Conjugacy Class Sums for Induced Modules: Construction and Applications*

Holger W. Gollan†
Institute for Experimental Mathematics
Ellernstraße 29
D-4300 Essen 12, Germany

Submitted by Gerhard O. Michler

ABSTRACT

We show how to construct conjugacy class sums for an arbitrary induced representation by using just one representative for each conjugacy class. Some ideas which speed up the calculation in special cases are presented together with examples. In the second part we give two applications of such class sums to monomial representations.

INTRODUCTION

Let G be a finite group, F any field, $H \leqslant G$ a subgroup of G, and N an FH-module. Then there is a well-known construction of the induced module $M = N\uparrow^G$, which is an FG-module of dimension $\dim M = \dim N \cdot |G : H|$. In general, this module is not irreducible, nor even indecomposable, even if N is irreducible. One way to get information about the composition factors of $N\uparrow^G$, at least in positive characteristic, is Parker's Meat-Axe [12]. Unfortunately, since it is a probabilistic algorithm, it may involve a lot of matrix multiplications and the computation of null spaces of large matrices. As in the paper by Gollan and Ostermann [6] on the special case of a permutation module, we would like to give an idea of how to work out at least the direct summands of an arbitrary induced module corresponding to the different

*This work has been supported by the Deutsche Forschungsgemeinschaft and Carleton University, Ottawa.

†E-mail: mat422@vm.hrz.uni-essen.de.

655 Avenue of the Americas, New York, NY 10010 0024-3795/93/$6.00

blocks of the group algebra FG. The basic idea will be the same: Use just one representative for each conjugacy class to compute the conjugacy class sums, and then use the character table of G to get the block idempotents, which finally give the desired decomposition. Unlike the Meat-Axe, this method also works in the case of $\operatorname{char} F = 0$, and it works there even better than in positive characteristic, since each block of FG contains exactly one irreducible module.

The idea for this paper goes back to a discussion with S. Linton about a joint paper by Linton, Michler, and Olsson [11] in which they use a model for the symmetric groups due to Inglis, Richardson, and Saxl [8] to compute Fourier transforms. They use basically the same approach presented here, but we will describe it in a different way, which will enable us first to give some hints on the implementation and second to generalize the monomial case they have to arbitrary induced modules. One of the two applications in the second part will be the use of class sums and models for the computation of Fourier transforms in the case of the smallest Janko group J_1 using the ideas of Linton, Michler, and Olsson [11].

In Section 1 we will go back to [6] and restate the result, since it is vital for our idea, whereas in Section 2 we look at what was said there about arbitrary induced modules. The basic idea which gets the thing working will be presented in Section 3 for a monomial representation, and will be generalized to arbitrary induced modules in Section 4. Section 5 will give some remarks on the implementation, sometimes restricted to special cases, and will reduce the general problem essentially to the word problem for matrix groups.

Part II gives two applications of conjugacy class sums. In Section 6 a joint effort with John D. Dixon (Carleton) to construct a list of primitive linear groups of small degrees is presented, together with an example of how to construct representations with the help of models and conjugacy class sums. Chapter 7 finishes the paper with an application to computing the k-fold convolution of a certain probability on the smallest Janko group J_1 using a model for J_1 [5], the ideas of Linton, Michler, and Olsson [11], and class sums.

We will assume that the reader is familiar with the basics of representation theory as may be found in the books by Feit [4], Puttaswamaiah and Dixon [13], or Landrock [10]. A good account of how to work with representations on the computer can be found in a paper by Schneider [14].

PART I. CONSTRUCTION

1. *The Case of a Permutation Module*

Throughout the paper G will always denote a finite group and $H \leqslant G$ will always be a subgroup of G. Furthermore, let F be a field, for the moment of arbitrary characteristic, and let N be an FH-module and $M = N\uparrow^G$ be the induced FG-module. In this section we will restrict ourselves to the special case where $N = I_H$, the trivial F-representation of H. In this situation the induced module $M = (I_H)\uparrow^G$ is the permutation module of G corresponding to the action of G on the cosets of H in G, and we get a map $\varphi : G \to S_m$, where $m = |G : H|$ is the index of H in G. This mapping does not have to be injective, which means that the permutation module does not have to faithful, but in any case we get G, via φ, as a transitive permutation group of degree m, possibly with several elements acting as the identity. Therefore we can go back to the paper by Gollan and Ostermann [6] on conjugacy class sums for permutation modules, and with some notation we can restate the main result.

CLASS SUM FORMULA. *Let G be a finite permutation group acting on a finite set Ω, not necessarily faithful. For a given $x \in G$ let $P(x) = \{(i, i^x) | i \in \Omega\} \subseteq \Omega^2$ be the set of "pairs" of x. Furthermore, let F be any field and $M = F\Omega$ the permutation module with G acting on the right. For a given $x \in G$ let $A = A_x = (a_{i,j})$ be the conjugacy class sum of the class x^G in this permutation representation. Then we have*

$$a_{i,j} = \frac{|x^G| \cdot \left|P(x) \cap (i,j)^G\right|}{\left|(i,j)^G\right|}.$$

REMARK. It should be noted that the formula is valid even in the case when G is not faithful, although in the original paper nothing is said about the faithfulness of G. The proof obviously does not depend on any assumption in this direction.

2. *The Case of an Arbitrary Induced Module—the Old Approach*

The last section of [6] dealt with the case of an arbitrary induced module and, unfortunately, gave some wrong impressions of what can be done in this more general situation. The reason for this was an assumption on what one wishes to look for in the arbitrary case. To illustrate this we restate the main assumption and give an example which shows that under this assumption one representative for a conjugacy class is not enough, even for a small case. We will come back to this example later to show how the new idea of the present paper works with just one representative.

