Werk

Titel: Numerische Mathematik

Verlag: Springer Verlag

Jahr: 1967

Kollektion: Mathematica

Werk Id: PPN362160546_0010

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN362160546_0010|LOG_0046

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Numerische Mathematik 10, 446—450 (1967)

High Speed Computation of Group Characters

JOHN D. DIXON

Received April 20, 1967

Abstract. This paper describes a practical procedure for computing the ordinary irreducible characters of finite groups (of orders up to 1000 or so). The novelty of the method consists of transposing the problem from the field of complex numbers into the field of integers modulo p for a suitable prime p. It is much easier to compute the modular characters in the latter field, and from these characters we can calculate the ordinary irreducible characters in algebraic form.

1. Introduction

In practice, the calculation of the (ordinary) irreducible characters of a finite group is more of an art than a science. Except for specific classes of groups, such as the symmetric groups, the easiest approach is not a systematic one, but one which depends on the particular properties which the group happens to display. On the other hand there is a classical method of systematically calculating the irreducible characters of a finite group. This method is described in BURNSIDE [1] § 223, and is briefly summarized below. In Sections 2 and 3 we describe a useful modification of this method which makes it feasible to use a high speed computer to calculate the characters of groups of moderately large order (see Section 4).

Let G be a finite group of order g with k conjugacy classes: $C_1=\{1\}, C_2, \ldots, C_k$ of orders $h_1, h_2, \ldots, h_k$, respectively. Define c_{rst} $(r, s, t=1, 2, \ldots, k)$ to be the number of solutions (x, y) to $xy=z$ with $x\in C_r$, $y\in C_s$, for given $z\in C_t$. (The number is independent of z.) Then G has k irreducible characters $\chi^1, \chi^2, \ldots, \chi^k$ of degrees $d_1, d_2, \ldots, d_k$, say. We shall write χ_r^i as the value of χ^i on the class C_r. It follows from elementary character theory that

$$\frac{h_r \chi_r^i}{d_i} \cdot \frac{h_s \chi_s^i}{d_i} = \sum_{t=1}^{k} c_{rst} \frac{h_t \chi_t^i}{d_i} \tag{1}$$

for $i, r, s=1, 2, \ldots, k$ (see [1] § 213 or [2] § 33). If we write M_r for the $k\times k$ matrix with (s, t)-th entry c_{rst}, then (1) may be interpreted as saying that the k column vectors

$$(h_1 \chi_1^i/d_i, h_2 \chi_2^i/d_i, \ldots, h_k \chi_k^i/d_i) \quad (i=1, 2, \ldots, k) \tag{2}$$

are common eigenvectors for the matrices M_r $(r=1, 2, \ldots, k)$. The well known character relations show that the vectors (2) form a linearly independent set. The method described by BURNSIDE consists in essence in the following steps.

Step 1. Calculate the group elements and the classes of conjugates.

Step 2. Calculate the structure constants c_{rst} and the matrices $M_1, M_2, \ldots, M_k$.

Step 3. Find a set of k linearly independent vectors $\boldsymbol{v}_i=(v_{i1}, v_{i2}, \ldots, v_{ik})$ $(i=1, 2, \ldots, k)$ each of which is an eigenvector for each M_r. We may normalize these vectors such that $v_{i1}=1$ for each i to correspond to (2) since $h_1 \chi_1^i/d_i=1$ by the choice of $C_1=\{1\}$. Note that the character relations ensure that these $\boldsymbol{v}_i$ are uniquely determined up to the order in which they occur (see Section 2).

Step 4. Calculate the degree d_i of the character χ^i by using the character relations. Specifically

$$\sum_{j=1}^{k} v_{ij} v_{ij'}/h_j = \sum_{j=1}^{k} h_j \chi_j^i \chi_{j'}^i/d_i^2 = g/d_i^2$$

where j' is defined by $x\in C_j \Leftrightarrow x^{-1}\in C_{j'}$.

Step 5. Calculate the characters

$$\chi_j^i = v_{ij} d_i/h_j \quad (i, j=1, 2, \ldots, k).$$

The difficulty in practice lies in Step 3, involving the calculation of common eigenvectors for a number of $k\times k$ matrices. Thus in the example given by BURNSIDE, the dihedral group of order 10, the calculations at Step 3 are already definitely nontrivial. Even with a highspeed computer it is clear that the calculations will become laborious, and the round-off errors serious, once k is moderately large. Moreover a further problem arises: the theoretical investigations for which characters are calculated require the characters in algebraic form rather than their numerical values. The following modification largely overcomes these difficulties.

