Available online at www.sciencedirect.com
ScienceDirect
Journal of Symbolic Computation 41 (2006) 1345–1359
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Irreducible constituents of monomial representations

Andrea Previtali*

Dipartimento di Fisica e Matematica, Università dell'Insubria, Via Valleggio, 11 Como–22100, Italy

Received 24 May 2005; accepted 8 September 2006
Available online 24 October 2006

Abstract

We describe an algorithm for obtaining the central primitive idempotents of the algebra associated with a monomial representation. As a consequence, we obtain its irreducible constituents. This is implemented in MAGMA, using an algorithm based on Dixon's modular approach. In the case of permutation representations, we get a simplified version of the algorithms of Michler and Weller.

Keywords: Ordinary representations and characters; Computational methods; Symbolic computation, algebraic computation

1. Introduction

Let G be a finite group and H a subgroup of G. Denote by V the permutation module afforded by right multiplication by G of the right cosets of H in G. In Michler (2001) Michler has described an algorithm yielding the irreducible constituents of the permutation character $\pi = (1_H)^G$ afforded by V, provided that π is multiplicity-free. In Michler and Weller (2002) Michler and Weller extend Michler's algorithm to any permutation character.

In this paper we extend further this algorithm to monomial characters. Our approach follows closely that of Michler and Weller. However, we introduce several theoretical and computational simplifications.

* Corresponding address: University of Insubria-Como, Dipartimento di Fisica e Matematica, Via Valleggio, 11 Room: V4.26, 22100 Como, Italy. Tel.: +39 031 2386316; fax: +39 031 2386119.
E-mail address: andrea.previtali@uninsubria.it.
URL: http://scienze-como.uninsubria.it/previtali/Research.html.

0747-7171/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2006.09.002

Let G and H be as above and let T denote a right transversal of H in G. We may define a diagonal action of G on $T \times T$ and call the orbits of this action *orbitals*. As is well known, there is a one-to-one correspondence between orbitals and the orbits of H on T. The latter are called *suborbits*. We can associate with any orbital a matrix, called the *adjacency matrix* of the orbital. Let μ be a linear character of H, $F = \mathbb{Q}(\mu)$, and V the FG-module affording μ^G. We distinguish a subset of orbitals which we call *μ-central* and show that $C = \mathrm{End}_G(V)$ is generated as a vector space by matrices that are in one-to-one correspondence with this subset. Define the *support* of a matrix as the list of positions corresponding to a non-zero entry. Then with any μ-central orbital we associate a generator for C whose support is the same as that of the adjacency matrix corresponding to the chosen orbital. Using the right regular representation for C with respect to this basis, we calculate $Z = \mathbf{Z}(C)$. Notice that this reduction is most effective when H is far from being a normal subgroup of G. In fact, the dimension of C is bounded above by the number of orbitals of G, or, equivalently, by the number of (H, H)-double cosets of G. This number coincides with the index of H in G if and only if H is a normal subgroup. We further reduce dimensions considering the right regular representation for Z.

In Chillag (1995, Theorem 1.1), Chillag proved that any semisimple, finite dimensional, commutative E-algebra A, with E a separable infinite field, is a *one-generator algebra*, that is $A = E[a]$ for some $a \in A$. We generalize this result to any separable field provided $|E| > \dim_E(A)$.

We specialize to $A = Z$ and $E = F$. So $Z = F[z]$, for some $z \in Z$. Using a *probabilistic* approach we determine z and use it to provide common eigenvectors for the elements of Z. This drastically improves on algorithms based on the determination of common eigenvectors, such as those of McKay, Dixon, and Schneider (see McKay (1970), Dixon (1967) and Schneider (1990)). These authors work with the regular permutation representation of G. In this situation Z is generated by the *conjugacy class sums* and the entries of the character table of G occur as components of common eigenvectors for Z. Applying Brauer's Theorem to splitting fields of group representations, we show that the eigenvalues of z belong to $\mathbb{Q}(\zeta_e)$, where ζ_e is a primitive eth root of 1, $e = \mathrm{Exp}(G)$.

As pointed out in Dixon (1967), it may not be possible to determine the eigenvalues of z when e is big. We find the smallest prime p satisfying $p \equiv 1 \pmod{e}$ and $p > \max(2|G : H|, \dim_F(Z))$. Set $L = \mathbb{F}_p$. Letting $l = |H/\ker(\mu)|$, we define a homomorphism θ_l from $\mathbb{Z}[\zeta_l]$ into L mapping ζ_l to ε_l, where $|\varepsilon_l| = l$. We extend θ_l to matrices over $\mathbb{Z}[\zeta_l]$ and obtain a *modular representation* for G over L composing the monomial representation M with θ_l. We find a generator for the center of the centralizer in the modular case. The existence of this generator is assured by the condition $p > \dim_F(Z)$. We lift the generator to an element $z \in Z$. A critical point is proving that in this reduction the dimension of the center is preserved and this is a consequence of the *Brauer–Nesbitt* Theorem (see Huppert (1998, Proposition 39.10)).

It turns out that z has distinct eigenvalues and hence is a generator for Z. We determine the *Lagrange* polynomials associated with its eigenvalues. Evaluating these polynomials in $\theta_l(z)$ provides the primitive central idempotents for Z. Pick $\varepsilon_e \in L$ such that $|\varepsilon_e| = e$ and define an algebra homomorphism θ_e from $\mathbb{Z}[\zeta_e]$ into L via $\theta_e(f(\zeta_e)) = \overline{f}(\varepsilon_e)$, where $\overline{f}$ is the reduction modulo p of f (see Dixon (1967)).

Using a direct trace calculation and some more information on the shape of the regular image of C, we obtain the image, via θ_e, of the character values of the irreducible constituents of the monomial character on any given conjugacy class. This requires determining some coefficients that generalize those obtained by Gollan and Ostermann (see Gollan and Ostermann (1990)). Finally we lift these values back into $\mathbb{Q}(\zeta_e)$. Notice that this requires knowledge of the conjugacy

classes and the power maps of G. We improve further Dixon's modular approach to the local lifting of such values. Namely in order to evaluate the character of an irreducible constituent on $g \in G$, we apply a *discrete Fourier transform* in $Q(\zeta_m)$, with $m = |g|$, instead of $Q(\zeta_e)$. We then coerce the output into the smallest cyclotomic field containing it. The latter task is not automatically implemented in MAGMA.

We specialize this analysis to the case when $\mu = 1_H$ and recover the results of Michler and Weller. However, our approach is simpler, in that we do not need to refer to association schemes. The direct trace calculation also allows us to avoid referring to Proposition 12.12 in Landrock's book (see Landrock (1983)).

Finally, we point out how the irreducible constituents obtained may be used to complete the character table of G. This turns out to be quite effective when G is a simple group. In this case our algorithm provides a collection of faithful characters to which we may apply various techniques: the Brauer–Burnside Theorem, the Schur Symmetrization Theorem, the Murnaghan orthogonal and symplectic splitting, the LLL, the MLLL, and the PSLQ algorithm and the Plesken Lattice Embedding Theorem (see Breuer (2002), Lenstra et al. (1982), Pohst (1987), and Ferguson et al. (1999)). In particular the integer relation finding algorithm MLLL, a version of LLL for not necessarily linearly independent vectors, has been implemented in the GAP 4.4.6 program system (see The GAP Group (2005, Ch. 25 and 69)). A similar technique has recently been implemented in MAGMA 2.12.19 by Unger (see Unger (2006)). He applies LLL to characters induced from suitable subgroups using a result of Brauer (see Huppert (1998, Theorem 34.2)).