To get to arbitrary induced modules, let N be an arbitrary FH-module with basis $v_1, \ldots, v_n$, and let $t_1 = 1, \ldots, t_m$ be a right transversal of H in G.

Then the induced module $M = N\uparrow^G$ has a basis $v_i \otimes t_j$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, and the action of an element $g \in G$ on a basis vector is given by

$$(v_i \otimes t_j)g = v_i h_j \otimes t_k, \tag{$*$}$$

where $t_j g = h_j t_k$ with $h_j \in H$. Therefore the matrix of g for its action on M is determined by two factors, first the permutation action of g on the right cosets of H in G, and second the matrices of the elements h_j corresponding to their action on N. Now, the main assumption of [6] was that one needed to look for elements $x \in G$ such that for any $g \in G$ the matrices of g and g^x differed only by a permutation of the nonzero blocks. For this to work for all $g \in G$, the element $x \in G$ must have the following property

$$(\mathscr{P}) \qquad t_j g = h_j t_{j^g} \;\Rightarrow\; t_{j^x} g^x = h_j t_{j^{gx}} \qquad \forall g \in G, j \in \{1, \ldots, m\}.$$

Here we view G as a permutation group acting on the set $\{1, \ldots, m\}$, corresponding to its action on the right cosets $\{Ht_j | 1 \leqslant j \leqslant m\}$. Then the following can be proved [6]:

LEMMA . *There are at most* $|Z(H)| \cdot m$ *elements in* G *with the property* $(\mathscr{P})$.

Actually, the elements of H occurring on the two sides of $(\mathscr{P})$ may be different and we still get what we want, as long as their matrices under φ are the same. The number of elements x with this weaker condition is at most $|Z(H)| \cdot m \cdot |\mathrm{Ker}\, \varphi|$, and obviously the case of a permutation module is the extreme one. Then each element of G satisfies the above condition.

So, knowing the induced matrix for a $g \in G$, there are in general only a few other matrices for elements in G which can be computed by just permuting the nonzero blocks, and one can get the impression that one representative is not enough to compute a complete conjugacy class sum.

Let us illustrate this with a small example, which we will meet again later in this paper.

EXAMPLE

Let $G = S_4 = \langle t = (1,2),\ s = (1,2,3,4) \rangle$ be the symmetric group on four letters, and let $H = \langle (1,2), (3,4) \rangle$ be a subgroup of order 4, isomorphic to the Klein four-group $V_4 \simeq C_2 \times C_2$. Now we define a linear representation $\varphi : H \to \{\pm 1\}$ by

$$\varphi((1,2)) = +1, \qquad \varphi((3,4)) = -1.$$

As a right transversal for H in G we choose

$$T = \{t_1 = 1,\, t_2 = (1,3),\, t_3 = (1,4),\, t_4 = (2,3),\, t_5 = (2,4),\, t_6 = (1,3,2,4)\}.$$

We are interested in the conjugacy class C of G of elements of order 2 and cycle structure 2^2 in the natural representation, so $C = \{x = (1,2)(3,4), y = (1,3)(2,4), z = (1,4)(2,3)\}$. To get on with our computation we have to get the matrices of the induced representation $\psi = \varphi\uparrow^G$ for the three elements of C. This is an easy task using $(*)$ and the choice of T and φ above, and we get

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

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

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

and therefore the conjugacy class sum $\hat{C}$ for the class C is given by

$$\hat{C} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

But the important thing to notice at this point is that the number of $+1$'s is different for different elements in the class, so going from one element to another is not only a permutation of the entries, not even in this small example. One can get around this here by choosing $t_3 = (1,4,3) = (3,4)(1,4)$. This multiplies the third row and column by -1, giving $+1$ twice in each of the matrices for the three elements of C. But it seems to be hard to choose the right transversal in the beginning to get things going in the right way.

Since permuting the entries usually is not enough, there has to be another idea to solve the problem with the help of only one representative. As we will see in the next chapter, this new idea is surprisingly close to the special case of a permutation module, and it uses this special case after transferring the problem with the help of a homomorphism to a permutation group.

3. *The Case of a Monomial Representation—the New Approach*

Let us first recall our basic notation: G is a finite group with a subgroup H, F is a field, and $\varphi : H \to \mathrm{GL}_n(F)$ is a representation of H over F of some degree n. For the moment we restrict to the case of $n = 1$ to get a feeling for the general case of an arbitrary n. So we have a linear representation $\varphi : H \to F$, and the induced representation $\psi = \varphi \uparrow^G : G \to \mathrm{GL}_m(F)$ is monomial, where $m = |G : H|$.

The idea is to use the class sum formula of Section 1, so we have to transform G into a permutation group acting on some set Ω. Since ψ is monomial, the image $\psi(G)$ acts on the set of all vectors of length m with exactly one nonzero entry taken from $\varphi(H)$, and this obviously generalizes the permutation case where $\varphi(H) = \{1\}$. Therefore we define

$$\Omega = \left\{(\alpha_1, \ldots, \alpha_m) \in F^m \middle| \exists 1 \leqslant i \leqslant m : \alpha_i \in \varphi(H),\ \alpha_j = 0\ \forall j \neq i\right\}.$$

Since there is only one nonzero entry α_i for each element in Ω, we might as well take this entry and its position to get a shorter notation for the elements of Ω, namely

$$\Omega = \left\{(i, \alpha_i) \middle| 1 \leqslant i \leqslant m,\ \alpha_i \in \varphi(H)\right\}.$$

Now we get a map $\kappa : \psi(G) \to S_\Omega$. Putting things together, we end up with a map $\rho = \kappa \circ \psi : G \to S_\Omega$, and we can view G as a permutation group on Ω. The map κ is even injective, so we get an embedding there, and this is the final key for the basic procedure:

PROCEDURE 1 (Class sum formula).

