

Recognising Aschbacher's Category \mathcal{C}_6

Peter Brooksbank

(Joint work with Alice Niemeyer and Ákos Seress)

Department of Mathematics

Bucknell University

`pbrooksb@bucknell.edu`

Finite Geometries, Groups and Computation

Pingree Park, September 4–9, 2004

“Matrix Group Project”

A central problem in computational group theory is that of finding a composition series for any group given by a generating set of matrices with entries in a finite field.

Even basic information about a given matrix group

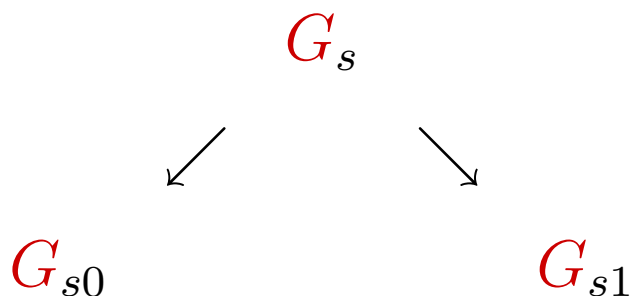
$$G = \langle X \rangle \leq GL(d, q),$$

such as its order, seems to require the deep structural knowledge afforded by its composition series.

“Composition tree”

One attack on the problem, led by Leedham-Green and O’Brien, proceeds by recursion to construct a **composition tree** for G .

The idea, given generators for some node G_s of the tree (a section of G), is to construct a **left child**, G_{s0} , as the kernel of some action of G_s , and a **right child**, G_{s1} , as the group induced under this action.



The algorithm then recurs to G_{s0} and G_{s1} .

Using Aschbacher's classification

Aschbacher demonstrated that every maximal subgroup, M , of a classical group belongs to one of a number of categories.

[base case] M is almost simple modulo scalars.

[recursive case] M preserves a geometric structure.

Given a node G_s (not a leaf) of the composition tree:

- Find a geometric structure Δ preserved by G_s .
- $G_{s1} :=$ the group induced by G_s on Δ .
- $G_{s0} :=$ subgroup of G_s centralising Δ .

Recur to G_{s1} and G_{s0} in 'right depth-first' order.

Category \mathcal{C}_6

If G is contained in a member of \mathcal{C}_6 then:

- $G \leq GL(r^m, q)$, where r divides $q - 1$.
- $R = O_r(G)$ is of symplectic type r^{1+2m} (or possibly $4 \circ 2^{1+2m}$).
- G acts on the $2m$ -space $R/Z(R)$ inducing a subgroup of $Sp_{2m}(r)$ or $\Omega^\pm_{2m}(2)$ (only when $r = 2$).

We will often denote the classical module $R/Z(R)$ simply by V , and the corresponding classical group generically by $Cl(V)$.

Recognising \mathcal{C}_6

We want an algorithm to recognise, **constructively**, when a given group $G = \langle X \rangle \leq GL(r^m, q)$ is contained in a member of \mathcal{C}_6 .

A positive output to the algorithm consists of the following:

1. A “**nice**” generating set for $R = O_r(G)$ (and verification that R has the correct order).
2. An “**effective homomorphism**” $\Psi: G \rightarrow Cl(V)$. (Given any $g \in G$, we require that we can find $g\Psi \in Cl(V)$ efficiently.)

Alice Niemeyer devised an effective algorithm to handle the case $m = 1$ for r odd.

I shall discuss the general problem, but focus on the cases where Ψ is an **epimorphism** (the “**full normaliser**” cases).

Algorithm in outline

The algorithm has two stages:

Stage 1: [construct $R = O_r(G)$]

1. Find any noncentral element $u \in O_r(G)$.
2. Take enough G -conjugates of u to generate R .

Stage 2: [“coordinatise” $R/Z(R)$]

1. Find $B \subset R$ such that $\overline{B} = \{bZ(R) \mid b \in B\}$ is a basis of the classical module $V := R/Z(R)$.
2. Give a procedure for linear algebra in V relative to \overline{B} .

