LMS/EPSRC Course
Computational Group Theory
St Andrews 2013

Permutation Groups 3: Composition Series

Alexander Hulpke
Department of Mathematics
Colorado State University
Fort Collins, CO, 80523, USA
http://www.math.colostate.edu/~hulpke

Towards Structure

A crucial tool on the way towards determining a permutation group's structure is the composition series.

Purposes include:

- Decomposing the group
- As a Tool for other tasks
- Showcase of new class of structural methods
- Verification of stabilizer chains.

Homomorphisms

As a basic tool we want to be able for a permutation group G to either:

- Find a homomorphism φ on G with "*smaller*" image. Or:
- Prove that G is simple.

Natural Source of Homomorphisms: Group Actions, in particular from permutation action.

If G is intransitive on Ω: Action on Orbit

If G is transitive, imprimitive on Ω: Action on blocks. (Find block systems by starting with block seed, Union of images.)

Primitive Groups

Otherwise G is **primitive**. The O'NAN-SCOTT theorem describes the possible structure.

Key component: The *Socle* Soc(G), subgroup generated by all minimal normal subgroups.

Lemma Soc(G) is direct product of minimal normal subgroups.

Proof: Take $M \leq \mathrm{Soc}(G)$, $M \lhd G$ maximal with this property. If $M \neq \mathrm{Soc}(G)$ there exists $N \lhd G$, minimally normal, $N \not< M$. Thus $M \cap N = \langle 1 \rangle$ and $\langle M, N \rangle = M \times N \leq \mathrm{Soc}(G)$ is larger, Contradiction.

Socle of a Primitive Group

Let $N \triangleleft G$ minimal normal.

Remember: Orbits of N are blocks, thus in primitive G we have that N is transitive.

Nontrivial $C_G(N) \triangleleft G$ will be normal, transitive.

Lemma $N \leq S_\Omega$ transitive. Then $C = C_{S_\Omega}(N)$ is *semiregular* (i.e. for all $\omega \in \Omega$: $\mathrm{Stab}_C(\omega) = 1$.)

Proof: Let $c \in \mathrm{Stab}_C(\omega)$, $\delta \in \Omega$. Then there is $g \in N$ such that $\delta = \omega^g = \omega^{(cg)} = \omega^{(gc)} = \delta^c$, thus $c \in \mathrm{Stab}_C(\delta)$ for every δ. Thus $c = 1$.

Socle Structure

Theorem Let G primitive on Ω. $S=\mathrm{Soc}(G)$. Then either

- a) S is minimally normal, *or*
- b) $S=N\times M$ with $N,M\lhd G$ minimal, $N\cong M$ nonabelian.

Proof: If S is not minimally normal then $S=N\times M$, $M\leq C_G(N)$ and $N\leq C_G(M)$. Both groups are transitive, semiregular, thus $|N|=|\Omega|=|M|$, both nonabelian.

For $n\in N$ exists unique $m(n)\in M$ such that $(1^n)^{m(n)}=1$. Then $\varphi: N\to M$, $n\to m(n)$ is isomorphism, as for $k,n\in N$:

$$1^{(k\cdot n\cdot m(k)\cdot m(n))}=1^{k\cdot m(k)\cdot n\cdot m(n)}=((1^k)^{m(k)})^{n\cdot m(n)}=1^{n\cdot m(n)}=1 \qquad \square$$

We thus have that $\mathrm{Soc}(G)\cong T^{\times m}$ with T simple. We say that $\mathrm{Soc}(G)$ is ***homogeneous of type*** T.

Abelian Socle

If S=Soc(G) is abelian, it is an elementary abelian regular normal subgroup.

A point stabilizer U=Stab$_G(\omega)$ intersects trivially with S, thus $G \leq \mathrm{AGL}_n(p)$ is an affine group (linear+translation).

Submodules yield blocks, thus S is irreducible under conjugation by U (or G).

(Finding S requires some work, algorithm exists.)

Vice versa irreducible action of a group U yields primitive group $U \ltimes C_p{}^n$.

Nonabelian Socle

If the Socle $S{=}\mathrm{Soc}(G) \cong T^{\times m}$ is not abelian then $C_G(S){=}\langle 1\rangle$.

The action of G on S thus is faithful. Therefore (up to isomorphism) $G{\leq}\mathrm{Aut}(\mathrm{Soc}(G))$.

T is simple nonabelian, $\mathrm{Aut}(T^{\times m}){=}\mathrm{Aut}(T) \wr S_m$.

The action on the m direct factors of S is a homomorphism with nontrivial kernel.

