Computational aspects of finite p-groups

Heiko Dietrich

School of Mathematical Sciences
Monash University
Clayton VIC 3800, Australia

5th – 14th November 2016
International Centre for Theoretical Sciences – Bangalore

Go to Overview

Welcome! And a bit about myself...

University of Braunschweig (2000-2009)

- one of the four GAP centres
- PhD (on p-groups with maximal class)

University of Auckland (2009-2011)

- work with Magma
- further research on p-groups

University of Trento (2011-2013)

- more work with GAP

Monash University (since 2013)

Welcome!

In this lecture series we discuss

Computational Aspects of Finite p-Groups.

A finite p-group is a group whose order is a positive power of the prime p.

Convention

Throughout, p is a prime; unless stated otherwise, all groups and sets are finite.

Lecture Material

Slides etc will be uploaded at `http://users.monash.edu/~heikod/icts2016`

Assumed knowledge

Some group theory...

Why p-groups?

There's an abundant supply of p-groups

ord.	#
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5
13	1

ord.	#
14	2
15	1
16	14
17	1
18	5
19	1
20	5
21	2
22	2
23	1
24	15
25	2
26	2

ord.	#
27	5
28	4
29	1
30	4
31	1
32	51
33	1
34	2
35	1
36	14
37	1
38	2
39	2

ord.	#
40	14
41	1
42	6
43	1
44	4
45	2
46	2
47	1
48	52
49	2
50	5
51	1
52	5

ord.	#
53	1
54	15
55	2
56	13
57	2
58	2
59	1
60	13
61	1
62	2
63	4
64	267
65	1

- there are $p^{2n^3/27+O(n^{5/3})}$ groups of order p^n
  proved and improved by Higman (1960), Sims (1965), Newman & Seeley (2007)
- conjecture: "almost all" groups are p-groups (2-groups)
  for example, 99% of all groups of order ≤ 2000 are 2-groups

Important aspects of p-groups

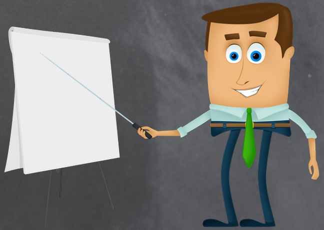
Some comments on p-groups

- Folklore conjecture: "almost all groups are p-groups"
- Sylow Theorem: every nontrivial group has p-groups as subgroups
- Nilpotent groups: direct products of p-groups
- Solvable groups: iterated extensions of p-groups
- Counterpart to theory of finite simple groups
- Challenge: classify p-groups...
- Many "reductions" to p-groups exist: Restricted Burnside Problem, cohomology, Schur multiplier, p-local subgroups, ...

p-groups are fascinating – and accessible to computations! So let's do it...

Outline of this lecture series

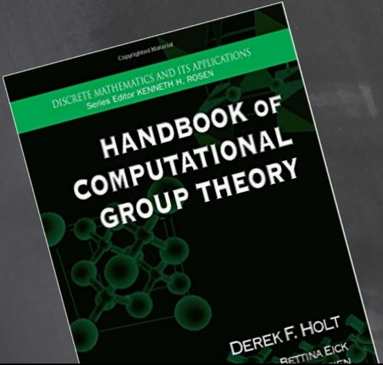
1. motivation
2. pc presentations ▸ Go there
3. p-quotient algorithm ▸ Go there
4. p-group generation ▸ Go there
5. classification by order ▸ Go there
6. isomorphisms ▸ Go there
7. automorphisms ▸ Go there
8. coclass theory ▸ Go there

