Computational Group Theory

Soria Summer School 2009
Session 2: Permutation groups

Technische Universiteit
Eindhoven
University of Technology

July 2009, Hans Sterk (sterk@win.tue.nl)

Where innovation starts

Permutation groups

- Permutation groups
- Schreier trees
- Schreier-Sims
- Applications

Technische Universiteit Eindhoven University of Technology

Permutation groups

- $\mathrm{Sym}(\Omega)$: **symmetric group** of permutations of set Ω
  - Special case: S_n if $\Omega = \{1, 2, \ldots, n\}$
- **Composition:** is read from left to right:

$$(1,2)(2,3) = (1,3,2)$$

  (and not $(1,2,3)$)

- **Permutation representation** of G: homomorphism $G \longrightarrow \mathrm{Sym}(\Omega)$. Each element $g \in G$ acts on Ω; notation ω^g. The **degree** of the representation is $|\Omega|$.
- **Permutation group:** subgroup of some $\mathrm{Sym}(\Omega)$

Interesting situations arise when Ω has some extra structure, examples:

- (the graph on the vertices of a) tetrahedron, cube,...
- A vector space $\mathbf{Z}_p^n$

Every group is a permutation group

For each $g \in G$ define $R_g : G \longrightarrow G$ by

$$h \mapsto hg$$

This is a bijection. Define

$$G \longrightarrow \mathrm{Sym}(G), \quad g \mapsto R_g$$

- Homomorphism: $R_h * R_k$ acts on g like R_{hk}:

$$(gh)k = g(hk)$$

- Injective: test R_h and R_k on e to find h and k.

So we find:

Theorem: Every group is a permutation group

Useful...

Permutation groups: orbits and stabilizers

G acts on Ω.

- **G-orbit of $\omega \in \Omega$:**

$$\omega^G = \{\omega^g \mid g \in G\}$$

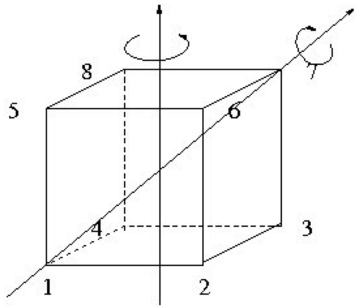
  - Orbits partition Ω; 'being in the same orbit' is an equivalence relation
  - **Transitive action:** $\omega^G = \Omega$
  - **t-transitive action:** if $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ are t-tuples of distinct elements, then there exists a $g \in G$ with $x_i^g = y_i$ for every i.
  - **Examples:** symmetries of the cube, S_n, A_n
- **Stabilizer of $\omega \in \Omega$:**

$$G_\omega = \{g \in G \mid \omega^g = \omega\}$$

  - subgroup of G
  - There is a relation between the cardinalities of G, G_ω and ω^G...

TU/e Technische Universiteit Eindhoven University of Technology

Orbits: examples



Cube with labels $1, \ldots, 8$.

- Rotation around z-axis: $s = (1,2,3,4)(5,6,7,8)$
- Rotation around diagonal: $t = (2,5,4)(3,6,8)$
- Orbit of 1: ....
- Group $\langle s, t\rangle$ transitive? And 2-transitive?
- Order of $\langle s, t\rangle$?
- Order of $\langle s, (2,3,7,6)(1,4,8,5)\rangle$?
- Order of $\langle s, (1,2)(3,4)(5,6)(7,8)\rangle$
- What is the whole group of symmetries?

Orbits, stabilizers: relating their cardinalities

If G acts on Ω, then:

a)

$$|G|/|G_\omega| = |\omega^G|$$

b) In particular, if G acts transitively:

$$|G|/|G_\omega| = |\Omega|$$

Proof: G acts on ω^G, hence we have

$$f : G \to \omega^G, \quad g \mapsto \omega^g$$

- f is surjective
- $$f(g) = f(h) \Leftrightarrow \omega^g = \omega^h \Leftrightarrow \omega^{hg^{-1}} = \omega \Leftrightarrow hg^{-1} \in G_\omega \Leftrightarrow G_\omega g = G_\omega h$$

  So every preimage has cardinality $|G_\omega|$, and the formulas follow.

Note that f induces a bijection between ω^G and the right cosets $G_\omega \backslash G$.

Technische Universiteit Eindhoven University of Technology

Orbits and stabilizers: Lagrange's theorem

In the same vein:

if $H < G$ is a subgroup, then G acts transitively on the right cosets $H\backslash G$ by right multiplication via:

$$Hh \mapsto Hhg$$

This induces a morphism

$$G \longrightarrow \mathrm{Sym}(H\backslash G)$$

The stabilizer of the coset H is the subgroup H itself, and the orbit of H is $H\backslash G$, so that we find:

Lagrange's theorem:

$$|G|/|H| = |H\backslash G|$$

In particular:

- $|H|$ divides $|G|$,
- the order of any element divides $|G|$.