Input: A finite group G, a subgroup $H \leqslant G$, and a monomial representation $\psi = \varphi \uparrow^G : G \to \mathrm{GL}_m(F)$, where $m = |G : H|$ and $\varphi : H \to F$ is a linear representation.

(1) Compute Ω as above.
(2) Compute $\kappa : \psi(G) \to S_\Omega$ and $\rho : G \to S_\Omega$.
(3) Use the old Class Sum Formula to get the conjugacy class sum for G via the permutation representation ρ.
(4) Use κ^{-1} to get the conjugacy class sum in the representation $\psi = \varphi \uparrow^G$.

The only thing that needs some explanation is the notation κ^{-1}. Since $\kappa : \psi(G) \to \rho(G)$ is an isomorphism, there is an inverse map $\kappa^{-1} : \rho(G) \to \psi(G)$. The important thing to note here is that this map extends to an epimorphism between the two algebras $F\rho(G)$ and $F\psi(G)$, which we call κ^{-1} again. With the help of this extension we find the conjugacy class sum for ψ under (4), since

$$\sum_{y \in x^G} \psi(y) = \sum_{y \in x^G} \kappa^{-1}\kappa(\psi(y)) = \kappa^{-1}\left(\sum_{y \in x^G} \rho(y)\right).$$

Some more remarks should be made about several things in the above construction.

REMARKS.

(i) There is more structure in the map ρ, since elements of $\psi(G)$ can move around the vectors of Ω in a very restricted way only, i.e., once the image of a vector $(\alpha, 0, \dots, 0)$ is known, also all the images of all the vectors of the form $(\gamma\alpha, 0, \dots, 0)$ for $\gamma \in \varphi(H)$ are known. Actually this gives ρ as a homomorphism $\rho : G \to C_k \wr S_m$, a wreath product, where $k = |\varphi(H)|$.

(ii) ρ is actually the permutation representation of G on the cosets of $\operatorname{Ker}\varphi$; therefore it is transitive, which helps in the computation of the conjugacy class sums (see [6]).

(iii) With (ii) in mind it is clear that, as in Section 1, ρ doesn't have to be a faithful permutation representation.

Now let us come back to our example from the end of Section 2 to see things in action. Since $\varphi(H) = \{\pm 1\}$, the set Ω is given by $\Omega = \{\pm e_i | 1 \leqslant i \leqslant 6\}$, where e_i is the ith standard vector with zeros in all positions except a 1 in coordinate i. So $|\Omega| = 12$, and we have to write G as a subgroup of S_Ω via

φ. This is an easy exercise, and we get the following images under ρ for the interesting elements:

$$\begin{aligned}
\rho((1,2)) &= (e_2, e_4)(-e_2, -e_4)(e_3, e_5)(-e_3, -e_5)(e_6, -e_6),\\
\rho((1,2,3,4)) &= (e_1, -e_2, -e_6, -e_5)\\
&\quad (-e_1, e_2, e_6, e_5)(e_3, -e_4, -e_3, e_4),\\
\rho((1,2)(3,4)) &= (e_1, -e_1)(e_2, -e_5)(-e_2, e_5)(e_3, -e_4)\\
&\quad (-e_3, e_4)(e_6, -e_6),\\
\rho((1,3)(2,4)) &= (e_1, -e_6)(-e_1, e_6)(e_2, e_5)(-e_2, -e_5)\\
&\quad (e_3, -e_3)(e_4, -e_4),\\
\rho((1,4)(2,3)) &= (e_1, e_6)(-e_1, -e_6)(e_2, -e_2)(e_3, e_4)\\
&\quad (-e_3, -e_4)(e_5, -e_5).
\end{aligned}$$

Using $\rho(s)$ and $\rho(t)$, we can compute the orbits of $\rho(G)$ on Ω^2, which correspond to the orbits of the stabilizer of one element of Ω, say $+e_1$, on Ω. But by remark (ii) above, this stabilizer is $\rho(\operatorname{Ker}\varphi)$, so in our case we are looking for the orbits of $\rho(\langle t\rangle)$, or equivalently the orbits of $\rho(t)$ on Ω. So we get the following orbits:

$$\{e_1\}, \{-e_1\}, \{e_2, e_4\}, \{-e_2, -e_4\}, \{e_3, e_5\}, \{-e_3, -e_5\}, \{e_6, -e_6\},$$

and therefore we have to compute seven entries of the conjugacy class sum. We do this by using $\rho(x) = (e_1, -e_1)(e_2, -e_5)(-e_2, e_5)(e_3, -e_4)(-e_3, e_4)(e_6, -e_6)$ and the old Class Sum Formula, and we get the following entries:

$$\begin{aligned}
a_{e_1, e_1} &= 0,\\
a_{e_1, -e_1} &= \frac{3\times(2+2)}{12} = 1,\\
a_{e_1, e_2} &= 0,\\
a_{e_1, -e_2} &= 0,\\
a_{e_1, e_3} &= 0,\\
a_{e_1, -e_3} &= 0,\\
a_{e_1, e_6} &= \frac{3\times(2+2+2+2)}{2\times 12} = 1.
\end{aligned}$$

This gives us all the entries of one row of the conjugacy class sum, corresponding to $+e_1$, in the permutation representation of G on Ω, and we get the following row:

$$\begin{array}{cccccccccccc} e_1 & -e_1 & e_2 & -e_2 & e_3 & -e_3 & e_4 & -e_4 & e_5 & -e_5 & e_6 & -e_6 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}$$

