
THE UNIVERSITY *of* EDINBURGH

# Computing with finite groups

John K.S. McKay

Ph.D. 1970

University of Edinburgh

## Summary

The character table of a finite group G is constructed by computing the eigenvectors of matrix equations determined by the centre of the group algebra. The numerical character values are expressed in algebraic form. A variant using a certain sub-algebra of the centre of the group algebra is used to ease problems associated with determining the conjugacy classes of elements of G. The simple group of order 50,232,960 and its subgroups PSL(2,17) and PSL(2,19) are constructed using general techniques.

A combination of hand and machine calculation gives the character tables of the known simple groups of order $< 10^6$ excepting Sp(4,4) and PSL(2,q). The characters of the non-Abelian 2-groups of order $\leq 2^6$ are computed.

Miscellaneous computations involving the symmetric group $S_n$ are given.

Acknowledgement

I thank my supervisors, Professor W.D. Munn and Professor S. Michaelson, for much patience and many kindnesses during the preparation of this thesis.

My thanks go also to my wife Wendy who has tirelessly typed and retyped the manuscript and organised me.

Contents

Page

TABLES

APPENDIX B - The character tables

The known simple groups of order $\leq 10^6$ excepting Sp(4,4) and PSL(2,q).

The Sylow 2-subgroup of Sz(8).

# Chapter 1

## Introduction

> `I believe that progress in group theory depends primarily on an intimate knowledge of a large number of special groups.'
>
> G. Higman
> Mathematical Reviews 1958.

Methods for investigating the structure of finite groups with a digital computer are described here. This thesis is not concerned with specific groups except in so much as they provide examples for computational techniques. The initial motivation of a major part of this study has been the problem of producing character tables of groups but methods of general use in working with finite groups have been developed in pursuing this end. Experience shows that no single method is likely to be efficient for investigating groups of widely differing structures, orders, and presentations.

The field covered by this work - the field of computational algebra - has been remarkably neglected until recently. This is in some ways surprising because of the susceptibility of finite groups to computational ideas and the interest in these groups and their representations by solid-state physicists, chemists and crystallographers.

This neglect may be accounted for in part by the immediate post-war development of the digital computer as a tool in the hands of applied mathematicians who wished to solve systems of differential equations numerically and in doing so developed the now well-established methods of computational numerical analysis. Because of this historical accident the mathematical use of computers has become associated by many almost exclusively with applied mathematics. The major reference to computing in algebra is Leech [ L1 ].

Although the methods described here are not new in concept, they do differ significantly in approach from the methods of classical pure mathematics. There are two main differences: for a method to be suitable for use on a computer it should (with qualifications concerning heuristic methods to be illustrated later) be constructive, whereas many proofs in text books are existential in nature; secondly, even if the method is constructive other constraints must be imposed if the method is to be a practical one. To illustrate the difference between the existential and the constructive outlook, the definition of a finite group in terms of a set of generators and defining relations, although often adequate for many purposes for the pure mathematician, tells us little directly about how to explicitly construct the distinct elements of the group.

Two conflicting restrictions in applying computers to

groups are those of time and space - for the sake of concreteness it is assumed that the time available for computation does not exceed 10 hours and that the method is suitable for a computer having no more than 100K words of fast store and an arbitrary amount of backing store with its appropriate slow access time. A feasible computation is defined as one lying within these limits. These two practical restrictions are severe and often a compromise has to be sought between them. It is clearly not enough to have an algorithm to solve the problem, it must also be feasible. What is not feasible now may become so by means of a new mathematical technique or an improvement in computing power. To give an extreme but illustrative example of feasibility: consider the problem of deciding whether two groups of order g, say, are isomorphic. This can be decided by setting up, or attempting to set up, a 1-1 correspondence between individual elements of the two groups. There are at most g! mappings to be examined. Even if the strong assumption that the groups are sufficiently small for all their elements to be directly accessible is made, it is not practical to examine all 1-1 mappings between the groups for any small order, say, greater than 8, and so methods must be found for paring down the problem by finding pairs of sets of elements - one set from each group - which must be mapped set-wise into each other. Thus if $G_1$ and $G_2$ can both be partitioned into sets of $s_i$ elements ($i = 1,2$,

...,k) then it is necessary to examine at most only $\prod_{i=1}^{k} s_i!$ mappings where $\sum_{i=1}^{k} s_i = g$, instead of g!. This constitutes a substantial improvement in many cases although the improvement may be slight for certain p-groups. An attempt may then be made to find a method particularly suited for p-groups.

Investigating the structure of finite groups with a computer may be regarded in two lights. It may be seen as an academic exercise providing mechanical methods of solution for problems which would not have arisen other than from a wish to use the machine. Alternatively, it may be regarded pragmatically as a useful practical tool in the hands of a pure mathematician. If the second attitude is adopted it is no longer necessary to expect the problem to be solved entirely by computer; it is sufficient that the mathematician can be materially helped. I feel strongly that motivation for computing should come from genuine problems in mathematics. This motivation provides a forcing ground for new computational techniques. The more difficult the problem, the greater the need to develop more powerful techniques. I envisage interaction between the mathematician and the computer. For example, in finding the set of defining relations for a simple group presented in terms of an explicit set of generators (say permutations or matrices over some field) a heuristic

approach could be adopted as follows:

Using an on-line console, relations between elements are derived with a utility program for manipulating permutations or matrices. When it is thought that sufficient relations have been found and words generating a subgroup have been decided upon, then an attempt at coset enumeration is carried out. If this fails, further relations may be sought and the attempt repeated until the enumeration succeeds. For reasons of time this approach can be carried out efficiently only by using an interactive technique with the machine.

It seems likely that within the next decade the computer will be used for exhaustively examining groups of low order, for examples or counter-examples of conjectures, and in investigating large groups by means of special programs. In the near future pure mathematicians will be stimulated into using machines as a common place aid to their work through immediate access to large computers using consoles in their own rooms.

The main part of this thesis contains the description of algorithms for determining character tables of finite groups by computer by constructing the class algebra of the group. This approach is critically dependent upon the construction of a function mapping the elements of G into their conjugacy classes. This map is difficult to compute for permutation groups if there are non-conjugate elements

which generate the same cyclic subgroup. The use of the rational class algebra lessens this problem but the existence of an outer automorphism of G which interchanges rational classes makes it difficult to distinguish even these classes. Conditions favouring the computation of characters via the class algebra are (i) the construction of a map from elements to their classes which is fast to compute and (ii) the existence of a class $C_i$ with the property that many of the values of $\chi_{si}/d_s$ are distinct. A weakness of the method is that it does not use facts usually available such as the existence of subgroups of small index.

Burnside [ B5 ] in 1911 gives a specimen calculation of the characters of the dihedral group of order 10 from its class algebra. The first description of the computation of characters with electronic computers in mind is a typescript by Hayes [ H7 ] written in 1963. His method is essentially to compute the roots of minimal polynomials satisfied by each of the class sums. He is unable to prove that the method does not generate spurious solutions and there is no indication that it has been programmed. For the September 1966 IBM Blaricum conference I described [ M6 ] methods which are basically those given here for character calculations. Dixon [ D2 ] in 1967 published a paper on high speed computation of group characters. He states that his method is practical for groups of order up

to 1000 or so and considers the calculations of the eigenvectors to be the most difficult part of the computation. For large groups the difficulty does not lie here but in the earlier steps of computing the classes and the class algebra. Dixon does not discuss this. The importance of his paper lies in his transposition of the eigenvalue problem from the field of complex numbers into the field of integers modulo a certain prime p. This transposition ensures that the arithmetic can be performed exactly. A weakness of this method is that p may be very large. In my view such difficulties as there are in computing eigenvectors are to major extent overcome by making them orthogonal, (see Chapter 7). The determination of the classes and the computation of the class algebra take an order of magnitude more time than the determination of the eigenvectors.

Character tables of the 311 non-Abelian 2-groups of order $\leq 2^6$ have been computed from Hall and Senior [ H2 ]. It is inconvenient to give all the character tables so a single one of order 64 (which is the Sylow 2-subgroup of Suzuki's simple group of order 29,120) is given. From the character tables a list of those 2-groups for which the number of irrationalities in the rows and in the columns is distinct has been compiled.

The character tables of the known simple groups of order $< 10^6$, excluding Sp(4,4) and PSL(2,q), are given.

Few of the tables are new although some have not been given explicitly before.

Techniques for searching for permutation characters are given and a method for exhibiting certain subgroups is described. These techniques are used in the construction, with G. Higman [ H9 ], of Janko's group of order 50,232,960. Independently and at the same time, Conway and Guy proved the existence of this group by coset enumeration.

Some computations involving the symmetric group are given including the computation of the character tables and tabulation of the largest degrees of irreducible representations of $S_n$ for $n \leq 75$.

Examination of character tables leads to the observation that the number m(G) of irreducible characters of odd degree in a known simple group G of order $< 10^6$ is a power of 2. This seems true for the symmetric and alternating groups also.

# Chapter 2

## Representations, characters, and the group algebra

For completeness a brief introduction is given to that part of the representation theory of finite groups which is needed later. A comprehensive account is given in Curtis and Reiner [ C5 ].

Throughout, unless explicitly stated to the contrary, G is a finite group of order g having conjugacy classes $C_i$ ($C_1 = \{e\}$) of order $h_i$ ($i = 1,2,\ldots,r$) and $C_i'$ is the class $\{x \mid x^{-1} \varepsilon C_i\}$.

A <u>representation</u> R of a group G over a field F is a homomorphism of G into a group of non-singular linear transformations of a finite dimensional vector space V, called the <u>representation space</u> of R, over F. The dimension of the space V is the <u>degree</u> of R. A representation is <u>faithful</u> if it is an isomorphism. Representations $R_1$ and $R_2$ are <u>equivalent</u> if they have the same representation space in which there exists a constant non-singular linear transformation T such that $R_1(x) = T^{-1}R_2(x)T$ for all $x \varepsilon G$. $R_1$ and $R_2$ are said to be <u>inequivalent</u> if they are not equivalent.

An <u>algebra</u> A(F) over a field F is a ring with an identity which is also a vector space over F. Multiplication

by scalars in the vector space and ring multiplication satisfy

$$\alpha(xy) = (\alpha x)y = x(\alpha y), \qquad \alpha \varepsilon F, \quad x,y \varepsilon A(F). \tag{2.1}$$

A subring of A(F) which is also an F-space of A(F) is a subalgebra of A(F). The group algebra A(G,F) of a group G over a field F is the ring of all formal sums

$$\sum_x \alpha_x x, \qquad \alpha_x \varepsilon F, \quad x \varepsilon G \tag{2.2}$$

which satisfy

$$\sum_x \alpha_x x + \sum_x \beta_x x = \sum_x (\alpha_x + \beta_x)x, \tag{2.3}$$

$$(\sum_x \alpha_x x)(\sum_y \beta_y y) = \sum_z \gamma_z z, \quad \text{with } \gamma_z = \sum_{xy=z} \alpha_x \beta_y. \tag{2.4}$$

The identity element of A(G,F) is the element $1_F \cdot e$ where $1_F$ is the identity of F and e is the identity of G.

There is an isomorphism of G into A(G,F) defined by the mapping $x \longrightarrow 1_F \cdot x$, $x \varepsilon G$. By identifying x with its image in A(G,F), G is viewed as naturally embedded in A(G,F).

A representation R' of the group algebra A(G,F) with representation space V over F is an algebra homomorphism from A(G,F) into the set of linear transformations of V into itself, that is,

$$R'(x + y) = R'(x) + R'(y) \tag{2.5}$$

$$R'(xy) = R'(x)\, R'(y) \tag{2.6}$$

$$R'(\alpha x) = \alpha R'(x), \quad R'(e) = 1 \qquad (2.7)$$

$$x,y \varepsilon A(G,F), \ \alpha \varepsilon F.$$

Let R be a representation of G as defined above, then there is a unique way of extending R by linearity to a representation R′ of A(G,F) over the same representation space V, namely by defining

$$R'\left(\sum_x \alpha_x x\right) = \sum_x \alpha_x R(x), \quad \alpha_x \varepsilon F, \ x \varepsilon G \qquad (2.8)$$

and conversely, any representation of A(G,F) yields a representation of G by restriction.

The group of non-singular linear transformations of an n-dimensional representation space V over a field F is isomorphic to the group, GL(n,F), of non-singular n x n matrices with coefficients in F. So a representation of G of degree n over F can be regarded as a homomorphism of G into GL(n,F). A <u>matrix representation</u> M afforded by R is the homomorphism M: $x \longrightarrow M(x)$ where $M(x) \varepsilon GL(n,F)$. Matrix representations $M_1$ and $M_2$ are equivalent if they have the same degree n and there is a constant non-singular matrix T such that

$$M_1(x) = T^{-1} M_2(x) T \qquad \text{for all } x \varepsilon G . \qquad (2.9)$$

The transformation M(x) can be represented uniquely by a matrix of degree n with entries in F once a basis for V has been chosen. Representations are equivalent whenever the matrix representations afforded by them are equivalent.

An invariant subspace of the representation space V is a subspace W of V such that $WR(x) \subseteq W$ for all $x \in G$. If $W \neq \{0\}$, R defines representations $R_1$ and $R_2$ of G with representation spaces W and V-W. These representations are called the constituents of R. A representation of G over F is irreducible (over F) if V has no invariant subspaces other than itself and {0}. The representation R is reducible (over F) if it is not irreducible (over F); it is completely reducible (over F) if V is the direct sum of irreducible invariant subspaces of V.

Alternatively, in terms of matrix representations, the matrix representation R of G over F is reducible over F if and only if there exists a constant non-singular matrix T with entries in F such that

$$T^{-1}R(x)T = \begin{array}{c|c} R_1(x) & U(x) \\ \hline 0 & R_2(x) \end{array} \qquad (2.10)$$

for all $x \in G$, where $R_1$ and $R_2$ are constituents of R.

R is completely reducible over F if and only if there exists a constant matrix T as above such that

$$T^{-1}R(x)T = \begin{array}{c|c} R_1(x) & 0 \\ \hline & \ddots \\ \hline 0 & R_k(x) \end{array} \qquad (2.11)$$

for all $x \in G$ and each $R_i$ irreducible over F.

A theorem due to Maschke [ C5 ] states that every representation of a group G over a field F is completely reducible if char(F) does not divide g. A representation of G over F such that char(F) divides g is known as a modular representation of G.

A representation of G over F may be considered as a representation over some extension field of F. A representation of G over F is absolutely irreducible if it remains irreducible over every extension field of F.

Henceforth, except where explicitly stated to the contrary, all representations are taken over C, the field of complex numbers. Consequences of this are that irreducibility implies absolute irreducibility and that every representation of G is completely reducible. Further, the matrices R(x), $x \varepsilon G$ are diagonalizable.

Let M(x) be a matrix representation of G afforded by the representation R. Define the character of R by the map $\varphi$: $G \longrightarrow C$ given by $\varphi$: $x \longrightarrow$ trace (M(x)) and say R affords $\varphi$. An irreducible character is a character afforded by an irreducible representation. The character is well-defined since equivalent representations afford the same character because equivalent matrices have the same trace. From this fact it is deduced that the character is a class function, that is, $\varphi(y^{-1}xy) = \varphi(x)$, $x,y \varepsilon G$. If $R = R_1 \oplus R_2$ then the character afforded by R is the sum of the characters afforded by $R_1$ and $R_2$. If R affords $\varphi$

then $\varphi(1)$ is the degree of R. It is proved in [ C5 ] that the number of inequivalent irreducible representations of a finite group G is the number of conjugacy classes of G.

Let $\chi_1(=1), \chi_2, \ldots, \chi_r$ be the characters of G afforded by the inequivalent irreducible representations of G. Let $x_j \varepsilon C_j$, $(j = 1,2,\ldots,r)$, then the r x r matrix X with entries $\chi_{ij} = \chi_i(x_j)$, $(i,j = 1,2,\ldots,r)$ is the <u>character table</u> of G. The importance of the characters lies in the existence of an inner product of characters satisfying fundamental orthogonality relations on the rows and columns. These orthogonality relations are as follows:

$$\frac{1}{g} \sum_{x \varepsilon G} \chi_i(x)\bar{\chi}_j(x) = \frac{1}{g} \sum_{k=1}^{r} h_k \chi_{ik} \bar{\chi}_{jk} = \delta_{ij} \qquad (2.12)$$

on the rows, and on the columns

$$\frac{1}{g} \sum_{i=1}^{r} \chi_i(x_s)\bar{\chi}_i(x_t) = \frac{1}{g} \sum_{i=1}^{r} h_s \chi_{is} \bar{\chi}_{it} = \delta_{st} \qquad (2.13)$$

where $\bar{}$ denotes complex conjugate and $\delta_{ij} = 0$, $i \neq j$, $\delta_{ii} = 1$. The orthogonality relations are equivalent to the statement that the matrix U with (i,j)th entry $u_{ij} = (\frac{h_j}{g})^{\frac{1}{2}} \chi_{ij}$, $(i,j = 1,2,\ldots,r)$, is unitary, that is $UU^* = I$ where $U^*$ is the complex conjugate transpose of U.

For an element $x \varepsilon G$ of period k, the character $\varphi(x)$ afforded by the representation R is a sum of kth roots of unity and $\varphi(x^{-1}) = \bar{\varphi}(x)$, since if $\mu$ is an eigenvalue of $R(x)$

then $\mu^{-1} = \bar{\mu}$ is the corresponding eigenvalue of $R(x^{-1})$.

The fundamental Schur's lemma [ C5 ] states that if T is a constant non-zero transformation and $R_1$, $R_2$ are irreducible representations of G and $TR_1(x) = R_2(x)T$ for all $x\varepsilon G$ then T is non-singular (and $R_1$ and $R_2$ are equivalent).

The centre C(A) of an algebra A is the subalgebra defined by $C(A) = \{z \mid zx = xz, \text{ for all } x\varepsilon A\}$. In A(G,C) define the class sum $c_i$ by $c_i = \sum_{x\varepsilon C_i} x$, $i = 1,2,\ldots,r$. The class sums form a basis for the centre of A(G,C) known also as the class algebra of G over C since

(i) the class sums lie in the class algebra, for

$$x^{-1}c_i x = \sum_{y\varepsilon C_i} x^{-1}yx = c_i;$$

(ii) the $c_i$, $i = 1,2,\ldots,r$ are linearly independent since they consist of sums of disjoint elements of G; and

(iii) if $x = \sum_x \mu_x x$, $\mu_x \varepsilon C$, $x\varepsilon G$, lies in the class algebra then $\sum_x \mu_x x = z = y^{-1}zy = \sum_x \mu_x y^{-1}xy$ and hence, by comparing coefficients, $\mu_{x^{-1}yx} = \mu_x$ for all $y\varepsilon G$, thus $\mu_x = \mu_y$ whenever x and y are conjugate in G so z is a C-linear combination of the class sums.

The structure of the class algebra is given by the fundamental system of equations

$$c_i c_j = \sum_{k=1}^{r} a_{ijk} c_k, \quad i,j = 1,2,\ldots,r. \tag{2.14}$$

These equations will be referred to as the class equations and the non-negative integer constants $a_{ijk}$ as the structure constants of the class algebra.

By taking an irreducible representation $R^s$ of degree $d_s$ of both sides of the equation $xc_i = c_i x$ for all $x \varepsilon G$, it is found that

$$R^s(x)R^s(c_i) = R^s(c_i)R^s(x) \quad \text{for all } x \varepsilon G, \tag{2.15}$$

and so, by Schur's lemma, either $R^s(c_i)$ is the $d_s$ x $d_s$ zero matrix or $R^s(c_i)$ is non-singular. In the latter case, let $m_{si}$ be an eigenvalue of $R^s(c_i)$. The matrix $[R^s(c_i)-m_{si}I]$ is singular and commutes with $R^s(x)$ for all $x \varepsilon G$. Thus, $R^s(c_i) = m_{si}I$, by applying Schur's lemma again.

