MATHEMATICS OF COMPUTATION, VOLUME 24, NUMBER 111, JULY, 1970

Computing Irreducible Representations of Groups

By John D. Dixon*

Abstract. How can you find a complete set of inequivalent irreducible (ordinary) representations of a finite group? The theory is classical but, except when the group was very small or had a rather special structure, the actual computations were prohibitive before the advent of high-speed computers; and there remain practical difficulties even for groups of relatively small orders (≤ 100). The present paper describes three techniques to help solve this problem. These are: the reduction of a reducible unitary representation into its irreducible components; the construction of a complete set of irreducible unitary representations from a single faithful representation; and the calculation of the precise values of a group character from values which have only been computed approximately.

1. Introduction. The object of this paper is to describe three techniques which should be useful in constructing irreducible representations and the characters of finite groups. Unlike some proposed solutions, none of these techniques depends on any special structure for the group considered, and combined these techniques should produce an efficient means of computing a complete set of irreducible representations. These techniques are: (a) an efficient method of reducing a reducible unitary representation (Section 2); (b) a method for constructing a complete set of irreducible unitary representations of a group from a single faithful unitary representation (Section 3); and (c) a method of obtaining the precise values of a character from values calculated only approximately (Section 4). Although we always refer to finite groups, it should be noted that many of the results are also valid for unitary representations of finitely generated infinite groups.

Notation. The term representation will always mean a matrix representation over the field $\mathbb{C}$ of complex numbers. It is well known that every representation of a finite group is equivalent to a representation in unitary matrices (for example, see [6, Theorem (3.1)]). Thus there is no loss in generality when we deal exclusively with unitary representations. By $\mathbf{M}(d)$ we denote the vector space of dimension d^2 over $\mathbb{C}$ consisting of all $d \times d$ matrices over $\mathbb{C}$, and $\mathbf{U}(d)$ will denote the group of all $d \times d$ unitary matrices. We also write I for the unit matrix and X^* for the complex conjugate transpose of X.

2. The Reduction of a Unitary Representation. The theory on which our method is based may be found in [6, Theorem (1.6)]. Briefly it is as follows. If $\mathbf{G}$ is a finite subgroup of order g in $\mathbf{U}(d)$, then $\mathbf{G}$ is irreducible unless for at least one element

Received September 22, 1969, revised December 8, 1969.

AMS Subject Classifications. Primary 2080; Secondary 6535, 6540.

Key Words and Phrases. Computation of group representations, computation of characters, reduction of unitary representations, irreducible components, tensor products, iterative processes, finite Fourier analysis.

* This work has been supported in part by the National Research Council of Canada Grant No. A7171.

E_{rs} of the standard basis for $\mathbf{M}(d)$ the matrix

$$E = \frac{1}{g} \sum_{X \in \mathbf{G}} X^* E_{rs} X$$

is *not* scalar. Indeed $EX = XE$ for all $X \in \mathbf{G}$ and when E is not scalar the eigenspaces of E reduce $\mathbf{G}$ (compare with our Theorem 2).

If we tried to apply this theory directly, then we would need to store or compute all the elements of the group $\mathbf{G}$. This would be very clumsy unless $\mathbf{G}$ is small. However, it turns out that E may be computed by an iteration process using only a set of generators for $\mathbf{G}$. This is what we now prove in Theorems 1 and 2.

THEOREM 1. *Let $\mathbf{S}$ be a finite set consisting of h elements of $\mathbf{U}(d)$ and suppose that the unit matrix $I \in \mathbf{S}$. We define a linear mapping $\sigma\colon \mathbf{M}(d) \to \mathbf{M}(d)$ by*

$$\sigma(B) = \frac{1}{h} \sum_{U \in \mathbf{S}} U^* B U.$$

Then for each $A_0 \in \mathbf{M}(d)$ we can define a sequence (A_n) in $\mathbf{M}(d)$ by putting $A_n = \sigma^n(A_0)$ for $n = 1, 2, \cdots$. Then (A_n) is always convergent in $\mathbf{M}(d)$ and its limit, say A, has the property $AU = UA$ for all $U \in \mathbf{S}$.

