Irreducible Constituents of Monomial Characters

PROF. ANDREA PREVITALI
UNIVERSITÀ DELL'INSUBRIA-COMO, ITALY
ANDREA.PREVITALI@UNINSUBRIA.IT
HTTP://SCIENZE-COMO.UNINSUBRIA.IT/PREVITALI

BERLIN, 1. AUGUST 2006

Cosets and Permutation Representation

H:= a subgroup of finite index, say n, of a group G;

T:= a right transversal of H in G, thus $G = \coprod_{t \in T} Ht$;

$(t \cdot g)$:= unique element in $T \cap Htg$;

$G/\mathrm{Core}_G(H)$ embeds into $\mathrm{Sym}(n)$;

We assume that G be a subgroup of $\mathrm{Sym}(n)$;

Double Cosets, Orbitals, and Suborbits

$T \times T$ becomes G-set via $(s,t) \cdot g := (s \cdot g, t \cdot g)$;

The G-orbits on $T \times T$ are called orbitals;

$X := (T \times T)//G$ a set of representatives of (H,H)-cosets;

$$(1,x) \cdot G \leftrightarrow x \cdot H \leftrightarrow HxH$$

define bijections between orbitals, suborbits and (H,H)-cosets;

Linear and Monomial Representations

W:= one-dimensional H-module;

μ:= linear character of H afforded by W

$$wh := \mu(h)w.$$

$K := \ker \mu$ and $\ell := |H : K|$;

$F := \mathbb{Q}(\zeta_\ell)$, where ζ_ℓ is a primitive ℓ-th root of $1 \in \mathbb{C}$;

$V := \bigoplus_{t \in T} W \otimes t$ is the FG-module affording the monomial representation μ^G;

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

where $s, t \in T$, $g \in G$, is the associated monomial matrix;

Centralizer Algebra

Definition: The orbital $(1,x)\cdot G$ is μ-central if $[H\cap H^x, x^{-1}] \leq \ker\mu$.

Theorem: (P. 2005) $\mathrm{End}_G(V) = \bigoplus_\Lambda Fc_\Lambda$, where Λ varies 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 $c_{(1,x)\cdot g} = \rho_{1x}(g)$,
   where $\rho_{st}(g) := \mu(tg(t\cdot g)^{-1}(s\cdot g)g^{-1}s^{-1})$, $s,t \in T$, $g \in G$..

Adjacency Algebra

If $\mu = 1_H$, the trivial character of H, then V becomes the permutation module P affording the permutation character $(1_H)^G$.

$a = a_\Lambda$ is the adjacency matrix of the orbital Λ, that is, $a_{st} = 1$ iff $(s,t) \in \Lambda$, $a_{st} = 0$ otherwise.

Corollary: (Higman , Bannai-Îto, Michler-Weller) $\mathrm{End}_G(P) = \bigoplus_\Lambda \mathbb{Q}a_\Lambda$.

Generalized Intersection Numbers

Reorder orbitals so that μ-central occur first and set $c_i := c_{\Lambda_i}$;

We call the structure constants p_{ij}^k with respect to the basis $(c_1, \ldots, c_r)$ of $C := \mathrm{End}_G(V)$ the generalized intersection numbers

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

Theorem: p_{ij}^k may be efficiently obtained as a sum of μ-values depending on the G-structure of $T \times T$. Moreover, $p_{i1}^k = \delta_{ik}$ and $p_{1j}^k = \delta_{jk}$. In particular, c_1 is the identity matrix and the first row of c_i is the i-th standard vector.

and Intersection Numbers

Corollary: When $\mu = 1_H$, p_{ij}^k is an intersection number and equals

$$|x_i \cdot H \cap x_{j'} \cdot Hx_k|,$$

where $x_j^{-1} \in Hx_{j'}H$.

Reducing Dimensions: Episode I

First reduction: $\sigma : c_j \longrightarrow (p_{ij}^k)$ is the right regular representation for $C = \mathrm{End}_G(V)$.

σ reduces the size of matrices from $n = |G : H|$ to r, the number of μ-central orbitals.

Example: For $G = \mathrm{PGL}_2(73)$, $P \in \mathrm{Syl}_{73}(G)$, $H = N_G(P)$, $n = 2628$ and $r = 36$.

Reducing Dimensions: Episode II

Using the special shape of $\sigma(c_i)$ we obtain heuristically a set of generators for $\sigma(C)$ (as an algebra) in $\lceil \log_2(r) \rceil$ steps.

$Z_0 := \mathbf{Z}(\sigma(C))$, the center of $\sigma(C)$, can be efficiently obtained solving a linear system with a small number of equations.

Second reduction: Let $\tau : Z_0 \to (F)_t$ be the right regular representation for Z_0, where $t = \dim_F(Z_0)$.

We will analyze $Z = \tau(Z_0)$.

One-generator Algebras

Definition: We say A is a one-generator algebra over a field E if $A = E[a]$ for some $a \in A$.

Theorem: (Chillag 1995 P. 2005) Let A be a commutative, semisimple, finite-dimensional E-algebra, E a separable field. If $|E| > \mathtt{dim}_E(A)$, then A is a one-generator algebra.

Probabilistic Search

Corollary Let $Z = \tau(Z_0)$, then $Z = F[z]$, for some z.

z is obtained using a probabilistic approach.

Theorem: 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.

Central Primitive Idempotents

Theorem: 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, $a_{ij} \in E$.

Extended Gollan-Ostermann numbers

Definition: Given a μ-central orbital Λ_j and $g \in G$ we define the extended Gollan-Ostermann number

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

where $u \in T$ satisfies $x_j \cdot hug = 1 \cdot u$, for some $h \in H$.

Irreducible Characters values

Theorem: 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, $d_i = \chi_i(1) = \frac{n a_{i1}}{f_i}$.

Corollary: When $\mu = 1_H$ we obtain an algorithm by Michler and Weller (2002).

Corollary: When G is finite and $H = 1$ we obtain an algorithm due to Frobenius and Burnside.

Modular reduction

Unfortunately arithmetic in the cyclotomic field $E = \mathbb{Q}(\zeta_e)$ might be expensive if $e = \mathrm{Exp}(G)$ is big;

Resort to a modular à la Dixon approach;

p a prime congruent to $1 \pmod e$ and $p > \max(2n, t)$;

$L := \mathbb{F}_p$ and $\varepsilon_e \in L^*$ such that $|\varepsilon_e| = e$;

Build homorphism θ from $\mathbb{Z}[\zeta_e]$ into L via

$$\theta(f(\zeta_e)) = f(\varepsilon_e).$$

Set $M_L(g) := \theta(M(g))$, where we extend θ to matrices and M is the monomial representation;

Using a theorem of Brauer and Nesbitt we may express the modular reduction $\theta(\chi_i(g))$ as in the cyclotomic case;

Knowing the power maps in G we may lift these modular values uniquely into E.