

# The CompositionTree project

Eamonn O'Brien

University of Auckland

July 2009

- Current status of CompositionTree
- Rewriting
- What's needed?
- Towards polynomial-time?

# Constructing the composition tree for $G$

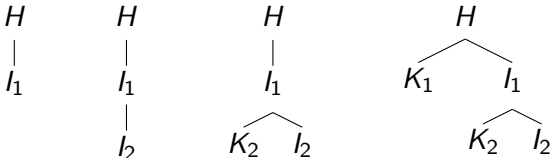
New implementation in MAGMA developed with Henrik Bäärnhielm (2008).



- Node: section  $H$  of  $G$ .
- Image  $I$ : image under homomorphism or isomorphism. Images correspond to Aschbacher category, but also others.
- Kernel  $K$ .
- *Leaf*: “composition factor” of  $G$ ; quasisimple, cyclic not necessarily of prime order.

Tree is constructed in “right depth-first order”.

If node  $H$  is not a leaf, construct recursively subtree rooted at  $I$ , then subtree rooted at  $K$ .



# Constructing kernels

Assume  $\phi : H \mapsto I$  where  $K = \ker \phi$ .



Sometimes easy to obtain theoretically generating sets for  $\ker \phi$ .

Otherwise, construct normal generating set for  $K$ , by evaluating relators in presentation for  $I$ , and take normal closure.

So we need a presentation for  $I$ .

To obtain presentation for node: **need only presentation for associated kernel and image.**

So inductively need to know presentations **only for the leaves.**

# Short presentations for finite simple groups

Theorem (Guralnick, Kantor, Kassabov, Lubotzky, 2008)

*Every non-abelian finite simple group of rank  $n$  over  $\text{GF}(q)$ , with possible exception of Ree groups  ${}^2G_2(q)$ , has a presentation with a bounded number of generators and relations and total length  $O(\log n + \log q)$ .*

Constructive version (L-G and O'B, ongoing): explicit short presentations for the classical groups on our standard generators.

Presentations now available for  $SL$ ,  $Sp$ ,  $SU$  in all characteristics.

Number of relations  $\simeq 20 + (\# \text{ for } A_n \text{ or } S_n)$ .

- Node has a list of **nice** generators.

Leaf: various. E.g. classical group: standard generators.

Internal: union of those associated with kernel and image.

Presentations, SLPs are on nice generators, usually shorter than on user-supplied generators.

Can rewrite to give SLPs on user-generators.

- Each leaf  $G$  has associated **standard copy**  $S$ : typically the corresponding finite quasi-simple group in a “small degree” (permutation or matrix) representation.

Two (effective) isomorphisms (possibly mod scalars)  $G \mapsto S$  and  $S \mapsto G$ .

$S \leq G/Z \leq \text{Aut}(S)$  so  $G \simeq Z.S.E.$

- Use determinant map to ensure that  $|Z|$  is a divisor of  $\gcd(d, q - 1)$ .
- Calculate the stable derivative  $D = G^{(\infty)}$  of  $G$ .
- Construct  $\phi : G \mapsto E$  by letting  $G$  act on cosets of  $H = \langle Z, D \rangle$ .

$$Hx = Hy \iff xy^{-1} \in H$$

Use L-G “order of element modulo normal subgroup” algorithm to determine to decide membership in  $H$ .

- Niemeyer & Praeger: classical groups natural representation.
- Babai, Kantor, Palfy, Seress: black-box algorithm to determine groups of Lie type.
- Malle & O'B: extensions to cover exceptionals and sporadics.

Liebeck & O'B (2007): black-box algorithm to determine characteristic.

Kantor & Seress (2009): three largest orders determine odd characteristic.

# Constructive recognition for classical groups

$SL(2, q)$  natural copy, defining char repn, and black-box.  
(Conder, Leedham-Green, O'B; Brooksbank)

$SL(3, q)$  natural copy, defining char repn, and black-box.  
(Lübeck, Magaard, O'B).

