Algorithms for polycyclic groups

Eamonn O'Brien

University of Auckland

September 2021

Introduction

Let F be free group on a non-empty set X.

Group presentation: X and a set $\mathcal{R}$ of words in X, written $\{X \mid \mathcal{R}\}$.

If R is the normal closure of $\mathcal{R}$ in F, the group G defined by the presentation is F/R and is written $\langle X \mid \mathcal{R} \rangle$.

Example

$$G = \langle a, b | a^4, b^2, a^b = a^{-1} \rangle$$

$$H = \langle a, b | a^4, b^2 = a^2, a^b = a^{-1} \rangle$$

What can we discover about the structure of G or H?

One area of substantial progress at algorithmic and computational level is in the study of particular quotients of G.

Examples include abelian, p-quotient, soluble quotients.

May discover that G infinite, by examining the invariants of its largest abelian quotient.

Can compute "useful" presentations for quotient Q of the group: those which have prime-power order, are nilpotent, or are soluble.

Central feature of these presentations is that they provide a solution to the *word problem* for Q:

Decide if two words in generators of Q represent the same element of Q.

Outline of lecture series

- Abelian quotients.
- Polycyclic generating sequences: basic properties.
- Polycyclic presentations: consistency and collection.
- Constructing polycyclic presentations.
- Generating descriptions of p-groups.
- An application: SmallGroups.

Abelian quotients

Lemma

G/N abelian if and only if $N \geq G'$.

Largest abelian quotient of G is G/G'.

Structure of this abelian group can be determined fairly readily.

Definition

B is in Smith Normal Form if for some $k \geq 0$ the entries $d_i = B_{i,i}$ for $1 \leq i \leq k$ are positive, B has no other non-zero entries, and $d_i | d_{i+1}$ for $1 \leq i \leq k$.

Smith normal form

Example

$$B := \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 & 0 \end{pmatrix}$$

is in Smith normal form.

Determine the structure of G/G'

1. Abelianise the presentation of G by adding relations to make G abelian.
2. $G/G' \cong \mathbb{Z}^n/B$ where B is a subgroup of $\mathbb{Z}^n$.
3. Describe B by a matrix $S(B)$.
4. To obtain the structure of $\mathbb{Z}^n/B$, we apply row-and-column operations to $S(B)$ to convert it to *Smith normal form* S.
5. We read off abelian invariants of $\mathbb{Z}^n/B$ from S.

Lemma

Suppose

$$B := \begin{pmatrix} d_1 & & & & & & & \\ & d_2 & & & & & & \\ & & \ddots & & & & & \\ & & & d_k & & & & \\ & & & & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 \; 0 & \cdots 0 \end{pmatrix}$$

is an $m \times n$ matrix in Smith normal form with $m \leq n$. Then

$$\mathbb{Z}^n / S(B) \simeq Z_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^s,$$

where $s = n - k$.

Example

$G = \langle x, y, z \,|\, (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2 \rangle$

Abelianise to obtain

$$\begin{aligned} G/G' &= \langle x, y, z \,|\, (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2, \\ &\quad xy = yx, xz = zx, yz = zy \rangle \end{aligned}$$

Describe B by $S(B) = \begin{pmatrix} 2 & 2 & -2 \\ -2 & 4 & 2 \\ 2 & -4 & -2 \end{pmatrix}$

Smith Normal form of $S(B)$ is $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Hence $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}$ and so it is infinite.

Polycyclic Groups

Definition

G is *polycyclic* if it has a descending chain of subgroups

$$G = G_1 \geq G_2 \geq \cdots \geq G_{n+1} = 1$$

in which $G_{i+1} \lhd G_i$, and G_i/G_{i+1} is cyclic. Such a chain of subgroups is called a *polycyclic series*.

Polycyclic groups: solvable groups in which every subgroup is finitely generated.

Example

$G = \mathrm{Alt}(4) = \langle (1,3)(2,4), (1,2)(3,4), (1,2,3) \rangle$ where
$V = \langle (1,3)(2,4), (1,2)(3,4) \rangle \lhd G$ and $\mathbb{Z}_2 = \langle (1,3)(2,4) \rangle \lhd V$.

So $\mathrm{Alt}(4) \rhd V \rhd \mathbb{Z}_2$.

Polycyclic sequences

Let G be polycyclic with polycyclic series

$$G = G_1 \geq G_2 \geq \cdots \geq G_{n+1} = 1.$$

Since G_i/G_{i+1} is cyclic, there exist $x_i \in G$ with $\langle x_i G_{i+1} \rangle = G_i/G_{i+1}$ for every $i \in \{1, \ldots, n\}$.

Definition

$X = [x_1, \ldots, x_n]$ such that $\langle x_i G_{i+1} \rangle = G_i/G_{i+1}$ for $1 \leq i \leq n$ is a *polycyclic generating sequence* (PCGS) for G.

Definition

Let X be a PCGS sequence for G. $R(X) := (r_1, \ldots, r_n)$ defined by $r_i := |G_i : G_{i+1}| \in \mathbb{N} \cup \{\infty\}$ is the sequence of *relative orders* for X. Let $I(X) := \{i \in \{1 \ldots n\} \mid r_i \text{ finite}\}$.

Example

$X := [(1,2,3),(1,2)(3,4),(1,3)(2,4)]$ is PCGS for $\mathrm{Alt}(4)$ where $R(X) = (3,2,2)$ and $I(X) = \{1,2,3\}$.

Relative orders exhibit information about G.

G is finite iff every entry in $R(X)$ is finite or, equivalently iff $I(X) = \{1 \ldots n\}$.

If G is finite, then $|G| = r_1 \cdots r_n$, the product of the entries in $R(X)$.

Example

Let $G := \langle (1,2,3,4), (1,3) \rangle \cong D_8$.

a) Let $G_2 := \langle (1,2,3,4) \rangle \cong C_4$.
Then $G = G_1 \geq G_2 \geq G_3 = 1$ is polycyclic series for G.

$X := [(1,3), (1,2,3,4)]$ and
$Y := [(2,4), (1,4,3,2)]$ are PCGS defining this series.
$R(X) = R(Y) = (2,4)$ and $I(X) = I(Y) = \{1,2\}$.

b) Let $G_2 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \cong V$ and
$G_3 := \langle (1,3)(2,4) \rangle \cong C_2$.

So $G = G_1 \geq G_2 \geq G_3 \geq G_4 = 1$.

$X := [(2,4), (1,2)(3,4), (1,3)(2,4)]$ and
$Y := [(1,2,3,4), (1,2)(3,4), (1,3)(2,4)]$ are polycyclic sequences defining this series.
$R(X) = R(Y) = (2,2,2)$ and $I(X) = I(Y) = \{1,2,3\}$.

Example

Let $G := \langle a, b \rangle$ with

$$a := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } b := \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

$G \cong D_\infty$, the infinite dihedral group.

A polycyclic sequence for G is $X := [a, ab]$ with relative orders $R(X) = (2, \infty)$ and $I(X) = \{1\}$.

Lemma

Let $X = [x_1, \ldots, x_n]$ be a polycyclic sequence for G with the relative orders $R(X) = (r_1, \ldots, r_n)$. For every $g \in G$ there exists a sequence $(e_1, \ldots, e_n)$, with $e_i \in \mathbb{Z}$ for $1 \leq i \leq n$ and $0 \leq e_i < r_i$ if $i \in I(X)$, such that $g = x_1^{e_1} \cdots x_n^{e_n}$.

Proof.

Since $G_1/G_2 = \langle x_1 G_2 \rangle$, we find that $gG_2 = x_1^{e_1} G_2$ for some $e_1 \in \mathbb{Z}$.

If $1 \in I(X)$, then $r_1 < \infty$ and we can choose $e_1 \in \{0 \ldots r_1 - 1\}$.

Let $h = x_1^{-e_1} g \in G_2$.