Technische Universiteit Eindhoven University of Technology

More on stabilizers and orbits

G acts on Ω:

- ω^G: the G-orbit of ω
- G_ω: the G-stabilizer of ω
- Ω_g: The fixed point set of g

$$\Omega_g = \{\omega \in \Omega \mid \omega^g = \omega\}$$

Cauchy-Frobenius lemma: If the finite group G acts on the finite set Ω, then the number of orbits equals

$$\frac{1}{|G|} \sum_{g \in G} |\Omega_g|$$

Proof: Exercise, but note that

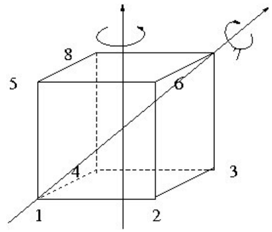
$$\sum_{\omega \in \Omega} \frac{1}{|\omega^G|}$$

is the total number of orbits.

Technische Universiteit Eindhoven University of Technology

Computing orders: strategy and example

Strategy: use repeatedly the orbit-stabilizer formula: $|G| = |G_\omega| \cdot |\omega^G|$



- The symmetry group obviously acts transitively, hence

$$|G| = 8 \cdot |G_1|$$

- Use $(2,5,4)(3,6,8)$ to see that the G_1-orbit of 2 contains precisely 3 elements. So

$$|G| = 8 \cdot 3 \cdot |G_{1,2}|$$

- The 'reflection' $(4,5)(3,6)$ shows: the $G_{1,2}$-orbit of 3 contains precisely 2 elements. Hence

$$|G| = 8 \cdot 3 \cdot 2 \cdot |G_{1,2,3}|$$

- Since $G_{1,2,3}$ is trivial: $|G| = 48$.

Exercise: The symmetry group of the cube also acts on the 6 faces. Do the computation with the permutations of the faces.

Computing orders: further examples

- **The icosahedron:** (20 faces, 12 vertices):

$$12 \cdot 5 \cdot 2 = 120$$

  12 vertices, 5 vertices at distance 1 from vertex 1, and a reflection leaving two neighbouring vertices fixed.

- **The cube:** The symmetry group also acts transitively on the 6 faces. Fixing 1 face, there is still an orbit of length 4. Fixing 2 neighbouring faces, there is still an orbit of length 2, so

$$6 \cdot 4 \cdot 2 = 48$$

- **The cube:** The symmetry group acts transitively on the 4 main diagonals:

$$4 \cdot 3 \cdot 2 = 24?$$

  What's going on?

Technische Universiteit Eindhoven University of Technology

Computing orbits

$G = \langle X \rangle$, generator set X. Computing the orbit of ω can be done as follows:

1) **orbit-to-be:=**$\{\omega\}$
2) Have each element of X act on ω; put elements $\neq \omega$ in a set **new**.
3) Update **orbit-to-be** by taking the union with **new**
4) Have each element of X act on **new**. Update, if necessary, **new** by putting in the elements found at this stage, but not yet in **orbit-to-be**.
5) Go back to 3),and continue.

Example $G = \langle a = (1,2,3,4)(5,6,7,8), b = (2,5,4)(3,6,8) \rangle$, orbit of 1

- Action of generators: $1^a = 2$ and $1^b = 1$ yielding: **new** $= \{2\}$ and **orbit-to-be** $= \{1,2\}$
- Action of generators: $2^a = 3$, $2^b = 5$ yielding: **new** $= \{3,5\}$ and **orbit-to-be** $= \{1,2,3,5\}$
- Action of generators: $3^a = 4$, $3^b = 6$, $5^a = 6$, $5^b = 4$, yielding

  new $= \{4,6,\}$ and **orbit-to-be** $= \{1,2,3,4,5,6\}$

- Action of generators: $4^a = 1$, $4^b = 2$, $6^a = 7$, $6^b = 8$ yielding

  new $= \{7,8\}$ and **orbit-to-be** $= \{1,2,3,4,5,6,7,8\}$

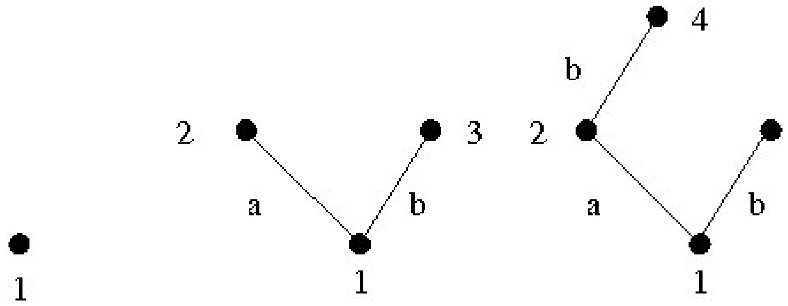
Schreier trees

Given: $G \leq \mathrm{Sym}(\Omega)$, $G = \langle X \rangle$, $\alpha \in \Omega$.

