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)

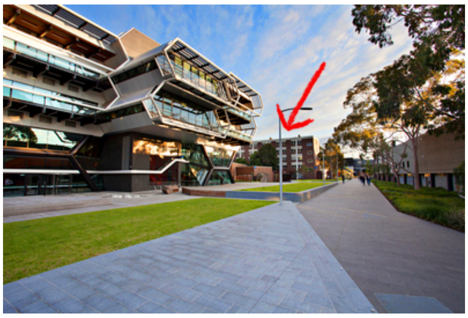
- one of the four GAP centres
- PhD (on p-groups with maximal class)

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.	#	ord.	#	ord.	#	ord.	#	ord.	#
1	1	14	2	27	5	40	14	53	1
2	1	15	1	28	4	41	1	54	15
3	1	16	14	29	1	42	6	55	2
4	2	17	1	30	4	43	1	56	13
5	1	18	5	31	1	44	4	57	2
6	2	19	1	32	51	45	2	58	2
7	1	20	5	33	1	46	2	59	1
8	5	21	2	34	2	47	1	60	13
9	2	22	2	35	1	48	52	61	1
10	2	23	1	36	14	49	2	62	2
11	1	24	15	37	1	50	5	63	4
12	5	25	2	38	2	51	1	64	267
13	1	26	2	39	2	52	5	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

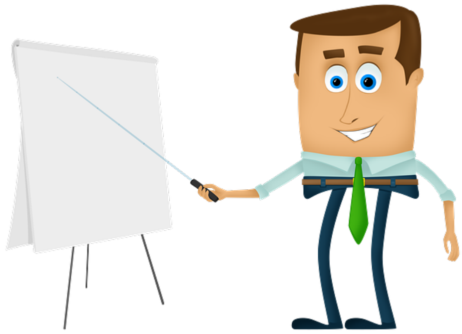
Some comments on p-groups

- 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

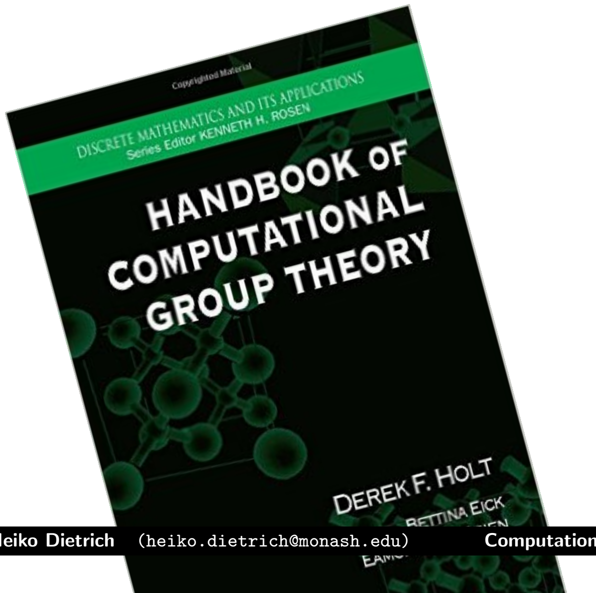
1. motivation
2. pc presentations ▸ Go there
3. p-quotient algorithm ▸ Go there
4. p-group generation ▸ Go there
5. classification by order ▸ Go there
6. isomorphisms ▸ Go there
7. automorphisms ▸ Go there
8. coclass theory ▸ Go there



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.

pc presentations

Go to Overview
Go to p-Quotient Algorithm

Polycyclic Presentations | Presentations | Central Series | Polycyclic Groups | Collection | WPCP's

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!

Heiko Dietrich (heiko.dietrich@monash.edu) Computational aspects of finite p-groups ICTS, Bangalore 2016

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

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

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 $G = \mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^3 = x_3,\ x_2^2 = x_3,\ x_3^5 = 1,\ x_2^{x_1} = x_2 x_3\rangle$; 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, $x_2^{x_1} = x_2 x_3 = x_2^3$ 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 $x_1^0 x_2^0 x_3^0 = 1 = x_1^0 x_2^0 x_3^1$ 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.

Polycyclic Presentations | Presentations | Central Series | Polycyclic Groups | Collection | WPCP's

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

$$x_k(x_jx_i) \text{ and } (x_kx_j)x_i \qquad \text{for } 1 \le i < j < k \le n,$$
$$(x_j^{s_j})x_i \text{ and } x_j^{s_j-1}(x_jx_i) \qquad \text{for } 1 \le i < j \le n,$$
$$x_j(x_i^{s_i}) \text{ and } (x_jx_i)x_i^{s_i-1} \qquad \text{for } 1 \le i < j \le n,$$
$$x_j(x_j^{s_j}) \text{ and } (x_j^{s_j})x_j \qquad \text{for } 1 \le j \le n,$$

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

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

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

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.

Polycyclic Presentations | Presentations | Central Series | Polycyclic Groups | Collection | WPCP's

Weighted power-commutator presentation

Example 10

Consider

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

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**)

p-quotient algorithm

Go to Presentations
Go to p-Group Generation

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**)

Conclusion Lecture 1

weighted polycyclic presentation (wpcp):

- all relative orders p
- induced polycyclic series is chief series
- relations are partitioned into definitions and non-definitions

Example

Consider

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

Here $\{x_1, x_2\}$ is a minimal generating set, and we choose $[x_2, x_1] = x_3$ and $x_1^2 = x_4$ and $[x_3, x_1] = x_5$ as definitions for x_3, x_4, and x_5, respectively.

Lecture 2: how to compute a wpcp?

Lower exponent-p series

Lower exponent p-series

The **lower exponent-p series** of a p-group G is

$$G = P_0(G) > P_1(G) > \ldots > P_c(G) = 1$$

where each $P_{i+1}(G) = [G, P_i(G)]P_i(G)^p$; the p-**class** of G is c.

Important properties

- each $P_i(G)$ is characteristic in G;
- $P_1(G) = [G, G]G^p = \Phi(G)$, and $G/P_1(G) \cong C_p^d$ with $d = \mathrm{rank}(G)$;
- each section $P_i(G)/P_{i+1}(G)$ is G-central and elementary abelian;
- if G has p-class c, then its nilpotency class is at most c;
- if θ is a homomorphism, then $\theta(P_i(G)) = P_i(\theta(G))$;
- G/N has p-class c if and only if $P_c(G) \leq N$;
- **weights:** any wpcp on $\{a_1, \ldots, a_n\}$ satisfies $a_i \in P_{\omega(a_i)}(G) \setminus P_{\omega(a_i)+1}(G)$.

Lower exponent-p series

Example 11

Consider

$$G = D_{16} = \mathrm{Pc}\langle a_1, a_2, a_3, a_4 \mid a_1^2 = 1,\ a_2^2 = a_3a_4,\ a_3^2 = a_4,\ a_4^2 = 1,\ [a_2, a_1] = a_3,\ [a_3, a_1] = a_4\rangle.$$

Here we can read off:

- $P_0(G) = G$
- $P_1(G) = [G, G]G^2 = \langle a_3, a_4\rangle$
- $P_2(G) = [G, P_1(G)]P_1(G)^2 = \langle a_4\rangle$
- $P_3(G) = [G, P_2(G)]P_2(G)^2 = 1$

So G has 2-class 3.

Computing a wpcp of a p-group

p-quotient algorithm[3]

Input: a p-group $G = F/R = \langle x_1, \ldots, x_n \mid \mathcal{R}\rangle$

Output: a wpcp of G

Top-level outline:

1. compute wpcp of $G/P_1(G)$ and epimorphism $G \to G/P_1(G)$, then iterate:
2. given wpcp of $G/P_k(G)$ and epimorphism $G \to G/P_k(G)$, compute wpcp of $G/P_{k+1}(G)$ and epimorphism $G \to G/P_{k+1}(G)$;

For the second step, we use the so-called p-*cover* of $G/P_k(G)$.

More general: a "p-quotient algorithm" computes a consistent wpcp of the largest p-class k quotient (if it exists) of any finitely presented group.

[3] **Historically:** MacDonald (1974), Havas & Newman (1980), Newman & O'Brien (1996)

Computing a wpcp of $G/P_1(G)$

Note that $G/P_1(G)$ is elementary abelian.

Computing wpcp of $G/P_1(G)$

Input: a p-group $G = F/R = \langle x_1, \ldots, x_n \mid \mathcal{R} \rangle$
Output: a wpcp of $G/P_1(G)$ and epimorphism $\theta\colon G \to G/P_1(G)$

Approach:

1. abelianise relations, take exponents modulo p, write these in matrix M
2. compute solution space of M over GF(p)

Then:

- dimension d of solution space is rank of G, that is, $G/P_1(G) \cong C_p^d$
- generating set of $G/P_1(G)$ lifts to subset of given generators;

  set $G/P_1(G) = \mathrm{Pc}\langle a_1, \ldots, a_d \mid a_1^p = \ldots = a_d^p \rangle$ and define θ by

$$\theta(x_i) = a_i \quad \text{for} \quad i = 1, \ldots, d;$$

  images of $\theta(x_j)$ with $j > d$ are determined accordingly.

Computing a wpcp of $G/P_1(G)$

Example 12

$G = \langle x_1, \ldots, x_6 \mid x_6^{10},\ x_1x_2x_3,\ x_2x_3x_4, \ldots, x_4x_5x_6,\ x_5x_6x_1,\ x_1x_6x_2 \rangle$ and $p = 2$

Write coefficients of abelianised and mod-2 reduced equations as rows of matrix, use row-echelonisation, and determine that solution space has dimension 2:

$$\begin{pmatrix} 1&1&1&0&0&0\\ 0&1&1&1&0&0\\ 0&0&1&1&1&0\\ 0&0&0&1&1&1\\ 1&0&0&0&1&1\\ 1&1&0&0&0&1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&0&0&0&1&1\\ 0&1&0&0&1&0\\ 0&0&1&0&0&1\\ 0&0&0&1&1&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{pmatrix};$$

Modulo $P_1(G)$, this shows that $x_1 = x_5x_6$, $x_2 = x_5$, $x_3 = x_6$, $x_4 = x_5x_6$, and **Burnside's Basis Theorem** implies that $G = \langle x_5, x_6 \rangle$. Lastly, set

$$G/P_1(G) = \mathrm{Pc}\langle a_1, a_2 \mid a_1^2 = a_2^2 = 1 \rangle,$$

and define $\theta\colon G \to G/P_1(G)$ via $x_5 \mapsto a_1$ and $x_6 \mapsto a_2$.
This determines $\theta(x_1) = a_1a_2$, $\theta(x_2) = a_1$, $\theta(x_3) = a_2$, and $\theta(x_4) = a_1a_2$.

Compute wpcp for $G/P_{k+1}(G)$ from that of $G/P_k(G)$

Given:

- wpcp of d-generator p-group $G/P_k(G)$ and epimorphism $\theta\colon G \to G/P_k(G)$

Want:

- wpcp of $G/P_{k+1}(G)$ and epimorphism $G \to G/P_{k+1}(G)$

In the following:

- $H = G/P_k(G)$ and $K = G/P_{k+1}(G)$ and $Z = P_k(G)/P_{k+1}(G)$
- note that Z is elementary abelian, K-central, and $K/Z \cong H$

Approach: Construct a *covering* H^* of H such that *every* d-generator p-group L with $L/M \cong H$ and $M \leq L$ central elementary abelian, is a quotient of H^*.

Thus, the next steps are:

1. define p-cover H^* and determine a pcp of H^*;
2. make this presentation consistent;
3. construct K as quotient of H^* by enforcing defining relations of G.

p-covering group: definition

Theorem 13: p-covering group

Let H be a d-generator p-group; there is a d-generator p-group H^* with:

- $H^*/M \cong H$ for some central elementary abelian $M \trianglelefteq H^*$;
- if L is a d-generator p-group with $L/Y \cong H$ for some central elementary abelian $Y \leq L$, then L is a quotient of H^*.

The group H^* is unique up to isomorphism.

Proof.

Let $H = F/S$ with F free of rank d. Define $H^* = F/S^*$ with $S^* = [S,F]S^p$.

Now S/S^* is elementary abelian p-group, so H^* is (finite) d-generator p-group.

Let L be as in the theorem, and let $\psi\colon L \to H$ with kernel Y.
Let $\theta\colon F \to H$ with kernel S. Since F is free, θ factors through L, that is,
$\theta\colon F \stackrel{\varphi}{\to} L \stackrel{\psi}{\to} H$, and so $\varphi(S) \leq \ker\psi = Y$. This implies that $\varphi(S^*) = 1$.
In conclusion, φ induces surjective map from $H^* = F/S^*$ onto L.

If H^* and $\tilde{H}^*$ are two such covers, then each is an image of the other.

p-covering group: presentation

Given: a wpcp $\mathrm{Pc}\langle a_1,\ldots,a_m \mid \mathcal{S}\rangle$ for $H = G/P_k(G) \cong F/S$
and epimorphism $\theta\colon G \to H$ with $\theta(x_i) = a_i$ for $i = 1,\ldots,d$

Want: a wpcp for $H^* \cong F/S^*$ where $S^* = [S,F]S^p$

Recall: each of $a_{d+1},\ldots,a_m$ occurs as right hand side of one relation in $\mathcal{S}$;
write $\mathcal{S} = \mathcal{S}_{\text{def}} \cup \mathcal{S}_{\text{nondef}}$ with $\mathcal{S}_{\text{nondef}} = \{s_1,\ldots,s_q\}$.

Theorem 14
Using the previous notation, $H^* = \mathrm{Pc}\langle a_1,\ldots,a_m,b_1,\ldots,b_q \mid \mathcal{S}^*\rangle$, where

$$\mathcal{S}^* = \mathcal{S}_{\text{def}} \cup \{s_1b_1,\ldots,s_qb_q\} \cup \{b_1^p,\ldots,b_q^p\}.$$

Note: $M = \langle b_1,\ldots,b_q\rangle \trianglelefteq H^*$ is elementary abelian, central, and $H^*/M \cong H$.

(see Newman, Nickel, Niemeyer: "Descriptions of groups of prime-power order", 1998)

In practice: fewer new generators are introduced.

p-covering group: example

Example 15
If $H = \mathrm{Pc}\langle a_1,a_2 \mid a_1^2 = a_2^2 = 1\rangle \cong C_2 \times C_2$, then

$$H^* = \mathrm{Pc}\langle a_1,a_2,b_1,b_2,b_3 \mid a_1^2 = b_1,\ a_2^2 = b_2,\ [a_1,a_2] = b_3,\ b_1^2 = b_2^2 = b_3^2 = 1\rangle;$$

indeed, $H^* \cong (C_4 \times C_2)\colon C_4$, thus we have found a consistent wpcp!