2. Outline of the Method

We first describe the idea behind the modified method, and then discuss some of the details in Section 3.

Let e be the exponent of G (that is, the least common multiple of the orders of the elements of G). If $x\in G$ has order m, then each character of x is a sum of m-th roots of unity, and in particular is a sum of e-th roots of unity. Thus, if ζ is a fixed complex primitive e-th root of unity, then the values of the characters of G all lie in $Z[\zeta]$, the ring of polynomials in ζ with integer coefficients. By Dirichlet's theorem on primes in an arithmetic progression there is a prime p such that e divides $p-1$, and then we can find an integer z such that $z^e\equiv 1 \pmod p$ and $z^f \not\equiv 1 \pmod p$ for all f, $0<f<e$. In fact any such integer z is a root (mod p) of the cyclotomic polynomial $F_e(X)$. Now an integer polynomial $f(X)$ vanishes at $X=\zeta$ if and only if the cyclotomic polynomial $F_e(X)$ divides $f(X)$ (see [3] § 53). Hence $f(\zeta)=0$ implies $f(z)\equiv 0 \pmod p$. This shows that there is a ring homomorphism θ from the ring $Z[\zeta]$ onto the ring Z_p of integers modulo p where θ is defined by

$$\theta: f(\zeta) \to f(z) \pmod p. \tag{3}$$

The homomorphism θ permits us to transpose our problem from the complex field into the finite field Z_p. It is well known that all h_i, d_i $(i=1, 2, \ldots, k)$ divide g, so none of them is divisible by p. However, by the character relations,

we have

$$\sum_{r=1}^{k} (h_r \chi_r^i/d_i) \cdot (h_r \chi_r^j/d_j)/h_r = \delta_{ij}\, g/(d_i\, d_j) \tag{4}$$

for $i, j = 1, 2, \ldots, k$. Thus, we conclude that θ maps the vectors (2) into a set of k vectors linearly independent over Z_p. Since θ is a homomorphism, these vectors will be common eigenvectors for the matrices $M_1, M_2, \ldots, M_k \pmod p$. The i-th of these eigenvectors has the eigenvalue $\theta(h_r \chi_r^i/d_i)$ for the matrix M_r ($r = 1, 2, \ldots, k$). The character relations then show that for $i \neq j$ there is at least one matrix M_s for which the i-th and j-th eigenvectors have different eigenvalues. This ensures that the set of k common eigenvectors for $M_1, M_2, \ldots, M_k \pmod p$ is essentially uniquely defined.

Thus we conclude that we may carry out Step 3 of Burnside's method, operating in Z_p. This is a much simpler process than in the complex field. For example, since Z_p is finite, we can actually try out each number in Z_p as a possible eigenvalue, and of course there is no round-off error problem arising from approximate calculation of eigenvalues. Steps 4 and 5 are also carried out in Z_p, and then the final step of the modified method is

Step 6. From the values of $\theta(\chi_j^i)$ calculate the values of χ_j^i $(i, j = 1, 2, \ldots, k)$.

3. Details of the Method

The calculations at Step 3 are carried out in Z_p in a direct manner. Let $\mathscr{V}$ be the vector space of all column k-vectors over Z_p. Starting with one matrix, say M_1, we calculate the null space of $M_1 - \lambda I \pmod p$ for successive values of $\lambda = 0, 1, \ldots, p-1$, and, if the null space is nonzero, we calculate a basis for the space. In general, at the r-th stage, we have already calculated subspaces $\mathscr{V}_1, \ldots, \mathscr{V}_s$ of $\mathscr{V}$ where each $\mathscr{V}_i$ is a set of common eigenvectors for the matrices $M_1, \ldots, M_{r-1}$, together with the zero vector, and where $\mathscr{V}$ is the direct sum $\mathscr{V}_1 \oplus \cdots \oplus \mathscr{V}_s$. Then, for each $\mathscr{V}_i$ of dimension >1, we consider the action of $M_r - \lambda I \pmod p$ on $\mathscr{V}_i$ for $\lambda = 0, 1, \ldots, p-1$, and hence reduce $\mathscr{V}_i$ to a direct sum of eigenspaces of M_r. The process terminates at the r-th stage if each $\mathscr{V}_i$ has dimension 1, and this will always happen for some $r \leqq k$. When this stage has been reached we define $\boldsymbol{v}_i$ as the basis element of the one-dimensional space $\mathscr{V}_i$ with $\boldsymbol{v}_i$ normalized so that the first component is 1.