More detailed description of the possible actions is given by the O'NAN-SCOTT Theorem. (Cf: ASCHBACHER's theorem, → Derek's lectures)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

Product Action: $m=rs$ with $s>1$. $G \leq W=A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n=ds$.

Twisted wreath: S regular and $n=|T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

Product Action: $m=rs$ with $s>1$. $G \leq W=A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n=ds$.

Twisted wreath: S regular and $n=|T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

Product Action: $m=rs$ with $s>1$. $G \leq W=A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n=ds$.

Twisted wreath: S regular and $n=|T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

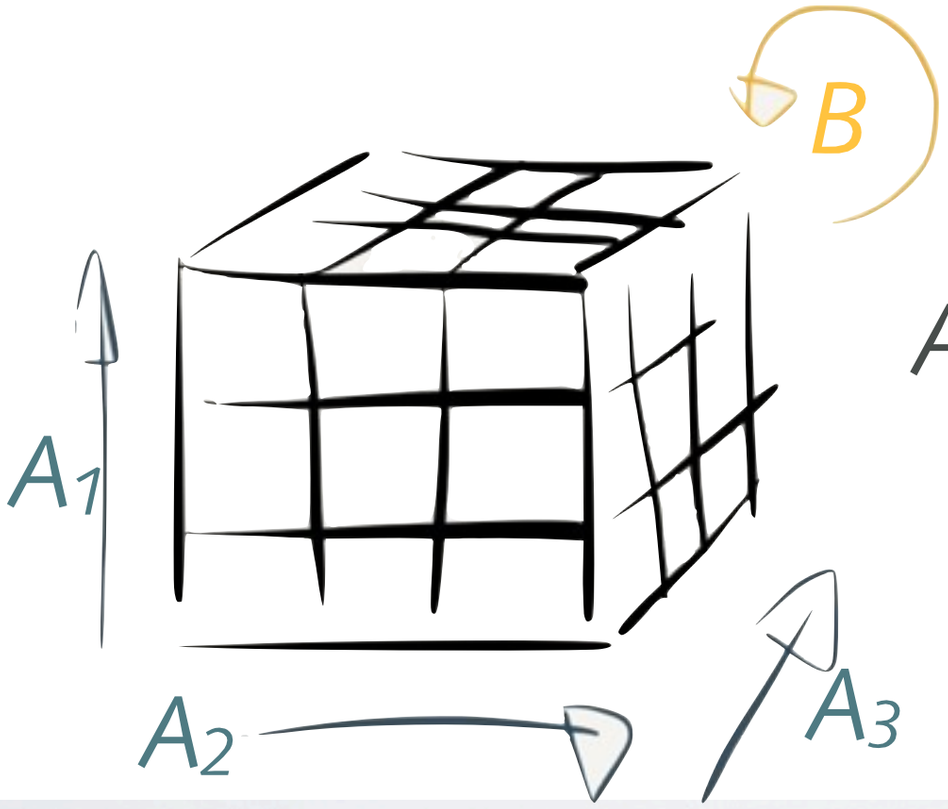
Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

$$\mathrm{Stab}_S(\omega)=\{\ (t,t,\ldots,t) \mid t \in T\ \}$$

isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem



$A \wr B = (A \times A \times \ldots \times A) \rtimes B$

Product Action: $m = rs$ with $s > 1$. $G \leq W = A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n = ds$.

Twisted wreath: S regular and $n = |T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

Product Action: $m=rs$ with $s>1$. $G \leq W=A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n=ds$.

Twisted wreath: S regular and $n=|T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

O'Nan-Scott Theorem

G primitive, $|\Omega|=n$. Let $S=\mathrm{Soc}(G)= T^{\times m}$. Then:

Affine: $G \leq \mathrm{AGL}_n(q)$.

Almost simple: $m=1$ and $H \trianglelefteq G \leq \mathrm{Aut}(S)$.

Diagonal: $m \geq 2$ and $n=|T|^{m-1}$. Further, $G \leq V=(T \wr S_m).\mathrm{Out}(T)$ in diagonal action.

Product Action: $m=rs$ with $s>1$. $G \leq W=A \wr B$ in product action, $A \leq S_d$ primitive, not regular, $B \leq S_s$ transitive. Thus $n=ds$.

Twisted wreath: S regular and $n=|T|^m$. G_ω isomorphic transitive subgroup of S_m. ($n \geq 60^6$.)

Use in Classifications

Reduces to maximal subgroups of simple groups (**C**lassification of **F**inite **S**imple **G**roups).

