Computational aspects of finite p-groups

Parts I and II

Heiko Dietrich

School of Mathematics
Monash University, Australia

15th December 2020
Zoomville Melbourne-Chongqing

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)

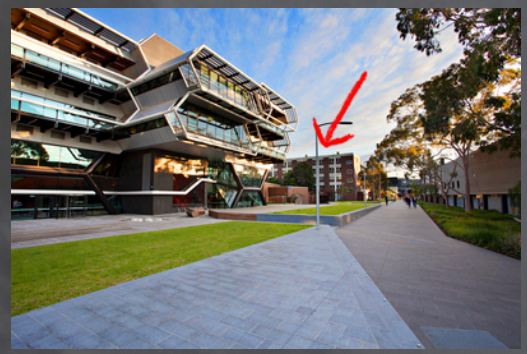
- work with Magma
- further research on p-groups

University of Trento (2011-2013)

- more work with GAP

Monash University (2013–)

- working in computational algebra (Associate Professor)



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.

Along the way: how to compute with (certain) finitely presented groups.

Convention

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

Material

Slides and recordings uploaded at `users.monash.edu/~heikod/cpg2020`

Assumed knowledge

Some basic 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)
  e.g. there are 49910529484 groups of order ≤ 2000, and 99% of them are 2-groups

Important aspects of p-groups

Some comments on p-groups

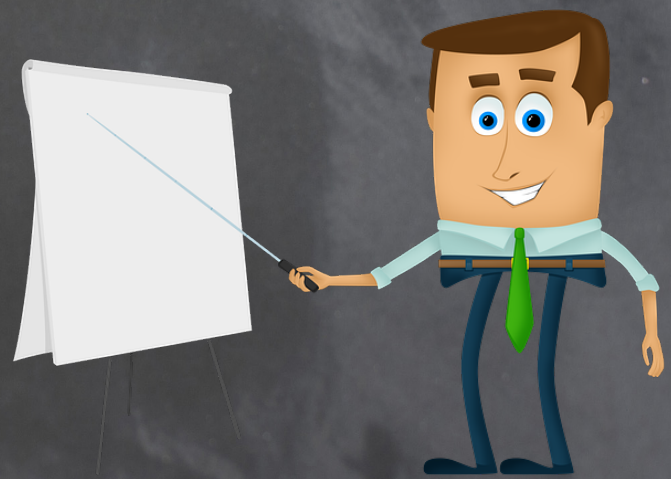
- Folklore conjecture: "almost all groups are p-groups"
- Sylow Theorem: every group has p-groups as subgroups
- Nilpotent groups: direct products of p-groups (different primes)
- Solvable groups: iterated extensions of p-groups (different primes)
- "Counterpart" to theory of finite simple groups
- Challenge: 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