Now we just have to translate this back into an element of the group algebra $F\psi(G)$. But this is no problem at all, because each element in the row above just tells us how many times the vector $+e_1$ is mapped onto a vector $\varepsilon_i e_i$, $\varepsilon_i \in \{\pm 1\}$, $1 \leqslant i \leqslant 6$. For all these cases we know exactly what the first row of a corresponding element in $F\psi(G)$ has to look like. To do this example explicitly, the first row of the conjugacy class sum for the monomial representation is the sum of the following rows:

$$\begin{array}{rrrrrrr} -e_1: & -1 & 0 & 0 & 0 & 0 & 0 \\ e_6: & 0 & 0 & 0 & 0 & 0 & 1 \\ -e_6: & 0 & 0 & 0 & 0 & 0 & -1 \end{array}$$

which gives the following first row:

$$-1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0$$

Having the first row and the transitivity of G on the cosets of H in G, one can easily compute the full matrix for the conjugacy class sum, which turns out to be exactly $\hat{C}$, as computed at the end of Section 2.

REMARKS.

(iv) Using this method to calculate block idempotents, one would, of course, first calculate the first row of the block idempotent as a linear combination of the first rows of the conjugacy class sums, and do the construction of the full matrix only at the end.

(v) One does not even have to compute the whole matrix for the block idempotent, since one only has to find the linearly independent rows of this matrix. They span the right invariant subspace, and the restriction of the action of $\psi(G)$ to this subspace gives the desired direct summands corresponding to the block under consideration. Usually the dimension of this subspace is already known at the beginning.

(vi) Some of the rows to add up cancel, and recognizing this early may save a lot of time and work.

(vii) Obviously the old case is a special case of the above with $\varphi(h) = 1$ $\forall h \in H$, because then $\operatorname{Ker} \varphi = H$, so we have just the permutation representation of G on the cosets of H in G.

Having done the linear case, it is now easy to generalize the above to arbitrary induced modules, and we will do this in the next section.

4. *The General Case*

Let us now come back to the general situation: We have a group G with a subgroup $H \leqslant G$ of index $|G : H| = m$. Moreover we have a field F and a representation $\varphi : H \to \mathrm{GL}_n(F)$ of H of degree n, and this gives an induced representation $\psi = \varphi \uparrow^G : G \to \mathrm{GL}_{nm}(F)$ of G. Note that the matrices in $\psi(G)$ are $m \times m$ monomial block matrices, i.e., there are $m \times m$ blocks of size n, and in each block row and column there is exactly one nonzero matrix.

Going from the linear case to an arbitrary induced module, nearly all of the above remains true, maybe with some slight modifications. The only thing that needs a closer look is the set Ω. Even here the generalization is easy, if we look at the old Ω in the right way. The elements have been vectors with exactly one nonzero entry, and this entry was an element of $\mathrm{Im}(\varphi)$. This element was an element of the field F, but we can also view it as a 1×1 matrix over F, and this point of view gives us the right generalization for Ω. So we no longer look at vectors with one nonzero entry, but we take m-tuples with this property. And the entries are no longer elements of the field F or 1×1 matrices over F, but $n \times n$ matrices. This leads to the following definition:

$$\Omega = \Big\{ (M_1, \dots, M_m) \Big| \exists 1 \leqslant i \leqslant m: \\ M_i \in \varphi(H) \subseteq \mathrm{Mat}_n(F),\ M_j = 0 \in \mathrm{Mat}_n(F)\ \forall j \neq i \ \Big\}.$$

Again we can write

$$\Omega = \big\{ (i, M_i) \big| 1 \leqslant i \leqslant m,\ M_i \in \varphi(H) \big\}.$$

Now it is easy to follow all the statements of Section 3 with this new set Ω under the general hypothesis, and it turns out that nearly everything remains true. Only a few modifications have to be made; e.g., in remark (i) the map ρ now becomes $\rho : G \to S_k \wr S_m$. Moreover, in contrast with remark (iv), now the first n rows of conjugacy class sums have to be computed.

This finishes the description of the procedure for computing conjugacy class sums for arbitrary induced modules, and we want to close this section by stating that procedure again for this general case:

PROCEDURE 2 (Class sum formula)

Input: A finite group G, a subgroup $H \leqslant G$, and an induced representation $\psi = \varphi\uparrow^G : G \to \mathrm{GL}_{nm}(F)$, where $m = |G:H|$ and $\varphi : H \to \mathrm{GL}_n(F)$ is a representation of degree n.

(1) Compute Ω as above.
(2) Compute $\kappa : \psi(G) \to S_\Omega$ and $\rho : G \to S_\Omega$.
(3) Use the old Class Sum Formula to get the conjugacy class sum for G via the permutation representation ρ.
(4) Use κ^{-1} to get the conjugacy class sum in the representation $\psi = \varphi\uparrow^G$.

In the next section we make some comments on the implementation of the procedure. As we will see, there is a nice way to work out things in the linear case.

5. *Notes on the Implementation*

There is a running version of the procedure, written as part of the computer algebra system AXIOM.[1] One reason for this was the capability of the system to work over finite fields as well as over the algebraic numbers. This implementation is used for the first application presented in the second part. There is also a C implementation, which was written for the second application.

Let us begin with some general remarks: The permutation representation $\rho(G)$ may be large, since it is the action of G on the cosets of $\operatorname{Ker}\varphi$ in G. In the worst case it may be the regular representation. So we look for ways to do the calculations in the representation $\psi(G)$ with κ and $\rho(G)$ in mind. Before we begin, let us introduce some notation. From the description

$$\Omega = \{(i, M_i) \mid 1 \leqslant i \leqslant m,\ M_i \in \varphi(H)\}$$

[1]AXIOM is a trademark of the Numerical Algorithms Group Ltd.

for Ω we can write the elements of $\psi(G)$ as a sequence of pairs, say

$$x = \left[(p_i, M_i)\middle|1 \leqslant i \leqslant m\right],$$

and the action of x on $\omega = (i, M) \in \Omega$ is given by $(i, M)^x = (p_i, M \cdot M_i)$. This represents a compact way to store and work with induced matrices and has been implemented into AXIOM as new datatypes as part of the procedure.

