J. Symbolic Computation (1986) **2**, 45–50

On the Computation of Group Characters

M. D. ATKINSON† AND R. A. HASSAN‡

† *School of Computer Science, Carleton University, Ottawa;*
‡ *Department of Computer Science,*
University of Baghdad, Al-Jadriya, Baghdad

(*Received* 9 *July* 1984)

Computational methods for finding the character table of a finite group require a stock of reducible characters and techniques for decomposing these characters into irreducible characters. A method for generating reducible characters from a representation of a group is proposed. Several new techniques for computing the irreducible decompositions of a set of characters are given; these techniques extend earlier results of Conway and M. Guy.

1. Introduction

For several years the most successful computational systems for calculating the character table of a large finite group have operated in two stages. In the first stage a set of (in general, reducible) characters is generated from a stock of one or more initially given characters. In the second stage, irreducible characters are found by decomposing these irreducible characters. These two stages are iterated with a user providing fine tuning interactively. Many techniques and examples are given in Conway (1984) and Neubüser *et al.* (1984). The purpose of this paper is to present some extensions and variations of these techniques. In section 2 we make some comments, additional to those of Neubüser *et al.* (1984), on character generation. In section 3 we propose extensions to the reduction techniques discussed in Conway (1984).

2. Character Generation

A frequently used method for obtaining characters is to form the various symmetrised powers of a character. This requires a knowledge of "power maps". If a matrix representation of the group is available some of these characters can be found without knowing the power maps as the following result shows.

THEOREM. *Let R be a t-dimensional representation of a group G afforded by the action of G on a vector space V. Let $R^{(s)}$ be the natural action of G on the sth exterior power of V and let $\varphi^{(s)}$ be the associated character. Then, for every $g \in G$,*

$$\sum_{s=0}^{t} \varphi^{(s)}(g)\lambda^s = \det(\mathrm{I}+\lambda R(g)).$$

PROOF. Let $g \in G$ be fixed, and let $v_1, v_2, \ldots, v_t$ be a basis of V consisting of eigenvectors of $R(g)$. Then $R(g)$ is diagonal with eigenvalues $w_1, w_2, \ldots, w_t$, say. From the definition of

0747–7171/86/010045+06 $03.00/0

$R^{(s)}(g)$ this matrix is also diagonal with diagonal entries which are products $w_{i(1)}w_{i(2)}\ldots w_{i(s)}$ and therefore

$$\varphi^{(s)}(g) = \sum w_{i(1)}w_{i(2)}\ldots w_{i(s)}$$

(summed over all s-tuples with $i(1) < i(2) < \ldots < i(s)$). Hence

$$\begin{aligned}\sum_{s=0}^{t} \varphi^{(s)}(g)\lambda^s &= \sum_{s=0}^{t} \sum w_{i(1)}w_{i(2)}\ldots w_{i(s)}\lambda^s \\ &= (1+w_1\lambda)(1+w_2\lambda)\ldots(1+w_s\lambda) \\ &= \det(I+\lambda R(g)).\end{aligned}$$

In the case of a permutation group the generating function takes the form

$$(1+\lambda)^{a_1}(1-\lambda^2)^{a_2}(1+\lambda^3)^{a_3}(1-\lambda^4)^{a_4}\ldots,$$

where the cycle structure of the permutation g is $1^{a_1}\,2^{a_2}\,3^{a_3}\ldots$. Curiously, the polynomial obtained from this one by replacing all minus signs by plus signs is also the generating function of a set of character values at g. In fact, more generally, the multivariate polynomial

$$\left(\sum x_i\right)^{a_1}\left(\sum x_i^2\right)^{a_2}\left(\sum x_i^3\right)^{a_3}\ldots \text{(summations over a fixed range } 1,\ldots,k)$$

is also the generating function of a set of character values at g. This follows from the Polya–Redfield theory of enumeration.

3. Character Reduction

In this section we shall suppose that we are given a set S of characters $\varphi_1,\ldots,\varphi_n$ of a group G from which we wish to obtain some or all of the set $\chi_1,\ldots,\chi_s$ of s irreducible characters by forming appropriate linear combinations of $\varphi_1,\ldots,\varphi_n$. At our disposal we have the matrix of inner products $m_{ij} = (\varphi_i, \varphi_j)$. In many cases rather more information might be available, in particular the Schur indicators of $\varphi_1,\ldots,\varphi_n$, but we intend here mainly to consider how inner product information is used.

