SOME TECHNIQUES FOR GROUP CHARACTER REDUCTION

M. D. Atkinson*
R. A. Hassan**

SCS-TR-30
August 1983

* School of Computer Science, Carleton University, Ottawa, K1S 5B6, Canada.

** Department of Computing Mathematics, University College, Cardiff, U.K.

This research was supported by the Natural Sciences and Engineering Research Council of Canada.

Abstract. Computer packages for determining the irreducible characters of a finite group commonly generate many reducible characters and try to decompose them. Methods are given here to ease this decomposition. They use only inter-character inner product information.

SOME TECHNIQUES FOR GROUP CHARACTER REDUCTION

M.D. ATKINSON and R.A. HASSAN

Although there exist many algorithms for obtaining information about a given finite group (for a survey, see [4]) the problem of finding all the irreducible characters of the group has not yet been satisfactorily solved. A general algorithm for this problem was given by Dixon [2]; it requires very explicit information about the group and works well only for small groups (of order up to about one thousand).

For large groups the computational methods which are used in practice are a mixture of simple-minded theory and haphazard inspiration. A very complete account of existing theory and trickery is given by Neubüser [3] in his description of the CAS system. We are indebted to him for making this available to us in pre-print form and for many other kindnesses. To set the scene for the results in this paper, we sketch below the general philosophical tradition which CAS and most other character theory systems follow.

One is given enough information about a finite group G that one can compute its number of conjugacy classes, their sizes, and class representatives. One is also given a small stock of characters ideally (but not necessarily) irreducible. Then one computes new characters by forming tensor products, symmetrised tensor products, inducing from subgroups (if possible), and restricting from overgroups. The result will be a large number of characters $\phi_1, \phi_2, \ldots, \phi_n$. The available information is just the inner product table (ϕ_i, ϕ_j) and perhaps the Schur indicators of $\phi_1, \phi_2, \ldots, \phi_n$. Of course in any particular case there may well be other exploitable information but in this paper we will consider simply how one might use the inner product information.

Let us therefore imagine that we somehow know characters $\phi_1, \phi_2, \ldots, \phi_n$ of G and we have a table $M = (m_{ij})$ of inner products $m_{ij} = (\phi_i, \phi_j)$. Then of course each ϕ_i has the form

$$\phi_i = \sum_{j=1}^{s} r_{ij} \chi_j$$

where $\chi_1, \chi_2, \ldots, \chi_s$ are the irreducible characters and every r_{ij} is a non-negative integer. The orthonormality of the irreducible characters implies that

$$M = RR^T$$

where R is the $n \times s$ matrix (r_{ij}). If we are able to find the matrix R then we have a good chance of finding one of the irreducible characters χ_k as a linear combination of $\phi_1, \phi_2, \ldots, \phi_n$. In fact the equation

$$\sum_{i=1}^{n} t_i \phi_i = \chi_k$$

is equivalent to the linear system of s equations

$$\sum_{i=1}^{n} t_i r_{ij} = \delta_{kj} , \quad j = 1, 2 \ldots s$$

in unknowns $t_1, t_2, \ldots, t_n$. Even when rank $R < s$ there may be some values of k for which a solution exists.

Solving these equations is straightforward but finding the matrix R is generally rather difficult because it demands a backtracking search with the consequent combinatorial explosion. Comments on this computation may be found in [3] and we shall remark here only that the character norms $m_{ii} = (\phi_i, \phi_i)$ should be small for the method to have the best chance of success. Consequently any preprocessing to reduce the norms of the stock of available characters is likely to be worthwhile. In [1] (which largely inspired our own efforts) the following handy criterion due to M. Guy was given.

LEMMA Let α, β be (proper) characters with inner product matrix $\begin{bmatrix} a & h \\ h & b \end{bmatrix}$, i.e. $a = (\alpha,\alpha)$, $b = (\beta,\beta)$, $h = (\alpha,\beta)$. Suppose that $0 < a \leq b$. If $ab-h^2 < b$ then $\alpha \leq \beta$ (i.e. $\beta-\alpha$ is a proper character). If $ab-h^2 = b$ then either $\alpha \leq \beta$ or we have

$$\alpha = \chi + m\theta \ , \ \beta = p\theta$$

where χ, θ are characters and χ is irreducible, $(\chi,\theta) = 0$, and m and p are positive integers.