By applying these results to the class equations (2.14) and comparing coefficients of the identity on both sides it is found that

$$m_{si}m_{sj} = \sum_{k=1}^{r} a_{ijk} m_{sk}, \quad i,j = 1,2,\ldots,r. \tag{2.16}$$

Finally, these may be written as the set of r matrix equations

$$A^i \underline{m}^s = m_{si}\underline{m}^s, \quad i,s = 1,2,\ldots,r \tag{2.17}$$

where $A^i$ is the r x r matrix with (j,k)th entry $a_{ijk}$, and

$$\underline{m}^s = \begin{bmatrix} m_{s1} \\ m_{s2} \\ \vdots \\ m_{sr} \end{bmatrix} \qquad i,j,k,s = 1,2,\ldots,r.$$

Theorem: The set of r x r matrix equations

$$A^i\underline{x} = \mu_i\underline{x}, \qquad i = 1,2,\ldots,r \tag{2.18}$$

has the unique (to within non-zero scalar multiples) complete set of eigenvectors $\underline{m}^s$, s = 1,2,...,r, and the eigenvalue of $A^i$ corresponding to the eigenvector $\underline{m}^s$ is $m_{si}$, i,s = 1,2,...,r.

Proof: Recall that $R^s$ is a homomorphism and therefore maps the identity of the class algebra into the identity matrix. But $R^s(1) = m_{s1}I$, so $m_{s1} = 1$ and the vectors $\underline{m}^s$, s = 1,2,...,r, are non-zero. It follows from the equations (2.17) that $\det\{A^i - m_{si}I\} = 0$. This shows that $m_{si}$ are eigenvalues of $A^i$ and that $\underline{m}^s$, s = 1,2,...,r, are a set of common eigenvectors of $A^i$ for all i = 1,2,...,r. More knowledge of the eigenvalues $m_{si}$ is needed to prove that the eigenvectors $\underline{m}^s$, s = 1,2,...,r, are a unique complete set. The character of $C_i$ afforded by $R^s$ determines $m_{si}$:

$$\text{trace}(R^s(c_i)) = \text{trace}\Big(\sum_{x\in C_i} R^s(x)\Big) = \sum_{x\in C_i} \text{trace}(R^s(x)) = h_i\chi_{si}.$$

But,

$$\text{trace}(R^s(c_i)) = \text{trace}(m_{si} I)$$

and so

$$m_{si} = \frac{h_i \chi_{si}}{d_s}, \qquad \text{where } d_s = \chi_{s1}. \tag{2.19}$$

The row orthogonality relations may be written in matrix notation as $M\bar{X} = D$ where the $(i,j)$th entry of $M$ is $m_{ij}$, $i,j = 1,2,\ldots,r$, and $D$ is the diagonal matrix with entries $d_{ii} = \frac{g}{d_i}$. Since $D$ is non-singular, $M$ is of rank $r$ and the space in which $M$ acts is spanned by the basis vectors $\underline{m}^s$, $s = 1,2,\ldots,r$, so the eigenvectors $\underline{m}^s$, $s = 1,2,\ldots,r$ form a complete set. Finally the set $\underline{m}^s$, $s = 1,2,\ldots,r$ is uniquely determined (to within constant non-zero scalar multiples) for suppose that $\underline{x}$ is a common eigenvector of $A^i$, $i = 1,2,\ldots,r$, with eigenvalue $\mu_i$ for each $A^i$, then

$$A^i\underline{x} = \mu_i\underline{x}, \qquad i = 1,2,\ldots,r, \text{ and } \underline{x} \neq \underline{0}. \tag{2.20}$$

The set $\underline{m}^s$, $s = 1,2,\ldots,r$, forms a basis for the space of right eigenvectors of the $A^i$, $i = 1,2,\ldots,r$, so

$$\underline{x} = \sum_{t=1}^{r} a_t \underline{m}^t \quad \text{for some } a_t \text{ not all zero.} \tag{2.21}$$

Suppose that $a_s \neq 0$ then

$$A^i\underline{x} = A^i\left(\sum_{t=1}^{r} a_t\underline{m}^t\right) = \sum_{t=1}^{r} a_t m_{ti}\underline{m}^t, \tag{2.22}$$

$$i = 1,2,\ldots,r$$

but

$$A^i\underline{x} = \mu_i\underline{x} = \sum_t a_t\mu_i\underline{m}^t, \qquad i = 1,2,\ldots,r, \tag{2.23}$$

and so

$$\sum_t a_t m_{ti}\underline{m}^t = \sum_t a_t\mu_i\underline{m}^t, \qquad i = 1,2,\ldots,r. \tag{2.24}$$

Comparison of the coefficients of $a_s(\neq 0)$ on both sides of (2.24) gives

$$\mu_i = m_{si}, \qquad i = 1,2,\ldots,r, \tag{2.25}$$

and substitution of $m_{si}$ for $\mu_i$ in (2.24) and rearranging gives

$$\sum_{t=1}^{r} a_t(m_{ti} - m_{si})\underline{m}^t = \underline{0}, \quad i = 1,2,\ldots,r, \tag{2.26}$$

and since the $\underline{m}^t$ are linearly independent

$$a_t(\underline{m}^t - \underline{m}^s) = \underline{0} \qquad t = 1,2,..,r. \tag{2.27}$$

Finally $a_t = 0$ for all $t \neq s$. Thus

$$\underline{x} = a_s\underline{m}^s, \quad (a_s \neq 0). \tag{2.28}$$

# Chapter 3

## The construction of the group

It is useful when discussing methods for investigating groups to distinguish between those methods for manipulating elements which are independent of the representation used, for example, methods for working with abstract words in generators, and those methods which depend in some way on the properties of a particular representation, for example, the classification of elements by their disjoint cycle structure which can be associated only with monomial or permutation representations.

Representation-independent methods are more general as representation matrices can be substituted after these methods have been used but there are some problems which are more easily solved when a faithful representation is used. An example is the word problem of deciding when two elements of a group are identical. This is because the representation matrix for each element is unique whereas the representation of an element as a word in a set of generators is not. To solve the word problem using a faithful representation it is necessary only to identify two matrices or permuations.

A representation-independent method is given for generating G which, in addition, gives a very economical way of storing elements. Janko's simple groups of order 175,560

and 604,800 are given as examples.

Coset enumeration

A group is well-defined when presented in terms of a set of generators and relations. However, such a definition does not immediately lead to a method for constructing the group elemnt by element. A technique for doing this by generating all the elements of G without repetition is described here. The method is based on coset enumeration which is described in detail in Leech [ L1 ].

Coset enumeration may be thought of basically as a method, easily adaptable for computer use, for drawing the Schreier coset diagram of a group. Let H be a subgroup of G, then the coset $Hx_i$ (the ith coset to be created) is joined to coset $Hx_j$ by a directed edge of colour k if $Hx_i g_k = Hx_j$ where $g_k$ is a generator of G. It follows from this that differing presentations of G do, in general, yield distinct Schreier diagrams and that the Schreier diagram is to be associated with the presentation of the group and not the group itself.

The Schreier diagram is stored in the computer as a coset table giving the effect on the cosets of H of multiplication by each generator of G and its inverse.

To use coset enumeration it is necessary to present the group G in terms of generators and defining relations and to present the subgroup H in terms of those words in the generators of G which generate it. By working through

the relations systematically the table is eventually filled up. Mendelsohn [ M8 ] has proved that this table is eventually filled and the process terminates if and only if the index [G:H] is finite.

Generation of the group elements

An element of G may be written as the product $h_i\varphi_j$ where $h_i \varepsilon H$ and $\varphi_j$ is a coset representative of H in G. The representation of an element in this form in unique once the coset representatives have been chosen. To construct the coset representatives the following lemma is needed.

Lemma: For each i ($\neq 1$) the equation $Hx_i g_k = Hx_j$, where j is less than i and $g_k$ is a generator of G (or its inverse), can be satisfied when the cosets are ordered as derived in the coset enumeration outlined above.

Proof: Consider the way in which the coset table is built up: a new coset is introduced only when the result of pre- or post-multiplying an adjacent coset by a generator or its inverse is not already in the coset table. The new coset ($\neq 1$) will be defined later than any previously defined coset so $i > j$, if necessary by inverting the generator $g_k$. The effect of coset collapse during the enumeration can only reduce the index of those cosets appearing adjacent to the new one.

Let $\varphi_i$ denote a coset representative for $Hx_i$. Choose $\varphi_1$ to be the identity and define inductively $\varphi_i = \varphi_j g_k^{-1}$ where $i > j$ and $Hx_i g_k = Hx_j$. Thus all the coset represent-

atives of H in G can be constructed.

Each element of G is represented as a product of two elements - one taken from H and the other from the set of coset representatives. These may be stored as ordered pairs of integers. Let the elements of H be ordered by the process of generation then (i,j) represents the element $h_i\varphi_j$ of G. This effects a large saving in the storage requirements to hold the group at the expense of a single multiplication of elements to generate each element of G. Further storage savings can be made if coset enumeration can be applied to H. More generally, it is necessary to obtain a chain of subgroups $G(=H_0) \supset H_1 \supset H_2 \supset \ldots \supset H_s$ such that the cosets of $H_i$ in $H_{i-1}$, $i = 1,2,\ldots,s$, can be enumerated and $H_s$ can be generated. Common candidates for $H_s$ are the identity and the cyclic groups. $H_s$ can be chosen to be any group for which a canonical word for each element is known.

The linear fractional groups PSL(2,p)

The linear fractional group PSL(2,p) of order $\frac{1}{2}p(p^2-1)$ of 2 x 2 matrices over a Galois field of p (an odd prime) elements is such a group. It is isomorphic to the group of transformations

$$z' \leftarrow \frac{az+b}{cz+d} \quad \text{with } a,b,c,d \in GF(p) \text{ and } ad-bc = 1.$$

It is generated by $\alpha,\beta$ and $\gamma$ where $\alpha$: $z \leftarrow z+1$,

$\beta$: $z \leftarrow \mu^2 z$ and $\gamma$: $z \leftarrow -z^{-1}$, and $\mu$ is a primitive element of GF(p), in terms of which there are $\frac{1}{2}p(p-1)$ elements of the form $\alpha^i\beta^j$ and $\frac{1}{2}p^2(p-1)$ elements of the form $\alpha^i\beta^j\gamma\alpha^k$. Note that it is in general necessary to have a representation-independent method for generating $H_s$ or to be able to extend the representation of $H_s$ to a representation of each of the subgroups in the chain and eventually to G itself.

To use the above method in its full generality, a solution to the following problem is needed:
Let $H_i$ be defined by the relations $R_{i,j}(g_1,g_2,\ldots,g_n) = 1$. By what relations in $g_1,g_2,\ldots,g_n$ is $H_{i+1}$ defined? Mendelsohn [ M9 ] has contributed a solution to this general problem. Fortunately it is frequently possible to generate G by using knowledge of G without having a general solution. In particular since a simple group has no proper non-trivial homomorphic images any non-trivial set of generators satisfying a set of relations for a simple group must generate that group.

The Hall-Janko group of order 604,800

Let G be the Hall-Janko simple group of order 604,800. It has been given by M. Hall as the group generated by three permutations on 00 to 99:

a = (00)(01)(02 03 04 05 06 07 08)(09 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 64)(65 66 67 68 69 70 71)
(72 73 74 75 76 77 78)(79 80 81 82 83 84 85)
(86 87 88 89 90 91 92)(93 94 95 96 97 98 99)

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 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).

The stabiliser of 00 is <a,b> and is isomorphic to $SU(3,3^2)$. G is a rank 3 group on the 100 cosets of $SU(3,3^2)$ and the three sub-orbits (transitive constituents) are of lengths 1, 36 and 63. The coset representatives of $SU(3,3^2)$

in G are the 100 permutations taking 00 to i, i = 00,01, ...,99. Similarly, thoseof PSL(2,7) in $SU(3,3^2)$ are found to be the 36 elements 1 and $b^i a^j$, i = 1,2,3,4,6, and j = 0, 1,...,6. Coset 26 is fixed by $x = b^4$ and $y^{-1} = ab^3$ which satisfy $x^2 = y^7 = (xy)^3 = [x,y]^4 = 1$ which are known to be relations for the simple group PSL(2,7). Since PSL(2,7) is simple, $\langle x,y \rangle$ = PSL(2,7). It is further found that $\langle x,u \rangle = S_4$ where $x^2 = (xu)^3 = u^4 = 1$ and $u = yxy^3$. Here it is necessary to show that x and u do not generate a factor group of $S_4$. It is found by coset enumeration that $[\langle x,y \rangle : \langle x,u \rangle] = 7$ so $\langle x,u \rangle = S_4$. A chain of subgroups for G is

$$G \supset SU(3,3^2) \supset PSL(2,7) \supset S_4 \supset C_4$$

index 100 36 7 6

where $C_4 = \langle u \rangle$.

The full chain is not used. The elements of PSL(2,7) are generated from their canonical form and then multiplied by coset representatives to give $SU(3,3^2)$ and then by the coset representatives of $SU(3,3^2)$ in G to give the full group.

Generation of a group using a chain of s subgroups such that $[H_{i-1} : H_i] = n_i$, i = 1,2,...,s requires a nested set of s loops of which the outer most has length $n_s$ and the inner-most has length $n_1$. The total number of multiplications is $n_1 n_2 \ldots n_s + n_2 n_3 \ldots n_s + \ldots + n_{s-1} n_s + n_s$. The order of G is $n_1 n_2 n_3 \ldots n_s$ and so the average number of multiplications per element of G is

$$1 + (n_1)^{-1} + (n_1n_2)^{-1} + \ldots + (n_1n_2\ldots n_s)^{-1}.$$

The index $n_1 = [G:H_1]$ of the largest proper subgroup in the chain is the important factor in estimating computing time and it should be as large as possible. For the above group generated from the canonical elements of PSL(2,7) it is necessary to store only 3 + 36 + 100 group elements, using only 139 x 100 = 13,900 words of store. It takes 80 minutes to generate G on the Atlas computer.

The Janko group of order 175,560

The simple group of order 175,560 described by Janko [ J2 ] in 1966 is generated by the following method. The computation was carried out on an English Electric KDF9 computer with 16K words of fast store of which 4K were used to contain the program.

Two facts concerning $J_1$ both of which are due to G. Higman are used:

(1) - The definition of $J_1$ in terms of the canonical generators a, b and c of PSL(2,11) and the involution d is

$$J_1 = \langle a,b,c,d \rangle$$

where

$$a^2 = (ab)^2 = b^5 = 1,$$
$$b^{-1}cbc^2 = (ac)^3 = c^{11} = 1,$$
$$d^2 = dbdb^{-1}(cd)^2 = (ad)^6 = (ac^2d)^5 = 1.$$

The subgroup PSL(2,11) of order 660 is generated directly in terms of its natural projective representation over a

centre of order 2 as a group of 2 x 2 matrices of unit determinant and entries over GF(11) with its centre factored out, i.e. each matrix is identified with its negative.

(2) - A symmetric tensor representation of degree 7 faithful on PSL(2,11) is derived from this representation. The derived representation extends to a representation of $J_1$.

The extension is made by taking the transformations $x \leftarrow ax+by$ and $y \leftarrow cx+dy$ to act in the space of homogeneous polynomials of degree 6 in x and y. In this space $x^{6-r}y^r \leftarrow (ax+by)^{6-r}(cx+dy)^r$, $r = 0,1,\ldots,6$.

By choosing matrices of simple form for $a,c \in PSL(2,11)$ correspondingly simple forms for $b = c^4ac^3ac^4a$ and d are found.

The matrices $\begin{bmatrix} 0 & 1 \\ 10 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ are chosen to represent a and c in the natural representation of PSL(2,11). Since $b = c^4ac^3ac^4a$, the matrix $\begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}$ is derived as the representation of b. In the tensor representation these extend to

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 10 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

$$C = \begin{matrix} 1 & 6 & 4 & 9 & 4 & 6 & 1 \\ 0 & 1 & 5 & 10 & 10 & 5 & 1 \\ 0 & 0 & 1 & 4 & 6 & 4 & 1 \\ 0 & 0 & 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

where capitals indicate the representing matrices for the corresponding small letter elements of $J_1$. The representing matrix for d is computed using the relation that b commutes with d so $D_{ij} = 0$ unless $i = j$ or $B_{ii} = B_{jj}$ $(i \neq j)$. This simplifies the form of D to that of a diagonal matrix augmented by possible non-zero entries in the (1,6), (6,1), (2,7) and (7,2) positions. It is noted that $C^{-1}$ has entries $(-1)^{j-i}C_{ij}$. The matrices CD and $DC^{-1}$ are compared and from the first row and entries (2,2) and (3,7) the form of D is derived as

$$D = \begin{matrix} x & 0 & 0 & 0 & 0 & -6w & 0 \\ 0 & -x & 0 & 0 & 0 & 0 & w \\ 0 & 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -x & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x \end{matrix}$$

but $d^2 = 1$ hence $x = \pm 1$. By comparison of $(AD)^3$ with $(AD)^{-3} = (DA)^3$, it is found from the (2,1) entry on each side that $-wx^2 = 2w^3$. Hence $w = 0$ or $2w^2 = -1$ yielding $w = 0$, 4 or 7. Finally, the unique solution $w = 7$ and

$x = -1$ is obtained from the relation $(AC^2D)^5 = 1$. It is thus shown that Janko's group has a modular representation of degree 7 over GF(11).

The above matrix computations were performed with an on-line program for matrix multiplication for use on a console to a PDP8 computer.

The cosets of PSL(2,11) in $J_1$ are enumerated from the presentation given. A set of 660 coset representatives of the centre of SL(2,11) in SL(2,11) is stored as 2 x 2 matrices. The 266 coset representatives of PSL(2,11) are stored as 7 x 7 matrices, one third of which is kept in the fast store at any one time. Each 7 x 7 matrix representing an element of PSL(2,11) is generated from the parameters a, b, c, d of a 2 x 2 matrix and then multiplied by those of the 266 coset representatives which are in the fast store.

# Chapter 4

## Generation of the conjugacy classes

Determination of the conjugacy classes of a group is a critical step in computing its character table whatever method is used. It appears necessary to be able to generate a conjugacy class element by element and to know to which class a given element belongs.

Definition: The centralizer of $x \varepsilon G$ is the set $Z(x) = \{z \mid zx = xz,\ z \varepsilon G\}$.

### Computing the centralizer of an element

For many groups it is feasible to pick a set of elements generating non-conjugate cyclic subgroups and to generate the group element by element and count the number of elements of G commuting with each representative element. An alternative method which gives a set of generators for Z(x) when the group is given in terms of generators and relations is as follows.

Let $Z_i$ be the subgroup of G generated by the words $w_o(=x), w_1, \ldots, w_i$, where $w_j$ $(j \leq i)$ is a non-trivial coset representative in G of $Z_{j-1}$ which commutes with x. For sufficiently large i no non-trivial coset representatives of $Z_i$ commute with x, thus $Z_i = Z(x)$. The computation of Z(x) is done by repeated coset enumeration on the cosets of

successive $Z_j$. The method can often be used even though the index of $\langle x \rangle$ in G is too large for coset enumeration. Cosets are enumerated until the store is full and an examination is made on the coset representatives suggested by the incomplete enumeration. Even though these may actually not be coset representatives, they prove a good source for elements commuting with x (provided that $\langle x \rangle \neq Z(x)$).

Generating the conjugacy classes

From the above, the class containing x consists of the conjugates of x by the coset representatives of Z(x). For small groups it has been found faster to generate the whole group by enumerating the cosets of the identity and forming the elements as faithful permutations. The cycle structure of each permutation is found and the permutations are then sorted according to their cycle structure. This is done by mapping the partitions of the degree of the permutations into the integers and then sorting on the integers as keys [ M4 ]. The conjugacy class of x is found by conjugating x by successive elements y of G and counting the number n of distinct elements $x^y$ and the maximum number m of times any single element has been formed: n and m are bounded by the order of the class containing x and $|Z(x)|$ respectively. The conjugacy class is complete when $nm = g$. The order of the class is then found as follows.

Let $\{f_i\}$ be the ordered set of increasing factors of g and let m′ and n′ be the current incomplete values of m and n respectively. If $f_{i-1} < m' \leq f_i$ and $f_{j-1} < n' \leq f_j$ for some i and j and $f_i \cdot f_j = g$, then $m = f_i$ and $n = f_j$. Let n′ be the number of elements known to be conjugate to x out of a set of S(x) possible candidates and let $f_{k-1} < n' \leq f_k < S(x) < f_{k+1}$, then $n = f_k$.

Let x be of period n, which may be computed as the l.c.m. of the cycle lengths for the permutation representing x and let (k,n) = 1 then

Lemma: The set of elements $x^k$ forms a complete conjugacy class with the same cycle type as that of x.

Proof: Denoting conjugacy by $\sim$, $x_1 \sim x_2$ implies $x_1^k \sim x_2^k$ and $x_1^k \sim x_2^k$ implies $x_1^{ak+bn} \sim x_2^{ak+bn}$ and a and b may be chosen so that ak+bn = 1 because (k,n) = 1. Now a power of x, if of different cycle type from x, will have more cycles but there is an a such that $(x^k)^a = x$ so the cycle types of x and $x^k$ are the same.

