Computational Group Theory

Soria Summer School 2009
Session 3: Coset enumeration

Technische Universiteit **Eindhoven** University of Technology

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

Where innovation starts

Coset enumeration: contents

- What is coset enumeration about?
- The set-up for coset enumeration
  - Subgroup tables
  - Relator tables
  - Coset table
- How to fill the tables
- Examples
- Theorem on coset enumeration

Technische Universiteit Eindhoven University of Technology

What is coset enumeration?

Given group G given by generators and relators, like $\langle x, y \mid x^2, y^2, (xy)^3 \rangle$

- **Coset enumeration:** a procedure to obtain the permutation representation of G on the set of cosets of a subgroup of finite index, so a morphism

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

- **Todd-Coxeter** coset enumeration: is what we discuss here; named after Todd and Coxeter.

Technische Universiteit **Eindhoven** University of Technology

Coset enumeration: basic set-up

- **Start:**
  - G: group given by generators (X) and relators (R);
  - H: subgroup $\langle Y \rangle$; each element of Y is expression in generators of X
- **Intermediate process:** construction of various tables
- **Output:** a table containing the (right) cosets and the action of the generators on the right cosets

Example:

coset	x	y
1	1	2
2	3	1
3	2	3

Here, H is labeled by 1, and there are two more cosets:

$$Hy \quad \text{and} \quad Hyx$$

The table describes a permutation representation of G into S_3, with x mapped to $(2,3)$ and y mapped to $(1,2)$.

Technische Universiteit Eindhoven University of Technology

Presentations of groups: some basics

$G = \langle x, y \mid x^2, y^2, (xy)^3 \rangle$ means

- Group elements are 'words' in x, x^{-1}, y, y^{-1}, like

$$xy^{-1}x^3$$

- The relators tell you which words represent e:

$$xy^{-1}x^3 = xy^{-1}x$$

  since $x^2 = e$

Formally: quotient of the free group on x and y by the normal closure of the subgroup generated by x^2, y^2, $(xy)^3$

Technische Universiteit Eindhoven University of Technology

Free groups (1)

- **Free group:**
  Group F is free on its subset X if every map

$$\phi : X \to \Gamma$$

  into a group Γ extends in a unique way to a morphism

$$\Phi : F \to \Gamma$$

- **Fact:**
  Free groups F_1 on X_1 and F_2 on X_2 are isomorphic iff $|X_1| = |X_2|$.
- **Construction:**
  Free groups can also be constructed explicitly

Free groups (2): outline of construction

- Set of symbols X: a (finite) set of symbols
  - X^{-1}: the set of symbols x^{-1} where $x \in X$
  - A_X or A: $X \cup X^{-1}$
- Strings or words:

$$x_1 x_2 \cdots x_r$$

with each $x_i \in A$. Empty string: e. Words can be concatenated.

- Equivalence relation on words:
  - Direct equivalence of v and w: if one can be obtained from the other by insertion or deletion of a subword $x\,x^{-1}$ for $x \in A$
  - $v \sim w$: equivalence relation generated by direct equivalence, so if there is a sequence

$$v = v_0, v_1, \ldots, v_r = w$$

s.t. v_i and v_{i+1} are directly equivalent.

- Candidate free group F_X: equivalence classes $[v]$ with multiplication

$$[u]\,[v] = [uv]$$

Technische Universiteit Eindhoven University of Technology

Free groups (3): construction

Theorem:

- F_X is free group on $[X] = \{[x] \mid x \in X\}$
- The map $X \to [X]$, $x \mapsto [x]$ is bijective

Idea of proof

- Given a map $\phi : X \to \Gamma$ into group Γ, extend to F_X:

$$\Phi([x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r}]) = \phi(x_1)^{s_1} \phi(x_2)^{s_2} \cdots \phi(x_r)^{s_r}$$

  Show that it is well-defined and unique.

- Then deal with a given map $[X] \to \Gamma$.
- $X \to [X]$ is bijective: Take an injective map $X \to \Gamma$ and apply the above

Technische Universiteit Eindhoven University of Technology

Group presentations

$G = \langle X \mid R \rangle$ is defined as

$$F_X / N$$

where N is the normal closure of $\langle R \rangle$.