This lemma is intended to be applied repeatedly to pairs of characters α, β among $\phi_1,\ldots,\phi_n$; whenever we can deduce that $\alpha \leq \beta$ we would replace β by $\beta-\alpha$.

The strong conclusion of Guy's lemma can only be obtained through the strong hypothesis on $ab-h^2$. The following theorem shows that from a weaker hypothesis one can still win information which may reduce the scale of the backtracking search. The result gives an indication of how badly the condition $\alpha \leq \beta$ may fail.

THEOREM 1 Let α,β be characters with inner product matrix $\begin{bmatrix} a & h \\ h & b \end{bmatrix}$ and suppose that $0 < a \leq b$. Of the irreducible characters $\chi_1, \chi_2,\ldots,\chi_s$ let $\chi_1, \chi_2,\ldots \chi_t$ have greater multiplicity in α than in β .

Suppose that

$$\alpha = \sum_{i=1}^{t} c_i \chi_i + \alpha^*$$

$$\beta = \sum_{i=1}^{t} d_i \chi_i + \beta^*$$

where $c_i > d_i$, $(\chi_i, \alpha^*) = (\chi_i , \beta^*) = 0$ for $i = 1, 2, \ldots, t$.

Then

$$\Sigma \; (c_i - d_i)^2 \leq (ab - h^2)/b \;.$$

Moreover if equality holds then $d_i = 0$ for $i = 1, 2, \ldots, t$ and α^*, β^* are multiples of some character θ .

Proof. From the equations defining α^*, β^* it follows that the inner product matrix for α^*, β^* is $\begin{bmatrix} a^* & h^* \\ h^* & b^* \end{bmatrix}$ where

$$a^* = a - \Sigma\, c_i^{\,2} \;,\; b^* = b - \Sigma\, d_i^{\,2} \;,\; h^* = h - \Sigma\, c_i\, d_i$$

Some rather heavy algebraic calculation now establishes that

$$a^* b^* - h^{*2} = ab - h^2 - b\, \Sigma\, (c_i - d_i)^2 - (b-a)\, \Sigma\, d_i\, (c_i - d_i)$$
$$- (a^* + b^* - 2h^*)\, \Sigma\, c_i d_i - \Sigma\, c_i\, (c_i - d_i)\, \Sigma\, d_i\, (c_i - d_i)$$

We call this equation the discriminant equality. The left hand side is the discriminant of the quadratic form $(x\alpha^* + y\beta^* \;,\; x\alpha^* + y\beta^*)$. Since this quadratic form is positive semi-definite its discrimant is non-negative and, unless α^*, β^* are dependent, is strictly positive. In particular

$$ab - h^2 - b\; \Sigma (c_i - d_i)^2 \geq (b-a)\; \Sigma d_i (c_i - d_i) + (a^* + b^* - 2h^*)\; \Sigma c_i d_i$$
$$+ \Sigma c_i\, (c_i - d_i)\;\; \Sigma d_i\, (c_i - d_i)$$

Since $h^* \leq \sqrt{a^* b^*} \leq \frac{1}{2}(a^* + b^*)$ each of the three terms on the right hand side of this inequality is non-negative and so the first part of the theorem is proved.

For the second part we just note that when equality holds then the three terms considered in the last inequality must be zero, and also $a^* b^* - h^{*2} = 0$. Hence each $d_i = 0$ and α^*, β^* are dependent.

EXAMPLE Consider two characters α, β with inner product matrix $\begin{bmatrix} 11 & 15 \\ 15 & 30 \end{bmatrix}$. Applying the lemma directly gives $\sum_{i=1}^{t} (c_i - d_i)^2 \leq 3$. Hence at most 3 of the irreducible multiplicities associated with α exceed those for β and the excesses are always 1. In many cases the discriminant equality permits more information to be gleaned. For this example consider the case $t = 3$. Then

$$0 \leq a^* b^* - h^{*2} = 15 - 19 \Sigma d_i (c_i - d_i) - (a^* + b^* - 2h^*) \Sigma c_i d_i$$
$$- \Sigma c_i (c_i - d_i) \Sigma d_i (c_i - d_i)$$

and it follows that $d_1 = d_2 = d_3 = 0$

At this point we remark that example inner product matrices such as the one above should, to be convincing, always be realisable as RR^T with R having non-negative integer values. This is true here for one possibility (among many) is

$$R = \begin{bmatrix} 1 & 1 & 3 & 0 & 0 \\ 0 & 0 & 5 & 2 & 1 \end{bmatrix}$$

All subsequent examples in this paper will also be realisable.