There are $\varphi(n)$ such values k. A check is made to see whether $x^{-1} \varepsilon C_x$ and if so, then the $[\varphi(n)/2]$ values are checked since $x^k$ and $x^{-k}$ belong to the same class; if not, then each of the values of k is checked.

## Computing the class of a given element

Besides computing classes, it is necessary to find an

easily computable function on the representation of the elements which characterizes the classes. More precisely,

Definition: A function f on G is a class function if $f(x) = f(y^{-1}xy)$ for all $x,y \in G$.

A class function induces a partition of the elements of G into equivalence classes. An easily computable function f, such that the equivalence classes induced by f are the conjugacy classes of G, is needed. There appear to be two possibilities.

A local property of a representation of x such as the trace, cycle structure, or even the number of cycles, may be used. There are several groups with representations for which local properties determining conjugacy are well-known. For example, two elements of the symmetric group on n symbols are conjugate if and only if the cycle structures of their natural permutation representations coincide; the general linear group GL(n,q) presents no difficulties since elements are conjugate if and only if they are similar in their natural matrix representations. Care must be taken in the case of modular representations because unlike ordinary representations the matrices representing elements are not necessarily diagonalizable. For example, the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ with entries in GF(p) have the same characteristic equations but are clearly not conjugate.

An alternative to the above is to search the conjugacy classes for the element whose class is required. The function then consists of a subroutine.

A combination of both approaches is useful: local properties are found to restrict the choice of possible classes then a search is made on these classes. The critical factor in computing the class of an element is the speed with which it can be done. The fastest method may use invariants from more than one representation.

Examples

In Janko's group of order 175,560 the traces of the representation of degree 7 characterize 7 classes and the first two coefficients of the characteristic polynomial distinguish a further 6 classes. The remaining two classes include the identity and so may be separated by inspection. The trace of the square of the matrix is computed instead of the second coefficient of the characteristic polynomial.

In the Hall-Janko group of order 604,800 the cyclic subgroups of each order are conjugate except for two classes of subgroups of order 5. One of these is distinguished by being centralized by an element of period 3. When an element of period 5 is generated it is necessary to check whether it commutes with an element of period 3.

## The rational conjugacy classes

The determination of the classes is the most difficult part of a program for computing group structure, in particular the character table of a group. This problem cannot be said to have been solved for larger groups. The reason for this is the difficulty in distinguishing between elements in distinct classes which generate the same conjugacy class of cyclic subgroups. To this end it is useful to introduce the rational conjugacy classes .

Definition: The rational conjugacy classes of G are the sets of those elements which generate conjugate cyclic subgroups.

In particular, x and $x^k$ are rationally conjugate elements whenever $(k, |\langle x \rangle|) = 1$.

The utility of rational classes is that frequently they are distinguished in permutation representations by the cycle types of elements in them. They are discussed further in connection with the class algebra.

# Chapter 5

## Construction of the normal subgroup lattice

The normal subgroup lattice of G is constructed from the class structure constants. The construction requires that the lattice satisfies the Jordan-Dedekind chain condition. To explain this some definitions are first given.

Definition: The least upper bound of X and Y, $X \lhd G$, $Y \lhd G$, is the complex $XY = \{xy \mid x \in X, y \in Y\}$ which is normal in G.

Definition: The greatest lower bound of X and Y, $X \lhd G$, $Y \lhd G$, is the set-theoretic intersection $X \cap Y$ which is also seen to be normal in G.

Definition: A basic normal subgroup $B_i$, $i = 1,2,\ldots,r$, is the normal closure of an element $x_i \in C_i$, that is, $B_i = \langle C_i \rangle$, $i = 1,2,\ldots,r$.

It may be that $B_i = G$ as will be the case, for example, for all non-trivial basic normal subgroups when G is simple. Since normal subgroups are unions of conjugacy classes of G, the set of basic normal subgroups will contain amongst its members the minimal normal subgroups of G.

Definition: A chain is a partially ordered set S of elements such that either $x \geq y$ or $y \geq x$ for all $x,y \in S$.

Definition: A maximal chain between x and y is a chain $x = x_0 > x_1 > \ldots > x_m = y$ where $x > y$ means that $x \geq a \geq y$

implies that $a = x$ or $a = y$. The length of the chain is m.

Definition: The Jordan-Dedekind chain condition states that all maximal chains between two elements have the same length.

Definition: A principal series is a maximal chain of subgroups of G: $G = H_0 \rhd H_1 \rhd \ldots \rhd H_m$ such that $H_i \lhd G$, $i = 1,2,\ldots,m$.

A better-known stronger result, which implies the Jordan-Dedekind chain condition, is contained in the Jordan-Hölder theorem, which states in part that all principal series for G have the same length (for a proof see [ C5 ]).

Definition: The level of a normal subgroup N is the length of a maximal chain N to I.

The normal subgroup lattice is built up level by level, the existence of each level being guaranteed by the Jordan-Dedekind chain condition. The number of levels is the number of terms in a principal series for G.

Lemma: A normal subgroup of level n+1 is either a basic normal subgroup or is the product of two normal subgroups of level n.

Proof: What has to be shown is that a normal subgroup of level n+1 which is not basic can be expressed as a product of two level n normal subgroups, for the Jordan-Dedekind chain condition ensures that it is the product of level n normal subgroups. Let the level n+1 normal subgroup be $N = N_1N_2\ldots N_k$ where the $N_i$, $i = 1,2,\ldots,k$ are level n normal subgroups. The normal subgroup $N_iN_j$, $i \neq j = 1,2,$

...,k, is contained in N but $N_iN_j$ is a level n+1 normal subgroup hence $N = N_iN_j$, $i \neq j = 1,2,\ldots,k$.

Computing the normal subgroup lattice

The basic normal subgroups are computed from the rational class algebra by forming the union of successive powers of a single rational conjugacy class until the union becomes closed under multiplication by that class (or until the number of elements in the union is greater than $\frac{1}{2}g$). It is necessary to know only whether the class structure constants are zero or not.

The computation follows the inductive scheme:

let $n_i \lhd G$,

$M_i = \{n_{i1}, n_{i2}, \cdots, n_{it}\}$;

$n_{ij} \varepsilon E_{i+1}$ if and only if $n_{ij} \supset n_{ik}$ for some k,

otherwise $n_{ij} \varepsilon L_i$;

$M_{i+1} = \{n_{ij}n_{ik} \mid n_{ij}, n_{ik} \varepsilon L_i,\ j < k\} \cup E_{i+1}$.

To start take $M_1 = \{B_2, B_3, \cdots, B_r\}$ and proceed until $M_s = \{G\}$.

The complex $n_in_j = n_jn_i$, where $n_i$ contains not more conjugacy classes than $n_j$, is computed by forming the set-theoretic union of the classes of $n_i$ and $n_j$ then forming the closure under multiplication by each of the classes in $n_i$ and $n_j$, or until the order of the set is larger than

$\frac{1}{2}|G|$ in which case it is the full group by Lagrange's theorem.

The normal subgroups are output as sets of conjugacy classes.

# Chapter 6

## Construction of the centre of the group algebra

The class algebra is determined by the structure constants $a_{ijk}$ where

$$c_i c_j = \sum_{k=1}^{r} a_{ijk} c_k, \quad i,j = 1,2,\ldots,r. \qquad (6.1)$$

A method for computing these constants is described here.

The constant $a_{ijk}$ is seen to be the number of ways a fixed element $z \varepsilon C_k$ can be written as a product xy of elements $x \varepsilon C_i$ and $y \varepsilon C_j$. Taking conjugates shows that $a_{ijk}$ is independent of which $z \varepsilon C_k$ is chosen.

Theorem The structure constants satisfy twelve basic symmetries.

Proof Consider the ordered triples (x,y,z), $x \varepsilon C_i$, $y \varepsilon C_j$ and $z \varepsilon C_k$ such that xyz = 1 or rearranging, such that $xy = z^{-1}$. This number is $a_{ijk}, h_k$, but classes commute so the suffixes i,j, and k may be permuted. Further, the number of triples such that xyz = 1 is also the number such that $z^{-1}y^{-1}x^{-1} = 1$ hence the three classes can also be simultaneously inverted giving an invariance group of order 12 acting on the structure constants.

Let $r_j$ be a representative element of $C_j$ and compute

$b_{ijk}$ as the number of products $xr_j \varepsilon C_k$. Then $b_{ijk}$ is the number of solutions of $x^{-1}z = r_j$ with $x\varepsilon C_i$, $z\varepsilon C_k$ but this is $a_{i'kj}$, hence $b_{ijk} = a_{i'kj}$. The number of products that it is necessary to compute to determine the $r^2$ integers $a_{ijk}$ for fixed i is not greater than $r|C_i| = rh_i$.

It is necessary to compute only those $a_{ijk}$ for which $j \geq i$ since $a_{ijk} = a_{jik}$. Suppose that $h_i$, $i = 1,2,\ldots,r$ are known then by suitable ordering of the class representatives the amount of computation needed can be minimised. To compute the $a_{ijk}$ it is necessary to compute $xr_j$, $x\varepsilon C_i$, for $j \geq i$.

Using this procedure, and assuming x runs through G, it is found that the number of products to be computed to determine all $a_{ijk}$ is a minimum when the representatives $y_j \varepsilon C_j$ are chosen so that $h_j \leq h_{j+1}$, $j = 1,2,\ldots,r-1$. The number of products in computing $C_i y_j$ is $h_i(r-j+1)$, so the total number is $\sum_{i \leq j} h_i(r-j+1)$. To minimise this sum the following theorem is needed.

Theorem: Let $p_1 > p_2 > \ldots > p_r > 0$ and let $0 < h_1 \leq h_2 \leq \ldots \leq h_r$ be sets of integers then $\sum_{i=1}^{r} h_i p_{t_i}$ (where $t_i$, $i = 1,2,\ldots,r$, is a permutation of $1,2,\ldots,r$) attains its minimum when $t_i = i$.

Proof: Suppose that the minimum is attained by $\sum_i h_i p_{t_i}$

where $t_k \neq k$ and $t_s = s$ for all $s > k$. Then $p_{t_k} < p_k$ and $p_k = p_t$ for some $i > k$. Interchanging $p_{t_k}$ and $p_k$ decreases the supposed minimum by $(p_{t_k}-p_k)(h_k-h_i) \geq 0$ which is a contradiction unless $h_k = h_i$ which gives the same valued minimum.

Taking $p_i = r-i+1$, $i = 1,2,\ldots,r$, it is necessary to compute $\sum_{i=1}^{r} h_i(r-i+1)$ products where $h_i \leq h_{i+1}$, $i = 1,2,\ldots,r-1$, in order to be able to compute all the $a_{ijk}$. A further minor improvement is obtained by noting that $\sum_j a_{ijk} = h_i$ since $\sum_j a_{ijk}$ is the number of ordered pairs of solutions $(x,y)$ to $xy = z$ where $x \varepsilon C_i$, $y \varepsilon G$, and $z \varepsilon C_k$ is a fixed element. With this improvement the number of products to be computed is reduced to $\sum_{i=1}^{r} h_i(r-i)$.

The above approach is useful when the classes of G cannot be generated one at a time and it is necessary to generate all the group, multiplying each element by class representatives.

For each distinct (i.e. not multiple) eigenvalue of $A^{(i)}$ the corresponding eigenvector of $A^{(i)}$ is uniquely determined (to within a non-zero scalar factor). When classes are generated one at a time this fact is used. The eigenvalues of $A^{(i)}$ are computed and if there are no repeated eigenvalues then the eigenvectors are found, else a new matrix $A^{(j)}$ is computed and the eigenvalues of

$\eta_i A^{(i)} + \eta_j A^{(j)}$ are found where $\{\eta_i\}$ is a set of random real numbers. New matrices are computed until $\sum_{i=1}^{k} \eta_i A^{(i)}$ has distinct eigenvalues. The eigenvectors are then computed. It is noted that only one of the class matrices corresponding to the classes of x and $x^k$, $(k,g) = 1$, is needed since the eigenvalues of these matrices are algebraic conjugates. When the available class functions are insufficient to separate the classes of G, as happens with permutation representations it may be convenient to compute the rational class algebra.

The rational class algebra

The maps $\varphi_s: x \longrightarrow x^s$, $x \varepsilon G$, $(s,g) = 1$, are 1-1 maps onto the conjugacy classes and so permute the conjugacy classes. Let $K_1 (=C_1)$, $K_2$, ..., $K_t$ to be the sets of transitivity under the maps $\varphi_k$. The $K_i$ are disjoint and any union of conjugacy classes invariant under the $\varphi_s$ is a union of these sets. The $K_i$, $i = 1,2,\ldots,t$ are called the rational classes of G. From the above remarks they form a basis for a subalgebra of the class algebra called the rational class algebra.

Theorem: If

$$K_u K_v = \sum_{w=1}^{t} d_{uvw} K_w \qquad (6.2)$$

then

$$d_{uvw} = \sum_{i,j} a_{ijk}, \quad c_k \varepsilon K_w \qquad (6.3)$$

with summation over all i,j such that $c_i \varepsilon K_u$, $c_j \varepsilon K_v$.

Proof:

$$c_i c_j = \sum_k a_{ijk} c_k$$

$$K_u c_j = \sum_{i,k} a_{ijk} c_k \quad \text{summed over i such that } c_i \varepsilon K_u$$

$$K_u K_v = \sum_{i,j,k} a_{ijk} c_k \quad \text{summed over j such that } c_j \varepsilon K_v$$

The left-hand side, $K_u K_v$, is invariant under the maps $\varphi_s$ therefore so is the right-hand side hence

$$\sum_{i,j} a_{ijk} = \sum_{i,j} a_{ijk^*}$$

if $c_k$ and $c_{k^*}$ lie in the same rational class.

Taking an irreducible representation $R^s$ of both sides of (6.2) and comparing coefficients gives

$$m_{su} m_{sv} = \sum_{w=1}^{t} d_{uvw} m_{sw} \tag{6.4}$$

where

$$m_{su} = \sum_{c_i \varepsilon K_u} m_{si}.$$

As before, this is a commutative associative algebra and the eigenvalues and eigenvectors can be computed.

In conclusion, this method of computing the character table by computing the rational class algebra is practical for groups having representations such that:

(1) rational class representatives can be found, and

(2) the rational class map can be computed.

These requirements are weaker than those needed for computation of the class algebra.

It is possible for groups to have isomorphic rational class algebras but distinct class algebras. This occurs with the two groups of order 16 designated by $F_3a_1$ and $F_3a_2$ in [ H2 ].

# Chapter 7

## Numerical Techniques

In practice, rather than use the basic matrix equations

$$A^i \underline{x} = \mu_i \underline{x}, \qquad i = 1,2,\ldots,r \tag{7.1}$$

derived from the class equations

$$c_i c_j = \sum_k a_{ijk} c_k, \qquad i,j = 1,2,\ldots,r \tag{7.2}$$

it is convenient for reasons of numerical accuracy to compute a set of orthogonal eigenvectors. To do this, $m_{si}$ is replaced by $w_{si} = m_{si}/h_i^{\frac{1}{2}}$ to obtain from (7.2)

$$h_i^{\frac{1}{2}} w_{si} h_j^{\frac{1}{2}} w_{sj} = \sum_{k=1}^{r} a_{ijk} h_k^{\frac{1}{2}} w_{sk}, \qquad i,j,s = 1,2,\ldots,r \tag{7.3}$$

and so

$$w_{si} w_{sj} = \sum_{k=1}^{r} e_{ijk} w_{sk}, \qquad i,j,s = 1,2,\ldots,r \tag{7.4}$$

where

$$e_{ijk} = \left(\frac{h_k}{h_i h_j}\right)^{\frac{1}{2}} a_{ijk}. \tag{7.5}$$

The eigenvectors $\underline{w}^s$, $s = 1,2,\ldots,r$ of the matrix equations

$$E^i \underline{x} = \eta_i \underline{x} \qquad i = 1,2,\ldots,r \tag{7.6}$$

where $[E^i]_{jk} = e_{ijk}$, are orthogonal since

$$\underline{w}^s \cdot \bar{\underline{w}}^t = g\delta_{st}/(d_s \cdot d_t), \qquad s,t = 1,2,\ldots,r \tag{7.7}$$

from the row orthogonality relations.

The degree $d_s$ is computed from the normalized ($w_{s1} = 1$) eigenvectors as

$$d_s = \frac{g}{\underline{w}^s \cdot \underline{w}^s} \tag{7.8}$$

The use of orthogonal eigenvectors gives an accuracy of more than six decimal places to the values of the characters of the groups computed. Using the original matrix equations (7.1) there were occasions when eigenvectors were computed inaccurately. On examination it was seen that this occurred when there were two real eigenvectors which differed from each other in only two components.

The eigenvalue of the matrix $B = \sum_i \alpha_i E^i$ corresponding to the normalized eigenvector $\underline{w}_s$ is $\sum_i \alpha_i w_{si}$. For distinct eigenvalues it is necessary that

$$\sum_i \alpha_i w_{si} \neq \sum_i \alpha_i w_{ti}, \qquad s \neq t \tag{7.9}$$

that is,

$$\underline{\alpha} \cdot (\underline{w}_s - \underline{w}_t) \neq 0, \qquad s \neq t \tag{7.10}$$

The random variables $\alpha_i$ are chosen from a uniform distribution in [0,1]. An unsuccessful attempt has been made at an error analysis of the equations

$$|\underline{\alpha} \cdot (\underline{w}_s - \underline{w}_t)| > \varepsilon, \quad s \neq t, \qquad s,t = 1,2,\ldots,r \tag{7.11}$$

where $\varepsilon$ is a constant dependent on the word-length of the

computer.

The set of r-tuples $\{\alpha_i\}$ for which (7.10) does not hold has measure zero in the set of all r-tuples $\{x_i\}$, $0 \leq x_i \leq 1$, $i = 1,2,\ldots,r$. This in itself is not of rigorous practical interest when computing, as, for example only finitely many numbers can be represented exactly in a computer. More importantly, there have been no coincidental eigenvalues deriving from an unfortunate choice of the $\{\alpha_i\}$. This has been borne out by several hundred computations with many groups.

The program used for computing eigenvalues is Head's [ H8 ] Atlas Autocode version of Francis' [ F3 ] QR algorithm. The basic algorithm is given by the scheme

$$A_i = Q_i R_i, \quad A_{i+1} = Q_i^* A_i Q_i = Q_i^* Q_i R_i Q_i = R_i Q_i \qquad (7.12)$$

where $^*$ denotes complex conjugate transpose, $Q_i$ is a unitary matrix, and $R_i$ is upper triangular with real positive elements on the diagonal.

Before using the QR algorithm the matrix is reduced to upper Hessenberg form by elementary transformations using dirhesse [ M1 ].

Inverse iteration is used to compute the eigenvectors. The iteration scheme is

$$\begin{aligned} LU\underline{x}_{i+1} &= \underline{y}_i \\ \underline{y}_{i+1} &= \underline{x}_{i+1} / \| \underline{x}_{i+1} \|_\infty \end{aligned} \qquad (7.13)$$

where LU is a decomposition of $A-\mu_o I$, L is lower triangular with unit diagonal and U is upper triangular. The approximation $\mu_o$ to the eigenvalue $\mu$ of A is calculated by the QR algorithm. Iteration starts with the components of the initial vector $\underline{y}_o$ all unityand continues until $\| \underline{x}_{i+1} \|_\infty > 10^{10}/(100r)$ then one more step is performed.

Danilevski's method for the characteristic polynomial

This method is used for obtaining the characteristic polynomial of a matrix and takes $O(n^3)$ operations.

