, a) gives the word

$$(b, (a, (b, c, a), b), d),$$

and this reduces both to (b, c, a) and to (b, c, d). Hence we find

$$(b, c, a) \equiv (b, c, d).$$

Now the computational method described in § 6 will stop, since

$$(b, c, a) \# (b, c, d).$$

But there is an obvious way to proceed: Since $(b, c, a) \equiv (b, c, d)$, clearly (b, c, a) is a function of b and c only, so we may introduce a new binary operator . and a new axiom

2. $(a, b, c) \to a\cdot b$.

Now axiom 1 may be replaced by

3. $a\cdot(b\cdot c) \to c$.

Axiom 3 now implies

$$c\cdot d \equiv a\cdot(b\cdot(c\cdot d)) \equiv a\cdot d$$

and again we find $c\cdot d \# a\cdot d$. Now as above we note that $c\cdot d$ is a function only of d, and so we introduce a further operator \$, a unary operator, with the new axiom

4. $a\cdot b \to b\$$.

Now axiom 2 is replaced by

5. $(a, b, c) \to b\$$

and axiom 3 reduces to

6. $a\$\$ \to a$.

We are left with axioms 4, 5, and 6, and axiom 4 is irrelevant since the purpose of the binary operator has been served. Thus, two words involving the ternary operator are equivalent as a consequence of axiom 1 if and only if they reduce to the same word by applying reductions 5 and 6. The free system on n generators has $2n$ elements.

Example 8. Another "random" axiom. If we start with

1. $(a\cdot b)\cdot(c\cdot(b\cdot a)) \to b$,

the computer finds that

$$c \equiv ((b\cdot a)\cdot c)\cdot((a\cdot b)\cdot(c\cdot(b\cdot a))) \equiv ((b\cdot a)\cdot c)\cdot b,$$

so $((b\cdot a)\cdot c)\cdot b \to$ c. This implies

$$b \equiv (((b\cdot a)\cdot c)\cdot b)\cdot(b\cdot a) \equiv c\cdot(b\cdot a),$$

and the original axiom now says

$$c \equiv b.$$

Clearly this is a totally degenerate system; following the general procedure outlined above, we introduce a new nullary operator e, and we are left with the axiom

$$a \to e.$$

The free system on n generators has one element.

Example 9. The cancellation law. In the previous two examples, we have seen how it is possible to include new operators in order to apply this reduction method to axioms for which the method does not work directly. A similar technique can be used to take the place of axioms that cannot be expressed directly in terms of "identities". Our axioms up to now have always been "identities"; for example, the reduction (a. $b)\cdot\ c \to a\cdot(b\cdot\ c)$ means essentially that

$$\text{for all words } a, b, c, \quad (a\cdot b)\cdot c \equiv a\cdot(b\cdot c).$$

A general reduction $\alpha \to \beta$ means that a $\equiv \beta$ for all values of the variables appearing in a and β. Of course many mathematical axioms are not simply identities; one common example is the ***left cancellation law***

$$\text{for all words } a, b, \text{ c, if } a\cdot b \equiv a\cdot c \text{ then } b \equiv c. \tag{7.1}$$

The left cancellation law can be represented as an identity in the following way. Consider a function $f(x, y)$ which satisfies the identity

$$f(a, a\cdot b) \to b. \tag{7.2}$$

If 8 represents any set of axioms, let $\mathcal{S}'$ be the set of axioms obtained by adding the left cancellation law (7.1) to $\mathcal{S}$, and let $\mathcal{S}''$ be the set of axioms obtained by adding the reduction (7.2) to 8 where f is a binary operator which does not appear in 8. Now we assert that any two words ***not*** involving f which can be proved equivalent in 8' can be proved equivalent in $\mathcal{S}''$. For whenever (7.1) is used, we must have already proved that $a\cdot b \equiv a\cdot c$, hence $f(a, a\cdot b) \equiv f(a, a\cdot$ c), hence $b \equiv c$ by (7.2). Conversely, any two words α and

β not involving *f* which can be proved equivalent in $\mathcal{S}''$ can be proved equivalent in 8’: For if (7.1) holds, there exists a binary operator *f* satisfying (7.2); one such binary operator for example can be defined by letting$f(x, y)$ equal z if y can be written in the form $x \cdot z$ (here z is unique by (7.1)), and letting $f(x; y)$ equal x otherwise. This function *f* has properties which are in fact somewhat stronger than (7.2) asserts, so if we can prove a $\equiv \beta$ under the weaker hypotheses $\mathcal{S}''$, we can prove $a \equiv \beta$ with 8’.

(The argument just given seems to rely on certain rules of inference not admissible in some logical systems. Another argument which systematically removes all appearances off from a proof of $\alpha \equiv \beta$ in the system $\mathcal{S}''' \equiv \equiv \mathcal{S} \cup \{(7.1), (7.2))$ can be given, but it will be omitted here; we will content ourselves with the validity of the more intuitive but less intuitionistic argument given.)

A system which has a binary operation . and both left and right cancellation laws, but no further axioms, can be defined by

1. $f(a, a \cdot b) \rightarrow b$
2. $g(a \cdot b, b) \rightarrow a.$

Here *f* and g are two new binary operators. Axioms 1 and 2 are complete by themselves, so they suffice to solve the word problem for any words involving$f$, $\cdot$, and g. Two words involving only . are equivalent if and only if they are equal.

If we add a unit element, namely a nullary operator e such that

3. $e \cdot a \rightarrow a$
4. $a \cdot e \rightarrow a,$

then the computer will complete the set by adding four more reductions:

5. $f(a, a) \rightarrow e$
6. $f(e, a) \rightarrow a$
7. $g(a, a) \rightarrow e$
8. $g(a, e) \rightarrow a.$

Example 10. Loops. Consider the axiom “for all a and b there exists c such that $a \cdot c \equiv b$”. This amounts to saying that there is a binary operation “\” such that $c = a\backslash b$, i.e. that $a \cdot (a\backslash b) \equiv b.$ (This law is a companion to the cancellation law (7.1) which asserts that at ***most*** one such c exists.)

In the mathematical system known as an abstract loop, we have the above law and its left-right dual, so there are three binary operators $\cdot$, \, and / which satisfy

1. $a \cdot (a\backslash b) \rightarrow b$
2. $(a/b) \cdot b \rightarrow a.$

There is also a unit element, so that

3. $e\cdot a \to a$

4. $a\cdot e \to a$.

The computer, when presented with these axioms, will generate

5. $e\backslash a \to a$

6. $a/e \to a$.

Axioms 1 through 6 form a complete set, but they do not define a loop; two important axioms have been left out of the above discussion, namely the left and right cancellation laws. So if we postulate two further binary operators f and g as in Example 9, with two further axioms

7. $f(a, a\cdot b) \to b$

8. $g(a\cdot b, b) \to a$,

the computer will now generate

9. $f(a, b) \to a\backslash b$

10. $g(a, b) \to a/b$

11. $a\backslash(a\cdot b) \to b$

12. $(a\cdot b)/b \to a$

13. $a/a \to e$

14. $a\backslash a \to e$

15. $a/(b\backslash a) \to b$

16. $(a/b)\backslash a \to b$.

Axioms 1, 2, . . . , 6, 9, 10, . . . , 16 form a complete set of reductions, and if we remove axioms 9 and 10 (which merely serve to remove the auxiliary functionsfand g) we obtain reductions for a free loop. This is a special case of the complete set given by Evans [4] who also adds relations between generators (i.e. between additional nullary operators).

Note that in Example 9 the cancellation laws had no effect on the word problem, while in this case the rules 11 through 16 could not be obtained from 1 through 4 without postulating the cancellation laws. On the other hand, when the mathematical system is known to be finite, the existence of a solution c to the equation $a\cdot c \equiv b$, for all a and b, implies the uniqueness of that solution. Thus laws 11 through 16 can be deduced from 1 through 4 in a finite system, but not in a free system on a finite number of generators.

The generation of the complete set above, starting from 1, 2, 3, 4, 7, 8, took 20 seconds. Axiom 9 was found quickly since

$$b\backslash a \equiv f(b, b\cdot(b\backslash a)) \equiv f(b, a).$$

Example 11. Group theory V. An interesting way to define a group with axioms even weaker than the classical axioms in Example 5 has been pointed out by 0. Taussky [**11**]. Besides the associative law,

1. $(a{\cdot}b){\cdot}c \rightarrow a{\cdot}(b{\cdot}c)$,

we postulate the existence of an idempotent element e :

2. $e{\cdot}e \rightarrow$ e.

Furthermore, each element has ***at least one right inverse*** with respect to e, i.e. there is a unary operator $^-$ such that

3. $a{\cdot}a^- \rightarrow \boldsymbol{e}$.

Finally, we postulate that each element has ***at most one left inverse*** with respect to e. This last assertion is equivalent to a very special type of cancellation law, which is more difficult to handle than (7.1) :

$$\text{for all } \boldsymbol{a}, \boldsymbol{b}, \text{ c, if } b{\cdot}a \equiv c{\cdot}a \equiv \text{e then } \boldsymbol{b} \equiv \boldsymbol{c}. \tag{7.3}$$

This axiom (7.3) can be replaced, as in Example 9, by identities involving new operators. Let ***f*** be a ternary operator and g a binary operator, and postulate the following axioms :

4. $f(e, \boldsymbol{a}, \boldsymbol{b}) \rightarrow \boldsymbol{a}$
5. $f(a{\cdot}b, \boldsymbol{a}, \boldsymbol{b}) \rightarrow g(a{\cdot}b, \boldsymbol{b})$.

It is easy to see that these axioms imply (7.3). Conversely, (7.3) implies the existence of such functions f and g, since we may define for example

$$f(x,\ y,\ z) = \begin{cases} y,. & \text{if } x \equiv e \\ x, & \text{if } x \not\equiv e \end{cases}$$

$$g(x,\ y) = \begin{cases} z, & \text{if } x \equiv e \text{ and } z{\cdot}y \equiv e \\ x, & \text{if x} \not\equiv \text{e or if there is no z such that z-y} \equiv e. \end{cases}$$

The latter function g is well defined when (7.3) holds.

Thus, axioms 4 and 5 may be regarded, just as in Examples 9 and 10, as equivalent to (7.3), if we consider the word problem for words that do not involve ***f*** and g. (Note: Actually a binary operation $f(x, \boldsymbol{y})$ could have been used, but since $f(a{\cdot}\boldsymbol{b}$, a) $\not\equiv g(a{\cdot}\boldsymbol{b}, \boldsymbol{b})$, we used a ternary operation so that axiom 5 could be considered as a reduction.)

The computer was presented with axioms 1 through 5, and an interesting sequence of computations began. One of the consequences of axioms 1 and 3 alone is that

$$e{\cdot}a^{--} \equiv (a{\cdot}a^-){\cdot}a^{--}\ \boldsymbol{3}\ a{\cdot}(a^-{\cdot}a^{--}) \equiv a{\cdot}e. \tag{7.4}$$

After 2 minutes and 15 seconds, the computation process derived its 29th consequence of axioms 1 through 5, namely that $\boldsymbol{a}^{--} \rightarrow a$. This meant that (7.4) became

$$e{\cdot}a \equiv a{\cdot}e$$

and the computer stopped since the definitions of § 2 imply that $e \cdot a \# a \cdot e$. (This is sensible for if we were to say $e \cdot a \to a \cdot e$, the computer would loop indefinitely trying to reduce the word $e \cdot e$.)

Now we restarted the process as in Examples 7 and 8 by introducing a new unary operator \$, with $e \cdot a \equiv a\$$. The axioms currently in the system at that time were thereby transformed to include the following, among others :

$$e\$ \to e$$

$$a\$\$ \to a\$$$

$$a \cdot e \to a\$$$

$$e \cdot a \to a\$$$

$$(ab)\$ \to a(b\$)$$

$$g(e, a\$> \to a^- .$$

In order to make the well-ordering come out correctly for these reductions we changed the weight of $\cdot$ from zero to one, changed the weight off from one to two, and made \$ a unary operator of weight one which was higher than . in the ordering of operators.

Another axiom in the system at this time, which had been derived quite early by superposing 3 onto 5 and applying 4, was

$$g(e, a^-) \to a.$$

This now was combined with the rule $a^{--} \to a$ to derive

$$g(e, a) \to a^-.$$

The reduction g(e, $a\$) \to a^-$ now was transformed to

$$a\$^- \to a^-$$

and, with the law $a^{--} \to a$, this became

$$a\$ \to a.$$

Thus, the \$ operator disappeared, and the traditional group axioms were immediately obtained. After approximately 3 minutes of computer time from the beginning of the computations, all ten reductions of Example 1 had been derived.

Actually it is not hard to see that, as in the discussion of Example 2, axioms 1 through 5 cannot be completed to a finite set of reductions. After $4\frac{1}{2}$ minutes execution time, the computer was deriving esoteric reductions such as

$$f(c, c \cdot (a^- \cdot b^-), b \cdot a) \to g(c, b \cdot a).$$

Since the process would never terminate, there was perhaps a logical question remaining whether any new reductions would be derived (besides the 10 in the final set of Example 1) that would give us ***more*** than a group. Of course we knew this would not happen, but we wanted a theoretical way to get this result as a consequence of axioms 1 through 5. This can be done in fact, by adding new axioms

$$g(a, \mathbf{b}) \to a \cdot b^-$$
$$f(a, \mathbf{b}, \mathbf{c}) \to \mathbf{b}$$

to the long list of axioms derived by the machine after 3 minutes. These axioms are now even stronger than 4 and 5, and together with the ten final axioms of Example 1 they form a complete set of twelve reductions. Thus we can be sure that axioms 1 through 5 do not prove any more about words in $\cdot$, $^-$, and e which could not be proved in groups.

The computer's derivation of the laws of group theory from axioms 1, 2, 3 and (7.3) may be reformulated as follows, if we examine the computations and remove references to ***f*** and g:

"We have $e \cdot a^{--} \equiv a \cdot e$, as in (7.4), hence

$$a \cdot e \ \mathbf{3} \ e \cdot a^{--} \equiv (e \cdot e) \cdot a^{--} \equiv e \cdot (e \cdot a^{--}) \equiv e \cdot (a \cdot e).$$

$$\therefore \ a^{--} \cdot e \equiv e \cdot (a^{--} \cdot e) \equiv (e \cdot a^{--}) \cdot e \equiv (a \cdot e) \cdot e \ \mathbf{3} \ a \cdot (e \cdot e) \equiv a \cdot e.$$

$$\therefore \ a^- \cdot (a \cdot e) \ \mathbf{3} \ a^- \cdot (a^{--} \cdot e) \equiv (a^- \cdot a^{--}) \cdot e \ \mathbf{3} \ e \cdot e \equiv \mathbf{e}.$$

So, by (7.3), **a-** is the left inverse of $a \cdot e$, and similarly **a--** is the left inverse of $a^{--} \cdot e \equiv a \cdot$ **e.** Hence

$$\boldsymbol{a}^{- - -} \ \doteq \boldsymbol{a}\text{-}.$$

But now ***a*** is the left inverse of **a-** by (7.3) and axiom 3, and so **a--** is the left inverse of $a^{---} \equiv$ **a-, so**

$$\boldsymbol{a}^{- -} \ \boldsymbol{z} \ \boldsymbol{a}.$$

This implies that a- is the left inverse of ***a*** ≡ **a--,** so each element has a unique left inverse. The left inverse of $a \cdot e$ is $(a \cdot e)^-$, and we have seen that the left inverse of a. e is $\boldsymbol{a}^-$, hence $(a \cdot \mathrm{e})^- = \boldsymbol{a}^-$. Now, taking primes of both sides, we see that $a \cdot e = \boldsymbol{a}$, and the rest of the properties of group theory follow as usual."

A simpler proof can be given if we start by observing that $(e \cdot a) \cdot a^- \equiv$ $\equiv e \cdot (a \cdot a^-) \equiv e \cdot e \ \mathbf{3} \ \mathbf{e} \ \equiv a \cdot a^-$;hence, by (7.3), $e \cdot a \equiv$ ***a. Now*** $(a \cdot e) \cdot a^- \equiv$ $\equiv a \cdot (e \cdot a^-) \equiv a \cdot a^- \equiv$ ***e;*** hence by (7.3), $a \cdot e \equiv$ ***a.***

The computer's proof is longer, but interesting in that it does not require application of (7.3) until after several consequences of axioms 1, 2, 3 alone are derived.

Example 12. $(l$, r) ***systems I.*** It is interesting to ask what happens if we modify the axioms of group theory slightly, postulating a ***left*** identity element and a ***right*** inverse. (Compare with Examples 1 and 3.) This leads to an algebraic system which apparently was first discussed by A. H. Clifford [**1**]. H. B. Mann [**8**] independently discussed this question, and called the systems "(I, ***r)*** systems". They are also called "left groups" [**2**].

Starting with the axioms

1. $e\cdot a \to a$
2. $a\cdot a^- \to e$
3. $(a\cdot b)\cdot c \to a\cdot(b\cdot c)$,

the computer extended them to the following complete set of reductions:

4. $e^- \to e$
6. $a\cdot(a^-\cdot b) \to b$
8. $a\cdot e \to a^{--}$
10. $a^{--}\cdot b \to a\cdot b$
16. $a^-\cdot(a\cdot b) \to b$
18. $a^{---} \to a$
29. $(a\cdot b)^- \to b^-\cdot a^-$.

(The numbers 4, 6, 8, etc. which appear here reflect the order of "discovery" of these reductions. The computation took 110 seconds. Of 26 axioms generated, 14 were never used to derive members of the final set, so the "efficiency ratio" in this case was 46%.) These ten reductions solve the word problem for free (l, r)-systems defined by axioms 1, 2, and 3.

Example 13. (r, l) systems. Similarly, we can postulate a right identity and a left inverse. This leads to an algebraic system dual to the system of Example 12, so it is not essentially different from a theoretical standpoint; but since the method of § 6 is not symmetrical between left and right, a test of these axioms was worth while as a further test of the usefulness of the method.

This set of axioms was substantially more difficult for the computer to resolve, apparently because the derivation of the law $(a\cdot b)^- \equiv b^-\cdot a^-$ in this case requires the use of a fairly complex intermediate reduction, $(a\cdot b)^-\cdot(a\cdot(b\cdot c))\to c^{--}$, which would not be examined by the computer until all simpler possibilities have been explored. When the roles of left and right are interchanged as in Example 12, the steps leading to $(a\cdot b)^- \equiv$ $\equiv b^-, a$ are much less complicated.

After $2\frac{1}{2}$ minutes of computation, the identity

$$b^{--}\cdot(a\cdot b)^- \equiv (c\cdot a)^-\cdot c$$

was derived, and computation ceased because $b^{--} . (a.\ b)^- \# (c\cdot a)^-. c$. However, it is plain that this quantity is a function of a alone, so we introduced a new unary operator $\$$ and the rule $(c\cdot a)^-\cdot c$-$a\,\$$. After another $2\frac{1}{2}$ minutes of computation the following complete set of 12 reductions for $(\boldsymbol{r}; \boldsymbol{l})$ systems was obtained:

$$\begin{array}{cc}
a\cdot e \to \boldsymbol{a} & b\cdot(a\cdot a^{-}) \to \boldsymbol{b} \\
a^{-}\cdot a \to \boldsymbol{e} & b\cdot(a\cdot(a^{-}\cdot c)) \to b\cdot c \\
(a\cdot b)\cdot c \to a\cdot(b\cdot c) & a^{-}\cdot(a\cdot b) \to \boldsymbol{a}\text{-\,-} \\
\boldsymbol{e}\text{-} \to \boldsymbol{e} & b\cdot(a^{--}\cdot c) \to b\cdot(a\cdot c) \\
e\cdot a \to \boldsymbol{a}\text{-\,-} & \boldsymbol{a}\text{-\,-\,-} \to a^{-} \\
a\cdot b^{--} \to a\cdot b & (a\cdot b)^{-} \to b^{-}\cdot a^{-}
\end{array}$$

plus the further reduction $\boldsymbol{a\$} \to \boldsymbol{a}\text{-}$ which was, of course, discarded.

Example 14. (I, ***r) systems II.*** If we introduce two left identity elements and two corresponding right inverse operators, we have the five axioms

1. $(a\cdot b)\cdot c \to a\cdot(b\cdot c)$,
2. $e\cdot a \to a$,
3. $f\cdot a \to \boldsymbol{a}$,
4. $a\cdot a^{-} \to \boldsymbol{e}$,
5. $a\cdot a^{\sim} \to f$.

(Compare with Example 5.) After 2 minutes of computation, the computer was only slowly approaching a solution to the complete set; at that point 35 different axioms were in the system, including things such as $\boldsymbol{a}\text{---} + a^{--}$, $a^{---\sim} \to a^{-\sim}$, $a\cdot a^{\sim --} \to$ e, etc. ; just before we manually terminated the computation, the reduction $\boldsymbol{a}\text{-}\ {}^{\sim -}\cdot \boldsymbol{b} \to a^{-}\cdot \boldsymbol{b}$ was generated.

It was apparent that more efficient use could be made of the computer time if we presented the machine with the information it had already derived in Example 12. Axioms 1, 2, and 4 by themselves generate a complete set of 10 axioms as listed in Example 12, and axioms 1, 3, 5 generate an analogous set of 10 with e and replaced by f and $^{\sim}$. Therefore we started the calculation again, with 19 initial axioms in place of the 5 above. (In general, it seems worth while to apply the computational method to subsets of a given set of axioms first, and later to add the consequences of these subsets to the original set, since the computation time depends critically on the number of axioms currently being considered.) Now a complete set of consequences of axioms 1 through 5 was obtained after $2\frac{1}{2}$ minutes of calculation; this complete set consists of the following 21 reductions.

$$\begin{array}{rl}
e^{-} \to \boldsymbol{e}, & f^{\sim} \to f; \\
e^{\sim} \to f, & f^{-} \to e; \\
e\cdot a \to \boldsymbol{a}, & f\cdot a - \boldsymbol{a}; \\
a\cdot a^{-} \to \boldsymbol{e}, & a\cdot a^{\sim} \to f; \\
a^{\sim\sim} \to a^{-\sim}, & a^{\sim-} \to a^{--}; \\
a^{---} \to a^{-}, & \boldsymbol{a}_{- - -} \to a^{\sim}; \\
a\cdot e - a^{--}, & a\cdot f - a^{-\sim};
\end{array}$$

$$(a\cdot b)\cdot c \to a\cdot(b\cdot c);$$

$$\boldsymbol{a}^{\sim}\cdot b - a^{-}\cdot b;$$

$$\begin{array}{rl}
(a\cdot b)^{-} - b^{-}\cdot a^{-}, & (a\cdot b)^{\sim} - b^{-}\cdot a^{\sim}; \\
a^{-}\cdot(a\cdot b) - \boldsymbol{b}, & a\cdot(a^{-}\cdot b) - \boldsymbol{b};
\end{array}$$

$$\boldsymbol{a}^{--}\cdot b - a\cdot b.$$

It is clear from this set what would be obtained if additional left inverse and right identity functions were supplied. Furthermore if we were to postulate that $a^{-} \equiv a^{\sim}$, then e $\equiv f$. If we postulate that e $\equiv f$, then it follows quickly that $\boldsymbol{a}$-- $\equiv a^{-\sim}$, hence $a^{-} \equiv a^{---} = a^{--\sim} \equiv a^{\sim}$.

Example 15. (1, ***r*) systems** *III.* Clifford's paper [1] introduces still another weakening of the group theory axioms; besides the associative law

1. $(a\cdot b)\cdot c - a\cdot(b\cdot c)$

and the existence of a left identity

2. $e\cdot a - \boldsymbol{a},$

he adds the axiom, "For every element $\boldsymbol{a}$ there exists a left identity e and an element $\boldsymbol{b}$ such that $b\cdot a = \boldsymbol{e}$." This was suggested by an ambiguous statement of the group theory axioms in the first edition of B. L. van der Waerden's *Moderne* ***Algebra*** [Berlin: Springer, 1930, p. 15]. Following the conventions of the present paper, this axiom is equivalent to asserting the existence of ***two*** unary operators, 'and *, with the following two axioms :

3. $a'\cdot a - \boldsymbol{a}^{*},$
4. $a^{*}\cdot b - \boldsymbol{b}.$

Clifford proved the rather surprising result that this set of axioms defines an (I, r) system; and that, conversely, every (I, ***r*)** system satisfies this set of axioms. Therefore we set the computer to work on axioms 1, 2, 3, 4, to see what the result would be.

After 2 minutes of computation, it was apparent that the system was diverging; 32 axioms were present, including

$$e''''''^{*} \to e''''''^{*}, \quad a^{*'''''*} \to a^{*'''''}, \quad a\cdot a''''' \to a'''''^{*}$$

and others of the same nature. It was not hard to show that, as in Example 2, no finite complete set of reductions would be found by the computational method.

But there is a "trick" which can be used to solve the word problem for words composed of the operators e, ′, *, and ·, by introducing two further unary operators \$ and # , such that $a'\cdot e \equiv a\#$, $a\cdot a' \equiv a\$$. One of the consequences which the machine had derived very quickly from axioms 1, 2, 3, 4 was that $a\cdot(a'\cdot b) \to b$; so, putting $b \equiv e$, *we* have $a\cdot a\# \equiv e$. Similarly the law $a'\cdot(a\cdot b) \to b$ had been derived, and it follows that $a' \equiv a'\cdot(a\cdot a') \equiv a'\cdot a\$ \equiv a'\cdot(e\cdot a\$) \equiv (a'\cdot e)\cdot a\$ \equiv a\#\ .a\$$.

Therefore if we take any word involving e, ′, *, and ·, we can replace each component of the form a’ by $a\#\cdot\alpha\$$. Then we have a word in the operators e, *, ·, #, and \$. For this new system, axiom 3 should be replaced by

3’. $a\#\cdot(a\$\cdot a) \to a^*$.

We also know from the above discussion that the axiom

5. $a\cdot a\# - e$

is a legitimate consequence of axioms 1, 2, 3, 4, and since axioms 1, 2 and 5 define an (l, r) system we added their consequences

6. $a\cdot e \to a\#\#$,

7. a# # # → a#,

etc., as determined in Example 12. The following complete set of 21 reductions was now obtained for words in e, *, . , # , and \$:

$$(a\cdot b)\cdot c \to a\cdot(b\cdot c);$$

$$e\cdot a - a, \qquad a\cdot a\# \to e, \qquad a\cdot e \to a\#\#;$$

$$a\#\#\# \to a\#, \qquad a\#\#\cdot b - a\cdot b;$$

$$a\cdot(a\#\cdot b) \to b, \qquad a\#\cdot(a\cdot b) - b;$$

$$(a\cdot b)\# \to b\#\cdot a\#;$$

$$e\# - e, \qquad e^* \to e;$$

$$a^*\cdot b - b, \qquad a\$\cdot b - b;$$

$$a\#\cdot a - a^*, \qquad a\cdot a^* \to a;$$

$$a^{**} - a^*, \qquad (a\cdot b)^* \to b^*;$$

$$a\$\# \to e, \qquad a^*\# - e, \qquad a\#^* \to e, \qquad a\$^* \to a\$.$$

This complete set can be used to solve the original word problem presented by axioms 1, 2, 3, 4.

Note that although, as Clifford showed, systems satisfying axioms 1, 2, 3, 4 are equivalent to (l, r) systems, the *free* systems are quite different. The free system on n generators $g_1, \ldots, g_n$ defined by the axioms 1, 2, 3 of Example 12 has exactly $n+1$ idempotent elements, namely e, $g_1'\cdot g_1, \ldots, g_n'\cdot g_n$; the free system on one generator defined by axioms 1,2,3,4 of the present example has infinitely many idempotent elements, e.g. a$ for each irreducible word a.

Example 16. Central groupoids II. (Compare with Example 6.) A natural model of a central groupoid with n^2 elements is obtained by considering the set S of ordered pairs $\{(x_1, x_2) | x_1, x_2 \in S_0\}$, where So is a set of ***n*** elements. If we define the product $(x_1, x_2)\cdot(y_1, y_2) = (x_2, y_1)$, we find that the basic identity $(a. b) . (b\cdot c) = b$ is satisfied.

If $x = (x_1, x_2)$, it is the product of two idempotent elements $(x_1, x_1)\cdot$ $\cdot (x_2, x_2)$. We have $(x_1, x_1) = (x\cdot x)\cdot x$, and $(x_2, x_2) = x\cdot(x\cdot x)$, and this suggests that we define, in a central groupoid, two unary functions denoted by subscripts 1 and 2, as follows:

1. $(a\cdot a)\cdot a - a_1$
2. $a\cdot(a\cdot a) - a_2$

in addition to the basic axiom

3. $(a\cdot b)\cdot(b\cdot c) - b$

which defines a central groupoid.

For reasons which are explained in detail in [7], it is especially interesting to add the further axiom

4. $a_2\cdot b - a\cdot b$

(which is valid in the "natural" central groupoids but not in all central groupoids) and to see if this rather weak axiom implies that we must have a "natural" central groupoid.

This is, in fact, the case, although previous investigations by hand had been unable to derive the result. The computer started with axioms 1, 2, 3, 4, and after 9 minutes the following complete set of 13 reductions was found :

$$\begin{array}{cccc}
(a_1)_1 \rightarrow \text{al}, & (a_1)_2 - a_1, & (a_2)_1 \rightarrow a_2, & (a_2)_2 \rightarrow a_2; \\
& (a\cdot b)_1 \rightarrow a_2, & (a\cdot b)_2 \rightarrow b_1; & \\
& a\cdot(b\cdot c) - a\cdot b_2, & (a\cdot b)\cdot c - b_1\cdot c; & \\
& a_2\cdot b \rightarrow a\cdot b, & a\cdot b_1 - a\cdot b; & \\
a\cdot a_2 \rightarrow a_2, & a_1\cdot a - a_1, & a_1\cdot a_2 - a. &
\end{array}$$

The computation process generated 54 axioms, of which 24 were used in the derivation of the final set, so the "efficiency rating" was 44%. This is the most difficult problem solved by the computer program so far.

As a consequence of the above reduction rules, the free system on ***n*** generators has $4n^2$ elements.

Example 17. Central groupoids III. If we start with only axioms 1, 2, and 3 of Example 16, the resulting complete set has 25 reductions :

$$\begin{array}{ll}
(a\cdot a)\cdot a \text{ - } \mathbf{al}, & a\cdot(a\cdot a) \to a_2; \\
a_1\cdot a_2 \text{ - } \boldsymbol{a}, & a_2\cdot a_1 \to a\cdot a; \\
a\cdot a_1 \text{ - } a\cdot a, & a_2\cdot a \text{ - } a\cdot a; \\
(a\cdot a)_1 \text{ - } a_2, & (a\cdot a)_2 \to a_1; \\
(a_1)_1\cdot a \text{ - } a_1, & a\cdot(a_2)_2 \to a_2; \\
a_1\cdot(a\cdot b) \text{ - } \boldsymbol{a}, & (a\cdot b)\cdot b_2 \text{ - } \boldsymbol{b}; \\
(a\cdot b)_1\cdot b \text{ - } a\cdot b, & a\cdot(a\cdot b)_2 \text{ - } a\cdot b; \\
(a\cdot b_1)\cdot b \to b_1, & a\cdot(a_2\cdot b) \text{ - } a_2; \\
(a\cdot a)\cdot(a_1)_2 \to a_1, & (a_2)_1\cdot(a\cdot a) \text{ - } a_2; \\
(a\cdot a)\cdot(a_1\cdot b) \text{ - } a_1, & (a\cdot b_2)\cdot(b\cdot b) \to b_1; \\
(a\cdot(b\cdot b))\cdot b_1 \text{ - } b\cdot b, & a_2\cdot((a\cdot a)\cdot b) \text{ - } a\cdot a;
\end{array}$$

$$(a\cdot b)\cdot(b\cdot c) \to \boldsymbol{b};$$

$$a\cdot((a\cdot b)\cdot c) \text{ - } a\cdot b, \qquad (a\cdot(b\cdot c))\cdot c \text{ - } b\cdot c.$$

Of course these 25 reductions say no more than the three reductions of Example 6, if we replace a_1 by $(a\cdot a)\cdot \boldsymbol{a}$ and a_2 by $a\cdot (a\cdot a)$ everywhere, so they have little mathematical interest. They have been included here merely as an indication of the speed of our present program. If these 25 axioms are presented to our program, it requires almost exactly 2 minutes to prove that they form a complete set.

Example 18. Some unsuccessful experiments. The major restriction of the present system is that it cannot handle systems in which there is a commutative binary operator, where

$$\boldsymbol{aob} \equiv \boldsymbol{boa}.$$

Since we have no way of deciding in general how to construe this as a "reduction", the method must be supplemented with additional techniques to cover this case. Presumably an approach could be worked out in which we use ***two*** reductions

$$\alpha \to \beta \text{ and } \beta \to \alpha$$

whenever we find that a $\equiv\beta$ but $\boldsymbol{a}\#\beta$, and to make sure that no infinite looping occurs when reducing words to a new kind of "irreducible" form. At any rate it is clear that the methods of this paper ought to be extended to such cases, so that rings and other varieties can be studied.

We tried experimenting with Burnside groups, by adding the axiom $a\cdot(a\cdot a)$ -e to the set of ten reductions of Example 1. The computer **almost** immediately derived

$$a\cdot(b'\cdot a) \equiv b\cdot(a'\cdot b)$$

in which each side is a commutative binary function of a and b. Therefore no more could be done by our present method.

Another type of axiom we do not presently know now to handle is a rule of the following kind:

$$\text{if a } \neq 0 \text{ then } a\cdot a' \rightarrow e$$

Thus, division rings would seem to be out of the scope of this present study even if we could handle the commutative law for addition.

The "Semi-Automated Mathematics" system of Guard, Oglesby, Bennett, and Settle [6] illustrates the fact that the superposition techniques used here lead to efficient procedures in the more general situation where axioms involving quantifiers and other logical connectives are allowed as well. That system generates "interesting" consequences of axioms it is given, by trial and error; its techniques are related to but not identical to the methods described in this paper, since it uses both "expansions" and "reductions" separately, and it never terminates unless it has been asked to prove or disprove a specific result.

8. **Conclusions.** The long list of examples in the preceding section shows that the computational procedure of § 6 can give useful results for many interesting and important algebraic systems. The methods of Evans [4] have essentially been extended so that the associative law can be treated, but not yet the commutative law. On small systems, the computations can be done by hand, and the method is a powerful tool for solving algebraic problems of the types described in Examples 4 and 6. On larger problems, a computer can be used to derive consequences of axioms which would be very difficult to do by hand. Although we deal only with "identities", other axioms such as cancellation laws can be treated as shown in Examples 9 and 11.

The method described here ought to be extended so that it can handle the commutative law and other systems discussed under Example 18. Another modification worth considering is to change the definition of the well-ordering so that it evaluates the weights of subwords differently depending on the operators which operate on these subwords. Thus, in Example 11 we would have liked to write

$$f(a\cdot b, a) \rightarrow g(a\cdot b, b),$$

and in Example 15 we would have liked to write

$$a' \rightarrow a\# .a\$.$$

These were not allowed by the present definition of well-ordering, but other well-orderings exist in which such rules are reductions no matter what is substituted for a and b.

REFERENCES

1. A. H. CLIFFORD: A system arising from a weakened set of group postulates. Ann. *Math.* 34 (1933), 865-871.
2. A. H. CLIFFORD and G. B. PRESTON: The algebraic theory of semigroups. Math. *Surveys* 7 (Amer. Math. Soc., 1961).
3. L. E. DICKSON: Definitions of a group and a field by independent postulates. *Trans. Amer. Math. Soc.* 6 (1905), 198-204.
4. TREVOR EVANS: On multiplicative systems defined by generators and relations. I. Normal form theorems. *Proc. Cumb. Phil. Soc.* *47* (1951), 637-649.
5. TREVOR EVANS: Products of points-some simple algebras and their identities. *Amer. Math. Monthly 74* (1967), 362-372.
6. J. R. GUARD, F. C. OGLESBY, J. H. BENNETT and L. G. SETTLE: Semi-automated mathematics. *.7. Assoc. Comp. Mach.* 16 (1969), 49-62.
7. DONALD E. KNUTH: Notes on central groupoids. *J. Combinatorial Theory* (to appear).
8. HENRY B. MANN: On certain systems which are almost groups. *Bull. Amer. Math. Soc.* 50 (1944), 879-881.
9. M. H. A. NEWMAN: On theories with a combinatorial definition of "equivalence". *Ann. Math. 43* (1942), 223-243.
10. J. A. ROBINSON: A machine-oriented logic based on the Resolution Principle. *J. Assoc. Comp. Mach.* 12 (1965), 23-41.
11. 0. TAUSSKY: Zur Axiomatik der Gruppen. *Ergebnisse eines Math. Kolloquiums Wien 4* (1963), 2-3.

The application of computers to research in non-associative algebras

LOWELL J. PAIGE

1. Introduction. The number of papers presented here at this conference indicate a wide area of computer applications in algebraic research; group theory, algebraic topology, galois theory, knot theory, crystallography and error correcting codes. I wish to confine my remarks to less specific details, and I will indicate where the computer has been used in my own research and in the work of others involved with non-associative systems.

It seems to me that the computer can and does play different roles in algebraic research.

I would classify the potential of computer assisted research in the following manner:

(A) The computer can provide immediate access to many examples of any algebraic structure so that reasonable conjectures may be formulated for more general (possibly machine free) investigation.

(B) The computer can be used for a search for counter-examples of a general conjecture.

(C) The computer can be used to provide the "proof" required in a mathematical argument.

In the next section, I shall attempt to indicate by means of various examples where the computer has led to success and failure in the categories listed above. Finally, I would like to suggest in the field of Jordan algebras the possibility of computer assistance to attack the general problem of identities in special Jordan algebras.