Theorem 1, like Guy's lemma, uses the inner product matrix of α and β in an optimal way. However, it does not take into account inner products arising from other characters. As we shall see such information can be valuable. To take a rather striking example, consider 3 characters α, β, γ with inner product matrix

$$\begin{bmatrix} 9 & 1 & 11 \\ 1 & 2 & 3 \\ 11 & 3 & 16 \end{bmatrix}$$

Guy's criterion can be applied to neither of the pairs (α, γ) and (β, γ). However the inner product matrix of $\alpha + \beta, \gamma$ is

$$\begin{bmatrix} 13 & 14 \\ 14 & 16 \end{bmatrix}$$

and Guy's criterion reveals that $\alpha + \beta \leq \gamma$:- a stronger conclusion than $\alpha \leq \beta$ and $\beta \leq \gamma$!

THEOREM 2 Let $\alpha, \beta, \gamma_1, \gamma_2, \ldots, \gamma_n$ be characters with inner product matrix

	α	β	γ_1	γ_2	$\ldots$	γ_n
α	a	h	p_1	p_2		p_n
β	h	b	q_1	q_2		q_n
γ_1	p_1	q_1				
γ_2	p_2	q_2				
.					M	
.						
.						
γ_n	p_n	q_n				

where $M = (m_{ij})$ and $m_{ij} = (\gamma_i, \gamma_j)$. Suppose that $0 < a \leq b$ and that $p_i \leq q_i$, $i = 1, 2, \ldots, n$. Let $x_1, x_2, \ldots, x_n$ be real variables and let $q(\underline{x})$ be the quadratic

$$\underline{x}\,[(a+b-2h-1)M - (\underline{q}-\underline{p})^T(\underline{q}-\underline{p})]\,\underline{x}^T + 2\underline{x}[a\,\underline{q}^T + b\,\underline{p}^T - h\underline{p}^T - h\underline{q}^T - \underline{q}^T]$$
$$+ ab-h^2-b$$

(with the obvious row vector notation). Then, if for some $\underline{x} \geq 0$, $q(\underline{x})$ is negative, we have $\alpha \leq \beta$.

Proof. If $x_1, x_2, \ldots, x_n$ are non-negative reals then $\alpha^* = \alpha + \Sigma\, x_i\, \gamma_i$ and $\beta^* = \beta + \Sigma\, x_i\, \gamma_i$ are positive class functions (i.e. linear combinations of the irreducible characters with positive or zero coefficients). The inner product of α^*, β^* is easily calculated from the given inner products; it is $\begin{bmatrix} A & H \\ H & B \end{bmatrix}$ where

$$A = a + 2\,\underline{x}\,\underline{p}^T + \underline{x}\,M\,\underline{x}^T$$

$$B = b + 2\,\underline{x}\,\underline{q}^T + \underline{x}\,M\,\underline{x}^T$$

$$H = h + \underline{x}\,(\underline{p}^T + \underline{q}^T) + \underline{x}\,M\,\underline{x}^T$$

The quadratic $q(\underline{x})$ is precisely the function $AB-H^2-B$ and so the condition of the theorem is the main condition of Guy's lemma. Note also that the inequalities on a, b, p_i and q_i together with the positivity of $\underline{x}$ ensure that $0 < A \leq B$. To complete the proof that $\alpha \leq \beta$ we must simply check that the proof of Guy's lemma requires only that $\beta^* - \alpha^*$ be a generalized character and that α^*, β^* be positive class functions.

The case $n = 1$ of this theorem is especially handy. Let α, β, γ be characters with inner product matrix

$$\begin{bmatrix} a & h & p \\ h & b & q \\ p & q & m \end{bmatrix}$$

where $a \le b$ and $p \le q$. If $[(a+b-2h-1)m - (q-p)^2]\, x^2 +$ $2x\,(aq+bp-hp-hq-q) + ab-h^2-b$ takes a negative value for some $x \ge 0$ then $\alpha \le \beta$. In particular we have (with the same notation)

COROLLARY If $a \le b$, $p \le q$ and $(a+b-2h)m - (q-p)^2 < m$ then $\alpha \le \beta$ and the character $\beta-\alpha$ contains or is contained in γ

Proof. The above quadratic certainly takes a negative value with $x \ge 0$ since the coefficient of x^2 is negative. Hence $\alpha \le \beta$, and $\beta-\alpha$ is a character. The inner product matrix of $\beta-\alpha$, γ is

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

Guy's lemma now shows that $\beta-\alpha \le \gamma$ or $\gamma \le \beta-\alpha$ according as $a+b-2h \le m$ or $a+b-2h \ge m$.