By induction on the length of a polycyclic sequence, we can assume that we know expression of the desired form for h; that is, $h = x_2^{e_2} \cdots x_n^{e_n}$.

Hence $g = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ as desired. □

Example

$G = \mathrm{Alt}(4)$

$X := [x_1 = (1,2,3), x_2 = (1,2)(3,4), x_3 = (1,3)(2,4)]$
is PCGS for G where $R(X) = (3,2,2)$ and $I(X) = \{1,2,3\}$.

$V = \langle x_2, x_3 \rangle$ and $H = \langle x_3 \rangle$.

$g = (1,2,4)$.

$gV = x_1^2 V$ so $x_1^{-2} g = (1,4)(2,3) \in V$.

Now $v := (1,4)(2,3)$ satisfies $vH = x_2 H$, so
$x_2^{-1} v = (1,3)(2,4) \in H$. Hence $x_2^{-1} v = x_3$ so $v = x_2 x_3$.

Hence $g = x_1^2 x_2 x_3$.

Normal form

Definition

The expression $g = x_1^{e_1} \cdots x_n^{e_n}$ is the *normal form* of $g \in G$ with respect to X.

The sequence $\exp_X(g) := (e_1, \ldots, e_n)$ is the *exponent vector* of g with respect to X.

Can define an injective map $G \to \mathbb{Z}^n : g \mapsto \exp_X(g)$ from G into the additive group of $\mathbb{Z}^n$. This is *not* a group homomorphism!

Polycyclic group to presentation?

Exponent vectors of elements of G can be used to describe relations for G in terms of X.

Lemma

Let $X = [x_1, \ldots, x_n]$ be a polycyclic sequence for G with relative orders $R(X) = (r_1, \ldots, r_n)$.

a) *Let $i \in I(X)$. The normal form of a power $x_i^{r_i}$ is $x_i^{r_i} = x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}}$.*

b) *Let $1 \leq j < i \leq n$. The normal form of a conjugate $x_j^{-1} x_i x_j$ is $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}}$.*

c) *Let $1 \leq j < i \leq n$. The normal form of a conjugate $x_j x_i x_j^{-1}$ is $x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} \cdots x_n^{c_{i,j,n}}$.*

Polycyclic presentation

Definition

A presentation $\{ x_1, \ldots, x_n \mid R \}$ is a *polycyclic presentation* if there is a sequence $S = (s_1, \ldots, s_n)$ with $s_i \in \mathbb{N} \cup \{\infty\}$ and integers $a_{i,k}, b_{i,j,k}, c_{i,j,k}$ such that R consists of the following relations:

$$\begin{aligned} x_i^{s_i} &= x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} \text{ for } 1 \leq i \leq n \text{ with } s_i < \infty, \\ x_j^{-1} x_i x_j &= x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}} \text{ for } 1 \leq j < i \leq n, \\ x_j x_i x_j^{-1} &= x_{j+1}^{c_{i,j,j+1}} \cdots x_n^{c_{i,j,n}} \text{ for } 1 \leq j < i \leq n. \end{aligned}$$

We describe the presentation by $\mathrm{Pc}\langle x_1, \ldots, x_n \mid R \rangle$. If G is defined by such a polycyclic presentation then G is a *PC-group*.

Group to presentation?

Every polycyclic group G has a polycyclic sequence X.

X induces a complete set of polycyclic relations.

The *power exponents* S of the presentation equal the relative orders $R(X)$ in this case.

Theorem

Every polycyclic sequence determines a (unique) polycyclic presentation. Thus every polycyclic group can be defined by a polycyclic presentation.

Example

Let $D_8 := \langle (1,3), (1,2,3,4) \rangle$ with polycyclic sequence $X := [(1,3), (1,2,3,4)]$ and relative orders $R(X) = (2,4)$.

Polycyclic presentation defined by X has generators x_1, x_2, power exponents $s_1 = 2$ and $s_2 = 4$. Relations are $x_1^2 = 1$, $x_2^4 = 1$, $x_1 x_2 x_1^{-1} = x_2^3$ and $x_1^{-1} x_2 x_1 = x_2^3$.

Example

S_4 has PCGS

$$X = [(3,4), (2,4,3), (1,3)(2,4), (1,2)(3,4)]$$

where $R(X) = (2,3,2,2)$.

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad x_1^2 = x_2^3 = x_3^2 = x_4^2 = 1, x_2^{x_1} = x_2^2, \\ x_3^{x_1} = x_3 x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3 x_4 \rangle$$

Presentation to group?

Every polycyclic presentation defines a polycyclic group.

Theorem

Let G be group defined by $\mathrm{Pc}\langle x_1, \ldots, x_n \mid R \rangle$ with power-exponents S. Then G is polycyclic and $X = [x_1, \ldots, x_n]$ is a polycyclic sequence for G. Its relative orders $(r_1, \ldots, r_n)$ satisfy $r_i \leq s_i$ for $1 \leq i \leq n$.

Proof.

Define $G_i := \langle x_i, \ldots, x_n \rangle \leq G$. The conjugate relations in R enforce that G_{i+1} is normal in G_i for $1 \leq i \leq n$. By construction, G_i/G_{i+1} is cyclic and hence G is polycyclic. Since $G_i = \langle x_i G_{i+1} \rangle$ by definition, X is a polycyclic sequence for G. Finally, the power relations enforce that $r_i = |G_i : G_{i+1}| \leq s_i$ for $1 \leq i \leq n$. □

Example

Let G be defined by the following polycyclic presentation with power exponents $S = (3, 2, \infty)$.

$$G := \mathrm{Pc}\langle\, x_1, x_2, x_3 \quad | \quad x_1^3 = x_3,\ x_2^2 = x_3,\ x_1^{-1}x_2x_1 = x_2x_3,\ x_1x_2x_1^{-1} = x_2x_3 \,\rangle.$$

Hence $X = [x_1, x_2, x_3]$ is a polycyclic sequence for G with relative orders $R(X) \leq (3, 2, \infty)$.

But coset enumeration shows that the precise relative orders are $R(X) = (3, 2, 1)$.

Hence the power exponents in a polycyclic presentation give an **upper bound** for the relative orders only. Cannot read off from the power exponents whether G is finite or infinite.

Inconsistent presentations

Equivalently: polycyclic presentations in which two **different** normal words represent the **same** element of the group.

Example

$$\mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^2 = x_2, x_2^2 = x_3, x_3^2 = 1, [x_2, x_1] = x_3, [x_3, x_1] = 1, [x_3, x_2] = 1 \rangle$$

$$x_1 x_2 = x_1 x_1^2 = x_1^2 x_1 = x_2 x_1 = x_1 x_2 x_3.$$

Hence, not every element of the presented group has a unique normal form.

Consistent presentations

A polycyclic presentation in which every element is represented by exactly *one* normal word is *consistent*.

Equivalently: a polycyclic presentation $\mathrm{Pc}\langle X \mid R \rangle$ with power exponents S is *consistent* if $R(X) = S$.

Effective algorithm to convert an inconsistent presentation to a consistent one.

Example

$G := \mathrm{Pc}\langle x_1, x_2 \mid x_1^3 = 1,\ x_2^2 = 1, x_2^{x_1} = x_2 \rangle$ defines $\mathbb{Z}_6$.

Collection

A method to determine the *normal form* for an element in a group given by a polycyclic presentation.