Let A be an n x n matrix. Suppose $a_{n,n-1} \neq 0$. Row n is reduced to zero except in column (n-1) where it is 1, by post-multiplying by the matrix $M_{n-1}$ which is the identity matrix $I_n$ with the (n-1,j) entry replaced by $-a_{nj}/a_{n,n-1}$, $j \neq n-1$, and $1/a_{n,n-1}$ for $j = n-1$. The matrix $M_{n-1}^{-1}$ is found to be the identity with row (n-1) replaced by row n of the matrix A. The method consists of the iteration

$$A_{k-1} = M_{k-1}^{-1} A_k M_{k-1}, \quad k = n, n-1, \ldots, 1 \qquad (7.14)$$

with $A_n = A$. The final matrix $A_1$ is in the form of the companion matrix:

$$\begin{matrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 \end{matrix} \qquad (7.15)$$

It has been assumed throughout that at the application of $M_{k-1}$, $a_{k,k-1} \neq 0$; if this is not so at any stage then, provided that $a_{k,j} \neq 0$ for some $j < k-1$, columns $(k-1)$ and $j$ and rows $(k-1)$ and $j$ are interchanged to make $a_{k,k-1} \neq 0$. A further possibility arises if $a_{k,j} = 0$ for all $j < k$. If so, then A has been reduced to the form

$$A = \begin{array}{c|c} X & Y \\ \hline 0 & B \end{array} . \qquad (7.16)$$

Now $P(A) = P(X) \cdot P(B)$, where $P(A)$ is the characteristic polynomial of A, so that the characteristic polynomial of A can be computed from those of X and B without reference to Y.

It seems that it should be possible to modify this method to obtain the rational canonical form of a matrix but attempts to do this have not so far been successful. Danilevski's method has not received much attention by numerical analysts as it is numerically unstable [ W1 ]. When working over finite fields, however, the computation is exact and instability is no problem.

Computing with finite fields

To do arithmetic in a finite field of $q = p^n$ elements on a computer the fastest method seems to be to use a table look-up for multiplication and addition although if multiplicative notation is used only the addition table is

needed. This occupies $q^2$ words of store which may be impractical for large q. An alternative is to represent the powers $x^i$ of a primitive element x of GF(q) by i and to store the elements $x^j = 1 + x^i$. A special convention is used for zero. For GF(q) this uses only q words of store. Multiplication is given by

$$x^i x^j = x^{i+j}, \qquad (7.17)$$

addition by

$$x^i + x^j = x^i(1+x^{j-i}), \quad i \leq j, \qquad (7.18)$$

and subtraction by

$$x^i - x^j = x^i + x^{j+\frac{1}{2}(q-1)} \qquad (7.19)$$

(in a field of odd characteristic). Irreducible polynomials defining GF(q) as an extension of GF(p) are given, for example in Dickson [ $D_1$ ]. The table of values of $1+x^i$ is worked out by hand.

Computational linear algebra over finite fields is distinguished from linear algebra over the complex field or the reals in several respects. There are no problems of stability since computation is exact. Any direct methods using only rational operations in the field can be mimicked for finite fields. Root extraction in the finite case may require a field extension. Since the field is a finite set there is no concept in finite fields corresponding to that of convergence so iterative techniques cannot be applied. Trial and error methods may be efficient and can be used,

for example, to find the roots of a polynomial by searching for zeros in successive extension fields.

# Chapter 8

## Subgroups and permutation characters

### Checking the character table

It has been found necessary to check character tables for consistency before using them as data for programs. Two tests are used: checks of orthogonality and checks of compatibility with the class algebra. The orthogonality test is carried out first and if satisfactory is followed by the compatibility tests. Tables can be orthogonal but inconsistent with the class algebra.

To check the character table the orthogonality relations are used in the form

$$U^*U = UU^* = I \qquad (8.1)$$

where $[U]_{ij} = u_{ij} = (h_j/g)^{\frac{1}{2}}\chi_{ij}$ and * denotes complex conjugate transpose. It is convenient to work with unitary matrices to avoid unnecessary difficulties with overflow.

A single orthogonality error in entry (i,j) of the character table shows up in the row orthogonality matrix UU* which will differ from I in row i and column i. Similarly, the column orthogonality matrix U*U will differ from I in row j and column j. When there are several orthogonality errors, the pattern of zeros in the incorrect rows and columns is a guide to the position of the errors.

If the (i,j) character entry is in error then the column positions of the zeros in row i of the row orthogonality matrix indicate the zero entries in column j of the character table. If it is assumed that i is known then j can often be found. A similar property holds for the column orthogonality matrix. This program was used to correct the character table of Lyons' possible new simple group.

It is of interest to see why the original orthogonal character table for Janko's simple group of order 50,232,960 failed to give the correct value for a certain structure constant. In the group there are three classes of elements of period 9; their characters differ only on three representations of degree 1920. The incorrect portion of the table is given as

| | $9_1$ | $9_2$ | $9_3$ | | | $9_1$ | $9_2$ | $9_3$ |
|---|---|---|---|---|---|---|---|---|
| 1920 | 3 | -3 | 0 | | 1920 | $\varphi_1$ | $\varphi_2$ | $\varphi_3$ |
| 1920 | -3 | 0 | 3 | instead of | 1920 | $\varphi_2$ | $\varphi_3$ | $\varphi_1$ |
| 1920 | 0 | 3 | -3 | | 1920 | $\varphi_3$ | $\varphi_1$ | $\varphi_2$ |

where $\varphi_i = -\varepsilon^{2.4^i} + \varepsilon^{4.4^i} + \varepsilon^{5.4^i} - \varepsilon^{7.4^i}$ and $\varepsilon^9 = 1$.

In the first instance the entries are the roots of $x^3-9x = 0$ whereas in the second they are the roots of $x^3-9x-9 = 0$. The symmetric polynomials of degree two or less in $x_1$, $x_2$ and $x_3$ take the same values in both cases so the two sets of entries have the same orthogonality properties. Comput-

ation of the structure constants $a_{ijk}$ involves a cubic expression in the characters and in particular the constant $a_{9_1 9_2 9_3}$ involves the product of $\varphi_1$, $\varphi_2$ and $\varphi_3$ and this gives differing answers in the two cases.

An independent check to the orthogonality check is to compute the structure constants $a_{ijk}$ of the class algebra

$$c_i c_j = \sum_{k=1} a_{ijk} c_k, \quad i,j = 1,2,\ldots,r \tag{8.2}$$

by means of the equations

$$a_{ijk} = \left(\frac{g h_i h_j}{h_k}\right)^{\frac{1}{2}} \sum_{s=1}^{r} \frac{u_{si} u_{sj} \bar{u}_{sk}}{d_s} \tag{8.3}$$

for $i,j,k = 1,2,\ldots,r$.

The structure constants are non-negative rational integers and satisfy the matrix equations

$$A^{(i)} \underline{m}^s = m_{si} \underline{m}^s, \quad i,s = 1,2,\ldots,r \tag{8.4}$$

where

$$[A^{(i)}]_{jk} = a_{ijk} \tag{8.5}$$

and

$$\underline{m}^s = (m_{s1}, m_{s2}, \ldots, m_{sr})^t .$$

Theorem: If the abowe checks are satisfied then there is a commutative associative algebra associated with the $a_{ijk}$ as defined by the equations (8.2).

Proof: From (8.4) the $A^{(i)}$, $i = 1,2,\ldots,r$ are diagonalizable by a common set of eigenvectors $\underline{m}^s$ and so commute, i.e.

$$[A^{(i)}A^{(j)}]_{st} = [A^{(j)}A^{(i)}]_{st}, \quad i,j,s,t = 1,2,\ldots,r \tag{8.6}$$

or

$$\sum_{k=1}^{r} a_{isk}a_{jkt} = \sum_{k=1}^{r} a_{jsk}a_{ikt}, \quad i,j,s,t = 1,2,\ldots,r \tag{8.7}$$

but from (8.3)

$$a_{jkt} = a_{kjt} \quad \text{and} \quad a_{jsk} = a_{sjk} \tag{8.8}$$

so

$$\sum_{k=1}^{r} a_{isk}a_{kjt} = \sum_{k=1}^{r} a_{sjk}a_{ikt}, \quad i,j,s,t = 1,2,\ldots,r \tag{8.9}$$

and this is the condition that the algebra with structure constants $a_{ijk}$ is associative. It is commutative by (8.8).

A useful check on character irrationalities is that $\frac{1}{2}(\chi^2(x) \pm \chi(x^2))$ are both values of characters if $\chi(x)$ is. This follows from the decomposition with respect to the general linear group of the Kronecker product of $\chi$ with itself into its symmetric and skew-symmetric parts.

Permutation characters

To each subgroup $H \subset G$ there occurs a transitive permutation character $\varphi$ of G on the cosets of H. Necessary cond-

itions for such a character to exist are given below [ L5 ]. It will be seen that they are most easily tested when [G:H] is small and H is a large subgroup of G.

(a) $\varphi(1)|g$,

(b) $\varphi(x) = 1 + \sum_{i=2}^{r} a_i \chi_i(x)$,

$$0 \leq a_i \leq \min(\chi_i(1), \varphi(1)/\chi_i(1)),$$

(c) $\varphi(x) \geq 0$ is a rational integer,

(d) $h_j\varphi(x)/\varphi(1)$ is a rational integer if $x \varepsilon C_j$,

(e) $\varphi(x^k) \geq \varphi(x)$ for integers $k \geq 0$, and

(f) if $\varphi(x) > 0$ then $(|\langle x \rangle| \cdot \varphi(x))|g$.

The only condition requiring comment is (d). The number of cosets of H fixed by x is $\varphi(x)$, thus $Hx_i x = Hx_i$ for $\varphi(x)$ distinct cosets $Hx_i$. The number n of distinct conjugates of x in H is given by

$$n = \frac{|H|\,\varphi(x)}{|C_G(x)|} = \frac{h_j\varphi(x)}{\varphi(1)}. \qquad (8.10)$$

Techniques for searching for a character $\varphi$ of G with the above properties use the rational representation table of G. Since $\varphi$ assumes only rational integral values, it will contain all algebraic conjugates of an irrational irreducible character with the same multiplicity. Each character is replaced by the sum of its algebraic conjugates. After removing duplicate rows and columns a table is obtained with columns indexed by classes of conjugate cyclic sub-

groups and rows indexed by rationally irreducible representations. Let t be the number of these representations.

(1) A table of factors of g is prepared by generating the factors from the prime decomposition of g and sorting them into increasing order of magnitude. These factors are, by (a), the only candidates for the degree $\varphi(1)$ of $\varphi$. The necessary conditions given for $\varphi$ to be a transitive permutation character may be checked in full generality for increasing values of the degree. In this way an upper bound to the order of any proper subgroup of G and candidates for permutation characters are obtained.

(2) The multiplicities $a_i$ are bounded above by k and all $(k+1)^{t-1}$ choices for suitable $\varphi$ are examined. By taking $k = 1$ the multiplicity-free characters are obtained. Although it is, in general, not true that permutation characters on the cosets of maximal subgroups are multiplicity-free, it appears reasonable to hope for this property to hold for at least one maximal subgroup of a simple group.

(3) A search is made for candidates by the number r of distinct rationally irreducible characters occurring as constituents of $\varphi$. Searching for multiplicity-free characters means examining $\binom{t-1}{r-1}$ characters.

The above methods are all bounded in utility by the time they take. For a group with many (say > 50) large rationally irreducible characters, only the third method

seems feasible. There is a method suggested by S. Lin [ L3 ] which proves useful in computing multiplicity-free characters. This method is bounded not by time but by storage considerations. It consists of constructing a table of t rows and n columns where n is the degree of the largest permutation character being sought. Each entry is either a zero or a one and so can be stored as a bit in the computer. Row i is associated with a rationally irreducible character of degree $d_i$, and $d_i \leq d_{i+1}$, $i = 1,2,\ldots,t-1$. The only non-zero entry in the first row is a 1 in the first column. The other rows are given entries according to the scheme

$$\text{row}_i = \text{row}_{i-1}^{\longrightarrow(d_i - d_{i-1})} \cup \text{row}_{i-1}^{\longrightarrow d_i}, \quad i=2,3,\ldots,t \tag{8.11}$$

where $\longrightarrow$ denotes a shift of k columns to the right. Degrees of the largest constituents of a character of degree j ($\leq$n) will be found from the rows in which there is a 1 in column j. To each constituent there will correspond one or more decompositions. The set of next largest constituent degrees is found from the rows containing 1 in column $j-d_i$ where $d_i$ is the largest constituent, and so on.

If it is assumed that a candidate for the character $\varphi$ has been obtained such that it satisfies (a) to (f), then from (8.10) the distribution in H of the elements of G is found. Sometimes a counting argument will eliminate $\varphi$ at

this stage. If $\varphi(1)$ is sufficiently small one can attempt to construct, by restriction to H, the character table of H. If a faithful representation of G is available an attempt may be made to construct H. This has been done for the simple subgroups PSL(2,p) = 17, 19 of the large Janko group $J_3$ of order 50,232,960 = $2^7 3^5 5 \cdot 17 \cdot 19$ which will be used as an illustration of the method.

# Chapter 9

## The simple group of order 50,232,960 and its subgroups

In 1967 Z. Janko [ J3 ] made the announcements: Let G be a finite non-abelian simple group with the property

(i) that the centralizer of an involution is an extension of an extra-special group of order 32 by SL(2,4),

then either

(ii) all the involutions are conjugate and G is a new simple group of order 50,232,960 = $2^7 3^5 5 \cdot 17 \cdot 19$

or,

(iii) there are two classes of involutions and G is a new simple group of order 604,800 = $2^7 3^3 5^2 7$.

There followed a list of further properties of G and character tables. Nowhere was the existence of G established. The existence and uniqueness of the group of order 604,800 of case(iii) has since been demonstrated by M. Hall and D. Wales [ H3 ].

This chapter is concerned with case (ii). By working from the character table, possible permutation characters

which suggest the existence of certain large subgroups are computed. One of these subgroups is $SL^*(2,16)$, an extension of $SL(2,16)$ by an automorphism of order 2. The existence of this subgroup was assumed by G. Higman who deduced generators and defining relations for G. Coset enumeration yielded a permutation group on the cosets of this subgroup. Subsequently J.G. Thompson has shown that the assumption of existence of the subgroup $SL^*(2,16)$ is justified as it can be deduced from the character table. S.K. Wong [ W2 ] has proved that a simple group of order 50,232,960 necessarily has property (i).

These results, together with the construction given here, prove the uniqueness to within isomorphism of a simple group of order 50,232,960.

The search for the permutation characters

A search is made for possible permutation characters. The group has 14 rationally irreducible characters. It takes six seconds to test the $2^{13}$ multiplicity-free characters. Besides the principal character, there are three characters which appear to be permutation characters of degrees 6156, 19380 and 20520. A further possible permutation character of degree 14688 is found when multiplicity-two is permitted. This computation takes 7 minutes and generates several more characters which either correspond to subgroups known to be present, such as centralizers and

normalizers of elements, or to subgroups of whose presence there is initially some doubt. The possible permutation characters and their values are given here; $\varphi_n$ denotes a character of degree n and is expressed in terms of its irreducible constituent degrees. A prime denotes an algebraic conjugate character.

$$\varphi_{6156} = 1 + 324 + 323+323' + 1140 + 1615 + 1215+1215'$$

$$\varphi_{19380} = 1 + 324 + 646+646' + 2754 + 816 + 3078 + 1140 + 1215+1215' + 1615 + 85+85' + 1920+1920'+1920''$$

$$\varphi_{20520} = 1 + 324 + 2754 + 816 + 3078 + 2432 + 1140 + 1615 + 1215+1215' + 85+85' + 1920+1920'+1920''$$

$$\varphi_{14688} = 1 + 85+85' + 2x1140 + 1615 + 1215+1215' + 2432 + 1920+1920'+1920''$$

$$\varphi_{12312} = \varphi_{6156} + 2x1140 + 1938+1938'$$

The last character is found in the course of an exhaustive search in which the factors of G are examined in increasing order of magnitude with no restrictions on the multiplicities except the natural onethat the multiplicity of a (complex) irreducible character should not exceed the minimum of its degree d and n/d where n is the index of the subgroup sought, The fact that there is only one rationally irreducible character of odd degree (1615) besides the principal character is of assistance. This search has been taken up to index

| Element Order | 1 | 2 | 4 | 8 | 6 | 12 | 5 | 10 | 15 | 17 | 19 | 3 | 3 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\|C_G(x)\|$ | $\|G\|$ | 1920 | 96 | 8 | 24 | 12 | 30 | 10 | 15 | 17 | 19 | 1080 | 243 | 27 |
| | 6156 | 76 | 12 | 0 | 4 | 0 | 1 | 1 | 1 | 2 | 0 | 36 | 0 | 0 |
| | 19380 | 20 | 12 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 30 | 21 | 6 |
| | 20520 | 40 | 8 | 0 | 4 | 2 | 0 | 0 | 0 | 1 | 0 | 0 | 27 | 3 |
| | 14688 | 96 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | 1 | 0 | 27 | 3 |
| | 12312 | 120 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 4 | 0 | 72 | 0 | 0 |

Table T-1

Values of possible permutation characters of Janko's simple group of order 50,232,960.

17442 during which two possible new degrees emerge including that of degree 12312 which presumably corresponds to a subgroup of index two in the subgroup of order 8160. The characters take the values shown in Table T-1.

The evidence of the characters above suggests the presence of subgroups SL(2,16), a group $SL^*(2,16)$ containing SL(2,16) as a subgroup of index two, PSL(2,17), PSL(2,19) and a solvable group of order 2592. Counts of the number of elements of each period as suggested by the characters are consistent with the presence of the named subgroups above. In particular, the subgroups PSL(2,17) and PSL(2,19) are constructed. No attempt has been made to check the existence of the solvable group of order $2^5 3^4$.

Coset enumeration

On the evidence of the possible permutation character G. Higman assumes the existence of a subgroup $SL^*(2,16)$ and is able to deduce a set of relations for G, namely:-

Let GF(16) consist of 0 and $\alpha^i$, $i = 0,1,\ldots,14$ where $1+\alpha = \alpha^{12}$. The elements of SL(2,16) are the matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad a,b,c,d \in GF(16), \quad \text{and} \quad ad-bc = 1;$$

its automorphism group is $< SL(2,16), u >$ where $u^4 = 1$, and

$$u^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} u = \begin{bmatrix} a^2 & b^2 \\ c^2 & d^2 \end{bmatrix}.$$

Let $H = \langle SL(2,16), u^2 \rangle$. If Janko's group exists and contains H then it is generated by H and an element t where

$$t^2 = 1$$

$$t \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} t = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$t \begin{bmatrix} 1 & \alpha^6 \\ 0 & 1 \end{bmatrix} t = \begin{bmatrix} 1 & \alpha^2 \\ 0 & 1 \end{bmatrix}$$

$$t \begin{bmatrix} \bar{\alpha}^5 & 0 \\ 0 & \alpha^5 \end{bmatrix} t = \begin{bmatrix} \bar{\alpha}^5 & 0 \\ 0 & \alpha^5 \end{bmatrix}$$

$$tut = u^3$$

$$\left( t \begin{bmatrix} \bar{\alpha}^3 & 0 \\ 0 & \alpha^3 \end{bmatrix} \right)^3 = 1$$

$$\left( t \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)^4 = u^2$$

$$\left( t \begin{bmatrix} 0 & \alpha^6 \\ \bar{\alpha}^6 & 0 \end{bmatrix} t \begin{bmatrix} 0 & \alpha^3 \\ \bar{\alpha}^3 & 0 \end{bmatrix} \right)^2 = 1$$

$$t \begin{bmatrix} \alpha^2 & 1 \\ 1 & 0 \end{bmatrix} t \begin{bmatrix} \alpha & \bar{\alpha}^6 \\ \alpha^6 & 0 \end{bmatrix} t \begin{bmatrix} 1 & \bar{\alpha}^3 \\ \alpha^3 & 0 \end{bmatrix} t \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} t \begin{bmatrix} \alpha & \bar{\alpha}^3 \\ \alpha^3 & 0 \end{bmatrix} = 1$$

In order to be able to use coset enumeration it is necessary to replace the matrices representing elements of

SL(2,16) by words in a set of generators of SL(2,16). By choosing the natural set of generators

$$a: \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad b: \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad c: \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

it is found that a sufficient set of relations for SL(2,16) is

$$a^2 = c^2 = b^{15} = (ac)^3 = (bc)^2 = abab^{-4}ab^3 = 1$$

Relations for G may now be written:

$$a^2 = b^{15} = c^2 = e^2 = t^2 = (te)^2 = (ta)^2 = (bc)^2 = (ea)^2 = (ec)^2 = 1,$$

$$(ac)^3 = b^4eb^{-1}e = baeb^{-1}abeb^{-1}a = (tbe)^3 = (tc)^4e = (b^2tbctc)^2 = 1,$$

$$b^3ab^{-3}tbab^{-1}t = (b^3t)^3 = bab^{-1}ctaeb^{-1}eb^{-1}ab^{-1}ctb^{-1}ab^{-2}actactb^{-1}ab^{-2}ct = 1$$

where $e = u^2$ and t is the extending involution.