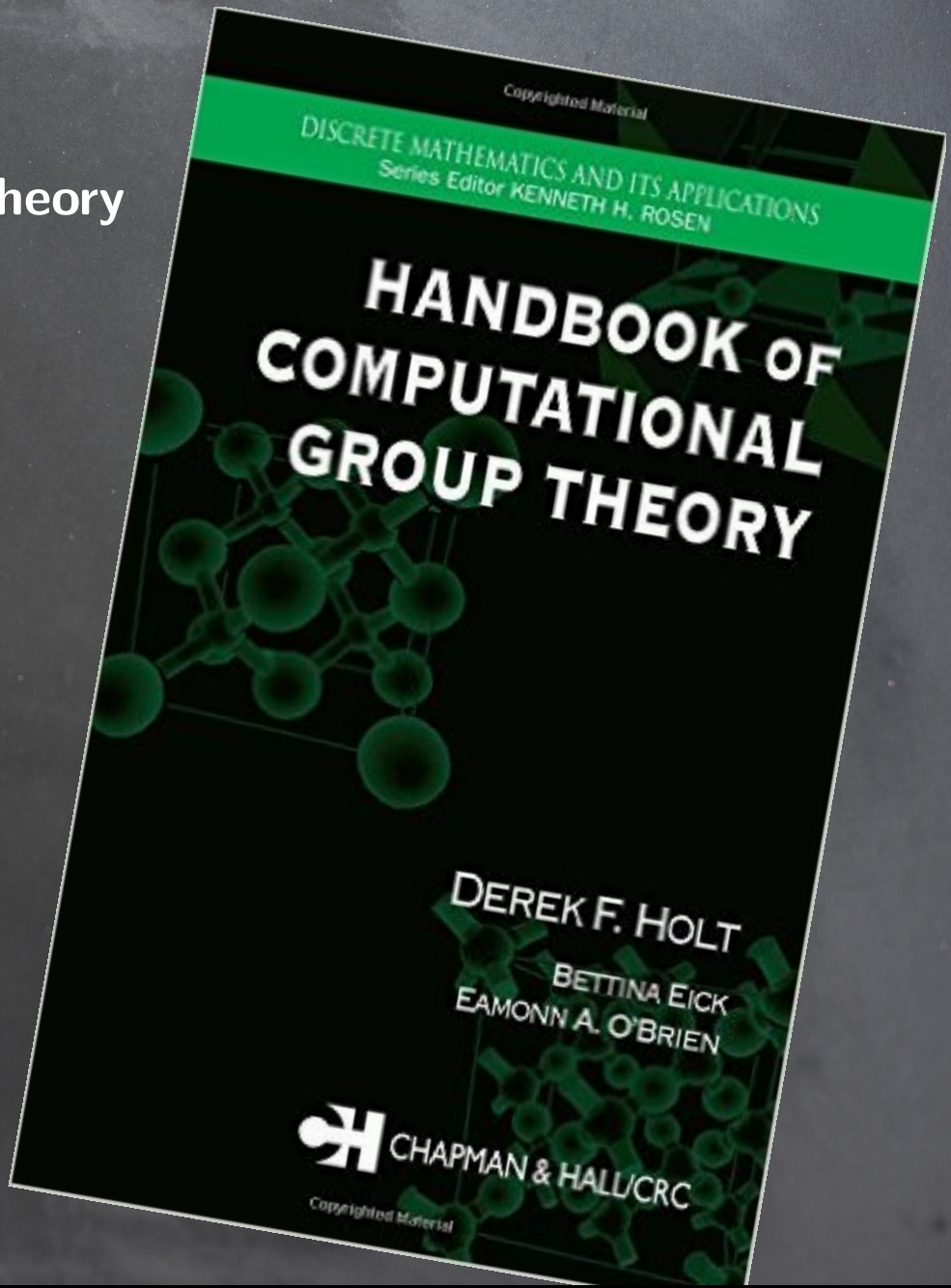
The draft outline is at follows:

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
9. other quotient algorithms ▸ Go there



Generic resource

Handbook of computational group theory
D. Holt, B. Eick, E. A. O'Brien
Chapman & Hall/CRC, 2005



Part I

pc presentations

Computing with groups

Main theme: How to compute with (p)-groups?

Related to the question: How to describe a group for a computer?

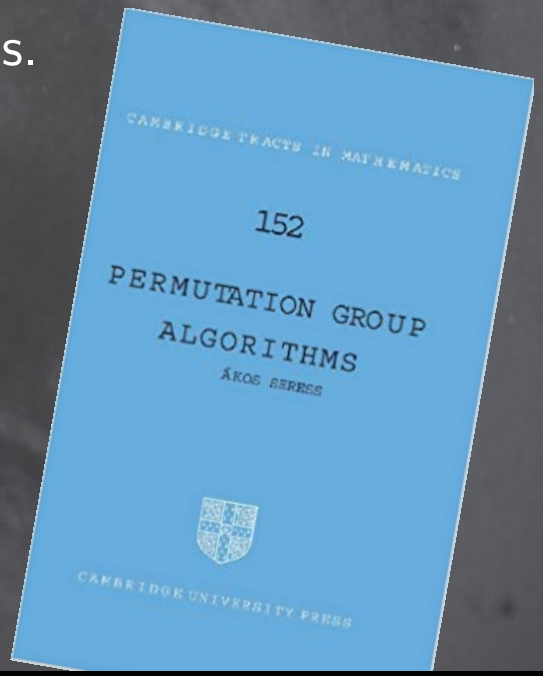
1. Permutation groups: By Cayley's Thm, every finite group is isomorphic to a permutation group that can be specified concisely by generators, eg