Lemma

Let $G = \mathrm{Pc}\langle X \mid R \rangle$ *be a polycyclic presentation with power exponents* S*. For every* $g \in G$ *there exists a word representing* g *of the form* $x_1^{e_1} \cdots x_n^{e_n}$ *with* $e_i \in \mathbb{Z}$ *and* $0 \leq e_i < s_i$ *if* $s_i < \infty$*.*

Definition

Let $G = \mathrm{Pc}\langle X \mid R \rangle$. Write word w in X as a string $w = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$ with $a_j \in \mathbb{Z}$. Assume that $i_j \neq i_{j+1}$ for $1 \leq j \leq r-1$ and $a_j \neq 0$ for $1 \leq j \leq r$.

a) A word w is *collected* if $w = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$ with $i_1 < i_2 < \cdots < i_r$ and $a_j \in \{1, \ldots, s_j - 1\}$ if $s_j < \infty$. Otherwise w is *uncollected*.

b) A word u in X is a *minimal non-normal subword* of the word w if u is a subword of w and it has one of the following forms:

   i) $u = x_{i_j}^{a_j} \cdot x_{i_{j+1}}$ for $i_j > i_{j+1}$,

   ii) $u = x_{i_j}^{a_j} \cdot x_{i_{j+1}}^{-1}$ for $i_j > i_{j+1}$,

   iii) $u = x_{i_j}^{a_j}$ for $r_{i_j} \neq \infty$ and $a_j \notin \{1 \ldots s_{i_j} - 1\}$.

Word is collected if and only if it does not contain a minimal non-normal subword.

Collected words

Example

$G = S_4$ has PCGS

$$X = [(3,4),(2,4,3),(1,3)(2,4),(1,2)(3,4)]$$

where $R(X) = (2,3,2,2)$ and

$$G = \mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = x_2^3 = x_3^2 = x_4^2 = 1, x_2^{x_1} = x_2^2, x_3^{x_1} = x_3x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3x_4\rangle$$

$$\begin{aligned} x_2x_1 &\mapsto x_1x_2^2 \\ x_1x_2^{-1} &\mapsto x_1x_2^2 \\ x_2^{-1}x_4x_1 &\mapsto x_1x_2x_4 \\ x_4x_3x_2x_1 &\mapsto x_1x_2^2x_4 \end{aligned}$$

Usually write *power-commutator* presentation.

$$\begin{aligned} \mathrm{Pc}\langle x_1, \ldots, x_n \mid x_i^p &= \prod_{k=i+1}^{n} x_k^{\alpha(i,k)},\ 0 \leq \alpha(i,k) < p\,,\ 1 \leq i \leq n\,, \\ [x_j, x_i] &= \prod_{k=j+1}^{n} x_k^{\beta(i,j,k)},\ 0 \leq \beta(i,j,k) < p, 1 \leq i < j \leq n \rangle. \end{aligned}$$

An example

Let G be D_{16}

$$\begin{aligned}\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = 1, x_2^2 = x_3x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle\end{aligned}$$

Normal form for elements of G is

$$x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4}$$

where $0 \leq \alpha_i \leq 1$.

Collection in finite p-groups

Every element of a p-group presented by a power-commutator presentation on $X := \{x_1, \ldots, x_n\}$ can be written as normal word

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

where $0 \leq \alpha_i < p$.

Collection: introduced by P. Hall (1934), in the context of nilpotent groups.

Consider collection in context of all semigroup words on X. Inverses of words may be ignored since they can be eliminated using the power relations.

The input to the process is a word, w.

- If w is normal the process terminates.
- If w is not normal, it has a *minimal non-normal subword* u, where

$$u = x_i^p \qquad \text{or} \qquad u = x_j x_i$$

and $1 \leq i < j \leq n$.

Now replace u by

$$\prod_{k=i+1}^{n} x_k^{\alpha(i,k)} \qquad \text{or} \qquad x_i x_j \prod_{k=j+1}^{n} x_k^{\beta(i,j,k)},$$

where $0 \leq \alpha(\ldots), \beta(\ldots) < p$, respectively.

- Resulting word, w, is now input to the process.

Replacement of minimal non-normal subwords by their normal equivalents results in the construction of a normal word from an arbitrary word.

Theorem

Collection terminates.

Proof uses induction on $|X|$: $w \mapsto x_1 v$.

If w contains more than one minimal non-normal subword, a rule is used to determine which of the subwords is replaced by its normal equivalent, thereby ensuring that the process is well defined.

Collection strategies

- *Collection to the left* – all occurrences of x_1 are moved left to the beginning of the word. Next, all occurrences of x_2 are moved left until they are adjacent to the x_1's. *etc.*
  P. Hall (1934).
- *Collection from the right* – the minimal non-normal subword occurring nearest the end of a word is selected for replacement.
  Havas & Nicholson (1976).
- *Collection from the left* – the minimal non-normal subword nearest the beginning of a word is chosen for collection.

  Leedham-Green & Soicher (1990); Vaughan-Lee (1990).

Efficiency of the collection process is affected by the rule.

Collection from the left: most efficient.

Example

Consider D_{16}.

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid \begin{array}{l} x_1^2 = 1, x_2^2 = x_3x_4, \\ x_3^2 = x_4, x_4^2 = 1, \\ [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ [x_3, x_2] = 1, [x_4, x_1] = 1, \\ [x_4, x_2] = 1, [x_4, x_3] = 1\rangle \end{array}$$

Suppose we collect $x_3x_2x_1$.

"To the left"

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = 1, x_2^2 = x_3x_4, x_3^2 = x_4, x_4^2 = 1, [x_2, x_1] = x_3, [x_3, x_1] = x_4, [x_3, x_2] = 1, [x_4, x_1] = 1, [x_4, x_2] = 1, [x_4, x_3] = 1\rangle$$

$$\begin{aligned} \underline{321} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 1\underline{32}43 \\ &= 123\underline{43} \\ &= 12\underline{33}4 \\ &= 1\underline{244} \\ &= 12 \end{aligned}$$

"From the right"

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = 1, x_2^2 = x_3x_4, x_3^2 = x_4, x_4^2 = 1, [x_2, x_1] = x_3, [x_3, x_1] = x_4, [x_3, x_2] = 1, [x_4, x_1] = 1, [x_4, x_2] = 1, [x_4, x_3] = 1\rangle$$

$$\begin{aligned} 3\underline{21} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 1324\underline{3} \\ &= 1\underline{32}34 \\ &= 123\underline{3}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

"From the left"

$$\begin{aligned}\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid\ & x_1^2 = 1, x_2^2 = x_3x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle\end{aligned}$$

$$\begin{aligned}\underline{32}1 &= 2\underline{31} \\ &= \underline{21}34 \\ &= 12\underline{33}4 \\ &= 1\underline{244} \\ &= 12\end{aligned}$$

An exercise

$G = S_4$

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = x_2^3 = x_3^2 = x_4^2, x_2^{x_1} = x_2^2, x_3^{x_1} = x_3x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3x_4\rangle$$

$x_3x_2x_1 \mapsto x_1x_2^2x_3$

- 11 steps using “To the left".
- 5 steps using “From the left".

Number of normal forms

Given a consistent power-commutator presentation, the set of elements of G can be regarded as the set of normal words and the group multiplication is defined by collection:

the product of two normal words is the word which results from collecting their concatenation.

Order of G is the number of normal words.

Usually write *power-commutator* presentation.

$$\begin{aligned} \mathrm{Pc}\langle x_1, \ldots, x_n \mid x_i^p &= \prod_{k=i+1}^{n} x_k^{\alpha(i,k)},\ 0 \leq \alpha(i,k) < p\,,\ 1 \leq i \leq n\,, \\ [x_j, x_i] &= \prod_{k=j+1}^{n} x_k^{\beta(i,j,k)},\ 0 \leq \beta(i,j,k) < p, 1 \leq i < j \leq n \rangle. \end{aligned}$$

An example

Let G be D_{16}

$$\begin{aligned}\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = 1, x_2^2 = x_3x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle\end{aligned}$$

Normal form for elements of G is

$$x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4}$$

where $0 \leq \alpha_i \leq 1$.

Power-commutator presentations: Additional properties

Assume that G, a d-generator p-group of order p^n, has a consistent power-commutator presentation on n generators, $a_1, \ldots, a_n$.

