Computing the socle of small finite permutation groups

Huon Wilson
Supervisor: Prof. J. Cannon (assisted by Dr. W. Unger)

September 18, 2014

The socle

Definition

The socle of a group G, written $\operatorname{soc} G$, is the subgroup generated by its minimal normal subgroups.

Minimal normal subgroups are direct products of isomorphic simple groups. $\operatorname{soc} G$ is a direct product of (some of) the minimal normal subgroups.

Example

Let $G = C_{12}$ generated by g. The normal subgroups are shown. Hence

$$\operatorname{soc} G = \langle g^4 \rangle \langle g^6 \rangle = \langle g^2 \rangle \cong C_3 \times C_2.$$

The socle

Definition

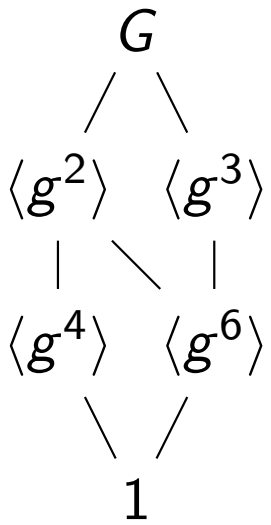
The socle of a group G, written $\operatorname{soc} G$, is the subgroup generated by its minimal normal subgroups.

Minimal normal subgroups are direct products of isomorphic simple groups. $\operatorname{soc} G$ is a direct product of (some of) the minimal normal subgroups.

Example

Let $G = C_{12}$ generated by g. The normal subgroups are shown. Hence

$$\operatorname{soc} G = \langle g^4 \rangle \langle g^6 \rangle = \langle g^2 \rangle \cong C_3 \times C_2.$$



Purpose of the socle

Improves performance for calculating other properties of groups:

- computing chief and composition series. (Cannon and Holt 1997)
- computing automorphism groups. (Cannon and Holt 2003)
- testing isomorphism of two groups. (Cannon and Holt 2003)
- finding conjugacy class representatives. (Cannon and Souvignier 1997)
- enumerating classes of subgroups. (Cannon, Cox, and Holt 2001; Cannon and Holt 2004)

Permutation groups

Definition

A group G is a *permutation group* if it is a subgroup of $\mathrm{Sym}(\Omega)$ for some set Ω. For finite Ω, WLOG a subgroup of S_n for some n.

The *degree* of a permutation group is $|\Omega|$. E.g. the degree of $S_n = n$.

Computational complexity

Why "small" groups?

It is reasonable and still interesting to restrict the degree of groups by some upper bound (e.g. 10^6 or 10^7).

- In computing, slow algorithms have running time $O(a^n)$, for some $a > 1$ and "size" parameter n.
- Fast algorithms are linear $O(n)$ or almost-linear, e.g., $O(n \log n)$.
- The runtime and memory use of many (permutation) group algorithms are exponential or high-degree polynomial in the degree of the input group, so computation in large degree groups is unfeasible.

The algorithm: basic idea

Let G be a finite permutation group on Ω. Due to Cannon and Holt 1997. There are 3 cases, with non-primitive cases reducing to the primitive one:

Intransitive Partition Ω into orbits of G^Ω and pull back the socles of the induced groups.

Imprimitive Find minimal block system(s) and pull back the socle(s) of the induced groups; doing more computation if there is only one minimal block system.

Primitive Decide which case of the O'Nan-Scott theorem G falls into, using the Classification of Finite Simple Groups, and deduce the socle with this information.

Group actions

Definition

A group G is said to *act on* a set Ω if there is a group homomorphism $\varphi : G \longrightarrow \mathrm{Sym}(\Omega)$. For $g \in G$, $\omega \in \Omega$, we write $\omega^g := \varphi(g)(\omega)$.

When considering the action of G on a set Ω we write G^Ω. A permutation group $G \leq \mathrm{Sym}(\Omega)$ has a natural action on Ω.

Let $\omega \in \Omega$. It has

- an *orbit*: $\omega^G := \{\omega^g \mid g \in G\} \subseteq \Omega$
- a *stabiliser*: $G_\omega := \{g \in G \mid \omega^g = \omega\} < G$

G^Ω is *transitive* if there is only one orbit, that is, $\omega_1^G = \omega_2^G$ for all $\omega_1, \omega_2 \in \Omega$.

Group actions

Definition

A group G is said to *act on* a set Ω if there is a group homomorphism $\varphi : G \longrightarrow \mathrm{Sym}(\Omega)$. For $g \in G$, $\omega \in \Omega$, we write $\omega^g := \varphi(g)(\omega)$.

When considering the action of G on a set Ω we write G^Ω. A permutation group $G \leq \mathrm{Sym}(\Omega)$ has a natural action on Ω.