$$D_4 = \langle (1,2,3,4), (1,2)(3,4) \rangle.$$

Computers can usually work efficiently with such descriptions.

If G is a subgroup of a permutation group, then powerful algorithms exist to investigate questions such as

- What is the order of G?
- Is $g \in \mathrm{Sym}(n)$ an element of G?
- What is the structure of G?
- ...



Computing with groups

Convenient ways to describe a group for a computer:

2. Matrix groups: A group can also be described by its action on a linear structure, such as vector spaces; this leads to matrix groups and representations. For example, take $G = \langle X \rangle \leq \mathrm{GL}_8(7)$ generated by

$$X = \left\{ \begin{pmatrix} 2&5&5&0&1&5&5&4\\ 4&3&0&2&5&3&5&3\\ 6&1&0&5&4&4&1&1\\ 5&2&2&3&5&3&2&4\\ 2&2&6&1&2&3&1&0\\ 6&2&4&4&4&2&0&5\\ 3&2&5&1&3&5&3&5\\ 2&1&6&3&5&4&1&6 \end{pmatrix}, \begin{pmatrix} 4&3&2&0&6&0&3&2\\ 4&2&0&2&3&5&0&2\\ 0&4&2&4&3&2&4&1\\ 1&0&5&6&3&2&6&1\\ 5&5&1&6&6&3&6&2\\ 4&3&1&0&2&6&5&1\\ 4&1&6&6&5&5&1&4\\ 4&6&5&2&5&6&5&0 \end{pmatrix} \right\}.$$

There are challenges, e.g. G has size $\approx 3.4 \cdot 10^{53}$, but there has been great progress in the *Matrix Group Recognition Project*.

Computing with groups

Convenient ways to describe a group for a computer:

3. Group presentations: A group can be defined by abstract generators and a set of relators/relations, for example,

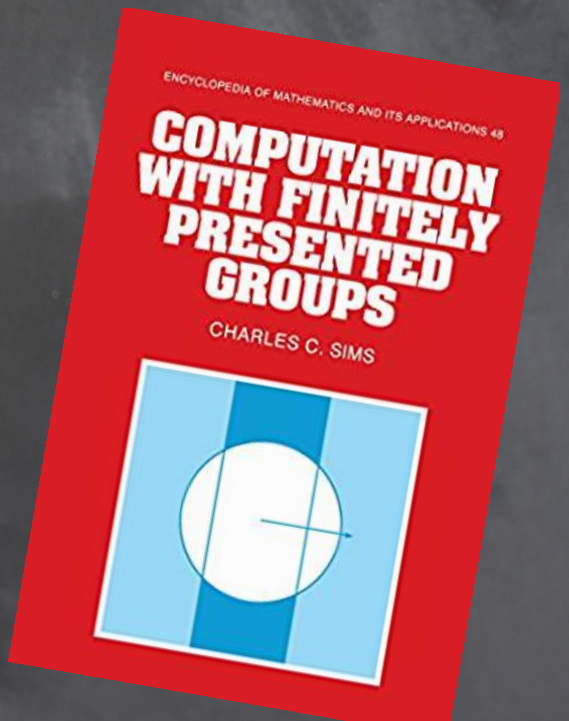
$$G = \langle r, m \mid r^4, m^2, \overbrace{r^m = r^3}^{\text{relation}} \rangle = \langle r, m \mid r^4, m^2, \overbrace{m^{-1}rmr^{-3}}^{\text{relator}} \rangle.$$

giving rise to the formal concept of group presentations.