Information allows for explicit lists:

- ≦50 (Sims, 1970s)
- ≦1000 nonaffine (Dixon & Mortimer, 1989)
- ≦255 affine (Theissen, 1997)
- ≦1000 affine (Roney-Dougal & Unger, 2000)
- $\leqq 3^8$ solvable (Eick & Hoefling, 2004)
- ≦4095 (Roney-Dougal, Quick, Coutts, 2012)

Proof Sketch

[Dixon, Mortimer: Permutation Groups, GTM163]

Assume Socle $S = T \times \ldots \times T$ nonabelian.

S acts transitively. Let $U = \mathrm{Stab}_S(1)$. $\alpha : U \to T_1$

- If U trivial then twisted wreath. Degree $\geqq 60^6$
- If $U^\alpha \neq T$, then $U = U^\alpha \times \ldots \times U^\alpha$, product action.
- Otherwise U is subdirect product (thus direct product) of T's. Consider $V = U \cap \ker \alpha$. If V trivial then diagonal type.
- Otherwise product action of almost simple or diagonal type.

Finding the Socle

To find Soc(G) for a primitive group we use

Schreier's Conjecture: T finite, simple, nonabelian. Then Out(T)=Aut(T)/T is solvable of derived length at most 3. Proof by inspection of all cases (CFSG).

Lemma Let $U \leq G$ be a 2-Sylow subgroup and $N=\langle Z(U)\rangle_G$ (normal closure). Then $S=N'''$.

Proof: As $2 \mid |T|$, U has elements in each copy of T. So $Z(U) \leq \mathrm{Aut}(T)^{\times m}$. As $1 \neq Z(U)$, also $T^{\times m} \leq \langle Z(U)\rangle_G \leq \mathrm{Aut}(T)^{\times m}$. But then the derived series of $\langle Z(U)\rangle_G$ ends in $T^{\times m}$.

Almost Simple Case

In the almost simple case $m=1$ and the action on the socle factors does not give any reduction.

However Out(T) is small and solvable, so it is easy to construct a homomorphism with kernel T.

Remaining case is that of simple group T. In this case use constructive recognition (Effective isomorphism to *natural* copy, → Derek's lectures) to identify T as a simple group.

In many cases order/degree of a primitive group can establish simplicity or identify the isomorphism type if simple.

Composition Series

Given a permutation group G, we search for a homomorphism φ with smaller image if one exists. Recurse to Image and Kernel (if nontrivial).

Pulling the kernels back through previous homomorphisms gives a composition series of G.

We can combine presentations of the simple factors to obtain a presentation of G.

(Respectively, presentations of the images to obtain kernel generators.)

Combining Presentations

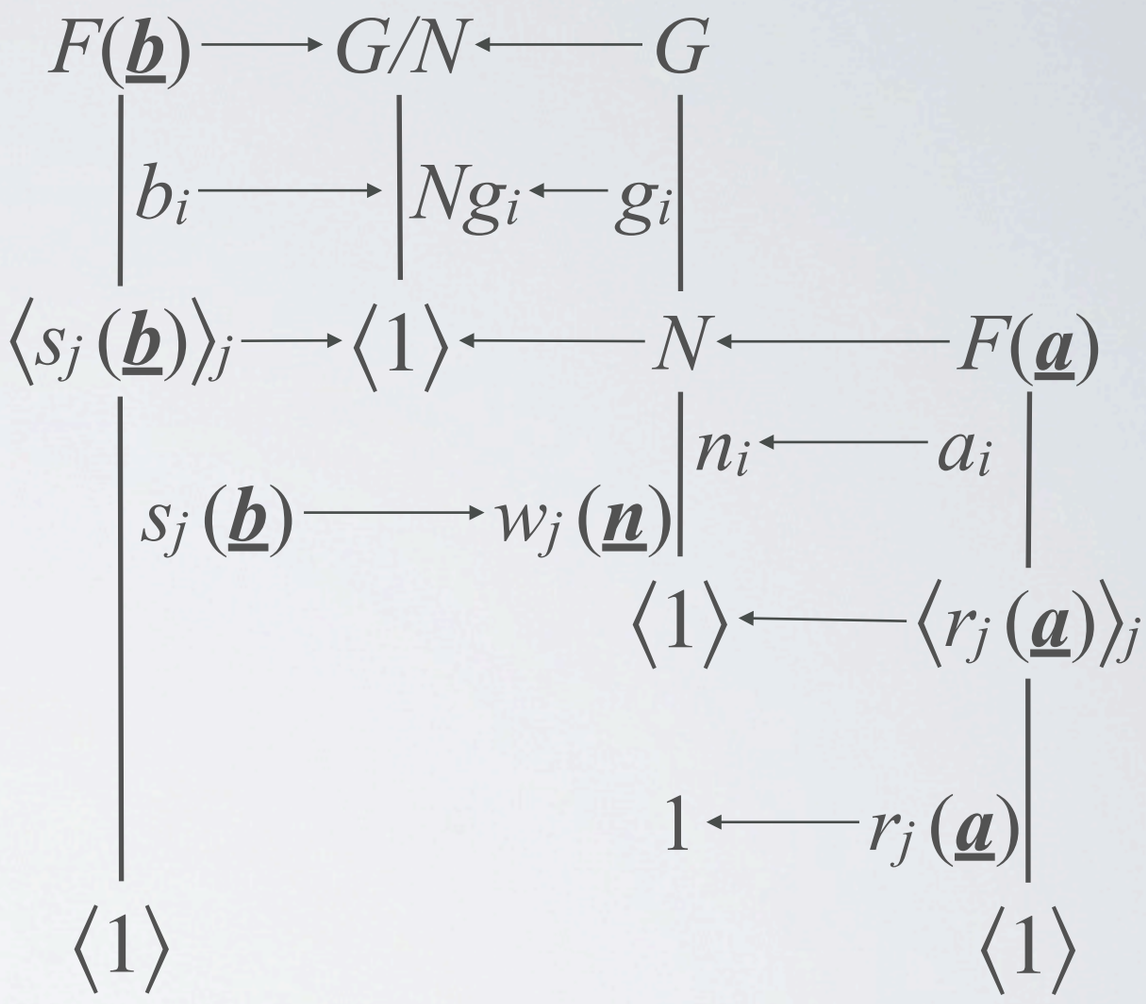
Let $N \triangleleft G$ with presentations