It is elementary to prove that, if $n = s$ and $\det M = 1$, every irreducible character can be realised as an integral combination of $\varphi_1,\ldots,\varphi_n$. When $\det M = 1$ or is moderately small it is probably worth investing a lot of effort searching for the correct integral combinations. Of course, one does not try integral combinations at random. A simple strategy (*Euclidean reduction*) was suggested by Conway (1984). One takes the characters in pairs φ_i, φ_j; if their inner product matrix

$$\begin{pmatrix} a & h \\ h & b \end{pmatrix}$$

has $|h| > a/2$ or $|h| > b/2$, then there is a generalised character in the integral span of φ_i, φ_j which has smaller norm than one of them; then one of φ_i and φ_j can be replaced by this generalised character. This is repeated until no further norm reduction is possible. Euclidean reduction is effective in many cases for producing characters of norm 1, but it can also fail badly.

EXAMPLE. If $n=5$ and the inner product matrix is

$$M=\begin{pmatrix} 2 & 1 & -1 & 1 & -1 \\ 1 & 2 & 0 & -1 & 1 \\ -1 & 0 & 2 & 0 & -1 \\ 1 & -1 & 0 & 3 & 1 \\ -1 & 1 & -1 & 1 & 87 \end{pmatrix},$$

then $\det M=1$, but Euclidean reduction allows no norm reduction even though φ_5 has norm 87. Note that M is certainly a possible matrix of inner products since the matrix

$$A=\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & 1 & 0 \\ 4 & -5 & 6 & 3 & 1 \end{pmatrix}$$

satisfies $M=AA^T$.

Euclidean reduction is obviously optimal when $n=2$. For $n=3$ and small $\det M$ it is also a reasonable strategy since we have

LEMMA. *Let M be the matrix of inner products of 3 generalised characters*

$$M=\begin{pmatrix} a & f & g \\ f & b & h \\ g & h & c \end{pmatrix}$$

with $a\leqslant b\leqslant c$ and $|f|\leqslant a/2$, $|g|\leqslant a/2$, $|h|\leqslant b/2$ (the latter 3 inequalities are the condition that no Euclidean reduction is possible). Then, if M is non-singular, a, b, c are bounded in terms of $\det M$. Moreover, if M is unimodular, then $M=I$.

PROOF. The lemma follows by writing $4\times\det M$ as

$$ab(c-b)+a(b^2-4h^2)+ab(c-a)+b(a^2-4g^2)+ac(b-a)+c(a^2-4f^2)+(abc+8fgh)$$

and noting that each of the seven summands is non-negative.

If we are unable to find all the irreducible characters as integral combinations of $\varphi_1, \ldots, \varphi_n$, either because M is not unimodular or for some other reason, we have to prepare for a time-consuming search for possible character decompositions of $\varphi_1, \ldots, \varphi_n$ consistent with M. It was recommended by Conway (1984) and our own experience supports it, that the calculations should use proper characters only; we should return to the originally given set S and discard any improper characters which may have been introduced. The execution time of the search will depend crucially on the norms of the φ_i. These norms should be as small as possible and it is advisable to invest some effort in reducing them. A strategy broadly similar to Euclidean reduction can be used. Here we search for pairs φ_i, φ_j for which $\varphi_i\subseteq\varphi_j$ (that is, $\varphi_j-\varphi_i$ is a proper character). Whenever such a pair is found we replace φ_j by $\varphi_j-\varphi_i$. This strategy is made possible by the following result of M. Guy (in Conway, 1984).

LEMMA. *Let α, β be characters with inner product matrix*

$$\begin{pmatrix} a & h \\ h & b \end{pmatrix}.$$

If $a \leqslant b$ and $ab - h^2 < b$, then $\alpha \subseteq \beta$.

This lemma is optimal in that if the inequalities on a, b, h do not hold, then there exists a group having two characters α, β with these inner products for which $\alpha \subseteq \beta$ is false. However, the lemma does not make optimal use of all the inner product information.

EXAMPLE. Suppose that three characters α, β, γ have inner product matrix

$$M = \begin{pmatrix} 9 & 1 & 11 \\ 1 & 2 & 3 \\ 11 & 3 & 16 \end{pmatrix}.$$

This is a possible matrix of inner products since, for example, $M = AA^T$ where

$$A = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 1 & 2 & 2 & 1 \end{pmatrix}.$$

Guy's criterion applies to neither of the pairs $\{\alpha, \gamma\}$ and $\{\beta, \gamma\}$; however, these inner products imply that $\alpha + \beta \subseteq \gamma$ which is stronger than $\alpha \subseteq \gamma$ and $\beta \subseteq \gamma$.