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 has at most 8 elements;
- $D_8 = \langle r, m \rangle$ with $r = (1, 2, 3, 4)$ and $m = (1, 3)$ satisfies the relations of G; one can show that $G \cong D_8$.



Group presentations

Finitely presented groups

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, $\langle X \mid \mathcal{R} \rangle$ is the "largest" group generated by X that satisfies R.

Such a description seems natural and is very concise. However, there are some fundamental problems when computing with finitely presented groups:

- What is size of G? Is G finite? Is G trivial?
- Given a word w in the generators, is $w = 1$ in G?
- What is G? ...

Finitely presented groups

As mentioned before, it is in general very difficult to obtain any immediate information about the structure from a group presentation.

Example

- $n = 1, \ldots, 7$: $|\langle x, y \mid y^x x^y, yxyx^n y^{2n} x^n \rangle| = 1,\ 336,\ 1,\ 120,\ 1,\ 24360,\ 4080.$
- The group $\langle a, b, c \mid b^a = b^2, c^b = c^2, a^c = a^2 \rangle$ is trivial (Higman'50), but $\langle a, b, c, d \mid b^a = b^2, c^b = c^2, d^c = d^2, a^d = a^2 \rangle$ is infinite.
- The Baumslag group $\langle a, b \mid b = [b, b^a] \rangle$ has $b = 1$ in every finite quotient.

Word problem (Dehn 1910): For $u, v \in \langle S \mid \mathcal{R} \rangle$, decide whether $u = v$.

Theorem (Novikov 1955, Boone 1959)

There is a finite presentation $G = \langle S \mid \mathcal{R} \rangle$ for which there is no algorithm that, given two words u and v over S, decides whether $u = v$ in G.

ILLINOIS JOURNAL OF MATHEMATICS
Volume 30, Number 2, Summer 1986

A SIMPLE PRESENTATION OF A GROUP WITH UNSOLVABLE WORD PROBLEM

BY

DONALD J. COLLINS

In memoriam—William W. Boone

In my experience, many topologists suffer acute anxiety when it o
them that some fundamental group they are working with may hav
able word problem. One form of therapy I have known to be empl
say that groups with unsolvable word problems are monstrous, c
objects and that no-one could ever write one down in his lifetime
of this note is to deny even this succour by giving, in a modest am
and in complete detail, a group presentation with unsolvable wor
will be apparent, such an example exists, implicitly, in the lite
article simply makes the example explicit.

Generators:

$$a, b, c, d, e, p, q, r, t, k.$$

Relations:

$$p^{10}a = ap,\ p^{10}b = bp,\ p^{10}c = cp,\ p^{10}d = dp,\ p^{10}e = ep,$$
$$qa = aq^{10},\ qb = bq^{10},\ qc = cq^{10},\ qd = dq^{10},\ qe = eq^{10},$$
$$ra = ar,\ rb = br,\ rc = cr,\ rd = dr,\ re = er,$$
$$pacqr = rpcaq,\qquad p^2adq^2r = rp^2daq^2,$$
$$p^3bcq^3r = rp^3cbq^3,\qquad p^4bdq^4r = rp^4dbq^4,$$
$$p^5ceq^5r = rp^5ecaq^5,\qquad p^6deq^6r = rp^6edbq^6,$$
$$p^7cdcq^7r = p^7cdceq^7,$$
$$p^8caaaq^8r = rp^8aaaq^8,$$
$$p^9daaaq^9r = rp^9aaaq^9,$$
$$pt = tp,\ qt = tq,$$
$$k(aaa)^{-1}t(aaa) = k(aaa)^{-1}t(aaa)$$

Seems hopeless . . . so what can one do with finitely presented groups?