A **Schreier tree** with root α for X is a tree rooted at α and with edges labelled by the elements of X s.t.

- **Vertices:** α^G
- **Labelled edges:** For each edge i, j with i closer to α than j there is a $g \in X$ s.t. $i^g = j$. Notation for the edge: $[i, g, j]$.

Example: $G = \langle a = (1,2)(3,4), b = (1,3)(2,4) \rangle$, root 1.



Schreier trees can be constructed as suggested.

Schreier trees: how to use them

For $\omega \in \alpha^G$, a vertex in the tree

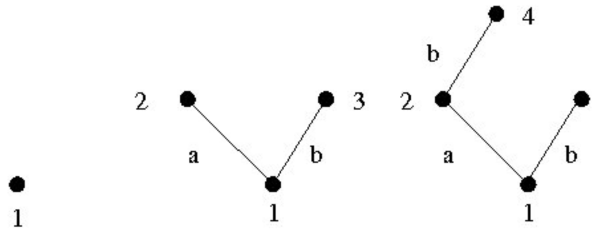
- follow the path/edges down the tree until α is reached:

$$g_1, g_2, \ldots, g_k$$

- Then

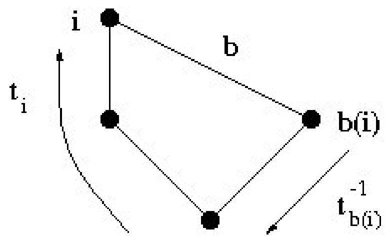
$$\omega = \alpha^{g_k g_{k-1} \cdots g_1}$$

- This yields a permutation $t_\omega = g_k g_{k-1} \cdots g_1$, expressed as a product of generators, mapping α to ω.



From the picture we see that $1^{ab} = 4$.

Schreier trees and stabilizers (1)



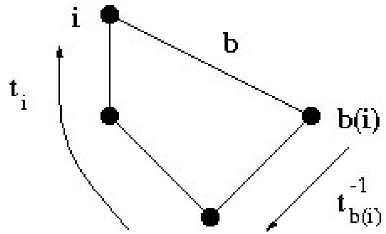
Elements of G_α can be constructed as follows.

- Take $i \in \alpha^G$, a vertex, and $b \in X$
- Then i^b is a vertex
- From the Schreier tree we find

$$t_i \quad \text{and} \quad t_{i^b}$$

- Then $t_i b t_{i^b}^{-1}$ is an interesting element.

Schreier trees and stabilizers (2)



What does $t_i b t_{i^b}^{-1}$ do?

- t_i takes α to i
- then b takes i to i^b
- and $t_{i^b}^{-1}$ takes i^b back to α

So $t_i b t_{i^b}^{-1}$ is an obvious element of G_α. An element of this form is called a **Schreier generator.**

Theorem (Schreier's lemma):

$$G_\alpha = \langle t_i b t_{i^b}^{-1} \mid i \in \alpha^G, \, b \in X \rangle$$

Schreier's lemma: proof

$$G_\alpha = \langle t_i b t_{i^b}^{-1} \mid i \in \alpha^G, \, b \in X \rangle$$

Proof (of $\subseteq$):

- $g = b_1 \cdots b_r \in G_\alpha$
- j maximal s.t. $\alpha, \alpha^{b_1}, \ldots, \alpha^{b_1 \cdots b_j}$ is path in Schreier tree. Then $j < r$.
- Let $\beta = \alpha^{b_1 \cdots b_j}$ and take the Schreier generator

$$t_\beta b_{j+1} t_{\beta^b}^{-1}$$

- Replace g by

$$(t_\beta b_{j+1} t_{\beta^b}^{-1})^{-1} g = t_{\beta^b} b_{j+2} \cdots b_r$$

- Do the same thing with this product: in the next step at least b_{j+2} is absorbed into a Schreier generator, etc.