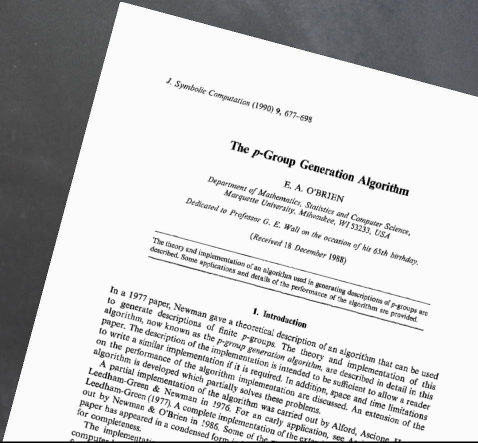


Main resources*

*thanks to E. A. O'Brien for providing some slides

- **Handbook of computational group theory**
  D. Holt, B. Eick, E. A. O'Brien
  Chapman & Hall/CRC, 2005
- **The p-group generation algorithm**
  E. A. O'Brien
  J. Symb. Comp. 9, 677-698 (1990)





J. Symbolic Computation (1990) 9, 677–698

The p-Group Generation Algorithm

E. A. O'BRIEN

Department of Mathematics, Statistics and Computer Science, Marquette University, Milwaukee, WI 53233, USA

Dedicated to Professor G. E. Wall on the occasion of his 65th birthday.

(Received 18 December 1988)

The theory and implementation of an algorithm used in generating descriptions of p-groups are described. Some applications and details of the performance of the algorithm are provided.

1. Introduction

In a 1977 paper, Newman gave a theoretical description of an algorithm that can be used to generate descriptions of finite p-groups. The theory and implementation of this algorithm, now known as the *p-group generation algorithm*, are described in detail in this paper. The description of the implementation is intended to be sufficient to allow a reader to write a similar implementation if it is required. In addition, space and time limitations on the performance of the algorithm implementation are discussed. An extension of the algorithm is developed which partially solves these problems.

A partial implementation of the algorithm was carried out by Alford, Ascione,

pc presentations

▸ Go to Overview

▸ Go to p-Quotient Algorithm

Groups and computers

How to describe groups in a computer?

For example, the dihedral group D_8 can be defined as a ...

- ... permutation group

$$G = \langle (1,2,3,4), (1,3) \rangle;$$

- ... matrix group

$$G = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle \leq \mathrm{GL}_2(3);$$

- ... finitely presented group

$$G = \langle r, m \mid r^4, m^2, r^m = r^3 \rangle.$$

Best for p-groups: (polycyclic) presentations!

Group presentations

Let F be the free group on a set $X \neq \emptyset$; let $\mathcal{R}$ be a set of words in $X \sqcup X^{-1}$. If $R = \mathcal{R}^F$ is the normal closure of $\mathcal{R}$ in F, then

$$G = F/R$$

is the group defined by the **presentation** $\{X \mid \mathcal{R}\}$ with **generators** X and **relators** $\mathcal{R}$; we also write $G = \langle X \mid \mathcal{R}\rangle$ and call $\langle X \mid \mathcal{R}\rangle$ a presentation for G. Informally, it is the "largest" group generated by X and satisfying the relations R.

Example 1

Let $X = \{r, m\}$ and $\mathcal{R} = \{r^4, m^2, \overbrace{m^{-1}rmr^{-3}}^{\text{relator}}\}$, and

$$G = \langle X \mid \mathcal{R}\rangle = \langle r, m \mid r^4, m^2, \underbrace{r^m = r^3}_{\text{relation}}\rangle.$$

What can we say about G? Well... $r^m = r^3$ means $rm = mr^3$, so:

- $G = \{m^i r^j \mid i = 0, 1 \text{ and } j = 0, 1, 2, 3\}$, so $|G| \leq 8$;
- $D_8 = \langle r, m\rangle$ with $r = (1,2,3,4)$ and $m = (1,3)$ satisfies $\mathcal{R}$; thus $G \cong D_8$.

Group presentations

Problem: many questions are algorithmically undecidable in general; eg

- is $\langle X \mid \mathcal{R} \rangle$ finite, trivial, or abelian?
- is a word in X trivial in $\langle X \mid \mathcal{R} \rangle$?

However:

- group presentations are very compact definitions of groups;
- many groups from algebraic topology arise in this form;
- some efficient algorithms exist, eg so-called "quotient algorithms"; (see also C. C. Sims: "Computation with finitely presented groups", 1994)
- many classes of groups can be studied via group presentations.