Homomorphisms: can do!

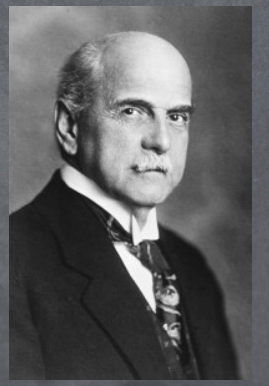
The following is a **fundamental tool** when working with fin. pres. groups:

Theorem (von Dyck's Theorem)

Let $G = \langle g_1, \ldots, g_n \mid \mathcal{R} \rangle$ and let $H = \langle h_1, \ldots, h_n \rangle$ be a group.
If every relator $w(g_1, \ldots, g_n) \in \mathcal{R}$ satisfies

$$w(h_1, \ldots, h_n) = 1 \in H,$$

then there is an epimorphism $\varphi\colon G \to H$ with each $\varphi(g_i) = h_i$.



For a given group H, this can be used to find an epimorphism $G \to H$.

Example

Let $G = \langle g, h \mid g^2, h^2, (gh)^6 \rangle$ and $H = \mathrm{Sym}_3$. Is there an epimorphism $G \to H$?
Are there generators $a, b \in H$ that satisfy $a^2 = b^2 = (ab)^6 = 1$?
Yes, take $a = (1,2)$ and $b = (2,3)$.
Now $g \mapsto a$ and $h \mapsto b$ extends to an epim. $G \to H$, so H is a quotient of G.

Von Dyck's result is the crux of quotient algorithms, which attempt to find an epimorphism $G \to H$ onto some *nicer* group H.

Special types of presentations: can do!

Recall the example

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

We figured out that $G = \{m^i r^j : i = 0, 1 \text{ and } j = 0, 1, 2, 3\}$ has $|G| \leq 8$, and von Dyck's Theorem shows that there is an epimorphism $\varphi\colon G \to D_8$ with

$$\varphi(m) = (1, 3) \quad \text{and} \quad \varphi(r) = (1, 2, 3, 4).$$

We can work well with G because it's presentation has a *special form*.

Finitely presented groups are very useful:

- group presentations are very compact definitions of groups;
- many groups from algebraic topology arise in this form;
- some efficient methods exist, eg coset enumeration (or quotient algorithms);
- many classes of groups can be studied via group presentations.

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

Background: p-groups.... Action!

Orbit-Stabiliser Theorem

If G acts on a set Ω, then $|\omega^G| = |G|/|\mathrm{Stab}_G(\omega)|$ for all $\omega \in \Omega$.

This can be used to prove the following:

Actions

If a p-group G acts on Ω, then $|\Omega| \equiv |\mathrm{Fix}_G(\Omega)| \bmod p$.

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.

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 1

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 2

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 3

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 $R(X) = [r_1, \ldots, r_n]$.
So $G = G_1 \geq \ldots \geq G_{n+1} = 1$ with each $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$ of order r_i.
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 4

A pcgs of $G = \mathsf{Alt}(4)$ 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 $R(X) = [r_1, \ldots, r_n]$;
as before let $G_i = \langle g_i, \ldots, g_n \rangle$. 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 5

Let $G = \mathsf{Alt}(4)$ 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 it can happen that

$$R(X) = \underbrace{[r_1, \ldots, r_n]}_{\text{rel. orders}} \neq \underbrace{[s_1, \ldots, s_n]}_{\text{power exp.}}.$$

Consistent pc presentations

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

Example 6

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

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

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

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

This implies that $5 \nmid |x_2|$, and so $x_3 = x_2^2$ and $x_3^5 = 1$ force $x_3 = 1$ in G.

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

Consistent pc presentation

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

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

Collection

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

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

Collection

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

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

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

or

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

Collection is a method to obtain collected words.