These relations yield the 6156 cosets expected. Coset enumeration on the cosets of the subgroup generated by atc and b shows that these two elements already generate G. Further examination by hand enables the original generators to be expressed in terms of these two, namely:

$$b^{-5}xb^5x^{-1}b^{-5} = a, \quad a^{-1}x^{-1}axax^{-1}a = t, \quad (ax)^4 = e$$

where $x = atc$.

Construction of the subgroups PSL(2,17) and PSL(2,19)

Once a non-trivial permutation is found for the generators of G, necessarily faithful since G is simple, this representation can be used in a search for elements of G which generate subgroups given by certain defining relations. Two subgroups whose existence is suggested by the possible permutation characters are PSL(2,17) and PSL(2,19). If these subgroups exist they are certainly maximal subgroups of G since no possible permutation characters for degrees dividing 20520 or 14688 other than the principal character are found.

Mennicke and Behr [ B2 ] have given generators and defining relations for PSL(2,p), p an odd prime:

$$PSL(2,p) = \langle t,u \rangle$$
$$t^2 = u^3 = (tu)^p = \{tutu(ut)^{\frac{1}{2}(p+1)}\}^3 = 1.$$

For $p \geq 5$ non-trivial elements satisfying these relations must generate PSL(2,p) since it is simple and has no proper factor groups. From the defining property (ii) the class in G to which the involution t must belong if the subgroup exists is known. In G there are two classes of elements of period 3 but from the permutation characters it is seen that the subgroups of index 20520 and 14688 contain only the class of elements of period 3 which has no fixed

points in the representation on the 6156 cosets of SL*(2,16). Representative elements of the classes in G to which t and u must belong are found and then by conjugating at random tne relations are examined to see whether they are satisfied.

A preliminary analysis is useful in order to determine whether the computation is unlikely to succeed within a reasonable time. The probability of finding elements $x\varepsilon C_i$ and $y\varepsilon C_j$ such that their product $xy\varepsilon C_k$ can be estimated as follows. There are $h_i h_j$ ordered pairs $(x,y)$, $x\varepsilon C_i$, $y\varepsilon C_j$ with products xy of which $a_{ijk}h_k$ lie in $C_k$. The probability that a pair $(x,y)$, $x\varepsilon C_i$, $y\varepsilon C_j$ chosen at random from their classes so that $xy(=z)\varepsilon C_k$ is given by $p_{ijk} = \frac{a_{ijk}h_k}{h_i h_j}$. Alternatively elements could be chosen at random to satisfy $zy^{-1} = x$ or $x^{-1}z = y$. The three probabilities are $p_{ijk}$, $p_{kj'i}$ and $p_{i'kj}$. Provided that $a_{ijk} \neq 0$, there is some choice to maximize the probability. The symmetry relations satisfied by the structure constants show that the numerators of these three probabilities have the same value and so (provided that $a_{ijk} \neq 0$) the classes can be chosen to maximize the probability by minimizing the denominator. Let this denominator be $h_i h_j$. In G there is a unique class $C_i$ of involutions and these have a centralizer of order 1920. There are two classes of elements of period 3 but examination of permutation characters on the cosets of the two subgroups reveals the class $C_j$ to be that of elements

centralized by the Sylow 3-subgroup of G of order 243. Elements of order 17 and 19 are self-centralizing. From computed class structure constants it is found that there are 119 ordered pairs $(x,y)$, $x\varepsilon C_i$, $y\varepsilon C_j$ such that $xy$ is a fixed element of period 17. For a product of period 19 the corresponding figure is 95. The probability of a random pair $(x,y)$, $x\varepsilon C_i$, $y\varepsilon C_j$ being chosen such that $xy$ has period 17 is found to be $\frac{42}{323}$ and for period 19 it is $\frac{30}{323}$. These probabilities take into account that for both periods 17 and 19 there are two classes of elements, an element not being conjugate to its inverse.

The probabilities are upper bounds on the probability of generating the subgroups since further relations have to be checked and it may be that the whole group is generated and the further relations are never satisfied. Since the subgroups sought are simple it is sufficient to find elements satisfying the further relations; in more general cases it would be necessary to show that the elements do not generate a factor group of the group given by the defining relations.

The products $xy$ are generated at random using the permutation representation of degree 6156. The cycle structure of each product is examined to see whether it contains a cycle of length 17 or 19 in which case it has that period since there are no elements whose periods are multiples of 17 or 19. If a cycle of length 17 or 19

occurs the final relation is checked and since the groups are simple, they have been constructed if the final relation is satisfied. If not, the computation is repeated with a new random product. After two minutes of computation the generators for both subgroups were found. Using Behr and Mennicke's relations and the generators given above, it is found that

$$PSL(2,17) = \langle t, [t,b]^x \rangle$$

and

$$PSL(2,19) = \langle t, [t,b]^z \rangle$$

where $[t,b] = tb\ tb^{-1}$, $x = atcb$, $z = (b\ atcb)^3$.

A random element should strictly be defined as one chosen from a uniform probability distribution on the elements of G. It is assumed that the method given below gives an approximation to such a distribution although the only property that is used is that a large number of distinct elements are generated.

A random element is computed by forming the word $w_{i+1}$ from the word $w_i$ ($w_0=1$) by multiplying it by one of the two generators of G chosen at random with equal probability. Since the periods of the two elements are 12 and 15 it is to be expected that there are few repetitions in the initial sequence generated. In fact, it is not the product xy which is chosen at random. One of the elements x or y can be conjugated at random with the same effect. For if a

and b are independent random elements of G then $a^{-1}xab^{-1}yb$ and $xab^{-1}yba^{-1}$ are conjugate and the transforming element $ba^{-1}$ is a random element of G.

# Chapter 10

## Conversion of numerical values of characters to their algebraic form

Approximate numerical values for the irreducible characters are computed from the components of eigenvectors. These approximations, although useful, are not easily transformed by eye into sums of roots of unity. An efficient method for doing this is given here.

Let x be an element of period n and let $\chi(x)$ be an irreducible character of degree d to which $\chi_N(x)$ is a numerical approximation. Let $\chi(x) = \sum_{i=1}^{d} \omega^{k_i}$, $0 \leq k_i < n$, where $\omega$ is a primitive nth root of unity. The problem is to determine a set $\{k_i\}$ from $\chi_N(x)$. The terms of the sum may be arranged so that $k_1 \leq k_2 \leq \ldots \leq k_d$. Each of the $\binom{d+n-1}{d}$ such possible sets yielding sums $S_t$ could be generated starting from 0,0,...,0 and ending at n-1,n-1,...,n-1 and a sum chosen for which $|S_t - \chi_N(x)|$ is a minimum. This method can be improved. The problem may be visualised in the complex plane by representing each term in the sum by a unit vector which lies at an angle which is a multiple of $2\pi/n$ to the horizontal. The sum itself is represented by a set of vectors joined up end to end from the origin to $\chi(x)$. The terms are generated as described above but

after choosing the first s terms a check is made to see whether the distance from the sum of the first s terms to $\chi_N(x)$ is less than d-s; if not the exponent of $\omega$ in the sth term is altered. Even with this improvement the algebraic form of the character of an element such that n, and d are both greater than 10 (say) could be very time-consuming to determine. In cases such as are presented by the representations of some large simple groups, e.g. Janko's simple group of order 50,232,960 which has irrational irreducible characters for which d = 1920 and n = 9, it is quite unrealistic to use this method.

Instead of trying to fit d terms in the sum, d-k terms are fitted where $k = \sum_{i=1}^{s} a_i p_i$, $a_i \geq 0$ and $p_i$, i=1,2,...,s are distinct prime factors of n. If such a set of d-k terms can be found then a further k terms which contribute zero to the sum can be added, namely $\sum_{i=1}^{s} a_i \left( \sum_{t=0}^{p_i-1} \omega^{td_i} \right)$ where $n = p_i d_i$. (The converse statement, namely, if $P(\omega) = \sum_{i=0}^{n} c_i \omega^i = 0$ and $c_i \geq 0$ then $\sum_{i=0}^{n} c_i = \sum_{i=1}^{s} a_i p_i$ for some $a_i \geq 0$ appears open. No counter-examples have been found. If the converse is not satisfied for some character then the method will still work but may take more time.)

If n has only one prime factor $p_1$ then k takes only

those values which are multiples of $p_1$ but if n has more prime factors then there is a useful expression for the values k may take. A lemma from number theory is needed [ H6 ].

Lemma: If $p_1$ and $p_2$ are co-prime positive integers then $a_1p_1 + a_2p_2$, $(a_1, a_2 \geq 0)$ takes all values not less than $k = (p_1-1)(p_2-1)$.

Let $p_1$ and $p_2$ be the two smallest prime divisors of n. Besides the values not less than k, it may also be necessary to use those other exceptional values of $\sum_i a_i p_i$ $(a_i \geq 0)$ which are less than k. If $k < d$ then the number of terms used starts at 0 and increases to d-k and if no fit has been found the number of terms is increased to those values corresponding to the exceptional values of k. If still no fit has been made the numerical value of the character is output. In practice this has indicated a fault.

If the value of a character is numerically an integer then the term fitting is not done since certain integral values, e.g. -1 can be time-consuming to fit.

To show that the sum of terms found to fit closely to the numerical approximation to the character is algebraically correct it is necessary to show that no other character of degree d or less has value within the error disc for the numerical value of the character which has been computed from a component of an eigenvector. In the absence of

further knowledge concerning the character, such as the character being that of a subgroup and therefore of lesser degree, this requires finding a lower bound to the non-zero minimum of $\varphi(\omega) = |\sum_{i=1}^{d-k} \omega^{k_i} - \sum_{i=1}^{d} \omega^{m_i}|$ over the set $\{m_i\}$.

Theorem:

Let $\varphi(\omega) = |\sum_{i=1}^{d-k} \omega^{k_i} - \sum_{i=1}^{d} \omega^{m_i}|$. Then

$|\varphi(\omega)| \geq (2d-k)^{1-\varphi_n}$ where $\varphi_n$ is Euler's totient function.

Proof: Let $N(\omega) = \prod_{i=1}^{\varphi_n} \varphi(\omega_i)$ where $\omega_i$ runs over the set of $\varphi_n$ algebraic conjugates of $\omega$. $N(\omega)$ is a norm of $\omega$ and is $\geq 1$ in absolute value since the norm of a non-zero algebraic integer is a non-zero rational integer. Now

$$|\varphi(\omega_i)| \leq |\sum_{i=1}^{d-k} |\omega^{k_i}| + \sum_{i=1}^{d} |\omega^{m_i}|| = 2d-k$$

so,

$$|\varphi(\omega_i)| \geq (\prod_{\substack{j=1 \\ j\neq i}}^{\varphi_n} |\varphi(\omega_j)|)^{-1} \geq (2d-k)^{1-\varphi_n}.$$

The theorem is proved by taking $\omega_i = \omega$.

Character table output

The output routine for printing out the characters in algebraic form takes for input the output of the routine

which computes the character value on an element of period n as a sum of nth roots of unity. The expression $\sum_{k=0}^{n-1} a_k \omega^k$ is stored in an array b with $b_k = a_k$, $a_k \geq 0$, $k = 0,1,\ldots,n-1$. The number of non-zero entries in b is minimized by repeatedly subtracting 1 from all entries and noting which gives the minimum number of non-zero entries. Subtracting 1 is equivalent to subtracting $\sum_{i=0}^{n-1} \omega^i = 0$. The integer term is output first followed by cosines and exponentials. For example, if n = 9 and b contains

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 0 | 0 | 2 | 1 | 1 | 1 | 3 |

then it is changed to

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | -1 | -1 | 1 | 0 | 0 | 0 | 2 |

and printed out as the expression 2+2c1-e2-e3+e4+e8. When n=2t, the integer term is $b_o - b_t$.

The character tables are aligned and divided into pages of the correct size by the output program.

The output routines are sophisticated and they depend greatly on the flexibility of the Atlas Autocode alphabetic handling facilities for output.

A pair of permutations can be input to output the tables with the classes and representations in any specified order. This has been done to make it easier to compare versions of the same table differing by permutations of the

rows and columns.

# Chapter 11

## Computations with the symmetric group

### The character table of the symmetric group $S_n$

Because of the ease with which calculations on the symmetric group can be made and also because of the interest of physicists in the group, the symmetric group was the first group whose character table was computed automatically. This was published by Bivins, Metropolis, Stein and Wells [ B3 ] in 1954. Their work was contemporary with that of Comet [ C1 ]. The characters of the symmetric group occur naturally in applications in genetics [ J1 ], card shuffling [ H5 ], sorting [ B1 ], physics [ H4 ] and symmetric functions [ M2 ] besides being of interest in their own right in the theory of finite groups.

Definition: A partition of n is an unordered set of positive integers $\{a\} = (a_1, a_2, \ldots, a_k)$ such that $\sum a_i = n$. The $a_i$ are called the parts of a. Conventionally $a_i \geq a_{i+1}$ $i = 1,2,\ldots,k-1$.

The partition a of n is associated with its Ferrers-Sylvester diagram. For example, the diagram

$$\begin{array}{cccc} * & * & * & * \\ * & * & * & \\ * & * & & \end{array} \qquad (11.1)$$

represents the partition (4,3,2) of 9.

Definition: The conjugate partition to (4,3,2) is obtained by interchanging the rows and columns of the diagram, deriving the partition (3,3,2,1). The conjugate partition to {a} is denoted by $\{\bar{a}\}$.

Let {a} and {b} be distinct partitions of n. They are naturally ordered so that {a} precedes {b} whenever $a_i = b_i$, $i = 1,2,\ldots,k$, and $a_{k+1} > b_{k+1}$.

Each representation and each class of the symmetric group $S_n$ may be associated with a partition of n. If $\chi_{ab}$ is the character of the symmetric group associated with the representation {a} and the class {b} then

$$\chi_{\bar{a}b} = \varepsilon_b \chi_{ab} \qquad (11.2)$$

where $\varepsilon_b = \mp 1$ according to whether the partition {b} has an odd or even number of even parts.

The interest in the program [ M3 ] for computing symmetric group characters lies in two facts. It uses a new technique [ M4 ] whereby a partition is stored in the computer by a single non-negative integer not greater than the number p(n) of partitions of n thus ensuring a considerable saving of space at the expense of storing an auxiliary table of $\frac{1}{2}n^2$ entries. The algorithms are the first published for the symmetric group in a high-level language. The algorithm is written with applications to symmetric polynomial problems in mind [ M2 ] and generates one character on each entry to the routine but requires very minor modification to generate a full character table

efficiently. The method used is the standard recursive algorithm of Murnaghan and is described in Littlewood [ L5 ].

Rules for computing the symmetric group characters

Rules for computing $\chi_{ab}$ where $\{a\} = (a_1,a_2,\ldots,a_s)$, $\{b\} = (b_1,b_2,\ldots,b_t)$ and $a_i \geq a_{i+1}$, $i = 1,2,\ldots,s-1$, $b_j \geq b_{j+1}$, $j = 1,2,\ldots,t-1$, are:

1. $\chi_{ab} = \sum \chi_{a'b'}$ where $\{a'\} = (a_1,a_2,\ldots,a_i-b_1,a_{i+1},\ldots,a_s)$ and $\{b'\} = (b_2,b_3,\ldots,b_t)$ and the summation is over $i = 1,2,\ldots,s$.

2. (i) $(a_1,a_2,\ldots,a_{i-1},a_i,a_{i+1},\ldots,a_s) =$
$- (a_1,a_2,\ldots,a_i-1,a_{i-1}+1,a_{i+1},\ldots,a_s)$, and

(ii) in particular, if for any $i$, $a_i+1 = a_{i+1}$ then $(a_1,a_2,\ldots,a_s) = 0$.

3. $(a_1,a_2,\ldots,a_s) = 0$ if $a_s < 0$.

4. $(a_1,a_2,\ldots,a_s) = (a_1,a_2,\ldots,a_{s-1})$ if $a_s = 0$.

5. $(0) = 1$.

An example

Writing $(4,3,1)(4,2,2)$ for $\chi_{(4,3,1)(4,2,2)}$ then

$$\begin{aligned}(4,3,1)(4,2,2) &= (0,3,1)(2,2)+(4,-1,1)(2,2)+(4,3,-3)(2,2)\\ &= -(2,1,1)(2,2) - (4,0,0)(2,2) + 0\\ &= -(0,1,1)(2) - (2,-1,1)(2) - (2)(2)\end{aligned}$$

$$= 0 + (2,0,0)(2) - (2)(2)$$

$$= (0) - (0)$$

$$= 0.$$

The degrees of the irreducible characters of $S_n$

A question has been raised by Bivins and others [ B3 ], namely:-

For what partitions of n does the degree of an irreducible character of $S_n$ attain its maximum value and how does this maximum behave for large n?

This was apparently motivated by the practical considerations of number overflow in the computer. It is of interest to be able to estimate the largest value either as a function of n or as a recursively defined function whose arguments form a partition associated with a particular irreducible representation of the symmetric group.

To try to throw light on this question it seems necessary to be able to compute the largest degree and a partition for which it occurs. Such a program was written for a 4000 word 12 bit store PDP8 computer. The degree of the character associated with the class $\{a\} = (a_1, a_2, \ldots, a_k)$ where $a_i \geq a_{i+1}$, $i = 1,2,\ldots,k-1$ and $\sum_{i=1}^{k} a_i = n$, is given by [ B3 ]

$$d_a = \frac{n! \prod_{i<j} (b_i - b_j)}{\prod_i (b_i!)} \qquad \text{where } b_i = a_i + k - i \quad (11.3)$$

Lemma: $d_a \leq \sqrt{n!}$ .

Proof: By using the column orthogonality relations on the degrees, the sum of the squares of the degrees of the irreducible characters of $S_n$ is n!.

To minimise the amount of computing with large numbers the computation is performed by working with the exponents of the prime factors occurring in the expression for $d_a$. This is described in [ M5 ]. The prime factors of all numbers not greater than n are kept in the store for direct use in building up the set of exponents of the primes. To evaluate the magnitude of $d_a$, an expandible multilength number is repeatedly multiplied by a single-length number.

The degree is computed only for those partitions {a} which precede or coincide with their conjugates (see 11.2). This has the advantage of economy by using the partition with the smaller number of parts.

The maximal degrees of table T-2a have been printed in decimal using Lunnon's [ L4 ] multiple-length arithmetic package for Atlas.

