

Exploiting the geometry

Eamonn O'Brien

University of Auckland

www.math.auckland.ac.nz/~obrien/bath-n.pdf

August 2009

Aschbacher (1984)

G maximal subgroup of $GL(d, q)$, let V be underlying vector space

- G preserves some **natural linear structure** associated with the action of G on V , and has normal subgroup related to this structure,
- or G is **almost simple modulo scalars**: $T \leq G/Z \leq Aut(T)$ where T is simple.

Theorem

$G \leq \text{GL}(d, q)$ acts on $V := \mathbb{F}_q^d$, and Z is the subgroup of scalar matrices of G . If G is a maximal subgroup of $\text{GL}(d, q)$, then one of the following is true:

- C1. G acts reducibly.
- C2. G acts imprimitively.
- C3. G acts on V as a group of semilinear automorphisms of a d/e -dimensional space over $\text{GF}(q^e)$, for some $e > 1$.
- C4. G preserves a decomposition of V as a tensor product.
- C5. G is definable modulo scalars over a subfield.
- C6. $d = r^m$, prime r , and $G \leq$ normaliser of $\text{ES}(r^{2m+1})$, or a symplectic type group of order 2^{2m+2} .
- C7. G preserves a decomposition of V as $V_1 \otimes V_2 \otimes \cdots \otimes V_m$, all of dimension $r > 1$, where $d = r^m$.
- C8. G is classical group in its natural representation.
- C9. $T \leq G/Z \leq \text{Aut } T$, for non-abelian simple group T .

A constructive version of Aschbacher's theorem

Given $G = \langle X \rangle \leq GL(d, F)$ acting on V .

Constructively decide (at least one of) its Aschbacher categories.

If $\ker \phi = N \triangleleft G$ exists, then construct both N and $\text{im } \phi$.

Desirable: Polynomial-time decision.

A constructive version of Clifford's theorem

Let non-scalar $N \triangleleft G$. Consider the restriction of V to N .

For some $t \geq 1$, V decomposes as direct sum $W_1 \oplus W_2 \oplus \cdots \oplus W_t$ of irreducible FN -modules, all same dimension.

For some $r, s \geq 1$, with $rs = t$, the W_i s partition into r sets, each containing s pairwise-isomorphic FN -modules.

If V_1, V_2, \dots, V_r are each the sum of s pairwise isomorphic W_i s, so that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$, then G permutes the V_i s transitively.

- If $r > 1$ then G acts imprimitively on V (C2).
- If $r = 1$ and $t > 1$ and the W_i are absolutely irreducible as FN -modules, then V is a tensor product preserved by G (C4).
- If $r = 1$ and the W_i are not absolutely irreducible as FN -modules, then G is semilinear (C3).

Otherwise, $r = s = 1$ and N acts absolutely irreducibly on V .

$N/Z(N) \cong N_0 \times N_0 \times \cdots \times N_0$ of m copies of simple group N_0 .

If N_0 is cyclic, then G normalises a symplectic-type group (C6).

Otherwise N_0 is non-abelian simple.

- If $m > 1$ G is tensor-induced (C7).
- If $m = 1$, G is almost simple.

The SMASH algorithm

Holt, Leedham-Green, O'B, Rees (1996): constructive realisation.

Assume G acts absolutely irreducibly on V and $S \subseteq G$ contains at least one non-scalar element.

SMASH investigates whether G preserves decomposition with respect to $\langle S \rangle^G$.

Problem

How can we construct elements of relevant N ?

Many heuristics apply.

Example

Assume $\phi : G \mapsto S_r$. If $|g|$ not valid for S_r , then $g \in \ker \phi$.

Further developed and analysed by Neunhöffer (2008).

C1: Reducible groups

Maximal subgroups of $GL(d, q)$ in C1 are maximal parabolics.

MEATAXE: Las Vegas algorithm to decide whether or not G acts irreducibly on V .

Original: Parker (1984).

Generalised by Holt & Rees (1994), analysis completed by Ivanyos & Lux (2000).

$G = \langle X \rangle$, M is FG -module, A is F -algebra spanned by X .