$SX(d, q)$  natural copy, odd characteristic (L-G, O'B)

$SL(d, q)$  natural copy, even characteristic (L-G, O'B)

$SX(d, q)$  odd defining char, black-box repns (Burns, ongoing)

- “Small” dimensional cases for  $Sp(d, q)$  and  $SU(d, q)$ : black box (Brooksbank, ongoing).
- $SL(d, q)$  black box and  $Sp(d, q)$  odd char (Kantor & Seress)
- Small degree representations of  $SL(d, q)$  (Magaard, O'B, Seress): adjoint representation, Ryba (2007).

Wilson (1996): standard generators for sporadic  $G = \langle X \rangle$

Bray and Wilson: black-box algorithms to find these in  $X$ .

## **Presentations on standard generators:**

- Th: presentation of Havas, Soicher, Wilson; nice words provided by Bray to move from their generators to standard
- Ly: presentation of C. Parker (2002) and his “nice” words.
- ON, Fi24' and HN: obtained by rewriting known “nice” presentations onto standard generators.

- $A_n$ : Bratus & Pak (2000), Holt; Beals et al. (2001-05).  
Black-box.
- Exceptional groups:
  - Bäärnhielm (2006-2009): algorithms for matrix representations of Suzuki, large and small Ree groups.
  - Kantor & Magaard (ongoing): black-box algorithms.

# Default constructive recognition

- Random Schreier: with careful choice of base points (Murray & O'B, O'B & Wilson).
- REDUCTION algorithm of Holmes et al. (2008): reduces constructive membership problem in  $G$  to three instances of the same problem for involution centralisers in  $G$ .

Centraliser of involution: solved using COMPOSITIONTREE.

Analysis of REDUCTION applies to odd char only; practical also for even char, small field since involutions can be found.

# Output and verification of COMPOSITIONTREE

Given  $G = \langle X \rangle$  as input. Output:

- a composition series:  $1 = G_0 \triangleleft G_1 \triangleleft G_2 \cdots \triangleleft G_m = G$ .
- A representation  $S_k = \langle X_k \rangle$  of  $G_k/G_{k-1}$
- Computable maps  $\tau_k : G_k \rightarrow S_k$ ,  $\phi_k : S_k \rightarrow G_k$   
 $\tau_k$  epimorphism with kernel  $G_{k-1}$   
for  $g \in S_k$ ,  $\phi_k(g)$  is element of  $G_k$  satisfying  $\tau_k \phi_k(g) = g$ .
- Function to write  $g \in G$  as word in  $X$  and “nice” generators.

Obtain  $H$ , a group with composition factors the leaves.

So  $H \leq G$ , perhaps **proper**.

Now construct presentation for  $H$  and verify that  $G$  satisfies the relations for  $H$ .

# Composition series to characteristic series $\mathcal{C}$ ?

$G$  has characteristic series  $\mathcal{C}$  of subgroups:

$$1 \leq O_\infty(G) \leq S^*(G) \leq P(G) \leq G$$

Derek Holt: modify output of composition tree to produce  $\mathcal{C}$ .

Obtain as the first kernel  $O_p(G)$ .

Elliot Costi (2009)

“Constructive membership testing in classical groups”

- $G = \mathrm{SX}(d, q)$ : algorithms to write element of  $G$  as SLP on our standard generators.

Complexity:  $O(d^3 \log q)$

- $G$  is defining char (projective) irreducible representation of  $\mathrm{SX}(d, q)$ .

Complexity:  $O(d^4 n^3 \log^3 q + d^2 n^4 \log q)$ .

Complete implementation available.

- Stabiliser of subspace algorithm.

Input: unipotent  $K \leq \text{GL}(d, q)$  and  $U \leq V$ .

Output: a canonical element  $\overline{U}$  of the orbit of  $U$  under  $K$ ; and  $k \in K$  such that  $U^k = \overline{U}$ , and generators for the stabiliser of  $U$  in  $K$ .