The algorithm in this paper has been implemented in a stand-alone program written in MAGMA (see Bosma and Cannon (2005)) and may be downloaded from the author's Web-page together with some experimental data included in the tables of the last section. In this paper we provide a rough description of the algorithm implemented in MAGMA. As far as we know this conversion has not been carried out systematically by Michler and Weller. Their code could be used to get generators of Z as integral matrices. However, their methods are comparatively inefficient; they need to feed these matrices into MAPLE, calculate common eigenvectors, fetch them back into MAGMA and apply their formula to get constituents. Their algorithm assumes that the ground field is a cyclotomic extension of the rationals. This might require a prohibitive amount of time if G has large exponent.

We follow the notation in Isaacs (1976), Huppert (1998) and Graham et al. (1989). Given a ring R and an integer n, $(R)_n$ denotes the ring of matrices over R of degree n and 1_n is the identity in $(R)_n$. Given integers a, b, n, by $a \equiv_n b$ we mean $a \equiv b \pmod{n}$ and by $a \perp b$ we mean $\gcd(a, b) = 1$. $\mathrm{Irr}(G|\chi)$ is the set of irreducible characters of G occurring as constituents of the character χ. Given an algebraic element α over some field E, $\min_E(\alpha)$ denotes the minimal polynomial of α over E. Given a group element g we denote by $|g|$ its order.

2. Orbitals, generalized intersection matrices and centralizer algebras

Let G be a finite group and H a subgroup of G. From a theoretical point of view G may be any group, but for computational reasons we will always assume that G is given as a permutation group of not too large degree (experimental data show that 10^6 might be a reasonable bound). Fix a right transversal T for H in G, so $G = \bigsqcup_{t \in T} Ht$. Then G acts via right multiplication on T. We denote by $\cdot$ this action, namely $t \cdot g$ is the unique element in $Htg \cap T$. The recipe

$$(t, s) \cdot g = (t \cdot g, s \cdot g)$$

endows $T \times T$ with a G-set structure. We call the orbits of G on $T \times T$ *orbitals*. Since G acts transitively on the H-cosets by right multiplication, orbitals are in one-to-one correspondence with the orbits of H on T (*suborbits*). In fact, the correspondence is given by $(1, x) \cdot G \leftrightarrow x \cdot H$. Moreover, any orbital $(1, x) \cdot G$ corresponds to the unique double coset HxH. Let X denote a set of double-coset representatives. For example X can be obtained as follows. Fix an ordering in T, set $t_1 = 1_G$, and identify it with the set $[n] := \{1, \ldots, n\}$, where $n = |G : H|$. Let $\{1\} = \mathcal{O}_1, \ldots, \mathcal{O}_d$ be the suborbits, set $m_i = \min(\mathcal{O}_i)$ and let x_i be a fixed element such that $1 \cdot x_i = m_i$; then $X = \{x_i\}$ and $|X| = d$.

Definition 1. Given an orbital Λ, define $a_\Lambda \in (\mathbb{Z})_n$ such that its (t, s)-entry is 1 if $(t, s) \in \Lambda$, 0 otherwise. We call a_Λ the *adjacency matrix* associated with Λ.

Definition 2. Given a matrix a, we define the *support* of a, $\mathrm{Supp}(a)$, as the set $\{(s, t) : a_{st} \neq 0\}$.

Let $\langle v \rangle$ be the one-dimensional module for H affording μ, namely $vh = \mu(h)v$. Set $K = \ker(\mu)$ and $F = \mathbb{Q}(\zeta_l)$, where $\mathbb{C}^* \ni \zeta_l$ has order $l = |H/K|$. Namely, F is the *minimal cyclotomic field* realizing μ. Then $V = \bigoplus_{t \in T} v \otimes t$ becomes an FG-module via

$$(v \otimes t)g = v \otimes tg = \mu(tg(t \cdot g)^{-1})(v \otimes t \cdot g).$$

So V affords a representation M defined via

$$M(g)_{st} = \mu(sg(s \cdot g)^{-1})\delta_{s \cdot g, t},$$

where $s, t \in T$, $g \in G$. We define

$$\rho_{st}(g) = \mu(tg(t \cdot g)^{-1}(s \cdot g)g^{-1}s^{-1}).$$

Definition 3. Given an orbital $\Lambda = (1, x) \cdot G$, $x \in X$, set $H_x = H \cap H^x$. We say that Λ is *μ-central* if $[H_x, x^{-1}] \leq K = \ker(\mu)$.

The above condition is equivalent to $\mu(h_1) = \mu(h_2)$ when $h_1 = x^{-1}h_2x$ belongs to H_x. Notice that $1 = [H_x, xx^{-1}] = [H_x, x^{-1}][H_x, x]^{x^{-1}}$. So $[H_x, x^{-1}] \leq K$ forces $[H_x, x]^{x^{-1}} \leq K$. Since $H_x^{x^{-1}} = H_{x^{-1}}$, we get $[H_{x^{-1}}, x] \leq K$. Thus the set of μ-central orbitals is closed with respect to inversion $\Lambda_i = Hx_iH \leftrightarrow \Lambda_{i'} = Hx_i^{-1}H$.

We prove that $C = \mathrm{End}_G(V)$ is generated as an F-vector space by matrices corresponding to μ-central orbitals.

Theorem 4. $\mathrm{End}_G(V) = \bigoplus_\Lambda Fc_\Lambda$, *where Λ runs in the family of all μ-central orbitals, and $c = c_\Lambda$ is a matrix such that*

(1) $\mathrm{Supp}(c) = \Lambda$;
(2) *if* $\Lambda = (1, x) \cdot G$, $x \in X$, *then* $c_{(1,x)\cdot g} = \rho_{1x}(g)$.

Proof. Let $M(g) = D(g)P(g)$, where $D(g) = \mathrm{diag}(\mu(sg(s \cdot g)^{-1}))$ and $P(g) = (\delta_{s \cdot g, t})$ denote the diagonal and permutation part of the monomial matrix $M(g)$. Since $a_{st} = e_sAe_t'$, for any matrix $A = (a_{st})$, where e_s is a standard vector and e_t' is the transpose of e_t, the (s, t) entry of $c^{M(g^{-1})}$ equals

$$\mu(sg(s \cdot g)^{-1}(t \cdot g)g^{-1}t^{-1})c_{(s,t)\cdot g}.$$

Hence $c_{(s,t)\cdot g} = \rho_{st}(g)c_{(s,t)}$, for $c \in C$. Therefore any element of C is a linear combination of matrices whose support is contained in some orbital. So assume that $\mathrm{Supp}(c) \subseteq \Lambda = (1, x) \cdot G$, $x \in X$.

Consider two elements $y, z \in G$ connecting $(1, x)$ to (s, t), that is

$$(1, x) \cdot y = (s, t) = (1, x) \cdot z.$$

Notice that this condition is equivalent to $yz^{-1} \in H \cap H^x = H_x$. Moreover, $(x \cdot y)^{-1}(1 \cdot y) = (x \cdot z)^{-1}(1 \cdot z)$. We call this element w.