If we look at the old formula for the conjugacy class sums, we see that we basically have to work out orbits of $\psi(G)$ on Ω^2 or, since $\psi(G)$ is transitive on Ω, orbits of a stabilizer of one $\omega \in \Omega$ on Ω. For this special element ω we may choose $\omega = (1, \mathrm{Id}) \in \Omega$, so we are looking for the orbits of S on Ω, where $S = \mathrm{Stab}_{\psi(G)}(\omega) = \psi(\mathrm{Ker}\,\varphi)$. Now let $x = [(p_i, M_i)] \in \psi(G)$ be any element. We want to work out the conjugacy class sum $x^{\psi(G)}$. Using some of the remarks in [6], we see that it is enough to look at representatives for cycles of x, viewed as a permutation on Ω. Therefore let $[(i, M), (i, M)^x]$ be such a representative. We have to find $g \in \psi(G)$ such that $(i, M)^g = (1, \mathrm{Id})$. Then

$$\left[(i, M), (i, M)^x\right]^g = \left[(i, M)^g, (i, M)^{xg}\right] = \left[(1, \mathrm{Id}), (i, M)^{xg}\right],$$

and we know the orbit of S on Ω that is involved, namely the one containing $(i, M)^{xg}$. Now, since the elements of $\psi(G)$ are induced matrices, we can divide the search for g into two parts. First we look for a $g' = [(q_i, N_i)] \in \psi(G)$ such that $(i, M)^{g'} = (1, M')$, so $q_i = 1$, $M' = M \cdot N_i$. This obviously involves only the action of G on the cosets of H in G. The second step is to find an element $h \in \psi(G)$ with $(1, M')^h = (1, \mathrm{Id})$. Now it is easy to see that $h \in \psi(H)$, say $h = \psi(h')$, and that $\varphi(h') = M'^{-1}$.

From the computational point of view the first part deals with a Schreier vector and the successive action of generators of $\psi(G)$, which is easy in general, whereas in the second part we have to look for an element of H with a given image under φ. This seems to be hard in general; it is like the word problem for matrix groups. But there may be cases where it is easy, because $\varphi(H)$ is well known. This is certainly the case when $\varphi(H)$ is cyclic and we know the generator, and this situation occurs when we are in the monomial case, since then $\varphi(H)$ is a finite subgroup of the multiplicative group F^* and therefore cyclic.

Another improvement works in all cases. Suppose we know the solution for one pair $[(i, M), (i, M)^x]$. Then it is easy to solve the first step of the above reduction for any other pair $[(i, \tilde{M} \cdot M), (i, \tilde{M} \cdot M)^x]$ with $\tilde{M} \in \varphi(H)$. Since we know a $g \in \psi(G)$ with

$$\left[(i, M), (i, M)^x\right]^g = \left[(1, \mathrm{Id}), (i, M)^{xg}\right] = \left[(1, \mathrm{Id}), (j, M')\right],$$

it follows that

$$\left[(i, \tilde{M} \cdot M), (i, \tilde{M} \cdot M)^{x}\right]^{g} = \left[(i, \tilde{M} \cdot M)^{g}, (i, \tilde{M} \cdot M)^{xg}\right]$$
$$= \left[(1, \tilde{M}), (j, \tilde{M} \cdot M')\right],$$

so we can avoid the first step of the calculation for all but one pair for each $1 \leqslant i \leqslant m$, which saves a lot of multiplications.

There is still another improvement which works extremely well in the monomial case, and may also save time in the general situation. In Remark (vi) of Section 3 and the example there, we have seen that sometimes things add up to zero. The reason for this, which can already be seen in the example, is that there are two elements with the same nonzero position in the same orbit of Ω under S; in the example this is the orbit $\{e_6, -e_6\}$. To see this, let us go to the general situation, and let us suppose that there is an $1 \leqslant i \leqslant m$ and two matrices $M_1, M_2 \in \varphi(H)$ with $M_1 \neq M_2$ such that $\omega_1 = (i, M_1)$ and $\omega_2 = (i, M_2)$ are in the same orbit. This means that there is a $g \in \psi(\operatorname{Ker} \varphi) = S$ with

$$\omega_1^g = (i, M_1)^g = (i^g, M_1^g) = \omega_2 = (i, M_2).$$

Now remember that the elements of $\psi(G)$ are $m \times m$ monomial block matrices. Therefore this just means that the ith block row of g has its nonzero matrix in the ith block column, hence on the diagonal, and that this matrix is just $M_g = M_1^{-1} \cdot M_2 \neq \mathrm{Id}$. Now let T be the set of all such elements in S which have their nonzero matrix of the ith block row on the diagonal. It is easy to see that T is a group, since the product of two such elements is again in T. But this means that the matrices M_h for $h \in T$ on the ith diagonal block position form a group T' as well. Since id, $g \in S$ and $M_g \neq \mathrm{Id}$, this group is not the identity, and therefore T' is a nontrivial subgroup of $\varphi(H)$. Now let $\{\omega_1, \omega_2, \ldots, \omega_k\}$ be the orbit of ω_1 under T. Then, at a certain point in our calculations, we have to sum all the matrices M_j with $\omega_j = (i, M_j)$. But the set of all these M_j is just the set of all $M_1 \cdot M_h$, where M_h runs over all matrices in T'. Therefore

$$\sum_{j=1}^{k} M_j = \sum_{M_h \in T'} M_1 \cdot M_h = M_1 \cdot \sum_{M_h \in T'} M_h.$$

Since T' is a nontrivial matrix group the sum $\sum_{M_h \in T'} M_h$ basically counts the multiplicity of the trivial representation in the natural representation of T'.