As an example of the Corollary consider characters α, β, γ with inner product matrix

$$\begin{bmatrix} 4 & 7 & 5 \\ 7 & 17 & 16 \\ 5 & 16 & 20 \end{bmatrix}$$

According to the Corollary $\alpha \le \beta$ and $\beta-\alpha \le \gamma$. In practice we would replace β by $\beta^* = \beta-\alpha$ and γ by $\gamma^* = \gamma-\beta^*$.

The inner product matrix of $\alpha, \beta^*, \gamma^*$ is

$$\begin{bmatrix} 4 & 3 & 2 \\ 3 & 7 & 4 \\ 2 & 4 & 5 \end{bmatrix}$$

whose entries are noticeably smaller than those of the original matrix.

Unfortunately Theorem 2 is not optimal in that there exist characters $\alpha, \beta, \gamma_1, \gamma_2, \ldots$ whose inner product matrix allows $\alpha \leq \beta$ to be deduced even though the conditions of the theorem are not met. An example of this is the inner product matrix of characters α, β, γ

$$\begin{bmatrix} 11 & 13 & 3 \\ 13 & 17 & 5 \\ 3 & 5 & 14 \end{bmatrix}$$

Certainly there exist character decompositions of α, β, γ which realise this matrix but a case by case analysis shows that all of them have $\alpha \leq \beta$. On the other hand the relevant quadratic is $10x^2 - 6x + 1$ which is positive everywhere.

Finally we point out that the technique of Theorem 2 which was used to improve Guy's lemma can equally well be used to improve Theorem 1. As an example consider characters α, β, γ with inner product matrix

$$\begin{bmatrix} 9 & 11 & 1 \\ 11 & 21 & 14 \\ 1 & 14 & 31 \end{bmatrix}$$

Using the notation and conclusion of Theorem 1 we have

$$\Sigma\, (c_i - d_i)^2 \leq (9 \times 21 - 11^2)/21 = 3$$

However the inner product matrix of $\alpha + \gamma x$, $\beta + \gamma x$ is

$$\begin{bmatrix} A & H \\ H & B \end{bmatrix} = \begin{bmatrix} 31x^2 + 2x + 9 & 31x^2 + 15x + 11 \\ 31x^2 + 15x + 11 & 31x^2 + 28x + 21 \end{bmatrix}$$

Since Theorem 1 applies to positive class functions we have

$$\sum (c_i - d_i)^2 \leq \left\lfloor \min_{x \geq 0} (AB - H^2)/B \right\rfloor = \left\lfloor \min_{x \geq 0} \frac{79x^2 - 36x + 68}{31x^2 + 28x + 21} \right\rfloor = 1$$

REFERENCES

1. J.H. Conway, Character Calisthenics, Proceedings of the International Conference on Computational Group Theory, Academic Press (to appear)

2. J.D. Dixon, High Speed Computation of Group Characters, Numer. Math. 10 (1967), 446-550

3. J. Neubüser, H. Pahlings, W. Plesken, CAS: Design and Use of a System for the Handling of Characters of Finite Groups, Proceedings of the International Conference on Computational Group Theory, Academic Press (to appear)

4. J. Neubüser, Computing with Groups and Their Character Tables, Physica 114A (1982) 493-506

CARLETON UNIVERSITY
School of Computer Science

Bibliography of SCS Reports

SCS-TR-1 THE DESIGN OF CP-6 PASCAL
Jim des Rivieres and Wilf R. LaLonde, June 1982.

SCS-TR-2 SINGLE PRODUCTION ELIMINATION IN LR(1) PARSERS:A SYNTHESIS
Wilf R. LaLonde, June 1982.

SCS-TR-3 A FLEXIBLE COMPILER STRUCTURE THAT ALLOWS DYNAMIC PHASE ORDERING
Wilf R. LaLonde and Jim des Rivieres, June 1982.

SCS-TR-4 A PRACTICAL LONGEST COMMON SUBSEQUENCE ALGORITHM FOR TEXT COLLATION
Jim des Rivieres, June 1982.

SCS-TR-5 A SCHOOL BUS ROUTING AND SCHEDULING PROBLEM
Wolfgang Lindenberg, Frantisek Fiala, July 1982.