- Constructively decide membership in unipotent group.

# Defining characteristic representations

$H = \mathrm{SL}(d, q)$ ,  $G \leq \mathrm{GL}(n, F)$  is (projective) irreducible representation in defining char acting on  $V$ ,  $\phi : H \rightarrow G$ .

Let  $K$  be maximal parabolic subgroup of  $\mathrm{SL}(d, q)$  that fixes the space spanned by first basis element.

$$\begin{pmatrix} \det^{-1} & 0 & & 0 \\ \star & & & \\ \vdots & & \mathrm{GL}(d-1, q) & \\ \star & & & \end{pmatrix}$$

Since  $K\phi$  is  $p$ -local, it stabilises a proper  $K\phi$ -submodule  $U$  of  $V$ .

Consider elementary abelian  $E \leq H$  generated by

$$\begin{pmatrix} 1 & \star & \dots & \star \\ 0 & & & \\ \vdots & & I_{d-1} & \\ 0 & & & \end{pmatrix}$$

# Critical reduction

Construct  $x \in E\phi$  as an SLP that maps  $W := U^g$  to  $U$ .

Hence  $U^{gx} = U$  and so preimage of  $gx$  is in  $K$ .

So we have “killed” the first row of the preimage of  $gx$ .

Dualise to kill first column, obtaining  $g_1 := \begin{pmatrix} \alpha & 0 \\ 0 & A \end{pmatrix}$

$t\phi := g_1^{-1} \cdot T_{1,j}^\phi \cdot g_1 \in E\phi$  where  $T_{1,j}$  is transvection with non-zero entry in  $(1,j)$  position.

Use **membership test** for  $t\phi$  in  $E\phi$  to obtain preimage  $t \in E$ .

Read off from  $t$  (scalar multiple of)  $j$ -th row of preimage in  $SL(d, q)$  of  $g_1$ .

So reduce problem to **natural representation** in rank  $d - 1$ .

- Schneider *et al.*: black SL, Sp on our standard generators.
- Kantor-Seress rewriting: available as part of MAGMA implementation for  $SL(d, q)$  on a larger generating set.
- Brooksbank rewriting: small rank cases in MAGMA.

# What is needed?

- Constructive recognition:
  - classical groups in even char, all reps;
  - exceptional groups.
- Presentations for exceptional groups on “standard” generators.
- Black-box rewriting algorithms.

## Problem

*Can we prove that `CompositionTree` runs in polynomial time?*

Critical component: deciding Aschbacher category.

Classical group in natural representation? Polynomial.

Reducibility or absolutely reducibility? Polynomial.

## 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.

One problem case:  $G$  both imprimitive and semilinear, may learn only that  $G$  is imprimitive.

# Smaller Field modulo scalars?

Glasby, Leedham-Green, O'B (2005): If  $G'$  acts absolutely irreducibly, then polynomial-time algorithm to decide.

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

- lie in the Smaller Field mod scalars category;
- are semilinear;
- or have non-absolutely irreducible derived group.

# Normaliser of a $p$ -group

$R \trianglelefteq G \leq \text{GL}(d, q)$  of order  $r^{2n+1}$  or  $2^{2n+2}$ ,  
where  $d = r^n$  and  $r|(q-1)$ .

Niemeyer (2006):  $d = r$ .

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

Polynomial-time when  $G$  is normaliser of  $R$ , or  $d = r^2$ .

Both available within COMPOSITIONTREE.

Holt *et al.* (1996):

## Lemma

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

## Problem

*Construct the **stabiliser** in  $G$  of a block  $W$ .*

L-G & O'Brien (1997): internal description via projective geometry to deduce when  $G$  preserves a tensor decomposition of  $V = U \otimes W$ .

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 corresponding  $u$ -projective geometry.

## Problem

*Identify and construct easily “large” subgroups  $H$  which are guaranteed to act reducibly on at least one factor in a tensor decomposition. Prove that the number of  $FH$ -submodules is polynomial in terms of input.*