For both mathematical and computational reasons, the power-commutator presentation for G has additional structure:

1. $\{a_1, \ldots, a_d\}$ is a generating set for G.
2. For each a_k in $\{a_{d+1}, \ldots, a_n\}$, there is at least one relation whose right hand side is a_k. Exactly one of these relations is taken as the *definition* of a_k. Either:
   - $a_i^p = a_k$ where $i < k$ and a_i is a pth power of some generator or $i \leq d$,
   - $[a_j, a_i] = a_k$ where $i < j < k$ and $i \leq d$.

3. The power-commutator presentation has a *weight* function defined on it: a generator is assigned a weight corresponding to the stage at which it is added.

   A function, ω, is defined on the generators of the power-commutator presentation according to the following rules:

   (i) $\omega(a_i) = 1$ for $i = 1, \ldots, d$;

   (ii) if the definition of a_k is $a_i^p = a_k$, then $\omega(a_k) = \omega(a_i) + 1$;

   (iii) if the definition of a_k is $[a_j, a_i] = a_k$, then $\omega(a_k) = \omega(a_j) + \omega(a_i)$.

   $\omega(a_n)$ is the class of G.

Example

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

a_3 has definition $[a_2, a_1]$ and weight 2;

a_4 has definition a_1^2 and weight 2;

a_5 has definition $[a_3, a_1]$ and weight 3.

Why are such features desirable?

Because they permit more efficient algorithms to be developed, both at construction and application stage.

For example, the weights of generators can be used to reduce the amount of computation needed to decide whether or not a given power-commutator presentation is consistent.

How do we compute such presentations?

Given a finitely-presented group, how can we compute a polycyclic presentation for a quotient?

A power-commutator presentation for a finite p-quotient may be constructed using a *p-quotient algorithm*.

First such algorithm described by Macdonald (1974).

Focus on an algorithm developed by Havas, Newman and O'Brien: H & N (1980), N & O'B (1996).

The p-quotient algorithm: A top-level outline

Let G be a p-group.

Algorithm uses a chain of normal subgroups

$$G = G_0 \geq G_1 \geq \ldots \geq G_k \geq G_{k+1} \ldots \geq G_c = 1$$

Works down this chain, using the power-commutator presentation constructed for G/G_k to write down a presentation for G/G_{k+1}.

Write down a presentation for a group H^* which is a downward extension of $H := G/G_k$ and has $K := G/G_{k+1}$ as a quotient.

Factor a normal subgroup from H^* to obtain a presentation for K.

A central series

p-quotient algorithm uses a variation of the lower central series known as the *lower exponent-p central series*.

$$G = P_0(G) \geq \ldots \geq P_{i-1}(G) \geq P_i(G) \geq \ldots$$

where $P_i(G) = [P_{i-1}(G), G]P_{i-1}(G)^p$ for $i \geq 1$.

Observe $P_i(G)/P_{i+1}(G) \leq Z(G/P_{i+1}(G))$ and $P_i(G)/P_{i+1}(G)$ is elementary abelian.

If $P_c(G) = 1$ and c is the smallest such integer then G has *exponent-p class* c.

Basic properties of the central series

1. A group with exponent-p class c is nilpotent and has nilpotency class at most c.
2. If θ is a homomorphism of G then $P_i(G)\theta = P_i(G\theta)$.
3. If $N \lhd G$ and the quotient G/N has class c then $P_c(G) \leq N$.
4. If G is a finite p-group then $P_1(G)$ is the Frattini subgroup of G.

Example

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

Can read off terms of central series.

$$\begin{aligned} P_0(G) &= G \\ P_1(G) &= \langle a_3, a_4 \rangle \\ P_2(G) &= \langle a_4 \rangle \\ P_3(G) &= 1 \end{aligned}$$

G has (nilpotency and exponent p-) class 3.

A summary

Given a description of a group G, a prime p, and a positive integer c, the p-quotient algorithm constructs a weighted consistent power-commutator presentation for the largest p-quotient of G having class c.

Description of G is usually a finite presentation.

The initial step

First iteration of the p-quotient algorithm computes a consistent power-commutator presentation for $G/P_1(G)$ and an epimorphism from G onto $G/P_1(G)$.

Since $P_1(G) = [G, G]G^p = \Phi(G)$, $G/P_1(G)$ is the Frattini quotient of G.

How do we compute $G/P_1(G)$?

Fp-presentation is used to set up a homogeneous system of equations over $GF(p)$:

these equations are obtained by abelianising the relations, taking exponents modulo p, and then writing the result additively.

Solve them to obtain rank of $G/P_1(G)$.

An example

Assume that the input finite presentation is:

$$\{b_1, \ldots, b_6 \quad | \quad b_1 b_2 = b_3, b_2 b_3 = b_4, b_3 b_4 = b_5, \\ b_4 b_5 = b_6, b_5 b_6 = b_1, b_6 b_1 = b_2\}$$

and that $p = 2$.

Equations are the following:

$$b_1 + b_2 = b_3 \quad b_2 + b_3 = b_4 \quad b_3 + b_4 = b_5$$
$$b_4 + b_5 = b_6 \quad b_5 + b_6 = b_1 \quad b_1 + b_6 = b_2$$

Solve this system of equations by row-echelonisation to obtain the following solutions:

$$b_3 = b_1 + b_2, \; b_4 = b_1, \; b_5 = b_2, \; b_6 = b_1 + b_2 \, .$$

Solution space has dimension 2 and a consistent power-commutator presentation is

$$\mathrm{Pc}\langle a_1, a_2 \,:\, a_1^2 = 1, a_2^2 = 1, [a_2, a_1] = 1\rangle$$

Mod $P_1(G)$, $b_1 = a_1, b_2 = a_2, b_3 = a_1 a_2$,
$b_4 = a_1, b_5 = a_2, b_6 = a_1 a_2$.

In general, if d is the dimension of the solution space, then the output from the first iteration is power-commutator presentation for $G/P_1(G)$:

$$\mathrm{Pc}\langle a_1, \ldots, a_d \mid a_i^p = 1, [a_j, a_i] = 1, 1 \leq i < j \leq d \rangle$$

Mod $P_1(G)$, each b_i can be expressed in terms of the a_j.

$\{a_1, \ldots, a_d\}$ is a subset of $\{b_1, \ldots, b_n\}$.

The general iteration

Takes as input:

1. the finite presentation $\{X \mid \mathcal{R}\}$ for G;
2. a consistent power-commutator presentation for the factor group $H = G/P_k(G)$;
3. an epimorphism $\theta : G \mapsto H$, specified by the images of the generators of G.

The output of this iteration is:

1. a consistent power-commutator presentation for the factor group $K = G/P_{k+1}(G)$;
2. an epimorphism from G to K.

The general iteration

Can be divided into 4 distinct steps.

Step 1. Write down presentation for p-covering group

Assume we have constructed a consistent power-commutator presentation for $H = G/P_k(G)$.

We now construct a group H^* which has the property that $K = G/P_{k+1}(G)$ is a homomorphic image.

We want H^* to satisfy the following:

(i) $H^*/P_k(H^*)$ is isomorphic to H.

(ii) $G/P_{k+1}(G)$ is a homomorphic image of H^*.

(iii) H^* is a d-generator group;

(iv) H^* has class at most $k+1$;

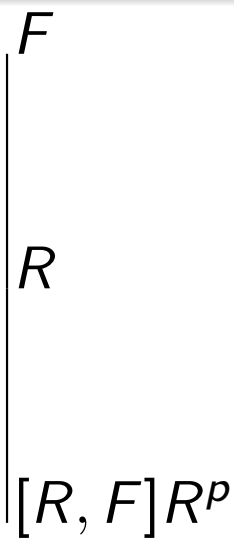
(v) H^* is the largest group satisfying (i) to (iv).