Given $g \in G$, one finds (the matrix representing) $g\Psi \in Cl(V)$ by writing each element of \overline{B}^g as a vector relative to \overline{B} .

Testing membership in $O_r(G)$

We wish to regard G essentially as a “black box group” modulo its r -core. Thus we need an algorithm that decides, for given $u \in G$, whether $u \in O_r(G)$.

$e := r * (2, r)$.

$Z := \{\text{id}_G\}$.

for suitably many choices $x \in G$ do

$z := [u, u^x]$;

$Z := Z \cup \{z^i\}_{i=1}^e$.

end for

if $|Z| > e$ then return false; else return true

Stage 1: $r = 2$

The algorithm in this case is very basic.

Let R denote $O_r(G)$. For $g \in G$, let \bar{g} denote $gR \in G/R$, and let \tilde{g} denote the transformation of $V := R/Z(R)$ induced by g .

repeat

 choose $g \in G$; $n := |\bar{g}|$; $u := g^n$

until $u \notin Z(R)$

return u

Whether or not g powers up to a suitable u is determined by a condition involving n and the transformation $\tilde{g} \in Cl(V)$.

Good news: Enough elements of $Cl(V)$ satisfy this condition.

Stage 1: $r > 2$

Simple powering method fails. Instead we proceed as follows:

repeat

choose $g \in G$;

until $n := |\bar{g}| = r^m + 1$

$[G/R \cong Sp_{2m}(r)]$

$\iota := g^{n/2}$

$[\bar{\iota} \text{ is } -1 \text{ on } R/Z(R)]$

repeat

choose $x \in G$

until $u := [\iota, \iota^x] \notin Z(R)$

return u

Theorem

There is a Las Vegas algorithm which, given any input group $G = \langle X \rangle \leq GL_d(q)$, the normaliser of a symplectic type r -group, where $d = r^m$, produces a generating set for $R = O_r(G)$, and an effective epimorphism $\Psi: G \rightarrow Cl(R/Z(R))$.

The algorithm requires

$$O(\log d[\omega_G + \xi_G + d^3(|X| + \log d)])$$

field operations, where

$$\xi_G = \# \text{ field ops to choose a random element of } G \quad (\xi_G \geq |X|d^\omega).$$

$$\omega_G = \# \text{ field ops to find } |g| \text{ for any given } g \in G.$$

Computing the image, $g\Psi$, of any given $g \in G$ requires $O(d^\omega \log^2 d)$ field operations.

Performance

Here is a sample of some performance tests (run on my desktop machine) for a GAP implementation of the algorithm. CPU time is the average completion time, in seconds, over 10 runs.

group	representation	CPU time
$3^{1+6}.Sp_6(3)$	$GL_{27}(4)$	0.5
$2^{1+12}.\Omega_{12}^+(2)$	$GL_{64}(3)$	3.5
$2^{1+12}.\Omega_{12}^+(2)$	$GL_{64}(11)$	4.5
$3^{1+8}.Sp_8(3)$	$GL_{81}(4)$	3.5
$5^{1+6}.Sp_6(5)$	$GL_{125}(16)$	10
$2^{1+14}.\Omega_{14}^+(2)$	$GL_{128}(3)$	18

Perfect subgroups

We have only discussed the case when G is a full normaliser (that is, when the homomorphism Ψ is an epimorphism):

$$r^{1+2m} \cdot Sp_{2m}(r), \quad 2_{\pm}^{1+2m} \cdot \Omega^{\pm}_{2m}(2) \quad \text{or} \quad (4 \circ 2^{1+2m}) \cdot Sp_{2m}(2)$$

One also has to deal with perfect subgroups of these groups.

Case $r = 2$: The naive powering method works, in practice, for all of the examples we've been able to construct. We do not yet have a theoretical result for all cases.

Case $r > 2$: The central involution method requires that we are given the full normaliser. We are in the process of devising variations to handle the other possibilities.