We prove that

$$\rho_{1,x}(y) = \rho_{1,x}(z), \tag{1}$$

for all such pairs iff Λ is μ-central. In fact, $\rho_{1,x}(y) = \rho_{1,x}(z)$ iff $w^{-y^{-1}} w^{z^{-1}}$ belongs to $K = \ker(\mu)$ iff $[y^{-1}z, w] \in K^z$ iff $[h^z, w] \in K^z$ iff $[h, w^{z^{-1}}] \in K$, where $y^{-1}z = h^z$, with $h = yz^{-1} \in H_x$. But

$$w^{z^{-1}} = x^{-1}xz(x \cdot z)^{-1}(1 \cdot z)z^{-1} = x^{-1}h_1,$$

for some $h_1 \in H$. Since $[h, x^{-1}h_1] = [h, h_1][h, x^{-1}]^{h_1}$ and $H' \leq K = K^{h_1}$ we obtain $[h, x^{-1}] \in K$ for any $h \in H_x$. Since $[ab, c] = [a, c]^b[b, c]$, we see that $[H_x, x^{-1}]$ is a group and Eq. (1) for all pairs y, z with $yz^{-1} \in H_x$ is equivalent to $[H_x, x^{-1}] \leq K$. Now assume that Λ is a μ-central orbital and $(s, t), (s', t') \in \Lambda$. Then $\rho_{st}(y) = \rho_{st}(z)$ for all y, z such that $(s, t) \cdot y = (s', t') = (s, t) \cdot z$. We argue as before splitting the path from (s, t) to (s', t') into a length-2 path through $(1, x)$, $x \in X$, where $(s, t), (s', t') \in (1, x) \cdot G$. Thus $c = c_\Lambda$ defined via $c_{st} = \rho_{st}(y)$, $(s, t) = (1, x) \cdot y$, $\Lambda = (1, x) \cdot G$, is a well defined non-zero matrix in C with $\mathrm{Supp}(c) = \Lambda$. □

Definition 5. We call c_Λ as given in Theorem 4 a *μ-adjacency matrix* for any μ-central orbital Λ.

Corollary 6. *Let V denote the permutation module affording $(1_H)^G$; then* $\mathrm{End}_G(V) = \bigoplus_\Lambda \mathbb{Q}a_\Lambda$, *where a_Λ denotes the adjacency matrix associated with the orbital Λ.*

Proof. In this case $\mu = 1_H$, so $K = \ker(1_H) = H$. But $[h, x^{-1}] = h^{-1}h_1 \in H$, where $h = h_1^x$ is a typical element of H_x. Thus all orbitals are 1_H-central and $\rho_{1x}(y) = 1$, for any $y \in G$. □

We order orbitals so that $\{\Lambda_1, \ldots, \Lambda_r\}$ is the set of all μ-central orbitals. In particular, $\dim(C) = r$. In order to study C we would like to embed it into $(F)_r$. Notice that $n \geq d \geq r$. For example, if G is the O'Nan group ON and H is isomorphic to the first Janko group J_1, then $n = 122\,760$ and $d = r = 7$. As a further example where $n >> d > r$, let $G = \mathrm{PGL}_2(73)$, $P \in \mathrm{Syl}_{37}(G)$, $H = N_G(P) = P \rtimes (2 \times 2)$, and $\mu \neq 1_H$; then $n = 2628$, $d = 37$, and $r = 36$.

Notice that $n = \sum_{x \in X} |H : H_x|$, so $n = d$ iff $H = H_x = H^x$ for any $x \in X$ iff $H \trianglelefteq G$. We further abbreviate c_{Λ_i} as c_i for all μ-central orbitals Λ_i.

Definition 7. We describe as *generalized intersection numbers* the structure constants p_{ij}^k for $C = \mathrm{End}_G(V)$ as a subalgebra of $(F)_n$ with respect to the basis $\{c_1, \ldots, c_r\}$. Namely

$$c_i c_j = \sum_{k=1}^{r} p_{ij}^k c_k. \tag{2}$$

We may assume that $x_1 = 1$ so that $c_1 = 1_n$, and hence $c_j \xrightarrow{\sigma} (p_{ij}^k)$ defines an algebra isomorphism (the *right regular representation*) between C and a subalgebra of $(F)_r$. We describe p_{ij}^k in terms of μ-values. For a simpler statement we build T as follows. For $x_i \in X$, we have

$1 \cdot x_i = m_i = \min(\mathcal{O}_i)$. Let $n_i = |\mathcal{O}_i| = |H : H_{x_i}|$. Write $\mathcal{O}_i = \{\omega_{i1}, \ldots, \omega_{in_i}\}$ and fix $h_{ij} \in H$ such that $m_i \cdot h_{ij} = \omega_{ij}$, then $T = \{x_i h_{ij} : 1 \le i \le d, 1 \le j \le n_i\}$ is a right transversal for H in G. We may further assume that $h_{i1} = 1$, so that $X \subseteq T$.

Proposition 8. *Let $T = \{x_i h_{ij} : 1 \le i \le d, 1 \le j \le n_i\}$ be a right transversal for H in G; then*

$$p_{ij}^k = \sum_{s=1}^{n_i} \mu(h_{is}^{-1} x_j h x_i h_{is} (h x_k)^{-1}),$$

where the sum is extended to all s such that $m_j \cdot h = m_k \cdot (x_i h_{is})^{-1}$, for some $h \in H$. In particular, $p_{i1}^k = \delta_{ik}$, $p_{1j}^k = \delta_{jk}$, and $p_{ij}^1 = \overline{\mu}(h_1 h) n_i \delta_{i'j}$, where $x_i^{-1} = h_1 x_{i'} h$.

Proof. Considering the $(1, x_k)$ entry in Eq. (2), we deduce that p_{ij}^k equals $\sum_{w \in T} (c_i)_{(1,w)} (c_j)_{(w,x_k)}$. Then we get non-zero terms only if $w = x_i h_{is}$, $1 \le s \le n_i$, and $(w, x_k) \in \Lambda_j$. The latter condition is equivalent to the existence of $g \in G$ such that $(1, x_j) \cdot g = (w, x_k)$. So $g = hw$, where $m_j \cdot h = m_k \cdot w^{-1}$. Thus $(c_i)_{(1,w)} = \rho_{1x_i}(h_{is}) = \mu(h_{is}^{-1})$ and $(c_j)_{(w,x_k)} = \rho_{1x_j}(g) = \mu(x_j h w x_k^{-1} h^{-1})$, where $w = x_i h_{is}$. Assume now that $j = 1$. Then $(p_{i1}^k) = 1_r$ which is the image of 1_n. Let $i = 1$; then $n_1 = 1$ and $h_{11} = 1$. So $p_{1j}^k = \mu(x_j h x_k^{-1} h^{-1})$, where $m_j \cdot h = m_k$. But this forces $j = k$ and we may choose $h = 1$. Finally consider $k = 1$; then $p_{ij}^1 = \sum_{s=1}^{n_i} \mu(h_{is}^{-1} x_j h x_i h_{is} h^{-1})$, where $m_j \cdot hw = 1$, so $m_j \in 1 \cdot x_i^{-1} H = m_{i'} \cdot H$. Thus $j = i'$ and $i = j'$. Let $x_i^{-1} = h_1 x_{i'} h$. Since $x_{i'} h x_i \in H$, then $\mu(h_{is}^{-1} x_{i'} h x_i h_{is} h^{-1}) = \mu(x_{i'} h x_i h^{-1})$ and $p_{ij}^1 = n_i \overline{\mu}(h_1 h) \delta_{i'j}$. □

In order to efficiently test the existence of $h \in H$ such that $m_j \cdot h = m_k \cdot (x_i h_{is})^{-1}$ we construct *bases and strong generating sets* for both H and G (for a more detailed account we refer the reader to Seress (2003, Ch. 4)). This allows us also to drastically reduce storage problems, since we may find presentations with respect to strong generators and express the transversal T in terms of words in such generators.

The term 'generalized intersection numbers' is explained by the following corollary, where we prove that for $\mu = 1_H$ they coincide with the so-called *intersection numbers*.

Corollary 9. *Let $a_i a_j = \sum_{k=1}^d p_{ij}^k a_s$, a_i the adjacency matrix corresponding to the orbital Λ_i. Then $p_{ij}^k = |m_i \cdot H \cap m_{j'} \cdot H x_k|$, where $m_{j'} \in 1 \cdot x_j^{-1} H$.*

Proof. By Proposition 8, p_{ij}^k counts the elements $1 \cdot w$ where $w = x_i h_{is}$ and $m_k \cdot w^{-1} \in m_j \cdot H$. Now $w = x_i h_{is}$ iff $1 \cdot w \in m_i \cdot H$. Moreover, $m_k \cdot w^{-1} \in m_j \cdot H$ iff $x_j h w x_k^{-1} \in H$, for some $h \in H$, iff $w \in H x_j^{-1} H x_k$ iff $1 \cdot w \in m_{j'} \cdot H x_k$. □

This corollary was obtained in Michler and Weller (2002), quoting non-elementary results for association schemes.