H^* is the *p-covering group* of $H = G/P_k(G)$.

Defining the *p-covering group*

Theorem

Let H be a d-generator p-group, let F be the free group of rank d, and let $F/R \cong H$. Then the p-covering group, H^*, of H is $F/[R,F]R^p$.



$R/[R,F]R^p$ is elementary abelian and can be viewed as a vector space over $GF(p)$.

Construct pcp for p-covering group of $G/P_k(G)$

Look at output of kth stage of the algorithm.

This is a consistent power-commutator presentation, say $\{a_1, \ldots, a_n : \ldots\}$, for $H := G/P_k(G)$.

Each of the $n - d$ generators, $a_{d+1}, \ldots, a_n$, is defined by one of the relations – it occurs as the right hand side of one of the relations.

Thus, there are $n - d$ *definitions* that define the generators $a_{d+1}, \ldots, a_n$.

The remaining q relations are non-defining and have general form:

$$[a_j, a_i] = a_{j+1}^{\alpha_{j+1}} \dots a_n^{\alpha_n}, 1 \leq i < j \leq n$$

$$\text{or } a_i^p = a_{i+1}^{\alpha_{i+1}} \dots a_n^{\alpha_n},$$

where $1 \leq i \leq n$ and $0 \leq \alpha_k < p$.
To obtain presentation for H^*, we transform the power-commutator presentation for $H := G/P_k(G)$ as follows.

1. New generators $a_{n+1}, \dots, a_{n+q}$ are introduced, one for each non-defining relation.
2. Each of the remaining (non-definition) relations is modified by inserting one of these generators to its right hand side.
3. Relations making these new generators central and of order p are added.

Example

$G := C_2 \times C_2$:

$$\{ a_1, a_2 \mid [a_2, a_1] = 1, \; a_1^2 = 1 \; a_2^2 = 1 \}$$

Add new generators or *tails* corresponding to a generating set for $R/[R, F]R^p$ and relations to make these central and of order p.

$$\{ a_1, a_2, a_3, a_4, a_5 \mid [a_2, a_1] = a_3, \; a_1^2 = a_4, \; a_2^2 = a_5, \; a_j^2 = 1, [a_j, a_i] = 1, 3 \leq i < j \leq 5 \}$$

Example

Let $H = D_8$.

$$\{a_1, a_2, a_3 \mid [a_2, a_1] = a_3, [a_3, a_1] = 1, [a_3, a_2] = 1, a_1^2 = 1, a_2^2 = a_3, a_3^2 = 1\}$$

$$\{a_1, a_2, a_3, a_4, \ldots, a_8 \mid [a_2, a_1] = a_3, [a_3, a_1] = a_4, [a_3, a_2] = a_5, a_1^2 = a_6,\ a_2^2 = a_3 a_7, a_3^2 = a_8, a_j^2 = 1, 4 \leq j \leq 8, [a_j, a_i] = 1, 4 \leq i < j \leq 8\}$$

Step 2. Make the presentation for H^* consistent

The presentation for H^* obtained in this way on $\{a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+q}\}$ is usually not consistent.

How do we make it consistent?

Wamsley (1974) and Vaughan-Lee (1984):

Certain associativity conditions suffice to ensure that a power-commutator presentation is consistent.

Consistency Theorem

Theorem

A power-commutator presentation on $\{a_1, \ldots, a_n\}$ *is consistent if the following are satisfied:*

$$
\begin{array}{lcll}
(a_k a_j)a_i & = & a_k(a_j a_i), & 1 \leq i < j < k \leq n\,,\ i \leq d; \\
(a_j^{p-1} a_j)a_i & = & a_j^{p-1}(a_j a_i), & 1 \leq i < j \leq n\,,\ i \leq d; \\
(a_j a_i)a_i^{p-1} & = & a_j(a_i a_i^{p-1}), & 1 \leq i < j \leq n\,; \\
(a_i a_i^{p-1})a_i & = & a_i(a_i^{p-1} a_i), & 1 \leq i \leq n\,.
\end{array}
$$

How do we interpret this theorem? The words on each side of a condition are collected, where the brackets indicate the subwords to be replaced first in the collection.

The consistency algorithm

This theorem provides the basis of an algorithm which takes as input a power-commutator presentation for a p-group and modifies it to produce a consistent one.

Consider the list of words obtained from these conditions: if each pair of words 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 procedure gives a new relation which holds in the group.

Since the presentation for $G/P_k(G)$ was consistent, this relation only involves the new generators introduced.

We deduce that one of $a_{n+1}, \ldots, a_{n+q}$ is redundant.

Applying the tests

Consider the inconsistent presentation for G:

$$\{\ a_1, a_2, a_3 \quad | \quad a_1^2 = a_2, a_2^2 = a_3, a_3^2 = 1, \\ [a_2, a_1] = a_3, [a_3, a_1] = 1, [a_3, a_2] = 1\ \}\,.$$

Apply the 4th of the tests to a_1^3:

$$a_1^3 = (a_1 a_1)a_1 = a_2 a_1 = a_1 a_2 a_3$$

but

$$a_1^3 = a_1(a_1 a_1) = a_1 a_2\,.$$

Deduce the relation that $a_3 = 1$ and, therefore, a power-commutator presentation for G is

$$\{\ a_1, a_2\ |\ a_1^2 = a_2, a_2^2 = 1, [a_2, a_1] = 1\ \}\,.$$

If we apply our consistency algorithm, it is now consistent.

The p-covering group of D_8

$$\{a_1, a_2, a_3, a_4, \ldots, a_8 \mid [a_2, a_1] = a_3, [a_3, a_1] = a_4, [a_3, a_2] = a_5$$
$$a_1^2 = a_6, a_2^2 = a_3 a_7,$$
$$a_3^2 = a_8, a_j^2 = 1, 4 \leq j \leq 8$$
$$[a_j, a_i] = 1, 4 \leq i < j \leq 8\}$$

$$a_2^3 = a_2(a_2 a_2) = a_2 a_3 a_7$$

$$a_2^3 = (a_2 a_2)a_2 = a_3 a_7 a_2 = a_3 a_2 a_7 = a_2 a_3 a_5 a_7.$$

Hence a_5 is trivial.

$$a_2(a_2 a_1) = a_1 a_3 a_5 a_7 a_8$$
$$(a_2^2)a_1 = a_1 a_3 a_4 a_7$$

Hence $a_4 = a_5 a_8$. Conclude $a_3^2 = a_4 a_5$.

A consistent power-commutator presentation for the 2-covering group of D_8 is

$$\begin{aligned}\{a_1, a_2, a_3, a_4, a_6, a_7 \quad | \quad & [a_2, a_1] = a_3, \\ & [a_3, a_1] = a_4, \\ & [a_3, a_2] = 1 \\ & a_1^2 = a_6, \\ & a_2^2 = a_3 a_7, \\ & a_3^2 = a_4, \\ & a_j^2 = 1, 4 \leq j \leq 7 \\ & [a_j, a_i] = 1, 4 \leq j \leq 7\}\end{aligned}$$

Application of this algorithm provides us with a homogeneous system of equations over $GF(p)$.

Each equation is obtained by collecting each of the relevant test words in the two ways indicated, equating the resulting normal words, and reducing resulting relation as much as possible.

Step 3. Enforce defining relations

Know that $K = G/P_{k+1}(G)$ is a homomorphic image of H^*.

We have as input an epimorphism $\theta : G \mapsto H$, specified by the images of the generators of G.

Define a map

$$\tau : G \mapsto K : g \mapsto (g\theta)u_g$$

where u_g is an unknown element of $P_k(G)/P_{k+1}(G)$.

Hence u_g is central and of order p in K.

τ is a homomorphism and the images of the generators of G under τ satisfy relators of G.

$\theta : G \mapsto H$ and $\tau : G \mapsto K : g \mapsto (g\theta)u_g$
Let r be a relator of G.