Let's discuss how to define p-groups by a useful presention!

Background: central series

Center

If G is a p-group, then its center $Z(G) = \{g \in G \mid \forall h \in G\colon g^h = g\}$ is non-trivial.

This leads to the **upper central series** of a p-group G defined as

$$1 = \zeta_0(G) < \zeta_1(G) < \ldots < \zeta_c(G) = G$$

where $\zeta_0(G) = 1$ and each $\zeta_{i+1}(G)$ is defined by $\zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G))$; it is the fastest ascending series with central sections.

Related is the **lower central series**

$$G = \gamma_1(G) > \gamma_2(G) > \ldots > \gamma_{c+1}(G) = 1$$

where $\gamma_1(G) = G$ and each $\gamma_{i+1}(G)$ is defined as[1] $\gamma_{i+1}(G) = [G, \gamma_i(G)]$; it is the fastest descending series with central sections.

The number c is the same for both series; the **(nilpotency) class** of G.

[1] As usual, $[A, B] = \langle [a, b] \mid a \in A, b \in B\rangle$ where $[a, b] = a^{-1}b^{-1}ab = a^{-1}b^a$

Example: central series

Example 2

Let $G = D_{16} = \langle r, m \rangle$ with $r = (1, 2, 3, 4, 5, 6, 7, 8)$, $m = (1, 3)(4, 8)(5, 7)$.
Then G has class $c = 3$; its lower central series is

$$G > \langle r^2 \rangle > \langle r^4 \rangle > 1$$

and has sections[2] $G/\gamma_2(G) \cong C_2 \times C_2$, $\gamma_2(G)/\gamma_3(G) = C_2$, and $\gamma_3(G) = C_2$.
We can refine this series so that all section are isomorphic to C_2:

$$G > \langle r \rangle > \langle r^2 \rangle > \langle r^4 \rangle > 1.$$

In general: every central series of a p-group G can be refined to a **composition series**

$$G = G_1 > G_2 > \ldots > G_{n+1} = 1$$

where each $G_i \trianglelefteq G$ and $G_i/G_{i+1} \cong C_p$; thus G is a **polycyclic group**.

[2] If n is a positive integer, then C_n denotes a cyclic group of size n.

Polycyclic groups

Polycyclic group

The group G is **polycyclic** if it admits a **polycyclic series**, that is, a subgroup chain $G = G_1 \geq \ldots \geq G_{n+1} = 1$ in which each $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is cyclic.

Polycyclic groups: solvable groups whose subgroups are finitely generated.

Example 3

The group $G = \langle (2,4,3), (1,3)(2,4) \rangle \cong \mathrm{Alt}(4)$ is polycyclic with series

$$G = G_1 > G_2 > G_3 > G_4 = 1$$

where

$$\begin{aligned} G_2 &= \langle (1,3)(2,4), (1,2)(3,4) \rangle \ = \ V_4 \ \trianglelefteq \ G_1 \\ G_3 &= \langle (1,2)(3,4) \rangle \ \trianglelefteq \ G_2 \end{aligned}$$

Each G_i/G_{i+1} is cyclic, so there is $g_i \in G_i \setminus G_{i+1}$ with $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$; for example, $g_1 = (2,4,3)$, $g_2 = (1,3)(2,4)$, $g_3 = (1,2)(3,4)$.

Polycyclic Sequence

Polycyclic sequence

Let $G = G_1 \geq \ldots \geq G_{n+1} = 1$ be a polycyclic series.
A related **polycyclic sequence** X with **relative orders** $R(X)$ is

$$X = [g_1, \ldots, g_n] \quad \text{with} \quad R(X) = [r_1, \ldots, r_n]$$

where each $g_i \in G_i \setminus G_{i+1}$ and $r_i = |g_i G_{i+1}| = |G_i/G_{i+1}|$.
A polycyclic series is also called **pcgs** (polycyclic generating set).