Schreier trees: finding stabilizers and orders

Here is the 'algorithm' it leads to:

- Start with the empty set **stabilizer-to-be**
- For every $b \in X$ and vertex $i \in \alpha^G$ check if

$$[i, b, i^b]$$

  is an edge
- If not, add $t_i b t_{i^b}^{-1}$ to **stabilizer-to-be**
- In the end **stabilizer-to-be** is a generating set for G_α

TU/e Technische Universiteit Eindhoven University of Technology

Some remarks

- **Decreasing the number of generators:** G^i is the pointwise stabilizer of $\{1, \dots, i\}$.
  - Work step by step through the following:
  - If $g, h \in X \cap G^{i-1}$ with $i^g = i^h \neq i$, replace X by

$$(X \setminus \{h\}) \cup \{gh^{-1}\}$$

    (possibly remove 'trivialities'). After this step all elements in $X \cap G^{i-1}$ but not in G^i act differently on i.

- G is still generated by the output X.
- The number of generators is at most

$$\sum_{i=1}^{n-1}(n-i) = \binom{n}{2}$$

Technische Universiteit Eindhoven University of Technology

Schreier trees: order and membership

Orders: Stabilizers can be used to compute orders of permutation groups. Let G act on $\Omega = \{1, 2, \ldots, n\}$.

- First we compute

$$G_1 \quad \text{and} \quad G\text{-orbit of } 1$$

  since $|G| = |G_1| \cdot |G\text{-orbit of } 1|$

- If G_1 is not trivial, compute the G_1-orbit of 2 and $|(G_1)_2|$, etc.

Membership: A trivial variation can be used to test membership of an element:

- For a subgroup G of S_n and an element $g \in G$, compare

$$|G| \quad \text{and} \quad |\langle G, g\rangle|$$

There are more efficient ways of testing membership.

Technische Universiteit Eindhoven University of Technology

Schreier trees: (normal) subgroups

Subgroup: $G = \langle X \rangle < S_n$, $H = \langle Y \rangle < S_n$.

- To test if $H < G$: test memberschip of G for every element $y \in Y$

Normal subgroup: In addition:

- Test membership of H for every $x^{-1}yx$, with $y \in Y$ and $x \in X$.

TU/e Technische Universiteit Eindhoven University of Technology

Bases and strong generating sets

- **Base** B **for** G**:** $B = [b_1, \ldots, b_k]$ **of elements in** Ω **s.t.**

$$G_{b_1,\ldots,b_k} = \{1\}$$

- **Stabilizer chain wrt** B**:**

$$G \geq G_{b_1} \geq G_{b_1,b_2} \geq \cdots G_{b_1,\ldots,b_k} = \{1\}$$

- **Strong generating set for** G **(wrt** B**):** a generating set X s.t. every $G_{b_1,\ldots,b_i}$ is generated by

$$G_{b_1,\ldots,b_i} \cap X$$

The algorithm described before can be upgraded to produce a base and a corresponding strong generating set. Usually, this is done with the **Schreier-Sims algorithm**

Technische Universiteit Eindhoven University of Technology

Computing bases and strong generating sets

The algorithm described earlier allows to compute bases and (strong) generating sets for the group G.

- Start with $B = [1, 2, \ldots, n]$
- Compute generators of the various stabilizers G_1, $G_{1,2}$, etc.
- Adapt B if necessary
- Join the generators to obtain generators of G.

Schreier-Sims is basically the above algorithm, but with avoidance of redundant generators.

Technische Universiteit Eindhoven University of Technology

Writing elements as words in the generators

- **Ingredients:**
  - Base $B = [b_1, \ldots, b_k]$,
  - Stabilizer chain $G^0 \geq G^1 \cdots$
  - Strong generating set X
- **Schreier trees:** $G^{i+1} \backslash G^i \sim b_{i+1}^{G^i}$; describe the action of G^i on the cosets of G^{i+1} by a Schreier-tree T_{i+1}.
- **Sifting:** expresses a g in terms of X or shows $g \notin G$

1) g fixes $b_1, \ldots, b_k$:
   If $g = 1$, then $g \in G$, else $g \notin G$
2) g fixes $b_1, \ldots, b_i$, but moves b_{i+1}:
   If $b_{i+1}^g \notin b_{i+1}^{G^i}$, then $g \notin G$, else use a Schreier tree to find

$$b_{i+1}^g = b_{i+1}^{s_1 \cdots s_r}$$

   with $s_1, \ldots, s_r \in X \cap G^i$. Then $g(s_1 \cdots s_r)^{-1}$ fixes $b_1, \ldots, b_{i+1}$.

  - Etc.

Some exercises

1) Finish the proof of the Cauchy-Frobenius lemma.
2) Compute the order of the symmetry groups of the five regular polyhedra.
3) Construct Schreier trees for a group of your choice and find generators of some stabilizers.

Technische Universiteit Eindhoven University of Technology