2. Examples of computer assisted research. My own introduction to computer assistance in research arose in an investigation of complete mappings of finite groups. This problem stems from an early attempt to construct a finite projective plane by means of homogeneous coordinates from a neofield, and the problem for groups may be stated briefly as follows: ***Let G be a finite group (written multiplicatively) and let θ be a bijection of G. For what groups G is the mapping $\eta: x \to x \cdot \theta(x)$ a bijection of* G?**

A complete solution for this problem in the case that G is abelian was obtained in 1947 [1]. I obtained some fragmentary results for non-abelian groups in 1951 [2] and Professor M. Hall generalized the results for the abelian case in 1952 [3].

It was at this time (1953) that I sought help from the computer and obtained a detailed analysis of complete mappings for groups of small order. The memory capacity of SWAC at that time prevented any large-scale analysis, but the results were of such a nature that Professor Hall and I reconsidered the problem. We gave a complete solution to the problem for solvable groups and stated the following conjecture in 1955 [4]:

CONJECTURE: ***A finite group G whose Sylow 2-subgroup is non-cyclic possesses a complete mapping.***

This conjecture has never been verified nor has a counterexample been found. Computers could certainly provide more evidence, but the solution of the problem has rather dubious applications to the original problem of projective planes. There is, however, an interesting footnote to the conjecture. I felt that I could provide a solution if the following published problem of 1954 were true:

PROBLEM. ***Let G be a finite group and S_2 a Sylow 2-subgroup. In the coset decomposition of G by S_2, does there exist an element of odd order in each coset ?***

The problem remained unsolved until Professor John Thompson provided a counterexample in 1965. His example was the group of 2 x 2 unimodular matrices over the Galois Field GF(53). It is easy to see that the Sylow 2-subgroup of Thompson's example is non-cyclic, and there is reason to suppose that this example might provide a counter-example to our original conjecture; however, the order of this group (148,824) makes it seem unlikely that even today's computers would be capable of providing the answer.

My experience with computers and 10 x 10 orthogonal lattice squares was not a particularly successful venture. In 1958, I wrote, "consequently, the total time necessary to do an exhaustive search for latin squares orthogonal to our example would be approximately 4.8 X 10^{11} machine hours". Perhaps the time computation was correct but we are all well aware that the counter-example to Euler's conjecture was provided the next year.

An example of a computer-provided counter-example to another of Euler's conjectures occurred last January when L. J. Lander and T. R. Parkin published the following numerical relation [5] :

$$27^5+84^5+110^5+133^5 = 144^5.$$

Let me turn now to an example from loop theory for a more favorable experience with a "machine suggested" conjecture. First, a brief review of the pertinent loop theory.

Two loops (G, $\cdot$) and $(H, \times)$ are said to be isotopic if there exists a triple of bijections (α, β, γ) of G to H such that

$$(x\alpha)\times(y\beta) = (x\cdot y)\gamma$$

for all x, y of G . Professor R. H. Bruck raised the following problem in 1958 [6]:

Find necessary and sufficient conditions upon a loop G in order that every loop isotopic to G is isomorphic to G.

The answer to this problem, as was pointed out by Bruck, would have interesting interpretations to projective planes.

It is well known that a group G has the property that it is isomorphic to all of its loop isotopes. A student at the University of Wisconsin, working under the direction of Professor H. Schneider, examined all loops of order 7 on a computer and discovered that the only loop isomorphic to all of its loop isotopes was the cyclic group. He has proved subsequently that any loop of prime order satisfying the property that it was isomorphic to all of its loop isotopes must be the cyclic group. Moreover, I understand that he is now considering a generalization of this result to loops of prime power order.

Another example which comes to mind involves a question raised by Professor T. A. Springer [7] concerning elements in a Chevalley group; specifically,

"Is the centralizer, G_x, of a regular unipotent element x, an abelian group ?"

Dr. B. Lou, working under the direction of Professor Steinberg at the University of California, Los Angeles, has given the answer to this question in those cases left open by Springer, and a considerable portion of her work in the associated Lie algebras was done on a computer.

It would be a matter of serious negligence in surveying the applications of computers to non-associative systems if one were not to mention the work of Professor Kleinfeld [8] on Veblen-Wedderburn systems with 16 elements, or that of Professor R. Walker [9] in extending these results to a listing of finite division algebras with 32 elements. Finally, the work of Professor D. Knuth [10] in providing new finite division algebras is an excellent example of computer assisted research.

3. Jordan algebra identities. The problem of determining identities satisfied by the elements of a non-associative algebra is one area in which the computer could be expected to make research contributions. For example, Professor R. Brown of the University of California has discovered an identity in one variable for certain algebras arising in his investigation of possible representations of the Lie group associated with E_7.

Professor M. Osborne of the University of Wisconsin has published all of the possible identities of degree 4 or less for commutative algebras. These were done without the aid of a computer. However, Professor Koecker of Munich has sought computer assistance in determining all possible identities of a non-associative algebra where the degree of the identity is restricted to degree 6 or less. The early estimates of the machine time required for this problem are of the order of 10^7 years and hence it seems appropriate to make rather severe restrictions on the type of identities desired. I would like to illustrate the possible use of the computer with an example from the area of Jordan algebras.

Let us recall a few facts concerning Jordan algebras. An abstract Jordan algebra $\mathfrak{A}$ over a field Φ is a non-associative algebra satisfying the identities

$$\boldsymbol{ab} = \boldsymbol{ba},$$
$$(a^2b)a = a^2(ba)$$

for all $\boldsymbol{a}, \boldsymbol{b} \in \mathfrak{A}$.

The simplest examples of Jordan algebras arise from associative algebras. Thus, let $\mathfrak{A}$ be an associative algebra over a field Φ of characteristic not two. In terms of the associative multiplication of elements in $\mathfrak{A}$, written $a \cdot \boldsymbol{b}$, define a new multiplication

$$\boldsymbol{ab} = \tfrac{1}{2}(a \cdot b + b \cdot a).$$

If we retain the vector space structure of $\mathfrak{A}$ and replace the associative multiplication, $a \cdot b$, by the new multiplication, ***ab*, *we*** obtain a Jordan algebra which we denote by $\mathfrak{A}^+$.

If a Jordan algebra $\mathfrak{J}$ is isomorphic to a subalgebra of an algebra $\mathfrak{A}^+$ ($\mathfrak{A}$ associative), then $\mathfrak{J}$ is called a ***special*** Jordan algebra. One of the fascinating aspects of Jordan algebras is that there exist Jordan algebras which are not special; these Jordan algebras are called exceptional.

The best known example of an exceptional Jordan algebra is constructed as follows : Let C be an eight-dimensional generalized Cayley algebra over the field Φ. Denote the involution in C by x → $\bar{x}$, where $x+\bar{x} \in \Phi$. Consider the set H(C) of 3 X 3 matrices

$$\begin{bmatrix} \alpha & c & \bar{b} \\ \bar{c} & \beta & a \\ b & \bar{a} & \gamma \end{bmatrix},$$

where $\boldsymbol{a}, \beta, \gamma \in \Phi$ and $\boldsymbol{a}, \boldsymbol{b}$, c $\in$ C; i.e. the hermitian 3 ***X*** 3 matrices. Multiplication for the elements of H(C) is the usual Jordan product

$$XY = \tfrac{1}{2}[X \cdot Y + Y \cdot X]$$

and it is not difficult to see that H(C) is a Jordan algebra. Professor A. A. Albert and I [**11**] have shown that H(C) is not the homomorphic image of any special Jordan algebra, and this implies that there are identities satisfied by special Jordan algebras which are not valid for all Jordan algebras. A search for these identities presents interesting possibilities for a computer.

In order that I might sketch a possible attack on the problem of identities in special Jordan algebras, we shall need a few more results about special Jordan algebras which are due to Professor P. M. Cohn.

Let $A^{(n)}$ be the free associative algebra on the set of generators $\{x_1, x_2, \ldots, x_n\}$ and denote by $J_0^{(n)}$ the Jordan subalgebra of $A^{(n)+}$ generated by $\{x_1, x_2, \ldots,$ x,}. On $A^{(n)}$ define a linear mapping x-+x*, the reversal operator, by the equation

$$(x_{i_1}x_{i_2} \ldots x_{i_k})^* = x_{i_k}x_{i_{k-1}} \ldots x_{i_2}x_{i_1}$$

for monomials consisting of products of the generators $x_1, x_2, \ldots, x_n$. Since the monomials form a basis for $A^{(n)}$, the reversal operator * is uniquely determined and

$$(xy)^* = y^*x^*, \quad X^{**} = X$$

for all x, $y \in A^{(n)}$. An element x of $A^{(n)}$ is said to be reversible (symmetric) if $x^* = x$. The set of all reversible elements $H^{(n)}$ of $A^{(n)}$ is easily seen to be a Jordan subalgebra of $A^{(n)+}$; furthermore,

$$H^{(n)} \supseteq J_0^{(n)}$$

for all n. Cohn has shown that

$$H^{(2)} \cong J_0^{(2)} \text{ and } H^{(3)} \cong J_0^{(3)}$$

and otherwise $J_0^{(n)}$ is properly contained in $H^{(n)}$.

The exceptional Jordan algebra ***H(C)*** described earlier is generated by three elements. Hence, it is the homomorphic image of the free Jordan algebra $J^{(3)}$ on three generators. On the other hand, ***H(C)*** is not the homomorphic image of $J_0^{(3)}$ (the free special Jordan algebra on three generators). Thus, we know that the natural homomorphism v from

$$\nu : J^{(3)} \to J_0^{(3)}$$

has a non-zero kernel $K^{(3)}$. A basis for $K^{(3)}$ has not been found. Professor Glennie **[12]** has shown that there are no elements of degree less than 7 in $K^{(3)}$ and that there are elements of degree 8 in $K^{(3)}$. It should be clear that any non-zero element of $K^{(3)}$ will provide an identity for special Jordan algebras which is not valid for all Jordan algebras.

The importance of Cohn's relationship, $\boldsymbol{H}^{(3)} \cong J_0^{(3)}$, lies in the fact that we have an explicit way to write the elements of the free special Jordan algebra $J_0^{(3)}$ in terms of reversible elements. Hence, treating $J_0^{(3)}$ as a graded algebra (by degree), we can compute the number of basis elements of a fixed degree. For example, if we let the generators of $J_0^{(3)}$ be a, ***b*** and c, then the number of basis elements for the vector subspace spanned by all elements of total degree 8 and degrees 3,3 and 2 in ***a, b*** and c respectively is 280.

A computer attack for the determination of the elements in $K^{(3)}$ for the natural mapping

$$\nu : J^{(3)} \to J_0^{(3)}$$

may now be described.

We may linearize the defining identity $(a^2b)a = a^2(ba)$ of a Jordan algebra to obtain the identities:

$$\begin{aligned}&(wx)(yz) + (wy)(zx) + (wz)(xy)\\ &\qquad = [w(xy)]z + [w(yz)]x + [w(zx)]y \qquad (3.1)\end{aligned}$$

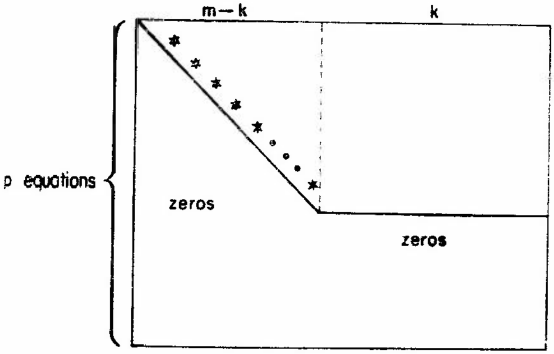
and

$$\begin{aligned}&w[x(yz)] - w[(xy)z]\\ &\qquad = [(wx)z]y + [(wy)z]x - [(wz)x]y - [(wy)x]z. \qquad (3.2)\end{aligned}$$

Again, for convenience, let us denote the generators of $J^{(3)}$ by ***a***, ***b*** and c. If we are interested in the identities of degree 8, then we might as well restrict our attention to identities involving the generators ***a***, ***b*** and c. Moreover, it is known that any identity linear in one of the generators is valid for all special Jordan algebras [13]. Hence, we may begin by considering those of degree 3 in ***a***, degree 3 in ***b*** and degree 2 in c.

We can now proceed to select w, x, y, z in (3.1) and (3.2) in all possible ways so as to yield monomials $a^{\alpha}b^{\beta}c^{\gamma}$ compatible with the total degree being 8 and involving ***a***, ***b*** and c to the total degree 3, 3 and 2 respectively. This will give us a set of homogeneous equations in the various monomial elements of $J^{(3)}$. Many duplications will be present and obvious reductions may be made by using the commutative law. Let us assume that we have p equations in ***m*** elements. The ***m*** elements may be ordered and we proceed to reduce the equations to echelon form.

Graphically, we would reach a stage where our equations would have the form



The diagonal elements would be non-zero and the ***k*** elements would span the vector subspace of elements of $J^{(3)}$ of total degree 8 and degree 3, 3 and 2 in ***a***, ***b*** and c. We know that $k \geqslant 280$, since the homomorphism v would imply that a similar reduction could be made for the corresponding elements of $J_0^{(3)}$.

If $k = 280$, then we could show that v was bijective on the elements of degree 8 and of the form we are considering. This is not the case.

If $k > 280$, then we could select 281 of the k elements and take their images in $J_0^{(3)}$. We could then express one of these elements in terms of the other 280 and this would provide an identity valid in $J_0^{(3)}$ and ***not*** in $J^{(3)}$; hence an element of $K^{(3)}$. In this manner we would probably obtain K- 280 elements of $K^{(3)}$ and consequently a basis for $K^{(3)}$.

The beginning of this program had been established when Professor Glennie informed me of a method which appeared to be more promising. Details will be found in the following paper in this volume.

REFERENCES

1. L. J. PAIGE: A note on finite Abelian groups. *Bull. Amer. Math. Soc. 53 (1947),* 590–593.
2. L. J. PAIGE: Complete mappings of finite groups. *Pacific J. Math.* 1 (1951), 111-1 16.
3. MARSHALL HALL JR.: A combinatorial problem on Abelian groups, *Proc. Amer. Math. Soc. 3 (1952), 584-587.*
4. MARSHALL HALL and L. J. PAIGE: Complete mappings of finite groups. *Pacific* J. ***Math.*** 5 (1955), 541-549.
5. L. J. LANDER and T. R. PARKIN: A counterexample to Euler's sum of powers conjecture. *Math. Comp.* 21(1967), 101-102.
6. R. H. BRUCK: *A Survey of Binary Systems,* pp. 59-60 (Springer-Verlag, 1958).
7. T. A. SPRINGER: Some arithmetical results on semi-simple Lie algebras. *Pub. Math. Inst. Des Hautes Etudes Scientifique, 30* (1966), 475-498.
8. ERWIN KLEINFELD: Techniques for enumerating Veblen-Wedderburn systems. *J. Assoc. Comp. Mach. 7* (1960), 330-337.
9. R. J. WALKER: Determination of division algebras with 32 elements. *Proc. Symp. App. Math. Amer. Math. Soc.* 15 (1962), **83–85.**
10. DONALD E. KNUTH: Finite semifields and projective planes. *J. of Algebra* 2 (1965), 182-217.
11. A. A. ALBERT and L. J. PAIGE: On a homomorphism property of certain Jordan algebras. *Trans. Amer. Math. Soc. 93* (1959), 20-29.
12. C. M. GLENNIE: Some identities valid in special Jordan algebras but not valid in all Jordan algebras. *Pacific J. Math.* 16 (1966). 47-59.
13. I. G. MACDONALD, Jordan algebras with three generators. *Proc. London Math. Soc.* (3) 10 (1960), 395-408.

Identities in Jordan algebras

C. M. Glennie

THE main part of this paper is the calculation of the dimensions of certain subspaces of Jordan algebras. From a knowledge of these dimensions we deduce a theorem on identities in Jordan algebras. This is given in the third and fmal section. In the first section we set up some notation and give some preliminary results. The results are not new but it is convenient to gather them together here. The second section gives the statement and proof of the main theorem. The reader should consult the preceding paper by L. J. Paige in this volume for background material.

1. We shall work throughout over a fixed but arbitrary field of characteristic zero and shall not refer to the ground field again. The restriction on the characteristic can almost certainly be relaxed but this would require further investigation which we have not carried out. We shall be working in certain free Jordan and free associative algebras and shall use $a, b, c, \dots$ to denote the free generators. In particular places we shall writep, q, r, . . . instead of $a, b, c, \dots$ when the result we are stating remains true if the variables are permuted or if we wish to indicate a typical monomial. The element $pqrs+srqp$ in an associative algebra will be denoted by $\overline{pqrs}$, and called a tetrad. Similarly $pqrst + tsrqp$ is $\overline{pqrst}$ and so on. Tetrads such as $\overline{abcd}$, $\overline{dcba}$, $\overline{acef}$, $\overline{feca}$ in which the letters appear in alphabetical or reversed alphabetical order will be called ordered tetrads. As associative products occur only under bars we shall also use juxtaposition to denote the Jordan product $\frac{1}{2}\overline{pq}$. Products in the Jordan algebras will be left normed, i.e. xyz means $(xy)z$ and so on. We use the following notation.

$L(n)$ subspace of the free Jordan algebra on n generators spanned by monomials linear in each generator,

$M(n)$ subspace of the free special Jordan algebra on n generators spanned by monomials linear in each generator,

$N(n)$ subspace of the free associative algebra on n generators spanned by the $\frac{1}{2}n!$ elements $\bar{w}$ arising from the $n!$ monomials w linear in each generator,

$S(n)$ ($n \geqslant 2$) subspace of L(n) spanned by monomials pw where w is a monomial linear in each of the generators other than p,

$T(n)$ (n $\geqslant$ 3) subspace of L(n) spanned by monomials pqw where w is a monomial linear in each of the generators other than p and q,

$U(n)$ (n $\geqslant$ 2) subspace of s(n) spanned by monomials pw with $p \neq a$,

$V(n)$ (n $\geqslant$ 3) subspace of $T(n)$ spanned by monomials pqw with $p \neq$ a and $q \neq$ a,

$[W]$ subspace spanned by the subset W of a vector space,

$R(x)$ the mapping y $\rightarrow$ yx, x and y elements in the Jordan algebra under consideration,

$P(x, y, z)$ $R(x)R(yz)+R(y)R(zx)+R(z)R(xy)$,

$Q(x, y, z)$ $R(yz)R(x)+R(zx)R(y)+R(xy)R(z)$,

$S(x, y, z)$ $R(x)R(z)R(y)+R(y)R(z)R(x)$.

With the above notation the linearized form of the Jordan identity $xyy^2 = xy^2y$ is

$$xP(y, z, t) = xQ(y, z, t) \tag{1}$$

or

$$xR(yzt) = xP(y, z, t)-xS(y, z, t). \tag{2}$$

From (1) and (2) we have at once

$$xR(yzt) = xQ(y, z, t)-xS(y, z, t). \tag{3}$$

It is clear that $M(n) \subseteq N(n)$. We have also

Lemma 1. *For $n \geqslant 3$, $U(n)+V(n) = L(n)$.*

Proof. Let w $\in L(n)$. Then w is a sum of elements aR where R is a monomial in operators $R(x)$ and each x is a monomial in some of the generators $b, c, \ldots$. If x contains more than two generators then by (2) $R(x)$ can be expanded as a sum of words $R(y)$ where each y contains fewer generators than x. Repeating such expansions as often as necessary gives the result.

Corollary. *5'(n) $+\,T(n) = L(n)$ and $S(n)+V(n) = L(n)$.*

Lemma 2. dim $S(n) \leqslant$ n dim $L(n-1)$, dim $T(n) \leqslant \frac{1}{2}n(n-1)$ dim $L(n-2)$, dim $U(n) \leqslant$ (n $-$ 1) dim $L(n-1)$, dim $V(n) \leqslant \frac{1}{2}(n-1)(n-2)$ dim $L(n-2)$.

Proof. The proofs of these inequalities follow at once from the definitions of S(n), etc.

The following relations, in which $p, q, r, \ldots$ denote distinct elements from $b, c, d, \ldots$ and x is a monomial in the remaining generators, are either clear from the definitions of the operators or follow easily from (1), (2), (3) and previous relations in the set.

$$xQ(p, q, r) \in U(n) \tag{4}$$

$$xP(p, q, r) \in U(n) \tag{5}$$

$$xS(p, q, r) \in U(n) \tag{6}$$

$$xR(pqr) \in U(n) \tag{7}$$

$$x(qr(st)) - xQ(q, r, st) \in U(n) \tag{8}$$

$$x(qr)(st) - xQ(q, r, st) \in U(n) \tag{9}$$

$$xp(qr(st)) - xP(p, qr, st) \in U(n) \tag{10}$$

$$x(qrp)(st) + x(stp)(qr) - xQ(p, qr, st) \in U(n). \tag{11}$$

The following lemmas are due to Cohn. Proofs will be found in [1].

LEMMA 3. *abed-(sgn π)pqrs $\in M(4)$ where p, q, r, s is the permutation π of a, b, c, d.*

LEMMA 4. *$M(n) + [W(n)] = N(n)$ for $n = 1, \ldots, 7$ where $W(n) = \phi$ (the empty set) for $n = 1, 2, 3$, $W(4) = \{abcd\}$, $W(5) = \{pqrst\}$, $W(6) = \{pqrstu+pqrsut,\ pqrs(tu),\ pqrstu-pqrsut\}$, $W(7) = \{pqrstuv+pqrsutv,\ pqrs(tu)v,\ pqrstuv-pqrsutv\}$. In the cases $n = 5, 6, 7$ the set is to include all elements obtained by replacing p, q, r, ... by any permutation of a, b, c, ... such that pqrs is an ordered tetrad.*

Let U be a subspace of the vector space V and $W = \{w_1, \ldots, w,\}$ be a subset of V. If r_i $(i = 1, \ldots, m)$ denotes the relation

$$\sum_{j=1}^{n} \lambda_{ij} w_j \in U$$

amongst the elements of W and $R = \{r_1, \ldots, r_m\}$ we shall call the $m \times n$ matrix $\Lambda = (\lambda_{ij})$ the word-relation matrix for *W and R.* We have

LEMMA 5. dim $(U+[W]) \leqslant$ dim U+(n-rank A).

Proof. Let r = rank A. We can find r elements from W each expressible as a linear combination of some element in U and the remaining n-r elements of W. So $U+[W]$ is spanned by any basis of U together with n-r elements from W, and the result follows.

2. THEOREM 1. *For $n = 1, \ldots, 7$, dim $L(n)$ = dim $M(n)$. The dimensions are respectively* 1, 1, 3, 11, 55, 330, 2345.

Proof. The mapping $a \to a$, $b \to b$, etc., can be extended to a linear transformation of $L(n)$ onto $M(n)$. So dim $M(n) \leqslant$ dim $L(n)$. For each n we now find a number $d(n)$ such that dim $L(n) \leqslant d(n)$ and dim $M(n) \geqslant d(n)$. It follows at once that dim$L(n)$ = dim $M(n) = d(n)$. We shall use w(n) to denote the number of elements in $W(n)$. For simplicity we write L for $L(m)$ and so on when dealing with the case $n = m$.

$n = 1$. Take $d = 1$. L is spanned by a single monomial. So dim $L \leqslant d$. By Lemma 4, $M = N$. So dim M = dim $N = 1 \geqslant d$.

$n = 2$. Take $d = 1$. L is spanned by the single monomial ab. So dim $L \leqslant d$. By Lemma 4, $M = N$. So dim M = dim $N = 1 \geqslant d$.

$n = 3$. Take $d = 3$. L is spanned by abc, bca, cab. So dim $L \leqslant d$. By Lemma 4, $M = N$. So dim M = dim $N = 3 \geqslant d$.

$\boldsymbol{n} = 4$. Take $\boldsymbol{d} = 11$. $\boldsymbol{L}$ is spanned by the twelve monomials *upqr;* $ap(qr)$, $a(pq)r$ (see proof of Lemma 1). These are subject to the relation

$$aP(b, c, d) = aQ(b, c, d)$$

and the word-relation matrix has rank 1. So by Lemma 5 (with $U = \{0\}$) dim $\boldsymbol{L} \leqslant 11 = \boldsymbol{d}$. From Lemma 4 we have that $M + [W] = \mathrm{N}$ where $w = 1$. So $\dim M \geqslant \dim N - \dim\ [W] \geqslant \dim N - w \geqslant$ 12-1 $= 11 = \boldsymbol{d}$.

$\boldsymbol{n} = 5$. Take $\boldsymbol{d} = \boldsymbol{55}$. Since $pqr(st) = stR(pqr) = \boldsymbol{stQ(p, q}, r) - stS(p, \boldsymbol{q}, \boldsymbol{r})$ we have that $\boldsymbol{V} \mathbf{C}\ U$ and $U = \boldsymbol{L}$. Then dim $\boldsymbol{L}$ = dim $U \leqslant 5$ dim $\boldsymbol{L(4)} =$ $= 5 \times 11 = 55 = d$. From Lemma 4, $M + [W] = N$ with $w = 5$. So dim $\boldsymbol{M} \geqslant$ dim N $-$ w $= 60 - 5 = 55 = \boldsymbol{d}$.

$n = 6$. Take $\boldsymbol{d} = 330$. From Lemma 2, dim $U \leqslant 5$ dim $\boldsymbol{L(5)} = \boldsymbol{275}$. $\boldsymbol{V}$ is spanned by (i) 60 elements $apqr(st)$, (ii) 30 elements $a(pq)r(st)$, (iii) 30 elements $ap(qr)(st)$. From (1), (8), (9), (10), (11) we have

$$ap(qr)(st) - a(qrp)(st) - a(stp)(qr) \in U.$$

Defining $T(p, \boldsymbol{q}, \boldsymbol{r}; \boldsymbol{s}, \boldsymbol{t})$ as

$$[Q(q, r, \mathrm{P}) - S(q, r, p)]R(st) + [Q(s, t, \mathrm{P}) - S(s, t, p)]R(qr)$$

we have

$$ap(qr)(st) - aT(p, q, r, s, t) \in U. \tag{12}$$

Also, from (5):

$$apqP(r, s, t) \in U \tag{13}$$

$$a(pq)P(r, s, t) \in U. \tag{14}$$

and from (1) :

$$aP(p, q, r)R(st) - aQ(p, q, r)R(st) \in U. \tag{15}$$

(12) to (15) give respectively 30, 20, 10, 10 relations. Setting up the word-relation matrix for the 120 spanning elements of $\boldsymbol{V}$ and these 70 relations we get a 70×120 matrix of which the rank is 65. Then by Lemma 5, dim $(U + \boldsymbol{V}) \leqslant$ dim $U + (120 - 65)$. So

$$\dim \boldsymbol{L} \leqslant \dim (U + \boldsymbol{V}) \leqslant 275\mathrm{f}\ 55 = 330 = \boldsymbol{d}.$$

From Lemma 4, $\boldsymbol{M}$**+** [W] = N with w = 45. Now let $\boldsymbol{W'}$ be the subset of $\boldsymbol{W}$ consisting of the 30 elements $pqrstu + \overline{pqrsut}$, $\overline{pqrs}(tu)$, and let N' = $= \boldsymbol{M}$**+** $[\ W']$. We have 45 relations amongst elements of $\boldsymbol{W}$- W' obtained from

$$\overline{\boldsymbol{abcdef}} - \overline{\boldsymbol{abcdfe}} + \overline{\boldsymbol{bcdefa}} - \overline{\boldsymbol{bcdeaf}} + \overline{\boldsymbol{cdefab}} - \overline{\boldsymbol{cdefba}} + \overline{\boldsymbol{acdfeb}} \text{-} \overline{\boldsymbol{acdfbe}} \in N' \tag{16}$$

by permuting $\boldsymbol{a}, \boldsymbol{b}$, c, d, e, f and using Lemma 3. We have a further 6 relations obtained from

$$\overline{cdefab} - \overline{cdefba} + \overline{\boldsymbol{defbac}} \text{-} \overline{\boldsymbol{defbca}} + \overline{efbcad} - \overline{\boldsymbol{efbcda}}$$
$$+ \overline{fbcdae} - \overline{fbcdea} + \overline{\boldsymbol{bcdeaf}} - \overline{\boldsymbol{bcdefa}} \in \boldsymbol{N} \tag{17}$$

by permuting a, b, c, d, e, f and using Lemma 3. (16) is the linearized form of

$$abcdab-abcdba \in N'$$

which comes from

$$\overline{ac}db^2a - cdb^2aa + cdb^2a^2 \quad bdca^2b + \overline{dca^2b}b - \overline{dca}^2b^2 = 0$$

using Lemma 3 and

$$\overline{pqrst} = \overline{qrstp}-\overline{rstpq}\overline{fstpqr}- \quad \overline{tpqrs}+\overline{pqrst}. \tag{18}$$

(17) comes from $\sum(\overline{cdef}ub- \overline{cdef}(ab)) = 0$ where the sum is taken over the cyclic permutations of b, c, d, e, f and Lemma 3 is used where necessary. The rank of the word-relation matrix for the 15 elements in $W- W$ and the 51 relations above is 15. So dim N = dim $(N'+$ [W- $W'])\leqslant$ dim $N'+15-15=$ dim N'. Whence N = N'. So dim $M\geqslant$ dim N-30 = 360-30 = 330 $= d$.

$n = 7$. Take $d = 2345$. From Lemma 2, dim S $\leqslant$ 7 dim $L(6) = 7x330 =$ $= 2310$. V is spanned by elements of types (i) $apqrs(tu)$, (ii) $a(pq)rs(tu)$, (iii) $ap(qr)s(tu)$, (iv) $apq(rs)(tu)$, (v) $a(pq)(rs)(tu)$. Now $tuR(apqrs)$, $tuR(a(pq)rs)$, $tuR(apq(rs))$, and $tuR(a(pq)(rs))$ are in S. This follows at once on expanding the operator R using (3) and then using (3) again where necessary. So $L = S+ V$ is spanned by S and the set of 180 elements $ap(qr)s(tu)$. Now let X be the set of the 48 elements of type (iii) in which $q = b$ and $t = c$ or $q = c$ and $t = b$. Consider the following table, in which each element is to represent the set of elements obtained from it by replacing p, q, r, s by all permutations of d, e, f, g:

	$ap(bq)r(cs)$	$ap(cq)r(bs)$	
$ap(qr)b(cs)$	$ap(bq)c(rs)$	$ap(cq)b(rs)$	$ap(qr)c(bs)$
$ab(pq)r(cs)$	$ap(qr)s(bc)$	$ap(bc)q(rs)$	$ac(pq)r(bs)$
$ab(cp)q(rs)$	$ab(pq)c(rs)$	$ac(pq)b(rs)$	$ac(bp)q(rs)$

Each element in the table can be expressed modulo S as a linear combination of elements in higher rows. Thus, for example:

$$ap(qr)b(cs) = -ap(bq)r(cs)-ap(br)q(cs) \pmod{S}$$

since $apQ(q, r, b)R(cs) = apP(q, r, b)R(cs)$ and the elements in this last expression are all of type (iv) and so in S. The expression for $ab(cp)q(rs)$ arises from

$$cpQ(a, b, q)R(rs)+rsQ(a, c, p)R(bq) + bqQ(a, r, s)R(cp) - aQ(bq, cp, rs) \in S.$$

So we now have that $S+$ [X] $= L$. But there are further relations modulo S amongst the elements of X. These are:

$$\sum ap(bq)r(cs) \in S \tag{19}$$

$$\sum ap(cq)r(bs) \in S, \tag{20}$$

where in each case s is fixed as one of d, e, f, g, and the sum is taken as p, q, r run over all the permutations of the remaining variables, and

$$ap(bq)r(cs) + ap(cq)r(bs) - ar(bp)s(cq) - ar(cp)s(bq) \in S, \tag{21}$$

where the sum is taken as p, q run over the permutations of two of the variables and r, s over the permutations of the remaining two. For (19) it is sufficient to show that $ap(bp)p(cs)$is in S for (19) can then be obtained by linearization. But $2ap(bp)p(cs) + abpp(cs) \in S$ and $abp^2p(cs) = abpp^2(cs) \in S$ (20) is obtained similarly. (21) is the linearized form of $ap(bp)r(br) - ar(bp)r(bp) \in S$. Now

$$\begin{aligned}8[ap(bp)r(br) - ar(bp)r(bp)] &\equiv 8\,[ap(bp)r(br) + ap(br)r(bp) + ar(br)p(bp)]\\ \text{(by (19) and (20))} \qquad &\equiv 2(abp^2br^2 + apr^2pb^2 + arb^2rp^2)\\ &\equiv - a[R(b^2p^2)R(r^2) + R(p^2r^2)R(b^2)]\\ &\quad + R(r^2b^2)R(p^2)\\ &\equiv aP(b^2, p^2, r^2) \equiv 0 \text{ (all congruences mod S).}\end{aligned}$$

We now have 14 relations (4 each of (19) and (20) and 6 of (21)) amongst the 48 elements of X, and the word-relation matrix has rank 13. So

$$\dim L = \dim (S + U) \leqslant \dim S + (48 - 13) \leqslant 2310 + 35 = 2345 = d.$$

Now $M + [W] = N$ from Lemma 4. If W' consists of the 210 elements $pqrstuv + \overline{pqrs}utv$, $\overline{pqrs}(tu)v$ it follows from work done in the $n = 6$ case that $M + [W'] = N$. Also we have

$$pqrsqsp + pqrssqp + qprspsq + qprsspq \in M. \tag{22}$$

To establish (22) we use the following (congruences are modulo M):

$$\begin{aligned}8p^2q^2rs^2 &= p^2q^2rs^2 + \overline{q^2p^2rs^2} + \overline{rq^2p^2s^2} + \overline{rp^2q^2s^2}\\ &\equiv 8\overline{pq^2rs^2p} + 8\overline{qp^2rs^2q}\\ \overline{pq^2rs^2p} &\equiv 2rs^2pqqp \equiv 4pqrsqsp\\ \overline{pq^2rs^2p} &\equiv 2pq^2rssp \equiv 4rspqsqp \equiv 4pqrssqp\end{aligned}$$

and the relations obtained by interchanging p and q. If we linearize (22) and substitute all permutations of a, b, c, d, e, f, g we obtain 315 relations corresponding to the 3 15 words $pq(rs)t(uv)$. But we know that dim $(S + U)$ -dim $S \leqslant 35$. So at most 35 of these relations are linearly independent. If we choose 35 relations corresponding to 35 words in U which are linearly independent mod S we can set up the word-relation matrix for these and the 105 words of W' involved in them. The rank of this matrix is 35 (see comment at end of proof of theorem). So dim $M \geqslant$ dim N-(210-35) = 2345 = d. This completes the proof of the theorem.

Comment. The proof requires at several stages the calculation of the rank of a matrix. In all cases but the last this calculation was carried out by hand. The work involved is not as bad as might be feared because of the large number of zero entries and the pattern of blocks within the matrix. For the last matrix (which has 35 rows and 105 columns) use was made of the KDF9 computer at Edinburgh University. The program was designed to print out a basis for the space of vectors x such that $xA = 0$ for a given matrix A. In the present case the matrix was augmented by five rows known to be linearly dependent on the chosen 35. The print-out showed correctly the known linear dependences and this was regarded as being a check on the accuracy of the program.

3. In [2], the cases $n \leqslant 5$ of Theorem 1 were proved although no explicit values for the dimensions were established. An example of an identity in three variables valid in all special Jordan algebras but not valid in all Jordan algebras was given. This identity is of total degree 8, so in a linearized form shows that Theorem 1 is not valid for $n > 7$. The following theorem, which is a corollary of Theorem 1, bridges the gap left in [2] for $n = 6, 7$.

THEOREM 2. *A multilinear identity of total degree 6 or 7 which is valid in all special Jordan algebras is valid in all Jordan algebras.*

It should be possible using the methods of Part 2 to find dim $L(8)$, dim $M(8)$ and the degree 8 multilinear identities holding in special Jordan algebras but not in all Jordan algebras. These correspond to the elements in the kernel of the canonical linear transformation of $L(8)$ onto $M(8)$.

I should like to record my gratitude to Mr. J. K. S. McKay for his encouragement in general and his help with the programming and computer work in particular.

REFERENCES

1. P. M. COHN: On homomorphic images of special Jordan algebras. *Canadian* J. Maths, 6 (1954), 253-264.
2. C. M. GLENNIE: Some identities valid in special Jordan algebras but not valid in all Jordan algebras. *Pacific J. Maths.* 16 (1966), 47-59.

On property D neofields and some problems concerning orthogonal latin squares

A. D. KEEDWELL

THE concept of the property D neofield arose from the attempt to find an explanation for the non-existence of pairs of orthogonal latin squares of order 6. The intention was to formulate a standard method of constructing a pair of orthogonal squares of any sufficiently small order r distinct from 6. The reason for failure when $r = 6$ could then be observed.

The standard method devised (which is reported fully in [**1**]) is essentially a modification of the Bose method for constructing a complete set of mutually orthogonal latin squares from a field. This construction can be exhibited as follows. One square L_1 is the Cayley table of the addition group of the field and its rows may be regarded as permutations $S_0 \equiv \boldsymbol{I}, S_1, S_2, \ldots, S_{r-1}$ of its first row. If $0, 1, x, \ldots, x^{r-2}$, denote the elements of the field, the remaining squares L_i^* ($i = 2, 3, \ldots, r-1$) are as follows

$$L_i^* = \begin{array}{|llll}
\hline
0.M^{i-1}S_0 & 1.M^{i-1}S_0 & & x^{r-2}M^{i-1}S_0 \\
0.M^{i-1}S_1 & 1.M^{i-1}S_1 & \vdots\,. & x^{r-2}M^{i-1}S_1 \\
\ldots & \cdot \quad \cdot & & \ldots \\
0.M^{i-1}S_{r-1} & 1.M^{i-1}S_{r-1} & \ldots & x^{r-2}M^{i-1}S_{r-1}
\end{array}$$

where $\boldsymbol{M} \equiv (0)(1\, x\, x^2 \ldots x^{r-2})$ and the first columns of all the squares are the same.