Evaluate r in the images of the generators of G under τ.

Collect the result to give normal word in the generators $a_{n+1}, \ldots, a_{n+q}$ of H^*.

The image $r\tau$ has form $(r\theta)u_r$ where u_r is a word in the u_g.

Since r is a relator of G, and $r\theta = 1$, deduce the relation $u_r = 1$.

Hence, the images of the relations are collected to yield a homogeneous system of equations over $GF(p)$.

Step 4. Elimination

Final step eliminates the redundancies which arise among the new generators from consistency and imposition of defining relations.

Suppose that t new generators are added and that r independent relations are found between them.

Then a consistent power-commutator presentation for the largest class $k+1$ quotient has $t-r$ more generators than one for the largest class k quotient.

All relations involve only $a_{n+1}, \ldots, a_{n+t}$.

Eliminating r of these generators using the relations amounts to solving a system of r linear equations in t unknowns over $GF(p)$.

Let $M = \langle a_{n+1}, \ldots, a_{n+q} \rangle$. Let N be kernel of natural homomorphism from K onto H; so N is homomorphic image of M.

To obtain pcp for K, compute the kernel of map from M to N.

Theorem

The result of collecting the set of words in $\{a_1, \ldots, a_n\}$ listed in Consistency Theorem in the power-commutator presentation for H^* is a set S contained in M.

The result of evaluating the relators of G in the images of the generators of G under θ in the power-commutator presentation for H^* is a set T contained in M.

Then N is isomorphic to $M/\langle S \cup T \rangle$.

Since we have a vector space defined over $GF(p)$, use Gaussian Elimination to obtain a basis for N. If all the new generators are eliminated, deduce that $G/P_k(G)$ is the largest p-quotient of G.

Summary of procedure for one class

1. Add new generators (tails) to the presentation for H – corresponding to a generating set for $R/[R, F]R^p$.

   Add relevant relations to make these central and of order p. So obtain presentation for H^*.

2. Make the resulting presentation consistent.

3. Impose the relations in $\mathcal{R}$.

4. Eliminate the redundancies among the new generators from resulting presentation.

A sample calculation

Calculate the largest 2-quotient of G having finite presentation:

$$\{ b_1, b_2, b_3 \mid b_1 b_2 = b_3, b_2 b_3 = b_1, b_3 b_1 = b_2 \}.$$

The solution space for $G/P_1(G)$ has dimension 2; b_3 is eliminated at the first stage, so a consistent power-commutator presentation for $G/P_1(G)$ is

$$\{ a_1, a_2 \mid a_1^2 = 1, a_2^2 = 1, [a_2, a_1] = 1 \}$$

Mod $P_1(G)$, $b_1 = a_1, b_2 = a_2, b_3 = a_1 a_2$.

Now construct $G/P_2(G)$.

A cpcp for 2-covering group of $C_2 \times C_2$ is:

$$\begin{aligned}\{\ a_1, a_2, a_3, a_4, a_5 \quad | \quad & [a_2, a_1] = a_3, \\ & a_1^2 = a_4, \\ & a_2^2 = a_5, \\ & a_j^2 = 1, [a_j, a_i] = 1, 3 \leq i < j \leq 5\}\end{aligned}$$

Now impose relations where

$$\begin{aligned}\theta \quad : \quad & b_1 \mapsto a_1, \\ & b_2 \mapsto a_2, \\ & b_3 \mapsto a_1 a_2\end{aligned}$$

Collect the relations to get equations: for example,
$b_2 b_3 = b_1$ implies that $a_2 a_1 a_2 = a_1$ so $a_1 a_3 a_5 = a_1$.

$$a_1 a_2 = a_1 a_2, \quad a_1 a_3 a_5 = a_1, \quad a_2 a_3 a_4 = a_2$$

Deduce that $a_3 = a_4 = a_5$.

Hence consistent power-commutator presentation for class 2 quotient is

$$\{\ a_1, a_2, a_3 \quad | \quad a_1^2 = a_3, a_2^2 = a_3, [a_2, a_1] = a_3\ \}.$$

G has Q_8 as a quotient.

If we now seek to construct $G/P_3(G)$, all new generators introduced are later eliminated.

Therefore, largest 2-quotient of G is Q_8.

Why are such presentations useful?

- If we have a consistent power-commutator presentation for G, we can solve the *word problem* for G.

  Given two arbitrary words w_1 and w_2 in the generators of G, compute normal forms for each of w_1 and w_2. If normal forms are identical, then the two words are identical.

- Such a presentation exhibits a normal series $\{G_k\}$ for G. Many of the algorithms developed to compute properties of p-groups work down a chain of factor groups.

  General paradigm: Solve the problem for G/G_k.

  Now extend to solve the problem for G/G_{k+1}.

  Example: determine the number of conjugacy classes of G.

Applications

- The Burnside Problem
- Proving groups infinite

The Burnside Problem

One motivation for the development of a p-quotient algorithm came from study of long-standing Burnside Problem.

Burnside (1902) posed two questions:

(i) Given a finitely-generated group in which every element has finite order, is the group necessarily finite?

(ii) Let $B(d, n)$ denote the largest d-generator group in which every element has exponent dividing n: that is, $g^n = 1$ for all $g \in G$. Is $B(d, n)$ finite? If so, what is its order?

Burnside: $B(d, 2)$ is finite, abelian, and has order 2^d.

Golod (1964): using work with Šafarevič, answer to (i) is "no".

Levi & van der Waerden (1933): the order of $B(d, 3)$ is $3^{d+\binom{d}{2}+\binom{d}{3}}$.

Tobin (1954): order of $B(2, 4)$ is 2^{12}.

Sanov (1940) and M. Hall (1958): all groups of exponent 4 and 6 are finite.

Adian & Novikov (1968): "no" for all odd $n \geq 4381$.

Other improvements.

Grün (1940) posed related problem, now known as Restricted Burnside Problem:

Problem

Is there a largest finite quotient, $R(d, n)$, of $B(d, n)$ and, if so, what is its order?

Zel'manov (1991): There is always a largest finite quotient.

Implementations of the p-quotient algorithm have been used to determine the order and compute power-commutator presentations 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); N & O'B (1996)
$B(5,4)$	2^{2728}	Newman & O'B (1996)
$R(2,7)$	7^{20416}	O'B & Vaughan-Lee (2002)

Survey article on the (Restricted) Burnside problem:
Vaughan-Lee & Zel'manov (1999).

Proving groups infinite

Golod-Šafarevič: if H is a non-trivial finite p-group, then $r(H) > d(H)^2/4$.

Let G be a group and p prime. Let $P_1(G) = [G, G]G^p$ and $P_2(G) = [P_1(G), G]P_1(G)^p$. Then $G/P_1(G)$ and $P_1(G)/P_2(G)$ are elementary abelian, of ranks $d_p(G)$ and $e_p(G)$ respectively. Newman (1990) proved the following.

Theorem

Let G be a group with a finite presentation on b generators and r relators. For some prime p, let $d = d_p(G)$ and $e = e_p(G)$. If any of the following conditions hold

(i) $r - b \leq d^2/4 - d$;

(ii) $r - b < d^2/2 + (-1)^p d/2 - d - e$;

(iii) $r - b \leq d^2/2 + (-1)^p d/2 - d - e + (e - (-1)^p d/2 - d^2/4)d/2$;

then G has arbitrarily large finite p-quotients; so is infinite.

The generalised Fibonacci groups

$$G_n(m,k) = \langle\, x_1, \ldots, x_n \mid x_i x_{i+m} = x_{i+k} \quad (i = 1, \ldots, n) \,\rangle$$

where the subscripts are taken modulo n.

Fibonacci groups where $m = 1, k = 2$: introduced by Conway (1965).

For $n \geq 10$, all such groups infinite.