$N \cong \langle a_1,\ldots,a_l \mid r_1(\underline{a}),r_2(\underline{a}),\ldots\rangle$

$G/N \cong \langle b_1,\ldots,b_m \mid s_1(\underline{b}),s_2(\underline{b}),\ldots\rangle$

Let $n_i \in N$ image of a_i in N.

$g_i \in G$, Ng_i image of b_i in G/N.



Find words $v_{i,j}$, w_j such that
$w_j(n_1,\ldots,n_l) = n_i{}^{g_j} \in N$ and
$w_j(n_1,\ldots,n_l) = s_j(g_1,\ldots,g_m) \in N$. Then

$\langle a_1,\ldots,a_l,b_1,\ldots,b_m \mid r_1(a),r_2(a),\ldots,\ s_j(\underline{b}) = w_j(\underline{a}),\ a_i{}^{b_i} = v_i(\underline{a})\rangle$

is a presentation for G.

Proof: Relators define G with normal N, factor G/N.

Verification of Chain

The resulting presentation for G is based on the composition factors recognized.

Back to Random Schreier-Sims:
Composition series, with randomized stabilizer chains for G and factors.

If any randomized calculation failed, the resulting presentation will describe a ***smaller*** group. Detect this by evaluating the presentation on G. Otherwise we know $|G|$.

So we can certify a stabilizer chain for G.

Randomized Algorithms

A *Monte Carlo* algorithm can give wrong result (with selectable probability ϵ),

A *Las Vegas* algorithm, in addition tests for correctness, never returns a wrong result but failure (or unbounded run time) possible.

The randomized stabilizer chain calculation is Monte Carlo. Verification makes it Las Vegas. The only question is run time.

Randomized stabilizer chain is nearly linear $\mathcal{O}(n \log^c n)$. Can one sustain this?

Upgrade to Las Vegas

To maintain good run time for the verification, we need algorithms for

- Homomorphisms for decomposing to primitive factors and for splitting primitive factors.
- Constructive recognition of simple permutation groups.
- Write down a presentation for the simple factors. (Also used in recognition)

To maintain complexity, runtime for simple T must be $\mathcal{O}(\log^c |T|)$. This means presentations must be of length $\mathcal{O}(\log^c |T|)$.

Short Presentations

Such short presentations are known for:

- Cyclic Groups (trivial)
- Sporadic Groups (trivial)
- Alternating Groups (Coxeter, Moser 1972)
- Lie Type of rank >1 (Steinberg 1962, Babai, Goodman, Kantor, Luks, Pálfy, 1997)
- $PSL_2(q)$ (Todd 1936)
- Suzuki groups (Suzuki 1964)
- $PSU_3(q)$ (H., Seress 2001)

Only the Ree groups ${}^2G_2(q)$ remain ...

Permutation Group Recognition

The decomposition of a permutation representation is exactly the analog of matrix group recognition, decomposing with Aschbacher's theorem.

As some reductions of matrix groups reduce to permutation groups, one can really consider this recognition as the *same* process working on permutation groups and matrix groups.

The `recog` package in GAP (NEUNHÖFFER, SERESS) does exactly this.