Example 16
If $H = \mathrm{Pc}\langle a_1,a_2,a_3 \mid a_1^2 = a_3^2 = 1, a_2^2 = a_3, [a_2,a_1] = a_3\rangle \cong D_8$, then

$$H^* = \mathrm{Pc}\langle a_1,a_2,a_3,b_1,\ldots,b_5 \mid \mathcal{T} \cup \{b_1^2,\ldots,b_5^2\}\ \rangle \quad \text{with}$$

$$\mathcal{T} = \{a_1^2 = b_1, a_2^2 = a_3b_2, a_3^2 = b_3, [a_2,a_1] = a_3, [a_3,a_1] = b_4, [a_3,a_2] = b_5\};$$

this pcp has power exponents $[2,2,2,2,2,2,2,2]$.
However, $H^* \cong (C_8 \times C_2)\colon C_4$, so presentation is **not consistent**!

Next step: make the presentation of H^* consistent.

p-covering group: consistency algorithm

By Theorem 8, the presentation $H^* = \mathrm{Pc}\langle u_1, \ldots, u_{m+q} \mid \mathcal{S}^* \rangle$ with $(u_1, \ldots, u_{m+q}) = (a_1, \ldots, a_m, b_1, \ldots, b_q)$ is consistent if and only if

$$u_k(u_j u_i) = (u_k u_j)u_i \qquad (1 \leq i < j < k \leq m+q)$$
$$(u_j^p)u_i = u_j^{p-1}(u_j u_i) \text{ and } u_j(u_i^p) = (u_j u_i)u_i^{p-1} \qquad (1 \leq i < j \leq m+q)$$
$$u_j(u_j^p) = (u_j^p)u_j \qquad (1 \leq j \leq m+q).$$

Consistency Algorithm[4]: find consistent presentation for H^*

- If each pair of words in the above "consistency checks" collects to the same normal word, then the presentation is consistent.
- Otherwise, the quotient of the two different words obtained from one of these conditions is formed and equated to the identity word: this gives a new relation which holds in the group.
- The pcp for H is consistent, so any new relation is an equation in the elementary abelian subgroup M generated by the new generators $\{b_1, \ldots, b_q\}$, which implies that one of these generators is redundant.

[4] **Historically:** Wamsley (1974), Vaughan-Lee (1984)

p-Quotient Algorithm | p-Class | Algorithm | Covering Group | Example | Burnside Problem

p-covering group: consistency algorithm

By Theorem 8, the presentation $H^* = \mathrm{Pc}\langle u_1, \ldots, u_{m+q} \mid \mathcal{S}^* \rangle$ with $(u_1, \ldots, u_{m+q}) = (a_1, \ldots, a_m, b_1, \ldots, b_q)$ is consistent if and only if

$$u_k(u_j u_i) = (u_k u_j)u_i \qquad (1 \leq i < j < k \leq m+q)$$
$$(u_j^p)u_i = u_j^{p-1}(u_j u_i) \text{ and } u_j(u_i^p) = (u_j u_i)u_i^{p-1} \qquad (1 \leq i < j \leq m+q)$$
$$u_j(u_j^p) = (u_j^p)u_j \qquad (1 \leq j \leq m+q).$$

Example 17

Consider $G = \mathrm{Pc}\langle u_1, u_2, u_3 \mid u_1^2 = u_2,\ u_2^2 = u_3,\ u_3^2 = 1,\ [u_2, u_1] = u_3 \rangle$.
The last test applied to u_1 yields

$$u_1^3 = (u_1^2)u_1 = u_2 u_1 = u_1 u_2 u_3 \quad \text{and} \quad u_1^3 = u_1(u_1^2) = u_1 u_2,$$

so $u_3 = 1$ in G, hence $G = \mathrm{Pc}\langle u_1, u_2 \mid u_1^2 = u_2,\ u_2^2 = 1 \rangle \cong C_4$.

Heiko Dietrich (heiko.dietrich@monash.edu) Computational aspects of finite p-groups ICTS, Bangalore 2016

Construct K from cover H^* of H

So what have we got so far...

- p-group $G = F/R = \langle x_1, \ldots, x_n \mid \mathcal{R} \rangle$
- consistent wpcp of $H = G/P_k(G) = \mathrm{Pc}\langle a_1, \ldots, a_m \mid \mathcal{S} \rangle$
- epimorphism $\theta \colon G \to H$ with $\theta(x_i) = a_i$ for $i = 1, \ldots, d$
- consistent wpcp of cover $H^* = \mathrm{Pc}\langle a_1, \ldots, a_m, b_1, \ldots, b_q \mid \mathcal{S}^* \rangle$; note that $H^*/M \cong H$ where $M = \langle b_1, \ldots, b_q \rangle$

Want:

- consistent wpcp of $K = G/P_{k+1}(G)$ and epimorphism $G \to G/P_{k+1}(G)$

Know:

- $K/Z \cong H$ where $Z = P_k(G)/P_{k+1}(G)$ is elementary abelian, central
- K is quotient of H^*

Idea:

- construct K as quotient of H^*: add relations enforced by G to $\mathcal{S}^*$

Construct K from cover H^* of H

So what have we got so far...

- p-group $G = F/R = \langle x_1, \ldots, x_n \mid \mathcal{R} \rangle$
- consistent wpcp of $H = G/P_k(G) = \mathrm{Pc}\langle a_1, \ldots, a_m \mid \mathcal{S} \rangle$
- epimorphism $\theta \colon G \to H$ with $\theta(x_i) = a_i$ for $i = 1, \ldots, d$
- consistent pcp of cover $H^* = \mathrm{Pc}\langle a_1, \ldots, a_m, b_1, \ldots, b_q \mid \mathcal{S}^* \rangle$; note that $H^*/M \cong H$ where $M = \langle b_1, \ldots, b_q \rangle$

Enforcing relations of G:

- know that $K = G/P_{k+1}(G)$ is quotient of H^*
- lift $\theta \colon G \to H$ to $\hat{\theta} \colon F \to H^*$ such that $\hat{\theta}(x_i) = a_i$ for $i = 1, \ldots, d$
- for every relator $r \in \mathcal{R}$ compute $n_r = \hat{\theta}(r) \in M$; let L be the subgroup of M generated by all these n_r
- by von Dyck's Theorem $H^*/L \to K$ and $G \to H^*/L$ are surjective; since K is the largest p-class $k+1$ quotient of G, we deduce $K = H^*/L$

Finally: find consistent wpcp of $K = H^*/L$ and get epimorphism $G \to K$

Big example: p-quotient algorithm in action

Let $G = \langle x, y \mid [[y,x],x] = x^2,\ (xyx)^4,\ x^4,\ y^4,\ (yx)^3y = x\rangle$ and $p = 2$.

First round:

- compute $G/P_1(G)$ using abelianisation and row-echelonisation:

  obtain $H = G/P_1(G) \cong \mathrm{Pc}\langle a_1, a_2 \mid a_1^2 = a_2^2 = 1\rangle$
  and epimorphism $\theta\colon G \to H$, which is defined by $(x,y) \to (a_1,a_2)$.
- construct covering of H by adding new generators and tails:

  $H^* = \mathrm{Pc}\langle a_1,\ldots,a_5 \mid a_1^2 = a_3, a_2^2 = a_4, [a_2,a_1] = a_5,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle$
- the consistency algorithm shows that this presentation is consistent
- evaluate relations of G in H^*:
  - $1 = [[a_2,a_1],a_1] = \hat\theta([[y,x],x]) = \hat\theta(x^2) = a_1^2 = a_3$ forces $a_3 = 1$
  - $(xyx)^4, x^4, y^4$ impose no conditions
  - $a_1a_3 = \hat\theta((yx)^3y) = \hat\theta(x) = a_1$ also forces $a_3 = 1$
- construct $G/P_2(G)$ as $H^*/\langle a_3\rangle$; after renaming a_4, a_5:

$$G/P_2(G) \cong \mathrm{Pc}\langle a_1,\ldots,a_4 \mid a_1^2 = 1, a_2^2 = a_4, [a_2,a_1] = a_3,\ a_3^2 = a_4^2 = 1\rangle$$

  and epimorphism $G \to G/P_2(G)$ defined by $(x,y) \to (a_1,a_2)$.

Big example: p-quotient algorithm in action

$G/P_2(G) = \mathrm{Pc}\langle a_1,\ldots,a_4 \mid a_1^2 = 1, a_2^2 = a_4, [a_2,a_1] = a_3,\ a_3^2 = a_4^2 = 1\rangle$

Second round:

- construct covering of $H = G/P_2(G)$ by adding new generators and tails:

$$\begin{aligned} H^* = \mathrm{Pc}\langle a_1,\ldots,a_{12} \mid\ & a_1^2 = a_{12}, a_2^2 = a_4, a_3^2 = a_{11}, a_4^2 = a_{10}, \\ & [a_2,a_1] = a_3, [a_3,a_1] = a_5, [a_3,a_2] = a_6, [a_4,a_1] = a_7, \\ & [a_4,a_2] = a_8, [a_4,a_3] = a_9,\ a_5^2 = \ldots = a_{12}^2 = 1\rangle \end{aligned}$$

- the consistency algorithm shows only the following inconsistencies:
  - $a_2(a_2a_2) = a_2a_4$ and $(a_2a_2)a_2 = a_4a_2 = a_2a_4a_8$ $\Longrightarrow \boldsymbol{a_8 = 1}$
  - $a_2(a_1a_1) = a_2a_{12}$ and $(a_2a_1)a_1 = a_1a_2a_3a_1 = \ldots = a_2a_5a_{11}a_{12}$ $\Longrightarrow \boldsymbol{a_5a_{11} = 1}$
  - $a_2(a_2a_1) = a_1a_2^2a_3^2a_6 = a_1a_4a_6a_{11}$ and $(a_2a_2)a_1 = a_1a_4a_7$ $\Longrightarrow \boldsymbol{a_6a_7a_{11} = 1}$
  - $a_3(a_2a_2) = a_3a_4$ and $(a_3a_2)a_2 = a_2a_3a_6a_2 = a_2^2a_3a_6^2 = a_3a_4a_9$ $\Longrightarrow \boldsymbol{a_9 = 1}$
- removing redundant gens (and renaming), we obtain the consistent wpcp

$$\begin{aligned} H^* = \mathrm{Pc}\langle a_1,\ldots,a_8 \mid\ & a_1^2 = a_8, a_2^2 = a_4, a_3^2 = a_7, a_4^2 = a_6,\ a_5^2 = \ldots = a_8^2 = 1 \\ & [a_2,a_1] = a_3, [a_3,a_1] = a_7, [a_3,a_2] = a_5a_7, [a_4,a_1] = a_5\rangle \end{aligned}$$

Big example: p-quotient algorithm in action

Still second round:

- $G = \langle x, y \mid [[y,x],x] = x^2, (xyx)^4, x^4, y^4, (yx)^3 y = x\rangle$ and $p = 2$;
- epimorphism $\theta\colon G \to H$ onto $H = G/P_2(H)$ defined by $(x,y) \to (a_1, a_2)$
- $H^* = \mathrm{Pc}\langle a_1, \ldots, a_8 \mid a_1^2 = a_8, a_2^2 = a_4, a_3^2 = a_7, a_4^2 = a_6,\ a_5^2 = \ldots = a_8^2 = 1$
  $[a_2,a_1] = a_3, [a_3,a_1] = a_7, [a_3,a_2] = a_5a_7, [a_4,a_1] = a_5\rangle$

Evaluate relations of G in H^*:

- $a_7 = [[a_2,a_1],a_1] = \hat\theta([[y,x],x]) = \hat\theta(x^2) = a_1^2 = a_8$ forces $a_7 = a_8$
- $(xyx)^4$ forces $a_6 = 1$; x^4 and y^4 impose no condition
- $\hat\theta((yx)^3 y) = \hat\theta(x)$ forces $a_7a_8 = 1$

Now construct $G/P_3(G)$ as $H^*/\langle a_7a_8, a_6\rangle$; after renaming:

$$G/P_3(G) = \mathrm{Pc}\langle a_1, \ldots, a_6 \mid a_1^2 = a_6, a_2^2 = a_4, a_3^2 = a_6, a_4^2 = 1,\ a_5^2 = a_6^2 = 1,$$
$$[a_2,a_1] = a_3, [a_3,a_1] = a_6, [a_3,a_2] = a_5a_6, [a_4,a_1] = a_5\rangle$$

and the epimorphism $G \to G/P_3(G)$ is defined by $(x,y) \to (a_1,a_2)$.

Big example: p-quotient algorithm in action

In conclusion:
We started with

$$G = \langle x, y \mid [[y,x],x] = x^2, (xyx)^4, x^4, y^4, (yx)^3 y = x\rangle$$

and computed $G/P_3(G)$ as

$$\mathrm{Pc}\langle a_1, \ldots, a_6 \mid a_1^2 = a_6,\ a_2^2 = a_4,\ a_3^2 = a_6,\ a_4^2 = a_5^2 = a_6^2 = 1,$$
$$[a_2,a_1] = a_3, [a_3,a_1] = a_6, [a_3,a_2] = a_5a_6, [a_4,a_1] = a_5\rangle$$

with epimorphism $G \to G/P_3(G)$ defined by $(x,y) \to (a_1,a_2)$.

One can check that $|G| = |G/P_3(G)| = 2^6$, hence $G \cong G/P_3(G)$.

In particular, we have found a consistent wpcp for G.

In general: if our input group is a finite p-group, then the p-quotient algorithm constructs a consistent wpcp of that group.

Motivation and Application: Burnside problem

Burnside Problems

- **Generalised Burnside Problem** (GBP), 1902:
  Is every finitely generated torsion group finite?
- **Burnside Problem** (BP), 1902:
  Let $B(d,n)$ be the largest d-generator group with $g^n = 1$ for all $g \in G$.
  Is this group finite? If so, what is its order?
- **Restricted Burnside Problem** (RBP), ∼1940:
  What is order of largest finite quotient $R(d,n)$ of $B(d,n)$, if it exists?

- Golod-Šafarevič (1964): answer to GBP is "no";
  (cf. Ol'shanskii's Tarski monster)
- Various authors: $B(d,n)$ is finite for $n = 2,3,4,6$, but in no other cases with $d > 1$ is it known to be finite; is $B(2,5)$ finite?
- Higman-Hall (1956): reduced (RBP) to prime-power n.
- Zel'manov (1990-91): $R(d,n)$ always exists! (**Fields medal 1994**)

Motivation and Application: Burnside problem

Burnside groups:

- $B(d,n) = \langle x_1,\ldots,x_d \mid g^n = 1 \text{ for all words } g \text{ in } x_1,\ldots,x_n\rangle$
- $R(d,n)$ largest finite quotient of $B(d,n)$; exists by Zel'manov

Recall: the p-quotient algorithm computes a consistent wpcp of the largest p-class k quotient (if it exists) of any finitely presented group.

Implementations of the p-quotient algorithm have been used to determine the order and compute pcp's for various of these groups.