Newman (1990) proved $G_9(1,2)$ infinite using previous theorem.

Remaining cases: $G_9(1,3)$ and $G_9(1,4)$

Cavicchiolli, O'B and Spaggiari (2008) study these.

The p-group generation algorithm

Description of the algorithm: O'Brien (1990), Newman (1977).

The p-group generation algorithm calculates (presentations for) particular extensions, *immediate descendants*, of a finite p-group.

Let G be a d-generator finite p-group of class c.

H is a *descendant* of G if H has generator number d and $H/P_c(H) \cong G$.

A group is an *immediate descendant* of G if it is a descendant of G and has class $c+1$.

Example

$D_8 = \mathrm{Pc}\langle\, a_1, a_2, a_3 \mid [a_2, a_1] = a_3 \,\rangle$ is immediate descendant of $C_2 \times C_2$. Also D_{16} is descendant of $C_2 \times C_2$.

Specification of input and output

Algorithm takes as input a d-generator p-group, G, and a description of the automorphism group of G.

It produces as output a *complete* and *irredundant* list of the immediate descendants of G together with a description of their automorphism groups.

G is a p-quotient of F/R and is described by a power-commutator presentation.

A consistent power-commutator presentation is written down for the *p-covering group*, F/R^*, of G, where $R^* = [R, F]R^p$.

Theorem

Every immediate descendant of G is isomorphic to a factor group of F/R^*.

R/R^* is elementary abelian and is the *p-multiplicator* of G.

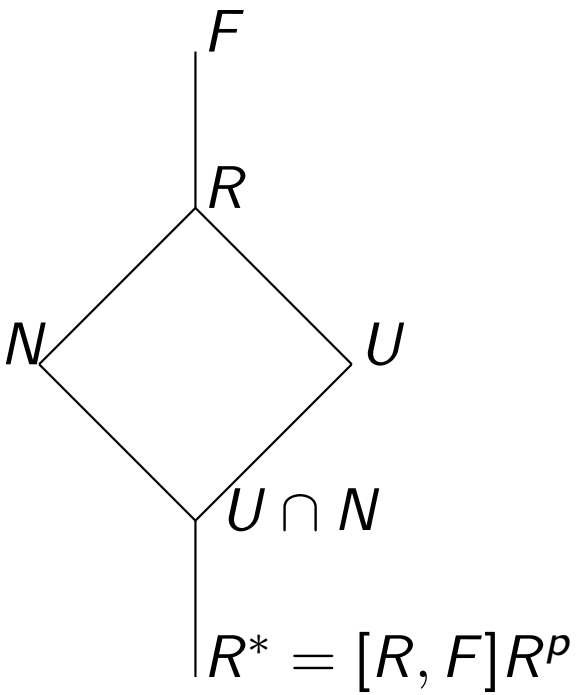
The *nucleus* of G is $P_c(G^*)$.

An *allowable subgroup* is a subgroup of R/R^* which is the kernel of a homomorphism from G^* onto an immediate descendant of G.

The allowable subgroups are characterised as follows.

Lemma

A subgroup is allowable if and only if it is a proper subgroup of the p-multiplicator of G which supplements the nucleus.



Example

The 2-covering group G^* of $G := D_{16}$ is

$$\mathrm{Pc}\langle\, a_1, \ldots, a_4, a_5, a_6, a_7 \quad | \quad a_1^2 = a_6, a_2^2 = a_3 a_4 a_7, \\ a_3^2 = a_4 a_5, a_4^2 = a_5, [a_2, a_1] = a_3, \\ [a_3, a_1] = a_4, [a_4, a_1] = a_5 \rangle.$$

The 2-multiplicator is $\langle a_5, a_6, a_7 \rangle$ and the nucleus is $\langle a_5 \rangle$.

The subgroups $\langle a_6, a_7 \rangle$, $\langle a_5 a_6, a_7 \rangle$, $\langle a_6, a_5 a_7 \rangle$ are allowable and the corresponding immediate descendants have order 32.

The subgroup $\langle a_5 a_6, a_5 a_7 \rangle$ is also allowable, but the resulting quotient is isomorphic to the quotient of G^* by $\langle a_6, a_5 a_7 \rangle$.

On taking factor groups of G^* by all allowable subgroups a *complete* list of immediate descendants is obtained.

This list usually contains redundancies.

To eliminate these redundancies, an obvious equivalence relation is defined on the allowable subgroups.

Definition

Two allowable subgroups U_1/R^* and U_2/R^* are *equivalent* if and only if their quotients F/U_1 and F/U_2 are isomorphic.

A complete and irredundant set of immediate descendants of G can be obtained by factoring G^* by one representative of each equivalence class.

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

Action of automorphisms of G

An *extension* of each automorphism, α, of G to an automorphism, α^*, of G^* is defined.

$\mathrm{Aut}(G)$ induces a linear action on R/R^*.
For $\alpha \in \mathrm{Aut}(G)$, extend it to automorphism α^* of G^*.

If G is generated by $a_1, a_2, \ldots, a_d$ then we choose preimages $x_1, x_2, \ldots, x_d$ in G^* for $a_1, a_2, \ldots, a_d$, and preimages $y_1, y_2, \ldots, y_d$ in G^* for $a_1\alpha, a_2\alpha, \ldots, a_d\alpha$.

Then $x_1, x_2, \ldots, x_d$ generate G^*.

Define α^* by setting $x_i\alpha^* = y_i$ for $i = 1, 2, \ldots, d$.

Lemma

The action of α^* when restricted to R/R^* is uniquely determined by α, and α^* induces a permutation of the allowable subgroups.

Theorem

The equivalence classes of allowable subgroups are exactly the orbits of the allowable subgroups under the action of these permutations.

Hence, to solve the isomorphism problem, we determine orbits of supplements to N/R^* in R/R^* under the induced action of $\mathrm{Aut}(G)$.

Designate one element of each orbit as its representative and factor G^* by each representative in turn to obtain a complete and irredundant list of immediate descendants of G.

An example

We construct the immediate descendants of $G := C_2 \times C_2$

$$\mathrm{Pc}\langle\, a_1,\ a_2 \mid a_1^2 = 1,\ a_2^2 = 1,\ [a_2, a_1] = 1 \,\rangle.$$

Its 2-covering group G^* is

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

where we list only non-trivial relations.

The 2-multiplicator $\langle a_3, a_4, a_5 \rangle$ is elementary abelian and it coincides with the nucleus.

Hence every proper subgroup of the 2-multiplicator supplements the nucleus and so is allowable.

The automorphism group of G is isomorphic to $\mathrm{GL}(2,2)$.

Choose as its generators

$$\alpha_1 : \quad \begin{aligned} a_1 &\longmapsto a_1 a_2 , \\ a_2 &\longmapsto a_2 \end{aligned} \qquad \alpha_2 : \quad \begin{aligned} a_1 &\longmapsto a_2 \\ a_2 &\longmapsto a_1 . \end{aligned}$$

Extensions of these automorphisms to G^* are:

$$\alpha_1^* : \quad \begin{aligned} a_3 &\longmapsto a_3 , \\ a_4 &\longmapsto a_3 a_4 a_5 \\ a_5 &\longmapsto a_5 \end{aligned} \qquad \alpha_2^* : \quad \begin{aligned} a_3 &\longmapsto a_3 \\ a_4 &\longmapsto a_5 \\ a_5 &\longmapsto a_4 . \end{aligned}$$

Construct the immediate descendants of order 8.

The 7 allowable subgroups of rank 2 are

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

The orbits of the allowable subgroups induced by α_1^* and α_2^* are

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

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

$$\begin{aligned}
&\mathrm{Pc}\langle\, a_1, a_2, a_3 \quad | \quad [a_2, a_1] = a_3 \,\rangle \\
&\mathrm{Pc}\langle\, a_1, a_2, a_3 \quad | \quad a_1^2 = a_3,\ a_2^2 = a_3,\ [a_2, a_1] = a_3 \,\rangle \\
&\mathrm{Pc}\langle\, a_1, a_2, a_3 \quad | \quad a_1^2 = a_3 \,\rangle.
\end{aligned}$$

These are: D_8, Q_8 and $C_2 \times C_4$, respectively.