Since the squares $L_1 = \{S_0, S_1, \ldots, S_{r-1}\}$ and $L_2^* = \{MS_0, MS_1, \ldots, MS_{r-1}\}$ are orthogonal, it follows from a theorem due to H. B. Mann that the permutations $S_0^{-1}MS_0, S_1^{-1}MS_1, \ldots, S_{r-1}^{-1}MS_{r-1}$ are a sharply transitive set. Conversely, when these permutations form a sharply transitive set, the squares L_1 and L_2^* will be orthogonal. It is useful to observe that, again by a result due to H. B. Mann, the squares L_1 and $L_2 = \{MS_0M^{-1}, MS_1M^{-1}, \ldots, MS_{r-1}M^{-1}\}$ will also be orthogonal. Moreover, the permutations MS_iM^{-1}, being conjugate to the permutations S_i, are easy to compute, and the squares L_1 and L_2 have the same first row.

When we exhibit the permutations $S_i^{-1}MS_i$ as in Diagram 1, we observe that the $\boldsymbol{r} \times \boldsymbol{r}$ matrix obtained is the Cayley table of the addition group of the field, and that, if the first row and column are disregarded, the quotients of the elements in corresponding places of any two adjacent secondary diagonals are constant. Moreover, in each such diagonal, the element of the pth row and qth column is x times the element of the $(p+1)$th row and $(q-1)$th column, so each element appears exactly once in each secondary diagonal. Since the equation $1+x^s=0$ is soluble in the field, one secondary diagonal consists entirely of zeros.

$$\begin{array}{lcllll}
M & = & (0)(1 & x & \dots & x^{r-2}) \\
S_{r-1}^{-1}MS_{r-1} & = & (x^{r-2})(1+x^{r-2} & x+x^{r-2} & \dots & x^{r-2}+x^{r-2}) \\
S_{r-2}^{-1}MS_{r-2} & = & (x^{r-3})(1+x^{r-3} & x+x^{r-3} & \dots & x^{r-2}+x^{r-3}) \\
 & & \cdots & \cdots & \cdots & \cdots \\
 & & \cdots & \cdots & \cdots & \cdots \\
S_2^{-1}MS_2 & = & (x)(1+x & x+x & \dots & x^{r-2}+x) \\
S_1^{-1}MS_1 & = & (1)(1+1 & x+1 & \dots & x^{r-2}+1)
\end{array}$$

***Diagram* 1**

The above observations lead us to the realization that a sufficient condition for the existence of a pair of orthogonal latin squares of order r is that an (r- 1) x (r- 1) matrix A_r^* should exist with the following properties: (i) the integers 0 to r- 1 appear at most once in each row and column, and the integer $(r$- $1)-$ i never occurs in the ith row; (ii) the main secondary diagonal consists entirely of $(r$- 1)'s; (iii) all other secondary diagonals comprise the elements 0, I,. . ., $(r$-$2)$ written cyclically; and (iv) the differences between the elements in corresponding places of each two adjacent secondary diagonals (excluding the main secondary diagonal) are all distinct and none is equal to 1. For the details, see [**1**]. We exhibit an example of such a matrix for the case $r=10$ in Diagram 2.

$$\begin{array}{ccccccccc}
5 & 3 & 0 & 2 & 7 & 6 & 1 & 4 & 9 \\
2 & 8 & 1 & 6 & 5 & 0 & 3 & 9 & 4 \\
7 & 0 & 5 & 4 & 8 & 2 & 9 & 3 & 1 \\
8 & 4 & 3 & 7 & 1 & 9 & 2 & 0 & 6 \\
3 & 2 & 6 & 0 & 9 & 1 & 8 & 5 & 7 \\
1 & 5 & 8 & 9 & 0 & 7 & 4 & 6 & 2 \\
4 & 7 & 9 & 8 & 6 & 3 & 5 & 1 & 0 \\
6 & 9 & 7 & 5 & 2 & 4 & 0 & 8 & 3 \\
9 & 6 & 4 & 1 & 3 & 8 & 7 & 2 & 5
\end{array}$$

Diagram 2

A matrix A_r^* having the above properties is completely determined by its first row and may easily be obtained by computer by successive trial.

We require a first row $e_0, e_1, \ldots, e_{r-3}$ such that (i) the e_i are all different and are the integers $0, 1, \ldots, r-3$ in some order, (ii) the $r-3$ differences $d_i = e_i - e_{i-1}$ are all different (taken modulo $(r-1)$) and are the integers $2, 3, \ldots, r-2$ in some order, and (iii) the elements $e_i - i$ (for $i = 0, 1, \ldots, r-3$) are all different modulo $(r-1)$ and are the integers $0, 1, \ldots, r-3$ in some order.

It is necessary and sufficient for the existence of an array A_r^* that a property D neofield of order r should exist, and the recognition of this fact allows the above computer search to be made more economic. A neofield N is called a property D neofield if (i) its multiplicative group is cyclic, and (ii) there exists a generator x of N such that $(1+x^t)/(1+x^{t-1}) = (1+x^u)/(1+x^{u-1})$ implies $t = u$ for all integers t, u (taken modulo $r-1$). The divisibility property (ii) will be referred to as property D. It is easy to see that the Cayley table of the addition loop of such a neofield, with first row and column deleted, forms an array A_r^* if we replace powers of x by their indices and 0 by $r-1$. Since $1+1=0$ in a neofield of even order and $1+x^{(r-1)/2} = 0$ in a neofield of odd order (see [3]), it follows that the integer i must not occur in the ith column of an array A_r^* when r is even and that there is a corresponding restriction when r is odd. Thus, for example, when r is even, we know that $e_i \neq i \pm 1$, and this fact reduces the time required for the search for arrays A_r^* considerably.

A study of property D neofields leads to a number of interesting conjectures.

(i) Do there exist property D neofields of all finite orders r except 6? Certainly this is true for all $r < 21$.

(ii) Can it be proved that both commutative and non-commutative D-neofields exist for all $r > 14$ and that the number of isomorphically distinct D-neofields of assigned order r increases with r?

(iii) Do there exist planar property D neofields which are not fields? None of those so far obtained by the author are planar either in the sense of Paige [3] or of Keedwell [1], as is proved in [2].

(iv) Is it true that, if a finite D-neofield of even order has characteristic 2 (or, equivalently, has the inverse property), then it is a field? Is the result true when the neofields in question are restricted to being commutative?

It remains to explain the non-existence of matrix arrays A_r^* when $r = 6$. As explained in detail in [1], the necessary and sufficient condition for the existence of an array A_r^* (or of a property D neofield of order r) may be re-formulated as follows : “A necessary and sufficient condition that an array A_r^* exists for a given integer r is that the residues $2, 3, \ldots, r-2$, modulo $(r-1)$, can be arranged in a row array P_r in such a way that the partial sums of the first one, two, $\ldots$, $(r-3)$, are all distinct and non-zero modulo $(r-1)$ and so that, in addition, when each element of the array is reduced by 1, the new array P_r' has the same property.” In the case when $r = 6$, P_r comprises the integers 2, 3, 4 and P_r' comprises 1, 2, 3. Since

$2+3=0$ (mod 5), we require that the integers 2, 3 be not adjacent in either array, and this is clearly impossible. Thus, the non-existence of orthogonal latin squares of order six appears to be due to a combinatorial accident.

Our general method for the construction of a pair of mutually orthogonal latin squares of assigned order r may easily be extended to give a method for constructing triples. It is easy to see that the latin squares $L_1 = \{S_0, S_1, . . , S_{r-1}\}$, $L_2^* = \{MS_0, MS_1, . . . , MS_{r-1}\}$, and $L_3^* = \{M^2S_0, M^2S_1, . ..) M^2S_{r-1}\}$, where $M \equiv$ (I- 1) (0 1 . . . r-2) and $S_0 \equiv I, S_1, \ldots, S_{r-1}$ are permutations of the natural numbers 0, 1, . . . , $r-1$, will be mutually orthogonal provided that the two sets of permutations $S_i^{-1}MS_i$ and $S_i^{-1}M^2S_i$, $i = 0, 1, \ldots$ **r** – 1, are both sharply transitive on the symbols 0, 1, ... $r-1$. Since $S_i^{-1}M^2S_i = (S_i^{-1}MS_i)^2$, it is clear from Diagram 3 that a sufficient condition for the existence of such a triple of mutually orthogonal latin squares of order 10 is that a 9×9 matrix ***A* = *(a,)*, *i* =** 1 to 9, $j = 0$ to 8, exist with the properties:

(i) each of the integers 0, 1, . . . , 9 occurs at most once in each row and column, and the integer ***i*** does not occur in the ***(i+*** 1)th column or the (9 – i)th row;

(ii) if $a_{1j_1} = a_{2j_2} = . . . = a_{9j_9} = \boldsymbol{r}$ then (a) the integers $r+1$, a_{1j_1+1}, $a_{2j_2+1}, \ldots, a_{9j_9+1}$ are all different (all addition being modulo 9), $r = \boldsymbol{0}$, 1, 2, . ..) 8, and (b) the integers $r+2$, a_{1j_1+2}, $a_{2j_2+2} \ldots$, a_{9j_9+2} are all different ;

(iii) if $a_{1j_1} = a_{2j_2} = . . . = a_{9j_9} = 9$ then (a) the integers 9, $\boldsymbol{a}_{j_1+1}$, $a_{2j_2+1}, \ldots, a_{9j_9+1}$ are all different, and (b) the integers 9, $\boldsymbol{a}_{j_1+2}$, a_{2j_2+2}, . . . , $\boldsymbol{a}_{j_9+2}$ are ail different.

To the disappointment of the author, it turns out that the arrays A_9^* corresponding to the property ***D*** neofields of order 10 have properties (i), (ii) (a), (iii) (a), and (iii) (b), but fail to satisfy property (ii) (b).

For the purpose of searching for 9×9 matrices of type ***A,*** a computer programme was written which would insert successively the integers a_{10}, $a_{11}, \ldots, a_{98}$ and would backtrack to the preceding place in the event that a place could not be filled successfully. Details of the construction of this programme so as to require as few instructions as possible, of the computer time needed, and of the results appear in [1] and so need not be repeated here.

$$\begin{array}{lcl}
S_0^{-1}MS_0 & = & (9)(0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8) \\
S_1^{-1}MS_1 & = & (8)(a_{10} \quad a_{11} \quad a_{12} \quad a_{13} \quad a_{14} \quad a_{15} \quad a_{16} \quad a_{17} \quad a_{18}) \\
\ldots & \ldots & \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
\ldots & \ldots & \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
S_9^{-1}MS_9 & = & (0)(a_{90} \quad a_{91} \quad a_{92} \quad a_{93} \quad a_{94} \quad a_{95} \quad a_{96} \quad a_{97} \quad a_{98})
\end{array}$$

Diagram 3

REFERENCES

1. A. D. Keedwell: On orthogonal latin squares and a class of neofields. *Rend. Mat. e Appl.* (5) **25** (1966), 519-561.
2. A. D. Keedwell: On property *D* neofields. *Rend. Mat. e Appl.* (5) **26** (1967), 384-402.
3. L. J. Paige: Neofields. *Duke Math. J.* 16 (1949), 39-60.

A projective configuration

J. W. P. HIRSCHFELD

1. In ageometry over a field, four skew lines not lying in a regulus have two transversals (which may coincide or lie only in a quadratic extension of the field). From this come the following theorems.

The double-six theorem (Schläfli, 1858): Given five skew lines with a single transversal such that each set of four has exactly one further transversal, the five lines thus obtained also have a transversal-the completing line of the double-six.

Grace's extension theorem (Grace, 1898): Given six skew lines with a common transversal such that each set of five gives rise to a double-six, the six completing lines also have a transversal-the Grace line.

Conjecture: Given seven skew lines with a common transversal such that each set of six gives rise to a Grace figure, the seven Grace lines also have a transversal.

2. The double-six is self-polar and lies on a unique cubic surface, which contains 27 lines in all. The configuration exists for all fields except $GF(q)$ for $q = 2$, 3 and 5 [1].

The six initial lines in the Grace figure are chords of a unique twisted cubic and are polar to the completing lines, which are also chords of the cubic. However, ***the theorem as it stands is true only if the six completing lines of the double-sixes are skew to one another.*** This is not necessarily true, as the six lines may be concurrent. The configuration exists for $GF(9)$ but not for $GF(q)$ with $q < \mathbf{9}$ [2].

The conjecture depends only on the incidences of the lines. So, if it is true over the complex field, it is true over any finite field large enough for the seven Grace lines to exist.

Wren [3] mentions that both he and Grace attempted the conjecture but were not able to achieve anything. Grace proved his theorem by, in fact, first establishing a slightly more general result. He proved a theorem for linear complexes, which was then applied to special linear complexes, which was in turn dualized to the theorem of the extension of the double-six.

In all, no one was very hopeful of extending Grace's theorem, which itself was regarded as something of a fluke. Further scepticism set in on finding that the conditions of linear independence on the initial set of lines were not even sufficient for Grace's theorem.

For the conjecture, the field $GF(31)$ was chosen and, using a computer, an initial set of lines found for which the seven Grace lines existed. The latter did not have a common transversal. Hence *the conjecture is false.*

3. A theoretical approach to the problem is more difficult to envisage. In Grace's figure, all was symmetry. There were two sets of 12 and 32 lines involved forming 32 double-sixes: each of the 32 lines met 6 of the 12 and could provide a starting point for the construction.

In the conjecture, the line b meets $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ which have in fours the further transversals b_{ijk}. Then there are 21 double-sixes like

$$\begin{matrix} \alpha_{12} & a_3 & a_4 & a_5 & a_6 & a_7 \\ b & b_{123} & b_{124} & b_{125} & b_{126} & b_{127} \end{matrix}$$

and 21 lines α_{ij}. The six lines α_{ij} ($j \neq i$) have a transversal β_i, the Grace line, giving seven lines β_i. There are also seven twisted cubics t_i, where t_i has the 12 chords a_j, α_{ij} ($j \neq i$). The seven t_i have a point P in common. The dual result to this is that there is a unique plane π meeting b and the 7 a_i in a conic C. The cubics t_i and t_j have in common the 6 chords α_{ij}, a_k ($k \neq i$, j), which is the full complement for two twisted cubics with a point in common.

Apart from the 71 lines so far obtained-1 b, 7 a_i, 35 b_{ijk}, 21 α_{ij}, 7 β_i— there are 105 further lines β^i_{jk} like β^1_{23}, the line common to the reguli $(b_{145}b_{146}b_{147})$, $(b_{154}b_{156}b_{157})$, $(b_{164}b_{165}b_{167})$, $(b_{174}b_{175}b_{176})$; there is no reason to suppose that $\beta^3_{12} = \beta^2_{13} = \beta^1_{23}$. However, the five lines β^k_{ij} ($k \neq i$, j) all lie in a regulus.

Since seven lines are under discussion (both the 7 a_i and the 7 β_i), Cayley's problem of seven lines lying on a quartic surface would appear relevant. There are 34 linear conditions to determine a quartic surface and 5 conditions for it to contain a given line. There are but 33 conditions for b and the 7 a_i to lie on a quartic surface. Hence there is a linear family $F_0 + \lambda F_1$ of quartic surfaces through these lines. One member of the pencil, F_1 say, contains P (as a node) and hence the 7 cubics t_i. Another, F_0 say, has b as a double line, so that any two members of the pencil touch along b. The curve of degree 16 common to all the surfaces consists of b (twice), $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ plus a rational irreducible septimic S, which is quadrisecant to each a_i and unisecant to b. Both F_0 and F_1 are uniquely defined.

The pencil of planes through b meets F_0 residually in a pencil of conics, eight of which break up into a pair of lines a_i, a'_i ($i = 1, \ldots, 8$). The conic C lies on F_0 and meets one of a_8, a'_8, which are incidentally both trisecant to S. In this way, F_0 contains $2^7 = 128$ conics. Several special cases may occur for this set of eight pairs of lines. Seven pairs, by the nature of the construction, must lie in the field. The eighth pair may lie in a quadratic extension of the field. There may be a node at the intersection of a pair of lines (which then counts twice). Also there may occur a second isolated node collinear with the first and a point of b forming a torsal line of F_0 and making a_7, a_7', say, coincide. This torsal line then contains three nodes, four being required before it is a double line. The last case was in fact the one to occur in the computed example.

In the calculated example, the 7 lines β_i were not in fact quite general: one pair had a point in common. The seven lines therefore lay on a quartic surface, which was unique. This surface contained another three lines. It is not at all clear if there is always a quartic surface through the 7 β_i.

It is also possible for the 7 cubics t_i to coincide, in which case one member of the family of surfaces through the a_i is ruled.

Attempts to connect the 7 β_i to the pencil $F_0 + \lambda F_1$ and to obtain some contradiction from the 176 lines mentioned above were unsuccessful.

My gratitude is to Dr. D. Barton for calculating the lines, to Mr. J. M. Taylor for help with the further computing and to Prof. J. G. Semple and Dr. J. A. Tyrrell for the exegesis of the pencil of quartic surfaces.

REFERENCES

1. J. W. P. Hirschfeld: Classical configurations over finite fields: I. The double-six and the cubic surface with 27 lines. ***Rend. Mat. e Appl. 26*** (1967), fasc. 1-2.
2. J. W. P. Hirschfeld: Classical configurations over finite fields: II. Grace's extension of the double-six. ***Rend. Mat. e Appl. 26*** (1967), fasc. 3-4.
3. T. L. Wren: Some applications of the two-three birational space transformation. *Proc. London Math. Soc. (2)* 15 (1916), 144.

The uses of computers in Galois theory

W. D. MAURER

ANY competent mathematician can learn FORTRAN in a few weeks and can immediately start applying it toward solving problems which are *finite* in nature. Constructing all the subgroups of a finite group, finding the incidence numbers of a finite simplicial complex, and taking the partial derivatives of a large symbolic expression in several variables, are examples of such problems, which take large amounts of programming but very little "hard" mathematical thinking. Such procedures are now widely recognized as having great value in preliminary investigations as well as for teaching purposes. The majority of good problems in mathematics, however, are not finite in nature, and many mathematicians feel that the computer is out of place in this environment. It is clear that we cannot ask the computer to look at all cases, when the number of cases is in-finite. Of course, in many situations, we can think of mathematical arguments which will reduce an infinite problem to a finite problem, and this is what is currently done in Galois theory, as detailed below. It is our hope, however, that these mathematical arguments will eventually themselves be generated and applied by the computer, so that the computer may be brought directly to bear on an infinite problem.

The problem of calculating the Galois group of a polynomial over the rationals is remarkable among mathematical algorithms for the paucity of its input-output. A single polynomial is given as input and a single group code, or the Cayley table of a group, is returned as output. It is the purpose of this paper to describe the computational difficulties that arise in computing such groups and to indicate how they may be solved.

It has been noticed several times that, although the splitting fields whose automorphism groups are the Galois groups of polynomials over the rationals are infinite fields, the problem of calculating these automorphism groups is actually a finite problem. The best known statement to this effect was made by van der Waerden in [1]. Van der Waerden's method of calculating a Galois group proceeds as follows: Let the polynomialfhave degree n over the field Δ (in our case, Δ is the field of rational numbers) and let Σ be the splitting field. Consider the ring Σ $(u_1, \ldots, u_n, z)$ of polynomials, with coefficients in Σ, in the $(n+1)$ variables $u_1, \ldots, u_n, z$. Form in this ring the expression $\theta = \alpha_1 u_1 + \ldots + \alpha_n u_n$, where the α_i are the roots of the polynomial (which are in Σ). For each permutation s in the symmetric group S_n, consider it as a permutation of the variables u_i and form the transformed expression $s\theta$. (For example, if $s = (1\ 2)$, then $s\theta = \alpha_1 u_2 + \alpha_2 u_1 + \alpha_3 u_3 + \alpha_4 u_4 + \ldots + \alpha_n u_n$.) Finally, form the product F of all the expressions $z - s\theta$ for all s in the symmetric group S,,. Now $\boldsymbol{F}$is a symmetric function of the α_i, and hence can be expressed in terms of the elementary symmetric functions of the α_i. These are precisely the coefficients off, and in fact lie in Δ, so that $\boldsymbol{F}$is actually in the smaller ring $\Delta(u_1, \ldots, u_n$, z). Decompose $\boldsymbol{F}$into irreducible factors $F_1, \ldots, F_n$ in this ring, and apply the permutations s as above to the resulting equation

$$\boldsymbol{F} = F_1 \cdot \ldots \cdot F_n$$

Now: For an arbitrary factor (say F_1), ***those permutations which carry this factor into itself form a group which is isomorphic to the Galois group of the given equation.***

It is clear that this is a finite method if the associated factorization is a finite method, and this is shown in [**1**], vol. 1, p. 77. On the other hand, van der Waerden's book first appeared in 1931, a long time before the first computers, and he pays no attention to considerations of speed. Some older mathematical algorithms, such as the Todd-Coxeter algorithm, adapt very well to computers, but it is clear that this is not one of them; even for a polynomial of degree 4, twenty-four polynomials must be multiplied and the result decomposed into irreducible factors in five variables.

Simpler methods are given by van der Waerden in the case in which the polynomial has degree less than or equal to 4. These methods have been improved on by Jacobson [**2**], vol. 3, pp. 94-95. We note first that if the given polynomial has a linear factor, we may divide by that factor to obtain a new polynomial with the same Galois group. After all linear factors have been removed, a polynomial of degree 4 or less is either irreducible or is a quartic polynomial with two quadratic factors. The Galois group in this case is the direct sum of two cyclic groups of order 2 unless both polynomials have the same discriminant or unless one discriminant divides the other and the quotient is a square. Quadratic factors of a polynomial may easily be found by Kronecker's method (cf. [**1**], vol. 1, p. 77). Therefore we are reduced to the case in which the polynomial is irreducible. If it is linear, the group is of order 1. If it is quadratic, the group is of order 2. If it is cubic, the group is of order 3 if the discriminant is a square, and is otherwise the symmetric group on three letters (of order 6). There finally remains the case of an irreducible quartic, and here Jacobson's algorithm is as follows:

(1) Calculate the resolvent cubic of the equation. This may be done pirectly from the coefficients: if the equation is $x^4 - a_1 x^3 + a_2 x^2 - a_3 x + a_4$,

then the resolvent cubic is $x^3-b_1x^2+b_2x-b_3$, where $b_1=a_2, b_2=a_1a_3-4a_4$, and $b_3=a_1a_4+a_3^2-2a_2a_4$.

(2) Calculate the Galois group of the resolvent cubic.

(3) The Galois group of the original equation may now be derived from the following table :

If the Galois group of the resolvent cubic is	***then the Galois group of the original equation is***
the identity	the Klein four-group
a cyclic group of order 2	a cyclic group of order 4 ***or*** a dihedral group of order 8
the alternating group A_3 (cyclic of order 3)	the alternating group A_4 (of order 12)
the symmetric group S_3 (of order 6)	the symmetric group S_4 (of order 24)

where there is only one ambiguity-the case in which the Galois group of the resolvent cubic is of order 2. In this case, the Galois group of the original equation is the cyclic group of order 4, if and only if it is ***not*** irreducible over the field obtained by adjoining the square root of the discriminant of the resolvent cubic.

This method easily lends itself to calculation. The only apparent difficulty is in the last step, and this is easily resolved by Kronecker's method applied at two levels.

It is of some interest to note that heuristic methods may be used even in a procedure as obviously combinatorial and manipulative as the one described above. The heuristics are, however, not of the usual kind. Most heuristic programs try various approaches, some of which are expected to fail. In Galois theory, however, we find ourselves faced more than once with the following situation ***: A program** X **solves a problem exhaustively. A program Y may be run which decreases the number of cases that** X **must treat, However, the program Y may take so long to run that no timing advantage is conferred by running it. Therefore, an estimate of the running time of** X**, of the improved** X **after running** Y**, and of Y is made, and a decision made on this basis as to whether to run Y. The result is that, for different input data, the program will perform the calculations in different ways, attempting to choose the fastest way as it goes (for the given data).***

An example of this occurs in irreducibility test routines. The program X is the Kronecker's method program. The program Y finds the factors, if any, modulo some integer. The number of steps in Kronecker's method is the product $n_1n_2\cdot\,.\,.\,.\,\cdot n_k$, where each n_i is twice the number of factors of some integral polynomial value (including itself and 1). The irreducibility test modulo $\boldsymbol{p}$, for prime $\boldsymbol{p}$, involves checking all the possible factors mod *p;* for a factor of degree *k,* as above, this is p^k. Since each of the n_i in Kronecker's method is at least 4, the number of steps in the program Y is always less than the number in *X* ifp = 2 or 3, and often ifp = 5. On the other hand, the test modulo *p* may give information of a quite varying nature. The polynomial may be irreducible mod *p,* in which case it is irreducible. Or it may have factors mod *p;* then each factor must correspond to a factor mod *p* or a product of factors mod *p.* An equation of order 6 cannot have an irreducible factor of order 3 if it decomposes mod *p* into three irreducible factors of degree 2. It is also possible that the factors mod p_1 do not agree with the factors mod p_2. A polynomial of degree 6 which has three irreducible factors of degree 2 (mod p_1) and two irreducible factors of degree 3 (mod p_2) must itself be irreducible.

Another example occurs on a more global level. It is possible to find the Galois group of an equation mod *p* by an obvious exhaustive process, since in this case we are searching for the set of all automorphisms of *a finite* field. This must then be a subgroup of the Galois group over the rationals. This calculation may reduce the amount of time taken to calculate the Galois group over the rationals by eliminating possibilities. If the Galois group mod *p* is the symmetric group, then the Galois group over the rationals must be the symmetric group. If the Galois group mod *p* contains any odd permutation (such as, for example, a transposition) then the Galois group over the rationals cannot be the alternating group or any subgroup of it. We can calculate roughly how long it will take us to find the Galois group modulo the next prime *p,* and compare this with the time estimate of the calculation of the Galois group over the rationals by other methods.

REFERENCES

1. B. L. van der Waerden: *Modern Algebra* (Frederick Ungar Publishing Co., New York, 1949-1950).

2. N. Jacobson: *Lectures in Abstract Algebra* (D. Van Nostrand Company, Princeton, N.J., 1951-1964).

An enumeration of knots and links, and some of their algebraic properties

.I. H. Conway

Introduction. In this paper, we describe a notation in terms of which it has been found possible to list (by hand) all knots of 11 crossings or less, and all links of 10 crossings or less, and we consider some properties of their algebraic invariants whose discovery was a consequence of this notation. The enumeration process is eminently suitable for machine computation, and should then handle knots and links of 12 or 13 crossings quite readily. Recent attempts at computer enumeration have proved unsatisfactory mainly because of the lack of a suitable notation, and it is a remarkable consequence that the knot tables used by modern knot theorists derive entirely from those prepared last century by Kirkman, Tait, and Little, which we now describe.

Tait came to the problem via Kelvin's theory of vortex atoms, although his interest outlived that theory, which regarded atoms as (roughly) knots tied in the vortex lines of the ether. His aim was a description of chemistry in terms of the properties of knots. He made little progress with the enumeration problem until the start of a happy collaboration with Kirkman, who provided lists of polyhedral diagrams which Tait grouped into knot-equivalence classes to give his tables [9], [10], **[11]** of alternating knots with at most 10 crossings. Little's tables [4], [5], [6] of non-alternating knots to 10 crossings and alternating knots of 10 and 11 crossings were based on similar information supplied by Kirkman.

Tait's and Little's tables overlap in the 120 alternating lo-crossing knots, and Tait was able to collate his version with Little's before publication and so correct its only error. The tables beyond this range are checked here for the first time. Little's table [6] of non-alternating knots is complete, but his 1890 table [5] of alternating 1 l-crossing knots has 1 duplication and 11 omissions. It can be shown that responsibility for these errors must be shared between Little and Kirkman, but of course Kirkman should also receive his share of the praise for this mammoth undertaking. (Little tells us that the enumeration of the 54 knots of [6] took him 6 years — from 1893 to 1899 — the notation we shall soon describe made this just one afternoon's work!)

Our tables of links, and the list of non-alternating 1 l-crossing knots, appear here for the first time, so cannot be collated with any earlier table, and for this reason the corresponding enumerations have been performed three times.

The enumeration here described was completed some 9 years ago, and a survey calculation of knot-polynomials was then made before an envisaged computer calculation. However, this survey brought to light certain algebraic relations between these polynomials which made the computer redundant. But we suspect that our table will find its main use as a basis for more sophisticated computer calculations with the many algebraic knot-invariants.

1. **Notation for tangles.** This paper is an abbreviated form of a longer one in which completeness is proved by means of a process for locating any knot or link within range of the table, but for reasons of space we only sketch this process here. For the same reasons, we describe our ideas rather informally, feeling that most readers will find that this helps rather than hinders their comprehension. Since most of what we say applies to links of 2 or more components as well as knots, we use "knot" as an inclusive term, reserving "proper knot" for the l-component case.

In the light of these remarks, we define a ***tangle*** as a portion of knot-diagram from which there emerge just 4 arcs pointing in the compass directions NW, NE, SW, SE, hoping that Fig. 1 clarifies our meaning.

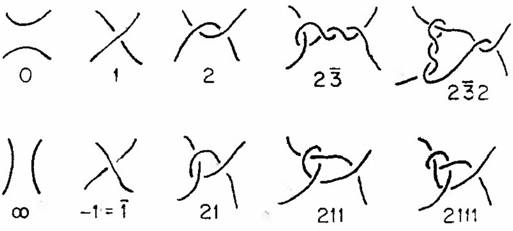


FIG. 1

The NW arc we call the ***leading string*** of the tangle, and the NW-SE axis its ***principal diagonal.*** The typical tangle t we represent diagrammatically by a circle containing an L-shaped symbol with the letter t nearby. The 8 tangles obtained from t by rotations and reflections preserving the "front" of t are indicated by making the corresponding operations on the L-shaped symbol, leaving the original letter t outside. The 8 other tangles obtained by reflecting these in the plane of the paper have the corresponding "broken" forms of the L-symbols, with the original letter t appended. Figure 2 shows how we represent the tangles t, t_h, t_v, $t_{hv} = t_r$, $-t$, t_h being the result of rotation in a "horizontal" or E-W axis, t_v that of rotation in the "vertical" or N-S axis, and -t that of reflection in the plane of the paper.

Tangles can also be combined and modified by the operations of Fig. 3, leading from tangles ***a*** and ***b*** to new tangles ***a+b, (ab), a+,*** and ***a-***. Tangles which can be obtained from the particular tangles 0 and ∞ by these operations we call ***algebraic***. In particular, we have the *integral* tangles $\boldsymbol{n} = 1+1+\dots+1$ and $\bar{n} = -n = \bar{1}+\bar{1}+\dots+\bar{1}$, both to n terms. If ***m, n, p,*** . . ., *s*, ***t,*** are integral tangles, the tangle ***mnp*** . . . ***st,*** abbreviating

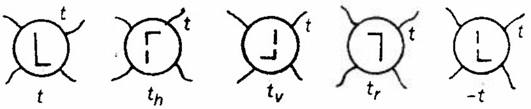


FIG. 2

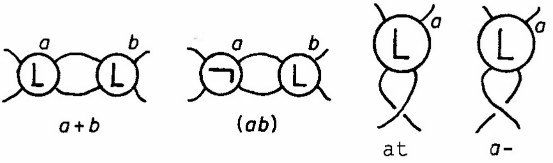


FIG. 3

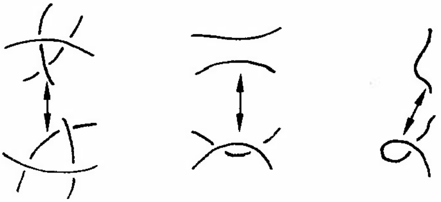


FIG. 4

((. . .***(mn)p***.. .*s*)*t*), the brackets being associated to the left, is called a *rational* tangle. Figure 1 shows the step-by-step formation of the particular rational tangles 2 $\bar{3}$ 2 and 2 1 1 1 as examples. In the tables, the "comma" notation (a, ***b,*** . . ., ***c***) = *a*0+*b*0+ . . . + *c*0 is preferred to the sum notation, but is only used with 2 or more terms in the bracket. Figure 3 shows that *a*0 is the result of reflecting a in a plane through its principal diagonal, and ***ab*** = *a*0+ ***b***. The abbreviation ***a-b*** denotes a6 (not a+ 6 or ***(a-)b),*** and outermost brackets are often omitted, in addition to those whose omission is already described above.

The tangles a and ***b*** are called ***equivalent*** (written ***a*** ≐ ***b)*** if they are related by a chain of ***elementary knot deformations*** (Fig. 4). The importance of the class of rational tangles is that we can show that the rational tangles ***ijk*** . . . ***lm*** and ***npq***. . .***stare*** equivalent if and only if the corresponding continued fractions $m+\frac{1}{l+}\cdots\frac{1}{+k+}\frac{1}{j+}\frac{1}{i}$ and $t+\frac{1}{s+\ldots+}\frac{1}{q+}\frac{1}{p+}\frac{1}{n}$ have the same value, so that there is a natural 1-1 correspondence between the equivalence classes of rational tangles and the rational numbers (including $\infty = 1/0$). The continued fractions $2+\frac{1}{-3+}\frac{1}{2}$ and $1+\frac{1}{1+}\frac{1}{1+}\frac{1}{2}$ have the same value $8/5$, and so the tangles $2\ \bar{3}\ 2$ and $2\ 1\ 1\ 1$ of Fig. 1 are equivalent. Using this rule, we can reduce any rational tangle to a standard form, either one of 0, ∞, 1, -1, or a form $mnp \ldots st$ in which $|m| \geqslant 2$ and $m, n, \ldots$, s, t have the same sign except that t might be 0. Each rational tangle other than 0 and ∞ has a definite *sign,* namely the sign of the associated rational number.

2. **Notation for knots.** An edge-connected 4-valent planar map we shall call a *polyhedron,* and a polyhedron is *basic* if no region has just 2 vertices. The term *region* includes the infinite region, which is regarded in the same light as the others, so that we are really considering maps on the sphere. We can obtain knot diagrams from polyhedra by substituting tangles for their vertices as in Fig. 5 — for instance we could always substitute tangles 1 or -1. Now let us suppose that a knot diagram K can be obtained by substituting algebraic tangles for the vertices of some non-basic polyhedron P. Then there is a polyhedron Q with fewer vertices than P obtained by "shrinking" some 2-vertex region of P, and plainly K can be obtained by substituting algebraic tangles for the vertices of Q, as in Fig. 5. Thus any knot diagram can be obtained by substituting algebraic tangles for the vertices of some *basic* polyhedron P — in fact P and the manner of substitution are essentially unique, but we do not need this.

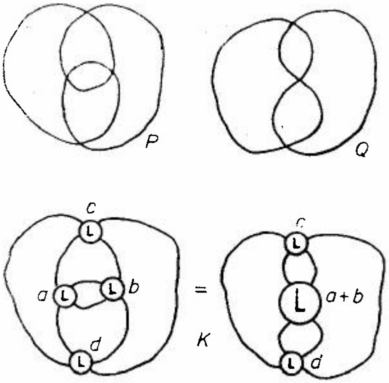


FIG. 5. Derivation of knots by substitution of tangles into polyhedra.

Only 8 basic polyhedra are needed in the range of this table (Fig. 6), although for convenience we have given one of them two distinct names. The notations (2X3)* = 6*, (2X4)* = 8*, (2X5)* = 10*, (3X3)* = 9* extend obviously to $(a \times b)^*$.

The knot obtained from the polyhedron P^* by substituting tangles $a, b, \ldots, k$ in the appropriate places we call $P^*a.\ b.\ \ldots\ .\ k$. To save space, we omit substituents of value 1, telescoping the dots which would have separated them so as to show how many have been omitted. Thus 8*2:3.4:.5 abbreviates 8*2.1.3.4.1.1.5.1, the final dots being omitted from the abbreviation. We also omit the prefixes 1*, 6*, 6** from certain knot names — the original form is recovered by prefixing 1* if the abbreviation has no dots, 6** if it has an initial dot, and 6* otherwise. The symbol 10−*** abbreviates 10***$\bar{1}.\bar{1}.\bar{1}.\bar{1}.\bar{1}$.

3. Some tangle equivalences. Flyping. The reader should now be able to interpret any knot name taken from our table, but he will not yet appreciate the reasons which make our ragbag of conventions so suspiciously efficient at naming small knots. Much of this efficiency arises from the fact that the notation absorbs Tait's "flyping" operation (Fig. 7), which replaces $1 + t$ by $t_h + 1$, or i $+ t$ by $t_h + \bar{1}$. For rational tangles t we have $t \doteq t_h \doteq t_v \doteq t_r$, and so when a, $b, \ldots,$ c are all rational, the exact positions of the terms 1 or $\bar{1}$ in (a, $b, \ldots,$ c) are immaterial, and we can collect them at the end. Thus $(1, 3, 1, 2) \doteq (3, 1, 1, 2) \doteq (3, 2, 1, 1)$.

Now using another part of our notation, we can also replace a pair of terms t, 1 in such an expression by the single term t^+, or a pair t, $\bar{1}$ by t- . Supposing again that $a, b, \ldots, c$ are rational, this justifies the equivalences

$$(a, b, c, 1) \doteq (a, b, c+) \doteq (a, b+, c) \doteq (a+, b, c)$$

and

$$(a, b, c, \bar{1}) \doteq (\mathrm{a}, b, c-) \doteq (a, b\text{-}, c) \doteq (a\text{-}, b, c),$$

showing that in such expressions the postscripts + and − can be regarded as floating, rather than being attached to particular terms. We therefore collect these postscripts on the rightmost term, cancelling + postscripts with − postscripts. If this process would leave in the bracket only a single tangle c followed by p + signs and q − signs, we replace the entire expression by cn, where $n = p$-q.