The equation given in Step 4 can now be used to compute $d_i^2 \pmod p$. In order that d_i is uniquely defined by this congruence, we add a further condition on p, namely $p > 2d_i$ $(i = 1, 2, \ldots, k)$. This condition is certainly satisfied if

$$p > 2\sqrt{g} \tag{5}$$

because $g = \sum_i d_i^2$. Once d_i has been calculated, Step 5 is straightforward.

Finally, to carry out Step 6 (reconversion to the complex field) we proceed as follows. Let ζ be a fixed primitive e-th root of unity, and suppose that R is an irreducible representation of G affording the character χ of degree d. Then, for each $x \in G$, $\chi(x)$ is the sum of the d eigenvalues of $R(x)$, and these eigenvalues are all e-th roots of unity. Thus $\chi(x) = \zeta^{s_1} + \cdots + \zeta^{s_d}$, say, and similarly $\chi(x^n) =$

$\zeta^{ns_1}+\cdots+\zeta^{ns_d}$ for $n=0, 1, \ldots$. Using the identity

$$\sum_{j=0}^{e-1}\zeta^{jt}=\begin{cases}e & \text{if } e \text{ divides } t\\ 0 & \text{otherwise}\end{cases} \tag{6}$$

we conclude that ζ^s occurs as an eigenvalue with multiplicity $m(s)$ in $R(x)$ where

$$m(s)=(1/e)\sum_{n=0}^{e-1}\chi(x^n)\,\zeta^{-sn}. \tag{7}$$

Hence

$$\chi(x)=\sum_{s=0}^{e-1}m(s)\,\zeta^s$$

where $m(s)$ is defined in (7). However, under the homomorphism θ defined in (3), we obtain from (7)

$$m(s)\equiv(1/e)\sum_{n=0}^{e-1}\theta\left(\chi(x^n)\right)z^{-sn}\pmod{p}, \tag{8}$$

and from the condition (5) we see that $m(s)$ is uniquely defined by (8) and the condition $0\leqq m(s)\leqq d<p$. Thus Step 6 involves calculating integers m_{ijs} such that $0\leqq m_{ijs}<p$ and

$$m_{ijs}\equiv(1/e)\sum_{n=0}^{e-1}\theta(\chi_{j(n)}^i)\,z^{-sn}\pmod{p}\quad(i,j=1,2,\ldots,k;\ s=0,1,\ldots,e-1) \tag{9}$$

where $j(n)$ is defined by $x\in C_j\Leftrightarrow x^n\in C_{j(n)}$. Then

$$\chi_j^i=\sum_{s=0}^{e-1}m_{ijs}\zeta^s\quad(i,j=1,2,\ldots,k).$$

4. Some Computational Details

We conclude with a few observations on the actual computations involved in the use of the modified method. In the program written by the author, the generators of the group are read in as permutations, and the elements of the group, the conjugacy classes, and the matrices $M_1, M_2, \ldots, M_k$ are calculated from these. The prime p is supplied from a table of primes using a knowledge of the order of the group or an estimate of the exponent of the group from the degree of the permutations involved. The calculations modulo p are simplified by first calculating a primitive root and a table of indices (see, for example, [4] Chapter VI). Some of the calculations involved in Step 3 are avoided by a judicious ordering of the matrices M_r; for example, $M_1=I$, and so this matrix plays no part in the reduction of the eigenspaces. Finally, the calculations involved in (9) can be simplified by observing that if the class C_j consists of elements of order l, then it is sufficient to carry out the calculation for m_{ijs} over l-th roots (rather than e-th roots).

The author's program has been run on the IBM 360/50 at the Computing Centre of the University of New South Wales. As written, the program only makes use of the internal core storage of the machine and will handle groups of orders up to 550; the use of auxillary storage would extend this range. The

time taken to compute the irreducible characters of a group depends on the number of classes as well as the order. As typical examples, the nine characters of the simple group of order 504 were calculated in ten minutes and the twenty characters of one of the groups of order 128 were calculated in two minutes.

Acknowledgements. The author is indebted to Mr. Z. STAR who gave him valuable assistance in details of the computer program.

References

1. BURNSIDE, W.: Theory of groups of finite order, 2nd ed. reprint. New York: Dover 1955.
2. CURTIS, C. W., and I. REINER: Representation theory of finite groups and associative algebras. New York: Wiley 1962.
3. VAN DER WAERDEN, B. L.: Modern algebra, vol. 1. New York: Frederick Ungar 1949.
4. VINOGRADOV, I. M.: Elements of number theory. 5th ed. New York: Dover 1954.

Department of Pure Mathematics
University of New South Wales
Box 1, P. O.
Kensington, N.S.W., Australia