Important observation: each $G_i = \langle g_i, g_{i+1}, \ldots, g_n \rangle$ and $|G_i| = r_i \cdots r_n$.

Example 4

Let $G = D_{16} = \langle r, m \rangle$ with $r = (1,2,3,4,5,6,7,8)$ and $m = (1,3)(4,8)(5,7)$.
Examples of pcgs:

- $X = [m, r]$ with $R(X) = [2, 8]$: $G = \langle m, r \rangle > \langle r \rangle > 1$;
- $X = [m, r, r^4]$ with $R(X) = [2, 4, 2]$: $G = \langle m, r, r^4 \rangle > \langle r, r^4 \rangle > \langle r^4 \rangle > 1$;
- $X = [m, r, r^3, r^2]$ with $R(X) = [2, 1, 2, 4]$; note that $\langle r, r^3, r^2 \rangle = \langle r^3, r^2 \rangle$.

Normal Forms

Lemma: Normal Form

Let $X = [g_1, \ldots, g_n]$ be a pcgs for G with $R(X) = [r_1, \ldots, r_n]$.
If $g \in G$, then $g = g_1^{e_1} \cdots g_n^{e_n}$ for unique $e_i \in \{0, \ldots, r_i - 1\}$.

We call $g = g_1^{e_1} \cdots g_n^{e_n}$ the **normal form** with respect to X.

Proof.

Let $g \in G$ be given; we use induction on n.

- If $n = 1$, then $G = \langle g_1 \rangle \cong C_{r_1}$ and the lemma holds; now let $n \geq 2$.
- Since $G/G_2 = \langle g_1 G_2 \rangle \cong C_{r_1}$, we can write $gG_2 = g_1^{e_1} G_2$ for a unique $e_1 \in \{0, \ldots, r_1 - 1\}$, that is, $g' = g_1^{-e_1} g \in G_2$.
- $X' = [g_2, \ldots, g_n]$ is pcgs of G_2 with $R(X') = [r_2, \ldots, r_n]$, so by induction $g' = g_1^{-e_1} g = g_2^{e_2} \cdots g_n^{e_n}$ for unique $e_i \in \{0, \ldots, r_i - 1\}$.
- In conclusion, $g = g_1^{e_1} \cdots g_n^{e_n}$ as claimed.

Example: Normal Forms

Example 5

A pcgs of $G = \mathrm{Alt}(4)$ with $R(X) = [3,2,2]$ is $X = [g_1, g_2, g_3]$ where

$$g_1 = (1,2,3), \quad g_2 = (1,2)(3,4), \quad g_3 = (1,3)(2,4).$$

This yields $G = G_1 > G_2 > G_3 > G_4 = 1$ with each $G_i = \langle g_i, \ldots, g_3 \rangle$.

Now consider $g = (1,2,4) \in G$.

First, we have $gG_2 = g_1^2 G_2$, so $g' = g_1^{-2} g = (1,4)(2,3) \in G_2$.

Second, $g'G_3 = g_2 G_3$, so $g'' = g_2^{-1} g' = (1,3)(2,4) = g_3 \in G_3$.

In conclusion, $g = g_1^2 g' = g_1^2 g_2 g'' = g_1^2 g_2 g_3$.

Polycyclic group to presentation

Let G be group with pcgs $X = [g_1, \ldots, g_n]$ and $R(X) = [r_1, \ldots, r_n]$; define $G_i = \langle g_i, \ldots, g_n \rangle$. There exist $a_{*,j}, b_{*,*,j} \in \{0, 1, \ldots, r_j - 1\}$ with:

- $g_i^{r_i} = g_{i+1}^{a_{i,i+1}} \cdots g_n^{a_{i,n}}$ (for all i, since $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle \cong C_{r_i}$)
- $g_i^{g_j} = g_{j+1}^{b_{i,j,j+1}} \cdots g_n^{b_{i,j,n}}$ (for all $j < i$, since $g_i \in G_{j+1} \trianglelefteq G_j$).