If, as a special case, we are in the monomial situation, then T' is a nontrivial matrix group of degree 1; hence there can be no trivial representation inside this natural representation; therefore $\Sigma_{M_h \in T'} M_h = 0$ and we get the cancellation we have seen in the example of Section 3. Using this, one can save a lot of unnecessary work during the computation. Moreover, it is clear that this works not only for the orbit $\{\omega_1, \ldots, \omega_k\}$, but for each $(i, M_j) \in \Omega$; hence in each conjugacy class sum the ith block in the first block row is a zero matrix.

PART II. APPLICATIONS

6. *Primitive Linear Groups of Small Degree*

As already mentioned in Part I, one can use the class sums to calculate block idempotents and to split off the direct summands belonging to the corresponding block. In characteristic 0 each character is a block on its own, and if a character has multiplicity one in the induced representation, then one can use the above method to find representing matrices for that character.

Since projectively there are only finitely many primitive linear groups over the complex numbers of a given degree, John D. Dixon and I am trying to give a list of all these groups for small degrees as explicit matrices. This will involve other methods of constructing these representations by Dixon [3], already existing lists of rational matrix groups (see Holt and Plesken [7]), and our method of conjugacy class sums. To illustrate this let us now go to another small example.

EXAMPLE. We look at the double cover $2\,A_5$ of the alternating group A_5. This group can be written as a finitely presented group [1]

$$G = 2\,A_5 = \langle r, s, t \,|\, r^2 = s^3 = t^5 = rst \rangle$$

Before we start let us fix some notation. Let $\omega = e^{2\pi i/5}$ be a 5th root of unity, and let $H = \langle t \rangle$, which is cyclic of order 10. We want to induce the linear representation φ of H defined by $\varphi(t) = -\omega$. Now we have to work with the action of G on the 12 cosets of H in G, and choosing the transversal as

$$T = \{1, r, s, srs, rt^2, rt, st^{-1}r^{-1}, sr^{-1}s^{-1},$$

$$rt^2s, srs^{-1}t^{-2}, st^{-1}r^{-1}t, st^{-1}rts^{-1}\},$$

we can write our generators as the following sequences:

$$r = \big[(2,1),(1,-1),(6,-\omega),(7,1),(8,-\omega^4),(3,\omega^4),(4,-1),(5,\omega),$$
$$(11,1),(12,1),(9,-1),(10,-1)\big]$$

$$s = \big[(3,1),(1,\omega^4),(2,-\omega),(8,1),(9,1),(4,-\omega^4),(5,-1),(6,\omega),$$
$$(7,1),(12,-\omega),(10,-\omega^4),(11,-1)\big]$$

$$t = \big[(1,-\omega),(6,1),(2,1),(3,-1),(4,1),(5,1),(11,1),(7,1),$$
$$(8,-\omega^4),(9,\omega),(10,1),(12,-\omega^4)\big].$$

Here the ith entry in a sequence gives the image of the point $(i, \mathrm{Id}) \in \Omega$ under the corresponding element, e.g. $(3, \mathrm{Id})^r = (6, -\omega)$. Since $\operatorname{Ker} \varphi = 1$, each orbit of the stabilizer contains only one element, and that makes things easier for this example. Let us now look at the conjugacy class of t. This class has cardinality 12, and, since all orbits of the stabilizer have length 1 and therefore all orbits of G on Ω^2 have length 12, we don't have to worry about all the entries in the old Class Sum Formula, but only about the intersections. To work out their cardinalities we just work through all elements (i, x) with $1 \leqslant i \leqslant 12$ and $x \in \varphi(H)$, so $x \in \{(-\omega)^0, \ldots, (-\omega)^9\}$. For all these elements we have to reduce the pair $[(i, x), (i, x)^t]$ to a pair of the form $[(1, 1), (j, x')]$. As in Section 5, we do the first step only once for each i and use the fact that $\varphi(H)$ is cyclic for the second step. Moreover, we can save even more work if we think about the cycles of t, viewed as a permutation on the elements (i, x). This leads to exactly four cases we have to handle.

The first case is $i = 1$. So we look at pairs

$$\big[(1,x),(1,x)^t\big] = \big[(1,x),(1,-\omega x)\big].$$

But this can be reduced to $[(1, 1), (1, -\omega)]$, and therefore we get to the orbit of $(1, -\omega)$ exactly 10 times.

The second, similar case deals with $i = 12$. One representative for this case is the pair

$$\big[(12,1),(12,1)^t\big] = \big[(12,1),(12,-(\omega^4))\big].$$

This can be reduced to some pair $[(1, x), (1, -(\omega^4)x]$, and we are in the first case again: just replace $-\omega$ by $-(\omega^4)$.