Group	Order	Authors
$B(3,4)$	2^{69}	Bayes, Kautsky & Wamsley (1974)
$R(2,5)$	5^{34}	Havas, Wall & Wamsley (1974)
$B(4,4)$	2^{422}	Alford, Havas & Newman (1975)
$R(3,5)$	5^{2282}	Vaughan-Lee (1988); Newman & O'Brien (1996)
$B(5,4)$	2^{2728}	Newman & O'Brien (1996)
$R(2,7)$	7^{20416}	O'Brien & Vaughan-Lee (2002)

Conclusion Lecture 2

Things we have discussed in the second lecture:

- lower exponent-p series, p-class
- p-quotient algorithm
- p-cover H^* (definition, pcp, consistent pcp)
- application: Burnside problems

p-group generation

Go to p-Quotient Algorithm
Go to Classification

Conclusion Lecture 2

Things we have discussed in the second lecture:

- the lower exponent-p series of a group G of p-class c is

$$G = P_0(G) > P_1(G) > \ldots > P_c(G) = 1$$

  where $P_{i+1}(G) = [G, P_i(G)]P_i(G)^p$; in particular, $P_1(G) = \Phi(G)$
- p-quotient algorithm: construct consistent wpcp of largest p-class c quotient of a finitely presented group (if it exists)
- if H has rank d and $H \cong F/R$ with F free of rank d, then the p-cover H^* is isomorphic to F/R^* where $R^* = [F, R]R^p$
- application: Burnside problems

Today: the p-group generation algorithm!

p-group generation: descendants

Idea: Constructing new p-groups from old ones!

Descendants of p-groups

Let G be a d-generator p-group of p-class c.
A **descendant** of G is a d-generator p-group H with $H/P_c(H) \cong G$; it is an **immediate descendant** if H has p-class $c+1$, that is, $P_c(H) > P_{c+1}(H) = 1$.

Example 18

The group $G = C_2 \times C_2$ has 2-class $c = 1$.

The 2-class of $D_8 = \langle x_1, x_2, x_3 \mid x_1^2,\ x_2^2 = x_3,\ x_3^2,\ [x_2, x_1] = x_3 \rangle$ is 2.
Since $D_8/P_1(D_8) \cong G$, the group D_8 is an immediate descendant of G.

The group D_{16} has 2-class 3 and satisfies $D_{16}/P_1(D_{16}) \cong C_2 \times C_2$.
Thus D_{16} is a descendant of G, but not an immediate descendant.

Every p-group K of p-class $c > 1$ is an immediate descendant of $K/P_{c-1}(K)$; if $c = 1$, then $K \cong C_p^d$ is elementary abelian.

p-group generation: p-covering

Given: a d-generator p-group G of p-class c.
Want: list of all immediate descendants H of G (up to isomorphism)
Fact: each $H/P_c(H) \cong G$ and $P_c(H)$ is H-central elementary abelian.

Recall Theorem 13: If H is a d-generator p-group with $H/Z \cong G$ for some central elementary abelian $Z \leq H$, then H is a quotient of the p-cover G^*.

Theorem 19
Every immediate descendant of G is a quotient of the p-cover G^*.

In the following we discuss the p-**group generation algorithm**:

p-group generation algorithm
Input: a p-group G and description of its automorphism group
Output: wpcp's of all immediate descendants of G, up to isomorphism, and a description of their automorphism groups

Descriptions of the algorithm in the literature: Newman (1977), O'Brien (1999)

p-group generation: allowable subgroups

In the following: $G = F/R$ with p-class c, and $G^* = F/R^*$ with $R^* = [R,F]R^p$.

Problem: What quotients of G^* are immediate descendants of G?

Definition

- The p-**multiplicator** of G is the kernel of $G^* \to G$, that is, R/R^*.
- The **nucleus** of G is $P_c(G^*)$; note that $P_c(G^*) \leq R/R^*$.
- If H is an immediate descendant, then there is an epi $G^* \to H$ whose kernel lies in R/R^*. An **allowable subgroup** is a subgroup $Z < R/R^*$ such that G^*/Z is an immediate descendant of G.

The next lemma characterises allowable subgroups:

Lemma 20
A subgroup $Z < R/R^*$ is allowable if and only if $ZP_c(G^*) = R/R^*$.

Thus: $Z < R/R^*$ is allowable if and only if it supplements the nucleus.

p-group generation: allowable subgroups

Recall: $G = F/R$ with p-class c, and $G^* = F/R^*$ with $R^* = [R, F]R^p$.

Lemma 20

A subgroup $Z < R/R^*$ is allowable if and only if $ZP_c(G^*) = R/R^*$.

Proof.

If $Z = M/R^\star$ is allowable, then F/M is an immediate descendant, and so $G \cong (F/M)/(P_c(F)M/M)$. We also know that $G = F/R \cong (F/M)/(R/M)$ by the isomorphism theorem. Since $P_c(G) = P_c(F)R/R = 1$, we have $P_c(F)M \leq R$. Together, it follows that $R = P_c(F)M$, and so $R/R^\star = P_c(G^*)Z$, as claimed.

Conversely, if $Z = M/R^\star$ satisfies $R/R^* = ZP_c(G^*) = MP_c(F)/R^*$, then $R = MP_c(F)$; factoring out M yields $R/M = P_c(F)M/M$.
This shows that $H = G^*/Z = F/M$ satisfies $P_c(H) = P_c(F)M/M = R/M$, so $H/P_c(H) = F/R = G$ and H is immed. desc. since $P_c(H) > P_{c+1}(H) = 1$.

p-Group Generation Algorithm | Descendants | Allowable Subgroups | Isomorphism Problem | Algorithm | Example

p-group generation: allowable subgroups

Example 21

The group $G = D_{16}$ has p-class $c = 3$ and 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_7 \mid a_1^2 = a_6,\ a_2^2 = a_3a_4a_7,\ a_3^2 = a_4a_5,\ a_4^2 = a_5,\ [a_2, a_1] = a_3,\ [a_3, a_1] = a_4,\ [a_4, a_1] = a_5,\ a_5^2 = a_6^2 = a_7^2 = 1\rangle.$$

The multiplicator is $\langle a_5, a_6, a_7\rangle \cong C_2^3$; the nucleus is $P_c(G^*) = \langle a_5\rangle$.

The subgroups $\langle a_6, a_7\rangle$, $\langle a_5a_6, a_7\rangle$, $\langle a_6, a_5a_7\rangle$ are allowable and the corresponding immediate descendants have order 32.

The subgroup $\langle a_5a_6, a_5a_7\rangle$ is also allowable, but the resulting quotient is isomorphic to the quotient of G^* by $\langle a_6, a_5a_7\rangle$.

Considering the factor groups of G^* by all allowable subgroups, a *complete* list of immediate descendants is obtained; this list usually contains isomorphic groups.

p-group generation: isomorphism problem

Recall: $G = F/R$ with p-cover $G^* = F/R^*$ and multiplicator R/R^*.

Equivalence of allowable subgroups

Two allowable subgroups U/R^* and V/R^* are **equivalent** if the corresponding immediate descendants F/U and F/V are isomorphic.

This definition of "equivalence" is useful ...

...only because the equivalence relation can be given a different characterisation by using the automorphism group of G.

p-group generation: isomorphism problem

Extended automorphism

Let $\alpha \in \mathrm{Aut}(G)$; suppose $G = F/R$ is generated by $a_1, a_2, \ldots, a_d$.
For $i = 1, \ldots, d$, let $x_i, y_i \in F$ such that $a_i = x_i R$ and $\alpha(a_i) = y_i R$ for all i.
Define $\alpha^* \colon G^* \to G^*$ by $\alpha^*(x_i R^*) = y_i R^*$ for all i.

Lemma 22

If $\alpha \in \mathrm{Aut}(G)$, then $\alpha^* \in \mathrm{Aut}(G^*)$ is an **extended automorphism**.
It is not uniquely defined by α, but its restriction to R/R^* is.

Proof [Sketch].
First show that α^* is a well-defined homomorphism; let $g = w(x_1, \ldots, x_d) \in F$:
If $g \in R$, then $1R = \alpha(gR) = w(y_1, \ldots, y_d)R$, so $w(y_1, \ldots, y_d) \in R$.
So if $g \in R^*$, then $w(y_1, \ldots, y_d) \in R^*$; recall $R^* = [F, R]R^p$.
The hom α^* is surjective: $G^* = \langle y_1 R^*, \ldots, y_d R^* \rangle$ since $R/R^* \leq \Phi(G^*)$.

Two extensions of α differ only by elements in R/R^*, and words in R are products of p-th powers and commutators. Since R/R^* is elementary abelian and central, the restriction of α^* to R/R^* is uniquely defined by α.

p-group generation: isomorphism problem

Lemma 23

Let $G = F/R$ be as before, and let U/R^* and V/R^* be allowable subgroups. Then $F/U \cong F/V$ if and only if $\alpha^*(U/R^*) = V/R^*$ for some $\alpha \in \text{Aut}(G)$.

Proof [Sketch].

"$\Rightarrow$". Let $\varphi\colon F/U \to F/V$ be an isomorphism. Since F/U is an immed. desc., $(F/U)/P_c(F/U) = G$, and so $P_c(F/U) = R/U$; similarly, $P_c(F/V) = R/V$, and so $\varphi(R/U) = R/V$. Thus φ induces $\alpha \in \text{Aut}(G)$ with extension $\alpha^* \in \text{Aut}(G^*)$. Now we show that $\alpha^*(U/R^*) = V/R^*$: if $g = w(x_1, \ldots, x_d) \in U$, then

$$1V = \varphi(gU) = w(\varphi(x_1U), \ldots, \varphi(x_dU)) = w(y_1V, \ldots, y_dV) = w(y_1, \ldots, y_d)V,$$

which implies $\alpha^*(gR^*) = w(y_1, \ldots, y_d)R^* \in V/R^*$, and so $\alpha^*(U/R^*) = V/R^*$.

"$\Leftarrow$". If H is a group, $N \trianglelefteq H$, and $\gamma \in \text{Aut}(H)$, then $H/N \cong H/\gamma(N)$. This shows that if $\alpha^* \in \text{Aut}(G^*)$ maps U/R^* to V/R^*, then $F/U \cong F/V$.

Via α^*, every $\alpha \in \text{Aut}(G)$ yields a unique permutation $\pi(\alpha)$ of allowable subgrps.

p-group generation: automorphisms

Given: $G = F/R$ and immediate desc. $H = F/M$ for some allowable M/R^*

Want: automorphisms of H, that is, *isomorphisms* $F/M \to F/M$

Recall: every $\alpha \in \text{Aut}(G)$ yields a permutation $\pi(\alpha)$ of allowable subgrps.

Let Σ be the stabiliser of M/R^* under the action of $\text{Aut}(G)$, that is,

$$\Sigma = \langle \zeta \in \text{Aut}(G) \mid \pi(\zeta) \text{ stabilises } M/R^* \rangle.$$

Use Σ to compute

$$S = \langle \zeta^*|_{F/M} \mid \zeta \in \Sigma \rangle \leq \text{Aut}(H),$$

and determine a generating set for

$$T = \langle \beta \in \text{Aut}(H) \mid \beta|_G = \text{id}_G \rangle.$$

Theorem 24

Using the previous notation, $\text{Aut}(H) = \langle S, T, \text{Inn}(H) \rangle$.

(see O'Brien, 1999)

p-group generation: the algorithm

p-**group-generation**(G, A, s)

Input: group $G = F/R$ of order p^n, its automorphism group A, integer $s \in \mathbb{N}$
Output: immediate descendants of G, up to isomorphism, of order p^{n+s}, and their automorphism groups

```
construct consistent wpcp of covering G* = F/R*
for each generator α of A do
    compute extension α*
    compute permutation π(α) of allowable subgroups of index p^s in R/R*
compute orbits of these allowable subgroups under the action of all π(α)
for each orbit representative Z = M/R* do
    compute a wpcp of the immediate descendant H = G*/Z ≅ F/M
    compute generators of the automorphism group of H
```


p-group generation: example

Consider $G = \mathrm{Pc}\langle a_1, a_2 \mid a_1^2 = a_2^2 = 1\rangle$ with 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

The multiplicator and nucleus coincide: $M = \langle a_3, a_4, a_5\rangle = P_1(G^*)$.

Thus: every proper subgroup of M is allowable.

Note that $\mathrm{Aut}(G) \cong \mathrm{GL}_2(2)$, with generators and extensions

$$\alpha_1\colon (a_1, a_2) \mapsto (a_1a_2, a_2) \qquad \alpha_1^*\colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_1a_2, a_2, a_3, a_3a_4a_5, a_5)$$
$$\alpha_2\colon (a_1, a_2) \mapsto (a_2, a_1) \qquad \alpha_2^*\colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_2, a_1, a_3, a_5, a_4).$$

For example, observe that

$$\alpha_1^*(a_3) = \alpha_1^*([a_1, a_2]) = [a_1a_2, a_2] = a_3$$
$$\alpha_1^*(a_4) = \alpha_1^*(a_1^2) = (a_1a_2)^2 = a_1^2a_2^2a_3 = a_3a_4a_5$$
$$\alpha_1^*(a_5) = \alpha_1^*(a_2^2) = a_2^2 = a_5$$

p-group generation: example

Consider $G = \mathrm{Pc}\langle a_1, a_2 \mid a_1^2 = a_2^2 = 1\rangle$ with 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

The multiplicator and nucleus coincide: $M = \langle a_3, a_4, a_5\rangle = P_1(G^*)$.

Thus: every proper subgroup of M is allowable.

Note that $\mathrm{Aut}(G) \cong \mathrm{GL}_2(2)$, with generators and extensions

$\alpha_1 \colon (a_1, a_2) \mapsto (a_1a_2, a_2)$ $\quad\alpha_1^* \colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_1a_2, a_2, a_3, a_3a_4a_5, a_5)$

$\alpha_2 \colon (a_1, a_2) \mapsto (a_2, a_1)$ $\quad\alpha_2^* \colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_2, a_1, a_3, a_5, a_4)$.