Proof. We shall use the norm $||\cdot||$ on $\mathbf{M}(d)$ defined by $||B||^2 = \text{trace } B^*B$. Our first step is to prove

$$||\sigma(B)|| = ||B|| \quad \text{implies that } UB = BU \quad \text{for all } U \in \mathbf{S}. \tag{1}$$

Indeed, for any $B \in \mathbf{M}(d)$ the properties of the norm show that

$$\begin{aligned} ||\sigma(B)|| &= \left|\left| h^{-1} \sum_{U \in \mathbf{S}} U^* B U \right|\right| \leqq h^{-1} \sum_{U \in \mathbf{S}} ||U^* B U|| \\ &= h^{-1} \sum_{U \in \mathbf{S}} ||B|| = ||B|| \end{aligned} \tag{2}$$

because the U are unitary. Moreover, the equality sign holds in (2) exactly when all the matrices U^*BU (for $U \in \mathbf{S}$) lie on the same ray through 0 in $\mathbf{M}(d)$. Now $I \in \mathbf{S}$ and so $||\sigma(B)|| = ||B||$ implies that there exist real numbers $\lambda_U \geqq 0$ such that $U^*BU = \lambda_U B$ for all $U \in \mathbf{S}$. But $||B|| = ||U^*BU||$ and so $||B|| = ||\lambda_U B|| = \lambda_U ||B||$. Thus, either $B = 0$ or else $\lambda_U = 1$ for all $U \in \mathbf{S}$. In either case we conclude that $UB = BU$ for all $U \in \mathbf{S}$, and so (1) is proved.

Now consider the sequence (A_n). It follows from (2) that the sequence $(||A_n||)$ of real numbers is monotonically decreasing, and so we have $\lim ||A_n|| = \mu$, say. The monotonicity of $(||A_n||)$ also shows that the sequence (A_n) lies in the compact ball $\{C \in \mathbf{M}(d) \mid ||C|| \leqq ||A_0||\}$, and so there is some subsequence (A_{n_k}) which converges to a limit, say A, in $\mathbf{M}(d)$. But $||A|| = \mu = \lim_{k\to\infty} ||A_{n_k+1}|| = \lim ||\sigma(A_{n_k})||$, and so the continuity of σ shows that $||A|| = ||\sigma(A)||$. Then (1) shows that $AU = UA$ for all $U \in \mathbf{S}$, and it remains to prove that (A_n) converges to A.

Put $B_n = A_n - A$ for $n = 0, 1, 2, \cdots$. Since $\sigma(A) = A$, (2) implies that $(||B_n||)$ is monotonically decreasing. But $\lim ||B_{n_k}|| = 0$ by the definition of A. Therefore $\lim ||B_n|| = 0$ and so the sequence (A_n) converges to A. This concludes the proof of the theorem.

Before stating Theorem 2 we introduce a little notation. Let E_{rs} $(r, s = 1, \cdots, d)$

be the standard basis for $\mathbf{M}(d)$; that is, E_{rs} is the matrix whose (r, s)th entry is 1 and whose other entries are all 0. We define a second basis H_{rs} $(r, s = 1, \cdots, d)$ for $\mathbf{M}(d)$ *by*

$$\begin{aligned} H_{rs} &= E_{rr} && \text{if } r = s, \\ &= E_{rs} + E_{sr} && \text{if } r > s, \\ &= i(E_{rs} - E_{sr}) && \text{if } r < s. \end{aligned}$$

Now, in the notation of Theorem 1, all the limits $\lim_{n\to\infty} \sigma^n(H_{rs})$ exist. Moreover, because all the H_{rs} are hermitian matrices, it is easily verified that these limits will also be hermitian.