The tables do not appear to reveal any simple recurrence relation between the partitions associated with the maximal degrees for $S_n$ and those for $S_k$ ($k < n$). It is notable, however, that frequently the partition for the maximal degree for $S_n$ differs from that for the maximal degree for $S_{n-1}$ in only a single part.

| $d_{max}$ | n |
|---|---|
| 2 | 3 |
| 3 | 4 |
| 6 | 5 |
| 16 | 6 |
| 35 | 7 |
| 90 | 8 |
| 216 | 9 |
| 768 | 10 |
| 2310 | 11 |
| 7700 | 12 |
| 21450 | 13 |
| 69498 | 14 |
| 292864 | 15 |
| 1153152 | 16 |
| 4873050 | 17 |
| 16336320 | 18 |
| 64664600 | 19 |
| 249420600 | 20 |
| 1118939184 | 21 |
| 5462865408 | 22 |
| 28542158568 | 23 |
| 117487079424 | 24 |
| 547591590000 | 25 |

Table T-2a

Maximal irreducible degree of $S_n$

Table T-2a(continued)

| $d_{max}$ | n |
|---|---|
| 2474843571200 | 26 |
| 1276091216400 | 27 |
| 574241047380 | 28 |
| 295284192942320 | 29 |
| 186513492189024 | 30 |
| 92418273851904 | 31 |
| 50385731994259200 | 32 |
| 26840130624552960 | 33 |
| 15798123760723200 | 34 |
| 7821859115070000000 | 35 |
| 4097164298370000000 | 36 |
| 222250513478508715200 | 37 |
| 159269428320995266560 | 38 |
| 93352262902757090918400 | 39 |
| 58965081685061803130880 | 40 |
| 36608637916673314652160 | 41 |
| 24558615441359064616320 | 42 |
| 14064743140340298422496480 | 43 |
| 8262872440618222005074496 | 44 |
| 5002839287614223484343200 | 45 |
| 3099186881321017005002484000 | 46 |
| 2036887351240042742340556800 | 47 |
| 1391087091494025164995795353600 | 48 |
| 1007882872827294505989182259200 | 49 |
| 721304417811716752220042035200 | 50 |

Table T-2a(continued)

| $d_{max}$ | n |
|---|---|
| 5486245628268990732913484759040 | 51 |
| 3602717344007809066611628632576 00 | 52 |
| 2416328017978835907706221223561800 | 53 |
| 1603208919826587650124498764814 0000 | 54 |
| 1123329400800148073512318500477315 00 | 55 |
| 780924182374434489607494144716850000 | 56 |
| 575949268858653096803260594834104 0000 | 57 |
| 392042285432517105673428107991024 00000 | 58 |
| 284360991016399770894957040134389760000 | 59 |
| 232199844171845578871179664651452416000 | 60 |
| 19896436084338134974427586952682903961600 | 61 |
| 14849327065029909321599194184305992806 4000 | 62 |
| 11280848154714909237752387831889958910 11200 | 63 |
| 8229081864439402212381478702631306868113280 | 64 |
| 6474451185906042071229064235458681106151 9360 | 65 |
| 4926488872069257784272444278606702029690 57200 | 66 |
| 4025571251354748853301084014788823689834654000 | 67 |
| 3047316791212510910697472612884064586737152 0000 | 68 |
| 2344179116438069879486783935009558355021660 16000 | 69 |
| 1788611255686599443441275423897069708421376000000 | 70 |
| 1406179814663421510092845752984654120312240000000 | 71 |
| 1307522743279523215389897609524063885285350440960 00 | 72 |
| 1099941833914297566548100976306304543754345185280000 | 73 |
| 939381429772200734646622546266562828224403049990 4000 | 74 |
| 755917304494811890687652071481759178624453984930 00000 | 75 |

| n | $\sqrt{n!}$ | $a.10^b$ | $d_{max}/\sqrt{n!}$ | Partition |
|---|---|---|---|---|
| | a | b | | |
| 3 | 2.45 | 0 | 0.816 | $2,1$ |
| 4 | 4.90 | 0 | 0.612 | $3,1$ |
| 5 | 1.10 | 1 | 0.548 | $3,1^2$ |
| 6 | 2.68 | 1 | 0.596 | $3,2,1$ |
| 7 | 7.10 | 1 | 0.493 | $4,2,1$ |
| 8 | 2.01 | 2 | 0.448 | $4,2,1^2$ |
| 9 | 6.02 | 2 | 0.359 | $4,3,1^2$ |
| 10 | 1.90 | 3 | 0.403 | $4,3,2,1$ |
| 11 | 6.32 | 3 | 0.366 | $5,3,2,1$ |
| 12 | 2.19 | 4 | 0.352 | $5,3,2,1^2$ |
| 13 | 7.89 | 4 | 0.272 | $5,4,2,1^2$ |
| 14 | 2.95 | 5 | 0.235 | $6,4,2,1^2$ |
| 15 | 1.14 | 6 | 0.256 | $5,4,3,2,1$ |
| 16 | 4.57 | 6 | 0.252 | $6,4,3,2,1$ |
| 17 | 1.89 | 7 | 0.258 | $6,4,3,2,1^2$ |
| 18 | 8.00 | 7 | 0.204 | $7,4,3,2,1^2$ |
| 19 | 3.49 | 8 | 0.185 | $7,5,3,2,1^2$ |
| 20 | 1.56 | 9 | 0.160 | $7,5,3,2^2,1$ |
| 21 | 7.15 | 9 | 0.157 | $7,5,3,2^2,1^2$ |
| 22 | 3.35 | 10 | 0.163 | $7,5,4,3,2,1$ |
| 23 | 1.61 | 11 | 0.178 | $7,5,4,3,2,1^2$ |
| 24 | 7.88 | 11 | 0.149 | $8,5,4,3,2,1^2$ |
| 25 | 3.94 | 12 | 0.139 | $8,6,4,3,2,1^2$ |

Table T-2b

| n | $\sqrt{n!}$ | $a \cdot 10^b$ | $d_{max}/\sqrt{n!}$ | Partition |
|---|---|---|---|---|
| | a | b | | |
| 26 | 2.01 | 13 | 0.123 | $8,6,4,3,2,1^3$ |
| 27 | 1.04 | 14 | 0.122 | $8,6,4,3,2^2,1^2$ |
| 28 | 5.52 | 14 | 0.104 | $8,6,5,3,2^2,1^2$ |
| 29 | 2.97 | 15 | 0.099 | 8,6,5,4,3,2,1 |
| 30 | 1.63 | 16 | 0.115 | $8,6,5,4,3,2,1^2$ |
| 31 | 9.07 | 16 | 0.102 | $9,6,5,4,3,2,1^2$ |
| 32 | 5.13 | 17 | 0.098 | $9,7,5,4,3,2,1^2$ |
| 33 | 2.95 | 18 | 0.091 | $9,7,5,4,3,2,1^3$ |
| 34 | 1.72 | 19 | 0.092 | $9,7,5,4,3,2^2,1^2$ |
| 35 | 1.02 | 20 | 0.077 | $9,7,6,4,3,2^2,1^2$ |
| 36 | 6.10 | 20 | 0.067 | $9,7,6,4,3^2,2,1^2$ |
| 37 | 3.71 | 21 | 0.060 | $10,8,6,4,3,2^2,1^2$ |
| 38 | 2.29 | 22 | 0.070 | $9,7,6,5,4,3,2,1^2$ |
| 39 | 1.43 | 23 | 0.065 | $10,7,6,5,4,3,2,1^2$ |
| 40 | 9.03 | 23 | 0.065 | $10,8,6,5,4,3,2,1^2$ |
| 41 | 5.78 | 24 | 0.063 | $10,8,6,5,4,3,2,1^3$ |
| 42 | 3.75 | 25 | 0.066 | $10,8,6,5,4,3,2^2,1^2$ |
| 43 | 2.46 | 26 | 0.057 | $11,8,6,5,4,3,2^2,1^2$ |
| 44 | 1.63 | 27 | 0.051 | $11,8,6,5,4,3,2^2,1^3$ |
| 45 | 1.09 | 28 | 0.046 | $11,9,7,5,4,3,2^2,1^2$ |
| 46 | 7.42 | 28 | 0.042 | $11,9,7,5,4,3,2^2,1^3$ |
| 47 | 5.09 | 29 | 0.040 | $10,8,7,6,5,4,3,2,1^2$ |
| 48 | 3.52 | 30 | 0.039 | $11,8,7,6,5,4,3,2,1^2$ |
| 49 | 2.47 | 31 | 0.041 | $11,9,7,6,5,4,3,2,1^2$ |
| 50 | 1.74 | 32 | 0.041 | $11,9,7,6,5,4,3,2,1^3$ |

Table T-2b(continued)

| n | $\sqrt{n!}$ a | $a.10^b$ b | $d_{max}/\sqrt{n!}$ | Partition |
|---|---|---|---|---|
| 51 | 1.25 | 33 | 0.044 | $11,9,7,6,5,4,3,2^2,1^2$ |
| 52 | 8.98 | 33 | 0.040 | $12,9,7,6,5,4,3,2^2,1^2$ |
| 53 | 6.54 | 34 | 0.037 | $12,9,7,6,5,4,3,2^2,1^3$ |
| 54 | 4.80 | 35 | 0.033 | $12,10,8,6,5,4,3,2^2,1^2$ |
| 55 | 3.56 | 36 | 0.032 | $12,10,8,6,5,4,3,2^2,1^3$ |
| 56 | 2.67 | 37 | 0.029 | $12,10,8,6,5,4,3^2,2,1^3$ |
| 57 | 2.01 | 38 | 0.029 | $12,10,8,6,5,4,3^2,2^2,1^2$ |
| 58 | 1.53 | 39 | 0.026 | $12,10,8,7,5,4,3^2,2^2,1^2$ |
| 59 | 1.18 | 40 | 0.024 | $12,10,8,7,6,5,4,3,2,1^2$ |
| 60 | 9.12 | 40 | 0.025 | $12,10,8,7,6,5,4,3,2,1^3$ |
| 61 | 7.12 | 41 | 0.028 | $12,10,8,7,6,5,4,3,2^2,1^2$ |
| 62 | 5.61 | 42 | 0.026 | $13,10,8,7,6,5,4,3,2^2,1^2$ |
| 63 | 4.45 | 43 | 0.025 | $13,10,8,7,6,5,4,3,2^2,1^3$ |
| 64 | 3.56 | 44 | 0.026 | $13,10,9,7,6,5,4,3,2^2,1^3$ |
| 65 | 2.87 | 45 | 0.023 | $13,11,9,7,6,5,4,3,2^2,1^3$ |
| 66 | 2.33 | 46 | 0.021 | $13,11,9,7,6,5,4,3^2,2,1^3$ |
| 67 | 1.91 | 47 | 0.021 | $13,11,9,7,6,5,4,3^2,2^2,1^2$ |
| 68 | 1.57 | 48 | 0.019 | $14,11,9,7,6,5,4,3^2,2^2,1^2$ |
| 69 | 1.31 | 49 | 0.018 | $14,11,9,7,6,5,4,3^2,2^2,1^3$ |
| 70 | 1.09 | 50 | 0.016 | $14,11,9,8,6,5,4,3^2,2^2,1^3$ |
| 71 | 9.22 | 50 | 0.015 | $14,11,9,8,6,5,4^2,3,2^2,1^3$ |
| 72 | 7.83 | 51 | 0.017 | $13,11,9,8,7,6,5,4,3,2^2,1^2$ |
| 73 | 6.69 | 52 | 0.016 | $14,11,9,8,7,6,5,4,3,2^2,1^2$ |
| 74 | 5.75 | 53 | 0.016 | $14,11,9,8,7,6,5,4,3,2^2,1^3$ |
| 75 | 4.98 | 54 | 0.015 | $14,11,10,8,7,6,5,4,3,2^2,1^3$ |

Table T-2b(continued)

## The number of characters of odd degree

The observation that the number of irreducible characters of odd degree is a power of 2 for the known simple groups of order $< 10^6$ leads to an examination of the number of characters of odd degree in $S_n$ and $A_n$. Tables T-3 and T-5 contain the results.

The degrees of $S_n$ need not be computed since all that is needed is whether the degree is even or odd. For each n, the power of 2 dividing n! is computed using the well-known relation for the power

$$k = [n/2] + [n/2^2] + \cdots .$$

Partitions are generated in their natural order and the power, d, of 2 in the denominator of (11.3) is computed. If $d < k$ then the degree is even. If not, then the power of 2 in the numerator is evaluated. It takes a minute to generate the number $m(S_n)$ of characters of odd degree for the symmetric group $S_n$, $n \leq 26$ and a further minute for the values for $n = 27, 28$. This is typical of computations involving partition generation which take a time exceeding $O(n \cdot p(n))$ for each n. The values of $m(A_n)$ were found by hand working out the partitions of n into odd unequal parts then converting these to self-conjugate partitions and evaluating the power of 2 in the corresponding degrees of $S_n$ (see Chapter 12, p. 94). If $m(S_n) = 2t$ then $m(A_n) = t + 2s$ where s is the number of self-conjugate partitions of n for which the representation of $S_n$ has 2 x odd degree.

| n | $m(A_n)$ | $m(S_n)$ |
|---|---|---|
| 4 | 4 | 4 |
| 5 | 4 | 4 |
| 6 | 4 | 8 |
| 7 | 4 | 8 |
| 8 | 8 | 8 |
| 9 | 8 | 8 |
| 10 | 8 | 16 |
| 11 | 8 | 16 |
| 12 | 16 | 32 |
| 13 | 16 | 32 |
| 14 | 32 | 64 |
| 15 | 32 | 64 |
| 16 | 16 | 16 |
| 17 | 16 | 16 |
| 18 | 16 | 32 |
| 19 | 16 | 32 |
| 20 | 32 | 64 |
| 21 | 32 | 64 |
| 22 | 64 | 128 |
| 23 | 64 | 128 |
| 24 | 64 | 128 |
| 25 | 64 | 128 |
| 26 | 128 | 256 |
| 27 | 128 | 256 |
| 28 | 256 | 512 |

Table T-3

Tabulation of m(G) for the alternating groups and symmetric groups

# Chapter 12

## The character tables

A brief statement of three techniques useful in computing character tables is given.

Brauer's theory [ B4 ]:

Let g be the order of a simple group and let p, a prime, divide g to the first power only, then

$$g = pqw(1+kp), \quad qt = p-1 \tag{12.1}$$

The normaliser of a Sylow p-subgroup has order pqw and its centralizer has order pw. By Burnside [ B5 ] $q > 1$. There are q ordinary characters $\chi_i$, $i = 1,2,\ldots,q$, of degree $d_i$, $i = 1,2,\ldots,q$, and t exceptional p-conjugate characters all of the same degree $d_o$. For the ordinary characters $\varepsilon_i d_i \equiv 1 \pmod p$ and for the exceptional characters $\varepsilon_o d_o \equiv -q \pmod p$ where $\varepsilon_i = \pm 1$. Further, the degree equation is

$$1 + \sum_{i=2}^{q} \varepsilon_i d_i + \varepsilon_o d_o = 0 \tag{12.2}$$

and $d_i \mid q(1+kp)$.

Induction from a subgroup:

The method is due to Frobenius [ F4 ]. Let $H \subset G$. For each character $\chi$ of H define $\chi'$ on G by $\chi'(x) = \chi(x)$ if $x \varepsilon H$ otherwise $\chi'(x) = 0$. Then the induced character $\chi^*(x)$

of G is given by

$$\chi^*(x) = \frac{1}{|H|} \sum_{y \in G} '(y^{-1}xy) \qquad (12.3)$$

The program described on page 54 is used to compute norms of characters induced from (and restricted to) subgroups.

Trivial intersection sets [ S3 ]:

A subset S of G is a trivial intersection set (T.I. set) if for $x \in G$, either $x^{-1}Sx \cap S \subseteq 1$ or $x^{-1}Sx = S$.

A generalized character is a sum of irreducible characters with integer coefficients.

Let S be a T.I. set such that

$$S \subseteq N_G(S) = N \subset G. \qquad (12.4)$$

If $\alpha, \beta$ are generalized characters of N which vanish on N-S and $\alpha(1) = 0$ then

$$\alpha^*(x) = \alpha(x) \quad \text{for } x \in S \qquad (12.5)$$

$$(\alpha,\beta)_N = (\alpha^*,\beta^*)_G, \qquad (12.6)$$

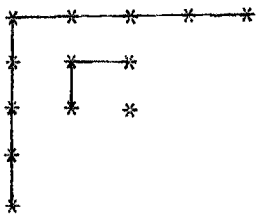
where $(\alpha,\beta)_G = \frac{1}{|G|} \sum_{x \in G} \alpha(x)\overline{\beta(x)}$ and $\alpha^*$ is the generalized character of G induced by $\alpha$.

The alternating groups

The characters of these groups are easily determined from those of the symmetric group. By Frobenius [ F5 ] the characters of $S_n$ associated with a self-conjugate

partition $\{r\}$ split in $A_n$ into two irreducible characters the values of which are half those on $S_n$ except for one class $\{c\}$ on which the value in $S_n$ is $\pm 1$. This class splits into two classes in $A_n$.

There is a 1-1 correspondence between self-conjugate partitions of n and partitions of n into unequal odd parts e.g. $\{r\} = (5,3^2,1^2)$ is associated with $\{c\} = (9,3,1)$ thus:

$\{r\} =$  $\{c\} =$  (12.7)

From the representation $\{r\}$ this correspondence gives the class $\{c\}$ which splits in the alternating group. If $\{c\} = (c_1,c_2,\ldots,c_s)$ then the characters into which $\{r\}$ splits in $A_n$ take the values

$$\tfrac{1}{2}\{ (-1)^{\frac{1}{2}(\tau-1)} \pm \tau^{\frac{1}{2}} i^{\frac{1}{2}(\tau-1)} \} \qquad \text{where } \tau = \prod_{i=1}^{s} c_i \qquad (12.8)$$

The simple groups

The character tables for the groups $SL(3,3)$, $SU(3,3^2)$, and $M_{11}$ are computed by treating the groups as permutation groups on 13, 28, and 11 letters respectively. The groups are generated as cosets of the stabiliser of a point and

are stored. No backing store is needed. Character computations for all larger groups use individual programs which contain many common subroutines.

PSL(3,4) is represented on 21 projective points. The character table on a stabiliser of a point is computed. By Steinberg [ S1 ] there is a character of degree 64 in PSL(3,4) which is the character of largest degree. This together with the orders of the centralizers of elements, is sufficient to complete the table.

$SU(4,2^2)$ is the group of 27 lines on a cubic surface [ C4 ] and is constructed as a permutation group storing the conjugacy classes on backing store.

Sz(8) is constructed using the doubly transitive representation on 65 letters and the rational class algebra is computed. The table is completed using Brauer's theory.

$M_{12}$ has been obtained as a transitive extension of degree 12 of $M_{11}$.

The computation for Janko's group of order 175,560 has already been described. This computation is believed to be the first construction of the character table of a large group by computer.

SL(3,5) is computed by inducing up the characters of the stabiliser of a point in the representation of the 31 projective points. Brauer theory is helpful here.

$M_{22}$ is obtained by inducing up the characters of $M_{21}$ which is isomorphic to PSL(3,4). Again Brauer theory is

helpful.

$PSU(3,5^2)$ is a difficult table to compute because it is represented on 126 letters and also because of the existence of an outer automorphism exchanging the three rational classes of elements of period 5. Brauer's theory tells us little since it is applicable only to the prime 7. Recourse is made to Frame [ F1 ]. Once the character of degree 20 is established the others can be constructed by splitting this character.

The rational character table of the Janko group of order 604,800 is computed as a permutation group on 100 letters by computing those structure constants $d_{uww}$ for which $K_u$ is a class of involutions in the centre of a Sylow 2-subgroup having 20 fixed points, or a class of elements of period 3 having 10 fixed points. The full character table can be computed from the rational table and induction from $SU(3,3^2)$. The computation took over 21 hours and may be regarded as beyond the limit of a feasible computation.

The character table of Sp(4,4) has been computed by hand by Duncan [ D3 ] and Hall [ H1 ] and these have been checked on the computer.

$SU(3,4^2)$ is computed on 65 letters. The rational class algebra is computed and this together with Brauer's theory for primes p=3 and 13 gives sufficient information to fill up the table degrees and classes. Recourse is

made to the theory of T.I. sets in inducing up a fragment of the table from the centralizer of order 300 of an element of order 5 to obtain the irrationalities.

2-groups

The book of Hall and Senior [ H2 ] provides a basis for the computation of the character tables of 2-groups of order $\leq 64$. The permutations given in the book were punched on to flexowriter paper tape using the same format as printed in the book. A sample of the input is given in table T-6.

The characters are computed using a standard program and no use has been made of the special structure of the groups. This is in contrast to the work of Ruud and Keown [ R1 ] whose program is especially developed for 2-groups. Their work is not yet completed at the time of writing.