Immediate descendants of $G = C_2 \times C_2$ of order 8:

There are 7 allowable subgroups of index 2 in M (that is, of rank 2), namely

$$\langle a_4, a_5\rangle,\ \langle a_4, a_3a_5\rangle,\ \langle a_3a_4, a_5\rangle,\ \langle a_3, a_5\rangle,\ \langle a_3, a_4a_5\rangle,\ \langle a_3, a_4\rangle,\ \langle a_3a_4, a_3a_5\rangle$$

There are 3 orbits of allowable subgroups induced by α_1^* and α_2^*:

$$\{\langle a_4, a_5\rangle, \langle a_4, a_3a_5\rangle, \langle a_3a_4, a_5\rangle\},\ \{\langle a_3a_4, a_3a_5\rangle\},\ \{\langle a_3, a_5\rangle, \langle a_3, a_4a_5\rangle, \langle a_3, a_4\rangle\}$$

p-group generation: example

Immediate descendants of $G = C_2 \times C_2$ of order 8

Recall that

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle$$

and allowable subgroups of rank 2 are

$$\{\langle a_4, a_5\rangle, \langle a_4, a_3a_5\rangle, \langle a_3a_4, a_5\rangle\}, \{\langle a_3a_4, a_3a_5\rangle\}, \{\langle a_3, a_5\rangle, \langle a_3, a_4a_5\rangle, \langle a_3, a_4\rangle\}.$$

Choose one rep from each orbit and factor it from G^* to obtain immediate descendants:

$$\mathrm{Pc}\langle a_1, a_2, a_3 \mid a_1^2 = a_2^2 = a_3^2,\ [a_2, a_1] = a_3\rangle \cong D_8$$
$$\mathrm{Pc}\langle a_1, a_2, a_3 \mid a_1^2 = a_3,\ a_2^2 = a_3,\ a_3^2 = 1,\ [a_2, a_1] = a_3\rangle \cong Q_8$$
$$\mathrm{Pc}\langle a_1, a_2, a_4 \mid a_1^2 = a_4,\ a_2^2 = a_4^2 = 1\rangle \cong C_2 \times C_4$$

p-group generation: example

Immediate descendants of $G = C_2 \times C_2$ of order 16

Recall that

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

Allowable subgroups of index 4 are $\langle a_3\rangle$, $\langle a_3^\delta a_4^\gamma a_5\rangle$, $\langle a_3^\zeta a_4\rangle$, with $\delta, \gamma, \zeta \in \{0, 1\}$. The orbits induced by α_1^* and α_2^* are

$$\{\langle a_3\rangle\},\ \ \{\langle a_5\rangle, \langle a_3 a_4 a_5\rangle, \langle a_4\rangle\},\ \ \{\langle a_4 a_5\rangle, \langle a_3 a_5\rangle, \langle a_3 a_4\rangle\}.$$

Choose one rep from each orbit to obtain 3 immediate descendants of order 16. Get $C_4 \times C_4$ and $C_2 \ltimes (C_2 \times C_4)$ and $C_4 \ltimes C_4$, for example,

$$G^*/\langle a_3\rangle = \mathrm{Pc}\langle\, a_1, a_2, a_4, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5, a_4^2 = a_5^2 = 1\rangle \cong C_4 \times C_4.$$

Immediate descendants of $G = C_2 \times C_2$ of order 32

There is one immediate descendant of order 2^5, namely G^*.

p-group generation: practical issues

Central problem: number of allowable subspaces (and size of orbits)

Example: The immediate descendants of $G = C_p^d$ of order p^{d+s} have p-class 2. For this group, $M = R/R^* = P_1(G^*)$ has rank $m = d(d+1)/2$; and each of the $O(p^{(m-s)s})$ subspaces of dim $m - s$ is allowable.

Approach: exploit characteristic structure.
Each $\alpha \in \mathrm{Aut}(G)$ acts on $M \leq G^*$ via $\alpha^* \in \mathrm{Aut}(G^*)$; so M is $\mathrm{Aut}(G)$-module.
In the example, $M = P_1(G^*) = (G^*)^2(G^*)'$ is a characteristic decomposition.
In general, identify characteristic submodules, then process chain of submodules.

More comments on practical issues: see O'Brien (1999)

Classifying p-groups

▸ Go to p-Group Generation

▸ Go to Isomorphisms

GNU: group number

How many groups of order p^n exist?

The number $\mathrm{gnu}(n)$ of groups of order n (up to isomorphism) has been studied in detail[5]; we recall a few bounds:

- **Pyber (1993):** $\mathrm{gnu}(n) \leq n^{(2/27+o(1))\mu(n)^2}$,
  where $\mu(n)$ is largest exponent in the prime-power factorisation of n.
  Idea: count choices for Sylow subgroups, Fitting subgroup, quotients, extensions,...
- **Higman (1960):** $\mathrm{gnu}(p^n) \geq p^{2/27(n^3-6n^2)}$
  Idea: count groups of p-class 2
- **Sims (1965), Newman & Seeley (2007):** $\mathrm{gnu}(p^n) \leq p^{2n^3/27+O(n^{5/3})}$
  Idea: enumerate presentations which define groups of order p^n
  Trivial bound: $\mathrm{gnu}(p^n) \leq p^{(n^3-n)/6}$

In conclusion: $p^{(2/27)n^3-O(n^2)} \leq \mathrm{gnu}(p^n) \leq p^{(2/27)n^3+O(n^{5/3})}$ as $n \to \infty$.

[5] Blackburn, Neuman, Venkataraman "Enumeration of finite groups", 2007

GNU: some 2-groups

Besche, Eick & O'Brien (2001) used 2-group generation:

order	#
1	1
2	1
4	2
8	5
16	14
32	51
64	267

order	#
128	2,328
256	56,092
512	10,494,213
1024	49,487,365,422
2048	>1,774,274,116,992,170

Number of groups of order ≤ 2000: 49,910,529,484
Number of groups of order 2^{10}: 49,487,365,422
Number of groups of order 2^{10} and class 2: 48,803,495,722

Folklore Conjecture
Almost all groups are 2-groups of 2-class 2.

GNU: p-groups of small order

Number of groups of order p^k, for $k = 1, 2, \ldots, 6$:

$\# \setminus p$	2	3	≥ 5
p	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	X
p^6	267	504	Y

where

$$X = 2p + 61 + 2\gcd(p-1,3) + \gcd(p-1,4)$$
$$Y = 3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5)$$

Order dividing p^4: Cole, Glover, Hölder, Young (all $\sim$ 1893)

Order p^5: Bagnera, Miller, de Séguier, James (1898-1980)

Order p^6: *many* faulty classifications;
eventually Newman, O'Brien, Vaughan-Lee (2004)

GNU: p-groups of small order

Number of groups of order p^7: O'Brien & Vaughan-Lee (2005) computed

# \ p	**2**	**3**	**5**	**≥ 7**
p^7	$2,328$	$9,310$	$34,297$	Z

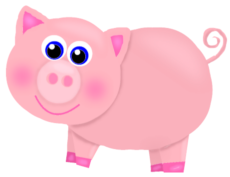
where

$$\begin{aligned} Z = {} & 3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 \\ & + (4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4) \\ & + (3p+31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9) \end{aligned}$$

Approach for $n = 5, 6, 7$:

- For $p < n$ use p-group generation.
- For $p \geq n$ use Baker-Campbell-Hausdorff formula and Lazard correspondence between category of nilpotent Lie rings of order p^n and category of p-groups of order p^n. Use analogue of p-group generation algorithm to classify the Lie rings.

GNU: PORC conjecture[6]



PORC Conjecture (Higman 1960)
For n fixed, $\mathrm{gnu}(p^n)$ is Polynomial On Residue Classes.

That is, there exists $m \in \mathbb{N}$ and polynomials $f_0, f_1, \ldots, f_{m-1}$ such that

$$\mathrm{gnu}(p^n) = f_{p \bmod m}(n).$$

Higman (1960): # groups of order p^n and p-class 2 is PORC.

Evseev (2008): # groups of order p^n whose Frattini subgroup is central is PORC.

Vaughan-Lee (2015): # groups of order p^8 and exponent p is PORC.

[6] For a survey see Vaughan-Lee "Graham Higman's PORC Conjecture" (2012)

Conclusion Lecture 3

Things we have discussed in the third lecture:

- (immediate) descendants
- p-group generation algorithm
- p-cover, nucleus, multiplicator, allowable subgroups, extended auts
- automorphism groups of immediate descendants
- the group number gnu for group order p^5, p^6, p^7
- PORC conjecture

Isomorphism testing

Go to Classifications
Go to Automorphisms

Conclusion Lecture 3

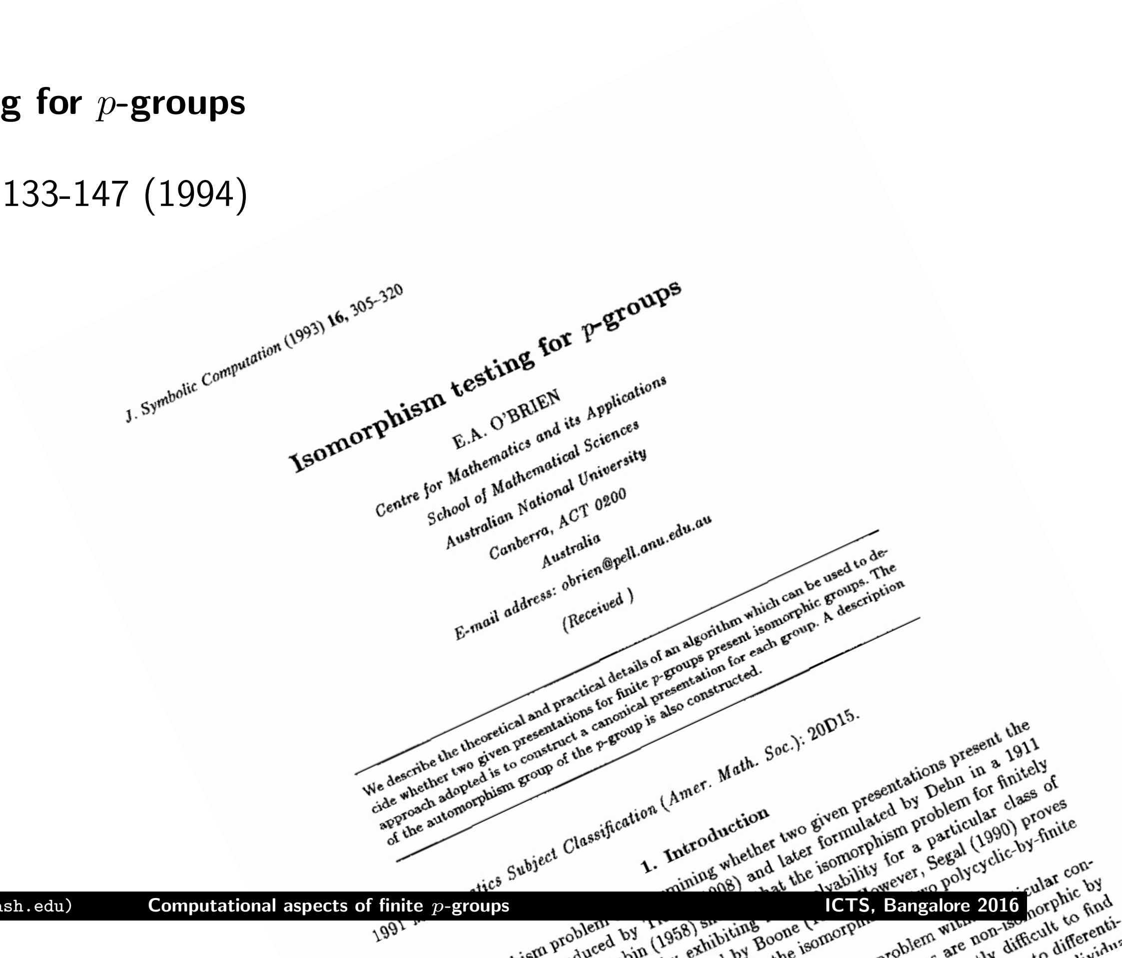
Things we have discussed in the third lecture:

- (immediate) descendants
- p-group generation algorithm
- p-cover, nucleus, multiplicator, allowable subgroups, extended auts
- automorphism groups of immediate descendants
- the group number gnu for group order p^5, p^6, p^7
- PORC conjecture

Isomorphism Testing | Standard Presentations | Example

Resources

Isomorphism testing for p-groups
E. A. O'Brien
J. Symb. Comp. 17, 133-147 (1994)



J. Symbolic Computation (1993) 16, 305–320

Isomorphism testing for p-groups

E.A. O'BRIEN
Centre for Mathematics and its Applications
School of Mathematical Sciences
Australian National University
Canberra, ACT 0200
Australia
E-mail address: obrien@pell.anu.edu.au

(Received)

We describe the theoretical and practical details of an algorithm which can be used to decide whether two given presentations for finite p-groups present isomorphic groups. The approach adopted is to construct a canonical presentation for each group. A description of the automorphism group of the p-group is also constructed.

... Subject Classification (Amer. Math. Soc.): 20D15.

1. Introduction

Standard Presentations

Problem: Decide whether two p-groups are isomorphic.

Standard presentation

For a p-group G use methods from the p-quotient and p-group generation algorithms to construct a **standard pcp** (std-pcp) for G, such that $G \cong H$ if and only if G and H have the same std-pcp.

Example: For each $j = 1, \ldots, p-1$ the presentation

$$\mathrm{Pc}\langle a_1, a_2 \mid a_1^p = a_2^j,\ a_2^p = 1\rangle$$

is a wpcp describing C_{p^2}; as a std-pcp one could choose

$$\mathrm{Pc}\langle a_1, a_2 \mid a_1^p = a_2,\ a_2^p = 1\rangle.$$

Similarly, a std-pcp for C_p^d is $\mathrm{Pc}\langle a_1, \ldots, a_d \mid a_1^p = \ldots = a_d^p = 1\rangle$.

Isomorphism test: computing std-pcp's

Let G be d-generator p-group of p-class c.
Std-pcp of $G/P_1(G)$ is $\mathrm{Pc}\langle a_1, \ldots, a_d \mid a_1^p = \ldots = a_d^p = 1\rangle$.

Suppose $H \cong G/P_k(G)$ with $k < c$ is defined by std-pcp; have $\theta\colon G \to G/P_k(G)$.

Find std-pcp of $G/P_{k+1}(G)$ using p-group generation:

The p-group generation algorithm constructs immediate descendants of H. Among these immediate descendants is $K \cong G/P_{k+1}(G)$. Proceed as follows:

- let $H \cong F/R$ (defined by std-pcp) and $H^* \cong F/R^*$;
- *evaluate relations* in H^* to get allowable M/R^* with $F/M \cong G/P_{k+1}(G)$;
- recall: $\alpha \in \mathrm{Aut}(H)$ acts as $\alpha^* \in \mathrm{Aut}(H^*)$ on allowable subgroups; two allowable U/R^* and V/R^* are in same $\mathrm{Aut}(H)$-orbit iff $F/U \cong F/V$; the choice of orbit rep determines the pcp obtained, and two elements from the same orbit determine different pcp's for isomorphic groups;
- associate with each allowable subgroup a unique *label*: a positive integer which runs from one to the number of allowable subgroups;
- let $\overline{M}/R^*$ be the element in the $\mathrm{Aut}(H)$-orbit of M/R^* with label 1.

Now $K = F/\overline{M}$ is isomorphic to $G/P_{k+1}(G)$; the pcp defining K is “standard”.