Now from the formula $x- = x\ \bar{1}\ 0$ and the continued fraction rule, it follows that we have the equivalences

$$2- \doteq -2,\ 3\text{ - G - }2\ 1\ ,\quad 2\ 1\text{ - k - }3\ ,\quad 2\,2 \doteq -2\,1\,1,$$

as particular cases of the equivalences

$$mn\ldots pql\text{-} \ \doteq\ -mn\ldots pr \ \ \text{and}\ \ mn\ldots pr- \ \doteq mn\ldots pq1,$$

for more general rational tangles, which hold whenever $r = q + l$. **This**

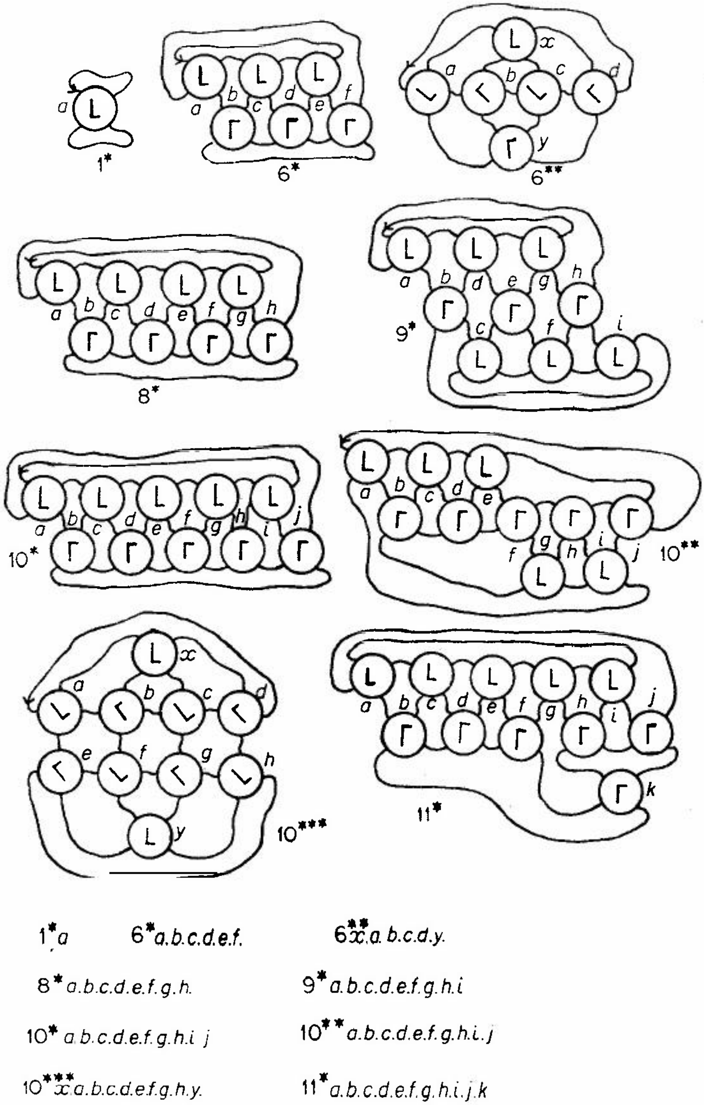


FIG. 6. The basic polyhedra

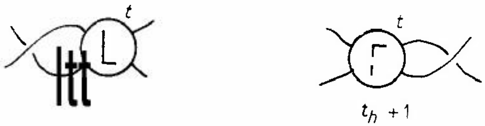


FIG. 7. Flyping — the equivalence of $1 + t$ and $t_h + 1$

leads to a kind of concealed flyping, instanced by:

$$(2\ 2, 3, 2, -1) \doteq (2\ 2, 3, -2) \doteq (2\ 2, -2\ 1, 2) \doteq (-2\ 1\ 1, 3, 2),$$

as illustrated in Fig. 8. Each of these expressions should be translated at sight into (2 2, 3, 2 −) which is regarded as the standard form. The reader should similarly be able to write down 2 2 3 on seeing any of the flyped variants shown in Fig. 9.

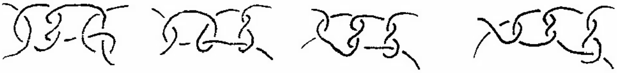


FIG. 8. Concealed flyping

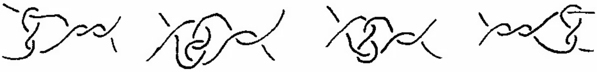


FIG. 9. Flyping variants of 2 2 3

4. **Equivalences for knots.** The following equivalences refer to the whole knot diagram rather than its component tangles. If two vertices of a triangular region are substituted 1 and − 1, then in all cases within range the first deformation of Fig. 10 produces a form with fewer vertices in the basic polyhedron. If the substituents x and y of 6** x . a. b . c . d. y are both 1, then the second deformation of Fig. 10 produces a form with basic polyhedron 1*. This increases the crossing number by 2, but we can use the continued fraction rule to reduce it by 2 again should any one of a, b, c, d be a negative rational tangle. If instead x and y are − 1 and 1, other reduction processes apply to all cases within range.

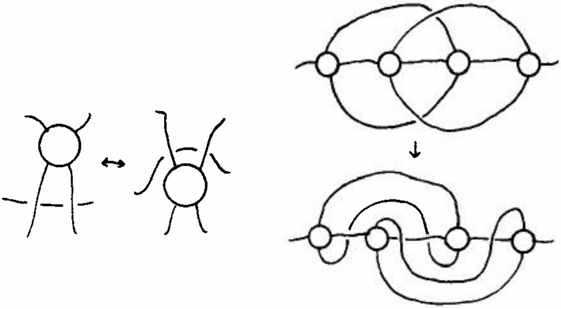


FIG. 10. Two knot reductions

In the tables, these and other equivalences have been taken into account, so that for example no substituent in the form 6**. a. b . c. d is negative rational (this remark explains our preference for the 6** form rather than the 6* form when two opposite vertices are substituted as 1). Unfortunately the use of such equivalences means that the user might at first fail to locate his knot in our table. He should in these circumstances apply some reasonable transformation and try again — success comes easily after a little experience.

These remarks have probably convinced the reader that our notation has little structural significance, although it might be convenient in practice. The following remarks show that at least it has some structure. Let us call the knot $\mathbf{1{*}t}$ a ***rational knot*** whenever $\boldsymbol{t}$ is a rational tangle. Then the double branched covering space of the rational knot obtained from the rational number $\boldsymbol{p/q}$ is just the lens space with parameters $\boldsymbol{p}$ and q, and in fact the rational knots are precisely the Viergeflechte, long recognized as an interesting class. More generally, if $\boldsymbol{p}$ and q are the determinants of the knots $1{*}t$ and ***l*tO, we*** call $\boldsymbol{p/q}$ the ***determinant fraction*** of the (arbitrary) tangle $\boldsymbol{t}$. Then the determinant fraction of $\boldsymbol{a+b}$ is $(ps+qr)/qs =$ $= (p/q)+(r/s)$ and that of ***(ab)*** is $(qs+pr)/ps = (p/q)^{-1}+$ ***(r/s),*** if those of $\boldsymbol{a}$ and $\boldsymbol{b}$ are $\boldsymbol{p/q}$ and ***r/s,*** which explains the continued fraction process. Under more restricted circumstances similar identities hold for the fractions obtained from Alexander polynomials, as we shall see later.

5. Orientation and string-labelling. An ***oriented knot*** will mean a proper knot with a preferred orientation (arrowhead) on its string. From any such knot we can obtain 3 others by simple geometric operations. Reflecting in a mirror gives us the enantiomorph, or ***obverse,*** $\neg K$ of K, reversing string orientation the ***reverse,*** K_r, of K, and doing both the ***inverse,*** $\neg K_r$, of $\boldsymbol{K}$. A knot equivalent to its obverse is ***amphicheiral,*** one equivalent to its reverse is ***reversible,*** and one 'equivalent to its inverse is ***involutory.*** (Our notation is more mnemonic than the usual one — the inverse in our sense is also the inverse in the cobordism group.) For links of more than one component the situation is more complicated, and we need a convention for labelling and orienting strings. The convention we adopt is easy to remember and apply, although it leads occasionally to unexpected labellings.

We orient the leading string of the tangle named a in Fig. 6 so as to point into that tangle, and label this string r_1. We now move along r_1 in the direction of its orientation, labelling the other strings r_2, $r_3, \ldots$ in the order of their first crossing with r_1, either over or under, and orient these strings so that their first crossing with r_1 is ***positive*** in the sense of Fig. 11. If any strings remain, we proceed along r_2 in the direction of its orientation, labelling the unlabelled strings crossing r_2 in the same way. Repeating this process with r_3, etc., if necessary, we eventually obtain a complete system of labels and orientations. This convention tends to ensure that the homological linking is positive, since the linking number of two strings is half the sum of the ε's of Fig. 11 over all crossings in which both those strings appear.

For the purposes of polynomial calculation, we replace the labels $r_1, r_2, r_3, \ldots$ by $r; s, t, \ldots$. We also need to describe links obtained by relabelling a given one in various ways. Let π be any function from the string labels $r; s, t, \ldots$ to the symbols $r, r^{-1}, s, s^{-1}, t, t^{-1}, \ldots$. Then for any labelled link K we define K_π to be the link obtained from K by relabelling all the r strings of K as s strings in K_π, if $n(r) = s$, and as reversely oriented s strings in K_π, if $\pi(r) = s^{-1}$, and so on. We define $|\pi|$ as the total number of strings whose orientation is reversed in this process, and $|K|$ to be the total number of strings in K. Note that two distinct strings can have the same label.

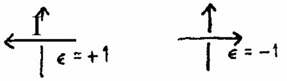


FIG. 11. A positive crossing ($\varepsilon = + 1$) and a negative crossing

In the table, we give only one knot from each enantiomorphic pair, and only one from each labelling and orientation class. We indicate the symmetries of proper knots in the column S by writing a for amphicheiral knots, r for reversible knots, i for involutory knots, f for knots with full symmetry (all of these properties), and n for knots for which no symmetry has been observed. For links of 2 components we give the generators of the (observed) symmetry group, r and s being the operations of reversing the r and s strings respectively, t the operation of transposing these strings, and q the operation of reflection in a mirror. The column S is left empty for links of 3 or more components.

6. Polynomials and potentials. Each labelled and oriented knot K has a ***potential function*** $\nabla_K = \nabla_K(r, s, \ldots)$ whichis a rational function with one variable for each string label appearing in K. We shall see in a moment that ∇_K is just a disguised and normalized form of the Alexander polynomial Δ_K, but it is in fact completely defined by the properties given below. We first have the symmetry properties

$$\nabla_K(r, s, \ldots) = \nabla_K(-r^{-1}, -s^{-1}, \ldots) = (-)^{|K|}\cdot\nabla_K(-r, -s, \ldots),$$

$$\nabla_{K_\pi}(r, s, \ldots) = (-)^{|\pi|}\cdot\nabla_K(\pi(r), n(s), \ldots).$$

$$\nabla_{\neg K}(r, s, \ldots) = (-)^{|K|+1}\cdot\nabla_K(r, s, \ldots),$$

the first of which makes it appropriate to use the abbreviation $\{f(r, s, \ldots)\}$ for $f(r, s, \ldots) + f(-r^{-1}, -s^{-1}, \ldots)$ in our table of potentials and elsewhere. If L is obtained from K by deleting a string labelled r in K, then

$$\nabla_K(1, s, t, \ldots) = (s^a t^b \ldots - s^{-a} t^{-b} \ldots)\cdot\nabla_L(s, t, \ldots).$$

where $a, b, \ldots$ are the total homological linking numbers of the deleted r string of K with the strings labelled $s, t, \ldots$ respectively. Finally, if

$K \circledast {}_r L$ is a ***product*** of K and L, obtained by tying each of them separately in a string labelled r, then

$$\nabla_{K \circledast_r L} = \nabla_K \cdot \{r\} \cdot \nabla_L .$$

Our tables list only knots which are ***prime*** in the sense of such products, and the assumption of primality is implicit elsewhere in this paper.

Our potential function is related to the Alexander polynomial Δ_K by the identity

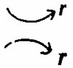
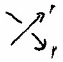
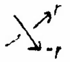
$$\Delta_K(r^2) = \{r\} \cdot \nabla_K(r)$$

if K is a proper knot, and by

$$\Delta_K(r^2, s^2, \ldots) = \nabla_K(r, s, \ldots)$$

otherwise, but it is important to realize that A, is defined to within multiplication by powers of the variables and -1, while ∇_K is defined absolutely.

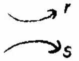
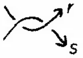
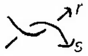
The most important and valuable properties of the potential function are for this reason not shared by the polynomial. Let K_0 yield $\boldsymbol{K+}$ and K_- on replacement of the tangle

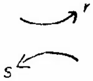
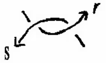
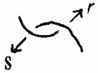
 by  and  respectively,

the labellings and orientations being significant. Then we have

$$\nabla_{K_+} = \nabla_{K_-} + \{r\} \cdot \nabla_{K_0},$$

called the ***first identity***, which enables us to compute any one of the three potentials from the other two.

The ***second identity*** relates knots K_{00}, $\boldsymbol{K{+}{+}}$, K_{--}, defined as above, but now using the tangles ,  and 

or alternatively ,  and 

The second identity asserts that

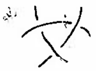
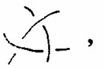
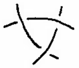
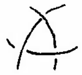
$$\nabla_{K_{++}} + \mathrm{VK\text{--}} = \{rs\} \cdot \nabla_{K_{00}}$$

in the first case, and

$$\nabla_{K_{++}} + \nabla_{K_{--}} = \{r^{-1}s\} \cdot \nabla_{K_{00}}$$

in the second case.

The *third identity* involves possibly three distinct string labels. If K_1 yields K_2, K_3, and K_4 on the replacement of

 by ,  and 

then we have

$$\nabla_{K_1}+\nabla_{K_2} = \nabla_{K_3}+\nabla_{K_4},$$

where now the labellings are immaterial.

These identities have many consequences which we cannot explore in detail here, although we shall give a few examples. Let t be a tangle whose 4 emerging strings are oriented and labelled as in Fig. 12. Define the *polynomial fraction* oft as the formal fraction

$$\frac{\{r\}\cdot\nabla_K}{\{r\}\cdot\nabla_L}$$

where K and L are the knots $1 * t$ and $1 * t0$. Then the identities which we asserted for determinant fractions in Section 4 hold also for polynomial fractions.

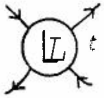


FIG. 12

If we consider generalized tangles with $2n$ emerging arcs instead of 4 (such as, for $2n = 6$, those of the third identity), then we can determine the potential of any knot obtained by joining the emergent arcs of two such tangles in terms of $n!$ potential functions associated with each tangle separately, provided that all the emerging strings have the same label. In the case $n = 2$ the $2!$ potentials are the numerator and denominator of the polynomial fraction. It becomes natural to think of such tangles as being -to within a certain equivalence relation-elements of a certain vector space in which our identities become linear relations, and there are many natural questions we can ask about this space. However, when the emerging arcs may have distinct labels, it is not even known whether the dimension of the tangle space is finite.

We have not found a satisfactory *explanation* of these identities, although we have *verified* them by reference to a "normalized" form of the 'L-matrix definition of the Alexander polynomial, obtained by associating the rows and columns in a natural way. This normalization is useful in other ways

-thus our symmetry formulae show that a 2-component link can only be amphicheiral if its polynomial vanishes identically. It seems plain -that much work remains to be done in this field.

7. Determinants and signature. We define the *reduced polynomial* $D_K(x)$ by the equation

$$D_K(x) = \{x\}\cdot \nabla_K(x, \mathrm{x}, \ldots),$$

and the *determinant* $\delta = \delta_K$ as the number $D_K(i)$. Our determinant differs from the usual one only by a power of i. The potential identities of the last section yield determinant identities when we put i for each variable.

Murasugi [7] has defined invariants called the *signature*, σ_K, and *nullity*, n_K, and described some of their properties. These invariants depend on the string orientations of K, but not on its labelling. We shall describe enough of their properties to enable their calculation to proceed in much the same way as that of the potential function.

For any knot K we have the identity

$$\delta_K = \delta_K^0 \cdot i^{\sigma_K},$$

where $\delta_K^0 = |\delta_K|$, and the condition

$$n_K > 1 \quad \text{if and only if} \quad \delta_K = 0,$$

the first of which determines σ_K modulo 4 provided $\sigma_K \neq 0$. But one of Murasugi's results is that

$$|\sigma_{K_+} - \sigma_{K_0}| + |n_{K_+} - n_{K_0}| = 1,$$

whenever $K+$ and K_0 are related as in the first identity. These two results determine σ_K completely in almost all cases, and make its calculation very swift indeed. Of course it should be remembered that σ_K and n_K are integers, and $1 \leqslant n_K \leqslant |K|$.

We have the relations

$$\sigma_{\neg K} = -\sigma_K \quad \text{and} \quad \sigma_{K \circledast, L} = \sigma_K + \sigma_L,$$

concerning obverses and products, and if we define σ_K^0 as $\sigma_K - \lambda_K$, where λ_K is the total linking of K (the sum of the linking numbers of each pair of distinct strings of K), then the reorienting identity is that σ_K^0, like δ_K^0, is an invariant of the unoriented knot K. In the tables, we give only these *residual* invariants, δ^0 being the numerator of the rational fraction which we give for rational knots.

8. Slice knots and the cobordism group. A proper knot which can arise as the central 3-dimensional section of a (possibly knotted) locally flat 2-sphere in 4-space *we* call a *slice knot.* A natural application of our tables is to the discovery of interesting slice knots, since for slice knots there are simple conditions on the polynomial, signature, and Minkowski units. In particular, we might hope to find a slice knot which is not a ribbon knot [3], since several published proofs that all slice knots are ribbon have been found to be fallacious.

The slice knots with 10 crossings or less were found to be

∞, 4 2, 3 1 1 3, 2 3 1 2, (3, 2 1, 2−), 2 1 2 1 1 2, 2 0:2 0:2 0, (3, 3, 2 1−),
6 4, 3 3 1 3, 2 4 2 2, 2 2 1 1 1 1 2, (4 1, 3, 2), (2 1, 2 1, 2 1+),·2 2·2 0,
·2·2·2 0·2 0, 1 0*, (3 2, 2 1, 2-j, (2 2, 2 1 1, 2−), (4, 3, 2 1−),
((3, 2)-(2 1, 2)), 3 : 2 : 2,

together with the composite knots 3 ※ $\bar{3}$, 2 2 ※ 2 2, 5 ※ $\bar{5}$, 3 2 ※ 3 2. The granny knot 3 ※ 3 and the knot ·2·2·2·2 0 satisfy the polynomial condition but not the signature condition, and so are not slice knots.

Now suppose that in the slab of 4-space bounded by two parallel 3-spaces we have an annulus ($S^1 \times I$) whose boundary circles lie in the two 3-spaces. Then the two knots defined by these circles we call *cobordant*. Cobordism is an equivalence relation, and the cobordism classes form a group under the product operation, the unit class being the class of slice knots, and the inverse of any class is the class of inverse knots to the knots of that class.

A search was made for cobordances between knots of at most 10 crossings and knots of at most 6 crossings, which in addition to the cobordances between slice knots, found only

3≅3212≅3, 21, 2≅222112≅22, 211, 2≅31, 3, 21≇211, 3, 21−.
2 2 ≅ 3, 2 1, 2 1 ≅ 3, 2 1, 2+
5 ≅ 3 4 1 2 ≅ 4, 3, 2 1
3 2 ≅ 3 1, 3, 2 1 ≅ 3, 3, 2 1 + ≅ 3, 2 1, 2++
3 ※ 3 ≅ .2.2.2.2 *0,*

all of these being to within sign and orientation.

All slice knots given were found to be ribbon knots. However, the presence of the particular knot 10* = (2 **X** 5)* leads us to examine the more general *a* strand *b* bight Turk's Head knot *((a* – 1) x *b)**. Andrew Tristram has proved that if *a* and *b* are odd and coprime this knot obeys all known algebraic conditions for slice knots, but despite a prolonged attack the only cases definitely known to be slice are the trivial cases with *a* or *b* = 1, and the cases *a* = 3, *b* = 5, and *a* = 5, *b* = 3. Since most of our methods for proving knots slice would also prove them ribbon, the way is left open for a conjecture that some of least of these are slice knots which are not ribbon knots.

9. Notes on the tables. Acknowledgments. The tables (pp. 343-357) list all proper knots of at most 11 crossings, and all links of at most 10 crossings, with various invariants tabulated over parts of this range. Knots listed separately are believed to be distinct, and the symmetries listed under S are believed to be a complete set. (The evidence is very strong—

each knot has been subjected to a reduction procedure which in every known case has been shown to yield all forms with minimal crossing number.) By the same token, all knots listed are believed to be prime.

The columns headed ∇, δ^0, σ^0 give the invariants of §§ 6 and 7, and for proper knots the column headed Δ gives a coded form of the polynomial or equally of the potential, *[a+ b+c* abbreviating the polynomial $a+b(r+r^{-1}) + c(r^2+r^{-2})$ or the potential $(a+ b\{r^2\}+ c\{r^4\})/\{r\}$. The column "units" gives the Minkowski units (for definition see **[8]**, but beware errors!) of ***K*** and its obverse, $+p$ meaning that $C_p = +1$ for both ***K*** and $\neg K$, $\mp p$ that C_p is -1 for ***K*** and 1 for $\neg K$, and so on. The units have been recomputed even in range of the existing tables, since these do not distinguish between a knot and its obverse. Under "λ" we give the linking numbers of pairs of strings, in the order λ_{rs}, λ_{rt}, I,,, ;I,,, I,,, λ_{tu}, but omitting linking numbers of non-existent strings.

The tables have been collated with the published tables of Tait (T in the tables) , Little[†] (L), Alexander and Briggs (A&B) **[1]**, and Reidemeister **[8]**, and with some unpublished polynomial tables computed by Anger **[2]** and Seiverson of the Princeton knot theory group. I thank Professor H. F. Trotter for making these available-they have enabled me to correct a number of (related) errors in the 10 crossing knot polynomials. Much of the material of §§ 7 and 8 of this paper arose as the result of some stimulating conversations with Andrew Tristram, whose assistance I gratefully acknowledge here.

Note added in proof.

An idea of Professor Trotter has led me to the discovery of an identity for the Minkowski units like those of the text for the other invariants. In fact we have, if $\boldsymbol{K} = K_0$, $\boldsymbol{L} = \boldsymbol{K}+$, that

$$C_p(K)\cdot C_p(L) = [i\delta_K/\delta_L(p)]_p,$$

where $[X]_p = \left(\frac{p^{-x}X}{P}\right)^x$, and $X(p) = (-1)^x X$ when $p^x \,||\, X$, and $\frac{a}{OP}$ is the Legendre symbol.

[†] **The 11 -crossing knot numbered 400 in the table is the knot which appeared twice in Little's table, as numbers 141 and 142, and the knots 401-411 are those omitted by Little.**

Knots to 8 crossings

A&B	T/L	knot	S	σ^0units	δ^0	A
0,	**1**	∞	***f***	0 +	1/1	[1
3,	**13**		*r*+2	±3	3/1	[−1+1
4_1	**1**	**22**	***f***	***0*** **-5**	**512**	[3−1
5,	**25**		*r*+4	+5	5/1	[1−1+1
52	**1**	**32**	*r*+2	∓7	7/3	[−3+2
6_1	**3**	**42**	***r***	0 +3	9/4	[5−2
6_2	**2**	**312**	*r*+2	**ill**	11/4	[−3+3−1
6_3	**1**	**2112**	***f***	***0*** **-13**	13/5	[5−3+1
7,	**77**		*r*+6	±7	7/1	**r - 1 + 1 - 1 + 1**
7_2	**6**	**52**	*r*+2	±11	11/5	[−5+3
7_3	**5**	**43**	**r-4**	+13	13/4	[3−3+2
7_5	**3**	**322**	*r*+4	***-17***	17/7	[5−4+2
7_4	**4**	**313**	***r-2***	∓3−5	15/4	[−7+4
7_6	**2**	**2212**	*r*+2	±19	19/7	[−7+5−1
7_7	**1**	**21112**	**r**	**0** ∓3∓7	21/8	[9−5+1
8_1	**18**	**62**	**r**	**O-13**	13/6	[7−3
8_2	**15**	**512**	*r*+4	***-17***	17/6	[3−3+3−1
8_3	**17**	**44**	***f***	0 +17	17/4	[9−4
8_4	**16**	**413**	*r*+2	**119**	19/5	**[- 5 + 5 - 2**
8_7	**13**	**4112**	***r-2***	±23	23/9	[−5+5−3+1
8_6	**11**	**332**	*r*+2	±23	23/10	[−7+6−2
8_{11}	**10**	**3212**	*r*+2	±3	27/10	**[- 9 + 7 - 2**
8_9	**12**	**3113**	***f***	0 +5	25/7	[7−5+3−1
8_{12}	**8**	**31112**	***r***	***0*** ***-29***	29/11	[11−7+2
8_8	**6**	**2312**	***r***	0 +5	25/9	[9−6+2
8_{12}	**5**	**2222**	***f***	**0** **-29**	29/12	[13−7+1
8_{14}	**2**	**2 2 1 1 2**	*r*+2	∓31	31/12	[−11+8−2
8_5	**14**	3, 3, 2	***r-4***	±3∓7	*21*	[5−4+3−1
8_{10}	**9**	3, 2 1, 2	***r-2***	∓3	**27**	[−7+6−3+1
8_{15}	**3**	2 1, 2 1, 2	*r*+4	∓3∓11	**33**	[11−8+3
8_{17}	**1**	.2.2	***i***	***O-37***	**37**	[11−8+4−1
8_{16}	**4**	.2.20	*r*+2	−5∓7	*35*	[−9+8−4+1
8_{18}	**7**	8*	***f***	***0*** −3+5	**45**	[13−10+5−1
8_{19}	**III**	**3,** 3, 2−	***r-6***	***t-3***	**3**	[1+0−1+1
8_{20}	**I**	3, 2 1, 2−	***r***	***0*** +3	**9**	[3−2+1
8_{21}	**II**	2 1, 2 1, 2−	*r*+2	∓3+5	*15*	[−5+4−1

2 string links to 8 crossings

Link	λ	s	σ^0	units	δ^0	Δ
0	0	q, r, s, t	0	+	O/l	0
2	+1	qr, qs, t	0	+	2/1	1
4	+2	rs, t	+1	+	4/1	$\{rs\}$
212	0	r, s, t	+1	+	8/3	$-\{r\}\{s\}$
6	+3	rs, t	i-2	∓3	6/1	$\{r^2s^2\}+1$
33	+3	qr, qs, t	0	+5	10/3	$\{r^2+s^2\}-1$
222	+2	rs, t	+1	∓3	12/5	$\{rs\}+\{r\}\ \{s\}$
412	+1	rs, t	+2	∓7	14/5	$1-\{r\}\{s\}\{rs\}$
3112	+1	rs, t	+b	+3	16/7	$1-\{r\}\{s\}\{r^{-1}s\}$
232	0	r, s, t				$-2\{r\}\{s\}$
3, 2, 2	0	r, s	−3	+	16	$\{r\}\{s\}\{r^2\}$
2 1, 2, 2	+2	rs	+1 -	5	20	$\{r^{-3}s\}+2\{r\}^3\{s\}$
.2	0	r, s	+1	±3	24	$\{r\}\{s\}+\{r\}^3\{s\}$
3,2,2-	+2	rs	−3	+	4	$\{r^{-3}s\}$
2 1, 2, 2−	0	r, s	+1	+	8	$-\{r\}\{s\}$
8	+4	rs, t	+3	+	8/1	$\{r^3s^3+rs\}$
53	+4	rs, t	-1	+	16/5	$\{r\}\{s\}+\{rs\}\{r^2s^{-2}\}$
422	+3	rs, t	+2	∓11	22/9	$\{2r^2s^2-r^2-s^2\}+3$
323	+4	rs, t	+1	∓3	24/7	$\{rs\}\{r^2+s^2-1\}$
3122	+3	rs, t	0	+13	26/11	$\{2r^2+2s^2+r^2-s^2\}-3$
242	+2	rs, t	+1	+5	20/9	$\{rs\}+2\{r\}\{s\}$
21212	+1	rs, t	+2	∓3+5	30/11	$1-\{r\}^2\{s\}^2$
211112	+1	r, s, t	+2	+17	34/13	$1+\{r\}^2\{s\}^2$
2 2, 2, 2	+1	rs	- 1	±7	28	$\{4r^{-1}s-2rs-r^{-3}s\}$
2 1 1, 2, 2	0	r, s	−1	+	32	$-\{r\}^3\{s\}$
3, 2, 2+	$2	rs	−3	∓7	28	$\{r^3s\}-2\{r\}\{s\}\{r^2\}$
2 1, 2, 2+	0	r, s	+1	+	32	$\{r\}^3\{s\}$
.21	0	r, s	+1 -	5	40	$\{r\}^3\{s\}-\{r\}\{s\}$
.2 : 2	+2	rs	- 1	- 3	36	$\{r^3s\}-4\{r\}\{s\}$
2 2,2,2-	0	r, s	-1	+	8	$\{r\}\{s\}$
2 1 1, 2, 2−	+2	rs	-1	±3	12	$\{2r^{-1}s-r^{-3}s\}$

9 crossing knots

A&B	T/L	knot	s	σ^0	*A*
9,	41	9	r	9/1	[1-1+1-1+1
9_2	38	72	r	15/7	[-7+4
9,	40	63	r	19/6	[-3+3-3+2
9,	39	54	r	21/5	[5-5+3
9,	33	522	r	27/5	[-5+5-4+2
9,	37	513	r	23/6	[-11+6
9,	34	423	r	31/9	[-7+6-4+2
9_{12}	31	4212	r	35/13	[-13+9-2
9_{11}	30	4122	r	33/14	[7-7+5-1
9_{14}	28	41112	r	37/14	[15-9+2
9,	26	342	r	29/13	[9-7+3
9_{10}	32	333	r	33/10	[9-8+4
9_{18}	25	3222	r	41/17	[13-10+4
9_{13}	39	3213	r	37/10	[11-9+4
9_{20}	21	31212	r	41/15	[11-9+5-1
9_{21}	18	31122	r	43/18	[-17+11-2
9_{26}	17	311112	r	47/18	[-13+11-5+1
9,	16	2412	r	31/11	[-11+8-2
9_{15}	15	2322	r	39/16	[-15+10-2
9_{19}	14	23112	r	41/16	[17-10+2
9_{23}	12	22122	r	45/19	[15-11+4
9_{17}	22	21312	r	39/14	[-9+9-5+1
9_{27}	8	212112	r	49/19	[15-11+5-1
9_{31}	2	2111112	r	55/21	[-17+13-5+1
9_{36}	24	22„ 3„ 2	r	37	[9-8+5-1
9_{25}	13	2 2, 2 1, 2	r	47	[-17+12-3
9_{22}	23	2 1 1, 3, 2	r	43	[-11+10-5+1
9_{30}	4	2 1 1, 2 1, 2	r	53	[17-12+5-1
9_{35}	36	3, 3, 3	r	27	[-13+7
9_{37}	19	3, 2 1, 2 1	r	45	[19-11+2
9_{16}	27	3, 3, 2+	r	39	[-9+8-5+2
9_{24}	20	3, 2 1, 2+	r	45	[13-10+5-1
9_{28}	6	2 1, 2 1, 2+	r	51	[-15+12-5+1
9_{33}	3	.2 1. 2	n	61	[19-14+6-1
9_{32}	7	.2 1. 2 0	n	59	[-17+14-6+1
9_{38}	5	.2.2.2	r	57	[19-14+5
9_{29}	11	.2.2 0.2	r	51	**i-15+12-5+1**
9_{39}	9	2: 2: 2 0	r	55	[-21+14-3
9_{41}	10	2 0: 2 0: 2 0	r	49	[19-12+3
9_{34}	1	8*20	r	69	**[23-16+6-1**
9_{40}	35	9*	r	75	[-23+18-7+1
9_{42}	IV	2 2„ 3„ 2-	r	7	[-1+2-1
9_{44}	I	2 2, 2 1, 2-	r	17	[7-4+1
9_{43}	V	2 1 1, 3, 2-	r	13	[1-2+3-1
9_{45}	III	2 1 1, 2 1, 2-	r	23	[-9+6-1
9_{46}	VI	3„ 3„ 2 1-	r	9	[5-2
9_{48}	VII	2 1, 2 1, 2 1-	r	27	[-11+7-1
9_{49}	II	-2 0: -2 0: -2 0	r	25	[7-6+3
9_{47}	VIII	8*-20	r	27	[-5+6-4+1

9 crossing 2 string alternating links, with basic polyhedron 1^*

link	λ	∇
612	+2	$\{r^{-1}s\}-\{r\}\{s\}\{r^2s^2\}$
5112	+2	$\{rs\}-\{r\}\{s\}\{r^{-1}s\}^2$
432	+1	$1-2\{r\}\{s\}\{rs\}$
414	0	$-\{r\}\{s\}(\{r^2+s^2\}+1)$
4113	0	$\{r\}\{s\}\{r^{-1}s\}^2$
3312	+2	$\{rs\}(1-\{r\}\{s\}\{r^{-1}s\})$
32112	+2	$\{rs\}+\{r\}\{s\}(1-\{r^2+s^2\})$
3132	+1	$1-2\{r\}\{s\}\{r^{-1}s\}$
31113	0	$\{r\}\{s\}(\{r^2+s^2\}-1)$
252	0	$-3\{r\}\{s\}$
22212	+1	$1-\{r\}\{s\}(\{rs\}+\{r\}\{s\})$
221112	+1	$1+\{r\}\{s\}(\{r\}\{s\}-\{r^{-1}s\})$
5, 2, 2	0	$\{r\}\{s\}(\{r^4\}+1)$
4 1, 2, 2	+2	$\{r^{-5}s\}+2\{r\}\{s\}\{r^2\}$
3 2, 2, 2	0	$\{r\}\{s\}(2\{r^2\}-1)$
3 1 1, 2, 2	+2	$\{2r^{-3}s-r^{-1}s\}+4\{r\}\{s\}$
2 3, 2, 2	+2	$\{2r^{-3}s-r^{-1}s\}+3\{r\}\{s\}$
2 2 1, 2, 2	0	$2\{r\}\{s\}(\{r^2\}-1)$
4, 3, 2	+3	$\{s^2\}-1+\{r\}\{s\}\{r^{-1}s\}\{s^2\}$
4, 2 1, 2	+1	$1+\{r^2s^{-4}\}+2\{r\}\{s\}\{r^{-1}s\}$
3 1, 3, 2	+1	$\{s^2\}-1+\{r\}\{s\}\{rs\}\{s^2\}$
3 1, 2 1, 2	+3	$\{r^2s^2\}+1+\{s\}^2(\{r^2+s^2\}-1)$
3, 3, 2 1	+2	$\{r^{-1}s\}(1 \quad \{r\}\{s\}\{r^{-1}s\})$
2 1, 2 1, 2 1	+3	$1+\{r^2s^2\}+\{rs\}\{r\}\{s\}+\{r\}^2\{s\}^2$
2 2, 2, 2+	0	$\{r\}\{s\}(4-\{r^2\})$
21 1, 2, 2+	+2	$\{2r^{-1}s-r^{-3}s\}+\{r\}\{s\}(\{r^2\}-3)$
3, 2, 2++	0	$\{r\}\{s\}(2\{r^2\}-1)$
2 1, 2, 2++	+2	$\{r^{-3}s\}+\{r\}\{s\}(3-\{r^2\})$
(3, 2) (2, 2)	+2	$\{r^{-5}s\}+2\{r\}\{s\}\{r^2\}$
(2 1, 2)(2, 2)	+2	$\{r^{-3}s\}+\{r\}^2(\{r^{-1}s\}-\{r\}\{s\})$

9 crossing 2 string links, otherwise

link	λ	V
.4	0	$\{r\}\{s\}(\{r^4-r^2\}+1)$
.3 1	0	$\{r\}\{s\}(2\{r^2\}-3)$
.2 2	0	$\{r\}\{s\}(3-2\{r^2\})$
.3.2	+1	$1-\{r\}\{s\}\{rs\}(\{r^2\}-1)$
.3.2 0	+1	$1+\{r\}\{s\}\{rs\}(\{r^2\}-1)$
.3 : 2	0	$2\{r\}\{s\}(\{r^2\}-1)$
.3 : 2 0	0	$-\{r\}\{s\}\{r^2\}(\{r^2\}-1)$
.2 1 : 2 0	+2	$\{rs\}+2\{r\}^3\{s\}$
.2.2.20	+1	$(\{s^2\}-1)(1+\{r\}\{s\}\{rs\})$
2 : 2 : 2	+3	$1+\{r^2s^4\}-3\{r\}\{\mathrm{s}\}\{rs\}$
2 : 2 0 : 2 0	0	$\{r\}\{s\}(3+\{r\}\{rs^2\})$
8*2	+1	$1-\{r\}\{s\}^3\{rs\}$
5,2,2-	+2	$\{r^{-5}s\}$
4 1,2,2-	0	$-\{r\}\{s\}\{r^2\}$
3 2, 2,2-	+2	$\{2r^{-3}s-r^{-1}s\}$
3 1 1,2,2-	0	$-2\{r\}\{s\}$
2 3, 2, 2−	0	$-\{r\}\{s\}$
2 2 1,2,2-	+2	$\{rs\}+2\{r^{-3}s-r^{-1}s\}$
4, 3,2-	+3	$1+\{r^{-2}s^4\}$
4, 2 1,2-	+1	$1+\{s\}\{r^{-2}s\}$
3 1, 3,2-	+3	$1+\{s^4\}+\{r\}\{rs^{-2}\}$
3 1,2 1,2-	+1	$\{s^2\}-1-\{r\}\{s\}\{rs\}$
3, 3,3-	+4	$\{r^{-3}s^3+rs\}$
3,2 1,2 1-	-1	$\{r\}\{s\}\{r^{-1}s\}-1$
(3, 2) (2, 2−)	0	$-\{r\}\{s\}\{r^2\}$
(2 1, 2) (2, 2−)	0	$\{r\}\{s\}+\{r\}^3\{s\}$
(3, 2−) (2, 2)	+2	$\{rs\}-\{r^3\}\{s\}$
(2 1, 2−) (2, 2)	+2	$\{rs\}+\{r\}^3\{s\}$
(3, 2) − (2, 2)	+2	$\{r^5s\}$
(2 1, 2) − (2, 2)	+2	$\{r\}\{r^2s\}+\{r^{-3}s\}$
2 : −2 0 : −2 0	+4	$\{r^3s+rs^{-3}\}$