The third and fourth cases are similar, so we will only deal with the third case in detail and just state the result for the fourth. Case 3 starts with a pair

$$\left[(2,1),(2,1)^t\right] = [(2,1),(6,1)]$$

This can be reduced by

$$[(2,1),(6,1)]^s = \left[(1,\omega^4),(4,-(\omega^4))\right],$$

which may be reduced further to

$$\left[(1,\omega^4),(4,-(\omega^4))\right]^{t^6} = \left[(1,1),(3,-(\omega^4))\right],$$

and since the pair we started with comes from a cycle of length 10, we know that we get this orbit exactly 10 times. Now multiplying with powers of $-\omega$ and using the action of powers of t, we can work out all the orbits corresponding to pairs $[(2, x), (6, x)]$; e.g., by the result at the end of Section 5 we get for the pair $[(2, \omega), (6, \omega)]$ that it can be reduced to

$$\left[(1,\omega^4\omega),(4,-\omega^4\omega)\right] = [(1,1),(4,-1)].$$

Doing this for all powers [therefore for all elements $(2, x)$] and being careful to avoid double counting, we see that we find the following orbits, each 10 times:

$$(3,-\omega^4),(4,-1),(5,\omega),(6,-\omega^2),(2,\omega^3).$$

In the same way the last case can be solved, and we find the following orbits, again each of them 10 times:

$$(4,\omega^4),(5,-1),(6,\omega),(2,-\omega^2),(3,\omega^3).$$

Putting all these things together, we find the following first row for the conjugacy class sum of the conjugacy class of t in this induced representation:

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

which can be extended to the whole matrix by multiplication with elements of $\psi(G)$; e.g., to get the fourth row, we have to multiply by an element $g = [(p_i, M_i)]$ with $p_4 = 1$, $M_4 = \mathrm{Id}$, say $g = trts$.

Doing the above for all conjugacy classes, we can e.g. construct one of the 2-dimensional representations of $2\,A_5$ by calculating the corresponding block idempotent (see [6]), and we get the following matrices:

$$r = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & -\omega \\ \omega^4 & 0 \end{pmatrix}, \qquad t = \begin{pmatrix} -\omega & 0 \\ -1 & -\omega^4 \end{pmatrix}.$$

Of course, this method works as well for larger groups and larger dimensions. As another example, a 10-dimensional representation of the smallest Mathieu group M_{11} is given in the appendix.

Both of these calculations have been performed using the AXIOM implementation of the procedure.

7. k-FOLD CONVOLUTIONS OF PROBABILITIES

The second application comes from statistics and deals with k-fold convolutions of certain probabilities on groups and Fourier transforms. To learn more about this the reader is referred to the book by Diaconis [2] and the paper by Linton, Michler, and Olsson [11]. We will also need a little knowledge about models of finite groups, especially for the smallest Janko group J_1; all necessary information about this can be found in Gollan [5]. We take J_1 as defined in Janko's original paper [9], i.e., $J_1 = \langle a, b \rangle \leqslant \mathrm{GL}_7(11)$. Then $u = a \cdot b$ has order 10, and $t = u^5$ is an involution. Let $H = \mathrm{Cen}_{J_1}(t)$ be the centralizer of t in J_1. Then $H = 2 \times A_5$ and $|J_1 : H| = 1463$. Now define a linear character λ of H by putting $\lambda(A_5) = +1$ and $\lambda(2) = -1$. Then the set $\{\lambda \uparrow^{J_1}, I_{J_1}\}$ is a model for J_1, i.e.

$$\sum_{\chi \in \mathrm{Irr}(J_1)} \chi = I_{J_1} + \lambda \uparrow^{J_1}.$$

Denote $\pi := \lambda \uparrow^{J_1}$, $\mathrm{id} := I_{J_1}$.

Now let f be any function on J_1. Then the Fourier transform $\hat{f}(\rho)$ of f at a representation ρ of J_1 is defined by

$$\hat{f}(\rho) = \sum_{g \in J_1} f(g) \cdot \rho(g)$$

Fourier inversion in our special situation can be written as (see [11])

$$f(g) = \frac{1}{|J_1|} \left\{ \mathrm{Tr}\left[\pi(g^{-1}) \cdot \hat{f}(\pi) \cdot M_{(1463)} \right] + \mathrm{Tr}\left[\mathrm{id}(g^{-1}) \cdot \hat{f}(\mathrm{id}) \cdot M_{(1)} \right] \right\},$$

where $M_{(d)}$ is a certain linear combination of block idempotents of dimension d, and hence of conjugacy class sums. Therefore we can compute this $M_{(d)}$ with our procedure. Now $\mathrm{id}(g^{-1}) \cdot \hat{f}(\mathrm{id}) \cdot M_{(1)} = (1)$, so the above simplifies to

$$f(g) = \frac{1}{|J_1|} \mathrm{Tr}\left(\pi(g^{-1}) \cdot \hat{f}(\pi) \cdot M_{(1463)} \right) + \frac{1}{|J_1|}.$$

The distance between two probabilities P and Q on J_1 is defined as

$$d(P, Q) := \frac{1}{2} \sum_{g \in J_1} |P(g) - Q(g)|.$$

If $Q = U$ is the uniform distribution, i.e. $U(g) = 1/|J_1|$ for all $g \in J_1$, then we get

$$d(f, U) = \frac{1}{2} \sum_{g \in J_1} \left| f(g) - \frac{1}{|J_1|} \right| = \frac{1}{2} \sum_{g \in J_1} \left| \mathrm{Tr}\left[\pi(g^{-1}) \cdot \hat{f}(\pi) \cdot M_{(1463)} \right] \right|$$

Now we define a special probability on J_1, namely $f(a) = f(b) = \frac{1}{2}$, $f(g) = 0$ elsewhere, and we ask for the distance of the k-fold convolution f^{*k} of f from the uniformity U. In a sense $f^{*k}(g)$ gives the probability of writing g as a word of length k in the two generators a and b, in other words a random walk on J_1.