Let $\omega \in \Omega$. It has

- an *orbit*: $\omega^G := \{\omega^g \mid g \in G\} \subseteq \Omega$
- a *stabiliser*: $G_\omega := \{g \in G \mid \omega^g = \omega\} < G$

G^Ω is *transitive* if there is only one orbit, that is, $\omega_1^G = \omega_2^G$ for all $\omega_1, \omega_2 \in \Omega$.

Blocks and block system

Let G^Ω be transitive.

Definition

A *block* is a set $\Delta \subseteq \Omega$ such that either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

The sets $\{\Delta^g \mid g \in G\}$ partition Ω and form a *block system*.

Example

Let $G = C_6 < S_6$ and $\Omega = \{1, \ldots, 6\}$ with the natural action. Block systems:

- $\{\{1\}, \ldots, \{6\}\}$
- $\{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$
- $\{\{1, 3, 5\}, \{2, 4, 6\}\}$
- $\{\{1, \ldots, 6\}\}$

Blocks and block system

Let G^Ω be transitive.

Definition

A *block* is a set $\Delta \subseteq \Omega$ such that either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

The sets $\{\Delta^g \mid g \in G\}$ partition Ω and form a *block system*.

Example

Let $G = C_6 < S_6$ and $\Omega = \{1, \ldots, 6\}$ with the natural action. Block systems:

- $\{\{1\}, \ldots, \{6\}\}$
- $\{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$
- $\{\{1, 3, 5\}, \{2, 4, 6\}\}$
- $\{\{1, \ldots, 6\}\}$

Primitive groups

Definition

G^Ω transitive is said to be *primitive* if the only blocks are trivial, that is, singleton sets and Ω itself.

Example

$G = C_6$, $\Omega = \{1, \ldots, 6\}$ is not primitive: the non-trivial block systems we saw previously.

Example

$G = \mathrm{Sym}(\Omega)$ is primitive: for any set $\Delta \subset \Omega$ with $|\Delta| \geq 2$ find $\delta_1 \in \Delta$, $\delta_2 \notin \Delta$, then $g = (\delta_1 \delta_2) \in G$ has $\Delta^g \cap \Delta \neq \emptyset, \Delta$.

Primitive groups

Definition

G^Ω transitive is said to be *primitive* if the only blocks are trivial, that is, singleton sets and Ω itself.

Example

$G = C_6$, $\Omega = \{1, \ldots, 6\}$ is not primitive: the non-trivial block systems we saw previously.

Example

$G = \mathrm{Sym}(\Omega)$ is primitive: for any set $\Delta \subset \Omega$ with $|\Delta| \geq 2$ find $\delta_1 \in \Delta$, $\delta_2 \notin \Delta$, then $g = (\delta_1 \delta_2) \in G$ has $\Delta^g \cap \Delta \neq \emptyset, \Delta$.

O'Nan-Scott theorem

Theorem

If G^Ω is primitive of degree $n = |\Omega|$, then $N := \operatorname{soc} G \cong S_1 \times \ldots \times S_m$ with $S_i \cong S$ for some simple group S, and either

1. *$S \cong C_p$ is abelian and N regular ($N_\omega = 1$), so N is an "earns".*
2. *S is non-abelian. Let $\mathcal{F} = \{S_1, \ldots, S_m\}$, one of the following holds:*
   - 2.1 *$\Omega = \Omega_1^m$. G^Ω has the wreathed product action. There is a group H such that H^{Ω_1} is primitive and $S \trianglelefteq H$.*
   - 2.2 *$n = |S|^{(a-1)b}$ for some a, b integers with $ab = m$ and $a > 1$, $b \geq 1$. The stabiliser N_ω is a product of "diagonal subgroups".*
   - 2.3 *same as previous with $a = 2$, $b = m/2$, but $G^{\mathcal{F}}$ has two orbits.*
   - 2.4 *$n = |S|^m$, $m \geq 6$, $N_\omega = 1$.*

All cases except 2.3 have G acting transitively by conjugation on $\mathcal{F}$.

O'Nan-Scott theorem

Theorem

If G^Ω is primitive of degree $n = |\Omega|$, then $N := \operatorname{soc} G \cong S_1 \times \ldots \times S_m$ with $S_i \cong S$ for some simple group S, and either

1. *$S \cong C_p$ is abelian and N regular ($N_\omega = 1$), so N is an "earns".*
2. *S is non-abelian. Let $\mathcal{F} = \{S_1, \ldots, S_m\}$, one of the following holds:*
   - 2.1 *$\Omega = \Omega_1^m$. G^Ω has the wreathed product action. There is a group H such that H^{Ω_1} is primitive and $S \trianglelefteq H$.*
   - 2.2 *$n = |S|^{(a-1)b}$ for some a, b integers with $ab = m$ and $a > 1$, $b \geq 1$. The stabiliser N_ω is a product of "diagonal subgroups".*
   - 2.3 *same as previous with $a = 2$, $b = m/2$, but $G^{\mathcal{F}}$ has two orbits.*
   - 2.4 *$n = |S|^m$, $m \geq 6$, $N_\omega = 1$.*

All cases except 2.3 have G acting transitively by conjugation on $\mathcal{F}$.