We close this section proving that there are not many symmetries among the p_{ij}^k's. We recall that i' is the unique index such that $x_i^{-1} \in H x_{i'} H$. Let $\Omega = [r]^3 = \{(i, j, k) : 1 \le i, j, k \le r\}$. We define $\gamma \in \mathrm{Sym}(\Omega)$ via

$$(i, j, k)^\gamma = (i', j, k),$$

and $\phi \in \hom(\mathrm{Sym}(3), \mathrm{Sym}(\Omega))$ via

$$(i_1, i_2, i_3)^{\phi(\xi)} = (i_{1^\xi}, i_{2^\xi}, i_{3^\xi}).$$

Let $\Sigma = \langle \gamma \rangle \wr \phi(\mathrm{Sym}(3)) \leq \mathrm{Sym}(\Omega)$. Then δ defined via

$$(i, j, k)^{\delta} = (i', j', k')$$

belongs to Σ.

When $\mu = 1_H$, then $p_{ij}^k = |m_i \cdot H \cap m_{j'} \cdot Hx_k| = |m_i \cdot Hx_k^{-1} \cap m_{j'} \cdot H| = p_{j'i'}^{k'}$. So the intersection numbers are invariant under $\delta(1, 2)$.

One can easily see that when $G = \mathrm{Sym}(3)$ and $H \in \mathrm{Syl}_2(G)$, these are the only elements of Σ preserving the intersection numbers.

3. 1-Generator algebras, central idempotents and character values

Clearly $\sigma(C)$, σ the right regular representation for C, is generated by $\sigma(c_1), \ldots, \sigma(c_r)$. Unfortunately getting $\sigma(c_i)$ might be expensive. We spare some energy as follows. Denote as π the projection of $\sigma(C)$ to the first row of $(F)_r$. Assume we already have a subalgebra C' of $\sigma(C)$. By Proposition 8, $\pi(C') = F^r$ implies $C' = \sigma(C)$. Let i be minimal such that $e_i \notin \pi(C')$, where e_i the ith vector of the standard basis for F^r, then calculate $\sigma(c_i)$ and replace C' with the F-algebra generated by C' and $\sigma(c_i)$. Experimentally the dimensions of the subalgebras obtained seem to double, so we expect $\sigma(C)$ to be generated by roughly $\lfloor \log_2(r) \rfloor$ matrices. At this point we may determine $Z = \mathbf{Z}(\sigma(C))$ solving a linear system in r unknowns and r_1 equations, where r_1 is the minimum generating number for C as an F-algebra. (This seems to be more efficient than using the MAGMA routine `Centre`.)

Proposition 10. *Let $z = \sum_{i=1}^r \alpha_i \sigma(c_i)$; then $z \in \mathbf{Z}(\sigma(C))$ iff $\sum_{i=1}^r \alpha_i (p_{ij}^k - p_{ji}^k) = 0$, where c_j varies among a minimal set of generators for C and $1 \leq k \leq r$.*

Proof. By Proposition 8, the coordinates of any element of $\sigma(C)$ may be read off from its first row. Hence $[z, \sigma(c_j)] = 0$ iff $\sum_{i=1}^r \alpha_i (p_{ij}^k - p_{ji}^k) = 0$, for $1 \leq k \leq r$. Now the assertion follows by letting c_j vary among a minimal set of generators for C (as an algebra). □

As in Michler and Weller (2002), we calculate the right regular representation τ of Z in $(F)_t$, where $t = \dim_F(Z)$. At this point Michler and Weller try to get a basis of common eigenvectors in F^t for the generators $z_1, \ldots, z_t$ of $\tau(Z)$. We simplify this problem proving that we only need to diagonalize a suitable matrix in $(F)_t$.

Definition 11. Let A be an algebra over the field E. We say that A is a 1-*generator algebra* if $A = E[a]$ for some element $a \in A$.

Emulating the proof by Serre of the Jordan–Chevalley decomposition of a matrix (see Humphreys (1978, Proposition 4.2, p. 17)) we prove the following.

Theorem 12. *Let A be a commutative, semisimple, finite dimensional E-algebra, E a separable field. If $|E| > \dim_E(A)$, then A is a 1-generator algebra.*

Proof. This result is proved in Chillag (1995, Theorem 1.1) in the case where E is infinite, so it is enough to consider the case where E is finite and $|E| = q$, say. Also, as noted in Chillag (1995), the Wedderburn Structure Theorem and the hypotheses on A show that A is a direct sum $\bigoplus_{i=1}^s E_i$ where each E_i is an extension field of E and the sum of the degrees $d_i = [E_i : E]$ is equal to $\dim_E(A)$. We shall now show that we can choose $\alpha_i \in E_i$ such that $E_i = E[\alpha_i]$ and the minimal polynomials for α_i and α_j over E are distinct when $i \neq j$. Then the characteristic

polynomial of $\alpha = \alpha_1 + \cdots + \alpha_s$ has distinct eigenvalues in its regular action on A, and so $A = E[\alpha]$ by Theorem 1.1 of Chillag (1995).

Clearly $\min_E(\alpha_i) = \min_E(\alpha_j)$ forces α_i, α_j to be Galois conjugate. Let A_i denote the set of all conjugates of α_i and assume, by induction, that $A_1, \ldots, A_{s-1}$ are disjoint. Notice that $|A_i| = d_i$. If $d_s = 1$, then pick $\alpha_s \in E^* \setminus \bigsqcup_{i=1}^{s-1} A_i$. Set $n = d_s$. By the Moebius Inversion Formula,

$$|\{\alpha \in \mathbb{F}_{q^n} : \mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]\}| = \sum_{d|n} \mu_{\mathbb{Z}}(d) q^{\frac{n}{d}},$$

where $\mu_{\mathbb{Z}}$ denotes the classical Moebius function. The right hand side term is greater than $q^n - \sum_{i=0}^{\frac{n}{r}} q^i$, where r is the smallest prime divisor of n. We claim that $f(q,n) = q^n - \frac{q^{\frac{n}{2}+1}-1}{q-1} - q + n > 0$, for $q, n \geq 2$. From

$$f(q,n) = q^{\frac{n}{2}+1}\left(q^{\frac{n}{2}-1} - \frac{1}{(q-1)}\right) + \frac{1}{q-1} - q + n,$$

we deduce that $f(q,n)$ is an increasing function in n for $n \geq 2$. Since $f(q,2) = (q-1)^2$, our claim follows. We obtain $|\{\alpha \in \mathbb{F}_{q^n} : \mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]\}| > q - n > \sum_{i=1}^{s-1} d_i = |\bigsqcup_{i=1}^{s-1} A_i|$, and hence there exists $\alpha_s \notin \bigsqcup_{i=1}^{s-1} A_i$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha_s]$. Thus we can choose α_i such that $E_i = E[\alpha_i]$ and $\min_E(\alpha_i) \neq \min_E(\alpha_j)$ for $i \neq j$. □

We remark that Chillag shows that $|E| > \dim_F(A)$ is a necessary condition. Moreover, he points out that such an algebra A always possesses an identity (see Chillag (1995, p. 149)).

We apply this result to the center of the endomorphism ring.