3 and 4 string links to 9 crossings

Link	λ		∇
2, 2, 2	+1+1+1		$\{rst\}-\{r\}\{s\}\{t\}$
.1	0 0 0		$\{r\}\{s\}\{t\}$
2,2,2-	+1+1−1		$-\{r^{-1}st\}$
2,2,2+	+1+1−1		$\{r\}\{s\}\{t\}-\{r^{-1}st\}$
4, 2, 2	+2+1+1		$\{r^{-1}s\}(\{rst\}-\{r\}\{s\}\{t\})-\{t\}$
3 1, 2, 2	+2+1+1		$\{rs\}(\{rst\}-\{r\}\{s\}\{t\})-\{t\}$
2, 2, 2+ +	+1+1+1		$\{rst\}-2\{r\}\{s\}\{t\}$
(2, 2) (2, 2)	+2+2 0		$\{r\}\{rs\}\{r^{-1}t\}+\{r\}\{s\}\{t\}$
.3	+1 0 0		$\{rs\}\{r\}\{s\}\{t\}$
.2 : 2 0	0+1−1		$-\{t\}-\{r\}\{s\}\{t\}\{rs\}$
4 , 2 , 2 -	+2+1−1		$-\{r^{-2}s^2t\}$
3 1,2,2-	+2+1−1		$\{t\}-\{\mathbf{rs}\}\{r^{-1}st\}$
(2, 2) (2, 2−)	+2 0 0		$-\{r\}\{s\}\{t\}$
(2, 2) − (2, 2)	+2+2 0		$\{r\}\{s\}\{t\}+\{r\}\{rs\}\{rt\}$
2, 2, 2, 2	+1+1 0	0+1+1	$\{rstu-rs^{-1}t^{-1}u\}-\{r\}\{s\}\{t\}\{u\}$
2, 2, 2, 2−	+1+1 0	Of 1 − 1	$\{rt^{-1}\}\{su^{-1}\}-\{rs^{-1}\}\{tu\}$
2 , 2 , 2 , 2 - -	+1+1 0	0+1+1	$\{rstu-rs^{-1}t^{-1}u\}$
2 1 2, 2, 2	o-i-1-1		$\{r\}\{s\}(\{rs^{-1}t\}+\{r\}\{s\}\{t\})-\{t\}$
21 1 1, 2, 2	0+1−1		$-\{r\}\{s\}(\{rs^{-1}t\}+\{r\}\{s\}\{t\})-\{t\}$
3, 2, 2, 2	+1+1−1		$(1-\{r^2\})\{r^{-1}st\}+\{r\}\{s\}\{t\}\{r^2\}$
2 1, 2, 2, 2	+1+1+1		$\{r^3st\}-\{r\}\{st\}-\{r\}^3\{s\}\{t\}$
4, 2, 2+	+2+1−1		$\{r\}\{s\}\{f\}\{r^{-1}s\}-\{r^{-2}s^2t\}$
3 1, 2, 2+	+2+1−1		$\{rs\}(\{r\}\{s\}\{t\}-\{r^{-1}st\})+\{t\}$
2, 2, 2+ + +	+1+1−1		$2\{r\}\{s\}\{t\}-\{r^{-1}st\}$
(2, 2+) (2, 2)	0+2 0		$-\{r\}\{s\}\{t\}-\{r\}^2\{s\}\{r^{-1}t\}$
(2, 2) 1 (2, 2)	0 0 0		$\{r\}\{s\}\{t\}+\{r\}^3\{s\}\{t\}$
.2 1 1	+1 0 0		$\{r\}^2\{s\}^2\{t\}$
.2 1 : 2	+2+1−1		$-\{r\}^2\{s\}^2\{t\}-\{r^{-2}s^2t\}$
.(2, 2)	*0 0 0*		$-\{r\}^3\{s\}\{t\}$
2 1 2 , 2 , 2 -	0+1+1		$\{r\}\{s\}\{rst^{-1}\}+\{t\}$
21 1 1, 2, 2−	0+1+1		$\{t\}-\{r\}\{s\}\{rst^{-1}\}$
3, 2, 2, 2 -	+1+1+1		$\{r^2\}(\{rst\}-\{r\}\{s\}\{t\})-\{rst\}$
2 1, 2, 2, 2−	+1+1−1		$\{\mathbf{r}\}\{r^{-2}st\}-\{rst\}-\{r\}\{s\}\{f\}$
3, 2, 2, 2− −	+1+1−1		$-\{r\}\{s^{-1}t\}-\{r^{-3}st\}$
(2, 2+) (2, 2−)	*0 0 0*		$\{r\}\{s\}\{t\}$
(2, 2+) − (2, 2)	0+2 0		$-\{r\}\{s\}\{r^2t\}$
.(2, 2−)	+2 0 0		$-\{r\}^2\{t\}\{r^{-1}s\}$
. − (2, 2)	*0 0 0*		0
2, 2, 2, 2+	+1+1 0	0+ 1 − 1	$\{rt^{-1}\}\{su^{-1}\}-\{rs^{-1}\}\{tu\}+$ $\{r\}\{s\}\{t\}\{u\}$

10 crossing alternating knots. Basic polyhedron 1*

T	knot	s	δ^0	A
120	82	r	17/8	[9-4
119	712	r	23/8	[−3+3−3+3−1
102	64	r	25/6	[13−6
122	613	r	27/7	[-7+7-3
117	61 12	r	33/13	[5−5+5−3+1
81	532	r	37/16	[7−7+6−2
78	5212	r	43/16	[−15+11−3
121	514	r	29/6	[5−5+5−2
101	5 113	r	39/11	[−7+7−5+3−1
108	51112	r	45/17	[17−11+3
80	433	r	43/13	[−13+11−4
24	4312	r	47/17	[−11+10−6+2
74	4222	r	53/22	[23−13+2
68	42112	r	57/22	[13−12+8−2
106	4132	r	43/19	[−9+9−6+2
79	4123	r	47/14	[−15+12−4
37	4114	*f*	41/9	[9−7+5−3+1
67	41122	r	55/23	[−19+14−4
107	41113	r	51/14	[−11+11−7+2
77	352	r	35/16	[−11+9−3
66	3412	r	45/16	[9−9+7−2
76	3313	r	49/13	[13−10+6−2
20	33112	r	59/23	[−15+13−7+2
65	3232	r	55/24	[−19+14−4
61	32212	r	65/24	[17−14+8−2
71	32113	r	61/17	[17−13+7−2
16	321112	r	71/27	[−19+16−8+2
105	3 13 12	r	53/19	[19−13+4
62	31222	r	63/26	[−17+15−7+1
60	312112	r	67/26	[−25+17−4
21	31132	r	57/25	[21−14+4
58	311122	r	69/29	[19−15+8−2
22	311113	f	65/18	[25−16+4
104	2512	r	37/13	[13−9+3
52	2422	r	49/20	[21−12+2
51	24112	r	51/20	[−19+13−3
15	2332	f	53/23	[19−13+4
49	23122	r	59/25	[−21+15−4
48	22312	r	61/22	[15−13+8−2
11	222112	r	75/29	[−21+17−8+2
41	221212	r	71/26	[−21+17−7+1
3	2211112	r	81/31	[27-19+7-1
14	212212	*f*	73/27	[23-17+7-1
43	2121112	r	79/30	[−25+19−7+1
1	21111112	*f*	89/34	[31-21+7-1

10 crossing alternating knots. Basic polyhedron 1^*

T	knot	*S*	δ^0	*A*
123	5, 3, 2	*r*	31	[−5+5−4+3−1
116	5, 2 1, 2	*r*	41	[7−7+6−3+1
36	4 1, 3, 2	r	49	[11−9+6−3+1
70	4 1, 2 1, 2	*r*	59	[−13+12−8+3
75	3 2, 3, 2	r	53	[13−11+7−2
18	3 2, 2 1, 2	*r*	67	[−19+15−7+2
109	3 1 1, 3, 2	*r*	59	[−15+13−7+2
57	3 1 1, 2 1, 2	*r*	73	[25−18+6
103	2 3, 3, 2	r	47	[−11+10−6+2
50	2 3, 2 1, 2	r	61	[21−15+5
64	2 2 1, 3, 2	*r*	65	[17−14+8−2
5	2 2 1, 2 1, 2	r	79	[−23+18−8+2
47	2 2, 2 2, 2	r	65	[27−16+3
42	2 2, 2 1, 1, 2	*r*	75	[−23+18−7+1
39	2 1 1, 2 1 1, 2	*r*	85	[29-20+7-1
118	4, 3, 3	r	33	[7−6+5−2
115	4, 3, 2 1	r	45	[9−8+6−3+1
69	4, 2 1, 2 1	*r*	57	[19−14+5
100	3 1, 3, 3	r	51	[−11+10−6+3−1
23	31,321	r	63	[−17+14−7+2
56	3 1, 2 1, 2 1	*r*	75	[−19+16−9+3
63	2 2, 3, 2 1	*n*	63	[−23+16−4
114	2 1 1, 3, 3	*r*	57	[21−14+4
2	2 1 1, 2 1, 2 1	r	87	[−29+21−7+1
53	2 2, 3, 2+	r	67	[−19+16−7+1
7	2 2, 2 1, 2+	r	77	[25−18+7−1
55	21 1, 3, 2+	r	73	[19−16+9−2
4	2 1 1, 2 1, 2+	*r*	83	[−27+20−7+1
72	3, 3, 2 1+	*r*	63	[−23+16−4
40	2 1, 2 1, 2 1+	r	81	[27-19+7-1
73	3, 3, 2++	*r*	57	[15−12+7−2
19	3, 2 1, 2++	r	63	[−17+14−7+2
45	2 1, 2 1, 2++	r	69	[21-16+7-1
35	(3, 2) (3, 2)	*i*	61	[15−12+7−3+1
59	(3, 2) (2 1, 2)	*n*	71	[−17+15−9+3
9	(2 1, 2) (2 1, 2)	*i*	75	[27-20+8-1

10 crossing knots
Alternating, basic polyhedron not 1*

T	knot	s	δ^0	A
99	.4.2	n	63	[−13+12−8+4−1
54	.31.2	n	85	[25−19+9−2
6	.22.2	n	87	[−25+20−9+2
113	.4.20	n	57	[11−10+8−4+1
17	.3 1.20	n	83	[−23+19−9+2
46	.22.20	n	81	[23−18+9−2
13	.21.21	i	101	[35-24+8-1
12	.21.210	r	99	[−33+24−8+1
95	.3.3.2	n	77	[23−17+8−2
33	.3.2.20	n	73	[17−14+9−4+1
44	.21.2.20	n	89	[25−20+10−2
111	.3.20.2	n	67	[−17+15−8+2
97	.3 0.2.2	n	71	[−15+14−9+4−1
8	.210.2.2	n	91	[−27+21−9+2
84	.2.21.2	r	***93***	***[33-22+7-l***
86	.2.210.2	r	87	[−33+22−5
92	.2.2.2.20	n	81	[23−18+9−2
31	.2.2.20.20	f	81	[19−16+10−4+1
112	3:2:2	**r**	***65***	[13−12+9−4+1
90	21:2:2	r	85	[29−21+7
98	3:2:20	n	73	[21−16+8−2
34	30:2:2	r	75	[−21+17−8+2
32	3:20:20	r	77	[19−15+9−4+1
83	21:20:20	r	91	[−29+22−8+1
96	30:2:20	n	75	[−17+15−9+4−1
10	210:2:20	n	93	[31−22+8−1
110	30:20:20	r	63	[−15+14−8+2
27	2.2.2.2	i	85	[21−17+10−4+1
89	2.2.2.20	n	83	[−25+20−8+1
91	2.2.20.2	**r**	***37***	[21−17+9−2
94	8*3	r	87	[−19+17−11+5−1
30	8*2 1	r	111	[−33+26−11+2
93	8*3 0	**r**	***93***	[27−21+10−2
29	8*20.20	i	109	[37-26+9-1
88	8*2:2	r	95	[−21+19−12+5−1
25	8*2:20	n	103	[−31+24−10+2
26	8*2:.2	i	***97***	[23−19+12−5+1
85	8*2:.20	n	101	[31−23+10−2
82	8*20::20	r	105	[37−26+8
28	9*2 0	r	115	[−35+27−11+2
87	9*.20	r	105	[31−24+11−2
38	10*	f	121	[29−24+15−6+1

Non-alternating

L	knot	S	δ^0	A
61	5, 3,2-	r	1	[−1+1+0−1+1
1I	5,2 1, 2−	r	11	[−1+2−2+1
31	4 1,3,2-	r	19	[−5+4−2+1
41	4 1,2 1, 2−	r	29	[7−6+4−1
61V	32,3,2-	r	11	[1+1−3+2
111	3 2, 2 1, 2-	r	25	[9−6+2
31V	31 1, 3, 2−	r	17	[5−4+2
411	3 1 1, 2 1, 2−	r	31	[−11+8−2
3v	2 3, 3, 2-	r	5	[1−1+1
4111	2 3, 2 1, 2−	r	19	[−7+5−1
6V	221,3,2-	r	23	[−3+4−4+2
1IV	221,21,2-	r	37	[13−9+3
2v	2 2, 2 2, 2-	r	15	[−5+4−1
21V	22,21 1,2-	r	25	[11−6+1
2VI	21 1, 2 1 1, 2−	r	35	[−7+8−5+1
6111	4,3,3-	r	3	[−3+2+0−1+1
311	4, 3,2 1−	r	9	[3−2+1
21	4, 2 1, 2 1−	r	21	[5−4+3−1
611	3 1. 3, 3-	r	15	[−1+2−3+2
3111	3 1, 3, 2 1−	r	27	[−7+6−3+1
2111	3 1, 2 1, 2 1−	r	39	[−13+10−3
51	22,3,3-	r	3	[−3+1+1
1111	22,21,21-	r	33	[13−8+2
211	21 1, 3, 2 1−	n	27	[−9+7−2
3VII	(3, 2) (3, 2−)	n	31	[−9+7−3+1
4VIII	(3, 2) (2 1, 2−)	n	41	[11−9+5−1
4VI	(2 1, 2) (3, 2−)	n	29	[7−6+4−1
3IX	(2 1, 2) (2 1, 2−)	n	43	[−13+10−4+1
6VIII	(3, 2)−(3, 2)	r	11	[−5+4−1−1+1
1VI	(3, 2)−(2 1, 2)	n	1	[3−1−1+1
6VII	(2 1, 2)−(2 1, 2)	r	17	[7−4+0+1
2vII	−3:2:2	r	25	[7−5+3−1
3x	−3:2:20	r	35	[−9+8−4+1
4VII	−3:20:20	r	49	[13-11+6-1
2VIII	−30:2:2	r	45	[15−10+4−1
3VIII	−30:2:20	r	49	[−11+9−4+1
4v	−30:20:20	r	21	[3−4+4−1
511	3: -20: − 20	r	5	[3−2+0+1
6VI	21: -20: -20	r	5	[3−2+0+1
21x	-30: -20: -20	r	35	[−11+9−3
3VI	8*-3 0	r	51	[−15+12−5+1
1V	8'2: -20	r	45	[17−11+3
4IV	8*2: .-20	r	39	[−15+10−2

10 crossing 2 string links

10
7 3
6 2 2
5 5
5 2 3
5 1 2 2
4 4 2
4 2 4
4 2 1 3
4 1 2 1 2
411112
3 4 3
3 3 2 2
3 2 2 3
3 2 1 2 2
3 1 4 2
3 1 2 1 3
3 1 1 2 1 2
3111112
2 6 2
2 3 2 1 2
231112
2 2 2 2 2
2 2 1 1 2 2
2 1 4 1 2
2 1 3 1 1 2
2112112
4 2, 2, 2
4 1 1, 2, 2
31 2, 2, 2
31 1 1, 2, 2
2 4, 2, 2
2 3 1, 2, 2
2 1 3, 2, 2
2 1 2 1, 2, 2
2 1 1 2, 2, 2
2 1 1 1 1, 2, 2
4, 2 2, 2
4, 2 1 1, 2
3 1, 2 2, 2
3 1, 2 1 1, 2
2 1 2, 3, 2
2 1 2, 2 1, 2
21 1 1, 3, 2
2 1 1 1, 2 1, 2
2 2, 3, 3
2 2, 2 1, 2 1
2 1 1, 3, 2 1

3, 3, 2, 2
3, 2 1, 2, 2
2 1, 2 1, 2, 2
3, 2, 3, 2
3, 2, 2 1, 2
2 1, 2, 2 1, 2
5, 2, 2+
4 1, 2, 2+
3 2, 2, 2+
3 1 1, 2, 2+
2 3, 2, 2+
2 2 1, 2, 2+
4, 3, 2-t
4, 2 1, 2+
3 1, 3, 2+
3 1, 2 1, 2+
3, 3, 3+
3, 2 1, 2 1+
2 2, 2, 2+ +
2 1 1, 2, 2+
3, 2, 2+ + +
2 1, 2, 2+ + +
(2 2, 2) (2, 2)
(2 1 1, 2) (2, 2)
(3, 2 1) (2, 2)
(3, 2+) (2, 2)
(2 1, 2+) (2, 2)
(3, 2) (2, 2+)
(2 1, 2) (2, 2+)
(3, 2) 1 (2, 2)
(2 1, 2) 1 (2, 2)
.4 1
.3 1 1
.2 3
.2 1 2
.2 1 1 1
.2 1 1.2
.2 11.20
.3.2 1
.3.2 1 0
.4 : 2
.3 1 : 2
.2 1 1 : 2
.2 2 : 2 0
.2 1 1 : 20
.3 : 2 1
.3 : 2 1 0
.2 1 : 2 1

.2 1.2.2
.2 1.2 0.2
.2.3.2
.2.3 0.2
.2.2 1.2 0
.2.2.2.2
.2.2 0.2.2 0
.(3, 2)
.(2 1, 2)
.(2, 2).2
.(2, 2).20
2 1 : 2 : 2 0
2 1 0 : 2 : 2
2 1 0 : 2 0 : 2 0
2.2.2 0.2 0
2.2 0.2.2 0
2 0.2.2.2 0
8*2 1 0
8*2.2 0
8*2 0 : 2 0
8*2 0 : .2 0
8*2 : : 2 0
9*2
9*.2
10**
4 2, 2, 2-
4 1 1, 2, 2-
3 1 2, 2, 2-
3 1 1 1, 2, 2−
2 4, 2, 2-
2 3 1, 2, 2-
2 1 3, 2, 2-
2 12 1, 2, 2−
21 12,2,2-
2 1 1 1 1, 2, 2−
4, 2 2, 2-
4, 2 1 1, 2-
3 1, 2 2, 2-
3 1, 2 1 1, 2−
2 1 2, 3, 2-
2 1 2, 2 1,2-
2 11 1,3,2-
2 11 1, 2 1,2-
2 2, 3, 21-
2 1 1, 3, 3-
211,21,21−

3, 3, 2, 2-
3, 2 1, 2, 2-
2 1, 2 1, 2, 2-
3, 2, 3, 2-
3, 2, 2 1, 2-
2 1, 2, 2 1, 2-
3, 3, 2, 2− −
3, 2 1, 2, 2− −
3, 2, 3, 2− −
3, 2, 2 1, 2− −
(2 2, 2) (2, 2−)
(2 1 1, 2) (2, 2−)
(2 2, 2−) (2, 2)
(2 1 1, 2−) (2, 2)
(3, 2 1) (2, 2−)
(3, 3−) (2, 2)
(2 1, 2 1−) (2, 2)
(3, 2+) (2, 2−)
(2 1, 2+) (2, 2−)
(2, 2+)(3, 2−)
(2, 2+) (2 1, 2−)
(2 2, 2) − (2, 2)
(2 1 1, 2)−(2, 2)
(3, 2 1) − (2, 2)
(3, 2+)−(2, 2)
(21, 2+)−(2, 2)
(2, 2+)−(3, 2)
(2, 2+)−(2 1, 2)
.(2, 2−).2
.(2, 2−).2 0
. −(2, 2).2
.-(2, 2).2 *0*
−2 1 0 : 2 : 2
−2 1 0 : 2 0 : 2 0
−2 1 0 : −2 0 : −20
2. -2.-2 0.2 0
2. -2 0. -2.2 0
8*2. −2 0
8*2 0 : - 2 0
8*−2 0 : - 2 0
8*2 0 : . - 2 0
9*.-2

10 crossing links with 3 or more strings

3 strings		4 strings	5 strings
6, 2, 2	6, 2, 2-	4, 2, 2, 2	2, 2, 2, 2, 2
5 1, 2, 2	5 1, 2, 2-	3 1, 2, 2, 2	2, 2, 2, 2, 2-
3 3, 2, 2	3 3, 2, 2-	2, 2, 2, 2+ +	2, 2, 2, 2, 2- -
3 2 1, 2, 2	3 2 1, 2, 2-	(2, 2, 2) (2, 2)	
2 2 2, 2, 2	2 2 2, 2, 2−	(2, 2) 2 (2, 2)	
2 2 1 1, 2, 2	2 2 1 1, 2, 2-	(2, 2) 1 1 (2, 2)	
4, 4, 2	4, 4, 2−	.(2, 2) 1	
4, 3 1, 2	4, 3 1, 2−	.(2, 2) : 2 0	
3 1, 3 1, 2	3 1, 3 1, 2−	10***	
2 2, 2, 2, 2	2 2, 2, 2, 2-	4, 2, 2, 2-	
2 1 1, 2, 2, 2	2 1 1, 2, 2, 2-	3 1, 2, 2, 2-	
2 1 2, 2, 2+	2 2, 2, 2, 2- -	4, 2, 2, 2−	
2 1 1 1, 2, 2+	(4, 2) (2, 2−)	(2, 2, 2) (2, 2 −)	
3, 2, 2, 2+	(3 1, 2) (2, 2−)	(2, 2, 2−) (2, 2)	
2 1, 2, 2, 2+	(3, 3) (2, 2−)	(2, 2, 2−) (2, 2−)	
4, 2, 2+ +	(2 1, 2 1) (2, 2−)	(2, 2, 2− −) (2, 2)	
3 1, 2, 2+ +	(3, 2 1−) (2, 2)	(2, 2, 2) − (2, 2)	
2, 2, 2+ + + +	(2, 2+ +) (2, 2−)	.(2, 2−) 1	
(4, 2) (2, 2)	(4, 2) − (2, 2)	.(2, 2−) : 2 0	
(3 1, 2) (2, 2)	(3 1, 2) − (2, 2)	. −(2, 2) : 2 0	
(3, 3) (2, 2)	(3, 3) − (2, 2)	10−***	
(2 1, 2 1) (2, 2)	(2 1, 2 1) − (2, 2)		
(2, 2+ +) (2, 2)	(2, 2+ +) − (2, 2)		
(2, 2+) (2, 2+)	(2, 2), 2, (2, 2 −)		
(2, 2+) 1 (2, 2)	(2, 2), -2, (2, 2)		
(2, 2), 2, (2, 2)	(2, 2), 2, − (2, 2)		
.5	(2, 2−), 2, (2, 2−)		
.3 2	.(2, 2−) : 2		
.2 2 1	. −(2, 2) : 2		
.3.3	2 0. −2. −2 0.2 0		
.3.3 0			
.3 : 3			
.3 : 3 0			
. 2 1 : 2 1 0			
.4 : 2 0			
.3 1 : 2 0			
.2 2 : 2			
.2.3.2 0			
.(2, 2) : 2			
.(2, 2+)			
20.2.20.20			
8*2.2			
8*2 : : 2			

Alternating 11 crossing knots. Basic polyhedron 1*

L	knot	L	knot	L	knot	L	knot
1	11	278	3 2 123	109	2 4, 2 1, 2	84	3, 3, 2 1, 2
5	9 2	324	3 2 1 2 1 2	268	2 3 1, 3, 2	357	3, 2 1, 3, 2
13	8 3	320	3 2 1 1 2 2	307	2 3 1, 2 1, 2	2 2 5	3, 2 1, 2 1, 2
60	7 4	341	3 2 1 1 1 1 2	31	21 3, 3, 2	220	2 1, 3, 2 1, 2
23	7 2 2	37	3 1 4 1 2	131	2 1 3, 2 1, 2	2 4 0	2 1, 2 1, 2 1, 2
3	7 1 3	119	3 1 3 2 2	290	2 1 2 1, 3, 2	3 0	5, 3, 2+
187	6 5	135	3 1 3 1 1 2	329	2 1 2 1, 2 1, 2	9 3	5, 2 1, 2+
27	6 2 3	311	3 1 2 3 2	113	2 1 1 2, 3, 2	2 4 9	4 1, 3, 2+
80	6 2 1 2	138	3 1 2 1 2 2	330	21 1 2, 2 1, 2	122	4 1, 2 1, 2+
22	6 1 2 2	298	3 1 2 1 1 3	130	2 1 1 1 1, 3, 2	3 0 0	3 2, 3, 2+
20	6 1 1 1 2	284	31 142	345	2 1 1 1 1, 2 1, 2	321	3 2, 21, 2+
250	5 4 2	314	3 1 1 3 1 2	17	5, 2 2, 2	124	3 1 1, 3, 2+
81	5 3 3	338	3 1 1 2 1 1 2	14	5, 2 1 1, 2	334	3 1 1, 2 1, 2+
24	5 2 4	134	3 1 1 1 3 2	246	4 1, 2 2, 2	120	2 3, 3, 2+
105	5 2 2 2	401	3 1 1 1 2 1 2	269	4 1, 2 1 1, 2	3 3 3	2 3, 2 1, 2+
232	52 13	128	3 1 1 1 1 1 3	282	3 2, 2 2, 2	319	2 2 1, 3, 2+
4	5 1 5	347	3 1 1 1 1 1 1 2	294	3 2, 2 1 1, 2	350	2 2 1, 2 1, 2+
79	5 1 2 3	32	2 6 1 2	116	3 1 1, 2 2, 2	3 1 7	2 2, 2 2, 2+
34	5 1 2 1 2	118	2 5 2 2	133	3 1 1, 2 1 1, 2	3 4 8	2 2, 2 1 1, 2+
90	5 1 1 2 2	117	2 5 1 1 2	126	2 3, 2 2, 2	342	211,211,2-t
104	5 1 1 1 1 2	293	24 3 2	132	2 3, 2 1 1, 2	19	4, 3, 3+
251	4 4 3	136	2 4 1 2 2	318	2 2 1, 2 2, 2	9 1	4, 3, 2 1+
248	44 12	313	2 3 3 1 2	328	2 2 1, 2 1 1, 2	2 7 0	4, 2 1, 2 1+
273	43 22	335	2 3 2 1 1 2	2	5, 3, 3	235	3 1, 3, 3+
272	43 1 1 2	127	2 3 1 3 2	78	5, 2 1, 2 1	299	3 1, 3, 2 1+
103	423 2	400	2 3 1 2 1 2	230	4 1, 3, 2 1	129	3 1, 2 1, 2 1+
275	4 2 2 3	346	2 3 1 1 1 1 2	85	3 2, 3, 3	108	2 2, 3, 3+
233	4 2 1 4	310	2 2 3 2 2	281	3 2, 2 1, 2 1	3 2 5	2 2, 2 1, 2 1+
283	42 12 2	344	2 2 2 2 1 2	107	3 1 1, 3, 2 1	337	2 1 1, 3, 21+
94	4 2 1 1 3	343	2 2 2 1 2 2	100	2 3, 3, 2 1	340	2 2, 3, 2++
29	4 1 4 2	349	2 2 2 1 1 1 2	83	2 2 1, 3, 3	353	2 2, 2 1, 2++
33	4 1 3 1 2	351	2 2 1 1 2 1 2	301	2 2 1, 2 1, 2 1	3 3 9	2 1 1, 3, 2++
35	4 1 2 1 3	327	2 2 1 1 1 2 2	26	2 1 2, 3, 3	356	2 1 1, 2 1, 2++
123	4 1 2 1 1 2	354	2 2 1 1 1 1 1 2	114	2 1 2, 3, 2 1	7 7	3, 3, 3++
271	41 132	38	2 1 5 1 2	287	2 1 2, 2 1, 2 1	312	3, 2 1, 2 1++
297	4 1 1 2 1 2	139	2 1 4 1 1 2	82	2 1 1 1, 3, 3	4 0 2	3, 3, 2+++
21	4 1 1 1 4	336	2 1 3 2 1 2	306	2 1 1 1, 3, 2 1	322	3, 2 1, 2+++
274	4 1 1 1 1 3	143	2 1 3 1 1 1 2	302	21 1 1, 2 1, 2 1	140	2 1, 2 1, 2+++
137	4 1 1 1 1 1 2	352	2 1 2 2 1 1 2	18	4, 2 2, 3	245	(2 2, 2) (3, 2)
106	3 6 2	332	2 1 1 3 1 1 2	89	4, 2 2, 2 1	289	(2 2, 2) (2 1, 2)
252	3 5 3	355	2 1 1 2 1 1 1 2	16	4, 2 1 1, 3	280	(21 1, 2) (3, 2)
296	3 422	231	4 2, 3, 2	102	4, 2 1 1, 2 1	3 0 4	(2 1 1, 2) (2 1, 2)
92	3 4 1 3	247	4 2, 2 1, 2	253	3 1, 2 2, 3	234	(3, 2 1) (3, 2)
279	3 3 23	15	41 1, 3, 2	292	3 1, 2 2, 2 1	266	(3, 2 1) (2 1, 2)
316	3 3 2 1 2	101	41 1, 2 1, 2	277	3 1, 2 1 1, 3	2 5 4	(3, 2+) (3, 2)
295	3 3 1 2 2	36	3 1 2, 3, 2	309	3 1, 2 1 1, 2 1	2 9 1	(3, 2+) (2 1, 2)
315	3 5 1 1 1 2	115	3 1 2, 2 1, 2	99	2 2, 2 2, 3	112	(2 1, 2+) (3, 2)
121	3 2 4 2	276	3 1 1 1, 3, 2	326	2 2, 2 1 1, 2 1	3 3 1	(2 1, 2+) (2 1, 2)
323	3 2 2 2 2	308	3 1 1 1, 2 1, 2	111	21 1, 2 1 1, 3	25	(3, 2) 1 (3, 2)
125	3 2 2 1 3	28	2 4, 3, 2	12	3, 3, 3, 2	96	(3, 2) 1 (2 1, 2)
						238	(2 1, 2) 1 (2 1, 2)

Alternating 11 crossing knots. Basic polyhedron not 1*

L	knot	L	knot	L	knot	L	knot
75	.41.2	7	.3.20.2.20	53	20.3.2.2	155	9*2.2
229	.41.20	43	.21.20.2.20	176	2.3.20.20	44	9*2.20
264	.3 11.2	50	.(3, 2).2	196	2.2 1.20.2 0	149	9*2 0.2
98	.3 11.20	200	.(2 1, 2).2	8	2 0.3.2 0.2	39	9*2:2
263	.2 3.2	51	.2.(3, 2)	64	20.2 1.20.2	161	9*2:20
97	.23. 20	195	.2.(2 1, 2)	167	2.2.2.2.2 0	168	9*2 0: .2 0
288	.2 12.2	178	.(3, 2).2 0	157	2.2.2.2 0.2 0	145	9*.2: .2
110	.2 1 2.2 0	204	.(2 1, 2).2 0	169	2.2 0.2.2.20	153	9*.2: .20
305	.2 1 1 1.2	177	.2 0.(3, 2)	212	8*2 2	147	9' : 2 0.2 0
303	.2 1 1 1.20	197	.2 0.(2 1, 2)	191	8*2 1 1	163	9*2 0 : : 20
74	.4.2 1	73	2 2:2:2	61	8*4 0	148	10*20
76	.4.2 10	65	2 1 1:2:2	214	8*3 1 0	150	10**2
265	.3 1.2 1	59	4:2:20	188	8*2 1 1 0	410	10**20
267	.3 1.2 10	226	3 1:2:20	48	8*3.20	151	10** : 2
285	.2 2.2 1	262	2 1 1 : 2 : 2 0	190	8*2 1.2 0	144	100** : 2 0
286	.2 2. 2 1 0	170	4 0:2:2	173	8*3 0.2 0	411	11*
58	.4.2.2	71	3 1 0:2:2	198	8*2 1 : 2		
219	.3 1.2.2	209	2 1 1 0:2:2	172	8*3 : 2 0		
256	.2 1 1.2.2	206	2 2:2 0:2 0	192	8'2 1 0 : 2		
244	.2 2.2.2 0	205	2 1 1:2 0:2 0	47	8*3 0:2 0		
261	.2 1 1.2.20	242	2 2 0:2:2 0	199	8*2 1 0 : 2 0		
11	.4.2 0. 2	257	2 1 1 0 : 2 : 2 0	193	8*2 1 : .2		
228	.3 1.2 0.2	9	4 0:2 0:2 0	49	8*3 : .2 0		
95	.2 1 1.2 0.2	227	3 1 0:2 0:2 0	201	8*2 1 0 : .2		
243	.2 2 0.2.2	63	2 1 1 0 : 2 0 : 20	174	8*3 0: .2 0		
260	.2 1 10.2.2	69	3:2 1:2	189	8*2 1'0: .2 0		
186	.2.4.2	217	3: 2 1 : 2 0	171	8*3 : : 2 0		
54	.2.3 1.2	237	2 1: 2 1 : 2 0	146	8*2 1 : : 2 0		
213	.2.2 2.2	86	3:2 1 0:2	46	8*3 0 : : 2 0		
10	.2.4 0.2	259	2 1:2 1 0:2	403	8*2.2 0.2		
184	.2.3 10.2	223	3 0:2 1:2	154	8*2.2 0.2 0		
72	.2.2 2 0.2	221	3:2 1 0:2 0	166	8*2.2 0:2		
66	.3.2 1.2	87	3 0:2 1:2 0	40	8*2.2 0:2 0		
224	.3.2 1.2 0	216	3 0:2 1 0:2	404	8*2 0.2 : 2		
255	.2 1.2 1.20	67	3 0:2 1 0:2 0	405	8*2 0.2:2 0		
70	.3.2 10.2	214	2 1 0: 2 1 0 : 20	156	8*2 0.2 0 : 2 0		
215	.3 0.2 1.2	194	2 1.2.2.2	164	8*2 0.2 : .2		
258	.2 1 0.2 1.2	56	3.2.2.2 0	41	8* 20.2 : .2 0		
218	.3.2.2 1	181	3.2.2 0.2	158	8*2 0.2 0: .2		
236	.2 1.2.2 1	55	3.2 0.2.2	165	8'2 : 2 : 2 0		
222	.3.2.2 10	202	2 10.2.2.2	162	8*2 : 2 0 : 2 0		
68	.3.2 0.2 1	180	3 0.2.2.2 0	62	8*2 0 : 2 0 : 2 0		
239	.2 1.2 0.2 1	207	2 10.2.2.20	42	8*2: .2 0: .2		
88	.3 0.2.2 1	6	3 0.2.2 0.2	152	8*2: .2: .2 0		
175	.3.2.2.2	45	2 10.2.2 0.2	57	9*3		
159	.2 1.2.2.2	179	3 0.2 0.2.2	406	9*2 1		
211	.2 1.2.2.20	160	2 10.20.2.2	185	9*3 0		
182	.3.2.2 0.2	203	2.2 1.2.2	407	9*.3		
52	.3 0.2.2.2	183	2.3.2.2 0	408	9*.2 1		
210	.2 1.2.20.20	208	2.2 1.20.2	409	9*.3 0		

Non-alternating 11 crossing knots

42,3,2−
42,212-
41 1,3,2-
41 1,21,2-
312,3,2−
312,21,2-
3111,3,2-
3111,21,2-
24,3,2-
24,21,2-
231,3,2−
23 1,21,2-
213,3,2-
21 3,21,2-
2121,3,2-
2121,21,2-
21 12,3,2-
2112,21,2-
21 11 1,3,2-
21111,21,2-
5,22,2−
5,211,2−
41,22,2−
41,21 1,2-
32,22,2-
32,211,2-
3 11,22,2-
311,211,2-
23,22,2−
23,211,2-
221,22,2−
221,211,2−
5,3,21−
41,3,3-
41,21,21-
32,3,21−
311,3,3-
311,21,21-
23,3,3-
2 3,21,21-
221,3,21-
2 12,3,3-
212,3,21-
212,21,21-
2 111,3,3-
21 11,3,21-
21 11,21,21-

4,22,3-
4,22,21−
4,21 1,3-
4,21 1,21−
31,22,3-
31,22,21−
31,211,3-
31,21 1,21-
22,22,21-
22,211,3−
211,211,21−
3,3,3,2-
3,3,21,2-
3,2 1,3,2-
3,2 1,2 1,2-
2 1,3,2 1,2-
21,21,21,2−
3,3,3,2−
3,3,21,2−−
3,21,3,2−−
(22,2)(3,2−)
(22,2)(21,2−)
(211,2)(3,2−)
(211,2)(21,2−)
(3,21)(3,2−)
(3,21)(21,2−)
(3,2+)(3,2−)
(3,2+)(21,2−)
(21,2+)(3,2−)
(21,2+)(21,2−)
(22,2−)(3,2)
(22,2−)(21,2)
(211,2−)(3,2)
(21 1,2−)(21,2)
(3,3−)(3,2)
(3,3−)(21,2)
(21,21−)(3,2)
(21,21−)(21,2)
(22,2)−(3,2)
(22,2)−(21,2)
(21 1,2)−(3,2)
(211,2)−(21,2)
(3,21)−(3,2)
(3,21)−(21,2)
(3,2+)−(3,2)
(3,2+)−(21,2)
(21,2+)−(3,2)
(21,2+)−(21,2)

.(3,2−).2
.(21,2−).2
.2.(3,2−)
.2.(21,2−)
.(3,2−).20
.(21,2−).20
.20.(3,2−)
.20.(21,2−)
.−(3,2).2
.−(21,2).2
.2.−(3,2)
.2.−(21,2)
.(3,2).20
.20.−(3,2)
−22:2:2
−220:2:20
−22:20:20
-22: -20: -20
22: -20: -20
−211:2:2
−2110:2:20
−211:20:20
−211:−20:−20
−40:2:2
−4:2:20
−40:20:20
-40: -20: -20
−310:2:2
−310:20:20
-3 1 o:-20: -20
−2110:2:2
−211:2:20
−2110:20:20
−2110:−20: −20
−30:21:2
−30:21:-20
−30:210:2
−210:30:2
-210: − 30: -20
−210:21:2
−210:−210:−20

2.-21.2.2
2.21.−2.2
2.-3.2.20
2.3.−2.20
20.3.−2.2
2.−3.−20.20
2.−21.−20.20
20. -3. -20.2
20.−21.−20.2
2.2.−2.2.20
2.2. -2.20.20
2.20.−2.2.20
8*−40
8*-310
8*-21 10
8*-3 0.20
8*3 : -20
8*−210:2
8*−30:20
8*30: -20
8*−210:20
8*-210: .20
8*−30: .20
8*-210: .20
8*30:: -20
8*3: : -20
8*2 1 :: -20
8*2. -20.2
8*2.−20.20
8*2.20.−20
8*2:2: -20
8*2:20:−20
8*2:−20:20
8*20:−20:20
8*20:20: -20
8*2: .-20: .2
8*2: .2: .-20
9*.-3
9*.-21
9*2. -2
9*20.−2
9*.2: .-2
9*.−2:.−2
9*.20: .-2
10*−20
10**−20

REFERENCES

1. J. W. Alexander and G. B. Briggs: On types of knotted curves. *Ann. of Math.* 28 (1926–27), 562.
2. A. L. Anger: Machine calculation of knot polynomials. Princeton Senior Thesis, 1959.
3. R. H. Fox: A quick trip through knot theory. ***Topology of 3-manifolds and related topics*** (Prentice-Hall, Englewood Cliffs, N.J., 1962).
4. C. N. Little: On knots, with a census to order *10. Trans. Conn. Acad. Sci.* **18** (1885), 374378.
5. C. N. Little: Alternate ± knots of order 11. *Trans. Roy. Soc. Edin.* ***36*** (1890), 253-255.
6. C. N. Little: Non-alternate ± knots. *Trans. Roy. Soc. Edin.* ***39*** (1900), 771-778.
7. K. Murasugi: On a certain numerical invariant of link types. *Trans. Amer. Math. Soc.* **117** (1965), **387-422.**
8. **K.** Reidemeister: ***Knotentheorie*** (reprint) (Chelsea, New York, 1948).
9. P. G. Tait: On knots, I.
10. P. G. Tait: On knots, II.
11. P. G. Tait: On knots, III.