- 1 Select random $\theta \in A$, determine its characteristic polynomial $c(x)$ of θ , and factorise it.
- 2 Let $\chi = p(\theta)$ where $p(x)$ is an irreducible factor of $c(x)$. Hence χ has non-trivial nullspace N .
- 3 Now compute FG -submodule of M generated by non-zero vector in N . If we obtain proper submodule, G acts **reducibly** on V . Otherwise repeat Steps 2 and 3 for M^T .
- 4 If $p(x)$ has **multiplicity one**, then $\theta|_N$ acts with minimal polynomial $p(x)$ on N and $\dim(N) = \deg(p)$. So N is irreducible as $F\langle\theta\rangle$ -module. Conclude G acts **irreducibly** on V .
- 5 Otherwise repeat the random selection.

$A \in \text{Mat}(d, F)$ is *cyclic*: its characteristic polynomial coincides with its minimal polynomial. The vector space of $1 \times n$ matrices over F is cyclic as an $F\langle A \rangle$ -module.

Definition

Let f a monic irreducible polynomial over F . A is **f -cyclic** if f divides the minimal polynomial $m(t)$ of A , but f does not divide $c(t)/m(t)$, where $c(t)$ is characteristic polynomial.

Family of f -cyclic matrices contains all cyclic matrices and also all matrices where f divides $c(t)$ with multiplicity one.

MEATAXE uses last case: proportion at least 0.08. Las Vegas algorithm, complexity $O(d^4 \log q)$.

Neumann & Praeger (2001), Glasby (2006), Glasby & Praeger (2009): analysis of MEATAXE using such matrices.

C3: Semilinear groups

Maximal subgroups in C3 are $GL(d/e, q^e).e$ where prime $e|d$.

FG -module is *absolutely irreducible* if it remains irreducible under any extension of F . Equivalently $C_{GL(n,q)}(G)$ just scalars.

G not absolutely irreducible: there is an extension field $E = GF(q^e)$ of F , where $e|d$, and V is a vector space of dimension d/e over E , with G acting linearly over E .

So $G \cong H \leq GL(d/e, q^e)$.

Semilinear: G acts semilinearly on V regarded as an E -space, where field automorphisms fix F .

So homomorphism $\alpha : G \mapsto \text{Gal}(E : F)$ where

$$(\lambda v)^g = \lambda^{g\alpha} v^g$$

for all $v \in V$, all $g \in G$, and all $\lambda \in E$.

Image is cyclic group, kernel is absolutely reducible and so conjugate to subgroup of $GL(d/e, q^e)$.

Holt & Rees (1994): polynomial-time extension of the MEATAXE to determine centralising field of FG -module.

Lemma

If G is semilinear, then V has a direct sum decomposition as isomorphic irreducible FG' -modules V_i , and G' does not act absolutely irreducibly on the V_i .

Holt *et al.* (1996): apply SMASH to normal generating set for G' to decide if absolutely irreducible group G acts semilinearly.

C2: Imprimitve groups

Maximal subgroups in C2 are stabilisers of direct sum decompositions $V = \bigoplus_{i=1}^r V_i$ where $\dim(V_i) = d/r = s$.

Holt *et al.* (1996): algorithm to decide if absolutely irreducible group G acts imprimitively on V .

MINBLOCKS: given a non-trivial subspace of a block of imprimitivity, find the block system with minimal block dimension that contains this subspace.

SMASH applies when G **does not act faithfully** on the system of blocks: use element orders and characteristic polynomials of random elements to find non-scalar $g \in G$ which must lie in the kernel of the homomorphism from G to S_r .

Lemma

Let absolutely irreducible G act imprimitively on V and let H be the stabiliser of one such block W . $\text{Hom}_{FH}(W, V)$ has dimension 1 over F .

Proof.

V is isomorphic to the induced module W^G , where W is regarded as an FH -module.

Thus, W must be irreducible as an FH -module, since otherwise V would not be irreducible as an FG -module.

Frobenius Reciprocity: $\text{Hom}_{FG}(W^G, V) = \text{Hom}_{FH}(W, V)$.

