Polycyclic presentations and the word problem

Bettina Eick

October 2, 2018

1 Polycyclic groups and their presentations

A group G is polycyclic if it has a polycyclic series; that is, a subnormal series $G = G_1 \geq G_2 \geq G_n \geq G_{n+1} = \{1\}$ with $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} cyclic.

- Choose $g_i \in G$ so that $\langle g_i G_{i+1} \rangle = G_i/G_{i+1}$ for $1 \leq i \leq n$. Then $(g_1, \ldots, g_n)$ is a polycyclic sequence for G.
- Write $o_i = |G_i/G_{i+1}| = |g_i G_{i+1}|$ for $1 \leq i \leq n$ and note that o_i can be finite or infinite. Then o_i is the relative order for g_i.
- A word of the form $g_1^{e_1} \cdots g_n^{e_n}$ with $e_i \in \mathbb{Z}$ and, if o_i is finite, then $0 \leq e_i < o_i$, is a *collected word*.

Note that $|G| = o_1 \cdots o_n$ and this is finite if and only if all o_i are finite.

1 Lemma: *Let $(g_1, \ldots, g_n)$ be a polycyclic sequence for G. Then for every $g \in G$ there exists a unique collected word $g_1^{e_1} \cdots g_n^{e_n}$ with $g = g_1^{e_1} \cdots g_n^{e_n}$.*

Hence each polycyclic sequence of G defines a bijection $G \to \mathbb{Z}_{o_1} \oplus \ldots \oplus \mathbb{Z}_{o_n}$ with $\mathbb{Z} = \mathbb{Z}_{o_i}$ if $o_i = \infty$ and $\mathbb{Z}_{o_i} = \{0, \ldots, o_i - 1\}$ otherwise. Note that this bijection is not a group homomorphism (unless G is abelian).

2 *Example:*

(a) S_4 has the polycyclic sequence $((1,2),(1,2,3),(1,2)(3,4),(1,3)(2,4))$ with relative orders $(2,3,2,2)$. The collected word for $(1,2,3)$ is $g_1^0 g_2^1 g_3^0 g_4^0$. The collected word for $(2,3)$ is $g_1^1 g_2^2 g_3^0 g_4^0$.

(b) Let $D = \langle a, b \rangle \leq GL(2, \mathbb{Z})$ with

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

Then G is polycyclic with $G = G_1$, $G_2 = \langle b \rangle$ and $G_3 = \{1\}$ and relative orders $(2, \infty)$. It follows that

$$G = \{a^{e_1} b^{e_2} \mid e_1 \in \{0,1\}, e_2 \in \mathbb{Z}\} = \{\begin{pmatrix} \pm 1 & 0 \\ x & 1 \end{pmatrix} \mid x \in \mathbb{Z}\}.$$

3 Lemma: *Let $(g_1, \ldots, g_n)$ be a polycyclic sequence for G.*

(a) *For $i < j$ there exist collected words $w^+_{i,j}$ and $w^-_{i,j}$ in the generators $g_{i+1}, \ldots, g_n$ with $g_i^{-1} g_j g_i = w^+_{i,j}$ and $g_i g_j g_i^{-1} = w^-_{i,j}$.*

(b) *For o_i finite there exists a collected word $w_{i,i}$ in the generators $g_{i+1}, \ldots, g_n$ with $g_i^{o_i} = w_{i,i}$.*

4 Theorem: *If $(g_1, \ldots, g_n)$ is a polycyclic sequence for G, then G has a finite presentation on n generators $g_1, \ldots, g_n$ with relations*

- $g_i^{-1} g_j g_i = w^+_{i,j}$ *for* $1 \leq i < j \leq n$,
- $g_i g_j g_i^{-1} = w^-_{i,j}$ *for* $1 \leq i < j \leq n$, $o_i = \infty$,
- $g_i^{o_i} = w_{i,i}$ *for* $1 \leq i \leq n$, $o_i \neq \infty$.

5 *Example:*

(a) A presentation for S_4 on the generators $(g_1, \ldots, g_4) = ((1,2), (1,2,3), (1,2)(3,4), (1,3)(2,4))$ has the relations

$$\begin{aligned} &g_1^2 = g_2^3 = g_3^2 = g_4^2 = 1, \\ &g_2^{g_1} = (1,3,2) = g_2^{-1}, \\ &g_3^{g_1} = g_3, \\ &g_4^{g_1} = (1,4)(2,3) = g_3 g_4, \\ &g_3^{g_2} = (1,4)(2,3) = g_3 g_4, \\ &g_4^{g_2} = (1,2)(3,4) = g_3, \\ &g_3^{g_4} = g_3. \end{aligned}$$

(b) A presentation for $D \leq GL(2, \mathbb{Z})$ on the generators $(g_1, g_2) = (a, b)$ has the relations

$$\begin{aligned} &g_1^2 = 1, \\ &g_1^{-1} g_2 g_1 = g_2^{-1}. \end{aligned}$$

2 Consistency

We now (briefly) consider the problem from a different point of view. Let $(r_1, \ldots, r_n)$ be a sequence with $r_i \in \mathbb{N}$ or $r_i = \infty$. Let P be a presentation on generators $g_1, \ldots, g_n$ with relations

- $g_i^{-1} g_j g_i = w^+_{i,j}$ for $1 \leq i < j \leq n$,
- $g_i g_j g_i^{-1} = w^-_{i,j}$ for $1 \leq i < j \leq n$, $r_i = \infty$,
- $g_i^{r_i} = w_{i,i}$ for $1 \leq i \leq n$, $r_i \neq \infty$.