In general one can exploit the other inner product information through

THEOREM. *Let α, β, γ be characters with inner product matrix*

$$M = \begin{pmatrix} a & h & p \\ h & b & q \\ p & q & m \end{pmatrix}$$

and suppose that $a \leqslant b$ and $p \leqslant q$ (necessary conditions that $\alpha \subseteq \beta$). Suppose that the quadratic

$$[(a+b-2h-1)m-(q-p)^2]x^2 + 2x[aq+bp-hp-hq-q] + [ab-h^2-b]$$

takes a negative value for some $x \geqslant 0$. Then $\alpha \subseteq \beta$.

PROOF. For any x, $\alpha + \gamma x$ and $\beta + \gamma x$ are class functions whose inner product matrix is

$$\begin{pmatrix} A & H \\ H & B \end{pmatrix} = \begin{pmatrix} a+2px+mx^2 & h+(p+q)x+mx^2 \\ h+(p+q)x+mx^2 & b+2qx+mx^2 \end{pmatrix}.$$

For $x \geqslant 0$ we have $A \leqslant B$. The proof of Guy's lemma given by Conway (1984) requires only that 'α' and 'β' in that lemma be positive class functions whose difference is a generalised character. Hence, if $AB - H^2 - B < 0$ for some $x \geqslant 0$, we can deduce that $\alpha + \gamma x \subseteq \beta + \gamma x$ and hence that $\alpha \subseteq \beta$. However, $AB - H^2 - B$ is precisely the quadratic given in the theorem.

COROLLARY. *With the same notation, suppose that $a \leqslant b$, $p \leqslant q$ and $(a+b-2h)m - (q-p)^2 < m$. Then $\alpha \subseteq \beta$. Moreover, the character $\beta - \alpha$ contains or is contained in γ according as $a+b-2h \geqslant m$ or $a+b-2h \leqslant m$.*

PROOF. The first part follows directly from the theorem (it states that the coefficient of x^2 is negative). For the second part note that the inner product matrix of the characters $\beta-\alpha$ and γ is

$$\begin{pmatrix} a+b-2h & q-p \\ q-p & m \end{pmatrix}$$

and apply Guy's lemma.

Although the theorem seems, in practice, to be very effective in proving that $\alpha \subseteq \beta$ (whenever this can be deduced from the inner products) it is not optimal. To see this consider the inner product matrix

$$M = \begin{pmatrix} 11 & 13 & 3 \\ 13 & 17 & 5 \\ 3 & 5 & 14 \end{pmatrix}$$

of three characters α, β, γ. The quadratic of the theorem is $10x^2-6x+1$ which is everywhere positive. On the other hand a case by case analysis shows that $\alpha \subseteq \beta$ in all possible irreducible decompositions of α, β, γ (there are several).

In Atkinson & Hassan (1983) an even more general condition is given which uses all the inner products involving one of α and β in the inner product table.

Before leaving these considerations arising out of Guy's lemma we shall point out one further direction in which it may be generalised. To say that $\alpha \subseteq \beta$ is to say that every irreducible character has multiplicity in α at most equal to its multiplicity in β. If we cannot establish that $\alpha \subseteq \beta$ it is sometimes useful to know how closely the condition can fail, that is, how many of α's multiplicities are greater than β's and by how much.

MULTIPLICITY LEMMA. *Let α, β be characters with inner product matrix*

$$\begin{pmatrix} a & h \\ h & b \end{pmatrix}$$

and suppose that $0 < a \leqslant b$. Of the irreducible characters $\chi_1, \ldots, \chi_s$, let $\chi_1, \ldots, \chi_t$ have greater multiplicity in α than in β. Write

$$\alpha = c_1\chi_1 + \ldots + c_t\chi_t + \alpha_2$$

$$\beta = d_1\chi_1 + \ldots + d_t\chi_t + \beta_2$$

where $c_i > d_i$, and $(\chi_i, \alpha_2) = (\chi_i, \beta_2) = 0$ for $i = 1, \ldots, t$. Then

$$\sum (c_i - d_i)^2 \leqslant (ab - h^2)/b.$$

Moreover, if equality holds, then $d_i = 0$ for $i = 1, \ldots, t$ and α_2 and β_2 are multiples of some character θ.