As there are 311 non-abelian 2-groups whose character tables have been computed a single sample is given in the Appendix.

| Order | Name | Number of Irrational Columns | Rows | Order | Name | Number of Irrational Columns | Rows |
|---|---|---|---|---|---|---|---|
| 32 | $F_3b$ | 6 | 4 | 64 | $F_{14}b_2$ | 8 | 12 |
| 32 | $F_3c_1$ | 6 | 8 | 64 | $F_{14}d_1$ | 12 | 8 |
| 32 | $F_3c_2$ | 6 | 8 | 64 | $F_{14}d_2$ | 12 | 8 |
| 32 | $F_3f$ | 10 | 8 | 64 | $F_{15}d_1$ | 6 | 4 |
| 64 | $F_3b$ | 12 | 8 | 64 | $F_{15}d_2$ | 6 | 4 |
| 64 | $F_3c_1$ | 12 | 16 | 64 | $F_{15}e_1$ | 8 | 6 |
| 64 | $F_3c_2$ | 12 | 16 | 64 | $F_{15}e_2$ | 8 | 6 |
| 64 | $F_3f$ | 20 | 16 | 64 | $F_{15}e_3$ | 8 | 6 |
| 64 | $F_3h$ | 20 | 16 | 64 | $F_{15}e_4$ | 8 | 6 |
| 64 | $F_3j$ | 20 | 18 | 64 | $F_{15}f_1$ | 10 | 8 |
| 64 | $F_3k$ | 16 | 20 | 64 | $F_{15}f_2$ | 10 | 8 |
| 64 | $F_3n_1$ | 20 | 22 | 64 | $F_{17}a_1$ | 8 | 12 |
| 64 | $F_3n_2$ | 20 | 22 | 64 | $F_{17}a_2$ | 8 | 12 |
| 64 | $F_3q$ | 24 | 22 | 64 | $F_{17}a_3$ | 8 | 12 |
| 64 | $F_8b$ | 14 | 12 | 64 | $F_{17}b_1$ | 10 | 12 |
| 64 | $F_8c_1$ | 14 | 16 | 64 | $F_{17}b_2$ | 10 | 12 |
| 64 | $F_8c_2$ | 14 | 16 | 64 | $F_{21}a_1$ | 8 | 10 |
| 64 | $F_8f$ | 18 | 16 | 64 | $F_{21}a_2$ | 8 | 10 |
| 64 | $F_{14}b_1$ | 8 | 12 | 64 | $F_{21}a_3$ | 8 | 10 |

Table T-4

The 2-groups of order $\leq 2^6$ with differing numbers of irrationalities in the rows and columns of their character tables.

| G | m(G) |
|---|---|
| $A_5$ | $2^2$ |
| $A_6$ | $2^2$ |
| $A_7$ | $2^2$ |
| $SL(3,3)$ | $2^2$ |
| $SU(3,3^2)$ | $2^3$ |
| $M_{11}$ | $2^2$ |
| $PSL(3,4)$ | $2^3$ |
| $A_8$ | $2^3$ |
| $SU(4,2^2)$ | $2^3$ |
| $Sz(8)$ | $2^3$ |
| $SU(3,4^2)$ | $2^4$ |
| $M_{12}$ | $2^3$ |
| $PSU(3,5^2)$ | $2^2$ |
| J | $2^3$ |
| $A_9$ | $2^3$ |
| $SL(3,5)$ | $2^3$ |
| $M_{22}$ | $2^3$ |
| H-J | $2^3$ |
| $Sp(4,4)$ | $2^4$ |
| $PSL(2,q)$ q odd | $2^2$ |
| $PSL(2,q)$ $q = 2^n$ | $2^n$ |

Table T-5

The number m(G) of irreducible characters of odd degree for the known simple groups of order $\leq 10^6$.

```
F27A2
64
16 16
α1=ac,bd,eg,fh,ik,jl,mo,np,AC.BD.EG.FH.IK.JL.MO.NP.
α2=adcb,ehgf,ilkj,mpon,ADCB.EHGF.ILKJ.MPON.
α3=aebfcgdh,imjnkolp,AEBFCGDH.IMJNKOLP.
α4=anhjdmgicpflboek,ANHJDMGICPFLBOEK.
α5=aAiIeEmMbBjJfFnNcCkKgGoOdDlLhHpP.
α6=bd,eh,fg,ip,jo,kn,lm,AN.BM.CP.DO.EJ.FI.GL.HK.
*

F27A1
64
16 16
α1=ac,bd,eg,fh,ik,jl,mo,np,AC.BD.EG.FH.IK.JL.MO.NP.
α2=adcb,ehgf,ilkj,mpon,ADCB.EHGF.ILKJ.MPON.
α3=aebfcgdh,imjnkolp,AEBFCGDH.IMJNKOLP.
α4=aphldogkcnfjbmei,APHLDOGKCNFJBMEI.
α5=aAiIeEmMbBjJfFnNcCkKgGoOdDlLhHpP.
α6=bd,eh,fg,ip,jo,kn,lm,AP.BO.CN.DM.EL.FK.GJ.HI.
*
F26A4
64
16
α1=ac,bd,eg,fh,ik,jl,mo,np,
α2=ik,jl,mo,np,
α3=abcd,efgh,ijkl,mnop,
α4=ijkl,mnop,
α5=aecg,bhdf,imko,jpln,
α6=ai,bj,ck,dl,em,fn,go,hp,
*

F26A3
64
16
α1=ac,bd,eg,fh,ik,jl,mo,np,
α2=ac,bd,eg,fh,
α3=abcd,ehgf,ijkl,mpon,
α4=eg,fh,ilkj,mpon,
α5=aecg,bfdh,ipkn,jmlo,
α6=ai,bj,ck,dl,ep,fm,gn,ho,
*

F26A2
64
16
α1=ac,bd,eg,fh,ik,jl,mo,np,
α2=ac,bd,eg,fh,
α3=abcd,ehgf,ijkl,mpon,
α4=eg,fh,ilkj,mpon,
α5=ae,bf,cg,dh,im,jn,ko,lp,
α6=ai,bj,ck,dl,em,fn,go,hp,
*

F26A1
64
8
α1=ac,bd,eg,fh,
α2=eg,fh,
α3=abcd,efgh,
α4=efgh,
α5=bd,fh,
α6=ae,bf,cg,dh,
*
```

Table T-6

Sample Input

# Bibliography


BAER, R.M., and BROCK, P.

B1: Natural sorting over permutation spaces. Math. Comp., 1968, 22, 385-410.

BEHR, H., and MENNICKE, J.

B2: A presentation of the groups PSL(2,p). Canad. J. Math., 1968, 20, 1432-1438.

BIVINS, R.L., METROPOLIS, N., STEIN, P.R., and WELLS, M.B.

B3: Characters of the symmetric groups of degrees 15 and 16. Math. Comp., 1954, 8, 212-216.

BRAUER, R.

B4: On groups whose order contains a prime to the first power. Amer. J. Math., 1942, 64, 401-440.

BURNSIDE, W.

B5: The theory of groups of finite order. Cambridge University Press (2nd ed.), 1911.

COMÉT, S.

C1: On the machine calculation of characters of the symmetric group. Comptes Rendus, 12me Congres Math. Scand. Lund., 1954, 18-23.

COMÉT, S.

C2: Improved methods to calculate the characters of the symmetric group. Math. Comp., 1960, 14, 104-117.

COXETER, H.S.M., and MOSER, W.O.J.
C3: Generators and relations for discrete groups. Springer (2nd ed.), 1965.

COXETER, H.S.M.
C4: Factor groups of the braid group. Proc. 4th Canad. Math. Congress, 1959, 95-122.

CURTIS, C.W., and REINER, I.
C5: Representation theory of finite groups and associative algebras. John Wiley, 1962.

DICKSON, L.E.
D1: Linear groups with an exposition of the Galois field theory. (Leipzig, 1901), Dover edition, 1958.

DIXON, J.D.
D2: High speed computation of group characters. Num. Math., 1967, 10, 446-450.

DUNCAN, A.
D3: Doctoral thesis. Cambridge University, 1969.

FRAME, J.S.
F1: Some irreducible monomial representations of hyper-orthogonal groups. Duke Math. J., 1935, 1, 442-448.

FRAME, J.S.
F2: The simple group of order 25,920. Duke Math. J., 1936, 2, 477-484.

FRANCIS, J.G.F.
F3: The QR transformation. Computer J., 1961-1962, 4, 265-271,332-345.

FROBENIUS, G.
F4: Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen. SitzBer. Preuss. Akad., 1896, 501-515.

FROBENIUS, G.
F5: Über die Charaktere der alternierenden Gruppe. SitzBer. Preuss. Akad., 1896, 303-315.

GREEN, J.A.
G1: The characters of the finite general linear groups. Trans. Amer. Math. Soc., 1955, 80, 402-447.

HALL, M.
H1: Unpublished.

HALL, M., and SENIOR, J.K.
H2: Groups of order $2^n$ ( $n \leq 6$). Macmillan, New York, 1964.

HALL, M., and WALES, D.
H3: The simple group of order 604,800. J. Algebra, 1968, 9, 417-450.

HAMERMESH, M.
H4: Group theory and its application to physical problems. Addison-Wesley, 1962.

HANNAN, E.J.
H5: Group representations and applied probability. J. Applied Prob., 1965, 2, 1-68.

HARDY, G.H., and WRIGHT, E.M.
H6: An introduction to the theory of numbers. Oxford (4th ed.), 1960, Chapter 5.

HAYES, D.R.
H7: The calculation of the character table of a given finite group. 1963 (unpublished).

HEAD, T.
H8: Diploma in Computer Science. Edinburgh University, 1966.

HIGMAN, G., and McKAY, J.
H9: On Janko's simple group of order 50,232,960. Bull. Lond. Math. Soc., 1969, 1, 89-94 and 219.

JAMES, A.T., and PAPAZIAN, H.P.
J1: Enumeration of quad types in diploids and tetraploids. Genetics, 1961, 46, 817-829.

JANKO, Z.
J2: A new finite simple group with Abelian Sylow 2-subgroups and its characterization. J. of Algebra, 1966, 3, 147-186.

JANKO, Z.
J3: Some new simple groups of finite order, I. Symposia Mathematica, 1968, 1, 26-64.

LEECH, J.
L1: Coset enumeration. Article in Computational problems in abstract algebra, Pergamon, 1970, 21-35.

LEECH, J., (ed.)
L2: Computational problems in abstract algebra. Pergamon, 1970.

LIN, S.
L3: Private communication.

LUNNON, W.F.
L4: Multiple length arithmetic for Atlas, (unpublished).

LITTLEWOOD, D.E.
L5: The theory of group characters. Oxford (2nd ed.), 1950.

MARTIN, R.S., and WILKINSON, J.H.
M1: Similarity reduction of a general matrix to Hessenberg form. Num. Math., 1968, 12, 349-368.

McKAY, J.K.S.
M2: On the representation of symmetric polynomials. Comm. ACM, 1967, 10, 428-429.

McKAY, J.K.S.
M3: Symmetric group characters. Comm. ACM, 1967, 10, 451, and 1968, 11, 14.

McKAY, J.K.S.
M4: Three algorithms for partitions. Comm. ACM, 1965, 8, 493.

McKAY, J.K.S.
M5: On the evaluation of multiplicative combinatorial expressions. Comm. ACM, 1968, 11, 392.

McKAY, J.K.S.
M6: A method for computing the character table of a finite group. Article in Computers in Mathematical Research, North Holland, 1967, 140-148.

McKAY, J.K.S.
M7: Partitions in natural order. Comm. ACM, 1970, 13, 52.

MENDELSOHN, N.S.

M8: An algorithmic solution for a word problem in group theory. Canad. J. Math., 1964, 16, 509-516, and 1965, 17, 505.

MENDELSOHN, N.S.

M9: Defining relations for subgroups of finite index of groups with a finite presentation. Article in Computational problems in abstract algebra, Pergamon, 1970, 43-44.

RUUD, P.G., and KEOWN, R.

R1: The computation of irreducible representations of finite group of order $2^n$, $n \leq 6$. Article in Computational problems in abstract algebra, Pergamon, 1970, 205-216.

STEINBERG, R.

S1: Representations of algebraic groups. Nagoya Math. J., 1963, 22, 33-56.

STEINBERG, R.

S2: The representations of GL(3,q), GL(4,q), PGL(3,q) and PGL(4,q). Canad. J. Math., 1951, 3, 225-235.

SUZUKI, M.

S3: Applications of group characters. Proc. Symp. Pure Math., Amer. Math. Soc., 1959, 1, 88-89.

WILKINSON, J.H.

W1: The algebraic eigenvalue problem. Oxford, 1965.

WONG, S.K.

W2: A new finite non-Abelian simple group of Janko. Bull. Austral. Math. Soc., 1969, 1, 59-79.

# Appendix A

# *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 $C_i$. $A(G, \mathbf{C})$ denotes the group algebra of $G$ over the complex field $\mathbf{C}$.

**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



App A 1

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 $\quad H_i\colon\ r_k(g_1, g_2, \ldots, g_s) = 1,\quad k = 1, 2, \ldots, m_i,$

and $\quad H_{i+1}\colon\ \{w_j(g_1, g_2, \ldots, g_s)\},\quad j = 1, 2, \ldots, n_i,$

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) $Hx_i = Hx_kg_j^{-1}$ *or* (ii) $Hx_i = Hx_kg_j$ *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 $\phi_i = \phi_kg_j^{-1}$ or $\phi_i = \phi_kg_j$ where $\phi_k$ 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

$$f(x) = f(y^{-1}xy), \quad x, y \in G.$$

$f$ 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 $K$ presents no difficulties since two elements are conjugate if and only if their representing matrices are similar. We know that the transforming matrix belongs to the group since it is the group of *all* invertible $n \times n$ 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

$$g = \sum_x g/|Z(x)|, \quad x \in C_i',$$

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, $\sum$ 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 $\alpha_{ijk}$ may be interpreted in two ways: first, in the manner in which they occur in (1), and second, $\alpha_{ijk}$ 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 $\alpha_{ijk}$.

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 $\beta_{ijk}$; then $\alpha_{ijk} = \dfrac{h_j}{h_k} \beta_{ijk}$.

The $r^3$ $\alpha_{ijk}$ satisfy symmetry relations most succinctly expressed by the relations satisfied by $\gamma_{ijk} = (h_i h_j)^{-1} \alpha_{ijk'}$. The $\gamma_{ijk}$ 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 $i$th 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:

$$M_l = \{n_{l1}, \ldots, n_{lt}\};$$

$$n_{lj} \in E_{l+1} \leftrightarrow n_{lj} \supset n_{lk} \text{ for some } k, \quad \text{otherwise} \quad n_{lj} \in L_l;$$

$$M_{l+1} = \{n_{lj} n_{lk} \mid n_{lj}, n_{lk} \in L_l\} \cup E_{l+1};$$

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 $A(G, \mathbf{C})$. 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 $R^s(x)$, $x \in A(G, \mathbf{C})$, 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

$$m_i^s m_j^s = \sum_k \alpha_{ijk} m_k^s, \quad 1 \leqslant i, j \leqslant r, \tag{4}$$

which may be written

$$A^i m^s = m_i^s m^s, \quad [A^i]_{jk} = \alpha_{ijk}, \quad 1 \leqslant i, j, k \leqslant r. \tag{5}$$

This collection of $r$ sets of matrix equations is fundamental to the computation of the characters. We shall show that the matrices $A^i$, $1 \leqslant i \leqslant r$, have a unique common set of $r$ eigenvectors.

First we find the eigenvalues of $A^i$. 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 $m^s$ and so (5) has a non-trivial solution. Therefore

$$\det (A^i - m_i^s I) = 0, \quad 1 \leqslant i \leqslant r. \tag{6}$$

This is true for all $s = 1, 2, \ldots, r$, hence the eigenvalues of $A^i$ are $m_i^s$, $1 \leqslant s \leqslant r$.

We use the row orthogonality properties of the characters to prove the $m^s$, $1 \leqslant s \leqslant r$, 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:

$$\sum_i h_i \chi_i^s \tilde{\chi}_i^t = g\, \delta_{st}, \quad 1 \leqslant s, t \leqslant r. \tag{8}$$

Defining the $r \times r$ matrices $M$ and $X$ by

$$M_{st} = m_i^s,\ X_{st} = \chi_i^s, \text{ then } MX^* = \operatorname{diag}\left\{\frac{g}{d_1}, \frac{g}{d_2}, \ldots, \frac{g}{d_r}\right\}$$

where * denotes complex conjugate transpose. The diagonal entries $g/d_i$ are all non-zero, hence the rank of $M$ is $r$.

Let $x$ be a vector such that $A^i x = m_i^s x$ for all $i = 1, 2, \ldots, r$, then $x = \sum_t a_t m^t$. Suppose $a_s \neq 0$. Then

$$\sum_t a_t m_i^t m^t = \sum_t a_t m_i^s m^t, \quad i = 1, 2, \ldots, r,$$

hence

$$\sum_i a_i m^i = \sum_i a_i m^s,$$

and so

$$x = a_s m_s .$$

We have the following situation.

The entries in the $i$th column of $M$ are the eigenvalues of $A^i$ and the rows of $M$ correspond to the common eigenvectors normalized so that $m_1^s = 1$. If the entries in the column of $M$ corresponding to the eigenvalues of $A^i$ are all distinct then the whole matrix $M$ can be determined from the matrix $A^i$ 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 $\pm 1$ 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

$$\Phi = \sum_i u_i A^i \quad \text{which has eigenvalues} \quad \sum_i u_i m_i^s, \quad 1 \leqslant s \leqslant r.$$

By choosing suitable values for the indeterminates we can arrange that the eigenvalues are distinct; if so, the eigenvectors of $\Phi$ 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 $p \neq q$ $(= 1, 2, \ldots, r)$ the eigenvalues corresponding to $m^p$ and $m^q$ should be separable, i.e.

$$\left| \sum_i \theta_i m_i^p - \sum_i \theta_i m_i^q \right| > \varepsilon(t) \quad \text{for all} \quad p \neq q = 1, 2, \ldots, r,$$

where the $\theta_i$ 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 $A^i$ is 1. We introduce a normalizing factor of $r^{-1}$ and choose $\theta_i$ 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 surface 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 $\Phi$ so that the first component is unity, we have the numerical values of $m_i^s$. To find the dimension of the representation we

use the relation, derivable from the row orthogonality relations

$$\frac{1}{g}\sum_{l}\frac{1}{h_l}|m_l^s|^2=\frac{1}{d_s^2}.$$

By multiplying $m_l^s$ by $d_s$ and dividing by $h_l$ 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 $\omega$ is a primitive $p$th 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 $0, 0, \ldots, 0$ and ending at $p-1, p-1, \ldots, p-1$, 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 $u=d-\sum_{i=1}^{k}c_ip_i$ $(c_i\geqslant 0)$ terms where $p_i$ are prime divisors of $p$. We now compute the values that $\sum_i c_ip_i$ 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 $\varepsilon$ in modulus, where $\varepsilon$ 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

$$P(\omega) = |\sum_{i=1}^{d} \omega^{k_i} - \sum_{i=1}^{d} \omega^{m_i}| \qquad 0 \leqslant k_i, m_i \leqslant p-1.$$

By forming the product of the conjugates of $P(\omega)$ we obtain a lower bound:

$$|P(\omega)| \geqslant (2d)^{2-p}.$$

**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 $2\times2$ 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 $C \in PSL(2, 11)$, 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

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 10 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 6 & 4 & 9 & 4 & 6 & 1 \\ 0 & 1 & 5 & 10 & 10 & 5 & 1 \\ 0 & 0 & 1 & 4 & 6 & 4 & 1 \\ 0 & 0 & 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We now need the representing matrix for $d$. $d$ commutes with $b$, hence $d_{ij} = 0$ except when $i = j$ or $b_{ij} = b_{jj}$ $(i \neq j)$. 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 $d^2 = 1$, hence $x = \pm 1$.

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 $h_i \in H$ and $x_j$ 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 | 1 | 1463 | 5852 | 5852 | 5852 | 9240 | 9240 | 9240 |
| Period | 1 | 2 | 3 | 5 | 5 | 19 | 19 | 19 |
| 1: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2: | 56 | 0 | 2 | 2+4c2 | 2+4c1 | −1 | −1 | −1 |
| 3: | 56 | 0 | 2 | 2+4c1 | 2+4c2 | −1 | −1 | −1 |
| 4: | 76 | 4 | 1 | 1 | 1 | 0 | 0 | 0 |
| 5: | 76 | −4 | 1 | 1 | 1 | 0 | 0 | 0 |
| 6: | 77 | 5 | −1 | 2 | 2 | 1 | 1 | 1 |
| 7: | 77 | −3 | 2 | 2c1 | 2c2 | 1 | 1 | 1 |
| 8: | 77 | −3 | 2 | 2c2 | 2c1 | 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

| | | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|
| Class | | | | | | | | |
| 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 | −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 | 1 | 0 |
| | 11: | 0 | 0 | −1 | 0 | 0 | 1 | 0 |
| | 12: | 1 | 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 $2\pi$/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. O. 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.

