Aschbacher's Theorem revisited with a view to Constructive Matrix Group Recognition

Max Neunhöffer

University of St Andrews

Auckland, 28.1.2009

Constructive recognition of matrix groups

Problem

Let $\mathbb{F}_q$ be the field with q elements und

$$M_1, \ldots, M_k \in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for $G := \langle M_1, \ldots, M_k \rangle$:

- The group order $|G|$ and
- an algorithm that, given $M \in \mathrm{GL}_n(\mathbb{F}_q)$,
  - decides, whether or not $M \in G$, and,
  - if so, expresses M as word in the M_i.
- The runtime should be bounded from above by a polynomial in n, k and $\log q$.
- A Monte Carlo Algorithm is enough. (Verification!)

If this problem is solved, we call

$\langle M_1, \ldots, M_k \rangle$ recognised constructively.

Reductions

Let $G := \langle M_1, \ldots, M_k \rangle \leq \mathrm{GL}_n(\mathbb{F}_q)$.

A reduction is a group homomorphism

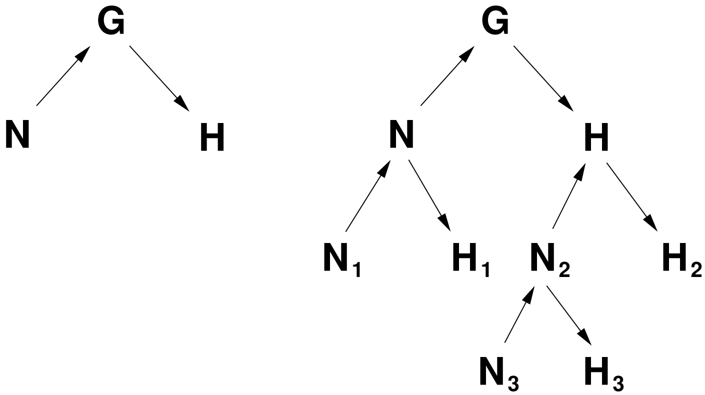
$$\begin{array}{cccccl} \varphi & : & G & \to & H & \\ & & M_i & \mapsto & P_i & \qquad \text{for all } i \end{array}$$

with the following properties:

- $\varphi(M)$ is explicitly computable for all $M \in G$
- φ is surjective: $H = \langle P_1, \ldots, P_k \rangle$
- H is in some sense "smaller"
- or at least "easier to recognise constructively"
- e.g. $H \leq S_m$ or $H \leq \mathrm{GL}_{n'}(\mathbb{F}_{q'})$ with $n' \log q' < n \log q$

Recursive reduction: composition trees

We get a tree:



Up arrows: inclusions

Down arrows: homomorphisms

Old idea, improvements are still being made

Which theorem of Aschbacher do I mean?

Theorem (Aschbacher 1984)

Let G_0 be a simple classical group over a finite field and $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Let $H < G$ such that $HG_0 = G$. Define geometrically classes $\mathcal{C}_1$ to $\mathcal{C}_8$ of subgroups of G. Then either H is a subgroup of at least one of the groups in classes $\mathcal{C}_1$ to $\mathcal{C}_8$, or the following hold:

- *There is a non-abelian simple group H_0 with $H_0 \leq H \leq \mathrm{Aut}(H_0)$.*
- *The natural H-module V is absolutely irreducible.*
- *This representation for H cannot be realised over a smaller field.*

There is a number of simplifying lies on this slide!

A variant . . .

Let $n \in \mathbb{N}$ and $\mathbb{F}_q$ the field with $q = p^e$ elements. Let $V := \mathbb{F}_q^{1\times n}$ be the $\mathbb{F}_q$-vector space of row vectors.

Theorem

Let $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ and $n \geq 2$. Then G lies in at least one of the classes $\mathcal{D}_1$ to $\mathcal{D}_9$ of subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$.

- I will not tell you on this slide what the classes $\mathcal{D}_1$ to $\mathcal{D}_9$ are.
- I will show you a sketch of the proof of this statement.
- This is not new, lots of people have worked on this.
- Alongside the proof, we will
  - define $\mathcal{D}_1$ to $\mathcal{D}_9$, and
  - keep an eye on how one can find reductions computationally.

Reducible: $\mathcal{D}_1$

G could lie in $\mathcal{D}_1$:

Definition of class $\mathcal{D}_1$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_1$ if there is a subspace $0 < W < V$ with $Wg = W$ for all $g \in G$.

We can decide computationally using the MeatAxe, whether such an invariant subspace W exists or not.

Assumption

From now on we assume that G acts irreducibly on V.

✓

Not absolutely irreducible: $\mathcal{D}_3$

G could act irreducibly but not absolutely irreducibly.

(G acts absolutely irreducibly iff $C_{\mathrm{GL}_n(\mathbb{F}_q)}(G) = \{c \cdot \mathbf{1}\}$.)

Lemma

If $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ acts irreducibly but not absolutely irreducibly on the natural module V, then G lies in $\mathcal{D}_3$.

We can decide computationally using the MeatAxe, whether G acts absolutely irreducibly on V.

Assumption

From now on we assume that G acts absolutely irreducibly on V.