Collection algorithm

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

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

Collection algorithm

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

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

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

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

Theorem

The collection algorithm terminates.

Collection algorithm

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

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

Example: collection

Consider the group

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

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

"to the left"

$$\begin{aligned} \underline{321} &= \underline{3123} \\ &= 13\underline{42}3 \\ &= 1\underline{32}43 \\ &= 123\underline{43} \\ &= 12\underline{33}4 \\ &= 1\underline{244} \\ &= 12 \end{aligned}$$

"from the right"

$$\begin{aligned} \underline{321} &= \underline{3123} \\ &= 13\underline{42}3 \\ &= 1\underline{324}3 \\ &= 1\underline{323}4 \\ &= 12\underline{33}4 \\ &= 1\underline{244} \\ &= 12 \end{aligned}$$

"from the left"

$$\begin{aligned} \underline{321} &= \underline{231} \\ &= \underline{21}34 \\ &= 12\underline{33}4 \\ &= 1\underline{244} \\ &= 12 \end{aligned}$$

(Newman & Niemeyer 2014)

Consistency checks

Theorem 7: consistency checks

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

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

where the subwords in brackets are to be collected first.

Example 8

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

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

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

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

We also require that 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. The associated **weight function** is

$$\omega(x_k) = \begin{cases} 1 & (1 \le k \le d) \\ \omega(x_i) + 1 & (x_k = x_i^p \text{ def.}) \\ \omega(x_j) + \omega(x_i) & (x_k = [x_j, x_i] \text{ def.}) \end{cases}$$

Weighted power-commutator presentation

Example 9

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 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)pcps useful?

- consistent pcps 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 $G = G/G_n$.
- every finite solvable group is an iterated extension of elementary abelian subgroups, so wpcps can be used more generally.

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

Conclusion Part I

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**)

5 minute break...

Entertainment for the break ...

Look at the group

$$G = \langle g_1, g_2, g_3 \mid g_1^4 = g_3, \quad g_2^4 = g_3, \quad g_3^4 = 1, \quad g_2^{g_1} = g_2, \quad g_3^{g_1} = g_3^2, \quad g_3^{g_2} = g_3 \rangle.$$

- Show that $|G| \leq 4^3$.
- Show that this pcpc is not consistent.
- Find a consistent polycyclic presentation for G.

Solution

- The exponents of this presentation are $(4, 4, 4)$ and the normalised words in the generators are $\{g_1^{e_1} g_2^{e_2} g_3^{e_3} \mid 0 \leq e_1, e_2, e_3 \leq 3\}$, so we have $|G| \leq 4^3$.
- We have $(g_3 g_1) g_1^3 = g_1 g_3^2 g_1^3 = g_1 g_3 g_1 g_3^2 g_1^2 = g_1^2 g_3^4 g_1^2 = g_1^4 = g_3$ and $g_3(g_1^4) = g_3^2$ in G, so $g_3 = g_3^2$ and $g_3 = 1$ in G.
- Using that $g_3 = 1$, we have that $G = \langle g_1, g_2 \mid g_1^4,\ g_2^4,\ g_2^{g_1} = g_2 \rangle$; obviously, this presentation is consistent and describes a group isomorphic to $C_4 \times C_4$.