Corollary 13. *Let Z be the right regular image in $(F)_t$ of the center of $\mathrm{End}_G(V)$; then there exists $z \in Z$ such that $Z = F[z]$.*

Proof. By Maschke's Theorem, $\mathrm{End}_G(V)$ is a semisimple algebra. Hence Z is a semisimple, commutative, and finite dimensional algebra over the minimal cyclotomic field F realizing all μ-values. Since F is infinite and separable, the result follows immediately from the previous theorem. □

In order to obtain z we use a probabilistic approach. Namely, we determine an F-vector basis $\{z_1, \ldots, z_t\}$ for Z and choose randomly integers $b_1, \ldots, b_t$ until $z = \sum_i b_i z_i$ is a generator for Z. This can be efficiently checked since z is a generator if and only if $\deg m(x) = \dim_F(Z)$ where $m(x)$ is the minimal polynomial of $z \in (F)_t$. Let E be a splitting field for Z, then $Z \otimes E > E[z]$ only if z has repeated eigenvalues. Since $Z \otimes E \simeq E^t$, this happens iff z lies in the union of the $\binom{t}{2}$ subvarieties $V_{ij} = \{z \in E^t : z_i = z_j\}$, $1 \leq i < j \leq t$, of codimension 1.

We prove that integer coefficients suffice.

Proposition 14. *Let F be an infinite field, Z a semisimple, finite dimensional, commutative algebra over F, $z_1, \ldots, z_t$ an F-basis for Z. Then $z = \sum_{i=1}^t a_i z_i$ satisfies $Z = F[z]$ unless $(a_1, \ldots, a_t) \in \mathbb{Z}^t$ lies in the union of $\binom{t}{2}$ hyperplanes $H_{ij} \leq E^t$, where E is a splitting field for Z.*

Proof. We may assume that $z_i = \mathrm{diag}(\zeta_{i1}, \ldots, \zeta_{it})$, $\zeta_{ij} \in E$. Let

$$H_{jk} = \left\{ v \in E^t : \sum_{i=1}^t v_i(\zeta_{ij} - \zeta_{ik}) = 0 \right\}.$$

Notice that for $j \neq k$, H_{jk} is a hyperplane of E^t; otherwise the jth and kth components of any element in Z would coincide against $\dim_F(Z) = t$. Now $z = \sum_{i=1}^{t} a_i z_i$ does not satisfy $Z = F[z]$ iff $(a_1, \ldots, a_t) \in H_{jk}$ for some $j \neq k$. □

We now show how to exploit a generator z for Z in order to obtain the primitive central idempotents e_i for the algebra $\mathbb{C}M(G)$, where M is the monomial representation affording μ^G. By Wedderburn's Theorem there is a one-to-one correspondence between the e_i's and the irreducible constituents χ_i of μ^G given by $\chi_i(g) = \mathrm{tr}(e_i M(g))$. We now provide a recipe which allows us to work on these idempotents at three different levels, namely in dimensions n, r, and t, exchanging information obtained in the smallest algebra. The key and simple idea is to obtain *Lagrange polynomials* interpolating the eigenvalues of z and use them to express the primitive central idempotents at any level. We recall that given t distinct scalars $\lambda_1, \ldots, \lambda_t$ the Lagrange polynomials $L_i(x)$ satisfy the system

$$L_i(x) \equiv \delta_{ij} \mod (x - \lambda_j).$$

Notice that the eigenvalues of z lie in any splitting field for G. According to a theorem of Brauer they belong to $\mathbb{Q}(\zeta_e)$, where $e = \mathrm{Exp}(G)$. This will allow us to apply Dixon's approach (see Dixon (1967)), solving what turns out to be in general a difficult problem, namely finding complex eigenvalues. Obtained the Lagrange polynomials we can easily read off the multiplicity $f_i = (\chi_i, \mu^G)$, where $\chi_i \in \mathrm{Irr}(G|\mu^G)$, and the coordinates of a central idempotent with respect to the μ-adjacency matrices. We recall that σ is the right regular representation of $C \leq (F)_n$ into $(F)_r$ and τ is the right regular representation of $\mathbf{Z}(\sigma(C))$ in $(F)_t$.

Theorem 15. *Let $Z = \tau(\mathbf{Z}(\sigma(C))) \leq (F)_t$ be generated by z and $E = \mathbb{Q}(\zeta_e)$, where $|\zeta_e| = \mathrm{Exp}(G)$. Then*

(a) *z admits distinct eigenvalues $\lambda_1, \ldots, \lambda_t$ in E^*, where $t = \dim_F(Z)$.*
(b) *Let $L_i(x)$ be the Lagrange polynomials relative to $\lambda_1, \ldots, \lambda_t$; then $L_i(z)$ are the central primitive idempotents of Z.*
(c) *Let $f_i = (\chi_i, \mu^G)$ be the multiplicity of χ_i in μ^G. Then $f_i^2 = \mathrm{rank}(\widehat{e}_i)$, where $\widehat{e}_i = L_i(\tau^{-1}(z))$ is a primitive central idempotent for $\sigma(C)$.*
(d) *Let $\widehat{e}_i = \sum_{j=1}^{r} a_{ij}\sigma(c_j)$, where c_j are the μ-adjacency matrices. Then a_{ij} is the $(1, j)$-entry of $\widehat{e}_i$. In particular, $a_{ij} \in E$.*

Proof. By Brauer's Theorem (see Isaacs (1976, Theorem 10.3)), E is a splitting field for G. Hence $EM(G) \simeq \bigoplus_{i=1}^{t}(E)_{d_i} \otimes 1_{f_i}$ and $C_E = C \otimes E \simeq \bigoplus_{i=1}^{t} 1_{d_i} \otimes (E)_{f_i}$. Thus $Z(C_E) = EM(G) \cap C_E$ splits over E. Since $Z = F[z]$, z must be a semisimple regular element, and hence admits t distinct non-zero eigenvalues. Notice that $Z_E = Z \otimes E \simeq \bigoplus_{i=1}^{t} E$ is a split torus in $(E)_t$ and $\widetilde{e}_i = L_i(z)$ corresponds to an elementary matrix, and hence is a primitive central idempotent. Notice that $\sigma(C_E) = \bigoplus_{i=1}^{t}(E)_{f_i} \otimes 1_{f_i}$. Let $\widehat{e}_i = L_i(\tau^{-1}(z))$; then $\widehat{e}_i = \mathrm{diag}(0, \ldots, 1_{f_i^2}, \ldots, 0)$, and hence $\mathrm{rank}(\widehat{e}_i) = f_i^2$. On the other hand, from $EM(G) \simeq \bigoplus_{i=1}^{t}(E)_{d_i} \otimes 1_{f_i}$ we deduce that f_i is the multiplicity of the block $(E)_{d_i}$ in $EM(G)$. Finally, by Proposition 8, $p^k_{1j} = \delta_{jk}$, so $a_{ij} = (\widehat{e}_i)_{1j} \in E$. □

From a computational perspective we would like to point out that in order to get $\tau^{-1}(z)$ we only need to keep track of the basis $\widehat{z}_1, \ldots, \widehat{z}_t$ of $\mathbf{Z}(\sigma(C))$ and of the integers $b_1, \ldots, b_t$ such

that $z = \sum_{i=1}^{t} b_i \tau(\widehat{z_i})$ is a generator for Z. We are now in the position to explicitly get the irreducible constituent χ_i of μ^G corresponding to the primitive central idempotent e_i. In order to determine $\chi_i(g)$ we generalize the so called *Gollan–Ostermann numbers* and apply a direct trace calculation that avoids any reference to Proposition 12.12 in Landrock (1983).

Definition 16. Let μ be a linear character of H, $H \leq G$, T a right transversal for H in G. Then we define the *extended Gollan–Ostermann number* corresponding to the μ-central orbital Λ_j and $g \in G$ as

$$p_j(g) = \sum_{u \in T} \mu(x_j g^{(hu)^{-1}}),$$

where the sum ranges over all $u \in T$ such that $m_j \cdot hug = 1 \cdot u$ for some $h \in H$. If none exists we set $p_j(g) = 0$.