A polycyclic presentation (PCP) for G

Let $H = \langle x_1, \ldots, x_n \mid \mathcal{R} \rangle$ such $\mathcal{R}$ contains exactly the above relations:

$$x_i^{r_i} = x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} \quad \text{and} \quad x_i^{x_j} = x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}}.$$

Then $H \cong G$ with pcgs $X = [x_1, \ldots, x_n]$ and $R(X) = [r_1, \ldots, r_n]$.

Proof.

Define $\varphi \colon H \to G$ by $x_i \mapsto g_i$. The elements $g_1, \ldots, g_n$ satisfy the relations in $\mathcal{R}$, so φ is an epimorphism by **von Dyck's Theorem**. By construction, H is polycyclic with pcgs X and order at most $|G|$. Thus, φ is an isomorphism.

Polycyclic group to presentation

Example 6

Let $G = \mathrm{Alt}(4)$ with pcgs $X = [g_1, g_2, g_3]$ and $R(X) = [3, 2, 2]$ where

$$g_1 = (1,2,3), \quad g_2 = (1,2)(3,4), \quad g_3 = (1,3)(2,4).$$

Then $g_1^3 = g_2^2 = g_3^2 = 1,\ g_2^{g_1} = g_2g_3,\ g_3^{g_1} = g_2,\ g_3^{g_2} = g_3$, and so

$$G \cong \langle x_1, x_2, x_3 \mid x_1^3 = x_2^2 = x_3^2 = 1,\ x_2^{x_1} = x_2x_3,\ x_3^{x_1} = x_2,\ x_3^{x_2} = x_3 \rangle.$$

Theorem

Every pcgs determines a unique polycyclic presentation;
every polycyclic group can be defined by a polycyclic presentation.

Pc presentation to group

Polycyclic presentation (pcp)

A presentation $\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ is a **polycyclic presentation** with **power exponents** $s_1, \ldots, s_n \in \mathbb{N}$ if the only relations in $\mathcal{R}$ are

$$\begin{aligned} x_i^{s_i} &= x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} && \text{(all } i\text{, each } a_{i,k} \in \{0, \ldots, s_k - 1)\\ x_i^{x_j} &= x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}} && \text{(all } j < i\text{, each } b_{i,j,k} \in \{0, \ldots, s_k - 1).\end{aligned}$$

We write $\mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ and **omit trivial commutator relations** $x_i^{x_j} = x_i$. The group defined by a pc-presentation is a **pc-group**.

Theorem

If $G = \mathrm{Pc}\langle x_1 \ldots, x_n \mid \mathcal{R}\rangle$ with power exps $[s_1, \ldots, s_n]$, then $X = [x_1, \ldots, x_n]$ is a pcgs of G. If $g \in G$, then $g = x_1^{e_1} \cdots x_n^{e_n}$ for some $e_i \in \{0, \ldots, s_i - 1\}$.

Careful: $(x_i G_i)^{s_i} = 1$ only implies that $r_i = |G_i/G_{i+1}|$ *divides* s_i, not $r_i = s_i$; so in general

$$R(X) = [r_1, \ldots, r_n] \neq [s_1, \ldots, s_n].$$

Consistent pc presentations

Note: Only power exponents (not relative orders) are visible in pc presentations.

Example 7

Let $G = \mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^3 = x_3,\ x_2^2 = x_3,\ x_3^5 = 1,\ x_2^{x_1} = x_2x_3\rangle$; this is a pc-group with pcgs $X = [x_1, x_2, x_3]$ and power exponents $S = [3, 2, 5]$.

We show $R(X) = [3, 2, 1]$, so $|G| = 6$:

First, note that $x_2^{10} = x_3^5 = 1$, so $|x_2| \mid 10$.

Second, $x_2^{x_1} = x_2x_3 = x_2^3$ so $x_2^{27} = x_2^{(x_1^3)} = x_2^{x_3} = x_2^{(x_2^2)} = x_2$, and thus $|x_2| \mid 26$.

This implies that $5 \nmid |x_2|$, and forces $x_3 = 1$ in G.