Note quite Magma... but GAP

Look at the group

$$G = \langle g_1, g_2, g_3 \mid g_1^4 = g_3, \quad g_2^4 = g_3, \quad g_3^4 = 1, \quad g_2^{g_1} = g_2, \quad g_3^{g_1} = g_3^2, \quad g_3^{g_2} = g_3 \rangle$$
$$= \mathrm{Pc}\langle g_1, g_2, g_3 \mid g_1^4 = g_3, \quad g_2^4 = g_3, \quad g_3^4 = 1, \quad g_3^{g_1} = g_3^2 \rangle$$
$$= \mathrm{Pc}\langle g_1, g_2 \mid g_1^4, \quad g_2^4 \rangle.$$

```
gap> F:=FreeGroup(["g1","g2","g3"]);;
gap> AssignGeneratorVariables(F);
#I  Assigned the global variables [ g1, g2, g3 ]
gap> R:=[g1^4/g3, g2^4/g3, g3^4, Comm(g1,g2), g3^g1/g3^2,g3^g2/g3];;
gap> G:=F/R;
<fp group on the generators [ g1, g2, g3 ]>
gap> Size(G);
16
gap> PcGroupFpGroup(G);
Error, the rewriting system must be confluent at /Volumes/daten/gap-4.11.0/lib/r
GroupByRws( col ) at /Volumes/daten/gap-4.11.0/lib/rwspcgrp.gi:1173 called from
PolycyclicFactorGroupByRelators( ElementsFamily( FamilyObj( fgrp ) ), Generators
 ) at /Volumes/daten/gap-4.11.0/lib/rwspcgrp.gi:1195 called from
PolycyclicFactorGroup( FreeGroupOfFpGroup( F ), RelatorsOfFpGroup( F )
 ) at /Volumes/daten/gap-4.11.0/lib/grppcfp.gi:23 called from
<function "PcGroupFpGroup">( <arguments> )
 called from read-eval loop at *stdin*:6
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue
brk>
```

Note quite Magma... but GAP

Look at the group

$$\begin{aligned} G &= \langle g_1, g_2, g_3 \mid g_1^4 = g_3, \quad g_2^4 = g_3, \quad g_3^4 = 1, \quad g_2^{g_1} = g_2, \quad g_3^{g_1} = g_3^2, \quad g_3^{g_2} = g_3 \rangle \\ &= \mathrm{Pc}\langle g_1, g_2, g_3 \mid g_1^4 = g_3, \quad g_2^4 = g_3, \quad g_3^4 = 1, \quad g_3^{g_1} = g_3^2 \rangle \\ &= \mathrm{Pc}\langle g_1, g_2 \mid g_1^4, \quad g_2^4 \rangle. \end{aligned}$$

```
gap>
gap> coll:=FromTheLeftCollector(3);;
gap> SetRelativeOrder(coll,1,4);;
gap> SetRelativeOrder(coll,2,4);;
gap> SetRelativeOrder(coll,3,4);;
gap> SetConjugate(coll,3,1,[3,2]);;
gap> SetConjugate(coll,3,2,[3,1]);;
gap> UpdatePolycyclicCollector(coll);
gap> G:=PcpGroupByCollector(coll);
Inconsistency at 3 1^m
fail
gap>
gap> coll:=FromTheLeftCollector(2);;
gap> SetRelativeOrder(coll,1,4);;
gap> SetRelativeOrder(coll,2,4);;
gap> UpdatePolycyclicCollector(coll);
gap> G:=PcpGroupByCollector(coll);
Pcp-group with orders [ 4, 4 ]
```

Part II

p-quotient algorithm

Recall from Part I

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.

We now discuss: 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 $a_i \in P_{\omega(a_i)-1}(G) \setminus P_{\omega(a_i)}(G)$.

Lower exponent-p series

Example 10

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.
- This quotient algorithm exemplifies the strategy of many other "quotient algorithms" for finitely presented groups.

[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 11

$G = \langle x_1, \ldots, x_6 \mid x_6^{10},\ x_1x_2x_3,\ x_2x_3x_4, \ldots, x_4x_5x_6,\ x_5x_6x_1,\ x_1x_6x_2 \rangle$ 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 12: 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 $M = S/S^*$ is central elem.-ab. p-group, so H^* is (finite) d-gen. 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. By Gaschütz, θ factors through L, that is,
$\theta\colon F \xrightarrow{\varphi} L \xrightarrow{\psi} H$, 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 $\mathcal{S} = \mathcal{S}_{\mathsf{def}} \cup \mathcal{S}_{\mathsf{nondef}}$ with $\mathcal{S}_{\mathsf{nondef}} = \{s_1, \ldots, s_q\}$.