Universal property:
Given:

- any map $\phi : X \to \Gamma$ into group Γ, with obvious extension to $A = X \cup X^{-1}$
- $\phi(x_1) \cdots \phi(x_r) = e_\Gamma$ for all $x_1 \cdots x_r \in R$

Then there is a unique morphism

$$\Phi : G \to \Gamma$$

extending ϕ

Coset enumeration: basic set-up (ctd)

- $G = \langle X \mid R \rangle$
- $H = \langle Y \rangle$ where Y consists of words in X

Todd-Coxeter enumeration is based on (here cosets are labeled by integers):

- **TC-1:** $1^h = 1$ for every $h \in Y$
- **TC-2:** $j^r = j$ for every coset j and every relator $r \in R$
- **TC-3:** $i^g = j \Leftrightarrow i = j^{g^{-1}}$ for all cosets i, j and $g \in X$

Coset enumeration: various tables

In the process 3 kinds of tables are produced:

- **Subgroup tables:** is made for every generator of the subgroup. Every such table contains information on
  - the specific generator of the subgroup, expressed in terms of the generators of the group
  - the action of the various factors on the subgroup
- **Relator tables:** for every relator a table is constructed containing information on
  - the specific relator expressed in terms of the generators of the group
  - the action of the various factors of the relator on the subgroup
- **Coset table:** contains (in the end) all cosets plus the action of the generators of H on the cosets of H

The tables are gradually filled in the process. During the process it may turn out that two possibly different cosets actually coincide.

Subgroup tables

For every generator $h = g_{j_1} \cdots g_{j_l}$ in Y of H, with $g_{j_i} \in X \cup X^{-1}$ a table with one row is constructed

- The $l+1$ columns are indexed by 'subgroup' and the elements $g_{j_1}, \ldots, g_{j_l}$
- A row of length $l+1$, starting and ending with 1 representing coset H
  - 2nd column: integer representing coset Hg_{j_1}
  - 3rd column: integer representing coset $Hg_{j_1}g_{j_2}$
  - etc.

  Integers have to be found out during the process.

Example of a partially filled subgroup table for a generator x^2:

subgroup	x	x^2
1	2	1

Relator tables

For every relator $r = g_{i_1} \cdots g_{i_k} \in R$, with $g_{i_j} \in X \cup X^{-1}$, a *relation table* with $k+1$ columns is constructed:

- The $k+1$ columns are indexed by 'relator', $g_{i_1} \ldots g_{i_k}$
- each row starts and ends with the same integer (representing a coset).
- The row starting with integer t is filled with the images of the coset corresponding to this integer under g_{i_1}, $g_{i_1}g_{i_2}, \ldots, g_{i_1} \cdots g_{i_k}$
- The number of rows is determined during the process

Example of a partially filled relator table for a relator $(xy)^3$:

relator	x	y	x	y	x	y
1	1	2	3	4	5	1
2	3	4	5	1	1	2
3						3
4						4
5						5

the last k of which are indexed by $g_{i_1}, \ldots, g_{i_k}$.

Coset table

The coset table records (at the end of the process) the permutation representation.

- The coset table has $|X| + 1$ columns
- The columns are indexed by 'coset', and the generators in X
- The first column contains the (integers representing the) cosets
- The g-th entry of row k contains k^g

coset	x	y
1	1	2
2	3	1
3	2	3

Sometimes columns for X^{-1} are added

TU/e Technische Universiteit Eindhoven University of Technology

How to fill the tables?

- We fill the subgroup and relator tables so that
  - if H'' is in the column indexed by g and H' is in the column directly left from g, then $H'g = H''$.
  - It is sometimes convenient to read this as $H' = H''g^{-1}$.
- Update the coset table whenever necessary
  - In particular, if an entry m^g is not (yet) one of the known cosets, we fill it with a new number s, and add a row starting with s to the relator tables and the coset table.
  - Similar action is taken for a spot corresponding to $m^{g^{-1}}$
- Scan for 'coincidences': two integers turn out to represent the same coset.

Time for an example...

Technische Universiteit Eindhoven University of Technology

Coset enumeration: example 1

Group G and subgroup H:

- $G = \langle x, y \mid x^2, y^2, (xy)^3 \rangle$, so

$$X = \{x, y\} \quad \text{and} \quad R = \{x^2, y^2, (xy)^3\}$$

- $H = \langle x \rangle$, so $Y = \{x\}$

There is one subgroup table, it corresponds to $Hx = H$:

subgroup	x
1	1

There are 3 relator tables, and 1 coset table:

	x	x
1	1	1
2		2
3		3
4		4
5		5

	y	y
1	2	1
2		2
3		3
4		4
5		5

	x	y	x	y	x	y
1	1	2	3	4	5	1
2						2
3						3
4						4
5						5

coset	x	y
1	1	2
2	3	
3		4
4	5	
5		1

First rows are filled plus the coset table so far.

Coset enumeration: example 1 (2)

	x	x
1	1	1
2	**3**	2
3		3
4	**5**	4
5		5

	y	y
1	2	1
2	**1**	2
3	**4**	3
4		4
5	**1**	5

	x	y	x	y	x	y
1	1	2	3	4	5	1
2	**3**	**4**	**5**	**1**	**1**	2
3						3
4						4
5						5

coset	x	y
1	1	2
2	3	
3		4
4	5	

At this point:

- $2^y = 1$ (2nd relator table) and $5^y = 1$ (3rd relator table), so '$2 = 5$', so we remove row 5
- From the 1st relator table:
  - $2^x = 3$
  - $5^x = 4$

  Since '$2 = 5$' we conclude '$3 = 4$' and get another collapse.