Since V is absolutely irreducible FG -module, $\text{Hom}_{FH}(W, V)$ has dimension 1 over F . □

We apply MINBLOCKS to images of composition factors of appropriate dimension to find W .

So if we can **construct the stabiliser** H in G of a block W , then we can find W !

Assume G preserves a maximal system of imprimitivity on r blocks of size s , so action is primitive and H must be a maximal subgroup of G of index r .

We construct H by working up a chain of subgroups, starting with a cyclic subgroup and then adjoining new generators.

Polynomial-time? Difficulty of analysis of SMASH imprimitive case.

C4: Tensor products

Leedham-Green & O'B (1997)

Tensor decomposition of FG -module V as $U \otimes W$ consists of a FE -isomorphism between V and $U \otimes W$, where E is a covering group of G .

Kernel C of the homomorphism $E \mapsto G$ is a central cyclic subgroup of E whose elements acts as scalars on both U and W . If $g \in C$ acts as α on U , it acts as α^{-1} on W .

Definition not **useful**: in principle, must consider the tensor product of all pairs of modules of suitable dimensions over **covering groups** of G .

An internal description

Construct a family of projective geometries whose flats are certain subspaces of V .

Show there is a one-to-one correspondence between this family of projective geometries and the set of equivalence classes of tensor decompositions of V .

Internal: contains set of subspaces of V which are required to satisfy axioms that depend only on structure of V .

Let $u|d$, the dimension of V .

Usual construction of projective space is to take subspaces of V .

Modify: take certain subspaces of dimension a multiple of u .

These correspond to subspaces $U \otimes X$ of $U \otimes W$, where U and W are F -spaces of dimension u and w respectively, and X varies over the subspaces of W , under an isomorphism taking V onto $U \otimes W$.

Definition

A set of subspaces P_0, \dots, P_w of V is in *general position* if, for all i , one has $V = \bigoplus_{j \neq i} P_j$.

All P_i have same dimension.

Given P_0, \dots, P_w in general position, and $v_i \in P_i$ such that $\sum_i v_i = 0$, each v_i determines the others.

So $v_0 \mapsto v_i$ defines linear isomorphism θ_i of P_0 onto P_i ; regard θ_i as linear map of P_0 into V .

For $x = (x_1, \dots, x_w) \in W$ define $\theta_x \in \text{Hom}(P_0, V)$ by $\theta_x = \sum_j x_j \theta_j$.

Let $\mathcal{G} = (P_0, \dots, P_w)$ be ordered $(w+1)$ -tuple in general position. For $X \subseteq W$, define $\mathcal{G}(X) = \bigcup_{x \in X} \theta_x(P_0)$.

Let $\mathcal{G} = (P_0, \dots, P_w)$ be ordered $(w + 1)$ -tuple in general position.
For $X \leq W$, define $\mathcal{G}(X) = \cup_{x \in X} \theta_x(P_0)$.

Definition

Let V be a F -space of dimension $d = uw$ and let \mathcal{G} be $w + 1$ subspaces of V of dimension u in general position.

Let $\mathcal{F}(\mathcal{G})$ be the collection of subspaces $\mathcal{G}(X)$, for all $X \leq W$.
The u -projective geometry defined by \mathcal{G} is $\mathcal{F}(\mathcal{G})$.

$\mathcal{G}(X)$ is a *flat*; if X has dimension one, then $\mathcal{G}(X)$ is a *point*.

Definition

A u -tensor decomposition of V is a linear isomorphism from $U \otimes W$ onto V , where U and W are fixed vector spaces, with U of dimension u . If α and β are u -tensor decompositions of V , they are equivalent if there are linear automorphisms ϕ and ψ of U and W respectively such that $\alpha = \beta(\phi \otimes \psi)$.

Theorem

Let V be a vector space of dimension uw . For each u -tensor decomposition $\alpha : U \otimes W \mapsto V$, define $\mathcal{F}(\alpha)$ to be $\{\alpha(U \otimes X) : X \leq W\}$. Then the map $[\alpha] \mapsto \mathcal{F}(\alpha)$ is a bijection between the set of equivalence classes $[\alpha]$ of u -tensor decompositions of V and the set of u -projective geometries on V .