} First published separately, but available together in Tait's ***Scientific Papers,*** **Vol. I,** pp. 273-347 (C.U.P., London, 1898).

Computations in knot theory

H. F. TROTTER

1. Computer representation of knots. The commonest way of presenting a specific knot to the human eye is by a diagram of the type shown in Fig. 1, which is to be interpreted as the projection of a curve in 3-dimensional space.

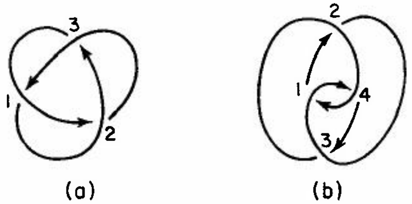


FIG. 1

There are obviously many ways of coding the information in such a diagram for a computer. Conway's notation [2] (which I learned of for the first time at the conference) seems to me much the best both for handwork and (perhaps with some modification) for computer representation. In some work done at Kiel [3, 4, 11] under the direction of Prof. G. Weise, one notation used is based on noting the cyclic order of vertices around the knot, and another is related to Artin's notation for braids. The simple notation described below is what I have actually used for computer input. It has proved reasonably satisfactory for experimental purposes.

To each vertex of the diagram there correspond two points on the knot, which we refer to as the upper and lower nodes. Each node has a successor arrived at by moving along the knot in the direction indicated by the arrows. Each vertex has one of two possible orientations, as indicated in Fig. 2. If the vertices are then numbered in an arbitrary order, a complete descrip-

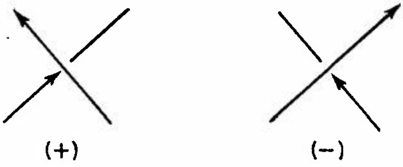


FIG. 2

tion of the diagram is obtained by listing, for each vertex, its orientation and the successors of its upper and lower nodes. The descriptions of the diagrams in Fig. 1 are then

```
(a) 1+L2 U2          (b) 1 -L4 L2
    2+L3 U3              2-U4 U3
    3+L1 U1              3-U1 U2
                         4-L1 L3
```

where *L*, *U* stand for "lower" and "upper".

This description is highly redundant, but the redundancy is at least in part a virtue, since it increases the likelihood that a coded description is correct if it is self-consistent. In practice, the notation is fairly easy to use, although errors in recording the orientations of vertices do crop up.

The coding just described is intended to be convenient to write down, and does not correspond directly to a useful internal representation for a knot. Some sort of list organization appears to be most appropriate, and the list-processing language ***L6*** [7] was chosen because it was available and seemed to be well-suited to the problem. In addition to efficient mechanisms for storage allocation and subroutine organization, ***L6*** has several distinctive features. It deals with blocks of computer words as single objects, and provides for declaration of fields (denoted by single letters) within blocks. A field may contain either a pointer to another block, or numerical or coded data. Indirect referencing (up to five levels deep) is denoted simply by concatenation. For example, XAT refers to field ***T*** of the block pointed to by field ***A*** of the block pointed to by pseudo-register X.

A program has been written which reads a knot description, making some elementary checks for consistency, and produces a linked list of blocks in which there is one block for each node. Each block contains fields which point to the preceding and following nodes and to the other node at the same vertex. Other fields contain the vertex number and indicators for the orientation of the vertex and the type of the node (upper or lower). The program will also handle links (i.e. knots with more than one component) and another field contains the number of the component to which the node belongs. In addition, each block contains two fields used to link it temporarily into various lists for housekeeping purposes during computation. In this representation it turned out to be quite easy to write a program to perform trivial simplifications of diagrams by application of the Reidemeister moves $\Omega.1$, $\Omega.2$ ([**12**], p. 7) (see Fig. 3).

2. Computation of algebraic invariants of knots. The most straightforward application of computers to knot theory is in the computation of known algebraic invariants. The first work of this kind that I know of was done in 1959 at Princeton [**1**] on an IBM 650 computer, and consisted of the calculation of Alexander polynomials for the alternating 10-crossing knots in Tait's tables [**15**]. Similar calculations were later made for the non-alternating 10-crossing knots and for the alternating 1 l-crossing knots in the tables of Tait and Little [**8, 9, 10, 15**]. (Conway independently did these calculations by hand for his own knot tables [**2**].) Programs for computing the Alexander polynomial and several other invariants are described in [**3**].

The most generally useful algebraic invariants of knots are connected with the homology of cyclic coverings of the complement of the knot. Seifert [**14**] showed that these invariants can be computed from an integer matrix constructed as follows. The first step is to find a non-self-intersecting orientable surface with the knot as boundary. (It is not altogether obvious that such a surface always exists, but Seifert actually indicates a method of constructing one for any knot diagram.) Unless the knot is trivial, the surface has a genus h greater than 0, and its first homology group is free abelian on $2h$ generators. A system of $2h$ closed curves which represent an integral basis for this homology group can be found on the surface. A Seifert matrix for the knot is then obtained by taking as ijth entry the linking number (in 3-space) of the ith basis curve with a curve obtained by lifting the jth basis curve slightly above the surface. (The side of the surface which is "above" is of course determined by the orientation of the surface.) Any knot has infinitely many different Seifert matrices belonging to it (and any Seifert matrix belongs to infinitely many distinct knots).

Programming an algorithm to find a Seifert matrix from a knot description is an interesting problem. An especially noteworthy program in [**3**] actually finds a Seifert surface and transforms it into the canonical form of a disk with attached bands, from which a Seifert matrix is then easily obtained. I have written an ***L6*** program which finds a set of basis curves and computes the matrix without first altering the surface.

Let us say that two Seifert matrices are s-equivalent if they are the first and last members of some finite sequence of matrices such that for each consecutive pair in the sequence there is some knot to which both matrices of the pair belong.

No purely algebraic characterization of s-equivalence is known, but it is closely related to the property of congruence of matrices. We say that matrices A and B are congruent over a ring R if $A = PBP'$ where P' is the transpose of P, and both P and its inverse have elements in R. It is quite obvious that two Seifert matrices which are congruent over the integers are s-equivalent, since any such change in the matrix can be obtained simply by choosing a different basis for the first homology group of the Seifert surface. The converse is known to be false, but a modified converse is true [**16**].

Before stating this converse we must remark that any Seifert matrix is s-equivalent to a non-singular one (unless it is s-equivalent to one belonging to the trivial knot), and that if V and W are s-equivalent non-singular matrices then $\det(V) = \det(W)$. (In fact $\det(V - tV') = \det(W - tW') = A(t)$, the Alexander polynomial of the knot.) The statement then is that two s-equivalent non-singular Seifert matrices are congruent over the subring of the rationals generated by the reciprocal of their common determinant, and are a *fortiori* congruent over the rationals. Note that for the special case of the determinant equal to ± 1, integral congruence and s-equivalence coincide.

Even the question of whether two Seifert matrices are congruent over the rationals presents some difficulty. Seifert matrices are not symmetric (indeed $V-V'$ is always non-singular, with determinant 1), so that ordinary quadratic form theory does not apply. This problem has been studied (see **[17]** and its bibliography) and it appears to reduce to questions about quadratic forms in algebraic number fields for which algorithmic solutions are (at least in principle) known.

Questions of congruence over the integers or some other subring of the rationals are of course much more complicated. One becomes involved with determining whether matrices are similar over the ring as an initial step. This problem is connected with that of determining whether two ideals in an algebraic number field are in the same class, and is in general even more difficult.

The prospect for completely general algorithms for determining the congruence classes of Seifert matrices does not therefore seem very hopeful. Something less than complete generality, however, can still be useful. A system of Fortran programs for manipulating integer matrices has been written, and has been used so far for computing Alexander polynomials from the Seifert matrices. Some calculations on individual knots have also been carried out, and in particular the knots labelled 9-28 and 9-29 in Reidemeister's table [7] have been shown to have integrally congruent Seifert matrices. This experience indicates that programs which will automatically decide the s-equivalence of Seifert matrices in a great many cases may be quite feasible. Such programs must combine calculation of nivariants which potentially may distinguish the matrices with a search (guided by the theory) for a demonstration of equivalence if the invariants turn out not to distinguish the matrices.

3. Manipulation of knot diagrams. The major project in knot theory in which it appears most reasonable to use a computer is to check and extend the tables of knots and their various computable invariants. Tables which are generally believed to be complete and accurate (except for a few errata noted by Seifert [**14**]) are given in Reidemeister's book **[12]** for all prime knots of less than ten crossings. These tables include, besides diagrams of the knots themselves, the Alexander polynomials, the torsion numbers of degrees 2 and 3, and the Minkowski invariants of the quadratic forms of these knots. Tables of knot diagrams for knots of up to 10 crossings, and of alternating knots of 11 crossings, published by Tait, Kirkman, and Little **[5, 6, 8, 9, 10, 15]** during the 1880's, have already been referred to. Conway has made more extensive tables, and found a few errors in the earlier ones.

So far as I know, no other attempts at tables of 10- or 11-crossing knots have been made.

While it seems feasible, although perhaps not easy, to get a program to create all possible knot diagrams of a given complexity, a real difficulty (which becomes more and more serious as the complexity of the diagrams increases) is that a given knot may appear in a number of different forms. Within the limits of the tables that have been made so far, it is humanly possible to recognize the equivalence of these forms, but it is not clear how to make a computer program to do this with any reasonable degree of efficiency.

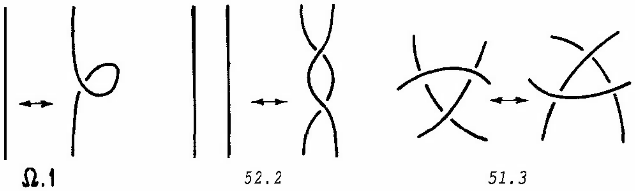


Fig. 3.

If two diagrams are suspected of representing the same knot, then one may attempt to transform one into the other by a sequence of Reidemeister moves, which are indicated schematically in Fig. 3. It is known that if the knots are in fact equivalent, then some sequence of moves which will convert one into the other does exist. It is not hard to make a program to carry out individual moves, but it appears difficult to program anything more efficient than an exhaustive search of all possibilities. Some interesting programs have been written at Kiel [**4**, **11**] which seem to work quite well and have been used successfully to tabulate all knots of up to 8 crossings. The empirical evidence furnished by the handwork of Tait, Little, and Conway, however, shows that the number of distinct diagrams of a given knot rises rapidly as the number of crossings increases, and it is not clear that these programs would be usable for classifying knots of more than 9 crossings.

Another possible technique is that of trying to reduce given projections of knots to a form with a minimum number of bridges or overpasses. (A bridge is a maximal sequence of consecutive upper nodes. In Fig. 1(a) there are 3 bridges. Figure 1(b), in spite of having more vertices, has only 2 bridges.) Practically all the knots of less than 12 crossings can be put in a form with not more than 4 bridges, and the great majority can be reduced to 2 or 3.

The advantage of diagrams with only a few bridges is that even though they may contain many vertices, they can be characterized by a comparatively small number of integers. A knot with only 2 bridges, for example, can be characterized by a pair of integers (a, b), with a odd and b relatively prime to a. Schubert [**13**] showed that knots (a, *b*) and (c, *d*) are equivalent if and only if a = c and either $b \equiv d$ (mod a) or $bd \equiv 1$ (mod a). The situation with 3 and 4 bridges is certainly a good deal more complicated. It appears to be easy enough to reduce diagrams to forms that have a good chance of having a minimal number of bridges. The crucial (as yet unanswered) question is whether there are criteria for the equivalence of the corresponding knots which are powerful enough to be helpful and simple enough to be usable. (Simple necessary and sufficient conditions are probably too much to hope for.)

Note added in proof. As his senior undergraduate thesis at Princeton in 1968, D. Lombardero wrote a Fortran program which accepts as input the description of a knot or link in Conway's notation and calculates a Seifert matrix for it. In part, the program uses an algorithm due to A. Tristram which was communicated to me by Conway at the conference. The computation of matrices and Alexander polynomials for all the knots listed by Conway required less than five minutes on an IBM 7094.

REFERENCES

1. A. L. ANGER: Machine calculation of knot polynomials. Princeton Senior Thesis, 1959.
2. J. H. CONWAY: An enumeration of knots and links, and some of their algebraic properties. These Proceedings, pp. 329-358.
3. P. GROSSE: Die Berechnung spezieller Knoteninvarianten mit Hilfe elektronischer Rechenanlagen, Diplomarbeit, Kiel, 1962.
4. J. KIELMANN: Koordinatenunabhängige Normierung und Erzeugung von Knoten, Diplomarbeit, Kiel, 1965.
5. T. P. KIRKMAN: The enumeration, description and construction of knots of fewer than ten crossings. *Trans. Roy. Soc. Edinburgh 32* (1885), 281-309.
6. T. P. KIRKMAN: The 364 unifilar knots of ten crossings enumerated and defined. *Trans. Roy. Soc. Edinburgh 32* (1885), 483-506.
7. K. C. KNOWLTON: A programmer's description of *L6. Comm. Assoc. Comp. Mach. 9* (1966), 616-625.
8. C. N. LITTLE: On knots, with a census for order ten. *Connecticut Trans. 7* (1885). 27–43.
9. C. N. LITTLE: Non-alternate ± knots, of orders eight and nine. *Trans. Roy. Soc. Edinburgh 35* (1889), 663-665.
10. C. N. LITTLE; Alternate ± knots of order 11. *Trans. Roy. Soc. Edinburgh 36* (1890), 253-255.
11. V. MALERCZYCK: Ein Verfahrung zur Aufzählung von Knoten mit Hilfe elektronischer Rechenanlagen, Diplomarbeit, Kiel, 1966.
12. K. REIDEMEISTER: *Knotentheorie*, Erg. d. Math. 1, No. 1, 1932 (reprint Chelsea, New York, 1948).
13. H. SCHUBERT: Knoten mit zwei Brücken. *Math. 2.65* (1956), 133-170.
14. H. SEIFERT: Über das Geschlecht von Knoten. *Math. Ann.* **110** (1934), **571-592.**
15. P. G. TAIT: On knots, I, II, III *(1877,* 1884, 1885). *Scientific Papers* **I, 273-347.**
16. H. F. TROTTER: Homology of group systems with applications to knot theory. *Ann. Math. 76* (1962), 464-498.
17. G. E. WALL: On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Australian Math. Soc. 3* (1963), 1-62.

Computer experiments on sequences which form integral bases

SHEN LIN

LET $S \equiv \{s_1, s_2, \ldots, s_k, \ldots\}$ be a sequence of positive integers and consider the set P(S) consisting of all numbers which are representable as a sum of a finite number of distinct terms from S. We say S is complete if all sufficiently large integers belong to P(S). For a complete sequence, we call the largest integer not in P(S) the threshold of completeness and denote it by $\theta(S)$. Necessary and sufficient conditions for various sequences to be complete have been studied by many authors [**1, 2, 3, 4**]. In particular, R. L. Graham [**4**] showed by elementary methods that any sequence generated by an integral valued polynomial f(x) is complete if f(x) satisfies the following (obviously necessary) conditions :

(1) The polynomial f(x) has positive leading coefficient, and

(2) For any prime p, there exists an integer m such that p does not divide $f(m)$.

The method he used in the proof is constructive in nature, and with it he also determined the threshold of completeness for the sequence of squares $S \equiv \{1, 4, 9, \ldots\}$ as 128 and for the sequence of cubes $S \equiv \{1, 8, 27, \ldots\}$ as 12758. A closer look at his method reveals that it is easily adaptable for machine implementation. Indeed, it is possible to prove that some sequences are complete and find their thresholds of completeness by a computer in spite of the fact that the solution to this problem appears to require the verification of an infinite number of cases, namely, that all numbers larger than the threshold are indeed representable as a sum of distinct terms from S. To be able to do this, we require that the sequence S satisfy the following property which we shall call condition A.

Condition A. There exists an integer j_S such that for all $k \geqslant j_S$ *we* have $2s_k \geqslant s_{k+1}$.

All sequences which we shall consider satisfy this condition trivially. In addition, we may without loss of generality assume that the sequence $S \equiv \{s_1, s_2, \ldots, s_k, \ldots\}$ is arranged in a nondecreasing manner, i.e. $s_i \leqslant s_j$ if $i < j$.

In the following, we shall show how one may use the computer to prove some sequences complete and find their thresholds of completeness. The method was suggested to me by Dr. R. L. Graham of the Bell Telephone Laboratories to whom I give my sincerest thanks here.

Given a sequence S $\equiv \{s_1, s_2, \ldots, s_k, \ldots\}$ satisfying condition A. Assume that the integer j_S is known such that for all $k \geqslant j_S$, we have $2s_k \geqslant s_{k+1}$. Let $P_k(S)$ denote the set of all numbers which are **represent**able as a sum of distinct terms taken from the first k terms $\{s_1, s_2, \ldots, s_k\}$ of S, including zero. $P_k(S)$ may be computed recursively as follows :

$$P_1(S) = \{0, s_1\},$$

$$P_{k+1}(S) = P_k(S)\ U\{P_k(S) + \{s_{k+1}\}\},$$

where, as usual, $A+B \equiv \{x \mid x = a+b,\ a \in A,\ b \in B\}$.

Suppose all integers from a through b ($\geqslant a$) belong to $P_k(S)$ while a- 1 and $b+$ 1 do not. Then we call *[a, b]* an ***interval*** in $P_k(S)$ and define its length as $b+$ 1 -a. For each $k \geqslant j_S$, as soon as $P_k(S)$ is computed, we determine the interval $[x_k, y_k]$ in *P,(S)* having the longest length l_k (if there are two or more intervals with the same length, we pick the one with the **smallest** x_k) and compare it with s_{k+1}. If $l_k < s_{k+1}$, we set k to k+ 1, and go on, repeating the above procedures. If $l_k \geqslant s_{k+1}$, we have proven that S is complete and the determination of the threshold of completeness is now a relatively simple matter. We continue to calculate $P_k(S)$ successively until $s_{k+1} \geqslant x_k$ (x_k may decrease as k increases), and when this happens, the threshold of completeness $\theta(S)$ is then $x_k - 1$.

The justification for the above procedure is easily seen. When we find an interval $[x_k, y_k]$ in $P_k(S)$ such that $s_{k+1} \leqslant l_k = y_k - x_k + 1$ with $k \geqslant j_S$, we are guaranteed that all integers $\geqslant x_k$ belong to *P(S).* For $P_{k+1}(S)$ will contain all integers in the interval $[x_k + s_{k+1}, y_k + s_{k+1}]$ and hence all integers in the interval $[x_k, y_k + s_{k+1}]$, since $x_k + s_{k+1} \leqslant y_k + 1$ and the intervals $[x_k, y_k]$ and $[x_k + s_{k+1}, y_k + s_{k+1}]$ merge into one. By condition A, this merging will continue for ever since $l_{k+1} = y_{k+1} - x_{k+1} + 1 \geqslant y_k + s_{k+1} - x_k + 1 \geqslant 2s_{k+1} \geqslant s_{k+2}$. When $s_{k+1} \geqslant x_k$, no further s_{k+i}'s may be used to represent $x_k - 1$, and since all integers $\geqslant x_k$ belong to *P(S),* $x_k - 1$ is therefore the threshold of completeness for the sequence S.

In writing a computer program to find the thresholds of completeness for sequences using the above procedure, the most efficient way to generate and store the $P_k(S)$'s is of major concern. Two representations for numbers in $P_k(S)$ are used. First, in the characteristic function method, the set $P_k(S)$ is represented as a string of binary bits, the *(i*+ 1)th bit being a one if and only if the integer i belongs to $P_k(S)$ and zero otherwise. Zero is considered to be in $P_k(S)$ and hence the first bit of the string is always a 1. $P_{k+1}(S)$ is computed from $P_k(S)$ by shifting the entire bit string for $P_k(S)$ an amount equal to s_{k+1} and logically or-ing it to the original bit string for $P_k(S)$. When the threshold of completeness is less than half a million, this method is very fast since all computations can be done in core. When the numbers in $P_k(S)$ get to be larger than the limit of space available, a truncated version for $P_k(S)$ can be used effectively as long as the threshold is less than half the number of bits available. In the second method, $P_k(S)$ is stored as a sequence of intervals $[a_i, b_i]$ and $P_{k+1}(S)$ is obtained from $P_k(S)$ by constructing the new sequence of intervals $[a_i+s_{k+1}, b_i+s_{k+1}]$ and then merging the two sequences to produce the sequence of intervals for $P_{k+1}(S)$. This method has the advantage that the number of intervals becomes relatively constant after a while although it grows almost like a power of two in the beginning. For large problems, the limit for storage is exceeded very rapidly and auxiliary storages have to be used. Using the interval method we have computed the threshold of completeness for the sequence of fourth powers $S \equiv \{1, 16, 81, 256, \ldots\}$ to be 5,134,240. Note that if the characteristic function method were used, we would have to carry along a bit string of about 10 million bits. Various programming devices and techniques are employed in the program to reduce the running time but they will not be discussed here. Also, if $\Sigma_k = s_1+s_2+\ldots+s_k$ is the largest number in $P_k(S)$, the intervals are symmetric about $\frac{1}{2}\Sigma_k$; i.e. if $[a_i, b_i]$ is an interval in $P_k(S)$, then $[\Sigma_k - b_i, \Sigma_k - a_i]$ is also an interval. Observations like this help reduce the storage requirement for $P_k(S)$ by a substantial amount although they do make the logic for producing $P_{k+1}(S)$ from $P_k(S)$ much harder. As is well known to computer programmers, it is always a difficult problem to find the proper balance between storage space, running time, and simplicity of programming logic, and this program is no exception.

Having what we consider an efficient program to compute thresholds of completeness for sequences satisfying condition A, we turn next to a related problem. We say that a sequence S is essentially complete if all truncated sequences $S_n \equiv \{s_n, s_{n+1}, \ldots\}$ are complete. It is not difficult to see that all complete sequences generated by polynomials are essentially complete. A result of Roth and Szekeres [3] also guarantees that the sequence of primes, the sequence of squares of primes, etc., are essentially complete. Examples of complete sequences which are not essentially complete are the sequence of powers of 2, the Fibonacci sequence, and most Lucas sequences. A study of when Lucas sequences are essentially complete is being made by Stephen Burr, whose results will be published elsewhere. For essentially complete sequences, $\theta(S_n)$ exists for every n. Using the program, we were able to compute the thresholds of completeness for sequences such as the sequence of primes, the sequence of squares, the sequence of pseudoprimes (positive integers $\geqslant 2$ having at most 4 positive divisors), etc., for n up to a fairly large number. Some of the results obtained are briefly summarized in Tables 1 through 8 in Appendix A.

From the thresholds of completeness obtained, we observe that the ratios $\alpha_n \equiv \theta(S_{n+1})/s_n$ seem to settle down to a narrow region as n increases and that for the sequence of primes, this region is very close to 3. For the sequence of squares, the α_n's settle down to around 5. Since we know that all sufficiently large odd numbers can be expressed as a sum of three or fewer primes and all sufficiently large numbers can be expressed as a sum of five or fewer distinct squares, we are led to the following conjecture and theorem :

CONJECTURE. Lim sup ***a_n exists for all complete polynomial sequences and the sequence of primes, sequence of squares of primes, etc. In particular,*** [lim sup ***a_n] = 3 for the sequence of primes and*** [lim sup ***a_n] = 5 for the sequence generated by*** x^2.

Note that if this conjecture is true, then the status of the Goldbach conjecture can be settled by finite enumeration as can be seen from the following theorem :

THEOREM: ***Let $S \equiv \{s_1, s_2, \ldots, s_k, \ldots\}$ be an essentially complete sequence. Suppose there exists an N and an a such that for all $n \geqslant N$,***

$$a_n \equiv \frac{\theta(S_{n+1})}{s_n} < a.$$

Then all sufficiently large integers can be expressed as a sum of at most [a] distinct terms from S, where [x] stands for the largest integer $\leqslant x$. As a consequence thereof, S forms an integral basis for large numbers of order at most [a]. At any rate, the conclusion is true for all numbers y, $\theta(S_n) < y \leqslant \theta(S_{n+1})$, for which $a_n < a$.

Proof. Let y > $\theta(S_N)$; then we may find an $n \geqslant$ N such that $\theta(S_n) <$ y $\leqslant \theta(S_{n+1})$. Since y is greater than $\theta(S_n)$, y is representable as a sum of distinct terms from S_n, say $y = s_{i_1} + s_{i_2} + \ldots + s_{i_t}$ where each $s_{i_j} \geqslant s_n$. Hence y $\geqslant ts_n$. On the other hand, y $\leqslant \theta(S_{n+1}) < \alpha s_n$. Hence $t <$ ***a.*** Since t is an integer, $t \leqslant$ ***[a].***

While computer work cannot yet establish the validity of the assumption needed in the above theorem, we believe that it can give us a fairly good indication of what a may be, if it exists. It is hoped that experimental work of this kind can help us formulate meaningful conjectures that some one can prove at a later date.

APPENDIX A

Thresholds of completeness have been computed for many sequences, and the behavior of the respective α_n's studied. In the following tables we give a summary of the computed results obtained for some selected sequences. The generating function for each sequence $(s_i = f(i))$ is given on top of each table and max (α_n) means the largest a_n in the range between the two values of n heading the column in which the value of max(α_n) is found.

Table 1 $f(x) = x^2+1$

n	1	2	3	4	5	6	100	200	300	400
s_n	2	5	10	17	26	37	10,001	40,001	90,001	160,001
$\theta(S_n)$	51	131	255	282	360	465	54,916	196,116	415,347	726,436
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$		65.5	51.0	28.2	21.2	17.7	5.602	4.952	4.645	4.562
$\max(\alpha_n)$								5.673	5.328	4.880

Table 2 $f(x) = x^2$

n	1	2	34		5	6	50	100	150	200	250	350
s_n	1	4	9	16	25	36	2500	10,000	22,500	40,000	62,500	122,500
$\theta(S_n)$	128	192	223	384	492	636	17,072	60,928	129,184	222,208	339,968	659,456
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$							7.110	6.216	5.818	5.611	5.483	5.414
$\max(\alpha_n)$								7.110	6.346	5.893	5.729	5.621

Table 3 $P_n \equiv$ ***the sequence of primes***

n	1	2	3	4	5	100	500	1000	2000
s_n	2	3	5	7	11	541	3571	7919	17,389
$\theta(S_n)$	6	9	27	45	45	1683	10,779	23,859	52,247
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						3.217	3.028	3.017	3.004
$\max(\alpha_n)$							3.217	3.044	3.032

Table 4 $Q_n \equiv$ ***sequence of pseudo-primes***

n	1	2	3	4	5	500	1000	2000	3000
s_n	2	3	4	5	6	1082	2307	4891	7619
$\theta(S_n)$	1	2	8	8	12	2172	4625	9835	15,257
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						2.009	2.005	2.011	2.003
$\max(\alpha_n)$							2.049	2.037	2.025

TABLE 5 $P_n^2 \equiv$ *sequence of primes squared*

n	1	2	3	4	5	10	15	20
s_n	4	9	25	49	121	841	2209	5041
$\theta(S_n)$	17,163	35,355	124,395	149,403	160,155	269,715	405,003	573,715
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						509.858	219.038	132.259

TABLE 6 $f(x) = (x^2+x)/2$, *sequence of triangular numbers*

n	1	2	3	4	5	100	200	300	400	500	600
s_n	1	3	6	10	15	5050	20,100	45,150	80,200	125,250	180,300
$\theta(S_n)$	33	50	113	118	173	24,018	90,713	196,133	341,273	532,775	753,774
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						4.852	4.558	4.373	4.276	4.270	4.194
$\max(\alpha_n)$							5.008	4.599	4.529	4.433	4.413

TABLE 7 $f(x) = x^3$

n	1	2	3	4	5	10	20	30
s_n	1	8	27	64	125	1000	8000	27,000
$\theta(S_n)$	12,758	19,309	23,774	26,861	34,843	80,384	261,517	636,134
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						110.266	38.127	26.082

TABLE 8 $f(x) = x^3 + 1$

n	1	2	3	4	5	10	20	30
s_n	2	9	28	65	126	1001	8001	27,001
$\theta(S_n)$	8293	10,387	14,125	17,886	22,331	58,332	222,258	554,195
$\alpha_{n-1} = \dfrac{\theta(S_n)}{s_{n-1}}$						79.906	32.377	22.722

REFERENCES

1. J. L. BROWN: Note on a complete sequence of integers. ***American Math. Monthly 68*** (1961), 557-560.
2. HANS-EGON RICHERT: Über Zerlegungen in paarweise verschiedene Zahlen. *Norsk. Mat. Tiddsskr.* 31 (1949), 120-122.
3. K. F. ROTH and G. SZEKERES: Some asymptotic formulae in the theory of partitions. ***Q. J. Math. (2) 5*** (1954), 241-259.
4. R. L. GRAHAM: Complete sequences of polynomial values. ***Duke Math. J.*** 31 (1964), 275-286.

Application of computer to algebraic topology on some bicomplex manifolds[†]

HARVEY COHN

1. Introductory remarks. The present calculation is part of a series concerned with representing the (fundamental) domain of definition of certain algebraic function fields [1], [2] by computerized geometric visualization. The ultimate goal is to obtain topological information which perhaps can be of some value in understanding the algebraic function fields and some of the number theoretic identities involved.

We are dealing with Hilbert modular functions of two complex variables over certain real quadratic fields. The theory of algebraic functions of two complex variables is involved here and the suitability of a representation such as the Riemann surface is highly questionable in general. We restrict ourselves to a few carefully chosen cases where IS. B. Gundlach has recently shown [4], [5] the domain of definition to be representable as a compact manifold.

In order to visualize a bicomplex space, we must treat four (real) dimensions to within the limits of three-dimensional intuition. We attempt as an analogy the visualization of certain (ordinary) modular functions and their fundamental domains and we show to what limited extent the analogy can be pursued.

2. Modular group in one variable. Here we consider the upper half plane U

$$\operatorname{Im} z > 0 \tag{2.1}$$

subject to identifications under the (Klein) modular group G, namely

$$z_0 = S(z) = (az+b)/(cz+d), \qquad ad\text{-}bc = 1 \tag{2.2}$$

where a, b, c, d are integers. Alternatively, the transformations are represented by matrices $\pm S$ where

$$s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.3}$$

[†] Research supported by the U.S. National Science Foundation Grant G-6423 and computer support contributed by the Applied Mathematics Division of the Argonne National Laboratory of the U.S. Atomic Energy Commission.

We also consider G_2 the subgroup (of matrices or transformations) for which

$$S \equiv E \pmod 2 \tag{2.4}$$

where E is the unit matrix.

The fundamental domain F for G is classically given by the region F shown in Fig. 1. Thus F is determined by the inequalities

$$\left.\begin{array}{c} |\operatorname{Re} z| < \dfrac{1}{2} \\ |z| > 1 \end{array}\right\} \tag{2.5}$$

with boundary identified by making ∞A coincide with ∞ C according to $z_0 = z + 1$ while AB coincides with CB according to $z_0 = - 1/z$. (We have compactified, of course, by adjoining ∞.) (See [3], pp. 84, 127.)

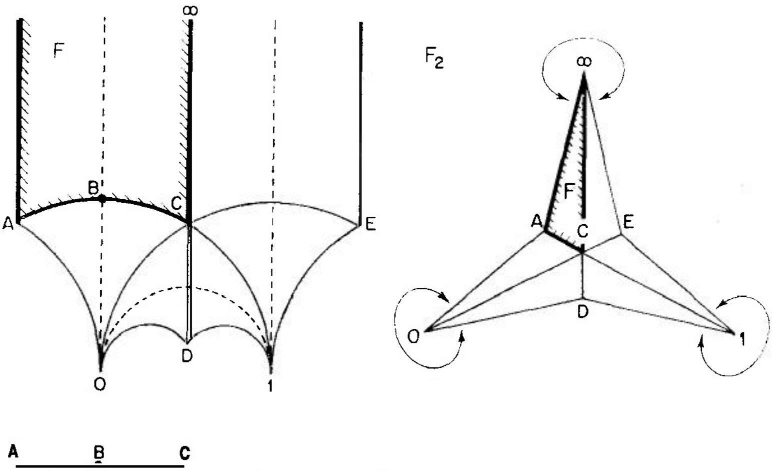


Fig. 1. Fundamental domain for G and G_2. We see F with floor ABC projected onto segment AC on the left. We see F_2 assembled from six replicas of F_1 on the right so as to form a 2-sphere.

In a one-dimensional world, we would see the floor of the region F or arc ABC projected as segment ABC (see interval in Fig. 1). Also, the walls of the region $F$are trivial by comparison. They are merely the boundaries of the fundamental region for G^∞ (the subgroup of G which leaves ∞ unchanged). Here G^∞ is simply

$$z_0 = z + n \quad (n \text{ integral}). \tag{2.6}$$

To visualize the fundamental domain F_2 for G_2 we would note that G_2 is a subgroup of G of index 6 with cosets determined by

$$\left.\begin{array}{l} S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; S_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; S_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ S_4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \; S_5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \; S_6 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \end{array}\right\} \tag{2.7}$$

Each right coset $G_2 S_m$ in G relocates F in a well-defined manner (to within equivalences under G_2). Thus F_2 consists of six replicas shown at the left of Fig. 1. (Naturally F_2 has no floor since it touches the real axis at 0 and 1.) It is easy to see, from the diagram on the right of Fig. 1, how the fundamental domain F_2 becomes a sphere under "trivial boundary identifications". The trivial boundary identifications are possible only because the floor of F, namely $|z| = 1$, is mapped into itself under z_0= -l/z, the transformation mapping F into the region *(OABC)* immediately below it.

A deceptively simple intermediate stage is provided by the Picard modular group (like Klein's except that in (2.2), *a, b,* c, *dare* Gaussian integers). Here the three-dimensional representation makes for a simple analogy to Fig. 1 and indeed the analog of G and the analog of G_2 are 3-spheres (see [**6**]).

We know that going to four dimensions, the domain of definition of an algebraic function field in two complex variables cannot be a 4-sphere. Therefore, we know some degree of difficulty must be encountered in extending the construction of F_2 to two complex variables!

3. Hilbert modular group. We summarize the construction of the fundamental domain, here, only in sufficient detail to define necessary terms and symbols. The justification appears in earlier work ([**1**], [**2**]).

The theory is restricted to the quadratic field Q $\left(2^{\frac{1}{2}}\right)$. We deal with three closely related groups,

Γ_* = (ordinary) Hilbert modular group,
Γ = symmetrized Hilbert modular group,
Γ_2 = subgroup of $\Gamma \equiv E \pmod{2^{\frac{1}{2}}}$ (principal congruence subgroup).

Here we have the Cartesian product $U \times U$ of two upper half planes written as "formal" conjugates z, z'

$$\operatorname{Im} z > 0, \qquad \operatorname{Im} z' > 0. \tag{3.1}$$

We define Γ_* as the group of linear transformations (sometimes called "hyperabelian"),

$$z_0 = \Sigma(z) = (\alpha z+\beta)/(\gamma z+\delta), \quad z_0' = \Sigma'(z') = (\alpha' z'+\beta')/(\gamma' z'+\delta') \tag{3.2}$$

where a, $\beta, \ldots$, a', $\beta', \ldots$ are conjugate algebraic integers in Q $\left(2^{\frac{1}{2}}\right)$ and

$$\alpha\delta-\beta\gamma = \varepsilon_0^{2t}, \qquad \alpha'\delta'-\beta'\gamma' = (\varepsilon_0')^{2t} \tag{3.3}$$

where $\varepsilon_0 = 1+2^{\frac{1}{2}}$ is the fundamental unit $\left(\varepsilon_0^2 = 3+2\cdot 2^{\frac{1}{2}}\right)$, and t is an integer. The corresponding matrices are

$$\Sigma = \pm\varepsilon_0^t \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{3.4}$$

and likewise for the conjugate.