Theorem 17. *Let $e_i = L_i(\sigma^{-1}\tau^{-1}(z)) = \sigma^{-1}(\widehat{e_i})$; then the e_i's are the pairwise orthogonal primitive central idempotents for $EM(G)$. Moreover, $e_i = \sum_{j=1}^{t} a_{ij} c_j$ for some $a_{ij} \in E$. Let $p_j(g)$ be the extended Gollan–Ostermann numbers. If $\chi_i \in \mathrm{Irr}(G|\mu^G)$ corresponds to e_i, then*

$$\chi_i(g) = \frac{1}{f_i} \sum_{j=1}^{r} a_{ij} p_j(g),$$

where $f_i^2 = (\chi_i, \mu^G)^2 = \mathrm{rank}(\widehat{e_i})$. In particular, $d_i = \chi_i(1) = \frac{n a_{i1}}{f_i}$.

Proof. The first two claims follow immediately from Theorem 15. If χ_i corresponds to e_i, then $f_i \chi_i(g) = \mathrm{tr}(e_i M(g)) = \sum_j a_{ij} \mathrm{tr}(c_j M(g))$. So we are done if we get $p_j(g) = \mathrm{tr}(c_j M(g))$. Now $\mathrm{tr}(c_j M(g)) = \sum_{u,v \in T} (c_j)_{uv} M(g)_{v,u}$. Since $M(g)$ is monomial the right term equals $\sum_{u \in T} (c_j)_{uv} \mu(vgu^{-1})$, where v is uniquely determined by $u = v \cdot g$. On the other hand, $(c_j)_{uv} = \rho_{1x_j}(y)$, where $(u, v) = (1, x_j) \cdot y$. Thus $y = hu$ and $1 \cdot v = 1 \cdot x_j hu$, for some $h \in H$. So h satisfies $m_j \cdot h = 1 \cdot (u \cdot g^{-1})u^{-1} = 1 \cdot ug^{-1}u^{-1}$ and $\rho_{1x_j}(y) = \mu(x_j huv^{-1}h^{-1})$. Thus $(c_j)_{uv} M(g)_{vu} = \mu(x_j huv^{-1}h^{-1}vgu^{-1}) = \mu(x_j^h g^{u^{-1}})$; the second equality follows on moving h^{-1} to the left which we are allowed to do since $H' \leq \ker(\mu)$ and $x_j huv^{-1} \in H$. Thus $p_j(g) = \sum_{u \in T} \mu(x_j^h g^{u^{-1}})$, for all $u \in T$ such that there exists $h \in H$ conjugating m_j to $1 \cdot (u \cdot g^{-1})u^{-1}$. In particular, if $g = 1$, then such h exists only if $j = 1$ and in this case $h = 1$ works. Thus $p_j(1) = n\delta_{1j}$. If $EM(G) \simeq \bigoplus_{i=1}^{t} (E)_{d_i} \otimes 1_{f_i}$, then $d_i = \chi_i(1)$ and the latter value equals $\frac{1}{f_i} \sum_j a_{ij} \delta_{1j} = \frac{n a_{i1}}{f_i}$. □

Specializing again to the case where $\mu = 1_H$, the trivial character of H, we obtain in a slightly different form the Michler–Weller Theorem and, a fortiori, Frobenius's Theorem (see Michler and Weller (2002)). The difference simply reduces to a reordering of the constituents according to $\chi \leftrightarrow \overline{\chi}$.

Corollary 18. *Let P be the permutation representation of G induced by right multiplication on a right transversal of H in G. Let $E = \mathbb{Q}(\zeta_e)$, $|\zeta_e| = \mathrm{Exp}(G)$. Let e_i be the primitive central idempotents of $EP(G)$. Then there exist $a_{ij} \in E$ such that $e_i = \sum_{j=1}^{d} a_{ij} a_j$, where a_j are the adjacency matrices. Let σ be the right regular representation for $C = \mathrm{End}_G(V)$ with respect to the basis of adjacency matrices, V the permutation module. Then $\mathrm{rank}(\sigma(e_i)) = f_i^2$, for some $f_i \in \mathbb{N}$. Set $p_j(g) = |\{u \in T : ug^{-1}u^{-1} \in Hx_j H\}|$; then $\chi_i(g) = \frac{1}{f_i} \sum_j a_{ij} p_j(g)$.*

Proof. All claims are straightforward, apart from the shape of $p_j(g)$. Notice that for $\mu = 1_H$, $p_j(g) = |\{u \in T : 1 \cdot x_j h = 1 \cdot (u \cdot g^{-1})u^{-1}\}|$. The latter condition is equivalent to requiring that $(u \cdot g^{-1})u^{-1} \in Hx_jH$. Since $u \cdot g^{-1} = h_1 u g^{-1}$, the result follows. □

Notice that in the case of a permutation representation, $p_j(g^{-1})$ coincides with the Gollan–Ostermann number relative to j and g (compare Gollan and Ostermann (1990), Michler (2001), and Michler and Weller (2002)).

4. Dixon's modular approach

Unfortunately, working in large cyclotomic fields like $E = \mathbb{Q}(\zeta_e)$, $|\zeta_e| = e = \mathrm{Exp}(G)$, might require prohibitive amounts of time and storage. We prove that the approach introduced by Dixon to recover the constituents of the regular representation may be adapted to our context. By Dirichlet's Theorem, there exists a prime p such that $p \equiv_e 1$. Let $L = \mathbb{F}_p$; then $|g|$ divides $|L^*| = p - 1$ for any $g \in G$. Fix an element ε_e of L of order e. Define a homomorphism θ_e from $\mathbb{Z}[\zeta_e]$ into L via

$$\theta_e : f(\zeta_e) \mapsto f(\varepsilon_e),$$

for any $f \in \mathbb{Z}[x]$. Notice that given a factorization dk for e, θ_e induces by restriction a homomorphism θ_d from $\mathbb{Z}[\zeta_d]$ into L.

We would like to reproduce all calculations in Theorems 15 and 17 in the finite field L. Set $l = |H/K|$, where $K = \ker(\mu)$. Using the entries of $M(g)$, where M is the representation affording μ^G, we may extend θ_l to such matrices and define a representation M_L of G over L via

$$M_L : g \mapsto \theta_l(M(g)).$$

Theorem 19. *Let $t = \dim_F(Z)$, $r = \dim_F \mathrm{End}_G(V)$, $n = |G : H|$, $e = \mathrm{Exp}(G)$, $l = |H/\ker(\mu)|$, p a prime such that $p \equiv_e 1$ and $p > \max(2n, t)$, and $L = \mathbb{F}_p$. Let $A_L = LM_L(G)$, $C_L = \mathbf{C}(A_L)$ and $Z_L = \mathbf{Z}(C_L)$. Then*

(1) *$Z_L = \mathbf{Z}(A_L) = \theta_l(Z(FG) \cap (\mathbb{Z}[\zeta_l])_t)$ is a semisimple commutative algebra of dimension t;*
(2) *$Z_L = L[\overline{z}]$, for some $\overline{z} \in Z_L$;*
(3) *there exists $z \in Z$ such that $\theta_l(z) = \overline{z}$ and $Z = F[z]$;*
(4) *θ_e defines a homomorphism from $\mathbb{Z}[\zeta_e]$ into L with kernel the ideal I generated by p and $\zeta_e - c_e$, where $c_e \in \mathbb{N}$ and $c_e \equiv_p \varepsilon_e$;*
(5) *the Lagrange polynomials $L_i(x)$ associated with the eigenvalues of z belong to $S[x]$, where S is the localization of $\mathbb{Z}[\zeta_e]$ at I;*
(6) *θ_e extends to S and $\overline{e_i} = \theta_e(L_i(\tau^{-1}(z))) \in (L)_r$ are the primitive central idempotents of Z_L;*
(7) *$(L)_r \ni \overline{c_j} = \theta_e(\sigma(c_j))$, c_j the μ-adjacency matrices, are L-linearly independent;*
(8) *let $\overline{e_i} = \sum b_{ij}\overline{c_j}$; then $b_{ij} = \theta_e(a_{ij})$, where $e_i = \sum a_{ij}\sigma(c_j)$;*
(9) *$\theta_e(\chi_i(g)) = \frac{1}{\overline{f_i}} \sum_j b_{ij}\theta_l(p_j(g))$, where $\overline{f_i}$ is the reduction modulo p of $f_i = (\chi_i, \mu^G)$.*

Proof. Since $p \equiv_e 1$, $p \nmid |G|$ and A_L is a semisimple algebra by Maschke's Theorem. By Wedderburn's Theorem $\mathbf{Z}(A_L) = A_L \cap C_L = \mathbf{Z}(C_L)$. Since E and L are splitting fields for $A_E = EM(G)$ and A_L, a theorem of Brauer and Nesbitt implies $\dim_L(Z_L) = \dim_E(Z_E) = \dim_F(Z)$ (see Huppert (1998, Theorem 39.10)). Since $\theta_l(\mathbb{Z}) = L$, we also get $Z_L = \theta_l(Z(FG) \cap (\mathbb{Z}[\zeta_l])_t)$.