How to exploit this?

- 1 Find a candidate C for a flat in a u -projective geometry.
- 2 Investigate C to decide if it contains a point.

How do we find a flat? *Use reducible subgroups*

Let $H \leq G$ act reducibly on W . At least one of the H -invariant subspaces of V is a non-trivial flat of the form $U \otimes X$, where $X \leq W$, in the corresponding u -projective geometry.

Hence, **construct** $H \leq G$ that normalises sufficiently few subspaces of V that we can process these subspaces, but which also acts reducibly on W if required tensor factorisation exists.

Example

One natural class: p -local subgroup H .

If $p = \chi(F)$, then H cannot act irreducibly in any dimension > 1 .

A basic algorithm

- Construct a suitable $H \leq G$.
- Construct the H -submodule lattice of V and process all of the submodules which have dimension a multiple of u to decide if any of these is a flat in our geometry.
- If we find a point, then we have our geometry.
- If none is a flat, then we have ruled out the existence of a u -projective geometry.

Practical and theoretical problems?

p -local subgroups are “small”, so submodule lattice sometimes too large to construct.

Problem

Identify and construct easily “large” subgroups H which are guaranteed to act reducibly. Prove that the number of FH -submodules is polynomial in terms of input.

Example

Kleshchev (1990s): Choose $H := A_{n-1}$ as subgroup of A_n .

C3: Tensor Induction

G preserves a decomposition of V as

$$V_1 \otimes V_2 \otimes \cdots \otimes V_m$$

each V_i of dimension $r > 1$.

Let Z be the group of scalar matrices of $GL(d = r^m, q)$.

Hence $GZ/Z \leq PGL(r, q) \wr S_m$.

So there exists a homomorphism from G onto a *transitive* subgroup of S_m , with tensor-decomposable kernel.

Leedham-Green & O'B (2002):

algorithm searches for decomposition of V as a tensor product of m copies of a space U of dimension r , this decomposition preserved by G .

C5: Smaller field modulo scalars

Maximal subgroups of $GL(d, K)$: conjugates of $GL(d, F).Z$ where $F < K$ and Z is centre of $GL(d, K)$.

$G = \langle X \rangle$ absolutely irreducible subgroup of $GL(d, K)$, and $F < K$.

Glasby, Leedham-Green & O'B (2005): algorithm to decide if $G \cong H \leq GL(d, F).Z$.

Polynomial-time if G' acts absolutely irreducibly.

Clifford theory: if G is primitive, tensor-indecomposable, and not semilinear, then G' satisfies this.

Carlson, Neunhöffer, Roney-Dougal (2009): polynomial-time Las Vegas algorithm to find a non-trivial reduction of irreducible groups that either:

- lie in C5;
- are semilinear;
- or have non-absolutely irreducible derived group.

C6: Normaliser of a p -group

$G \leq \text{GL}(d, q)$ absolutely irreducible

$R \trianglelefteq G$ where R has order r^{2n+1} (extraspecial) or 2^{2n+2} (symplectic type), where $d = r^n$, $r|(q-1)$.

$\phi : G \mapsto \text{GL}(2n, r)$ where G acts by conjugation on $R/Z(R)$.

Niemeyer (2006): $d = r$.

Brooksbank, Niemeyer, Seress (2006): algorithm to produce nontrivial homomorphism from G to either $\text{GL}(2m, r)$ or $\text{Sym}(r^m)$ where $1 \leq m \leq n$.

Polynomial-time guaranteed when G is the full normalizer of R , or $d = r^2$.

A constructive version?

- Reducible. Polynomial time? **Yes.**
- Imprimitive? **No.**
- Semilinear? **Yes in almost all cases.**
- Tensor product? **No.**
- Defined mod scalars over subfield? **Yes in certain cases.**
- Normaliser of p -group? **Yes in certain cases.**
- Tensor induced? **No.**
- Classical group in natural representation? **Yes.**
- Almost simple modulo scalars?

Practical algorithms to decide membership available in MAGMA.