The Composition Tree

Eamonn O'Brien

University of Auckland

August 2011

Geometry following Aschbacher: general strategy

$G = \langle X \rangle \leq \mathrm{GL(d, q)}$.

1. Determine (at least one of) its Aschbacher categories.
2. If $N \lhd G$ exists, process N and G/N recursively.
3. Otherwise G is either classical group in natural representation or $T \leq G/Z \leq Aut(T)$ where T is simple.
   - "Reduce" from G to quasisimple group L.
   - Name L.
   - Set up "effective" isomorphisms between L and its standard copy S.

The C9 case

$L \leq G/Z \leq \mathrm{Aut}(L)$ so $G \simeq Z.L.E$.

- 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 $\phi : G \longmapsto E$ by letting G act on cosets of $H = \langle Z, D \rangle$.

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

  Use "order of element modulo normal subgroup" algorithm to determine to decide membership in H.

The composition tree for G

Bäärnhielm, Leedham-Green & O'B
Neunhöffer & Seress

$$
\begin{array}{ccc}
 & H & \\
K & & I
\end{array}
$$

- Node: section H of G.
- Image I: image under homomorphism or isomorphism. Images correspond to Aschbacher category, but also others e.g determinant map.
- Kernel K.
- Leaf is "composition factor" of G: simple modulo scalars. Cyclic not necessarily of prime order.

Constructing kernels

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

$$\begin{tikzcd}[column sep=small] & H \arrow[dl, dash] \arrow[dr, dash] & \\ K & & I \end{tikzcd}$$

Sometime easy to obtain theoretically generating sets for $\ker \phi$.
e.g. Smaller Field, Semilinear, normaliser of symplectic-type group.

We could use random method to construct kernel

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

To do so we **need** a presentation for I.

Verifying the outcome

Neunhöffer & Seress (2006): new generating set, Y, on "nice generators" for G.

Want presentation for G on Y.

If Y satisfies presentation, then we have verified tree.

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

So inductively need to know presentations **only for the leaves** – or composition factors.

Short presentations for finite groups

Babai and Szemerédi (1984): *length* of a presentation $P = \{X \mid R\}$ is number of symbols to write down the presentation.

Each generator is single symbol, relator is a string of symbols, exponents written in binary.

Example

S_n generated by $t_k = (k, k+1)$ for $1 \leq k < n$ with relations:

- $t_k^2 = 1$ for $1 \leq k < n$,
- $(t_{k-1} t_k)^3 = 1$ for $1 < k < n$,
- $(t_j t_k)^2 = 1$ for $1 \leq j < k-1 < n-1$.

Number of relations is $n(n-1)/2$, and presentation length is $O(n^2)$.

S_n acts on deleted permutation module: cost of evaluation of relations is $O(n^5)$.
Goal: short presentations on bounded number of relations.

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

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

Exploits results of:

- Campbell, Robertson and Williams (1990): $\mathrm{PSL}(2, p^n)$ has presentation on (at most) 3 generators and a bounded number of relations.
- Hulpke and Seress (2003): $\mathrm{PSU}(3, q)$

Previous best: Babai *et al.* (1997) presentation of length $O(\log^2 |G|)$. Modifications of Curtis-Steinberg-Tits presentations for groups of Lie rank at least 2.

Constructive version (L-G and O'B, ongoing): explicit short presentations for the classical groups on our standard generators. Complete for $\mathrm{SL}, Sp, \mathrm{SU}$.

Short presentations for S_n and A_n

Theorem (GKKL, 2006; Bray-Conder-LG-O'B, 2006)

A_n and S_n have presentations with a bounded number of generators and relations, and length $O(\log n)$.

Theorem (Bray-Conder-LG-O'B, 2006)

Let p be an odd prime, and let λ be a primitive element of $\mathrm{GF(p)}$, with inverse μ. Then

$$\{\, a, c, t \mid a^p, acacac^{-1}, (a^{(p+1)/2}ca^4c)^2, t^2, [t, a],$$
$$[t, ca^{\lambda}ca^{\mu}c], [t, c]^3, (tt^c tt^{ca})^2, (tt^c tt^{ca^{\lambda}})^2, (at^c)^{p+1} \,\}$$

is a 3-generator 10-relator presentation of length $O(\log p)$ for S_{p+2}, in which att^c stands for a $(p+2)$-cycle and t stands for a transposition.

Previous best results: length $O(n \log n)$ (Moore, 1897)

Theorem (GKKL, 2008)

A_n has presentation on 3 generators, 4 relations, length $O(\log n)$.

S_n: presentation of length $O(n^2)$ on $(1,2)$ and $(1,2,\ldots,n)$ and 78 relations.

Problem

Is there a $O(\log n)$ presentation for S_n on $(1,2)$ and $(1,2,\ldots,n)$ with a uniformly bounded number of relators?

Output of CompositionTree

Given $G = \langle X \rangle \leq \mathrm{GL(d, q)}$ as input.
Output:

- a composition series: $1 = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_m = G$.
- A representation $S_k = \langle X_k \rangle$ of G_k/G_{k-1}
- Effective maps $\tau_k : G_k \to S_k$, $\phi_k : S_k \to G_k$
  τ_k epimorphism with kernel G_{k-1}
- Map to write $g \in G$ as word in X.

Construct presentation for group defined by tree and verify that G satisfies the relations.