✓

Semilinear: $\mathcal{D}_3$

Definition of class $\mathcal{D}_3$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_3$ if

- the natural module V is irreducible and
- there is a finite field $\mathbb{F}_{q^s}$, for which we can extend the $\mathbb{F}_q$-vector space structure of V to an $\mathbb{F}_{q^s}$-vector space structure of dimension n/s, such that:

$$\forall g \in G\ \exists \alpha_g \in \mathrm{Aut}(\mathbb{F}_{q^s}) \text{ with:}$$

$$(v + \lambda w) \cdot g = v \cdot g + \lambda^{\alpha_g} \cdot w \cdot g$$

for all $v, w \in V$ and all $\lambda \in \mathbb{F}_{q^s}$.

(i.e. the action of G on V is $\mathbb{F}_{q^s}$-semilinear)

Non-absolutely irred. case: all automorphisms are trivial!

Subfield: $\mathcal{D}_5$

G could lie in $\mathcal{D}_5$:

Definition of class $\mathcal{D}_5$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_5$ if

- the natural module V is absolutely irreducible and
- there is a proper subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$ and $T \in \mathrm{GL}_n(\mathbb{F}_q)$ and $(\beta_g)_{g \in G}$ with $\beta_g \in \mathbb{F}_q$ such that

$$\beta_g \cdot T^{-1} g T \in \mathrm{GL}_n(\mathbb{F}_{q_0}) \text{ for all } g \in G.$$

We can decide computationally whether G lies in $\mathcal{D}_5$ (see Glasby, Leedham-Green, and O'Brien (2006) and Carlson, N. and Roney-Dougal (submitted)).

Assumption

From now on we assume that G does not lie in $\mathcal{D}_5$.

G/Z is simple: $\mathcal{D}_8$ or $\mathcal{D}_9$

From now on denote $Z := Z(G) = G \cap Z(\mathrm{GL}_n(\mathbb{F}_q))$.

The group G/Z could be simple.

If G/Z were cyclic, then G would be abelian and V not absolutely irreducible.

Then G/Z is either a classical simple group in its natural representation (then G lies in $\mathcal{D}_8$), or G lies in $\mathcal{D}_9$.

We cannot find a reduction in this case. Thus we have to recognise G constructively in some other way!

Assumption

Assume from now on that G/Z is not simple.

Classical in natural representation: $\mathcal{D}_8$

Definition of class $\mathcal{D}_8$

$G \le \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_8$ if G/Z contains a classical simple group in its natural representation in one of the following ways:

- G/Z contains $\mathrm{PSL}_n(\mathbb{F}_q)$ and $(n, q) \notin \{(2, 2), (2, 3)\}$,
- n is even, G is contained in $N_{\mathrm{GL}_n(\mathbb{F}_q)}(\mathrm{Sp}_n(\mathbb{F}_q))$ for some non-singular symplectic form, G/Z contains $\mathrm{PSp}_n(\mathbb{F}_q)$ and $(n, q) \notin \{(2, 2), (2, 3), (4, 2)\}$,
- q is a square, G is contained in $N_{\mathrm{GL}_n(\mathbb{F}_q)}(\mathrm{SU}_n(\mathbb{F}_{q^{1/2}}))$ for some non-singular Hermitian form, G/Z contains $\mathrm{PSU}_n(\mathbb{F}_{q^{1/2}})$ and $(n, q^{1/2}) \notin \{(2, 2), (2, 3), (3, 2)\}$,
- G is contained in $N_{\mathrm{GL}_n(\mathbb{F}_q)}(\Omega_n^{\epsilon}(\mathbb{F}_q))$, the corresponding $\mathrm{P}\Omega_n^{\epsilon}(\mathbb{F}_q)$ is simple and contained in G/Z. The group $\mathrm{P}\Omega_n^{\epsilon}(\mathbb{F}_q)$ is simple if and only if
  - $n \ge 3$, and
  - q is odd if n is odd, and
  - ϵ is $-$ if $n = 4$, and
  - $(n, q) \notin \{(3, 3), (4, 2)\}$.

G/Z almost simple: $\mathcal{D}_9$

Definition of class $\mathcal{D}_9$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_9$, if

- it is not in $\mathcal{D}_8$ and
- there is a non-abelian simple group $\overline{N}$ and a group T with $\overline{N} \leq T \leq \mathrm{Aut}(\overline{N})$ such that
  - $G/Z \cong T$ and
  - V gives rise to an absolutely irreducible projective representation for T,
    which is not realisable over a proper subfield of $\mathbb{F}_q$.

✓

Clifford theory

Let now $\overline{N}$ be a minimal normal subgroup of G/Z and let $Z < N \lhd G$ be the full preimage.

Theorem (Clifford)

The restriction $V|_N$ of the natural module to the normal subgroup N is a direct sum

$$V|_N = \bigoplus_{i=1}^{k} W_i$$

of irreducible N-modules W_i which are all G-conjugates of a single submodule $W \leq V|_N$, i.e. $W_i = Wg_i$ for some $g_i \in G$.

Now we distinguish cases for this decomposition.