As a convenience we omit the mention of the conjugate when dealing with statements where the meaning is clear. Thus when we refer to z as a point, we mean (z, z'), etc.

The group Γ is the supergroup over Γ_* formed by adjoining the generator $z_0 = z'$, or in full,

$$z_0 = z', \quad z_0' = z. \tag{3.5}$$

The group Γ_2 is the symmetrized subgroup of Γ_* formed by restricting Γ_* to substitutions for which the matrix Σ satisfies

$$\Sigma \equiv E \left(\bmod 2^{\frac{1}{2}}\right) \tag{3.6}$$

and adjoining the generator (3.5). Clearly Γ_2 is a subgroup of Γ of index 6 with the same equivalence classes (2.7) (if we ignore symmetry operations, which we can do since every a ≡ a' mod $2^{\frac{1}{2}}$).

The variables of $U \times U$ are reparametrized as follows :

We start with

$$z = x+iy, \quad z' = x'+iy' \tag{3.7}$$

and we introduce four new variables, namely R, R', S, S' as follows

$$x = R+2^{\frac{1}{2}}R', \quad x' = R-2^{\frac{1}{2}}R' \tag{3.8}$$

$$S = (y'-y)2^{\frac{1}{2}}/(y'+y), \quad S' = yy'. \tag{3.9}$$

We next consider Γ^∞, Γ_2^∞ the subgroups of (3.2) and (3.6) which keep the point at ∞ fixed. Thus

$$\Gamma^\infty\colon H(z) = \varepsilon_0^{2t}z+a+b\cdot 2^{\frac{1}{2}} \tag{3.10a}$$

$$\left.\begin{aligned} \Phi : R, R' \text{ defined modulo } 1,\\ 0 \leqslant S \leqslant 1, \quad 0 < S'; \end{aligned}\right\} \tag{3.10b}$$

and for the subgroups and superdomains,

$$\Gamma^\infty\colon H(z) = \varepsilon_0^{2t}z+2a+b\cdot 2^{\frac{1}{2}} \tag{3.1 la}$$

$$\left.\begin{aligned} \Phi^\infty : R \text{ (mod 2)}, \quad R'\text{(mod 1)}\\ 0 \leqslant S \leqslant 1, \quad 0 < S'. \end{aligned}\right\} \tag{3.11b}$$

Actually the above formulas (3.10b), (3.1 lb) must be further modified by a symmetry law. It is clear that the interchange (3.5) leads to the identification

$$(R, R', S, S') \equiv (R, -R', -S, S) \tag{3.12}$$

Hence if $S = 0$, we have the identification (modulo 1 always)

$$(S = 0)\colon R' \equiv -R' \ (R' = \text{constant}). \tag{3.13a}$$

We actually have an additional one at $S = 1$, namely

$$(\mathrm{S} = 1){:}\ R+2R' \equiv -(R+2R')\ (R+R' = \text{constant}). \tag{3.13b}$$

More explicitly this is the involution

$$\left.\begin{aligned}\boldsymbol{R} &\equiv 3R+4R' \\ \boldsymbol{R'} &\equiv -2R-3R'\end{aligned}\right\} \tag{3.14}$$

derivable from $\left(R-R'\cdot 2^{\frac{1}{2}}\right) \equiv \left(R+R'\cdot 2^{\frac{1}{2}}\right)\left(3+2\cdot 2^{\frac{1}{2}}\right)$. (This is the result of identifying S = – 1 with $S = +1$, under $z_0 = \varepsilon_0^2 z$.)

These involutions are shown in the upper and lower face of the cube in Fig. 2 for Γ^∞. If we are interested in Γ_2^∞ we take another cube alongside ($z_0 = z+1$); with the same involution on the two faces. The intermediate faces are tori. Now region Φ^∞ (or Φ_2^∞) can be seen to be topologically equivalent to the 3-sphere, as would be necessary to compactify Γ at ∞.

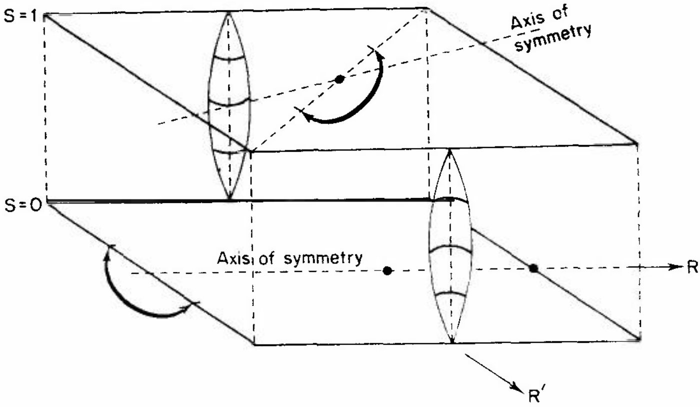


FIG. 2. Fundamental domain for Φ^∞. Here we see a unit cube with torus cross-sections (S = const.) but symmetries on $S = 0$ and $S = 1$ as explained in § 3. The spindle-shaped region of norm 2 is shown in two halves which adjoin (see § 5).

4. Assembling the floor. The floor of I' is the analogue of arc *AC* in Fig. 1. It is computed as a function [1]

$$S' = f(R, R', S) \text{ over } \Phi^\infty. \tag{4.1}$$

Thus the fundamental domain Φ consists of the values

$$S' \geqslant f(R, \boldsymbol{R'}, \boldsymbol{S}) \text{ over } \Phi^\infty, \tag{4.2}$$

subject to identifications on the floor (4.1). Every such point, in terms of z, z', is transformed into another such point by a transformation

$$z_0 = \Sigma(z),\ z_0' = \Sigma'(z') \tag{4.3}$$

or else, if symmetry is invoked,

$$z_0 = \Sigma'(z'),\ z_0' = \Sigma(z). \tag{4.4}$$

In the case of Fig. 1, the only transformation was $z' = -1/z$. Here, however, there can be very many, but we set them up into a minimal number. The computer program discovers the transformation

$$\Sigma(z) = (\alpha z+\beta)/(\gamma z+\delta)$$

which maps z into its transform z_0 (or z_0') by listing the eight rational parts of

$$\alpha = a+a'\cdot 2^{\frac{1}{2}},\ \beta = b+b'\cdot 2^{\frac{1}{2}},\ \gamma = c+c'\cdot 2^{\frac{1}{2}},\ \delta = d+d'\cdot 2^{\frac{1}{2}} \quad (4.5)$$

as well as listing z_0, the transformed point (with z_0') for each given point on the floor. (To keep the machine program free from symmetrization, sometimes z_0 was listed and sometimes z_0' depending on whether (4.3) or (4.4) happened to be theoretically correct.) The machine stored the transformations as

$$a+64\ a'+\ .\ .\ .\ +64^6 d+64^7 d$$

so that repeating transformations can be assigned the same identification numbers on each occurrence.

For each point of the floor subject to transformation $\Sigma(z)$, we have

$$\|\ \gamma z+\delta\ \| = |\ \gamma z+\delta\ |^2\ \ \gamma' z'+\delta'\ |^2 = 1 \qquad (4.6)$$

the analogue of $|z|^2 = 1$ in Fig. 1. There can be several such surfaces meeting at lower dimensional submanifolds of the floor but the pairing of points is more important than the transformation which does the pairing. (Thus, such banalities as round-off errors can change a transformation by slightly shifting a point, but this is not important by itself.)

In the calculation pursued here, 34 different transformations Σ occurred and the machine assigned numbers from 1 to 34 in the order of occurrence. We group them for later purposes in accordance with congruence classes (mod 2) as in (2.7). They are as follows:

Congruent to S_1:

$$\Sigma_7 = \begin{pmatrix} -1 & -2^{\frac{1}{2}} \\ 2^{\frac{1}{2}} & 1 \end{pmatrix},\quad \Sigma_{31} = \begin{pmatrix} 1 & 0 \\ 2^{\frac{1}{2}} & 1 \end{pmatrix},\quad \Sigma_8 = \begin{pmatrix} 1 & -2^{\frac{1}{2}} \\ 2^{\frac{1}{2}} & 1 \end{pmatrix},$$

$$\Sigma_{32} = \begin{pmatrix} -1 & 0 \\ 2^{\frac{1}{2}} & -1 \end{pmatrix};$$

Congruent to S3:

$$\Sigma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\quad \Sigma_{23} = \begin{pmatrix} 0 & -3+2\cdot 2^{\frac{1}{2}} \\ 1 & 0 \end{pmatrix},\quad \Sigma_{13} = \begin{pmatrix} 2^{\frac{1}{2}} & -1 \\ 1 & 0 \end{pmatrix},$$

$$\Sigma_{14} = \begin{pmatrix} -2^{\frac{1}{2}} & -1 \\ 1 & 0 \end{pmatrix},\quad \Sigma_{12} = \begin{pmatrix} 2^{\frac{1}{2}} & 1 \\ 1 & 2^{\frac{1}{2}} \end{pmatrix},\quad \Sigma_1 = \begin{pmatrix} 0 & -1 \\ 1 & 2^{\frac{1}{2}} \end{pmatrix},$$

$$\Sigma_{15}=\begin{pmatrix}-2^{\frac{1}{2}} & 1\\ 1 & -2^{\frac{1}{2}}\end{pmatrix},\quad \Sigma_3=\begin{pmatrix}0 & -1\\ 1 & -2^{\frac{1}{2}}\end{pmatrix};$$

Congruent to S_4:

$$\Sigma_{10}=\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix},\quad \Sigma_{21}=\begin{pmatrix}0 & -3+2\cdot 2^{\frac{1}{2}}\\ 1 & 1\end{pmatrix},\quad \Sigma_5=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix},$$

$$\Sigma_{30}=\begin{pmatrix}0 & -3+2\cdot 2^{\frac{1}{2}}\\ 1 & -1\end{pmatrix},\quad \Sigma_4=\begin{pmatrix}0 & -1\\ 1 & -1+2^{\frac{1}{2}}\end{pmatrix},\quad \Sigma_{11}=\begin{pmatrix}0 & -1\\ 1 & 1-2^{\frac{1}{2}}\end{pmatrix};$$

Congruent to S_5:

$$\Sigma_6=\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix},\quad \Sigma_{20}=\begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix},\quad \Sigma_{28}=\begin{pmatrix}1+2^{\frac{1}{2}} & -1\\ 1 & 0\end{pmatrix},$$

$$\Sigma_{25}=\begin{pmatrix}-1-2^{\frac{1}{2}} & -1\\ 1 & 0\end{pmatrix},\quad \Sigma_{33}=\begin{pmatrix}-1 & -3+2\cdot 2^{\frac{1}{2}}\\ 1 & 0\end{pmatrix},$$

$$\Sigma_{34}=\begin{pmatrix}1 & -3+2\cdot 2^{\frac{1}{2}}\\ 1 & 0\end{pmatrix};$$

Congruent to S_6:

$$\Sigma_{22}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix},\quad \Sigma_{16}=\begin{pmatrix}1-2^{\frac{1}{2}} & -2+2^{\frac{1}{2}}\\ 1 & 1\end{pmatrix},\quad \Sigma_{24}=\begin{pmatrix}1 & -2+2\cdot 2^{\frac{1}{2}}\\ 1 & 1\end{pmatrix},$$

$$\Sigma_9=\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix},\quad \Sigma_{19}=\begin{pmatrix}-1+2^{\frac{1}{2}} & -2+2^{\frac{1}{2}}\\ 1 & -1\end{pmatrix},$$

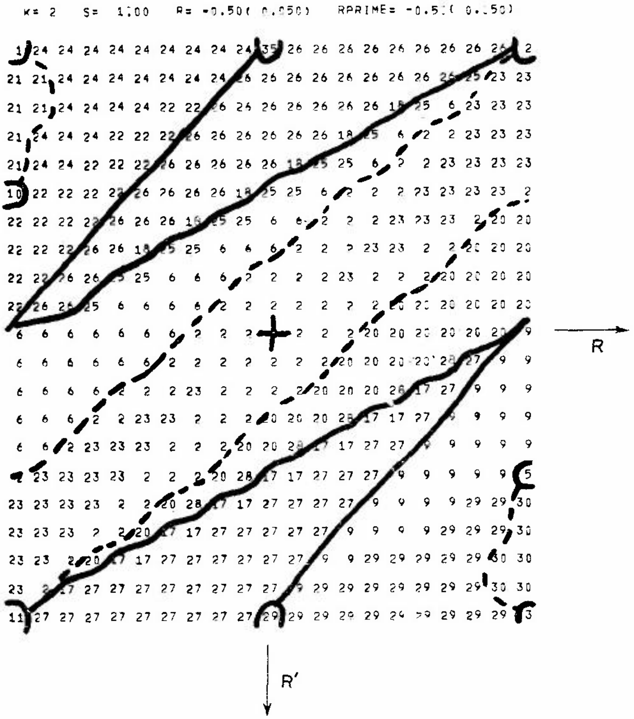
$$\Sigma_{29}=\begin{pmatrix}-1 & -2+2\cdot 2^{\frac{1}{2}}\\ 1 & -1\end{pmatrix},\quad \Sigma_{26}=\begin{pmatrix}-1 & -2+2^{\frac{1}{2}}\\ 1 & -1+2^{\frac{1}{2}}\end{pmatrix},$$

$$\Sigma_{18}=\begin{pmatrix}-1+2^{\frac{1}{2}} & 0\\ 1 & -1+2^{\frac{1}{2}}\end{pmatrix},\quad \Sigma_{27}=\begin{pmatrix}1 & -2+2^{\frac{1}{2}}\\ 1 & 1-2^{\frac{1}{2}}\end{pmatrix},$$

$$\Sigma_{17}=\begin{pmatrix}1-2^{\frac{1}{2}} & 0\\ 1 & 1-2^{\frac{1}{2}}\end{pmatrix}.$$

It is significant that the norm $|N(\gamma)| = 1$ except for those transformations congruent to S_1 (the identity), where $|N(\gamma)| = 2$.

If we refer to Fig. 3, we see a cross-section S = 1, on which many regions seem to be represented. We cannot be too sure of those represented by only one point, such as "region" 1, 10, 35, 11, 3, 5. Actually "region" 35 is a complete accident of round-off error while "region" 1 joins only at the corner point until S becomes smaller (about 0.43). To test whether points occur as accidents we have only to test cross-sections for values of S close to the one in question.



```
K= 2    S=  1.00    R= -0.50( 0.050)    RPRIME= -0.50( 0.050)

 1 24 24 24 24 24 24 24 24 24 35 26 26 26 26 26 26 26 26 26  2
21 21 24 24 24 24 24 24 24 26 26 26 26 26 26 26 26 25 25 23 23
21 21 24 24 24 24 22 22 26 26 26 26 26 26 26 18 25  6 23 23 23
21 24 24 24 22 22 22 26 26 26 26 26 26 18 25  6  2  2 23 23 23
21 24 24 22 22 22 26 26 26 26 26 18 25 25  6  2  2 23 23 23 23
10 22 22 22 22 26 26 26 26 18 25 25  6  2  2  2 23 23 23 23  2
22 22 22 22 26 26 26 18 25 25  6  6  2  2  2 23 23 23  2 20 20
22 22 22 26 26 18 25 25  6  6  6  2  2  2 23 23  2  2 20 20 20
22 22 26 26 25 25  6  6  6  2  2  2  2 23  2  2  2 20 20 20 20
22 26 26 25  6  6  6  6  2  2  2  2  2  2  2 20 20 20 20 20 20
 6  6  6  6  6  6  6  2  2  2  2  2  2  2 20 20 20 20 20 20  9
 6  6  6  6  6  6  2  2  2  2  2  2  2 20 20 20 20 28 27  9  9
 6  6  6  6  2  2  2 23  2  2  2  2 20 20 20 28 17 27  9  9  9
 6  6  6  2  2 23 23  2  2  2 20 20 20 28 17 17 27  9  9  9  9
 6  6  2 23 23 23  2  2  2 20 20 28 17 17 27 27  9  9  9  9  9
 2 23 23 23 23  2  2  2 20 28 17 17 27 27 27  9  9  9  9  9  5
23 23 23 23  2  2 20 28 17 17 27 27 27 27  9  9  9  9 29 29 30
23 23 23  2  2 20 17 17 27 27 27 27 27  9  9  9  9 29 29 29 30
23 23  2 20 17 17 27 27 27 27 27 27  9  9 29 29 29 29 29 30 30
23  2 17 27 27 27 27 27 27 27 27 29 29 29 29 29 29 29 29 30 30
11 27 27 27 27 27 27 27 27 27 29 29 29 29 29 29 29 29 29 29  3
```

FIG. 3. Pieces of floor of Φ lying in cross-section of $S = 1$. Note the consistency with the symmetry on $S = 1$ in Fig. 2. (The R' axis has inadvertently become directed downward because of the direction of the paper in the printer!)

We can, however, cut and paste and rearrange the sections so that the cross-section for $S = 1$ ***is still a torus, but that there are the least number*** of *different* ***regions showing.*** Clearly, region 21 is connected to region 23 by letting z become $z + 1$, etc. Moreover, two regions represent the same transformation as far as Φ^∞ is concerned, if for some H in Γ^∞ ***we*** have

$$H(\Sigma_a) = \Sigma_b. \tag{4.7}$$

Thus region 23 and 2 are the same, $\Sigma_{23} = \varepsilon_0^{-2}\,\Sigma_2$ but Σ_{22} and Σ_{26} must be different since they have different denominators.

It can be verified that for $|N(\gamma)| = 1$, ***two transformations with the same denominator are identifiable under*** (4.7). It is similarly easy to attend to the transformations where $|N(\gamma)| = 2$. Thus in Fig. 3, the black lines set apart regions in which ***(4.7)*** is ***not valid.*** A dotted line is used if the transformation ***H*** satisfies $H(z) \equiv z + 1$ (mod $2^{\frac{1}{2}}$), thus region 2 and region 6 are separated by a dotted line $(\Sigma_2 = \Sigma_6 + 1)$.

It is conjectured, in more general cases of $Q\left(k^{\frac{1}{2}}\right)$, that a single piece can be put together for each value of δ (mod γ), and this seems true from the computation here. We call $|N(\gamma)|$ the norm of the piece in question. Thus we have a "piece of norm 1" and a "piece of norm 2".

The piece of norm 2 is a spindle drawn in two halves in Fig. 2. It shrinks to a point at S = 0 and S = 1. We locate it for definiteness at an axis through ***R*** = 0, ***R'*** = $-\frac{1}{2}$ so that transformation 31 prevails. Thus the piece is mapped into itself (under equivalence classes in Γ^{∞}) by

$$z_0 = H\left(z/\left(2^{\frac{1}{2}}z + 1\right)\right) \qquad (4.8)$$

(or z_0 is the value symmetric to it, we shall not always repeat this). These $H(z)$ all belong to Γ_2^{∞}.

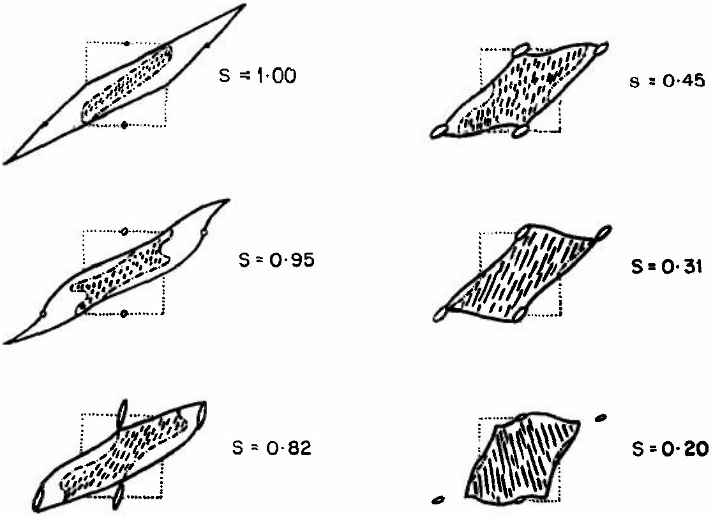


FIG. 4. Sections of the piece of the floor of Φ having norm 1. The shaded portion is explained in $4. Note the cross-sections of the spindle of norm 2 in four equivalent positions.

The piece of norm 1 is harder to draw. We show it in several cross-sections in Fig. 4. For S=O it is the square and for S= 1 it is the rectangle always dictated by the symmetries of the faces in Fig. 2. As S goes from 0 to 1 the cross-section becomes more and more oblique, attaching itself and detaching itself from images of the spindle (of norm 2) at critical values $S=0.31$ (approx.) and $S=0.82$ (approx.). For the piece of norm 1, we can show every transformation joins Σ_2, i.e. for H in Γ^∞

$$z_0 = \mathrm{H}(-1/z). \tag{4.9}$$

We use shading in Fig. 4 to show the portion which belong to Γ_2^∞. Thus in terms of H in Γ_2^∞, we have the following:

$$\text{"shaded portion"} \quad z_0 = H(-1/z),$$

$$\text{"blank portion"} \quad z_0 = H(-1/z+1).$$

The shading is not of topological interest as much as it shows that part of the piece of norm 1 must match equivalent points in the neighboring replica of Φ^∞ (formed by $z+1=z_0$), if we were to match this piece in the unit square by (4.9). Actually, it is more meaningful to match it with itself.

The piece of norm 1, *as reassembled for Fig. 4, is matched with itself under* $z_0 = -1/z$ (or $z_0' = -1/z$) *without use of the equivalence operations of* (4.9). To see this consider the two-dimensional boundaries of the reassembled piece of norm 1. They consist of the simultaneous equations

$$\| z \| = 1, \qquad \| \gamma z + \delta \| = 1 \tag{4.10}$$

if $\gamma z + \delta$ is the denominator of a neighboring region. Under $z_0 = -1/z$, the boundary is mapped into another boundary given by

$$\| z \,\mathrm{I\!I} = 1, \qquad \| \delta z - \gamma \| = 1. \tag{4.11}$$

The assertion now follows from the fact that the relation $z_0 = -1/z$ converts the piece into another piece of the same floor of norm 1, while the boundary was determined in an invariant fashion.

Any boundary segment (4.10) determines the height of the floor uniquely. These correspond to the points A and C in Fig. 1 which are determined by fixed points rather than by any analysis of the arc ABC. Note that the pair of points A, C constitutes a O-sphere just as the boundary of the piece of norm 1 is a 2-sphere.

The critical values of S are quite interesting by themselves, namely

$$S_1 = 0.3101\ldots = \left(4 - 6^{\frac{1}{2}}\right)/5$$

and

$$S_2 = 0.8165\ldots = 6^{\frac{1}{2}}/3$$

Actually the points of attachment and detachment are points at which S' takes the values believed to be the minimum for the whole floor, namely [1]

$$S' = \tfrac{1}{4}\left(-3 + 2\cdot 6^{\frac{1}{2}}\right) = 0.4747\ldots.$$

5. Approximate topological configuration. By using the previous information we can give an approximate description of the topological configuration.

First consider Φ. Here Φ has a manifold point at ∞ from which the three-dimensional base in Fig. 2 appears like a 3-sphere. It is divided into two pieces of norms 1 and 2 which are 3-cells, each folded into itself by transformations (4.8) and (4.9). (Recall that in the simple case, Fig. 1, the floor was one piece folded onto itself by $z_0 = - 1/z$.)

Next consider Φ_2. If we refer again to Fig. 1, we see that there are three replicas of the floor AC, DC, EC which transform into one another like the representatives of G/G_2 in (2.7). The fact that the reassembled piece of norm 1 is transformed into itself under $z_0 = -$ l/z, etc., enables us to reproduce three replicas of that piece in an analogue of Fig. 1. If we momentarily restrict ourselves to this piece (ignoring that of norm 2), we have a simple situation where the (spherical) boundaries of each of the three replicas meet in a 2-sphere analogous to the O-sphere A, C of Fig. 1. The analogy, however, is not kept because the piece of norm 2 does not map into itself under $z_0 = -$ l/z, etc., hence it is not representable as three replicas lying in the replicas of the floor. The boundary of this piece of norm 2 is nestled, however, in between the various boundaries of the pieces of norm 1, and the three-dimensional piece of norm 2 bulges out of the spherical boundary into parts of the three-dimensional floor. The situation is therefore somewhat more complicated than that of lower dimensional space (as it must be since the final configuration cannot be a 4-sphere!).

We are confronted with the need to study the self-mapping of the floor more carefully in order to make deductions concerning the topology of the fundamental domains @and Φ_2. There are very few cases which are analogous [5], possibly the other two involve $Q(3^{1/2})$, where the problem can be considered as an analogous pasting of 3 (or 4) 3-spheres. In any case, the numerical data are capable of further analysis for geometric or topological features than attempted here.

REFERENCES

1. H. COHN: A numerical study of the floors of various Hilbert fundamental domains. Math. of *Computation* 19 (1965), 594–605.
2. H. COHN: A numerical study of topological features of certain Hilbert domains. *Math.* of Computation 21 (1967), 76-86.
3. H. COHN: *Conformal Mapping on Riemann Surfaces,* McGraw Hill, 1967.
4. K. B. GIJNDLACH: Some new results in the theory of Hilbert's modular group, pp. 165-180, *Contributions to Function Theory* (Tata Institute, 1960).
5. K. B. GUNDLACH: Die Fixpunkte einiger Hilbertscher Modulgruppen. *Math. Annalen* 157 (1965), 369-390.
6. W. M. WOODRUFF: The singular points of the fundamental domain for the groups of of Bianchi, Ph.D. Dissertation, University of Arizona, 1967.

A real root calculus

HANS ZASSENHAUS

How can we construct a really closed algebraic extension over an algebraically ordered field ***F***?

We assume that ***F*** is constructively algebraically ordered (see **[1]**).

A ***real root calculus*** over ***F*** consists in solving the following two tasks :

(I) To assign to each polynomial ***P*** of $F[X]$ a non-negative integer NR(P). This number will turn out to be the maximal number of distinct roots of ***P*** in any algebraically ordered extension of ***F***.

(II) To assign to each polynomial U of $F[X]$ and to each index I satisfying the condition $0 < I \leqslant$ NR(P) uniquely a number SIGN(U, I, ***P***) which is one of the three numbers 1, 0, − 1. It should turn out to be the sign of the value of U for the Ith root of ***P*** in any algebraically ordered extension of ***F*** containing NR(P) distinct roots.

This task was first solved by Vandiver **[4]** in case the algebraic ordering of ***F*** was archimedean. Use had to be made of factorizations of polynomials of $F[X]$ into irreducible factors. The task was solved again by A. Hollkott **[2]** in his. 1941 thesis without taking recourse to Vandiver's additional two assumptions. Tarski **[3]** solved the task independently.

The real root calculus which is expounded here is based on A. Hollkott's thesis. For the benefit of English readers streamlined proofs of the necessary theorems are given.

1. Here are the theorems to be proven later:

THEOREM 1. (Between value theorem.) ***If*** $\boldsymbol{P} \in F[X], \boldsymbol{A} < \boldsymbol{B}, P(A)P(B) < \boldsymbol{0},$ ***then there can be constructed an algebraically ordered extension of F containing a*** root R ***or P satisfying the inequalities***

$$\boldsymbol{A} < \boldsymbol{R} < B.^{\dagger} \tag{1}$$

[†] As it stands, A, ***B*** denote elements of the algebraically ordered field ***F***. We agree, however, that ***A, B*** also are permitted to be one of the symbols ∞, ∞ which are subject to the rules: $-\infty < \boldsymbol{B}$ for any ***B*** of F, $A < \infty$ for any ***A*** of F, $-\infty < \infty$; furthermore $(-\infty)A = \infty(-A) = -\infty$, ∞A = --(-A) $= \infty$ for any positive element ***A*** of ***F;*** also $\infty + \infty = \infty = (-\infty)\ (-\infty)$, $\infty(-\infty) = (-\infty)\infty = -\infty$, finally $P(\infty) = A\infty$ if the leading coefficient of P is ***A*** and $P(-\infty) = P^{-}(\infty)\,(P^{-}(X) = \boldsymbol{P}(-\boldsymbol{X}))$. We set sign $\infty = 1$, sign (-CO) = − 1. It follows that sign ***(AB)*** = sign ***A*** . sign ***B*** whenever ***A, B, AB*** are elements of $F \cup \{\infty, -\infty\}$, that sign ***A*** = 1 if and only if ***A*** > 0 and that there are elements ***A, B*** of F such that sign ***P***(− CO) = sign ***P(Y),*** if $-\infty \leqslant Y \leqslant A$, and sign ***P(m)*** = sign P(Y), if $B \leqslant Y \leqslant \infty$ for Yin any algebraically ordered extension of ***F***.

The number of distinct roots of the non-zero polynomial P of $F[X]$ in any extension of Fis bounded by the degree of P. Hence there is a maximum $NR(P)$ to the number of distinct roots of P in any ordered extension[†] of F. Similarly, for any two elements A, B of $F \cup \{\infty, -\infty\}$ satisfying the inequality $A < B$ there is a maximum $\mathrm{NR}(P, A, B)$ to the number of distinct roots of P in the interval $[A, B) = \{Y | Y \in F \;\&\; A \leqslant Y < B\}$ in any algebraically ordered extension of F. We have

$$NR(P) = \mathrm{NR}(P, -\infty, \infty), \tag{2a}$$

$$\mathrm{NR}(P, A, B) = \mathrm{NR}(P, A, C) + \mathrm{NR}(P, C, B) \quad \text{if } A < C < B, \tag{2b}$$

$$\mathrm{NR}(P, -\infty, R(I, P)) = I - 1, \tag{2c}$$

provided that $R(1, P), \ldots, R(NR(P), P)$ are $NR(P)$ distinct roots of P in F ordered by their order of magnitude. We denote by P' the derivative

$$P'(X) = NA(0)X^{N-1} + (N-1)A(1)X^{N-2} + \ldots + A(N-1) \tag{3}$$

of the polynomial

$$P(X) = A(0)X^{N} + A(1)X^{N-1} + \ldots + A(N) \tag{4}$$

of degree

$$N = [P] \tag{5}$$

of $F[X]$. Thus $P'(X) = 0$ if $[P] = 0$ or if $P = 0$.

We denote by GCD (P, Q) the greatest common divisor with leading coefficient 1 of the two polynomials P, Q of $F[X]$, not both of which vanish. There is a well-known routine for finding GCD (P, Q).

The non-zero polynomial P of $F[X]$ is said to be *separable* if it is not divisible by any non-constant polynomial square. A necessary and sufficient condition is given by GCD $(P, P') = 1$. In any event, the polynomial P and the polynomial quotient $P/\mathrm{GCD}\,(P, P')$ have the same roots.

THEOREM 2. *For the non-zero polynomial P of $F[X]$ and for elements A, B of F satisfying $A < B$, there can be constructed an ordered extension of F that is generated by* NR(P, *A*, *B*) *distinct roots of P belonging to $[A, B)$.*

THEOREM 3. *Let $A, B \in F \cup \{\infty, -\infty\}$, let P be a separable polynomial of $F[X]$ and let F contain* NR(P') *distinct roots of P', say*

$$\mathrm{R}(1) < R(2) < \ldots < R(NR(P')) \tag{6}$$

$$P'(R(I)) = 0 \quad (1 \leqslant Z \leqslant \mathrm{NR}(P')). \tag{7}$$

Then the non-negative integer NR(P, *A*, *B*) *is equal to the number of changes of sign in the chain of values*

$$P(A), P(R(J)), \ldots, P(R(K)), P(B) \quad (J \leqslant K) \tag{8}$$

[†] By this we mean of course an extension of F with an algebraic ordering which restricts to the given algebraic ordering on F.

where either the indices J, K are so determined that $A < R(J)$, $R(K) < B$, $R(J-1) \leqslant A$ if $J > 1$, $B \leqslant R(K+1)$ if $K < \mathrm{NR}(P')$, or if that determination is impossible, then the terms $P(R(J)), \ldots, P(R(K))$ are to be dropped altogether. A change of sign is scored for any change of the sign function from one value to the next on the right excepting the case when zero is on the right.

THEOREM 4. *The maximal number* $\mathrm{NR}(P, A, B)$ *of "real roots" of P in the interval*

$$[A, B) = \{Y \mid Y \in F \ \& \ A \leqslant Y < B\} \tag{9}$$

depends only on the non-zero polynomial P of $F[X]$ and on the elements A, B of the algebraically ordered field F subject to the condition $A < B$, but not on the algebraically orderedfield F itself. In particular, it will not change if F is replaced by an ordered extension.

THEOREM 5. *Let σ be an order-preserving isomorphism of F on the algebraically ordered field σF. Let $E = F(R)$ be a finite ordered extension by a root R of the polynomial P of $F[X]$ and let $\hat{E} = \sigma F(\hat{R})$ be a finite ordered extension by R. Then there is an order-preserving isomorphism of E on $\hat{E}$ mapping R on $\hat{R}$ and restricting to σ on E if and only if $\sigma P(\hat{R}) = 0$ and* $\mathrm{NR}(P, -\infty, R) = \mathrm{NR}(\sigma P, -\infty, \hat{R})$.[†]

THEOREM 6. (Theorem of Rolle.[‡]) *If the polynomial P of $F[X]$ vanishes for two distinct arguments A, B of F then an ordered extension of F can be constructively generated by a root of P between A, B.*

THEOREM 7 (Mean value theorem.) *For any polynomial P of $F[X]$ and any two distinct elements A, B of F an ordered extension of F can be constructively generated by an element Y of F satisfying*

$$(P(B)-P(A))/(B-A) = P'(Y). \tag{10}$$

2. We are going to construct recursively on each of the degree levels $D = 1, 2, \ldots$ ordered extensions of F of complexity $1, 2, \ldots$ by the adjunction of root symbols $R(I, P)$ for polynomials P of degree not greater than D with coefficients in ordered extensions E of complexity $0, 1, 2, \ldots$ over F. For the root symbols it will be demanded that

$$P(R(I, P)) = 0, \tag{11}$$

$$\mathrm{NR}(P, -\infty, R(I, P)) = I-1, \tag{12}$$

hence the index I must be a natural number not greater than $\mathrm{NR}(P)$.

[†] By σP, of course, we denote the polynomial of $\sigma E[X]$ the coefficients of which are obtained by applying σ to the corresponding coefficients of P.

[‡] It will be noted that Sturm's theorem is not needed for our construction, though of course it provides a very valuable tool in real algebra (see e.g. 121,151). Theorems 6 and 7, though interesting in themselves, are placed at the end because they do not enter the construction, but are used only for the purpose of proving the other five theorems.

For this purpose we must assign to each polynomial U of $E[X]$ a sign function SIGN (U, I, P) assuming one of the 3 values 1, 0, $-$ 1 such that the operational rules

$$U(R(I, P)) + V(R(I, P)) = W(R(I, P)) \qquad (13)$$

$$U(R(I, P))V(R(I, P)) = T(R(I, P)) \qquad (14)$$

if $$U(X)+ V(X) = \mathrm{W(X)},\ U(X)V(X) = T(X),$$

define an ordered extension $E(R(I, \mathrm{P}))$ consisting of all symbols $U(R(I,P))$, according to the positivity rule

$$U(R(I, P)) > 0 \qquad (15)$$

if and only if SIGN $(U(R(I, \mathrm{P})))$= 1, and the equality definition

$$U(R(I, P)) = V(R(I, P)) \qquad (16)$$

if and only if SIGN $((\mathrm{U}\text{-}\ V)(R(I,P))) = 0$ when $(U\text{-}\ V)(X) = U(X) - V(X);$ also the conditions (11), (12) must be fulfilled.

As usual the expression $1(R(I, \mathrm{P}))$ is identified with $R(I, \mathrm{P})$ when Z(X) = X.

By definition the complexity of the ordered extension $E(R(I, \mathrm{P}))$ is 1 more than the complexity of E.

On the degree level 1 the construction with the desired properties is simple enough.

The algebraically ordered extensions of Pto be considered are Ffor each complexity.[†] If P is a constant polynomial over F, then $NR(P) = 0$. If P is the linear polynomial $AX+B$ of $F[X]$, and U is any polynomial of $E[X]$, then we have the defining equation

$$\mathrm{SIGN}\ (U,\ 1,\ P) = \mathrm{sign}\ (U(\text{-}B/A)), \qquad (17)$$

and the symbol $U(R(1, P))$ is canonically identified with $U(- B/A))$. Theorems 1-6 will be verified readily in case the degree of P is not greater than 1. We assume now that $D>1$, that all constructions on the degree level D- 1 of any prescribed complexity can be performed as specified above, and that Theorems 1-6 are demonstrated for polynomials P of degree smaller than D and for any field (in place of F) that can be constructed on the ievel $D - 1$.

We begin with a proof of Rolle's theorem for polynomials of degree D.