Note that $x_1^0x_2^0x_3^0 = 1 = x_1^0x_2^0x_3^1$ are two normal forms (wrt power exponents).

Consistent pc presentation

A pc-presentation with power exponents S is **consistent** if and only if every group element has a unique normal form with respect to S; otherwise it is **inconsistent**.

How to check consistency? $\rightsquigarrow$ use **collection** and **consistency checks**!

Collection

Let $G = \mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ with power exponents $S = [s_1, \ldots, s_n]$.

Consider a reduced word $w = x_{i_1}^{e_1} \cdots x_{i_r}^{e_r}$, that is, each $i_j \neq i_{j+1}$; we can assume $e_j \in \mathbb{N}$, otherwise eliminate using power relations.

Collection

Let $w = x_{i_1}^{e_1} \cdots x_{i_r}^{e_r}$ as above and use the previous notation:

- the word w is **collected** if w is the normal form wrt S, that is, $i_1 < \ldots < i_r$ and each $e_j \in \{0, \ldots, s_{i_j} - 1\}$;
- if w is not collected, then it has a **minimal non-normal subword** of w, that is, a subword u of the form

$$u = x_{i_j}^{e_j} x_{i_{j+1}} \quad \text{with } i_j > i_{j+1}, \quad \text{eg } u = x_3^2 x_1$$

or

$$u = x_{i_j}^{s_{i_j}} \quad \text{eg } u = x_2^5 \text{ with } s_2 = 5.$$

Collection is a method to obtain collected words.

Collection algorithm

Let $G = \mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ with power exponents $S = [s_1, \ldots, s_n]$.

Consider a reduced word $w = x_{i_1}^{e_1} \cdots x_{i_r}^{e_r}$, that is, each $i_j \neq i_{j+1}$;
we can assume $e_j \in \mathbb{N}$, otherwise eliminate using power relations.

Collection algorithm

Input: polycyclic presentation $\mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ and word w in X
Output: a collected word representing w

Repeat the following until w has no minimal non-normal subword:

- choose minimal non-normal subword $u = x_{i_j}^{s_{i_j}}$ or $u = x_{i_j}^{e_j} x_{i_{j+1}}$;
- if $u = x_{i_j}^{s_{i_j}}$, then replace u by a suitable word in $x_{i_j+1}, \ldots, x_n$;

  if $u = x_{i_j}^{e_j} x_{i_{j+1}}$, then replace u by $x_{i_{j+1}} u'$ with u' word in $x_{i_j+1}, \ldots, x_n$.

Theorem

The collection algorithm terminates.

Collection algorithm

If w contains more than one minimal non-normal subword, a rule is used to determine which of the subwords is replaced (making the process well-defined).

- **Collection to the left**: move all occurrences of x_1 to the beginning of the word; next, move all occurrences of x_2 left until adjacent to the x_1's, etc.
- **Collection from the right**: the minimal non-normal subword nearest to the end of a word is selected.
- **Collection from the left**: the minimal non-normal subword nearest to the beginning of a word is selected.

Example: collection

Consider the group

$$D_{16} \cong \mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = 1,\ x_2^2 = x_3x_4,\ x_3^2 = x_4,\ x_4^2 = 1,\ x_2^{x_1} = x_2x_3,\ x_3^{x_1} = x_3x_4 \rangle.$$

Aim: collect the word $x_3x_2x_1$.
Since power exponents are all "2", we only use generator indices:

"to the left"

$$\begin{aligned} 3\underline{21} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 1\underline{32}43 \\ &= 123\underline{43} \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

"from the right"

$$\begin{aligned} 3\underline{21} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 132\underline{43} \\ &= 1\underline{32}34 \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

"from the left"

$$\begin{aligned} \underline{32}1 &= 2\underline{31} \\ &= \underline{21}34 \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