By Theorem 12, $Z_L = L[\overline{z}]$, since $p > t$. Consider $z \in \mathbf{Z}(FG) \cap (\mathbb{Z}[\zeta_l])_t$ such that $\theta_l(z) = \overline{z}$. Then z is a semisimple element and it admits distinct non-zero eigenvalues in $E = \mathbb{Q}(\zeta_e)$.

We recall that θ_e is defined via $\theta_e(f(\zeta_e)) = \overline{f}(\varepsilon_e)$, where $f(x) \in \mathbb{Z}[x]$ and $\overline{f}$ denotes reduction modulo p. Let $I = \ker(\theta_e)$. Clearly $I \geq J = \langle \zeta_e - c_e, p \rangle$. Since $f(\zeta_e) \equiv_J f(c_e) \equiv_J f(c_e) \bmod p$, we get the converse inclusion $J \geq I$.

We extend θ_e to a ring homomorphism from $(\mathbb{Z}[\zeta_e])_t$ into $(L)_t$. We have that

$$\theta_e(\det(x1 - z)) = \det(x1 - \theta_e(z)).$$

Thus the eigenvalues of $\overline{z} = \theta_e(z)$ have shape $\theta_e(\lambda)$, λ an eigenvalue of z. Since $\overline{z}$ generates Z_L, $\theta_e(\lambda) \neq \theta_e(\lambda')$ for any pair λ, λ' of eigenvalues of z. So $\lambda - \lambda' \notin I$. Since

$$L_i(x) = \frac{\prod_{j \neq i} (x - \lambda_j)}{\prod_{j \neq i} (\lambda_i - \lambda_j)},$$

$L_i(x) \in S[x]$, where S is the localization of $\mathbb{Z}[\zeta_e]$ at I. We claim first that $\lambda_i \in \mathbb{Z}[\zeta_e]$. In fact, λ_i is integral over $\mathbb{Z}[\zeta_l]$ in E. By transitivity of integrality, λ is integral over $\mathbb{Z}$. But the ring of integers in E equals $\mathbb{Z}[\zeta_e]$ (see Ireland and Rosen (1982, Proposition 13.2.10)). Since $\mathbb{Z}[\zeta_e]/I \cong L$, I is a maximal and prime ideal, so $L_i(x) \in S[x]$.

Now $Z = F[z]$, since z has distinct non-zero eigenvalues. So $Z_L = \theta_e(\mathbb{Z}[z])$. Since $e_i = L_i(z)$ are the central primitive idempotents of Z, the same holds for $\overline{e_i} = \theta_e(e_i)$ in Z_L.

By Proposition 8, the first row of $\sigma(c_j)$ is the jth standard vector of E^r, and hence the $\overline{c_j}$ are L-linearly independent.

Since $\overline{e_i} \in \theta_e(C_L) \leq (L)_r$, there exist $b_{ij} \in L$ such that $\overline{e_i} = \sum_j b_{ij} \overline{c_j}$. On the other hand, $e_i = \sum_j a_{ij} \sigma(c_j)$. Since $e_i = L_i(z)$ and $L_i(x) \in S[x]$, $e_i \in (S)_r$. By the previous remark a_{ij} occurs in the first row of $\overline{e_i}$, so $a_{ij} \in S$. Thus we may apply θ_e to $e_i = \sum_j a_{ij} \sigma(c_j)$. Linear independence of $\overline{c_j}$ forces $b_{ij} = \theta_e(a_{ij})$.

By Theorem 17, $\chi_i(g) = \frac{1}{f_i} \sum_{j=1}^{r} a_{ij} p_j(g)$. Since $n = \sum_i f_i d_i$ and $p > 2n$, we have that $p \nmid f_i$. Moreover, $a_{ij} \in S$ and $p_j(g) \in \mathbb{Z}[\zeta_l]$ allows us to apply θ_e to the above formula and obtain $\theta_e(\chi_i(g)) = \frac{1}{\overline{f_i}} \sum_j b_{ij} \theta_l(p_j(g))$. □

We would like to point out that from the above theorem we may obtain $\theta_e(\chi_i(g))$ without using explicitly θ_e. In fact, we construct Z_L applying θ_l to the integral part of Z, find a generator for Z_L, determine its central primitive idempotents, calculate the coefficients b_{ij} using linear algebra over L and finally apply θ_l to the extended Gollan–Ostermann numbers $p_j(g)$.

The obvious advantage is that we only need to work in F instead of E. The non-obvious one is that from Theorem 12 we may deduce a deterministic algorithm to get a generator for Z_L, even if computationally a probabilistic approach seems to be more effective.

Notice that, as in Proposition 14, $\overline{z}$ generates Z_L iff $\overline{z}$ has distinct eigenvalues. Now Z_L is isomorphic to the split torus L^t in $(L)_t$. So the probability of picking a generator is $\prod_{j=1}^{t-1}(1 - j/p)$, an increasing function in the prime p.

In Dixon's original approach one has to work with sums of e terms in order to lift the modular reduction of character values back into E. We now make explicit a local version of Dixon's Theorem that avoids using E again.

Proposition 20. *Let $g \in G$ have order d, $\chi_i \in \mathrm{Irr}(G|\mu^G)$, ζ_d and ε_d elements of order d in $\mathbb{C}^*$ and L^*. Then*

$$\chi_i(g) = \sum_{j=0}^{d-1} m_{ij}\zeta_d^j,$$

where $\mathbb{N} \ni m_{ij}$ is uniquely determined by $m_{ij} \equiv_p \frac{1}{d}\sum_{s=0}^{d-1} \varepsilon_d^{-js}\theta(\chi_i(g^s))$, provided p is a prime $p \equiv_e 1$, $p > \max(2|G : H|, \dim_F(Z))$.

This has already been observed in the diploma thesis of Hulpke (see Hulpke (1993, p. 26)).

5. The algorithm

We provide a rough description of the algorithm implemented in MAGMA 2.12.19.

INPUT: A finite permutation group G, a subgroup H of G, and a linear character μ of H.

OUTPUT: A list $(f_1, \ldots, f_t) \in \mathbb{N}^t$ and a matrix $X \in (\mathbb{Q}(\zeta_e))_{t\times k}$, $k = k(G)$ the number of conjugacy classes of G, where $\mu^G = \sum_{j=1}^t f_j\chi_j$, $\chi_j \in \mathrm{Irr}(G)$, and $\chi_j(g_i) = X_{ji}$, g_i a representative for the ith class of G in some fixed order.