The assumption of Theorem 6, viz.

$$P(A) = 0 = P(B),$$

leads to a factorization

$$P(X) = (X- A)^{L}(X- B)^{M}Q(X)$$

[†] As A. Hollkott stresses correctly, in reality we do get new ordered fields even here in as much as the collection of symbols to be considered expands with increasing complexity. But in our case a canonical order-preserving isomorphism with Fis set up at each stage.

with positive exponents L, M such that

$$Q(A) \neq 0, \; Q(B) \neq 0,$$

and certainly the degree of Q is less than $D - 1$. By the induction assumption there is an ordered extension of F generated by a root $\hat{B}$ of P satisfying $A < \hat{B} < B$ such that NR $(Q, \mathrm{A}, \hat{B}) = 1$. It suffices then to prove Rolle's theorem under the additional assumption that there is no root of Q between A and B. By the between value theorem $Q(A)Q(B) > 0$. Upon differentiation we have

$$\begin{aligned}
P'(S) &= (X-A)^{L-1}(X-B)^{M-1}\hat{Q}(X),\\
\hat{Q}(X) &= (L(X-B)+M(X-A))Q(X)+(X-A)(X-B)\hat{Q}'(X),\\
\hat{Q}(A) &= L(A-B)Q(A),\\
\hat{Q}(B) &= M(B-A)Q(B),\\
\hat{Q}(A)\hat{Q}(B) &= -LM(A \quad B)^2Q(A)Q(B),\\
\hat{Q}(A)\hat{Q}(B) &< 0.
\end{aligned}$$

By the between value theorem applied to $\hat{Q}(X)$ there is an ordered extension of F generated by a root of $\hat{Q}(X)$ between A and B. This root also is a root of $P'(X)$ between A, B.

The mean value theorem follows in the customary way by application of Rolle's theorem to the polynomial

$$P(X)-P(B)(P(X)-P(A))/(B-A)-P(A)(P(X)-P(B))/(A-B).$$

We proceed to the proof of the between value theorem for a polynomial P of degree D. For convenience sake let $A < B$.

If at any stage of the ensuing construction we should meet an element R in an ordered extension E of F that was obtained on the D- 1 level such that $A < R < B$, $P(R) = 0$, then the elements $U(R)$ $(U \in F[X])$ with the operational rules as defined in E provide the required collection of symbols forming an ordered extension of F with a root of P between A and B. It will be assumed in the ensuing construction that this will not happen. For example, if it should happen that there is a non-trivial factorization $P(X) = M(X)L(X)$ in $E[X]$ such that both M and L are non-constant, then either $M(A)M(B) < 0$ or $L(A)L(B) < 0$ so that either M or L will have a root in an ordered extension of E on the D- 1 level.

Henceforth we assume that we will not meet non-trivial factorizations of P in $E[X]$. This implies that P is separable, because $P/\mathrm{GCD}\,(P, P')$ cannot be a proper divisor of P.

Now let E be an ordered extension of F generated by $\mathrm{NR}(P', A, B)$ distinct roots $R(J), \ldots, R(K)$ of P' belonging to $[A, B]$, according to Theorems 2, 3. Let

$$A = A(0) < A(1) < \ldots < A(S) = B$$

the set formed by the NR (P', A, B) roots of P' belonging to $[A, B)$ and the elements A, B in order of magnitude. There is a first index J such that $P(A(J))P(A(J+1)) < 0$.

By definition (and by Theorem 4) there is no root of P' between $A(J)$ and $A(J+1)$ either in E or in any ordered extension.

It follows from the between value theorem that the sign of P' between $A(J)$ and $A(J+1)$ is constant $\neq 0$.

It follows from the mean value theorem that P is strictly monotone in E as well as in any ordered extension of E. Hence for any chain

$$A(J) = B(0) < B(1) < \ldots < B(K) = A(J+1) \tag{18}$$

there is precisely one index H such that

$$0 \leqslant H < K, \quad P(B(H))P(B(H+1)) < 0.$$

For example for a given polynomial U of $F[X]$ of degree less than $[P]$ according to Theorem 2 an ordered extension $\hat{E}$ can be constructed containing NR $(U, A(J), A(J+1))$ roots of U in the interval $[A(J), A(J+1))$. The set formed by these roots of U together with $A(J)$ and $A(J+1)$ may be ordered according to (18). It follows that U will have no roots between $B(H)$ and $B(H+1)$, neither in $\hat{E}$ nor in any ordered extension of $\hat{E}$. Hence, according to the between value theorem, the sign of U is constant $\neq 0$ between $B(H)$ and $B(H+1)$ in $\hat{E}$ — even in any ordered extension.

Suppose we form a set consisting of $B(O), B(l), \ldots, B(K)$ and finitely many other elements of $\hat{E}$, say

$$A(J) = C(0) < C(1) < \ldots < C(L) = A(J+1),$$

then there is precisely one index G such that $0 < G < L$, $P(C(G))\ P(C(G+1)) < 0$. It follows, moreover, that $B(H) \leqslant C(G) < C(G+1) \leqslant B(H+1)$ and therefore the sign of U between $C(G)$ and $C(G+1)$ is constant and equal to the sign of U between $B(H)$ and $B(H+1)$. We will use this sign invariance of U at the appropriate time.

Let R be a root symbol. For each U we form the symbol $U(R)$.

If $U(B(H)) \neq 0$ then set

$$\text{SIGN } (U(R)) = \text{sign } (U(B(H))).$$

If $U(B(H)) = 0$, then there holds a factorization $U(X)' = (X- B(H))^M V(X)$ in $\hat{E}[X]$ for which $V(B(H)) \neq 0$. We define SIGN $(U(R)) =$ sign $V(B(H))$ and we remark that SIGN $(U(R))$ is equal to the sign of U between $B(H)$ and $B(H+1)$.

We set SIGN $(O(R)) = 0$.

Note that

$$\text{SIGN } C(R) = \text{sign } C$$

if C is a constant polynomial of $F[X]$.

In order to establish the between value theorem it will suffice to show that the collection of the symbols $U(R)$ $(U \in F[X];\ U = 0$ or $[U] < [P])$

with the operational rules

$$U(R)+V(R) = W(R) \tag{19}$$

if $U+V = W$ in $F(X]$,

$$U(R)+ V(R) = Q(R)P(R)+T(R) \tag{20}$$

if $U+V = QW+T$ in $F[X]$

and $T = 0$ or $[T] < [P]$,

$$U(R) = Y(R) \Leftrightarrow U = V,$$

$$\text{sign } (U(R)) = SIGN\ (U(R)) \tag{21}$$

forms an ordered extension of F if we identify $C(R)$ with C for any constant polynomial.

Moreover, identifying $l(R)$ with R, we shall find that

$$P(R) = 0, \tag{22}$$

$$A < R < B. \tag{23}$$

We note right away that

$$\text{SIGN } (-U(R)) = -\text{ SIGN } (U(R)),$$

$$\text{SIGN } ((\text{I -A})(\text{R})) = 1,$$

hence it suffices to show (22) and to show that the assumptions

$$SIGN\ (U(R)) = 1 \tag{24}$$

$$\text{SIGN } (V(R)) = 1$$

imply that

$$\text{SIGN } (W(R)) = 1 \tag{25}$$

and

$$\text{SIGN } (T(R)) = 1. \tag{26}$$

To show (25) under the assumptions (24), let C(O), . . . , $C(L)$ be the set formed by $A(J)$, $A(J+1)$ and the $N(U, A(J), A(J+1))$ roots of U, the $N(V, A(J), A(J+1))$ roots of V, and the $N(W, A(J), A(J+1))$ roots of W in a suitable ordered extension of E ordered by magnitude. It follows that U, V are positive between C(G), C(G+ 1) and that the sign of *Wis* equal to SIGN $(W(R))$ between C(G), $C(G+1)$.

The equation $$W(C) = U(C)+V(C)$$

which holds for $C = \frac{1}{2}(C(G)+ C(G+1))$ implies (25).

To show (26) under the assumption (25) let us firstly assume that

$$\text{GCD } (U, T) = \text{GCD } (V, T) = 1. \tag{27}$$

Now let C(O), . . . , C(L) be the set formed by $A(J)$, $A(J+1)$ and by the $N(U, A(J), A(J+1))$ roots of U, the $N(V, A(J), A(J+l))$ roots of V, the $N(Q, A(J), A(J+1))$ roots of Q, and the $N(T, A(J), A(J+1))$ roots of *Tin* a suitable ordered extension of E ordered by magnitude. It follows that U, V are positive between C(G), $C(G+1)$ and that the sign of W is equal to SIGN (W(R)) between C(G), C(G+ 1). Furthermore Q is of constant sign $\neq 0$ between C(G), $C(G+1)$. Moreover neither U and Tnor V and T have a root in common.

The equation

$$T(C) = U(C)\,V(C) - Q(C)P(C),$$

which holds for C = C(G) as well as for C = $C(G+1)$, implies that $T(C)$ is positive unless Q(C) P (C) $>$ 0. Hence (26) holds unless

$$\begin{aligned} Q(C(G))P(C(G)) &> 0, \\ Q(C(G+1))P(C(G+1)) &> 0. \end{aligned} \tag{28}$$

But by our assumption

$$P(C(G))\,P(C(G+1))<0, \quad Q(C(G))\;Q(C(G+1))>0,$$

so that (28) cannot hold.

In the general case we have in $F[X]$:

$$U = \hat{U}\hat{\hat{U}}, \quad T = \hat{T}\hat{\hat{U}}, \quad Q = \hat{Q}\hat{\hat{U}}$$

where SIGN (U) = 1 and $\hat{\hat{U}} = \pm$ GCD (U, T). Furthermore

$$V = \hat{V}\hat{\hat{V}}, \quad \hat{T} = \hat{\hat{T}}\hat{\hat{V}}, \quad \hat{Q} = \hat{\hat{Q}}\hat{\hat{V}},$$

where SIGN $(\hat{V}) = 1$ and $\hat{\hat{V}} = \pm$ GCD$(\hat{V}, T)$. Hence

$$\hat{U}\hat{V} = \hat{\hat{Q}}P + \hat{\hat{T}},\ GCD\left(\hat{U}, \hat{\hat{T}}\right) = 1 = \mathrm{GCD}\left(\hat{V}, \hat{\hat{T}}\right).$$

As was shown above, we have SIGN $\left(\hat{\hat{T}}\right) = 1$. Furthermore trivially

$$\mathrm{SIGN}\left(\hat{\hat{U}}\right) = \mathrm{SIGN}\left(\hat{\hat{V}}\right) = 1,$$

$$\mathrm{SIGN}\ (7') = \mathrm{SIGN}\left(\hat{\hat{U}}\hat{\hat{V}}\hat{\hat{T}}\right) = \mathrm{SIGN}\left(\hat{\hat{U}}\right)\mathrm{SIGN}\left(\hat{\hat{V}}\right)\mathrm{SIGN}\left(\hat{\hat{T}}\right) = 1.$$

In order to show (22) let us assume P in the form

$$P(X) = M(0)X^{[P]} + M(1)X^{[P]-1} + \ldots + M([P])$$

with coefficients in F. *Now* the equation (20) for

$$\begin{aligned} U(X) &= M(0)X^{[P]-1} + M(1)X^{[P]-2} + \ldots + M([P]-1), \\ V(X) &= X,\ Q(X) = 1,\ T(X) = -M([P]) \end{aligned}$$

shows that

$$U(R)V(R) = T(R)$$

which is tantamount to (22) for the special choice of U, V, T made above. We have to remark, of course, that for any polynomial U of $F[X]$ of degree less than $[P]$ the symbol $U(R)$ is equal to that symbol which is obtained by substitution of $Z(R)$ in U.

Using the same notations as before, assume that P is separable.

Denote by A4 the number of sign changes in the chain (8).

As a consequence of the between value theorem there will be constructed an ordered extension of F of complexity M in which P has M distinct roots in $[A, B)$. Hence $\mathrm{NR}(P, A, B) \geqslant M$. On the other hand, let E be an ordered extension of F with $\mathrm{NR}(P, A, B)$ distinct roots in $[A, B)$, say the roots

$$\mathrm{M}(1) < \mathrm{M}(2) < \ldots < M(\mathrm{NR}(P, A, B))$$

by order of magnitude when

$$A \leqslant \mathrm{M}(1), \quad M(\mathrm{NR}(P, A, B)) < B.$$

There is an ordered extension $\hat{E}$ of E with $\mathrm{NR}(P', A, B)$ roots of P' in $[A, B)$. These roots of P' together with A, B form the chain (8). Since P is separable, no root of P is a root of P' and vice versa. Hence each root $M(I) > A$ lies between two consecutive members of (8) with a sign change of P between them, as follows from the mean value theorem. If $\mathrm{M}(1) = A$ then by Rolle's theorem $\mathrm{M}(1) < R(J) < \mathrm{M}(2)$ and a sign change of P from A to $R(J)$ is scored. Therefore there are at least NR(P, A, B) sign changes in (8). Hence $M \geqslant \mathrm{NR}(P, A, B)$. Thus Theorem 3 is established.

We remark that for each non-constant polynomial P the polynomial $P/\mathrm{GCD}(P, P')$ is separable and shares its roots with P. Applying Theorem 3 to this polynomial we obtain Theorem 2.

Theorem 4 is also implied,

In order to prove Theorem 5 let $P/\mathrm{GCD}\,(P, P')$, and let E be an ordered extension of F on the level D- 1 of complexity $\mathrm{NR}(Z')$ which is generated by the adjunction of the $\mathrm{NR}(Z')$ roots $\mathrm{R}(1, Z') < R(2, Z') < \ldots < R(NR(Z'), Z')$ of Z' ordered by magnitude. Let $R(0, Z') = -\infty$, $R(\mathrm{NR}(Z') + 1, Z') = \infty$, $1 \leqslant \mathrm{Z} \leqslant \mathrm{NR(P)}$. There is precisely one index J such that the number of sign changes of P on the subchain $R(0, Z') \ldots R(J, Z')$ is equal to I- 1 and that P changes sign from

$$A = R(J, Z') \text{ to } \quad B = R(J+1, Z').$$

Using these particular values of A, B we repeat the construction performed above in order to prove the between value theorem. We use the root symbol $R\,(I, P)$ in place of R. We set

$$SIGN\,(U, I, P) = \mathrm{SIGN}\,(U(R(I, P))).$$

In this way we construct indeed an ordered extension $F(R(I, P))$ of F which is generated by the adjunction of one root $R(I, P)$ of P subject to the condition (12) as envisaged in the introduction.

Another application of the induction hypothesis now will yield the proof of Theorem 5. This is because the definition of the function SIGN $(U(R))$ in the proof of the between value theorem was forced upon us by the aim of the construction.

This completes the proof of the string of Theorems 1-7 by induction over the degree of P.

It is clear from the construction applied that the set of all polynomials with coefficients in $\boldsymbol{F}$ of all root symbols obtained by the construction on all degree levels and of all complexities with the previous operational rules will yield a constructive definition of an algebraic really closed overfield of $\boldsymbol{F}$.

To do the same thing in a more direct manner we observe that algebraic over algebraic is algebraic so that we establish constructively for any two root symbols $R(I, P)$, $R(J$, Q) with $P \in F[X]$, $Q \in F[X]$, two further root symbols $R(K, W)$, $R(L, T)$ (WE $F[X]$, $T \in F[X]$) such that

$$R(I, P) + R(J, Q) = R(K, W), \tag{29}$$

$$R(I, P)\, R(J, Q) = R(L, T). \tag{30}$$

In this way it is shown that the root symbols for polynomials of $F[X]$ with operational rules (29), (30) and positivity and equality as defined previously form an algebraic ordered extension P of $\boldsymbol{F}$. But in P every polynomial of odd degree has a root constructively as follows at once from the between value theorem. Similarly, every positive element of P is a square element. In other words P is really closed.

Again we must emphasize the remark made in A. Hollkott's thesis that $\boldsymbol{F}$ is embedded into P only up to isomorphism.

In particular the question whether the root symbol $R(I, P)$ is equal to an element of $\boldsymbol{F}$ in standard form R(1, X-A) $(A \in \boldsymbol{F})$ may be effectively undecidable for ill behaved groundfields (see [1]). However, for $\boldsymbol{F} = \boldsymbol{Q}$ it is clear that there is an effective procedure for finding all solutions of $\boldsymbol{P(A)} = 0$ in Q, the rational number field.

An ALGOL program for the real root calculus over Q has been written which implements a reduction discovered by H. Kempfert as well as the Sturm theorem of real algebra (see [5]). It will be discussed in a forthcoming joint paper by H. Kempfert and the author.

REFERENCES

1. A. Fröhlich and J. C. Shepherdson: Effective procedures in field theory. *Phil. Trans. Roy. Soc. London* **A 248** (1956), 407–432.
2. August Hollkott: Finite Konstruktion geordneter algebraischer Erweiterungen von geordneten Grundkörpern. Dissertation, Hamburg, 1941, pp. 1-65.
3. Alfred Tarski: *A Decision Method for Algebra and Geometry. (The* Rand Corporation, Santa Monica, Calif., 1948, III+60 pp.)
4. H. S. Vandiver: On the ordering of real algebraic numbers by constructive methods. *Ann. of Math. 37* (1936), *7-16.*
5. B. L. van der Waerden: *Algebra,* **2**, 7. Aufl., Heidelberger Taschenbiicher 23.

Some computational problems and methods related to invariant factors and control theory†

R. E. KALMAN

1. **Introduction.** The purpose of this modest talk is to point out some computational problems related to invariant factors in linear algebra. Our comments are intended as an interim progress report; full details will be published elsewhere, later.

As is well known, the determination of many invariants in linear algebra (for instance: minimal polynomials of a vector or a matrix, invariant subspaces, the rational canonical form of a matrix, the number of eigenvalues of a matrix in a half-plane or a circle) requires computation in the polynomial rings $\mathbf{R}[z]$ or $\mathbf{C}[z]$. These computations are rather awkward: first, because they involve checks of divisibility which must be exact; second, because polynomial arithmetic (especially matrix-valued polynomial arithmetic) is very awkward to program. Since the numbers desired are often integers (for instance: the degree of the minimal polynomial of a matrix), these problems tend to have some of the flavor of finite algebra, even though strictly speaking they belong to linear algebra.

The question arises: *Is it possible to bypass the machinery of polynomial algebra and relate everything to standard matrix computations, such as the determination of rank* ? This question is of some interest from the viewpoint of pure mathematics, since it concerns the representation of polynomial algebra (in the sense analogous to group representations) via matrices. Even more interesting perhaps are the implications on numerical analysis and computing art in general, since very little is known today about the relative *numerical* advantages and disadvantages of alternate computing procedures which are abstractly equivalent.

A very interesting and early

$$\text{“functor”} : \text{polynomials} \rightarrow \text{matrices}‡ \tag{1}$$

is that found in Hermite's famous paper [1] of 1856 (which introduced

† This work wassupported in part by NASA Grant NgR 05-020-073.

‡ We use the term “functor” in a nontechnical sense to mean vaguely: replace some mathematical object by a (linear) algebraic object.

"hermitian forms"). Hermite's functor has the special form

$$\{\text{polynomial } \pi \text{ of degree } n\} \rightarrow (n\times n \text{ symmetric matrix } P_\pi\} \qquad (2)$$

satisfying the property that

$$\{\text{number of roots of } \pi \text{ inside the unit circle}\} = \text{rank of } P_\pi. \qquad (3)$$

Our main object then is to try to exhibit other functors of this general type.

The motivation for this investigation is especially rich; in addition to pure and applied mathematics, it stems also from the modern mathematical theory of control and dynamical systems. For instance, a discussion of Hermite's functor in the style of Lyapunov stability theory and control theory was given in [2].

2. Common factors of polynomials. It is well known that the common factor of two polynomials can be determined by the Euclidean algorithm. If we wish to avoid (for numerical reasons) dividing polynomials, then we can make use of a well-known "functor" of type (1) known as the ***Euler–Sylvester determinant*** ([3], ch. 5, p. 104) which is defined as

$$\{\text{polynomials } f, g \text{ of degree } m, n\} \rightarrow \{\text{determinant } R_{f,g} \text{ of an } mn\times mn \text{ matrix}\}. \qquad (4)$$

Then f, g are relatively prime (have no common factor of degree > 0) if and only if $R_{f,g} \neq 0$.

The "functor" (4) is rather inefficient from the computational point of view since $R_{f,g}$ is a very large determinant. Moreover, if $R_{f,g}$ vanishes, so that f, g have *a* nontrivial greatest common divisor, it is not a simple matter to compute this common divisor.

We shall now exhibit a "functor" which is much more efficient for the above purposes.

Notations: let z = indeterminate, K = arbitrary field, deg f = degree of polynomial f. We assume that n = deg f > deg g (the special case deg f = deg g causes very little extra difficulty), and define the "codes"

$$f = z^n+f_1z^{n-1}+\ldots f_n \rightarrow F = \begin{bmatrix} 1 & 0 & & -f_n \\ & & & \cdot \\ & & & \cdot \\ & & \cdot & \cdot \\ & \cdot & & \\ & & 1 & -f_1 \end{bmatrix} \qquad (5)$$

$$g = g_1z^{n-1}+\ldots+g_n \rightarrow G = \begin{bmatrix} g_n \\ \cdot \\ \cdot \\ g_1 \end{bmatrix}. \qquad (6)$$

Finally, we write, as usual, (f, g) for the monic polynomial which is the greatest common factor off and g.

THEOREM. (i) $[G, FG, \ldots. F^{n-1}G] = g(f)$. *Hence* $\lambda_i(g(F)) = g(\varphi_i)$, *where* φ_i *are the roots off.*

(ii) deg (f, g) = *n-rank* [G, *FG*, . . . , $F^{n-1}G$].

(iii) $(f,$ g) = *g/h,where h is the minimal polynomial of the vector G relative to the matrix F, i.e.,*

$$F^{n-r}G+h_1F^{n-r-1}G+\ldots+h_{n-r}G = 0$$

with deg *h* = *r*, *r* = *minimum.*

Outline of proof. Fact (i) (and therefore the fact that $(f,$ g) = 0 if and only if rank [G, *FG*, . . . , $F^{n-1}G] = n$) was first proved in [**4**], Lemma 7. Note that in view of(i) (see [**3**], ch. 5, p. 107) the "functor"

$$(f, \text{g}) \to \det [\text{G}, FG, \ldots, F^{n-1}G] \tag{7}$$

is identical with the Euler-Sylvester "functor" $R_{f,g}$ ***which is now exhibited more efficiently using an n X n (rather than mn X mn) matrix.*** (The number $R_{f,g}$ is the classical resolvent off, g.)

The matrix

$$[G, FG, \ldots, F^{n-1}G],$$

which is to be thought of as made up of the (column) vectors G, *FG*, . . ., plays an important (and well-known) role in modern control theory under the names "controllability" and "observability".

The proof of (ii) and (iii) is a straightforward elaboration of (i), see [**5**].

The form and proof of this theorem suggests rephrasing the algebraic situation in module-theoretic terms. Recall (this is now classical) that any square matrix *F* (over the field *K*) induces a K[z]-module over $K_n = X$ regarded as an abelian group. To do this, we define

$$\text{scalar product: } K[z]\times K_n \to K_n,$$
$$: (f, x) \to f(F)x.$$

Given a fixed *F* (and fixed *n*), the condition

$$\text{rank } [\text{G}, FG, \ldots, F^{n-1}G] = n, \tag{8}$$

which is equivalent to

$$(f, g) = 0, \tag{9}$$

means in module language that

$$\textit{G generates the module X.} \tag{10}$$

This observation is closely related to the ***theory of realizations*** which (especially for our present purposes) may be regarded as a generalization of the classical theory of elementary divisors.

3. Theory of realizations. Consider the infinite sequence

$$\text{Y} = \{Y_k: k = 0, 1, \ldots, \quad Y_k = p\times m \text{ matrix over } K\}.$$

We say that Y has ***a finite-dimensional realization*** if and only if there exist matrices F, G, H over K such that

$$Y_k = HF^kG, \quad k = 0, 1, \ldots. \tag{11}$$

The matrix F is required to be $n \times n$ (then H is $p \times n$ and G is $n \times m$). We say that the realization is ***minimal*** if and only if n is the smallest integer for which (11) can be satisfied. The following theorem is fundamental:

If F_Y and $\hat{F}_Y$ belong to minimal realizations or the same Y, then they are similar.

A proof may be found in [5] or [6].

It is now clear that the theory of realizations generalizes the theory of elementary divisors: if A is some given matrix, then the set of all minimal realizations of the sequence $\{Y_k\} = \{A^k\}$ is identical with the similarity class of A, since all triples of the form (F, T, T^{-1}), with $T^{-1}FT = A$, are minimal realizations. So the following is a well-defined problem: Given $\{Y_k\}$ possessing a finite-dimensional realization, ***determine the similarity invariants of F belonging to some minimal realization.*** A rather detailed examination of this problem built around the classical machinery of invariant factors and elementary divisors is given in [7], to which the reader is referred also for additional motivation and background material.

In complete generality, that is, in terms of exhibiting efficient "functors" to linear algebra, the solution of the problem is definitely not known at present.? Let us review briefly what ***is*** known.

The simplest invariant of F (minimal) is given by the following result, which is new, turns out to be quite simple, and seems to be fundamental:

Let S_Y^N denote the blockwise $N \times N$ generalized Hankel matrix

$$S_Y^N = \begin{bmatrix} Y_0 & Y_1 & \cdots & Y_{N-1} \\ Y_1 & Y_2 & \cdots & Y_N \\ \cdot & \cdot & & \\ \cdot & & & \cdot \\ Y_{N-1} & Y_N & \cdots & Y_{2N-1} \end{bmatrix}$$

induced by the matrix sequence Y. Then dim F = rank S_Y^N ***for N sufficiently large. In other words, a finite-dimensional realization exists if and only if the rank of S_Y^N is eventually constant, and then***

$$n(Y) = \text{rank } S_Y^N = \sum_{i=1}^{q} \deg \psi_i \quad (\psi_{i+1} \quad \psi_i, \quad i = 1, \ldots, \text{q-l}),$$

where ψ_i are the invariant factors of the square matrix F belonging to any

† The computational experience of numerically determining minimal realizations has been summarized in [8], pp. 373–405. Four methods have been compared there: (i) classical elementary divisor theory (see [7]); (ii) partial fraction expansions and rank computations ([4], Section 8); (iii) direct application of elementary linear algebra ([4] Sections 7 and 8); (iv) Ho's algorithm via Hankel matrices 161.

minimal realization of Y. In particular, rank $S_Y^r = n(Y)$ ***for all*** $r \geqslant n(Y)$ ***or even*** $r \geqslant \deg \psi_1$.

Referring to the module language mentioned at the end of § 2, we can rephrase the preceding statements also as follows: ***The module induced by any F belonging to a minimal realization of Y is of dimension n(Y); this module is the direct sum of precisely q cyclic pieces, each with annihilating polynomial*** ψ_i. In short, the (numerical) sequence Y may be used to determine module invariants (***n, q,*** the ψ_i) with exactly the same ease (or difficulty) as it can be used to determine similarity invariants for ***F.***

It is clear that ***q,*** $\deg \psi_1$, and even the ψ_i could be determined by a combinatorial procedure examining the linear dependences of subsets of the matrix S_Y^n. The detailed prescriptions are easily inferred from [4–8]. It is, however, not yet clear if a "functorial" procedure can be obtained for this purpose. The clarification of this problem, in view of the situation sketched above, is clearly one of the outstanding present research problems in linear algebra.

This problem is closely related also to other unsolved elementary problems of a linear-algebraic type. Let us mention the following interesting

Conjecture. *("Parametrization* ***of minimal realizations.") Let (F, G,*** *H*) ***be a minimal realization of its own sequence*** $\{Y_k = HF^kG, k = 0, 1, \ldots\}$. ***Let X be the corresponding*** *K*[*z*]*-module,* ***with q cyclic pieces. Let*** $\psi_1, \ldots, \psi_q$ ***be the invariant factors of*** *X*, ***with*** $\psi_{i+1} \mid \psi_i$ ***and*** $\deg \psi_i = n_i$. ***(Thus*** $\psi_1 =$ ***minimal polynomial of X and*** $n_1 + \ldots + n_q = \dim X$.) ***Finally, let*** $m = p = q$ ***and*** rank $G = q$.

Then: For fixed q and fixed $(n_1, \ldots, n_q)$ ***the set of all such triples*** *plus* ***a set of measure zero (corresponding to triples which are not minimal) is a linear space over K whose dimension is precisely equal to***

$$\sum_{i=1}^{q} \min \{n_i, n_{i-1} - n_i\} + \sum_{j=1}^{q} (2j-1)n_j \quad (n_0 = \infty).$$

The first term in the above expression represents the minimal number of parameters necessary to specify all the invariant factors (given their degrees).

The second term is the dimension of the linear space of transformations leaving the rational canonical form of ***F*** invariant. (This number was first determined by Frobenius.) It can be shown that the dimension of the linear transformations leaving ***F*** invariant is precisely the same as the number of parameters in G which can be fixed over the whole class: For instance, if ***q*** = 1 or if $n_1 = \ldots = n_q$ all elements of G can be fixed. This is closely related to canonical forms of completely controllable pairs ***(F, G). See*** [7].

REFERENCES

1. C. HERMITE : Sur le nombre des racines d'une equation algtbrique comprises entre des limites données. *Oeuvres* 1(1900), 397-414.
2. R. E. KALMAN: On the Hermite-Fujiwara theorem in stability theory. ***Quart. Appl. Math.* 23** (1965), 279-282.
3. B. L. VAN DER WAERDEN: *Algebra,* 7th edition of *Modern Algebra* (Springer (Heidelberger Taschenbticher No. 12), 1966).
4. R. E. KALMAN: Mathematical description of linear dynamical systems. *SIAM J Control* 1 (1963), 152-192.
5. R. E. KALMAN: *Lectures on Algebraic System Theory* (Springer Lecture Notes in Mathematics, to appear).
6. B. L. Ho and R. E. KALMAN: Effective construction of linear state-variable models from input/output functions. *Regelungstechnik* **14** (1966), 545-548.
7. R. E. KALMAN: Irreducible realizations and the degree of a rational matrix. *SIAM J. Applied Math.* **13** (1965). 520-544.
8. R. E. KALMAN and T. S. ENGLAR: A user's manual for the automatic synthesis program (ASP), NASA Contractor Report CR-475, June 1966,526 pp.
9. R. E. KALMAN: On structural properties of linear, constant, multivariable systems. *Proc. 3rd IFAC Congress, London,* **1966.**

List **of** *participants*

THIS list includes all those who were present at the Conference, and also those who were not present but who contributed to the papers in this volume.

DR. E. ALTMANN, Rheinisch-Westftilisches Institut für Instrumentelle Mathetmatik, 53 Bonn, Wegelerstrasse 6, West Germany.

PROFESSOR P. B. BENDIX, Mathematics Department, California Institute of Technology, Pasadena, California 91109, U.S.A.

MR. C. BROTT, Mathematisches Seminar der Christian-Albrechts-Universität, Kiel, Neue Universitat, Olshausenstrasse 40-60, West Germany.

MR. R. BÜLOW, Mathematisches Seminar der Christian-Albrechts-Universitat, Kiel, Neue Universitat, Olshausenstrasse, 40-60, West Germany.

MR. C. M. CAMPBELL, Department of Pure Mathematics, University of St. Andrews, St. Andrews, Fife, Scotland.

MR. J. J. CANNON, Department of Pure Mathematics, University of Sydney, Sydney, Australia.

DR. R. F. CHURCHHOUSE, Atlas Computer Laboratory, Chilton, Didcot, Berkshire, England.

DR. C. R. J. **CLAPHAM,** Department of Mathematics, Ahmadu Bello University, Zaria, Northern Nigeria, West Africa.

DR. A. M. COHEN, Department of Mathematics, Welsh College of Advanced Technology, Cathays Park, Cardiff, Wales.

PROFESSOR HARVEY COHN, Department of Mathematics, University of Arizona, Tucson, Arizona 85721, U.S.A.

DR. J. H. CONWAY, Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge, England.

DR. B. CORBAS, Department of Pure Mathematics, The University, Reading, England.

DR. J. DÉNES, Central Research Institute for Physics, Hungarian Academy of Sciences, P.O.B. 49, Budapest 114, Hungary.

DR. M. J. DUNWOODY, Mathematics Department, University of Sussex, Falmer, Brighton, Sussex, England.

MR. V. FELSCH, Mathematisches Seminar der Christian-Albrechts-Universität, Kiel, Neue Universitlt, Olshausenstrasse 40-60, West Germany.

MRS. K. FERBER (*née* Espenhain), Mathematisches Seminar der Christian-Albrechts-Universitat, Kiel, Neue Universitat, Olshausenstrasse 40-60, West Germany.

DR. J. J. FLORENTIN, Centre for Computing and Automation, Royal School of Mines Building, Imperial College, London S.W.7, England.

PROFESSOR LESLIE FOX, Oxford 'University Computing Laboratory, 19 Parks Road, Oxford, England.

PROFESSOR J. S. FRAME, Department of Mathematics, Michigan State University, East Lansing, Michigan 48823, U.S.A.

DR. LEONHARD GERHARDS, Rheinisch-Westfalisches Institut für Instrumentelle Mathematik, 53 Bonn, Wegelerstrasse 6, West Germany.

DR. C. M. GLENNIE, Home Office Statistical Branch, Tolworth, Surrey, England.

MR. M. J. T. GUY, The University Mathematical Laboratory, Corn Exchange Street, Cambridge, England.

PROFESSOR MARSHALL HALL, Department of Mathematics, California Institute of Technology, Pasadena, California 91109, U.S.A.

PROFESSOR D. G. HIGMAN, Department of Mathematics, The University of Michigan, 3220 Angell Hall, Ann Arbor, Michigan 48104, U.S.A.

PROFESSOR G. HIGMAN, F.R.S., Mathematical Institute, University of Oxford, 24/29 St. Giles, Oxford, England.

DR. J. W. P. HIRSCHFELD, Mathematics Department, The University of Sussex, Falmer, Brighton, Sussex, England.

DR. J. HOWLETT, Atlas Computer Laboratory, Chilton, Didcot, Berkshire, England.

DR. D. R. HUGHES, Department of Mathematics, Westfield College, London N.W.3, England.

MR. E. J. HUTTON, I.C.T. Limited, Brandon House, 61 Broadway, Bracknell, Berkshire, England.

DR. R. E. INGRAM, S.J., University College, Dublin, Eire (died 6 th October 1967).

MR. H. JÜRGENSEN, Mathematisches Seminar der Christian-Albrechts-Universitat, Kiel, Neue Universitlt, Olshausenstrasse 40-60, West Germany.

PROFESSOR R. E. KALMAN, Stanford Electronics Laboratories, Stanford University, California 94305, U.S.A.

DR. A. D. KEEDWELL, Department of Mathematics, University of Surrey, Stag Hill, Guildford, Surrey, England.

PROFESSOR R. KEOWN, Department of Mathematics, University of Arkansas, Fayetteville, Arkansas, U.S.A.

PROFESSOR D. E. KNUTH, Mathematics Department, California Institute of Technology, Pasadena, California 91109, U.S.A.

PROFESSOR E. F. KRAUSE, Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104, U.S.A.

DR. A. LEARNER, Department of Mathematics, Queen Mary College, Mile End Road, London E.l, England.

MR. J. LEECH, Dept. of Computing Science, University of Stirling, Stirling, Scotland.

DR. SHEN LIN, Room 2C-523, Bell Telephone Laboratories Inc., Murray Hill, New Jersey 07971, U.S.A.

DR. W. LINDENBERG, Rheinisch-Westfalisches Institut für Instrumentclle Mathematik, 53 Bonn, Wegelerstrasse 6, West Germany.

MR. J. K. S. MCKAY, Atlas Computer Laboratory, Chilton, Didcot, Berkshire, England.

DR. D. H. MCLAIN, Computing Centre, University College of South Wales and Monmouthshire, Cathays Park, Cardiff, Wales.

DR. W. D. MAURER, College of Engineering, University of California, Berkeley, California 94720, U.S.A.

PROFESSOR N. S. MENDELSOHN, Department of Mathematics, University of Manitoba, Winnipeg, Manitoba, Canada.

PROFESSOR W. 0. J. MOSER, Department of Mathematics, McGill University, Montreal P.Q., Canada.

PROFESSOR THEODORE S. MOTZKIN, Department of Mathematics, University of California, Los Angeles, California 90024, U.S.A.

PROFESSOR W. D. MUNN, Mathematics Department, University of Stirling, Stirling, Scotland.

DR. J. NEUBÜSER, Mathematisches Seminar der Christian-Albrechts-Universitat, Kiel, Neue Universitat, Olshausenstrasse 40-60, West Germany.

PROFESSOR L. J. PAIGE, Department of Mathematics, University of California, 405 Hilgard Avenue, Los Angeles, California 90024, U.S.A.

DR. ROBERT J. PLEMMONS, Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37916, U.S.A.

PROFESSOR J. BARKLEY ROSSER, Math. Research Center, U.S. Army, University of Wisconsin, Madison, Wisconsin 53706, U.S.A.

CAPTAIN P. G. RUUD, Department of Mathematics, College of Science, Texas A. & M. University, College Station, Texas 77843, U.S.A.

MISS JEAN SCOTT, Computer Department, City University, St. John Street, London E.C.l, England.

PROFESSOR JOHN L. SELFRIDGE, Mathematics Department, University of Illinois, Urbana, Illinois 61801, U.S.A.

PROFESSOR CHARLES C. SIMS, Department of Mathematics, Rutgers, The State University, New Brunswick, New Jersey 08903, U.S.A.

DR. N. M. STEPHENS, School of Mathematics and Physics, University of East Anglia, Wilberforce Road, Norwich NOR 77H, England.

MR. H. P. F. SWINNERTON-DYER, Department of Pure Mathematics and Mathematical Statistics 16 Mill Lane, Cambridge, England.

PROFESSOR T. TAMURA, Department of Mathematics, University of California, Davis, California 95616, U.S.A.

PROFESSOR S. J. TOBIN, Department of Mathematics, University College, Galway, Eire.

MR. A. L. TRITTER, University of Oxford Mathematical Institute, 24/29 St. Giles, Oxford, England.

PROFESSOR H. F. TROTTER, Department of Mathematics, Fine Hall, Box 708, Princeton University, Princeton, New Jersey 08540, U.S.A.

DR. A. WAGNER, Department of Mathematics, Queen Elizabeth College, 61-67 Campden Hill Road, London W.8, England.

PROFESSOR G. E. WALL, Department of Mathematics, The University, Sydney, Australia.

PROFESSOR K.W. WESTON, Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556, U.S.A.

PROFESSOR H. ZASSENHAUS, Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, Ohio 43210, U.S.A.