W not absolutely irreducible: $\mathcal{D}_3$

Remember: $Z < N \lhd G$ such that N/Z is minimal normal.

Lemma

Let W be an irreducible submodule of $V|_N$. If W is not absolutely irreducible, then G lies in $\mathcal{D}_3$.

This is computationally under control, see "SMASH": Holt, Leedham-Green, O'Brien and Rees (1996) or Carlson, N., Roney-Dougal (submitted).

Assumption

From now on we assume that W is absolutely irreducible.

✓

$V|_N$ not homogeneous: $\mathcal{D}_2$

Assume that not all W_i are isomorphic to W.

Then G permutes the homogeneous components and lies in $\mathcal{D}_2$:

$$V|_N = \bigoplus_{i=1}^{k} W_i = \bigoplus_{j} \left(\bigoplus_{a} W_a^{(j)} \right)$$

where $W_a^{(j)} \cong W_b^{(l)}$ iff $j = l$.

Definition of class $\mathcal{D}_2$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_2$ if

- the natural module V is absolutely irreducible and
- there is $Z < N \lhd G$ such that $V|_N = \bigoplus_{i=1}^{k} W_i$ and the W_i are absolutely irreducible $\mathbb{F}_q N$-modules and not all isomorphic.

$V|_N$ homogeneous: $\mathcal{D}_4$

Assume that all W_i are isomorphic to W and $k > 1$.

If $\dim_{\mathbb{F}_q}(W) = 1$ then N would be scalar.

Definition of class $\mathcal{D}_4$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in class $\mathcal{D}_4$ if

- the natural module V is absolutely irreducible and
- there is $N \lhd G$ such that $V|_N = \bigoplus_{i=1}^k W_i$ with $k \geq 2$ and $W_i \cong W$ for all i, where W is an absolutely irreducible $\mathbb{F}_q N$-module with $\dim_{\mathbb{F}_q}(W) > 1$.

Assumption

We assume from now on that $W = V|_N$.

Minimal normal subgroups

Now look at the group structure of N/Z:

Lemma (Minimal normal subgroups)

Let $1 < K \triangleleft H$ be a minimal normal subgroup. Then

$$K \cong T_1 \times T_2 \times \cdots \times T_k$$

and the T_i are copies of a simple group which are all conjugate under H.

Therefore,

$$N/Z \cong T_1 \times T_2 \times \cdots \times T_k,$$

the T_i are pairwise isomorphic simple groups which are all conjugate under G/Z and thus G.

We distinguish 3 cases:

1. the T_i are cyclic groups of prime order r ($\mathcal{D}_6$)
2. the T_i are non-abelian simple and $k \geq 2$ ($\mathcal{D}_7$)
3. $k = 1$ and T_1 is non-abelian simple ($\mathcal{D}_8$ or $\mathcal{D}_9$)

Extraspecial: $\mathcal{D}_6$

Definition of class $\mathcal{D}_6$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_6$ if

- the natural module V is absolutely irreducible,
- $n = r^m$ for a prime r and
-
  - either r is odd and G has a normal subgroup E that is an extraspecial r-group of order r^{1+2m} and exponent r,
  - or $r = 2$ and G has a normal subgroup E that is either extraspecial of order 2^{1+2m} or a central product of a cyclic group of order 4 with an extraspecial group of order 2^{1+2m},
- and in both cases the linear action of G on the $\mathbb{F}_r$-vector space $E/Z(E)$ of dimension $2m$ is irreducible.

This class is in practice computationally under control.

Tensor-induced: $\mathcal{D}_7$

Definition of class $\mathcal{D}_7$

$G \le \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_7$ if

- the natural module V is absolutely irreducible and,
- there is $Z < N \lhd G$ such that for some $k > 1$,

$$N \cong \underbrace{T \circ \cdots \circ T}_{k \text{ factors}} \quad \text{(central product)},$$

where T/Z is a non-abelian simple group, such that:

  - $V|_N \cong W_1 \otimes_{\mathbb{F}_q} \cdots \otimes_{\mathbb{F}_q} W_k$ where the W_i are absolutely irreducible $\mathbb{F}_q T$-modules of the same dimension on which Z acts as scalars,
  - and G/N permutes the tensor factors transitively.

Finding reductions for groups in $\mathcal{D}_2$ and $\mathcal{D}_4$

$\mathcal{D}_2$ and $\mathcal{D}_4$ in this formulation have in common:

- In both cases there is an N with $Z < N \lhd G$.
- $V|_N$ is reducible such that the MeatAxe can:
  - determine whether $H \leq N$ for some $H \lhd G$ and
  - find a reduction in that case.

Since we can compute normal closures in G, all we need is to solve:

Problem

Find one element $n \in N \setminus Z$ with high probability.

✓

Finding a reduction for groups in $\mathcal{D}_7$

Also the definition of $\mathcal{D}_7$ involves N with $Z < N \lhd G$.

However, this time $V|_N$ is irreducible, so we do not notice, whether some $H \leq N$!

But: N in $\mathcal{D}_7$ lies itself in $\mathcal{D}_4$!

Idea

If we had a provably nice way to produce elements in a normal subgroup, then we could use the trick twice.