Characteristic structure

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

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

$O_\infty(G)$ = largest soluble normal subgroup of G, soluble radical

$S^*(G)/O_\infty(G) = \text{Socle}\ (G/O_\infty(G)) = T_1 \times \ldots \times T_k$ where T_i non-abelian simple

$\phi : G \longmapsto \mathrm{Sym}(k)$ is repn of G induced by conjugation on $\{T_1, \ldots, T_k\}$ and $P(G) = \ker\phi$

$P(G)/S^*(G) \leq \mathrm{Out}(T_1) \times \ldots \times \mathrm{Out}(T_k)$ and so is soluble

$G/P(G) \leq \mathrm{Sym}(k)$ where $k \leq \log|G|/\log 60$

Black-box model pioneered by Babai and Beals.

Babai, Beals, Seress (2009):

Theorem

$\mathcal{C}$ can be constructed directly in black-box groups in polynomial time (subject to Discrete Log solution and some other restrictions).

Work with Holt:

- refine composition series obtained from "geometric model" to obtain chief series reflecting this characteristic structure.
- exploit CompositionTree and resulting $\mathcal{C}$ as infrastructure for algorithms to solve "real" problems.

Cannon & Holt: exploit this model in many algorithms e.g. automorphism group, conjugacy classes of subgroups.

From composition series to $\mathcal{C}$?

Work with Derek Holt

$1 = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_m = G$

Computable maps $\tau_k : G_k \to S_k$, $\phi_k : S_k \to G_k$

$S_k = \langle X_k \rangle$ and $W_k = \{g_1, \ldots, g_s\}$, inverse images in G

For $k = 1, 2, \ldots, m$
  For each non-trivial subgroup C in $\mathcal{C}$ do
    For each $g \in W_k$ do
      decide whether there exists $h \in G_{k-1}$ such that $gh \in C$;
      If so, replace g by gh;

Outcome: union of some of the adjusted W_k will generate the three characteristic subgroups of G.

To solve problem for classical groups: constructively test irreducible modules for isomorphism.

Exploiting the characteristic series $\mathcal{C}$

Cannon, Holt et al. (2000s): use $\mathcal{C}$ in practical algorithms.

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

Also compute series

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = L \lhd G$$

where $N_i \trianglelefteq G$ and N_i/N_{i-1} is elementary abelian.
Framework sometimes called **Soluble Radical** model of computation.

The TF-model

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = L \leq S^*(G) \leq P(G) \leq G$$

where $N_i \trianglelefteq G$ and N_i/N_{i-1} is elementary abelian.

Given a **problem**:

Solve problem first in $G/L = G/N_r$, and then, successively, solve it in G/N_i, for $i = r-1, \ldots, 0$.

$H := G/L$ is a TF-group.
So H has a socle S which is direct product of non-abelian simple groups T_i and these are permuted under conjugation by H.

Problem may have nice solution for H.

In many cases, easy to reduce the computation for TF-group H to almost simple groups.

Examples of practical algorithms using TF-model

- Determine conjugacy classes of elements of G; (Cannon & Souvignier, 1997)
- Determine maximal subgroups of G; (Cannon & Holt, 2004) and (Eick & Hulpke, 2001)
- Determine the automorphism group of G; (Cannon & Holt, 2003)
- Determine conjugacy classes of subgroups of G; (Cannon, Cox & Holt, 2001)

Most algorithms are representation-independent.

Implementations use BSGS and Random Schreier for associated computations: so limited in range.

Plan to use CompositionTree for these.

Almost simple groups: Conjugacy classes

Wall (1963): description of conjugacy classes and centralisers of elements of classical groups.

Murray & Haller (ongoing): algorithms, which given d and q, constructs classes for $\mathrm{SX}(d,q) \le K \le \mathrm{CX}(d,q)$.

Constructive recognition: provides $\phi : K \longmapsto \bar{K}$.

Embed TF-group $H = G/L$ in direct product W of $\mathrm{Aut}(T_i) \wr \mathrm{Sym}(d_i)$, where T_i occurs d_i times as socle factor.

Conjugacy class representatives in wreath products described theoretically (Hulpke 2004; Cannon & Holt, 2006).

Example: Automorphism group of G

Cannon & Holt, 2003

$H := G/L$ permutes the direct factors of its socle S by conjugation.

Embed H in direct product D of $\mathrm{Aut}(T_i) \wr \mathrm{Sym}(d_i)$, where T_i occurs d_i times as socle factor of S.

$\mathrm{Aut}(H)$ is normaliser of the image of H in D.

Now lift results through elementary abelian layers, computing $\mathrm{Aut}(G/N_i)$ successively.

Suppose $N \leq M \leq G$, where both M, N char in G and M/N is elementary abelian of order p^d.

$\bullet G$

Suppose $A_M = \mathrm{Aut}(G/M)$ is known.

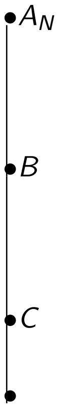
All automorphisms of G fix both M and N.

$\bullet M$

$A_N = \mathrm{Aut}(G/N)$ has normal subgroups $C \leq B$
B induces identity on G/M
C induces identity on both G/M and M/N.

$\bullet N$

M/N is $\mathbb{F}_p(G/M)$-module.



- Elements of C correspond to derivations from G/M to M/N.
- Elements of B/C correspond to module automorphisms of M/N. Can choose M and N to ensure that these tasks "easy".
- Hardest task: determine $S \leq A_M$ which lifts to G/N. $S \leq A'$, subgroup of A_M whose elements preserve the isomorphism type of module M/N.

G/N split extension of M/N by G/M?
If so, all elements of A' lift.
Otherwise, must test each element of A' for lifting.