Isomorphism test: example of std-pcp

The group

$$G = \langle x, y \mid (xyx)^3, x^{27}, y^{27}, [x,y]^3, (xy)^{27}, [y, x^3], [y^3, x] \rangle;$$

has order 3^7, rank 2, and 3-class 3; let $\mathcal{S}_1$ be the set of relators.

- $G/P_1(G)$ has std-pcp $H = \mathrm{Pc}\langle a_1, a_2 \mid a_1^3 = a_2^3 = 1 \rangle$, and we have an epimorphism $\theta\colon G \to H$ with $x, y \mapsto a_1, a_2$.
- use the p-quotient algorithm to construct covering

$$H^* = \mathrm{Pc}\langle\, a_1, \ldots, a_5 \mid [a_2, a_1] = a_3,\ a_1^3 = a_4,\ a_2^3 = a_5,\ a_3^3 = a_4^3 = a_5^3 = 1 \,\rangle.$$

- evaluate $\mathcal{S}_1$ in H^* via $\hat{\theta}$ to determine the allowable subgroup $U/R^* = \langle a_4^2 a_5 \rangle$ which must be factored from H^* to obtain $G/P_2(G)$, that is, F/U is isomorphic to $G/P_2(G)$ with wpcp

$$\mathrm{Pc}\langle a_1, \ldots, a_4 \mid [a_2, a_1] = a_3,\ a_1^3 = a_2^3 = a_4,\ a_3^3 = a_4^3 = 1 \rangle.$$

Isomorphism test: example of std-pcp

Recall:

$$\begin{aligned} H &= \mathrm{Pc}\langle a_1, a_2 \mid a_1^3 = a_2^3 = 1 \rangle; \\ H^* &= \mathrm{Pc}\langle\, a_1, \ldots, a_5 \mid [a_2, a_1] = a_3,\ a_1^3 = a_4,\ a_2^3 = a_5,\ a_3^3 = a_4^3 = a_5^3 = 1 \,\rangle, \end{aligned}$$

with 3-multiplicator $M = \langle a_3, a_4, a_5 \rangle$.

- A generating set for the automorphism group $\mathrm{Aut}(H) \cong \mathrm{GL}_2(3)$ is

$$\alpha_1 : \begin{array}{lcl} a_1 & \longmapsto & a_1 a_2^2, \\ a_2 & \longmapsto & a_1^2 a_2^2 \end{array} \quad \alpha_2 : \begin{array}{lcl} a_1 & \longmapsto & a_1, \\ a_2 & \longmapsto & a_1^2 a_2 \end{array} \quad \alpha_3 : \begin{array}{lcl} a_1 & \longmapsto & a_1^2 \\ a_2 & \longmapsto & a_2 \end{array}$$

- Note that

$$\begin{aligned} \alpha_1^*(a_3) &= \alpha_1^*([a_2, a_1]) = [a_1^2 a_2^2, a_1 a_2^2] = \ \ldots = a_3 \\ \alpha_1^*(a_4) &= \alpha_1^*(a_1^3) = (a_1 a_2^2)^3 = \ \ldots = a_4 a_5^2 \\ \alpha_1^*(a_5) &= \alpha_1^*(a_2^3) = (a_1^2 a_2^2)^3 = \ \ldots = a_4^2 a_5^2 \end{aligned}$$

so the matrices representing the action of α_i^* on M are

$$\begin{pmatrix} 1&0&0\\0&1&2\\0&2&2 \end{pmatrix}, \quad \begin{pmatrix} 1&0&0\\0&1&0\\0&2&1 \end{pmatrix}, \quad \begin{pmatrix} 2&0&0\\0&2&0\\0&0&1 \end{pmatrix}.$$

Isomorphism test: example of std-pcp

Recall that

$$H^* = \mathrm{Pc}\langle\, a_1,\ldots,a_5 \mid [a_2,a_1]=a_3, a_1^3=a_4, a_2^3=a_5,\ a_3^3=a_4^3=a_5^3=1\,\rangle,$$

and $G/P_2(G) \cong F/U$ for the subspace $U/R^* = \langle a_4a_5^2\rangle$, which is $\langle(0,1,2)\rangle$

- The Aut(H)-orbit containing U/R^* is

$$\{\langle a_5\rangle, \langle a_4a_5\rangle, \langle a_4^2a_5\rangle, \langle a_4\rangle\}.$$

- The orbit rep with label 1 is ... $\bar{U}/R^* = \langle a_5\rangle$.
- Factor H^* by $\langle a_5\rangle$ to obtain the std-pcp for $G/P_2(G)$ as

$$K = \mathrm{Pc}\langle a_1,\ldots,a_4 \mid [a_2,a_1]=a_3,\ a_1^3=a_4,\ a_1^3=\ldots=a_4^3=1\rangle.$$

Recall that U/R^* was found by evaluating the relations $\mathcal{S}_1$ of G.
But: for the std-pcp we factored out $\bar{U}/R^* = \delta(U/R^*)$ for some $\delta \in$ Aut(H^*).
For the next iteration we need to modify the set of relations $\mathcal{S}_1$ accordingly.

Isomorphism test: example of std-pcp

- An extended automorphism which maps $U/R^* = \langle a_4a_5^2\rangle$ to $\bar{U}/R^* = \langle a_5\rangle$ is

$$\delta:\quad a_1 \longmapsto a_1a_2a_3a_4 = a_1a_2[a_2,a_1]a_1^3, \qquad a_2 \longmapsto a_1a_2^2$$

- Apply δ to $\mathcal{S}_1 = \{(xyx)^3, x^{27}, y^{27}, [x,y]^3, \ldots\}$ to obtain

$$\mathcal{S}_2 = \{(xy[y,x]x^3xy^2xy[y,x]x^3)^3,\ (xy[y,x]x^3)^{27},\ (xy^2)^{27},\ldots\};$$

  it follows that $G = \langle x,y \mid \mathcal{S}_1\rangle \cong \langle x,y \mid \mathcal{S}_2\rangle$, see O'Brien 1994.
- Now iterate with $G \cong \langle x,y \mid \mathcal{S}_2\rangle$ and the std-pcp of $K \cong G/P_2(G)$ to compute the std-pcp of $G/P_3(G) \cong G$.

Practical issues: need *complete orbit* to identify element with smallest label. One idea is to exploit the characteristic structure of the p-multiplicator (as before).

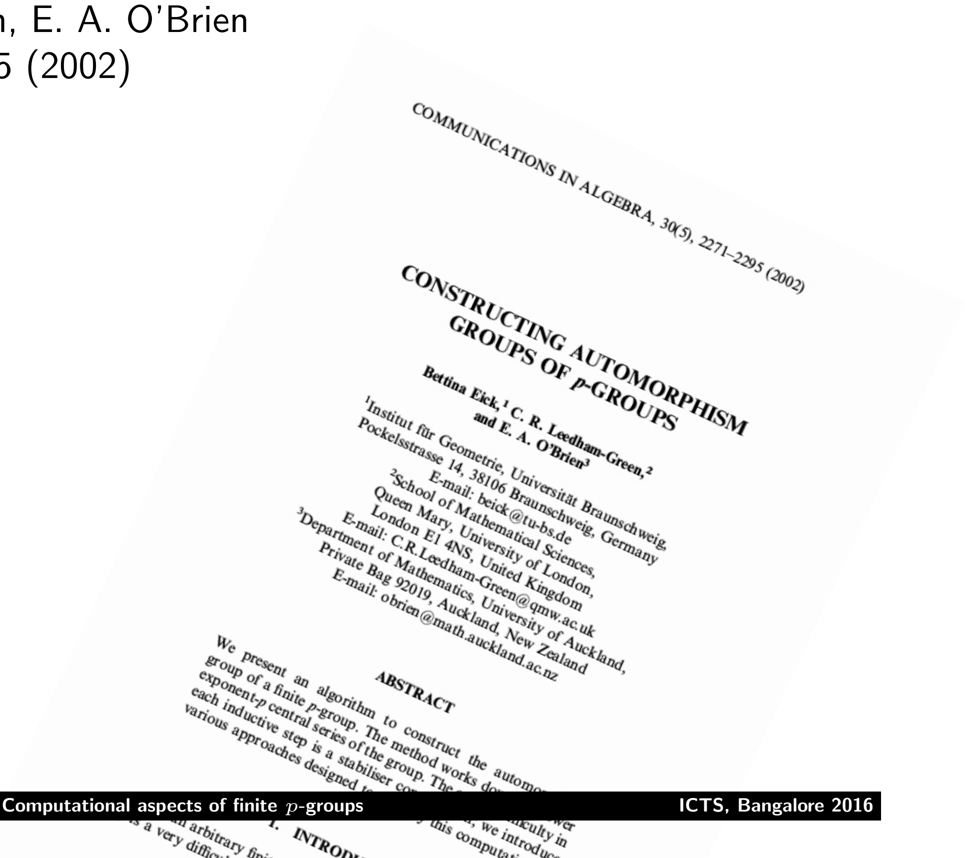
Note: The std-pcp is only "standard" because it has been computed by some deterministic rule. Std-pcps are a very efficient tool to partition sets of groups into isomorphism classes.

Automorphism groups

Go to Isomorphisms
Go to Coclass

Resources

Constructing automorphism groups of p-groups
B. Eick, C. R. Leedham-Green, E. A. O'Brien
Comm. Algebra 30, 2271-2295 (2002)


COMMUNICATIONS IN ALGEBRA, 30(5), 2271–2295 (2002)

CONSTRUCTING AUTOMORPHISM GROUPS OF p-GROUPS

Bettina Eick,[1] C. R. Leedham-Green,[2] and E. A. O'Brien[3]

[1]Institut für Geometrie, Universität Braunschweig, Pockelsstrasse 14, 38106 Braunschweig, Germany
E-mail: beick@tu-bs.de
[2]School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom
E-mail: C.R.Leedham-Green@qmw.ac.uk
[3]Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand
E-mail: obrien@math.auckland.ac.nz

ABSTRACT

Computing automorphism groups

Let G be a d-generator p-group with lower p-central series

$$G = P_0(G) > P_1(G) > \ldots > P_c(G) = 1.$$

In the following write $G_i = G/P_i(G)$.

We want to construct Aut(G).

Approach

Compute $\mathrm{Aut}(G) = \mathrm{Aut}(G_c)$ by induction on that series:

- $\mathrm{Aut}(G_1) = \mathrm{Aut}(C_p^d) \cong \mathrm{GL}_d(q)$
- construct $\mathrm{Aut}(G_{k+1})$ from $\mathrm{Aut}(G_k)$.

For the induction step use ideas from p-group generation.

Computing automorphism groups

Let $H = G_k$ and $K = G_{k+1}$; given $\mathrm{Aut}(H)$, compute $\mathrm{Aut}(K)$.

Recall from p-group generation:

- compute $H^* = F/R^*$ and the multiplicator $M = R/R^*$;
- determine allowable subgroup $U/R^* \leq M$ defining K, that is, $K \cong F/U$;
- each $\alpha \in \mathrm{Aut}(H)$ extends to $\alpha^* \in \mathrm{Aut}(H^*)$ which leaves M invariant; via this construction, $\mathrm{Aut}(H)$ acts on the set of allowable subgroups;
- let Σ be the stabiliser of U/R^* in $\mathrm{Aut}(H)$ under this action;
- every $\alpha \in \Sigma$ defines an automorphism of $F/U \cong K$; let $S \leq \mathrm{Aut}(K)$ be the subgroup induced by Σ;
- let $T \leq \mathrm{Aut}(K)$ be the kernel of $\mathrm{Aut}(K) \to \mathrm{Aut}(H)$.

Theorem

With the previous notation, $\mathrm{Aut}(K) = \langle S, T, \mathrm{Inn}(K) \rangle$.

For a proof see O'Brien (1999).

Computing automorphism groups

Recall from p-group generation:

- $H = G/P_k(G)$ and $K = G/P_{k+1}(G)$; we have $K/P_k(K) \cong H$;
- K is quotient of H^* by allowable subgroup U/R^*;
- $S \leq \mathrm{Aut}(K)$ induced by stabiliser Σ of U/R^* in $\mathrm{Aut}(H)$
- $T \leq \mathrm{Aut}(K)$ is kernel of $\mathrm{Aut}(K) \to \mathrm{Aut}(H)$;
- $\mathrm{Aut}(K) = \langle S, T, \mathrm{Inn}(K)\rangle$.

Problem: how to determine S and T efficiently?

Lemma

Let $\{g_1, \ldots, g_d\}$ and $\{x_1, \ldots, x_l\}$ be minimal generating sets for K and $P_k(K)$, respectively. Define

$$\beta_{i,j} \colon K \to K, \quad \begin{cases} g_i \mapsto g_i x_j \\ g_n \mapsto g_n \qquad (n \neq i). \end{cases}$$

Then $T = \langle \{\beta_{i,j} : 1 \leq i \leq d,\ 1 \leq j \leq l\}\rangle$, an elementary abelian p-group.

Main problem: Compute S, that is, the stabiliser Σ of U/R^* in $\mathrm{Aut}(H)$.

Induction step: example

Consider $G = \mathrm{Pc}\langle a_1, \ldots, a_4 \mid [a_2, a_1] = a_3, a_1^5 = a_4, a_2^5 = a_3^5 = a_4^5 = 1\rangle$;
this group has 5-class 2 with $P_1(G) = \langle a_3, a_4\rangle$.

Clearly, $H = G/P_1(G) = \mathrm{Pc}\langle a_1, a_2 \mid a_1^5 = a_2^5 = 1\rangle$ with $\mathrm{Aut}(H) \cong \mathrm{GL}_2(5)$.

Now compute:

- $H^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid [a_2, a_1] = a_3, a_1^5 = a_4, a_2^5 = a_5, a_3^5 = a_4^5 = a_5^5 = 1\rangle$
- the allowable subgroup $U/R^* = \langle a_5\rangle$ yields G as a quotient of H^*
- $\alpha_1 \colon (a_1, a_2) \mapsto (a_1^2, a_2)$ and $\alpha_2 \colon (a_1, a_2) \mapsto (a_1^4 a_2, a_1^4)$ generate $\mathrm{Aut}(H)$; their extensions act on the multiplicator $\langle a_3, a_4, a_5\rangle$ as
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 4 & 0 \end{pmatrix}$$
- the stabiliser Σ of U/R^* is generated by the extensions of α_1 and $\alpha_2\alpha_1\alpha_2^2$
- a generating set for T is $\{\beta_{1,4}, \beta_{2,4}, \beta_{1,3}, \beta_{2,3}\}$

This yields indeed $\mathrm{Aut}(G) = \langle T, S, \mathrm{Inn}(G)\rangle$, where S is induced by Σ

Stabiliser problem

To do: Compute stabiliser of allowable subgroup U/R^* under action of $\mathrm{Aut}(H)$.