Now construct immediate descendants of $C_2 \times C_2$ having order 16.

Generators for the seven cyclic allowable subgroups are

$$a_3,\ a_3^{\delta} a_4^{\gamma} a_5,\ a_3^{\zeta} a_4,$$

where each of δ, γ, ζ is 0 or 1.

The orbits of the allowable subgroups induced by α_1^* and α_2^* are

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

We choose 1 rep from each orbit to obtain 3 immediate descendants of order 16.

For example, factor G^* by a_3 to obtain $C_4 \times C_4$:

$$\mathrm{Pc}\langle\, a_1, a_2, a_3, a_4 \mid a_1^2 = a_3,\ a_2^2 = a_4 \,\rangle$$

Now construct immediate descendants of $C_2 \times C_2$ having order 32.

Factor G^* by trivial allowable subgroup:

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

where we list only non-trivial relations.

So $C_2 \times C_2$ has 1 immediate descendant of order 2^5.

Practical issues

Central limitation: # of allowable subspaces and consequent size of orbits.

Let's focus on p-class 2 for a moment.

$G = \mathbb{Z}_p^d$. $M := R/R^*$ has rank $m := \binom{d+1}{2}$ as vector space.

Aim: Construct all immediate descendants of order $p^{(d+k)}$.

All subspaces of dimension $m - k$ are allowable.

# of such subspaces is $O(p^{(m-k)k})$, precisely $\frac{\prod_{i=0}^{k-1}(p^m - p^i)}{\prod_{i=0}^{k-1}(p^k - p^i)}$

Example

Let $G = \mathbb{Z}_2^6$, elementary abelian of order 2^6. M has dimension 21.

To construct immediate descendants of order 2^8, must construct orbits on 733006703275 19-dimensional subspaces.

Exploit characteristic structure

$G = \mathbb{Z}_p^d$ acting on V, d-dimensional space.

$A = \mathrm{Aut}(G) \cong \mathrm{GL(d, p)}$ and acts on M.

Since M is a vector space of degree m over $\mathrm{GF}(p)$, it is an A-module.

In fact $M = V_1 \oplus V_2$, where V_1 has dimension $\binom{d}{2}$ and V_2 has dimension d.

Action of A on V_1 is the alternating square representation $\Lambda^2(V)$ for $V = \mathrm{GF}(p)^d$.

Action on V_2 is as $\mathrm{GL(V)}$.

- We consider orbits for action of A on V_1.
- For each orbit rep U, compute its stabiliser S in A.
- Now compute orbits of M/U under S.

More generally given G p-group, $A := \mathrm{Aut}(G)$. M is a A-module. Apply Meataxe to M to identify submodules. Process chain of submodules.

Example

Let $G = \mathbb{Z}_2^6$, elementary abelian of order 2^6. V_1 has dimension 15.

First step: construct orbits on 178940587 13-dimensional subspaces.

Second step: consider orbits of 10795 2-dimensional spaces in 8-dimensional space.

A requirement

We need to know the automorphism group of G, the input group to the algorithm.

A description of the aut gp of an immediate descendant is also returned by the algorithm.

The SmallGroups project

Classification: a topic of long-standing interest.

Cayley (1850s): initiated classification of groups.

Hölder (1890s): groups of square-free order, etc.

Most classifications: by hand, case-by-case, prone to error.

Besche, Eick, and O'B (2000): The "millennium project". Determination / count of groups of order up to 2000 and of "small" composition length.

Many extensions: Dietrich, Eick, Horn and others. Most known up to 20000.

Output available as SmallGroups

Most algorithms part of "grpconst"

Asymptotics

Let $\mathrm{gnu}(n)$ be number of groups of order n.

Pyber (1993)

$$\mathrm{gnu}(n) \leq n^{(2/27+o(1))\mu(n)^2}$$

$\mu(n)$ is largest exponent in the prime-power factorisation of n.

Higman (1960): lower bound for p-class 2 groups of order p^n is $p^{2n^3/27}$.

Sims (1965): upper bound for groups of order p^n
$\mathrm{gnu}(p^n)$ is $p^{2n^3/27+O(n^{8/3})}$.

Blackburn, Neumann & Venkataraman: 8/3 can be reduced to 5/2.

The problem: "Almost all" groups are p-groups of class 2

2^{10}	#
class 2	48 803 495 722
others	423 173 058

Higman (1960): lower bound for p-class 2 of order p^n is $p^{2n^3/27}$

Sims (1965): $\mathrm{gnu}(p^n)$ is $p^{2n^3/27+O(n^{8/3})}$.

Higman: Lower bound for # of orbits of subspaces in $\Lambda^2(V) \oplus V$ under action of $\mathrm{GL(V)}$.

Eick & O'Brien (1999): *precise* version of this for given d and p.

Consequence: can *count* these groups using Cauchy-Frobenius Theorem to count fixed-points for $\mathrm{GL}(\mathrm{d}, \mathrm{p})$ conjugacy class reps, so deduce # of orbits.

Record $\log_{10}$ of the # for $p = 2, 3, 5$.

	$p = 2$	$p = 3$	$p = 5$
p^8	4	5	7
p^9	6	9	13
p^{10}	10	15	22
p^{11}	15	22	33
p^{12}	21	32	46

Groups of order p^6 and p^7

Newman, O'B, Vaughan-Lee (2004)

O'B, Vaughan-Lee (2005)

p^6: various earlier classifications including Easterfield (1940), James (1980).

Classifications available in GAP and Magma as part of SmallGroups

Groups of order p^k for $k = 1, 2, \ldots, 6$

	$p = 2$	$p = 3$	$p \geq 5$
p	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	u
p^6	267	504	v

$$u = 2p + 61 + 2\gcd(p-1, 3) + \gcd(p-1, 4)$$

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

Order p^7

$p = 2$	$p = 3$	$p = 5$
2328	9310	34297

For $p > 5$ the number of groups of order p^7 is

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

Classification of p-groups for arbitrary p

Classify groups of order p^n for $n = 6, 7$ and $p > 5$ by classifying corresponding nilpotent Lie rings of order p^n.

Lazard correspondence: isomorphism between the category of nilpotent Lie rings with order p^n and the category of finite p-groups with order p^n provided $p \geq n$.

Use analogue of p-group generation algorithm to classify the Lie rings.

Use the Baker-Campbell-Hausdorff formula to translate Lie ring presentations into group presentations.

Higman's 1960 PORC conjecture

Conjecture

Fix n. The number of groups of order p^n is Polynomial On Residue Classes.

Higman (1960): the number of groups of order p^n whose Frattini subgroup is elementary abelian and central is PORC.

Evseev (2008): the number of isomorphism classes of groups of order p^n whose Frattini subgroup is central, considered as a function of the prime p, is PORC.

Variants of the p-group generation algorithm

- Automorphism group
- Isomorphism testing

Current implementations

ANU p-Quotient Program: C code; p-quotient algorithm, p-group generation algorithm, isomorphism testing, aut gp.

Program is available

- as a share package with GAP;
- as part of Magma;

A discussion of implementation aspects of the p-quotient algorithm in the GAP language: Celler, Newman, Nickel & Niemeyer (1993); also NNN (1997).

Implementation is also in GAP language.

Some of the algorithms also implemented in Magma language.

References

Papers available from www.math.auckland.ac.nz/~obrien

Derek F. Holt, Bettina Eick and E.A. O'Brien, Handbook of Computational Group Theory, 2005.

Charles C. Sims, Computing with finitely-presented groups, 1994.