THEOREM 2. *We keep the notation of Theorem* 1. *Suppose that* S *is a reducible set of matrices (or equivalently* S *generates a reducible subgroup of* $\mathbf{U}(d)$*). Then for at least one* H_{rs} *the limit* $\lim \sigma^n(H_{rs}) = H$, *say, is not scalar and we can reduce* S *into a number of not (necessarily irreducible) components as follows. Since H is hermitian, we can find an orthonormal basis* $v_1, \cdots, v_d$ *of the underlying d-dimensional unitary space such that this basis is made up by listing successively orthonormal bases for the eigenspaces for H for the different eigenvalues. Then, if C is the (unitary) matrix whose columns are* $v_1, \cdots, v_d$, *we have*

$$C^* UC = \begin{bmatrix} U_1 & & & \\ & U_2 & & \\ & & \ddots & \\ & & & U_k \end{bmatrix} \quad \text{for all } U \in \mathbf{S}.$$

Here the (r, s)*th entry of the matrix on the right-hand side is* $v_r^* U v_s$ *and this is* 0 *when* v_r *and* v_s *are eigenvectors for different eigenvalues of H.*

Proof. S is completely reducible because it is a subset of $\mathbf{U}(d)$ and by hypothesis S is not irreducible. It is easily proved (for example, see [4, Problem 10.3]) that this implies that there exists a nonscalar $B \in \mathbf{M}(d)$ such that $UB = BU$ for all $U \in \mathbf{S}$, and so $\sigma(B) = B$. Since the H_{rs} form a basis for $\mathbf{M}(d)$ there exist $\beta_{rs} \in \mathbb{C}$ such that $B = \sum \beta_{rs} H_{rs}$, and so $B = \lim \sigma^n(B) = \sum \beta_{rs} \lim \sigma^n(H_{rs})$ because σ is linear. Since B is not scalar, at least one $\lim \sigma^n(H_{rs})$ is not scalar. This proves the first part of the theorem.

Now suppose that $H = \lim \sigma^n(H_{rs})$ is not scalar. Then $HU = UH$ for all $U \in \mathbf{S}$ by Theorem 1, and this implies that for any eigenvalue α_j of H the corresponding eigenspace is mapped into itself by multiplication by any $U \in \mathbf{S}$; indeed, if $Hv = \alpha_j v$, then $H(Uv) = U(Hv) = \alpha_j(Uv)$. In particular this shows that $v_r^* U v_s$ is zero whenever v_r and v_s are eigenvectors for H for different eigenvalues. This proves the second part of the theorem.

Note. There should be no trouble in programming the process described in Theorem 2. A crucial point in the computation will be the calculation of the eigenvalues and eigenvectors of H, and this can be done using efficient iteration methods because H is hermitian. It is not hard to prove that the eigenvalues of H always lie in the interval $[-1, 1]$.

3. The Generation of a Full Set of Irreducible Representations. Let G be a finite group and let R: $\mathbf{G} \to \mathbf{U}(d)$ and S: $\mathbf{G} \to \mathbf{U}(d')$ be two representations of G.

Then we define $R \otimes S$: $\mathbf{G} \to \mathbf{U}(dd')$ by putting $(R \otimes S)(x) = R(x) \otimes S(x)$ where the right-hand side denotes the usual tensor (or Kronecker or direct) product of two matrices. It is readily verified that $R \otimes S$ is also a representation of $\mathbf{G}$. We shall require the following theorem due to Burnside (see [2, Section 226] or [4, Problem 11.27]). If R is a *faithful* representation of $\mathbf{G}$, then every irreducible representation of G is equivalent to an irreducible component of one of the representations: R, $R \otimes R$, $R \otimes R \otimes R$, $\cdots$. We also make the following observation from the elementary properties of the tensor product. If $R_1, \cdots, R_r$ and $S_1, \cdots, S_s$ are complete sets of inequivalent irreducible components of R and S, respectively, then each irreducible component of $R \otimes S$ is equivalent to an irreducible component of one of the $R_i \otimes S_j$.

We now outline an algorithm for obtaining all irreducible unitary representations of $\mathbf{G}$ from a single faithful unitary representation.