Our set-up is:

- consider $M = R/R^*$ as $\mathrm{GF}(p)$-vectorspace and $V = U/R^*$ as subspace;
- represent the action of $\mathrm{Aut}(H)$ on M as a subgroup $A \leq \mathrm{GL}_m(p)$;
- compute the stabiliser of V in A.

Simple Approach: Orbit-Stabiliser Algorithm – constructs the whole orbit!

We'll briefly discuss the following ideas:

1. exploiting structure of M
2. exploiting structure of A
3. exploiting structure of K (and G)

Stabiliser problem: exploiting structure of M

Task: compute stabiliser of allowable subspace $V \leq M$ under A.

Idea: exploit the fact that $N = P_{k+1}(H^*) \leq M$ is characteristic in H^*, and that $M = NV$ (since V is allowable)

Use this to split stabiliser computation in two steps:

- compute the stabiliser of $V \cap N$ as subspace of N:

  use `MeatAxe` to compute composition series of N as A-module; then compute orbit and stabiliser of $V \cap N$ stepwise[7]

- compute orbit of $V/(V \cap N)$ as subspace of $M/(V \cap N)$:

  $V/(V \cap N)$ is complement to $N/(V \cap N)$ in $M/(V \cap N)$, and $N/(V \cap N)$ is A-invariant; compute A-module composition series of M/N and $N/(V \cap N)$ and break computation up in smaller steps

[7] see Eick, Leedham-Green, O'Brien (2002) for details

Stabiliser problem: exploiting structure of A

Task: compute stabiliser of allowable subspace $V \leq M$ under A.

Idea: Consider series $A \trianglerighteq S \trianglerighteq P \trianglerighteq 1$, where

- P induced by $\ker(H \to \mathrm{Aut}(H/P_1(H)))$, a normal p-subgroup
- S solvable radical, with $S = S_1 \triangleright \ldots \triangleright S_n \triangleright P$, each section prime order.

Schwingel Algorithm for stabiliser under p-group P

One can compute a "canonical" representative of V^P and generators for $\mathrm{Stab}_P(V)$ **without** enumerating the orbit; see E-LG-O'B (2002).

Next, compute $\mathrm{Stab}_A(V)$ along $S = S_1 \triangleright \ldots \triangleright S_n \triangleright P$, using the next lemma:

Lemma

Let L be a group acting on Ω; let $T \trianglelefteq L$ and let $\omega \in \Omega$.
Then ω^T is an L-block in Ω, and $\mathrm{Stab}_L(\omega^T) = T\mathrm{Stab}_L(\omega)$.

If $l \in \mathrm{Stab}_L(\omega^T)$, then $\omega^l = \omega^t$ for some $t \in T$, hence $lt^{-1} \in \mathrm{Stab}_L(\omega)$.

Stabiliser problem: exploiting structure of A

Compute $\mathrm{Stab}_A(V)$ along $S = S_1 \triangleright \ldots \triangleright S_n \triangleright P$, using the next lemma:

Lemma

Let L be a group acting on Ω; let $T \trianglelefteq L$ and $\omega \in \Omega$.
Then ω^T is an L-block in Ω, and $\mathrm{Stab}_L(\omega^T) = T\mathrm{Stab}_L(\omega)$.

If orbit V^{S_i} and stabiliser $\mathrm{Stab}_{S_i}(V)$ are known, compute $\mathrm{Stab}_{S_{i-1}}(V^{S_i})$, and extend each generator to an element in $\mathrm{Stab}_{S_{i-1}}(V)$.

Advantage: Reduce the number of generators of $\mathrm{Stab}_S(V)$ substantially

Stabiliser problem: exploiting structure of K (and G)

Recall: we aim to construct Aut(G) by induction on lower p-central series with terms $G_i = G/P_i(G)$; initial step is Aut$(G_1) \cong \mathrm{GL}_d(p)$

Idea: Aut(G) induces a subgroup $R \leq$ Aut(G_1); instead of starting with Aut(G_1), start with $L \leq \mathrm{GL}_d(p)$ such that $R \leq L$ and $[L : R]$ is small.

Approach:

- construct a collection of characteristic subgroups of G, such as: centre, derived group, Ω, 2-step centralisers,...
- restrict this collection to $G_1 = G/P_1(G)$
- Schwingel has developed an algorithm to construct the subgroup $R \leq$ Aut$(G_1) \cong \mathrm{GL}_d(p)$ stabilising this lattice of subspaces of G_1

This aproach frequently reduces to small subgroups of $\mathrm{GL}_d(p)$ as initial group.

Conclusion Lecture 4

Things we have discussed in the forth lecture:

- std-pcp, isomorphism test for p-groups
- automorphism group computation

Lecture 4 is also the last lecture on the ANUPQ algorithms:

ANUPQ (ANU-p-Quotient program), 22,000 lines of C code developed by O'Brien; providing implementations of

- p-quotient algorithm
- p-group generation algorithm
- isomorphism test for p-groups
- automorphisms of p-groups

Implementations are also available in GAP and Magma; various papers discuss the theory and efficiency of these algorithms.

What's the Greek letter for "p" ...?

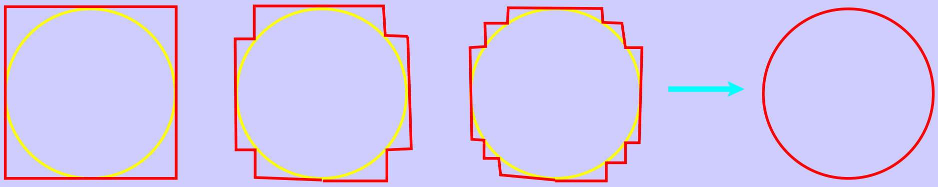
Automorphism Groups Algorithm Example Stabiliser Problem

π

Heiko Dietrich (heiko.dietrich@monash.edu) Computational aspects of finite p-groups ICTS, Bangalore 2016

"Theorem"
We have $\pi = 4$.

Proof.
We take a unit circle with diameter 1 and approximate its circumference (which is defined to be π) by computing its arc-length. Remember how arc-length is defined? Use a polygonal approximation!



In every iteration: cirumference is π, arc lenght of red curve is 4.
So in the limit: $\pi = 4$, as claimed.

Well . . . obviously that is wrong!

Everyone knows that the following is true . . .

"Theorem"
We have $\pi = 0$.

Proof.
We start with Euler's Identity $1 = e^{2\pi\imath}$, which yields $e = e^{2\pi\imath+1}$. Now observe:

$$e = e^{2\pi\imath+1} = \left(e^{2\pi\imath+1}\right)^{2\pi\imath+1} = e^{(2\pi\imath+1)^2} = e^{-4\pi^2} e e^{4\pi\imath}.$$

Since $e^{4\pi\imath} = 1$, this yields $1 = e^{-4\pi^2}$. Since $-4\pi^2 \in \mathbb{R}$, this forces $0 = -4\pi^2$.
Since $-4 \neq 0$, we must have $\pi = 0$, as claimed.

Coclass theory

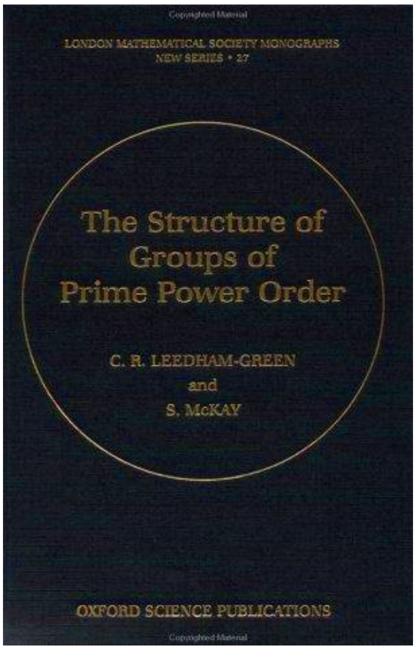
▸ Go to Automorphisms

▸ Go to End

Resources

The structure of groups of prime-power order
C. R. Leedham-Green, S. McKay
Oxford Science Publications (2002)

and some recent papers on coclass graphs
(Eick, Leedham-Green, Newman, O'Brien, D.)



Classifying p-groups by order

Recall:

order	#
1	1
2	1
4	2
8	5
16	14
32	51
64	267

order	#
128	2,328
256	56,092
512	10,494,213
1024	49,487,365,422
2048	$>$1,774,274,116,992,170

"*The precise structure of p-groups is too complex for the human intellect.*"
(Leedham-Green & McKay 2002)

Maximal class

Maximal class

A p-group G of order p^n has **maximal class** if it has nilpotency class $n-1$.

- Groups of maximal class have been investigated in detail. (Wiman 1954, Blackburn 1958, Leedham-Green & McKay 1976–1984, Fernández-Alcober 1995, Vera-López et al. 1995–2008)
- The 2- and 3-groups of maximal class are classified. (Blackburn: Description by finitely many *parametrised presentations*.)
- The 5-groups of maximal class are investigated in detail. (Leedham-Green & McKay, Newman 1990, D., Eick & Feichtenschlager 2007)
- For $p \geq 7$ such a classification is open.

Coclass

Maximal class is an important special case in **coclass theory**:

Coclass
A p-group G of order p^n and nilpotency class c has **coclass** $n - c$.

Thus:

- the p-groups of maximal class are the p-groups of coclass 1,
- coclass is an isomorphism invariant.

Strategy: Investigate the p-groups of a fixed coclass.
(Leedham-Green & Newman 1980)

Leedham-Green & Newman proposed five **Coclass Conjectures A–E** on the structure of the p-groups of a fixed coclass. Their proof was a first milestone in **coclass theory** and provided a deep insight in the structure of p-groups.

Coclass

Coclass Conjectures

Theorem A: There is a function $f(p, r)$ such that every p-group of coclass r has a normal subgroup of nilpotency class 2 and index at most $f(p, r)$.

Theorem B: There is a function $g(p, r)$ such that every p-group of coclass r has derived length at most $g(p, r)$.

Theorem C: Every pro-p group of coclass r is solvable.
($=$ inverse limit of finite p-groups of coclass r.)

Theorem D: There are only finitely many isomorphism types of infinite pro-p groups of coclass r.

Theorem E: There are only finitely many isomorphism types of solvable infinite pro-p groups of coclass r.

(Leedham-Green 1994, Shalev 1994)

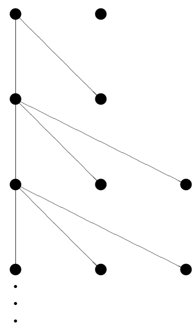
Coclass graph

Main approach since 1999: analyse **the coclass graph** $\mathcal{G}(p, r)$.

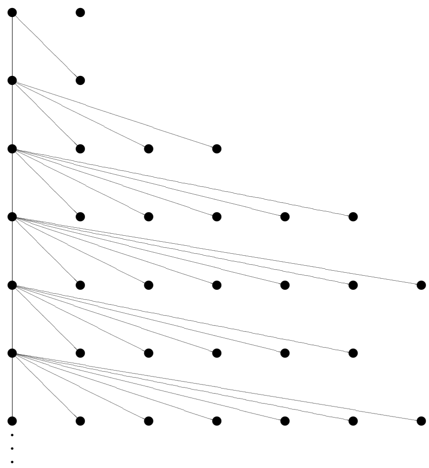
Vertices: Isomorphism type reps of finite p-groups of coclass r.

Edges: $G \to H$ if and only if $G \cong H/\gamma_{\mathrm{cl}(H)}(H)$; then $|H| = p|G|$.

Examples: $\mathcal{G}(2, 1)$ $\mathcal{G}(3, 1)$



D_{2^n} Q_{2^n} SD_{2^n}



Coclass graph

The infinite paths in $\mathcal{G}(p, r)$:

- There is 1-to-1 correspondence between the **infinite pro-p groups** of coclass r (up to isom.) and the *maximal* infinite paths in $\mathcal{G}(p, r)$.

It follows from the Coclass Theorems:

- The infinite paths are *well-understood* and finite in number!
- Only finitely many groups are not connected to an infinite path.

Number of infinite paths in $\mathcal{G}(p, r)$:

- p arbitrary and $r = 1$ (Blackburn): 1
- $p = 2$ and $r = 2, 3$ (Newman & O'Brien): 5, 54
- $p = 3$ and $r = 2, 3, 4$ (Eick): 16, ≥ 1271, ≥ 137299952383

Sorry!

We have to switch to the black board style because some figure are prepared for that...

Coclass Theory | Maximal Class | Coclass | Coclass Graph | Central Conjecture | Some results

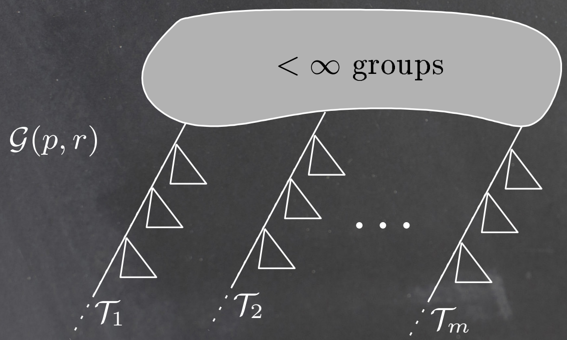
Sorry!

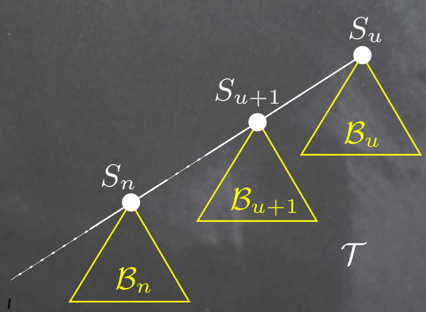
We have to switch to the black board style because some figure are prepared for that...

Heiko Dietrich (heiko.dietrich@monash.edu) Computational aspects of finite p-groups ICTS, Bangalore 2016

General structure of coclass graphs

$\mathcal{G}(p,r)$ can be partitioned into a finite subgraph and finitely many infinite trees each having a unique infinite path starting at its root.
These trees are the **coclass trees** of $\mathcal{G}(p,r)$.



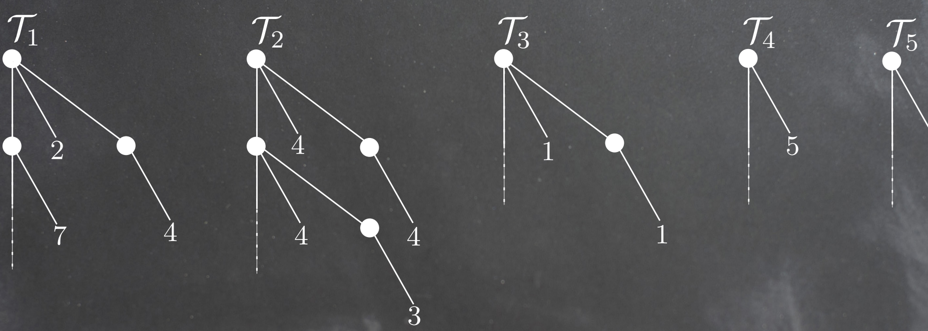


Let $\mathcal{T}$ be a coclass tree in $\mathcal{G}(p,r)$ with corresponding pro-p group S:

- The groups $S_n = S/\gamma_n(S)$ with $n \geq u$ form the **mainline** of $\mathcal{T}$.
- The finite subtrees $\mathcal{B}_n$ are the **branches** of $\mathcal{T}$.