## ALGORITHM 262
## NUMBER OF RESTRICTED PARTITIONS OF N [A1]

J K S McKay (Recd 7 Dec 1964 and 9 Mar 1965)
Computer Unit, University of Edinburgh, Scotland

```
procedure set (p, N), integer N, integer array p,
comment The number of partitions of n with parts less than
  or equal to m is set in p[n, m] for all n, m such that N ≥ n ≥
  m ≥ 0
    REFERENCES
  1 GUPTA, H, GWYTHER, C E, AND MILLER, J C P Tables of
      partitions In Royal Society Mathematical Tables, vol 4,
      Cambridge U Press, 1958
  2 HARDY, G H AND WRIGHT E M The Theory of Numbers
      Ch 19, 4th ed Clarendon Press, Oxford 1960,
begin integer m, n,
  p[0 0] = 1,
  for n = 1 step 1 until N do
  begin p[n, 0] = 0,
    for m = 1 step 1 until n do
      p[n, m] = p[n, m-1] +
        p[n-m, if n-m<m then n-m else m]
  end
end set
```

## ALGORITHM 263
## PARTITION GENERATOR [A1]

J K S McKay (Recd 7 Dec 1964 and 9 Mar 1965)
Computer Unit, University of Edinburgh, Scotland

```
procedure generate (p, N, position, ptn, length),
  integer array p, ptn, integer N, length, position,
comment The partitions of N may be mapped in their natural
  order, 1 − 1, onto the consecutive integers from 0 to P(N)−1
  where P(N)(=p[N, N]) is the number of unrestricted partitions
  of N The array p is set by the procedure set [Algorithm 262,
  Number of Restricted Partitions of N, Comm ACM 8 (Aug
  1965), 493] On entry position contains the integer into which
  the partition is mapped On exit length contains the number of
  parts and ptn[1 length] contains the parts of the partition in
  descending order
    REFERENCE
  1 LITTLEWOOD, D E The Theory of Group Characters Ch 5
      2nd ed Clarendon Press, Oxford, 1958,
begin integer m, n, psn,
  n = N, psn = position, length = 0,
A length = length + 1, m = 1,
B if p[n, m] < psn then begin m = m + 1, go to B end else
    if p[n, m] > psn then
C   begin
      ptn[length] = m, psn = psn − p[n, m−1], n = n − m,
      if n ≠ 0 then go to A, go to D
    end
    else m = m + 1, go to C,
D   end generate
```

## ALGORITHM 264
## MAP OF PARTITIONS INTO INTEGERS [A1]

J K S McKay (Recd 7 Dec 1964 and 9 Mar 1965)
Computer Unit, University of Edinburgh, Scotland

```
integer procedure place(p, n, ptn), value n,
  integer array p, ptn, integer n,
comment place is the inverse of the procedure generate [Al
  gorithm 263, Partition Generator, Comm ACM 8 (Aug 1965),
  493] The array p is set by the procedure set [Algorithm 262,
  Number of Restricted Partitions of N, Comm ACM 8 (Aug
  1965), 493] The procedure produces the integer into which
  the partition of n, stored in descending order of parts in ptn[1]
  onwards, is mapped,
begin integer j, d,
  d = 0
  if n = 0 then go to B,
  j = 0,
A j = j + 1, d = p[n, ptn[j]−1] + d, n = n − ptn[j],
  if n ≠ 0 then go to A,
B place = d
end place
```

# ALGORITHM 371
# PARTITIONS IN NATURAL ORDER [A1]

J. K. S. McKay (Recd. 28 Apr. 1967)
California Institute of Technology, Mathematics Division, Pasadena, CA 91109.

KEY WORDS AND PHRASES: partitions, number theory
*CR* CATEGORIES: 5.39

```
procedure partition (p, k, last); integer n, k;
  integer array p; Boolean last;
comment Partition may be used to generate partitions in their
  natural (reverse lexicographical) order. On entry the first k
  elements of the global integer array p[1:n] should contain a
  partition, p[1] ≥ p[2] ≥ ··· ≥ p[k], of n into k parts. In order to
  initialize m, the first entry must be made with last set true: this
  will result in p[1], p[2], ··· , p[k] and k remaining unaltered and
  last set false on exit. On all subsequent entries with last false, k
  is updated and p[1], p[2], ··· , p[k] will be found to contain the
  next partition of n with parts in descending order. On returning
  with the last partition, p[1] = p[2] = ··· = p[n], last is set
  true. To generate all partitions of n, p[1], k, last should be set
  to n, 1, true, respectively for the initial call: these variables
  must not be altered between successive calls for partition;
begin
  own integer m; integer t;
  if last then
  begin
    last := false;
    for m := 1 step 1 until k do
      if p[m] = 1 then go to c;
    m := k; go to c
  end;
  t := k - m;
  k := m;
  p[m] := p[m] - 1;
a: if p[k] > t then go to b;
  t := t - p[k];
  k := k + 1;
  p[k] := p[k-1];
  go to a;
b: k := k + 1;
  p[k] := t + 1;
  if p[m] ≠ 1 then m := k;
c: if p[m] = 1 then m := m - 1;
  if m = 0 then last := true;
end partition
```

## REMARK ON ALGORITHM 307 [A1]
## SYMMETRIC GROUP CHARACTERS

[J. K. S. McKay, *Comm. ACM 10* (July 1967), 451]

J. K. S. McKay (Recd. 13 Sept. 1967)
Dept. of Computer Science, University of Edinburgh, Edinburgh, Scotland

Three corrections are noted.

(1) Line 39:

**own integer array** *p*[0:*n*,0:*n*];

should be moved to the line after the **begin** in line 32.

(2) At *E* the line should read

*E*: **if** *rep*[*j*2] ≥ (**if** *j*2=*k* **then** 0 **else** *rep*[*j*2+1])
**then go to** *F*;

(3) Three lines, later

*coeff* := −1 *coeff*;

should read

*coeff* := −*coeff*;

# ALGORITHM 307
# SYMMETRIC GROUP CHARACTERS [A1]

J K S McKay (Recd 23 Sept 1966, 15 Feb 1967, and 10 Mar 1967)
Department of Computer Science, University of Edinburgh, Edinburgh, Scotland

```
integer procedure character (n, rep, longr, class, longc, first),
  value n rep, longr, class, longc,
  integer n, longr, longc, Boolean first,
  integer array rep, class,
comment character produces the irreducible character of the
  symmetric group corresponding to the partitions of the repre
  sentation and the class of the group S_n stored with parts in
  descending order in arrays rep[1 longr] and class[1 longc], re
  spectively Both arrays are preserved The method is similar
  to that described by Bivins et al [1] Comét describes a later
  method
    On first entry to character first should be set true in order to
  initialize the own array p[0 n, 0 n] This single initialization is
  sufficient for all symmetric groups of degree less than or equal
  to n character is intended for computing individual characters
  If a substantial part of the character table is required it is sug
  gested that procedure generate [Algorithm 263, Comm ACM
  8 (Aug 1965), 493)] be used to produce the partitions prior to
  use of character If this is done, then the own array p should be
  replaced by a suitable global array, and first should be set false
  to avoid unwanted initialization character uses procedures set,
  generate, and place [Algorithms 262, 263 264, Comm ACM 8
  (Aug 1965), 493]
```

REFERENCES

1 BIVINS, R L, METROPOLIS, N STEIN, P R, and WELLS M B Characters of the symmetric groups of degree 15 and 16 *MTAC 8* (1954), 212–216
2 LITTLEWOOD, D E *The Theory of Group Characters* Claren don Press Oxford, England 1958, 2d ed, Ch 5
3 COMÉT, S Improved methods to calculate the characters of the symmetric group *MTAC 14* (1960), 104–117

```
begin
  integer procedure degree (n rep, length)  value n length
    integer n, length, integer array rep
  comment degree gives the degree of the representation of the
    symmetric group on n symbols defined by the partition
    rep[1 length] with parts in descending order,
  begin
  own integer array p[0 n, 0 n]
    integer array q[1 length], integer i j, deg
    integer procedure fac(n), value n, integer n,
    fac = if n = 1 then 1 else n × fac(n−1),
    for i = 1 step 1 until length do
      q[i] = rep[i] + length − i
    deg = fac(n)
    for i = 1 step 1 until length do
    for j = i + 1 step 1 until length do
      deg = deg × (q[i]−q[j]),
    for i = 1 step 1 until length do
      deg = deg − fac(q[i]),
    degree = deg
  end degree,
  if first then
    begin set (p, n), first = false end,
  begin
    integer array pr[1 n], r[0 1, 0 p[n, n]−1],
    integer length, m, t old, new, index, i, char, k, coeff, u, pos,
      j1, j2,
    m = longc,
    new = n,
    index = 1,
    for i = 0 step 1 until p[n, n] − 1 do
      r[index, i] = 0,
    r[index, place(p, n, rep)] = 1,
    for t = 1 step 1 until m do
    begin if class[t] = 1 then go to identity,
      index = 1 − index, old = new, new = new − class[t],
      for i = 0 step 1 until p[new new] − 1 do
        r[index i] = 0,
      for u = p[old, old] − 1 step − 1 until 0 do
      begin if r[1 − index, u] = 0 then go to B,
        generate (p old, u, pr, length),
        k = length, j1 = 1
G       j2 = j1, coeff = r[1−index, u],
        for i = 1 step 1 until k do rep[i] = pr[i],
        if rep[1] = old then go to H,
        rep[j2] = rep[j2] − class[t],
        if rep[j2] + k − j2 < 0 then go to B,
E       if rep[j2] ≥ if (j2 = k then 0 else rep[j2+1]) then go to F,
        if rep[j2+1]= rep[j2] + 1 then go to J,
        i = rep[j2+1], rep[j2+1] = rep[j2] + 1,
        rep[j2] = i − 1, coeff = − 1 coeff, j2 = j2 + 1,
        go to E,
H       rep[1] = rep[1] − class[t]
F       pos = place(p, new, rep)
        r[index pos] = r[index, pos] + coeff,
J       j1 = j1 + 1, if j1 ≤ k then go to G,
B
      end
    end
A   char = r[index 0], go to Z,
identity  char = 0,
    for u = p[new,new] − 1 step − 1 until 0 do
    begin if r[index, u] = 0 then go to BB,
      generate(p new, u, pr, length),
      char = char + r[index u] × degree (new, pr, length),
BB
    end
Z   character = char
  end
end character
```

## On the Evaluation of Multiplicative Combinatorial Expressions

Key Words and Phrases: combinatorial expressions
*CR* Categories: 5.30

EDITOR:

Evaluating multiplicative arithmetic expressions that arise in combinatorial theory (multinomial coefficients, probabilities, and coupling coefficients) by straightforward computation can lead to difficulties with overflow even when the magnitude of the final result is representable. The method suggested here is fast and does not cause unnecessary overflow. It can be used in formulae involving integer factors not greater than some given $N$ (a typical value of 52 occurs in problems concerning the distribution of playing cards).

Three arrays are declared—*ex*, *hfac*, *lfac*[2:*N*]. *ex*[*n*] contains the exponent of $n$ in the result For all $n$, *hfac*[*n*] contains the largest prime factor of $n$ and *lfac*[*n*] contains $n \div hfac[n]$.

To begin, zero the array *ex* and set up the factors in *lfac* and *hfac*. Evaluate the expression by modifying the exponents in *ex*. For example, to divide by *k*!:

**for** *i* := 2 **step** 1 **until** *k* **do** *ex*[*i*] := *ex*[*i*] − 1;

When the result is complete, decompose the composite integer factors in decreasing order of magnitude into their prime factors. The final numerical result may then be obtained. The result is an integer if the exponents are all nonnegative (and no division will be required) otherwise the result is a rational fraction reduced to primitive form.

```
comment if den is 1 the result is num, otherwise the result is
  a rational fraction = num/den;
  num := 1;
  den := 1;
  for k := N step −1 until 2 do begin if ex[k]≠0
then begin
      if lfac[k] > 1 then
        begin
          ex[hfac[k]] := ex[hfac[k]] + ex[k];
          ex[lfac[k]] := ex[lfac[k]] + ex[k];
          ex[k] := 0; goto A;
        end;
      if ex[k] > 0 then num := num × k↑ex[k];
      if ex[k] < 0 then den := den × k↑ (−ex[k])
    end else A: end
```

I wish to thank the referee for his helpful suggestions and the ALGOL example

J. K. S. MCKAY,
*Atlas Computer Laboratory*
*Science Research Council, Chilton*
*Didcot, Berkshire, England*

# On the Representation of Symmetric Polynomials

J. K. S. McKay
*University of Edinburgh, Scotland*

Relations are given between certain symmetric polynomials in the light of the theory of the symmetric group. Such an approach unifies earlier work and lends insight to previously published work by Aaron Booker. A generalization of Graeffe's root-squaring technique for the determination of the roots of a polynomial is suggested.

## 1. Introduction

Relations between certain symmetric polynomials are given in [1] without reference to the characters of the symmetric group or the Schur functions related to them. Details of the group theory involved may be found in [2] and [3]. The algebra is developed further in [4].

A knowledge of the characters of the symmetric group is required for the evaluation of the coefficients occurring in the relations. Tables connecting various symmetric functions are found in [5], by David, Kendall, and Barton; these tables are for statistical use and contain no reference to the symmetric group. Symmetric group character tables are found in [2] for degrees up to 10, in [8] references are given for tables of degree less than or equal to 20. An ALGOL algorithm is given which produces characters of the symmetric group subject to storage limitations only.

## 2. Explicit Formulas for Certain Relations

The coefficients expressing the unitary symmetric polynomials $(1^n)$ (Booker's $Es$) in terms of products of the symmetric power sums $(n_i)$ (Booker's $As$) may be computed directly.

We may characterize each product of power sums occurring in the expression for $(1^n)$ by a partition of $n, \rho = \rho_1, \rho_2, \rho_3, \cdots, \rho_m$, where $\rho_k$ is associated with $A_k$ thus, e.g., $A_1^2 A_3$ is associated with the partition 3, 1, 1 (or 3, $1^2$) of 5. Each partition may be identified with a conjugacy class of the symmetric group.

Let the number of elements of the conjugacy class $C_\rho$ in the symmetric group on $n$ symbols be $h_\rho$. Then

$$h_\rho = \frac{n!}{1^\alpha \alpha!\, 2^\beta \beta! \cdots q^\omega \omega!} \tag{1}$$

where $\rho = 1^\alpha, 2^\beta, \cdots, q^\omega$.

Let $\chi_\rho = +1$ if $\rho$ has an even number of even parts and let $\chi_\rho = -1$ if $\rho$ has an odd number of even parts; i.e., $\chi_\rho$ is the alternating character of the symmetric group. Then

$$(1^n) = \frac{1}{n!} \sum_\rho h_\rho \chi_\rho A_\rho \tag{2}$$

where $A_\rho$ is the product of the power sums $(\rho_i)$. This is a special case, $\lambda = 1^n$, of the definition of the Schur function $\{\lambda\}$ as $(1/n!) \sum_\rho h_\rho \chi_\rho^\lambda A_\rho$.

The orthogonality relations noted by Booker are consequences of the fact that the rows of his table are the permutation characters of the coset representation induced on $S_5$ by the direct product of the symmetric groups given by the powers occurring in the typical expression of degree 5 for that row, e.g., from the *second* row and *fourth* column of Booker's table we can see that two left (right) cosets of $S_4 \times S_1$ are left invariant on pre-(post-) multiplication by any element of $S_5$ with cycle structure 3,1,1. The alternating representation will be included when the direct product is contained in the alternating group. This will occur only when the subgroup is the identity; i.e., the last row of the table.

Knowledge of the character table and the compound characters mentioned above is adequate to determine many relations between the symmetric polynomials.

The compound character may be found directly as in [2] giving

$$\phi_\rho^\lambda = \sum \frac{\alpha!}{\alpha_1!\,\alpha_2!\cdots}\,\frac{\beta!}{\beta_1!\,\beta_2!\cdots} \cdot \frac{\gamma!}{\gamma_1!\,\gamma_2!\cdots}\cdots\frac{\omega!}{\omega_1!\,\omega_2!\cdots}, \tag{3}$$

the summation being over all separations of $\rho$ satisfying

$$\alpha_i + 2\beta_i + 3\gamma_i + \cdots = \lambda_i,$$

$$\sum\alpha_i = \alpha,\ \sum\beta_i = \beta,\ \sum\gamma_i = \gamma,\ \cdots,\ \sum\omega_i = \omega$$

where $\rho = 1^\alpha, 2^\beta, 3^\gamma \cdots, q^\omega$ and $\lambda = \lambda_1, \lambda_2, \cdots, \lambda_p$ are partitions of $n$. $\phi_\rho^\lambda$ is the number of times expressions of the form $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_p^{\lambda_p}$ occur in $A_\rho$. Let us take as an example $S_3$, the symmetric group on 3 symbols. In general, for degree $n$ we have relations involving matrices of order $p(n)$, the number of partitions of $n$, since each suffix corresponds to a partition of $n$.

The suffices $i, j$ are the ordinal numbers of the partitions when taken in natural order.

$$\begin{bmatrix} A_1^3 \\ A_2A_1 \\ A_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 1 \end{bmatrix}\begin{bmatrix} \{3\} \\ \{2,1\} \\ \{1^3\} \end{bmatrix} \quad \text{where the entries are the simple characters } \chi_i^j \text{ of } S_3. \tag{4}$$

This may be inverted to obtain:

$$3!\begin{bmatrix} \{3\} \\ \{2,1\} \\ \{1^3\} \end{bmatrix} = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 0 & -2 \\ 1 & -3 & 2 \end{bmatrix}\begin{bmatrix} A_1^3 \\ A_2A_1 \\ A_3 \end{bmatrix} \quad \text{with entries } h_j\chi_j^i. \tag{5}$$

By computing $\phi_j^i$ we obtain

$$\begin{bmatrix} A_1^3 \\ A_2A_1 \\ A_3 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 6 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} \sum x_1^3 \\ \sum x_1^2x_2 \\ \sum x_1x_2x_3 \end{bmatrix} \quad \text{with entries } \phi_i^j. \tag{6}$$

From (4) and (6) we may derive the other equations by inversion and multiplication. An alternative approach is to derive (8) from the algorithm [11] given here.

$$3!\begin{bmatrix} \sum x_1^3 \\ \sum x_1^2x_2 \\ \sum x_1x_2x_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 6 \\ 0 & 6 & -6 \\ 1 & -3 & 2 \end{bmatrix}\begin{bmatrix} A_1^3 \\ A_2A_1 \\ A_3 \end{bmatrix} \tag{7}$$

hence by multiplication of (7) by (4)

$$\begin{bmatrix} \sum x_1^3 \\ \sum x_1^2x_2 \\ \sum x_1x_2x_3 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \{3\} \\ \{2,1\} \\ \{1^3\} \end{bmatrix} \tag{8}$$

and multiplying (5) by (6)

$$3!\begin{bmatrix} \{3\} \\ \{2,1\} \\ \{1^3\} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \sum x_1^3 \\ \sum x_2x_1^2 \\ \sum x_1x_2x_3 \end{bmatrix} \tag{9}$$

where the entries are the multiplicities of the irreducible characters $\chi^j$ in $\phi^i$.

## 3. Algorithms and Possible Applications

Two algorithms [10, 11] are given which, together, enable the tables given above to be computed.

The first algorithm computes the character $\chi_\rho^\lambda$ from the partitions $\lambda$ and $\rho$; the second is written in such a way as to express $\sum x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ in terms of the Schur functions and then express these as determinants in the coefficients of the monic polynomial with roots $x_i$. By this means the coefficients of the polynomial having as roots the $k$th powers of the roots of a given polynomial may be deduced. The method is found in [2]. This is a generalization of root-squaring. An analysis, which may be easily generalized, of Graeffe's method is found in [9].

Further work on root-powering is found in Kostovskii's thesis, Lvov University, and in [6] and [7].

RECEIVED JANUARY, 1966; REVISED SEPTEMBER, 1966

REFERENCES


1. BOOKER, A. Numerical evaluation of symmetric polynomials. *J. ACM 12* (1965), 90–95.
2. LITTLEWOOD, D. E. *The Theory of Group Characters*. Clarendon Press, Oxford, England, 1940.
3. ROBINSON, G. DE B. *Representation Theory of the Symmetric Group*. Edinburgh University Press, Edinburgh, Scotland, 1961.
4. MORRIS, A. O. On an algebra of symmetric functions. *Quart. J. Math. 16* (1965), 53–64.
5. DAVID, F. N., KENDALL, M. G., AND BARTON, D. E. *Symmetric Functions and Allied Tables*. Cambridge University Press, Cambridge, England, 1966.
6. KOSTOVSKII, A. N. A method of numerical solution of algebraic equations with roots of equal modulus *Soviet Math. 1* (1960), 225–228.
7. ——. The determination of strict inequalities between the moduli of roots in the transformation of algebraic equations by the Lobatchevskii-Graeffe method. *Soviet Math. 3* (1962), 1587–1589.
8. COMÉT, STIG. Calculation of the characters of the symmetric group. *Math. Tables Aids Comput. 14*, 70 (April, 1960).
9. GRAM, C. (ED.) *Selected Numerical Methods*. Regnecentralen, Copenhagen, 1962.
10. MCKAY, J. K. S. Algorithm 307. *Comm ACM 10*, 7 (July, 1967), 451–452.
11. BRATLEY, P., AND MCKAY, J. K. S. Algorithm 305. *Comm. ACM 10*, 7 (July, 1967), 450.