We begin with a faithful representation R: $\mathbf{G} \to \mathbf{U}(d)$ and a set $\mathbf{S}$ of generators for $\mathbf{G}$ such that the identity $1 \in \mathbf{S}$, and we read in the data $R(u)$ for all $u \in \mathbf{S}$. Next, using the method described in Section 2, we reduce R down to its irreducible components and store the components of $R(u)$ as $R_1(u), \cdots, R_s(u)$ $(u \in \mathbf{S})$. Then, by comparing the characters of these representations, we may choose out of the set $R_1, \cdots, R_s$ a set of reresentatives for the different classes of equivalent representations. If these inequivalent irreducible representations are $S_1, \cdots, S_m$ then we store $S_1(u), \cdots, S_m(u)$ $(u \in \mathbf{S})$. We now construct the tensor products $S_1 \otimes S_1$, $S_1 \otimes S_2$, $\cdots$ and at each step reduce the tensor product to its irreducible components and store the representatives of new classes of irreducible representations as $S_{m+1}(u)$, $\cdots$ $(u \in \mathbf{S})$. This procedure is continued until none of the tensor products $S_i \otimes S_j$ yields any new classes of representations. Then, by Burnside's Theorem quoted above, $S_1, S_2, \cdots$ is a complete set of irreducible representations for $\mathbf{G}$.

Notes. 1. When comparing the characters of two representations R_i and R_j in order to prove that they are equivalent it is not usually enough to check trace $R_i(u) =$ trace $R_j(u)$ for all $u \in \mathbf{S}$; usually it is also necessary to check the traces of certain products. However the simpler criterion is certainly sufficient if $\mathbf{S}$ contains at least one representative from each conjugacy class of $\mathbf{G}$. Perhaps it is worth noting that if $\mathbf{S}$ is a set which contains at least one element from each conjugacy class of $\mathbf{G}$ then we automatically have $\mathbf{S}$ as a set of generators for $\mathbf{G}$. Indeed, the subgroup $\mathbf{H}$ generated by $\mathbf{S}$ has the property that each element of $\mathbf{G}$ is conjugate in $\mathbf{G}$ to some element of $\mathbf{H}$, and this implies that $\mathbf{H} = \mathbf{G}$ when $\mathbf{G}$ is finite (see [4, Problem 1.10]).

2. Suppose that $\mathbf{S}$ consists of exactly one element from each conjugacy class of $\mathbf{G}$ (see Note 1). In this case, if we store the sizes of the conjugacy classes of $\mathbf{G}$, then much of the computation required in the algorithm described above can be simplified by the usual elementary character theoretic arguments. Such arguments will enable us to tell whether any tensor product $S_i \otimes S_j$ is irreducible and whether any of its irreducible components correspond to new classes of irreducible representations; and knowing that $\mathbf{G}$ has k conjugacy classes means we can stop as soon as we have stored the kth representation S_k.

3. In many cases we may find it easiest to take R as a representation in permutation matrices corresponding to a representation of $\mathbf{G}$ as a permutation group. In such cases R is clearly unitary.

4. The most obvious limitation for the application of this algorithm is the difficulty of reducing representations of large degree. If d is the largest degree of any

irreducible representation for G, then we may have to reduce representations of degree d^2 but no larger.

4. Finding the Precise Values of a Character from Approximate Values. In a previous paper [5] I have described a method of computing the character table of a finite group using modular arithmetic. Here I want to point out that one of the techniques of that paper can be used to obtain precise values of a character (in arithmetic or algebraic form) from quite rough estimates of its values. What is involved is essentially a finite Fourier analysis. The technique could be used to obtain the precise character table for a group G from the representations obtained by the method of Section 3.

Let χ be the character of a representation R of a finite group G, and let χ_i and $\tilde{\chi}_i$ denote, respectively, the precise value and some approximate value of the character χ on the conjugacy class $\mathbf{C}_i$ of G. Let $e \geqq 1$ be an integer such that $x^e = 1$ for all $x \in \mathbf{G}$. Let $x \in \mathbf{C}_i$. Then $R(x)^e = 1$ and so all the eigenvalues of $R(x)$ are eth roots of unity. Put $\zeta = \exp(2\pi i/e)$ and define $m_k \geqq 0$ as the multiplicity to which ζ^k occurs as an eigenvalue for $R(x)$. Now to each eigenvalue ζ^k for $R(x)$ there corresponds an eigenvalue ζ^{kn} for $R(x)^n$. Thus for $n = 0, 1, \cdots$ we have

$$\text{trace } R(x^n) = \text{trace } R(x)^n = \sum_{k=0}^{e-1} m_k \zeta^{kn}.$$