The graph $\mathcal{G}(2,2)$

The five coclass trees of $\mathcal{G}(2,2)$:
(Newman & O'Brien 1996)

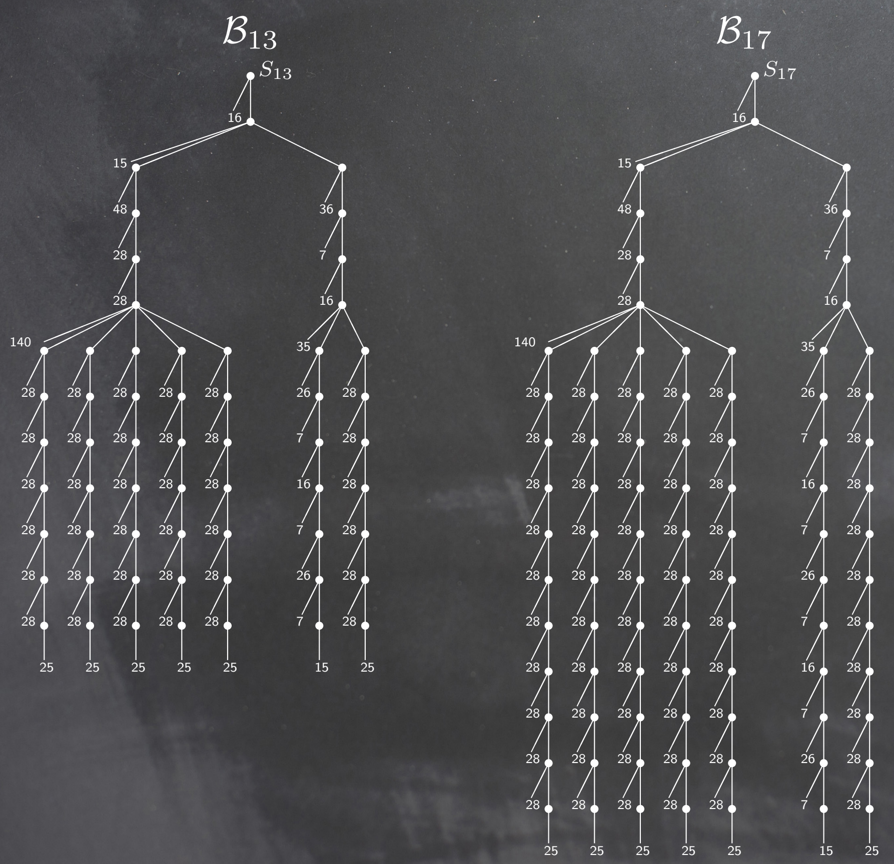


- The branches are isomorphic with periodicity 1 and 2, respectively.
- The roots have order $2^6, 2^6, 2^4, 2^4$, and 2^5, respectively.
- There are 19 groups which do not lie in any of these trees.

For arbitrary r: branches of trees in $\mathcal{G}(2,r)$ have *bounded depths*.

This does not hold for odd primes, except $(p,r) = (3,1)$.

Two branches in $\mathcal{G}(5,1)$



Based on significant computation with the p-group generation algorithm:

Central Conjecture

- $\mathcal{G}(p,r)$ can be described by a finite subgraph and *periodic patterns*.
- The p-groups of coclass r can be *classified*.
  ($\rightsquigarrow$ description by finitely many *parametrised presentations*)

Example: the groups in $\mathcal{G}(2,1)$ of order $2^n \geq 16$

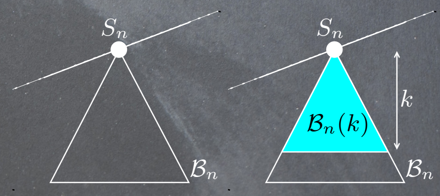
$$D_{2^n} = \mathrm{Pc}\langle a,b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{-1}\rangle,$$
$$SD_{2^n} = \mathrm{Pc}\langle a,b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{2^{n-2}-1}\rangle,$$
$$Q_{2^n} = \mathrm{Pc}\langle a,b \mid a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1}\rangle.$$

Known results:

- The Central Conjecture is proved for $p=2$.
  (Newman & O'Brien 1999, du Sautoy 2001, Eick & Leedham-Green 2008)
- Applications for $p=2$: Some invariants of the groups can be described in a uniform way. (Eick 2006, 2008)
- For odd primes: Only partial results are known.

Periodicity I

$\mathcal{T}$ coclass tree with branches $\mathcal{B}_u, \mathcal{B}_{u+1}, \ldots$
The **pruned branch** $\mathcal{B}_n(k)$ is the subtree of $\mathcal{B}_n$ induced by groups of depth at most k in $\mathcal{B}_n$.



Theorem (du Sautoy 2001, Eick & Leedham-Green 2008)
There exist integers $f = f(\mathcal{T}, k)$ and $d = d(\mathcal{T})$ such that for all $n \geq f$

$$\mathcal{B}_n(k) \cong \mathcal{B}_{n+d}(k).$$

Eick & Leedham-Green determined d, an upper bound for f, and proved:

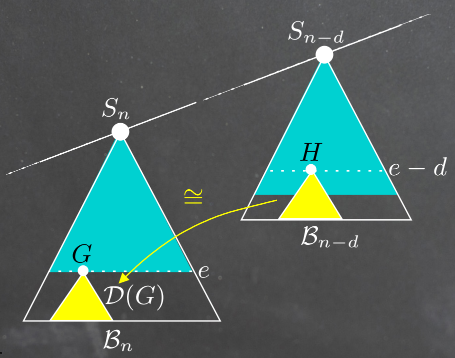
Theorem (Eick & Leedham-Green 2008)
The infinitely many groups in $\mathcal{B}_n(k)$, $n \geq u$, can be described by finitely many parametrised presentations.

These theorems prove the Central Conjecture for $p = 2$;
they are **not** sufficient to prove it for odd primes.

Periodicity II

For odd primes: Some coclass trees contain sequences of branches $\mathcal{B}_i, \mathcal{B}_{i+d}, \mathcal{B}_{i+2d}, \ldots$ with strictly increasing depths.

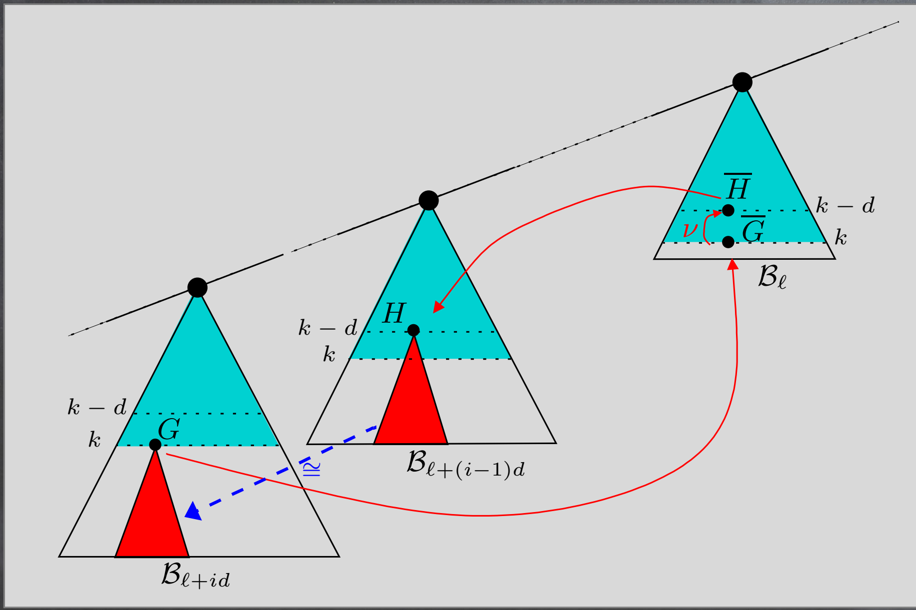
Problem: Describe the *growth* of these branches.



Conjecture (based on experiments for $\mathcal{G}(5,1)$ and $\mathcal{G}(3,2)$)
If e and n are large enough, then for every group G at depth e in $\mathcal{B}_n$ there exists a group H at depth $e - d$ in $\mathcal{B}_{n-d}$ such that $\mathcal{D}(G) \cong \mathcal{D}(H)$.

This conjecture is rather *vague* and only very little is known;
some important results for $\mathcal{G}(p, 1)$ exist.

Conjecture W



Conjecture W (Eick, Leedham-Green, Newman, O'Brien 2013)

Fix k and ℓ such that $\mathcal{B}_\ell(k) \cong \mathcal{B}_{\ell+jd}(k)$ for all j.
Let $\overline{K} \in \mathcal{B}_\ell$ be the group corresponding to $K \in \mathcal{B}_{\ell+jd}$.
There is a map ν from the groups at depth k in $\mathcal{B}_\ell$ to the groups at depth $k-d$ in $\mathcal{B}_\ell$ such that the picture holds... in particular, $\mathcal{D}(G) \cong \mathcal{D}(H)$

Important subtree: skeleton groups

Let $\mathcal{T}$ be a coclass tree in $\mathcal{G}(p,r)$, with associated pro-p group S.

Problem: the branches of $\mathcal{T}$ are usually pretty "thick" and "wide".

Skeleton groups (for split pro-p groups)

Let $S = P \ltimes T$ with $T \cong (\mathbb{Z}_p^d, +)$ and uniserial series $T = T_0 > T_1 > T_2 > \dots$
Let $\gamma\colon T \wedge T \twoheadrightarrow T_n$ be P-module hom and $m \geq n$ such that $\gamma(T_n \wedge T) \leq T_m$.
Let $T_{\gamma,m} = (T/T_m, \circ)$ with $(a+T_m) \circ (b+T_m) = a+b+\frac{1}{2}\gamma(a \wedge b) + T_m$;
then $C_{\gamma,m} = P \ltimes T_{\gamma,m}$ is the skeleton group defined by γ and m.

Theorem (Leedham-Green 1994)

If G is in $\mathcal{T}$, then there is $N \trianglelefteq G$ with order bounded by r and p, such that G/N is a "skeleton group"; the structure of skeleton groups is easier to understand, and the "skeleton of $\mathcal{T}$" is a significant subtree of $\mathcal{T}$.

The graph $\mathcal{G}(5,1)$

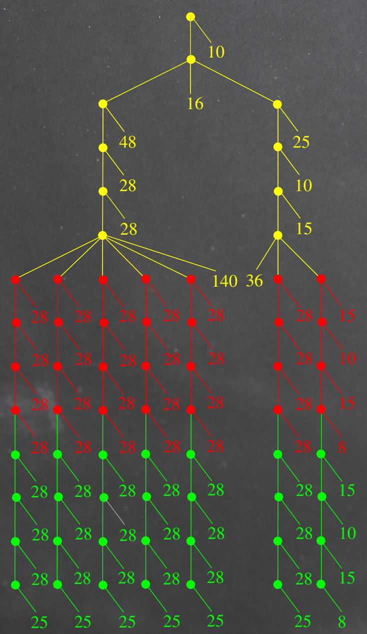
Shalev ("Problem 3", 1994): Classify the 5-groups of maximal class.

The graph $\mathcal{G}(5,1)$ has a unique coclass tree $\mathcal{T}(5)$; write $\mathcal{T}_k = \mathcal{B}_k(k-4)$.

Theorem (D. 2010)
The pruned branches $\mathcal{T}_k$ of $\mathcal{T}(5)$ can be described by a finite subgraph and the periodicities of type I & II. The groups in these pruned branches can be classified by finitely many parametrised presentations with ≤ 2 integer parameters.

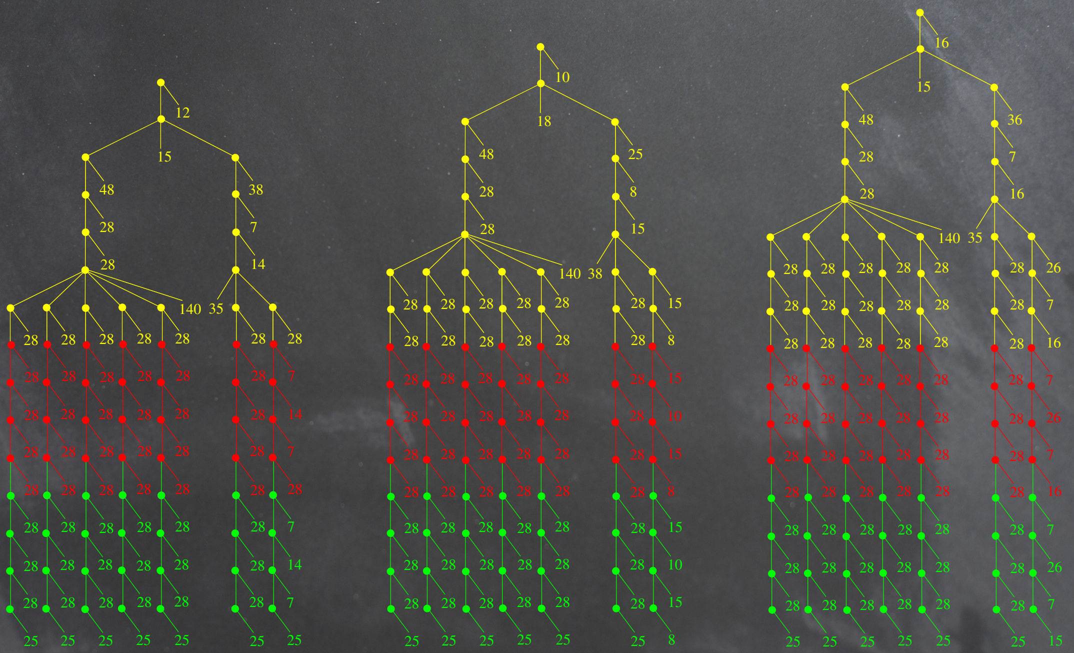
$\mathcal{G}(5,1)$: the trees $\mathcal{T}_{10+4x}$ with $x \geq 1$

Proved: $\mathcal{T}_{10+4x}$ consists of the yellow part and x copies of the red part:



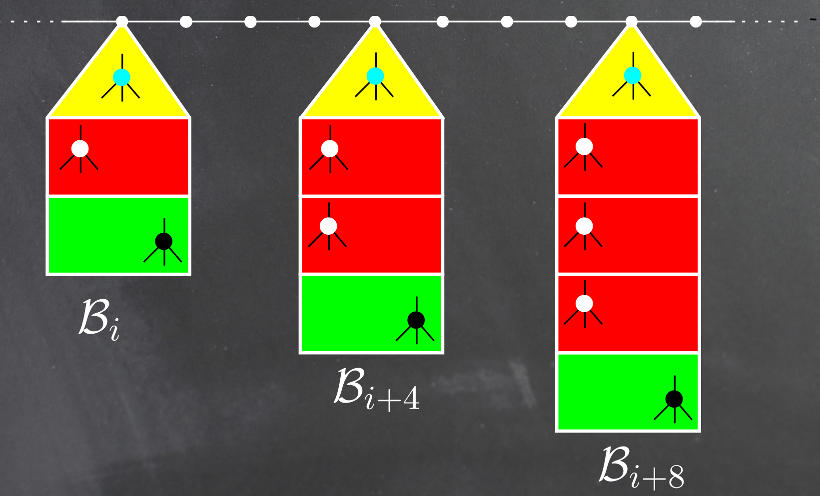
Conjecture: The difference $\mathcal{B}_{10+4x} \setminus \mathcal{T}_{10+4x}$ is the green part.