(1) Get the ordered list of conjugacy classes of G and power maps.
(2) Build the action of G on H-cosets.
(3) Determine the suborbits of H in this action.
(4) Get finite presentations with respect to strong generating sets.
(5) Store, using these presentations, double-coset representatives and a right transversal of H in G.
(6) Get the μ-central orbitals.
(7) Build $\sigma(C)$, the right regular image of the centralizer algebra, in $(\mathbb{Q}(\mu))_r$ starting from 1_r and adjoining non-redundant generators until we obtain an algebra of dimension r.
(8) Calculate the center Z of this algebra as the kernel of a linear transformation.
(9) Get z in the right regular image of Z such that its modular image $\overline{z}$ in $(L)_t$ generates Z_L, where $L = \mathbb{F}_p$ and $\mathrm{Exp}(G)$ divides $p - 1$.
(10) Calculate the eigenvalues and the associated Lagrange polynomials for $\overline{z}$.
(11) Calculate the primitive central idempotents for the modular reduction of $\sigma(C)$ in $(L)_r$.
(12) Get the list of multiplicities as square roots of the rank of the idempotents.
(13) Determine the Gollan–Ostermann matrix $(p_j(g_i)) \in (\mathbb{Q}(\zeta_e))_{r\times k}$, k the class number of G.
(14) Lift the modular values of the irreducible constituents into $\mathbb{Q}(\zeta_e)$.

6. Implementation issues and performance

We report in this section some examples run on a computer with a 1.5 GHz Pentium 4 processor and 2 Gb of RAM. The main bottleneck is related to the calculation of the extended Gollan–Ostermann numbers. Their determination becomes unfeasible when the degree of the representation is larger than 100.000.

We list the execution times in seconds for permutation characters in Table 1 and for monomial characters in Table 2.

For the examples we have used the group libraries in MAGMA. So $\mathrm{Tra}(d, n)$ ($\mathrm{Pri}(d, n)$) stands for the nth transitive (primitive) group of degree d, and $\mathrm{Per}(n)$ ($\mathrm{AS}(n)$) for the nth perfect (almost-simple) group according to the internal ordering in MAGMA 2.12.19.

Table 1
Monomial representations

G	$\lvert H\rvert$	Degree	$\lvert\mu\rvert$	t	Time
J_1	168	1045	3	8	3.53
J_1	120	1463	2	14	6.87
J_1	114	1540	6	9	13.58
J_1	110	1596	5	11	15.23
HS	252 000	176	2	2	2.60
HS	40 320	1100	2	4	13.35
HS	40 320	1100	2	4	11.34
J_2	2 160	280	2	4	1.21
J_2	1 152	525	3	3	1.48
J_2	720	840	3	4	3.93
J_2	600	1008	2	8	6.11
Co_3	1796 256 000	276	2	2	18.39
$G_2(4)$	184 320	1365	3	2	11.02
Per(122)	15 000	25	5	1	9.66
Per(122)	37 500	10	2	3	24.95
AS(98)	148	74	2	36	201.21

Table 2
Permutation representations

G	$\lvert H\rvert$	Degree	t	Time
J_1	660	266	5	0.31
J_1	168	1045	11	2.12
J_1	120	1463	10	4.26
J_1	114	1540	12	4.29
J_1	110	1596	13	4.63
HS	443 520	100	3	0.30
HS	40 320	1100	5	3.63
HS	40 320	1100	5	3.76
HS	11 520	3850	9	31.22
HS	10 752	4125	9	38.99
J_2	6048	100	3	0.18
J_2	2160	280	4	0.34
J_2	1920	315	6	0.42
J_2	1152	525	6	0.82
J_2	720	840	7	1.60
J_2	600	1008	8	2.27
J_2	336	1800	9	6.00
Suz	251 596 800	1782	3	15.90
Co_3	898 128 000	552	4	1.87
$3.PSU_6(2)$	13 685 760	2016	7	47.65
$G_2(4)$	604 800	416	3	0.98
$G_2(4)$	184 320	1365	4	6.17
$G_2(4)$	184 320	1365	4	7.04
$G_2(4)$	124 800	2016	3	18.65
$G_2(4)$	120 960	2080	4	16.84
Tra(20, 246)	288	100	6	0.74
Per(122)	120	3125	35	65.15
AS(98)	120	74	37	73.26
Pri(625, 345)	384	625	5	4.59

Acknowledgements

I would like to thank Prof. Gerhard Michler for helpful and animated discussions, Prof. Keith Dennis for allowing me to use the computer facilities during my one-month visit at Cornell University, Prof. John Murray and Prof. Mark Andrea de Cataldo for stylistic improvements, and the referees for several technical and mathematical suggestions.

This research was supported by F.A.R. 2004 funds from the University of Insubria and by grants from the Cofin project "Teoria dei Gruppi e Applicazioni" while the author was visiting the mathematical department of Cornell University.

References

Bosma, W., Cannon, J.J., 2005. Handbook of MAGMA Functions Version 2.12. http://magma.maths.usyd.edu.au/magma, University of Sydney.

Breuer, T., 2002. Constructing the Irreducible Characters of J_4 with GAP. http://www.gap-system.org.

Chillag, D., 1995. Regular representations of semisimple algebras, separable field extensions, group characters, generalized circulants, and generalized cyclic codes. Linear Algebra Appl. 218, 147–183.

Dixon, J.D., 1967. High speed computation of group characters. Numer. Math. 10, 446–450.

Ferguson, H.R.P., Bailey, D.H., Arno, S., 1999. Analysis of PSLQ, an integer relation finding algorithm. Math. Comp. 68, 351–369.

The GAP Group, 2005. GAP — Groups, Algorithms, and Programming, Version 4.4.6. http://www.gap-system.org.

Gollan, H.W., Ostermann, T.W., 1990. Operation of class sums on permutation modules. J. Symbolic Comput. 9, 39–47.

Graham, R., Knuth, D., Patashnik, O., 1989. Concrete Mathematics. Addison-Wesley.

Hulpke, J.A., 1993. Zur Berechnung von Charaktertafeln, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule. http://www.math.colostate.edu/~hulpke/paper/diplo_ahulpke.dvi.gz.

Humphreys, J.E., 1978. Introduction to Lie Algebras and Representation Theory. In: Graduate Texts in Mathematics, vol. 9. Springer-Verlag, New York, Berlin, Second printing, revised.

Huppert, B., 1998. Character Theory of Finite Groups. In: Walter de Gruyter Expositions in Mathematics, vol. 25.

Ireland, K., Rosen, M., 1982. A Classical Introduction to Modern Number Theory. In: Graduate Texts in Mathematics, vol. 84. Springer-Verlag, New York.

Isaacs, I.M., 1976. Character Theory of Finite Groups. In: Pure and Applied Mathematics, No. 69. Academic Press, New York, London.

Landrock, P., 1983. Finite Group Algebras and their Modules. In: London Mathematical Society Lecture Notes, Cambridge.

Lenstra, A.K., Lenstra, H.W., Lovász, L., 1982. Factoring polynomials with rational coefficients. Math. Ann. 261 (4), 515–534.

McKay, J., 1970. The construction of the character table of a finite group from generators and relations. In: Computational Problems in Abstract Algebra. Pergamon Press, Oxford, pp. 89–100.

Michler, G.O., 2001. The character values of multiplicity-free irreducible constituents of a transitive permutation representation. Kyushu J. Math. 55, 75–106.

Michler, G.O., Weller, M., 2002. The character values of the irreducible constituents of a transitive permutation representation. Arch. Math. 78, 417–429.

Pohst, M., 1987. A modification of the LLL reduction algorithm. J. Symbolic Comput. 4, 123–127.

Schneider, G.J.A., 1990. Dixon's character table algorithm revisited. J. Symbolic Comput. 9, 601–606.

Seress, Á., 2003. Permutation Group Algorithms. In: Cambridge Tracts in Mathematics, vol. 152. Cambridge University Press.

Unger, W.R., 2006. Computing the character table of a finite group. J. Symbolic Comput. 41 (8), 847–862.