We now use the identity

$$\sum_{n=0}^{e-1} \zeta^{(k-l)n} = e \qquad \text{if } e \text{ divides } k - l,$$

$$= \frac{\zeta^{(k-l)e} - 1}{\zeta^{(k-l)} - 1} = 0 \quad \text{otherwise.}$$

This gives us

$$m_l = e^{-1} \sum_{n=0}^{e-1} \sum_{k=0}^{e-1} m_k \zeta^{kn} \zeta^{-ln} = e^{-1} \sum_{n=0}^{e-1} \text{trace } R(x^n) \zeta^{-ln}. \tag{3}$$

Now for each conjugacy class $\mathbf{C}_i$ and each integer n we can define the conjugacy class $\mathbf{C}_{i(n)}$ as consisting of all z^n with $z \in \mathbf{C}_i$. With this notation (3) gives

$$m_l = e^{-1} \sum_{n=0}^{e-1} \chi_{i(n)} \zeta^{-ln}. \tag{4}$$

Now suppose that we only know the approximate values $\tilde{\chi}_i$ of χ. Then it follows from (4) that we can recover m_l as the integer closest to $e^{-1} \sum_{n=0}^{e-1} \tilde{\chi}_{i(n)} \zeta^{-ln}$ provided the errors in the values of χ are all less than $1/2$. Once the "Fourier coefficients" m_l are known, the value of χ_i can be computed precisely.

Note. The only new data needed for these computations are the values of the indices $i(n)$ defined above.

5. Acknowledgments. This work was stimulated by enquiries I received from Drs. S. Flodmark and E. Blokker (Institute of Theoretical Physics, Stockholm University) and by their work on this problem. They have written a successful program

in FORTRAN for computing the irreducible representations of groups of order up to 50. They also mentioned work of C. J. Bradley and D. E. Wallis (Oxford, England) on irreducible representations of finite solvable groups, work by B. S. Thomas (Physics Department, University of Florida) and the thesis of C. Brott (Neue Universität, Kiel 1966). This last deals with groups of orders up to 100 and higher but essentially only with monomial representations. Further references are given below.

Carleton University
Ottawa 1, Ontario, Canada

1. C. BROTT & J. NEUBÜSER, *A Program for the Calculation of Characters and Representations of Finite Groups*, Proc. Conf. Comput. Algebra (Oxford 1967), Pergamon Press, New York, 1969.
2. W. BURNSIDE, *Theory of Groups of Finite Order*, 2nd ed., Dover, New York, 1955. MR **16**, 1086.
3. J. CANNON, "Computers in group theory: a survey," *Comm. ACM*, v. 12, 1969, pp. 3–25.
4. J. D. DIXON, *Problems in Group Theory*, Blaisdell, Waltham, Mass., 1967. MR **36** #1514.
5. J. D. DIXON, "High speed computation of group characters," *Numer. Math.*, v. 10, 1967, pp. 446–450. MR **37** #325.
6. W. FEIT, *Characters of Finite Groups*, Benjamin, New York, 1967. MR **36** #2715.
7. J. K. MCKAY, "A method for computing the simple character table of a finite group," in *Computers in Mathematical Research*, R. F. Churchhouse and J. C. Herz (Editors), North-Holland, Amsterdam, 1968. MR **38** #1972.
8. J. K. MCKAY, *The Construction of the Character Table of a Finite Group from Generators and Relations*, Proc. Conf. Comput. Algebra (Oxford 1967), Pergamon Press, New York, 1969.
9. J. NEUBÜSER, *Investigations of Finite Groups on Computers*, Proc. Conf. Comput. Algebra (Oxford 1967), Pergamon Press, New York, 1969.
10. P. G. RUDD & E. R. KEOWN, *The Computation of Irreducible Representations of Finite Groups of Order* 2^n, $n \leqq 6$, Proc. Conf. Comput. Algebra (Oxford 1967) Pergamon Press, New York, 1969.