$\mathcal{G}(5,1)$: the trees $\mathcal{T}_{11+4x}$, $\mathcal{T}_{12+4x}$, and $\mathcal{T}_{13+4x}$



$\mathcal{G}(5,1)$: Periodicity classes

The origins of the periodicity classes in $\mathcal{T}_i$ with $14 \leq i \leq 17$:



"**Cyan**": 1 Parameter
"**White**": 2 Parameters
"**Black**": 1 Parameter (conjectured!)

Skip stuff

The graph $\mathcal{G}(3,2)$

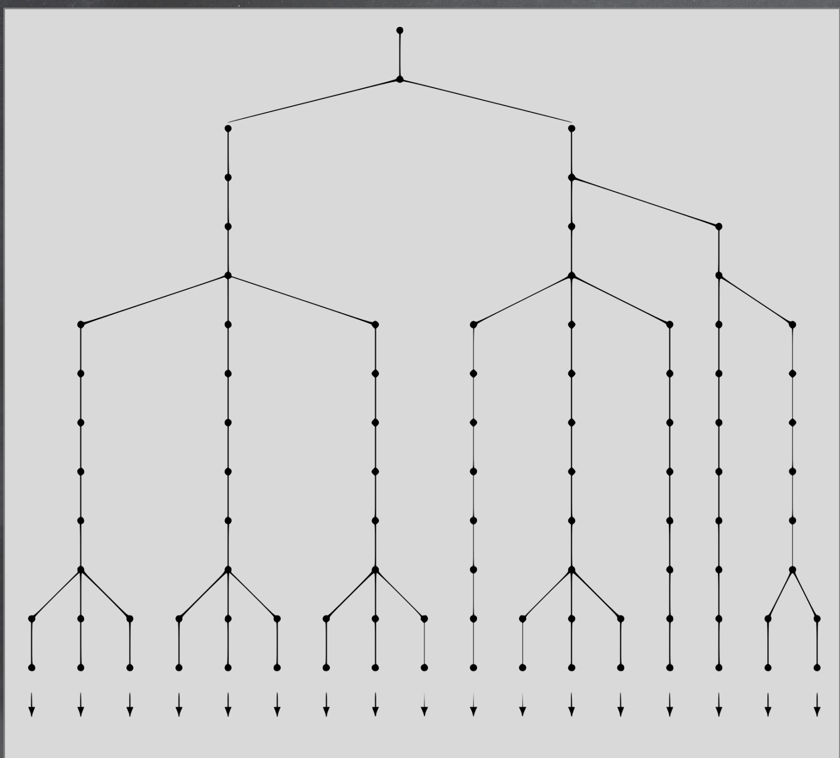
Theorem (Eick, Leedham-Green, Newman, O'Brien 2013)
Conjecture W holds for the skeletons in $\mathcal{G}(3,2)$.

Moreover:

- $\mathcal{G}(3,2)$ has 16 coclass trees, but only 4 have unbounded depths
- some coclass trees admit both, subsequences of branches of bounded depths and subsequences of branches of unbounded depths
- occurrence of "exceptional isomorphisms" between skeleton groups
- the "twigs" are described conjecturally

$\mathcal{G}(3,2)$: skeletons

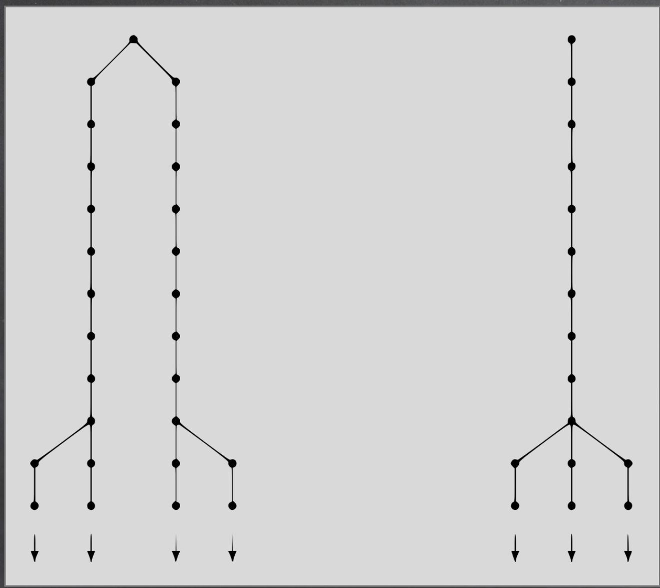
Skeletons of the split pro-3 group:



Conjectural description of twigs: usually depth 3 and up to 20,000 vertices

$\mathcal{G}(3,2)$: skeletons

Skeletons of the three non-split pro-3 groups;
skeleton only exists if class of root is congruent 0 modulo 3:



Conjectural description of twigs: up to depth 6 and 20,000 vertices

Know periodicity results

Most results and conjectures are motivated by **computer experiments**, in particular, with the p-group generation algorithm.

What is known so far:

- periodicity of type I for all graphs $\mathcal{G}(p,r)$,
- significant *local* results on periodicity of type II for the graphs $\mathcal{G}(p,1)$,
- most of $\mathcal{G}(5,1)$ and the skeleton structure of $\mathcal{G}(3,2)$

Comments on periodicity of type II:

- all known results consider pruned branches
- most results consider only skeleton groups
- $\mathcal{G}(5,1)$ and $\mathcal{G}(3,2)$ only have branches of finite width
- D. & Eick recently considered $\mathcal{G}(p,1)$ in more detail (2016)

There is still a lot to do – we're working on it . . .

skip stuff

A new result: maximal class and 'large' aut grps

Now consider $\mathcal{G}(p,1)$ with $p \geq 7$.

Let $\mathcal{T}$ be the coclass tree with branches $\mathcal{B}_j$ and *bodies* $\mathcal{T}_j = \mathcal{B}_j(j-2p+8)$.

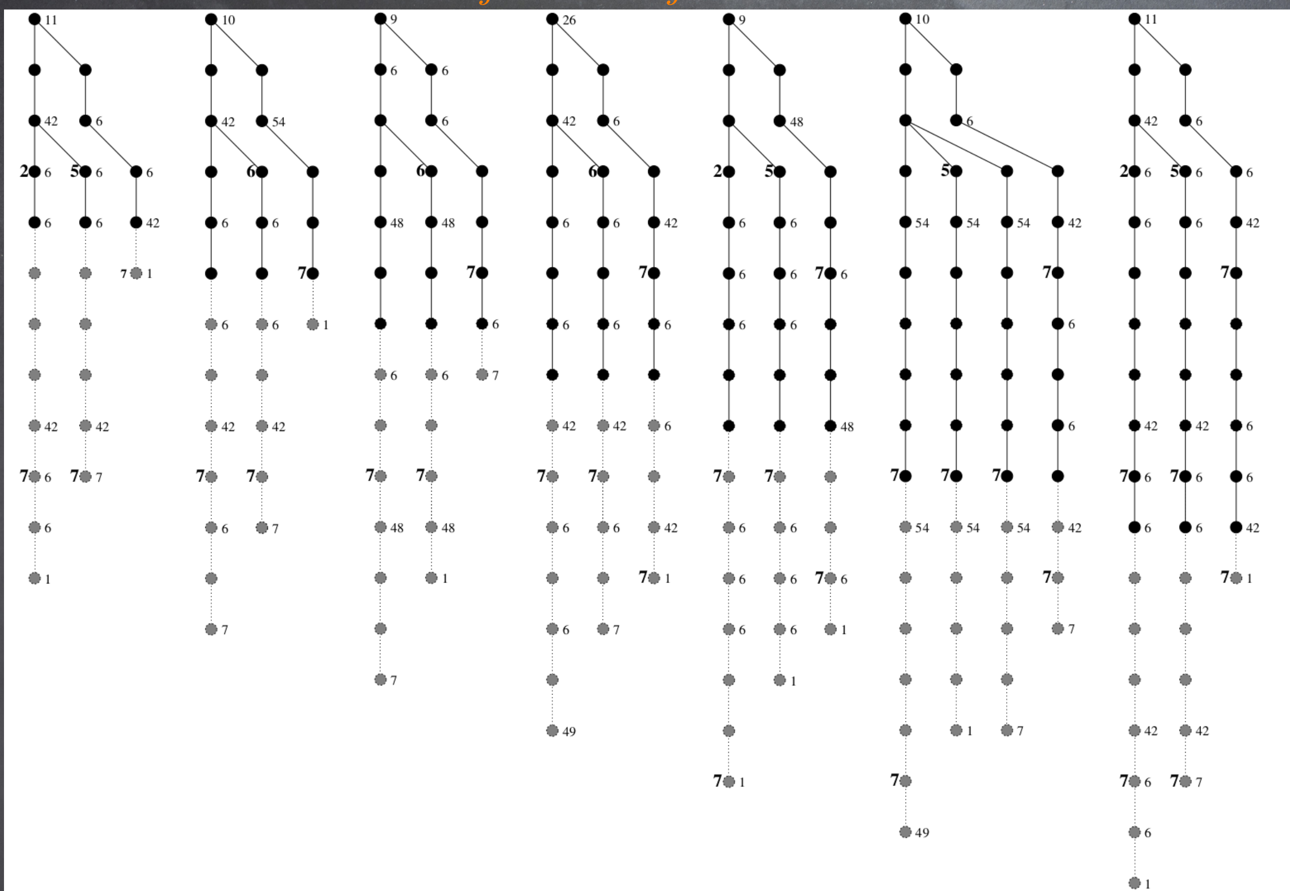
Motivated by the known periodicity results for $\mathcal{G}(p,1)$ and **promising computer experiments**, Bettina Eick and I studied the following subtrees of $\mathcal{T}$:

Definition

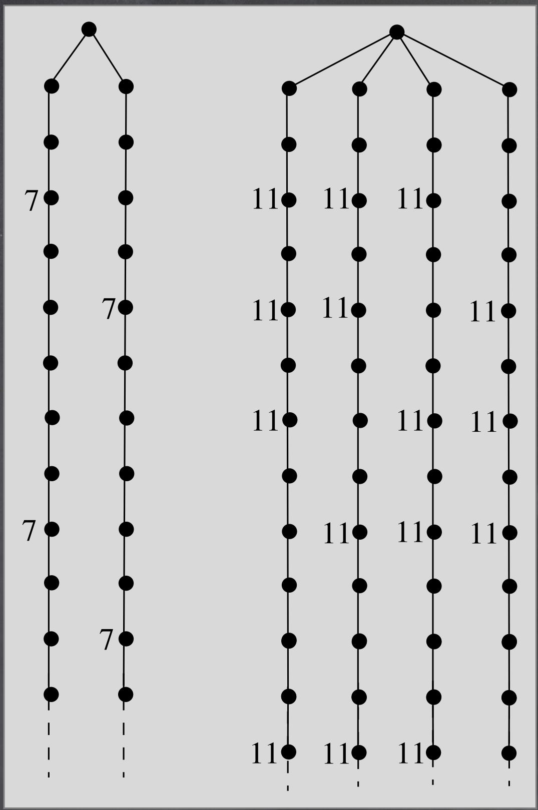
Let $\mathcal{B}_j^*$ be the subtree of $\mathcal{B}_j$ consisting of all groups whose automorphism group order is divisible by $p-1$. Let $\mathcal{S}_j^*$ be the subtree of the body $\mathcal{T}_j$ consisting of all *skeleton groups* whose automorphism group order is divisible by $p-1$.

(Note: $p-1$ is essentially the largest possible p'-part of that aut-group order.)

$\mathcal{G}(7,1)$: the trees $\mathcal{B}_j^*$ and $\mathcal{S}_j^*$ for $j = 10, \ldots, 16$



Conjectured structure of $\mathcal{S}_j^*$ for $p = 7, 11$



For $p = 7$**:**

- depth $j - 6$
- 2 groups $G_{j,1}, G_{j,2}$ at depth 1
- 7-fold ramifications at levels
  - $2 + 6\mathbb{N}$ in path of $G_{j,1}$
  - $4 + 6\mathbb{N}$ in path of $G_{j,2}$

For $p = 11$**:**

- depth $j - 14$
- 4 groups $G_{j,1}, \ldots, G_{j,4}$ at depth 1
- 11-fold ramifications at levels
  - $\{2,4,6\} + 10\mathbb{N}$ in path of $G_{j,1}$
  - $\{2,4,8\} + 10\mathbb{N}$ in path of $G_{j,2}$
  - $\{2,6,8\} + 10\mathbb{N}$ in path of $G_{j,3}$
  - $\{4,6,8\} + 10\mathbb{N}$ in path of $G_{j,4}$

p-groups of maximal class with 'large' aut-group

Let $\boldsymbol{d = p - 1}$ and $\boldsymbol{\ell = (p-3)/2}$.

Theorem (2016)

- The skeleton $\mathcal{S}_n^*$ has ℓ groups $G_{n,1}, \ldots, G_{n,\ell}$ at depth 1.
- Ramifications are always p-fold and occur exactly at depth

$$\{2, 4, \ldots, d-2\} \setminus \{d - 2i\} \; + \; d\mathbb{N}$$

in the path of $G_{n,i}$, for $i = 1, \ldots, \ell$.

The proof is heavily based on number theory and existing results for maximal class groups (19 pages, submitted 2016).

Conjectural description of twigs:
structure of twigs depends only on i, on $(e \bmod d)$, and on $(n \bmod d)$.

This is the first periodicity result supporting Conjecture W in the context of coclass trees with unbounded width.

The end . . .

Go to Coclass

Go to Overview

. . . . . . looking back:

1. motivation
2. pc presentations
3. p-quotient algorithm
4. p-group generation
5. isomorphism test
6. automorphism groups
7. coclass theory