Since convolution of f just means matrix multiplication for the Fourier transforms (see [2]), we can compute the distance with the following formula:

$$d(f^{*k}, U) = \frac{1}{2} \sum_{g \in J_1} \left| \mathrm{Tr}\left[\pi(g^{-1}) \cdot \hat{f}^{k}(\pi) \cdot M_{(1463)} \right] \right|$$

As mentioned in Section 5, there is a C implementation of the procedure for handling this question. It takes as input the monomial action of J_1 on the cosets of H, which just describes π, the conjugacy classes of J_1 in this

TABLE 1

k	$d(f^{*k}, U)$
1	0.999989
2	0.999977
3	0.999954
4	0.999909
5	0.999818
10	0.994725
25	0.157803
50	0.00403406
100	3.26295×10^{-6}
150	2.73239×10^{-9}
200	2.31437×10^{-12}

representation, and the character table of J_1. With this information the program computes

(1) base and strong generating set for J_1,
(2) the conjugacy class sums,
(3) the above matrix $M_{(1463)}$,
(4) the Fourier transform $\hat{f}(\pi)$.

Now the distances $d(f^{*k}, U)$ are computed step by step, and to go one step forward from k to $k+1$ the following things have to be done:

(5) Compute the matrix product $\hat{f}^{k+1}(\pi) \cdot M_{(1463)} = \hat{f}(\pi) \cdot [\hat{f}^k(\pi) \cdot M_{(1463)}]$.

(6) Run over all elements of J_1 with the help of base and strong generating set, and compute the sum of the traces.

As one can expect, the convergence against uniformity is slow. Some of the distances computed are given in Table 1. Each iteration step took around 17 min of CPU time on an IBM RS 6000-540. The situation here is obviously much harder than the case of symmetric groups (see [11]), but it shows that the method is feasible for other groups as well.

APPENDIX

The following two matrices give a 10-dimensional representation for M_{11}.

$$
\left.\begin{array}{cccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{13i\sqrt{2}+16}{6} & -\frac{3i\sqrt{2}}{2} & -\frac{3i\sqrt{2}}{2} & \frac{-i\sqrt{2}-16}{6} & i\sqrt{2}-3 & \frac{-i\sqrt{2}-16}{6} & -1 & i\sqrt{2}-3 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\frac{-7i\sqrt{2}+14}{6} & \frac{3i\sqrt{2}-2}{2} & \frac{3i\sqrt{2}-2}{2} & \frac{7i\sqrt{2}-2}{6} & 2i\sqrt{2}+1 & \frac{7i\sqrt{2}-2}{6} & 0 & 2i\sqrt{2}+1 & -1 & 0 \\
\frac{-i\sqrt{2}-10}{6} & -\frac{i\sqrt{2}}{2} & -\frac{i\sqrt{2}}{2} & \frac{-5i\sqrt{2}+4}{6} & -i\sqrt{2} & \frac{-5i\sqrt{2}+4}{6} & 0 & -i\sqrt{2} & 0 & -1
\end{array}\right),
$$

$$
\left.\begin{array}{cccccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{3i\sqrt{2}}{4} & \frac{3i\sqrt{2}}{4} & 0 & \frac{-i\sqrt{2}-1}{2} & \frac{-i\sqrt{2}-4}{4} & \frac{-i\sqrt{2}-2}{4} & \frac{-i\sqrt{2}-1}{2} & -1 & \frac{-i\sqrt{2}-4}{4} & \frac{-i\sqrt{2}-2}{4} \\
\frac{-3i\sqrt{2}-57}{11} & \frac{-3i\sqrt{2}+9}{11} & 1 & \frac{-9i\sqrt{2}+27}{11} & \frac{-30i\sqrt{2}+13}{11} & \frac{-14i\sqrt{2}+20}{11} & \frac{-3i\sqrt{2}+9}{11} & \frac{-32i\sqrt{2}+8}{11} & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0
\end{array}\right)
$$

The author would like to thank the Deutsche Forschungsgemeinschaft for its research grant as well as Carleton University for its financial support. Thanks are also due to the people at the Department of Mathematics and Statistics at Carleton, especially John D. Dixon, for all their help during my one-year stay at Ottawa.

REFERENCES

1 J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Oxford, U.P. 1985.

2 P. Diaconis, *Group Representations in Probability and Statistics*, Lecture Notes —Monogr. Ser. 11, Inst. of Mathematical Statistics, Hayward, Calif., 1988.

3 J. D. Dixon, *Constructing Representations of Finite Groups*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 1992.

4 W. Feit, *The Representation Theory of Finite Groups*, North Holland, Amsterdam, 1982.

5 H. W. Gollan, On the existence of models in some sporadic simple groups, *Arch. Math.*, to appear.

6 H. W. Gollan and T. W. Ostermann, Operation of class sums on permutation modules, *J. Symbolic Comput.* 9:39–47 (1990).

7 D. F. Holt and W. Plesken, *Perfect Groups*, Clarendon, Oxford, 1989.

8 N. F. J. Inglis, R. W. Richardson, and J. Saxl, An explicit model for the complex representations of S_n, *Arch. Math.* 54:258–259 (1990).

9 Z. Janko, A new finite simple group with abelian Sylow-2-subgroups, *J. Algebra* 3:147–186 (1966).

10 P. Landrock, *Finite Group Algebras and Their Modules*, London Math. Soc. Lecture Note Ser. 84, Cambridge U.P., 1983.

11 S. A. Linton, G. O. Michler, and J. B. Olsson, Fourier transforms with respect to monomial representations, *Math. Ann.*, to appear.

12 R. A. Parker, The computer calculation of modular characters: The Meat-Axe, in *Computational Group Theory* (M. Atkinson, Ed.), Academic, New York, 1984, pp. 267–274.

13 B. M. Puttaswamaiah and J. D. Dixon, *Modular Representations of Finite Groups*, Academic, New York, 1977.

14 G. J. A. Schneider, Computing with endomorphism rings of modular representations, *J. Symbolic Comput.* 9:607–636 (1990).

Received 30 October 1992; final manuscript accepted 10 May 1993