PROOF. If we write

$$\alpha = \alpha_1 + \alpha_2, \qquad \beta = \beta_1 + \beta_2,$$

then obviously

$$(\alpha_1, \alpha_2) = (\alpha_1, \beta_2) = (\beta_1, \alpha_2) = (\beta_1, \beta_2) = 0.$$

By direct calculation we have the following identity:

$$\begin{aligned}(\alpha_2, \alpha_2)(\beta_2, \beta_2) - (\alpha_2, \beta_2)^2 = {} & (\alpha, \alpha)(\beta, \beta) - (\alpha, \beta)^2 - (\beta, \beta)(\alpha_1 - \beta_1, \alpha_1 - \beta_1) \\ & - [(\beta, \beta) - (\alpha, \alpha)](\alpha_1 - \beta_1, \beta_1) \\ & - (\alpha_2 - \beta_2, \alpha_2 - \beta_2)(\alpha_1, \beta_1) \\ & - (\alpha_1, \alpha_1 - \beta_1)(\beta_1, \alpha_1 - \beta_1).\end{aligned}$$

The left-hand side of this identity is non-negative since the quadratic form $(x\alpha_2+y\beta_2, x\alpha_2+y\beta_2)$ is positive semi-definite. The right-hand side is

$$\begin{aligned} ab-h^2-b\sum(c_i-d_i)^2-(b-a)(\alpha_1-\beta_1,\beta_1)-(\alpha_2-\beta_2,\alpha_2-\beta_2)(\alpha_1,\beta_1) \\ -(\alpha_1,\alpha_1-\beta_1)(\beta_1,\alpha_1-\beta_1) \\ \leqslant ab-h^2-b\sum(c_i-d_i)^2 \quad \text{since} \quad \beta_1\subseteq\alpha_1. \end{aligned}$$

This proves the first part of the lemma. If equality holds, then the form $(x\alpha_2+y\beta_2, x\alpha_2+y\beta_2)$ has a zero and therefore α_2 and β_2 are dependent. Moreover, $(\beta_1, \alpha_1-\beta_1)=0$ from which it follows that $\beta_1=0$, and the second part is also proved.

This lemma can also be strengthened to take into account inner products of α and β with other characters (see Atkinson & Hassan (1985) for details).

Conway (1984) describes how Guy has extended his inclusion lemma to exploit the Schur indicators (which often are available). This extension is not just a simple numerical test; in fact it requires possibly several applications of the Euclidean reduction algorithm. As the next example shows, the multiplicity lemma is effective in cutting down the number of runs of this algorithm.

EXAMPLE. Suppose that α, β have inner product matrix

$$\begin{pmatrix} 21 & 31 \\ 31 & 50 \end{pmatrix}$$

and that i, j are the (known) Schur indicators of α, β. Guy's original criterion does not apply so we cannot deduce immediately that $\alpha\subseteq\beta$. However, $1\leqslant(ab-h^2)/b<2$ and so, if $\alpha\subseteq\beta$ does not hold, the lemma shows that there is (precisely) one irreducible character χ whose multiplicity in α is $y+1$ and whose multiplicity in β is y. The inner product matrix of $\alpha-(y+1)\chi$ and $\beta-y\chi$ is

$$\begin{pmatrix} 21-(y+1)^2 & 31-y(y+1) \\ 31-y(y+1) & 50-y^2 \end{pmatrix}$$

and this is positive definite only if $y=0$. Suppose the indicator of χ is k $(=-1, 0, 1)$. Then $\alpha-\chi$ and β have inner product matrix

$$\begin{pmatrix} 20 & 31 \\ 31 & 50 \end{pmatrix}$$

and their indicators are $i-k$ and j. Guy's technique (see Conway (1984) where this matrix is considered) shows that

$$|j-i+k|\leqslant 8, \quad |2i-2k-j|\leqslant 6, \quad |3i-3k-2j|\leqslant 8.$$

Since we know i and j it is trivial to check whether one of $k=-1, 0, 1$ satisfies these inequalities. If no such k exists we can conclude $\alpha\subseteq\beta$.

References

Atkinson, M. D., Hassan, R. A. (1983). Some techniques for group character reduction, Technical Report 30, School of Computer Science, Carleton University.

Conway, J. H. (1984). Character calisthenics. In: *Computational Group Theory*, pp. 249–266. London: Academic Press.

Neubüser, J., Pahlings, H., Plesken, W. (1984). CAS; design and use of a system for the handling of characters of finite groups. In: *Computational Group Theory*, pp. 195–247. London: Academic Press.