SCS-TR-6 ROUTING WITHOUT ROUTING TABLES
Nicola Santoro, Ramez Khatib, July 1982.

SCS-TR-7 CONCURRENCY CONTROL IN LARGE COMPUTER NETWORKS
Nicola Santoro, Hasan Hural, July 1982.

SCS-TR-8 ORDER STATISTICS ON DISTRIBUTED SETS
Nicola Santoro, Jeffrey B. Sidney, July 1982.

SCS-TR-9 OLIGARCHICAL CONTROL OF DISTRIBUTED PROCESSING SYSTEMS
Moshe Krieger, Nicola Santoro, August 1982.

SCS-TR-10 COMMUNICATION BOUNDS FOR SELECTION IN DISTRIBUTED SETS
Nicola Santoro, Jeffrey B. Sidney, September 1982.

SCS-TR-11 A SIMPLE TECHNIQUE FOR CONVERTING FROM A PASCAL SHOP TO C SHOP
Wilf R. LaLonde, John R. Pugh, November 1982.

SCS-TR-12 EFFICIENT ABSTRACT IMPLEMENTATIONS FOR RELATIONAL DATA STRUCTURES
Nicola Santoro, December 1982.

SCS-TR-13 ON THE MESSAGE COMPLEXITY OF DISTRIBUTED PROBLEMS
Nicola Santoro, December 1982.

SCS-TR-14 A COMMON BASIS FOR SIMILARITY MEASURES INVOLVING TWO STRINGS
R.L. Kashyap and B.J. Oommen, January 1983.

SCS-TR-15 SIMILARITY MEASURES FOR SETS OF STRINGS
R.L. Kashyap and B.J. Oommen, January 1983.

SCS-TR-16 THE NOISY SUBSTRING MATCHING PROBLEM
R.L. Kashyap and B.J. Oommen, January 1983.

SCS-TR-17 DISTRIBUTED ELECTION IN A CIRCLE WITHOUT A GLOBAL SENSE OF ORIENTATION
E. Korach, D. Rotem, N. Santoro, January 1983.

SCS-TR-18 A GEOMETRICAL APPROACH TO POLYGONAL DISSIMILARITY AND THE CLASSIFICATION OF CLOSED BOUNDARIES
R.L. Kashyap and B.J. Oommen, January 1983.

SCS-TR-19 SCALE PRESERVING SMOOTHING OF POLYGONS
R.L. Kashyap and B.J. Oommen, January 1983.

SCS-TR-20 NOT-QUITE-LINEAR RANDOM ACCESS MEMORIES
Jim des Rivieres, Wilf LaLonde and Mike Dixon, August 1982, Revised March 1, 1983.

SCS-TR-21 SHOUT-ECHO SELECTION IN DISTRIBUTED FILES
D. Rotem, N. Santoro, J. B. Sidney, March 1983.

SCS-TR-22 DISTRIBUTED RANKING
E. Korach, D. Rotem, N. Santoro, March 1983

SCS-TR-23 A REDUCTION TECHNIQUE FOR SELECTION IN DISTRIBUTED FILES : I
N. Santoro, J. B. Sidney, April 1983.

SCS-TR-24 LEARNING AUTOMATA POSSESSING ERGODICITY OF THE MEAN : THE TWO ACTION CASE
M.A.L. Thathachar and B. J. Oommen, May 1983

SCS-TR-25 ACTORS - THE STAGE IS SET
John R. Pugh, June 1983

SCS-TR-26 ON THE ESSENTIAL EQUIVALENCE OF TWO FAMILIES OF LEARNING AUTOMATA
M. A. L. Thathachar and B. J. Oommen, May 1983

SCS-TR-27 GENERALIZED KRYLOV AUTOMATA AND THEIR APPLICABILITY TO LEARNING IN NONSTATIONARY ENVIRONMENTS
B. J. Oommen, June 1983

SCS-TR-28 ACTOR SYSTEMS: SELECTED FEATURES
Wilf R. LaLonde, July 1983.

SCS-TR-29 ANOTHER ADDENDUM TO KRONECKER'S THEORY OF PENCILS
M. D. Atkinson, August 1983

SCS-TR-30 SOME TECHNIQUES FOR GROUP CHARACTER REDUCTION
M. D. Atkinson and R. A. Hassan, August 1983

SCS-TR-31 AN OPTIMAL ALGORITHM FOR GEOMETRICAL CONGRUENCE
M. D. Atkinson, August 1983