The algorithm: basic idea

Let G be a finite permutation group on Ω. Due to Cannon and Holt 1997. There are 3 cases, with non-primitive cases reducing to the primitive one:

Intransitive Partition Ω into orbits of G^Ω and pull back the socles of the induced groups.

Imprimitive Find minimal block system(s) and pull back the socle(s) of the induced groups; doing more computation if there is only one minimal block system.

Primitive Decide which case of the O'Nan-Scott theorem G falls into, using the Classification of Finite Simple Groups, and deduce the socle with this information.

The algorithm: basic idea

Let G be a finite permutation group on Ω. Due to Cannon and Holt 1997. There are 3 cases, with non-primitive cases reducing to the primitive one:

Intransitive Partition Ω into orbits of G^Ω and pull back the socles of the induced groups.

Imprimitive Find minimal block system(s) and pull back the socle(s) of the induced groups; doing more computation if there is only one minimal block system.

Primitive Decide which case of the O'Nan-Scott theorem G falls into, using the Classification of Finite Simple Groups, and deduce the socle with this information.

Case 1: Abelian socle factor

- If G has an elementary abelian regular normal subgroup (earns) T, we are in the first case (that is, $S = C_p$ for some prime p) and $\operatorname{soc} G = T$.
- Use ERNIE (Neumann 1987) to check for the existence of (and find) the earns.

Recall case 1: $S \cong C_p$ is abelian and N regular ($N_\omega = 1$), so N is an "earns".

Case 2: Non-abelian socle factor

If there is no earns, $\operatorname{soc} G \cong S^m$ with S non-abelian.
Find the final term T in the derived series of G (the soluble residual), i.e.

$$G \triangleright [G, G] = G_1 \triangleright [G_1, G_1] = G_2 \triangleright \ldots \triangleright [G_k, G_k] = T$$

$\operatorname{soc} G = T$ except for some situations in case 2.1.
Recall: the derived subgroup $[G, G]$ is the subgroup generated by

$$\{[g, h] \mid g \in G, h \in H\} = \left\{g^{-1}h^{-1}gh \,\middle|\, g \in G, h \in H\right\}.$$

Distinguishing $T \neq \operatorname{soc} G$

$T \neq \operatorname{soc} G$ happens exactly when there is t, m, u, s, n_1 such that $m \geq 5$, $|T| = tus^m$ and $n = n_1^m$ where

- $n_1 = |\Omega_1|$ for some set Ω_1
- $s = |S|$ for some non-abelian simple group S that acts primitively on Ω_1 (this S is the socle factor)
- u is the order of a transitive group K of degree m that is perfect ($[K, K] = K$)
- t divides $|\operatorname{Aut}(S)/S|^m$

Recall case 2.1: $\Omega = \Omega_1^m$. G^Ω has the wreathed product action. There is a group H such that H^{Ω_1} is primitive and $S \trianglelefteq H$.

Handling $T \neq \operatorname{soc} G$

If we have $T \neq \operatorname{soc} G$, then

- Take $\omega \in \Omega$, and find a shortest orbit Δ of G_ω on $\Omega \setminus \{\omega\}$.
- Find a block system Σ for G_ω^Δ such that G_ω^Σ is primitive.
- $\operatorname{soc} G$ is the normal closure in G of $[U, U]$, where U is the stabiliser $G_{\omega,\Delta\setminus\sigma}$ for any $\sigma \in \Sigma$.

Computing the socle factors

The (non-abelian) socle factors $S_1, \ldots, S_m$ are also of interest. In most cases, they are conjugate, so: find one, find them all.

- When $T \neq \operatorname{soc} G$, S_1 is the normal closure of $[U, U]$ ($U = G_{\omega, \Delta \setminus \sigma}$) in $\operatorname{soc} G$
- When $T = \operatorname{soc} G$, either $\operatorname{soc} G$:
  - is imprimitive: examine the kernel K of the action of $\operatorname{soc} G$ on a minimal block system. If $n \neq s^{m/2}$, then $S_1 = K$, otherwise pull back from factors of K^σ.
  - has two factors ($m = 2$): just search for two distinct normal closures.