We are left with:

	x	x
1	1	1
2	3	2
3	**2**	3

	y	y
1	2	1
2	1	2
3	4	3

	x	y	x	y	x	y
1	1	2	3	4	5	1
2	3	4	5	1	1	2
3	**2**	**1**	**1**	**2**	**3**	3

coset	x	y
1	1	2
2	3	**1**
3	**2**	4

Coset enumeration: example 1 (finish)

The final coset table

coset	x	y
1	1	2
2	3	1
3	2	4

yields a permutation representation of G into S_3 with

$$x \mapsto (2,3) \quad \text{and} \quad y \mapsto (1,2)$$

Since

- H is of index 3
- H has order ≤ 2, so G has order ≤ 6

our representation is an isomorphism

Same example in GAP


```
F:=FreeGroup("x","y"); %free group on x and y
x:=F.x;
y:=F.y;
rels:=[x^2,y^2,(x*y)^3];
G:=F/rels;
gens:=GeneratorsOfGroup(G);
xG:=gens[1];
yG:=gens[2];
H:=Subgroup(G,[xG]);
ct:=CosetTable(G,H);
# g1, g1^-1, g2, ...
Display(TransposedMat(ct));
[ [ 1, 1, 2, 2 ],
  [ 3, 3, 1, 1 ],
  [ 2, 2, 3, 3 ] ]
# g1, g2, ...
Display(TransposedMat(ct{[1,3..3]}));
[ [ 1, 2],
  [ 3, 1 ],
  [ 2, 3 ] ]
```


Technische Universiteit Eindhoven University of Technology

Coset enumeration: another example

$$G = \langle a, b \mid baba^{-2}, abab^{-2} \rangle$$

```
F:=FreeGroup("a","b"); %<free group on the generators [ a, b ]>
a:=F.a; %a
b:=F.b; %b
rels:=[b*a*b*a^-1*a^-1,a*b*a*b^-1*b^-1]; %[ b*a*b*a^-2, a*b*a*b^-2 ]
G:=F/rels; %<fp group on the generators [ a, b ]>
gens:=GeneratorsOfGroup(G); %[ a, b ]
aG:=gens[1]; %a
bG:=gens[2]; %b
H:=Subgroup(G,[aG*aG]); %Group([ a^2 ])
ct:=CosetTable(G,H);
[ [ 2, 1, 4, 8, 6, 7, 3, 5 ], [ 2, 1, 7, 3, 8, 5, 6, 4 ],
  [ 3, 5, 6, 1, 4, 2, 8, 7 ], [ 4, 6, 1, 5, 2, 3, 8, 7 ] ]
Display(TransposedMat(ct{[1,3..3]}));
[ [  2,  3 ],
  [  1,  5 ],
  [  4,  6 ],
  [  8,  1 ],
  [  6,  4 ],
  [  7,  2 ],
  [  3,  8 ],
  [  5,  7 ] ]
```

Left column: action of a; right column: action of b. Image has order 24.

Technische Universiteit Eindhoven University of Technology

Theorem on Todd-Coxeter enumeration

Theorem:
Given: H of finite index in G. Any Todd-Coxeter enumeration in which

a) each row is completely filled (or deleted) in finitely many steps

b) there are only finitely many steps between two scannings of the tables for coincidences,

will terminate.

Proof: The basic idea is to show that if the procedure does not terminate, the number of rows increases beyond any bound, yielding a transitive permutation action on an infinite set with H in the stabilizer, contradicting that H has finite index in G.

Technische Universiteit Eindhoven University of Technology

Sketch proof: step 1

Step 1: first rows of any table are stable after finitely many steps

- After finitely many steps all entries are filled.
- The first entry, 1, is 'stable', and the other entries can only change into smaller positive integers
- So the first rows remain stable after finitely many steps

Technische Universiteit Eindhoven University of Technology

Sketch proof: step 2

Step 1: first rows of any table are stable after finitely many steps

Step 2: Induction step, from $k-1$ stable rows to k stable rows

- Suppose first $k-1$ rows of every table are stable after finitely many steps
- Suppose a is the first entry of a k-th row
- Then a must have been defined as some b^g for some $b < a$ in the stable rows. (Possibly b has been replaced at some point by a smaller integer due to collapses.)
- So a occurs among the stable $k-1$ rows and is therefore stable.
- So this k-th row must be stable after a finite number of steps.

Sketch proof: step 3

Step 1: first rows of any table are stable after finitely many steps

Step 2: Induction step, from $k-1$ stable rows to k stable rows

Step 3: towards a contradiction
If the procedure does not end, then the number of rows must grow beyond any bound, yielding a transitive permutation action on an infinite set with H in the stabilizer, contradicting that H has finite index in G.

Exercise

$$G = \langle a, b \mid a^3, b^2, (ab)^3 \rangle$$

- Perform coset enumeration with respect to $H = \langle a \rangle$.
- Use this to show that $G \cong A_4$.