Theorem 13

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

$$\mathcal{S}^* = \mathcal{S}_{\mathsf{def}} \cup \{s_1 b_1, \ldots, s_q b_q\} \cup \{b_1^p, \ldots, b_q^p\}.$$

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 14

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

Example 15

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

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

$$\mathcal{T} = \{a_1^2 = b_1, a_2^2 = a_3 b_2, a_3^2 = b_3, [a_2, a_1] = a_3, [a_3, a_1] = b_4, [a_3, a_2] = b_5\};$$

this pcp has power exponents $[2, 2, 2, 2, 2, 2, 2, 2]$.

However, $H^* \cong (C_8 \times C_2) : C_4$, so presentation is **not consistent**!

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

p-covering group: consistency algorithm

By Theorem 7, 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

$$u_k(u_j u_i) = (u_k u_j)u_i \qquad (1 \le i < j < k \le m+q)$$

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

$$u_j(u_j^p) = (u_j^p)u_j \qquad (1 \le j \le m+q).$$

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-covering group: consistency algorithm

By Theorem 7, 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

$$u_k(u_j u_i) = (u_k u_j)u_i \qquad (1 \le i < j < k \le m+q)$$

$$(u_j^p)u_i = u_j^{p-1}(u_j u_i) \text{ and } \quad u_j(u_i^p) = (u_j u_i)u_i^{p-1} \qquad (1 \le i < j \le m+q)$$

$$u_j(u_j^p) = (u_j^p)u_j \qquad (1 \le j \le m+q).$$

Example 16

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

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
- then $H^*/L \to K$ and $G \to H^*/L$ (von Dyck!) 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:
$$H^* = \mathrm{Pc}\langle a_1, \ldots, a_{12} \mid a_1^2 = a_{12}, a_2^2 = a_4, a_3^2 = a_{11}, a_4^2 = a_{10},$$
$$[a_2, a_1] = a_3, [a_3, a_1] = a_5, [a_3, a_2] = a_6, [a_4, a_1] = a_7,$$
$$[a_4, a_2] = a_8, [a_4, a_3] = a_9,\ a_5^2 = \ldots = a_{12}^2 = 1\rangle$$

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

- removing redundant gens (and renaming), we obtain the consistent wpcp
$$H^* = \mathrm{Pc}\langle a_1, \ldots, a_8 \mid a_1^2 = a_8, a_2^2 = a_4, a_3^2 = a_7, a_4^2 = a_6,\ a_5^2 = \ldots = a_8^2 = 1$$
$$[a_2, a_1] = a_3, [a_3, a_1] = a_7, [a_3, a_2] = a_5a_7, [a_4, a_1] = a_5\rangle$$

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 $(x, y) \to (a_1, a_2)$
- $H^* = \mathrm{Pc}\langle a_1, \ldots, a_8 \mid a_1^2 = a_8, a_2^2 = a_4, a_3^2 = a_7, a_4^2 = a_6,\ a_5^2 = \ldots = a_8^2 = 1$
  $[a_2, a_1] = a_3, [a_3, a_1] = a_7, [a_3, a_2] = a_5 a_7, [a_4, a_1] = a_5 \rangle$

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 $a_7 a_8 = 1$

Now construct $G/P_3(G)$ as $H^*/\langle a_7 a_8, a_6 \rangle$; after renaming:

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

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

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

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), $\sim$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 pcps 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 Part II

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

. . . . . looking back:

1. motivation: how to compute with groups, fp-groups, p-groups
2. pc presentations: consistency, wpcps
3. p-quotient algorithm: p-cover, Burnside problems

Slides and recording (online soon):
`users.monash.edu/~heikod/cpg2020`

Please send me typos, errors, comments, or questions via e-mail:
`heiko.dietrich@monash.edu`

Thank you!