Consistency checks

Theorem 8: consistency checks

$\mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ with power exps $[s_1, \ldots, s_n]$ is consistent if and only if the normal forms of the following pairs of words coincide

$$\begin{array}{rl} x_k(x_jx_i) \text{ and } (x_kx_j)x_i & \text{for } 1 \leq i < j < k \leq n, \\ (x_j^{s_j})x_i \text{ and } x_j^{s_j-1}(x_jx_i) & \text{for } 1 \leq i < j \leq n, \\ x_j(x_i^{s_i}) \text{ and } (x_jx_i)x_i^{s_i-1} & \text{for } 1 \leq i < j \leq n, \\ x_j(x_j^{s_j}) \text{ and } (x_j^{s_j})x_j & \text{for } 1 \leq j \leq n, \end{array}$$

where the subwords in brackets are to be collected first.

Example 9

If $G = \mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^3 = x_3,\ x_2^2 = x_3,\ x_3^5 = 1,\ x_2^{x_1} = x_2x_3\rangle$, then

$$(x_2^2)x_1 = x_3x_1 = x_1x_3 \quad \text{and} \quad x_2(x_2x_1) = x_2x_1x_2x_3 = x_1x_2^2x_3^2 = x_1x_3^3.$$

Since $x_1x_3 = x_1x_3^3$ are both normal forms, the presentation is *not* consistent. Indeed, we deduce that $x_3 = 1$ in G.

Weighted power-commutator presentation

So far we have seen that every p-group can be defined via a consistent polycyclic presentation.

However, the algorithms we discuss later require a special type of polycyclic presentations, namely, so-called **weighted power-commutator presentations**.

Weighted power-commutator presentation

A **weighted power-commutator presentation** (wpcp) of a d-generator group G of order p^n is $G = \mathrm{Pc}\langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$ such that $\{x_1, \ldots, x_d\}$ is a minimal generating set G and the relations are

$$x_j^p = \prod\nolimits_{k=j+1}^{n} x_k^{\alpha(j,k)} \qquad (1 \leq j \leq n,\ \ 0 \leq \alpha(j,k) < p)$$

$$[x_j, x_i] = \prod\nolimits_{k=j+1}^{n} x_k^{\beta(i,j,k)} \qquad (1 \leq i < j \leq n,\ \ 0 \leq \beta(i,j,k) < p)$$

note that every $G_i = \langle x_i, \ldots, x_n\rangle$ is normal in G.

Moreover, each $x_k \in \{x_{d+1}, \ldots, x_n\}$ is the right side of some relation; choose one of these as the **definition** of x_k.

Weighted power-commutator presentation

Example 10

Consider

$$G = \mathrm{Pc}\langle\ x_1, \ldots, x_5 \quad \mid \quad x_1^2 = x_4,\ x_2^2 = x_3,\ x_3^2 = x_5,\ x_4^2 = x_5,\ x_5^2 = 1$$
$$[x_2, x_1] = x_3,\ [x_3, x_1] = x_5\ \rangle.$$

Here $\{x_1, x_2\}$ is a minimal generating set of G, and we choose:

- x_3 has definition $[x_2, x_1]$ and weight 2;
- x_4 has definition x_1^2 and weight 2;
- x_5 has definition $[x_3, x_1]$ and weight 3.

Weighted power-commutator presentation

Why are (w)pcp's useful?

- consistent pcp's allow us to solve the *word problem* for the group: given two words, compute their normal forms, and compare them
- the additional structure of wpcp's allows more efficient algorithms: for example: consistency checks, p-group generation (later)
- a wpcp exhibits a *normal* series $G > G_1 > \ldots > G_n = 1$: many algorithms work down this series and use induction: first solve problem for G/G_k, and then extend to solve the problem for G/G_{k+1}, and so eventually for $G = G/G_n$.

... how to compute wpcp's? $\rightsquigarrow$ p-quotient algorithm (next lecture)

Conclusion Lecture 1

Things we have discussed in the first lecture:

- polycyclic groups, sequences, and series
- polycyclic generating sets (**pcgs**) and relative orders
- polycyclic presentations (**pcp**), power exponents, and consistency
- normal forms and collection
- consistency checks
- weighted polycyclic presentations (**wpcp**)