Then P defines a polycyclic group with polycyclic series $G_i = \langle g_i, \ldots, g_n \rangle$. The generators $(g_1, \ldots, g_n)$ of P are a polycyclic sequence for G. But: the exponents $(r_1, \ldots, r_n)$ are not necessarily the relative orders $(o_1, \ldots, o_n)$ for this sequence.
We say that P is consistent if $r_i = o_i$ for $1 \leq i \leq n$.
There is a method available to check if a given presentation P is consistent. This is fairly expensive, but at least it exists. In the following we will only consider consistent polycyclic presentations.

3 The word problem

Suppose that P is a consistent polycyclic presentation on the generators $g_1, \ldots, g_n$ with relative orders $(o_1, \ldots, o_n)$. The word problem in this presentation can be solved by computing the collected word for an arbitrary word. This can be done using the *collection algorithm*. The basic idea of this algorithm is:

- Choose an uncollected subword of the form $g_j^x g_i^y$ with $i < j$ or g_i^z with $z > o_i$.
- Apply the relations to translate this (assume that $y > 0$):

$$\begin{aligned} g_j^x g_i^y &= g_i^y g_i^{-y} g_j^x g_i^y \\ &= g_i^y (g_i^{-y} g_j g_i^y)^x \\ &= g_i^y (g_i^{-y+1} g_i^{-1} g_j g_i g_i^{y-1})^x \\ &= g_i^y (g_i^{-y+1} w_{i,j}^+ g_i^{y-1})^x \\ &\ldots \\ &= g_i^y (\text{ word in } g_{i+1} \ldots g_n \end{aligned}$$

- Iterated application yields a collected word.

This algorithm allows different strategies. It is important how to choose the next uncollected subword to process. (Collection from the left, see work by Leedham-Green & Soicher [**?**].)
The algorithm is practical in many applications, but complexity is difficult to evaluate in general, see work by Gebhardt [3].
An improved version of collection is described by Assmann & Linton (2007).

6 *Example:* In $D = \langle g_1, g_2 \mid g_1^2 = 1, g_2^{g_1} = g_2^{-1} \rangle$ we collect

$$\begin{aligned} g_2^7 g_1^{13} g_2^{-3} g_1^2 &= g_2^7 g_1 g_2^{-3} \\ &= g_1 (g_2^7)^{g_1} g_2^{-3} \\ &= g_1 (g_2^{g_1})^7 g_2^{-3} \\ &= g_1 (g_2^{-1})^7 g_2^{-3} \\ &= g_1 g_2^{-10} \end{aligned}$$

4 Multiplication

A particular instance of the word problem is the multiplication of two collected words

$$(g_1^{x_1} \cdots g_n^{x_n})(g_1^{y_1} \cdots g_n^{y_n}) = g_1^{f_1(x,y)} \cdots g_n^{f_n(x,y)}.$$

Can one determine $f_1, \ldots, f_n$ as functions?

(a) Hall [4] proved that $f_1, \ldots, f_n$ are rational polynomials if G is torsion-free nilpotent and the polycyclic series associated with the presentation is a central series. Leedham-Green & Soicher [5], Sims [6] and Cant & Eick [1] exhibit methods to compute these Hall polynomials.

(b) Eick [2] proved that $f_1, \ldots, f_n$ are polynomials over $\mathbb{F}_p$ if G is a finite p-group and the polycyclic series is a central series. Again, such polynomials can be computed, but it is even more difficult than (a), since the exponent of the group plays a role.

(c) Du Sautoy (1990) extended Hall's result to group that have a normal torsion-free nilpotent normal subgroup with free abelian quotient.

7 *Example:* Let $G = \langle g_1, g_2, g_3 \mid g_2^{g_1} = g_2 g_3^a, g_3^{g_1} = g_3^{g_2} = g_3 \rangle$. Then $f_1 = x_1 + y_1$, $f_2 = x_2 + y_2$ and $f_3 = a x_2 y_1$.

References

[1] A. Cant and B. Eick. Hall polynomials. *Journal of symbolic comput.*, 2018.

[2] B. Eick. Collection by polynomials in finite p-groups. In *Computational and combinatorial group theory and cryptography*, volume 582 of *Contemp. Math.*, pages 95–103. Amer. Math. Soc., Providence, RI, 2012.

[3] V. Gebhardt. Efficient collection in infinite polycyclic groups. *J. Symb. Comput.*, 34:213 – 228, 2002.

[4] P. Hall. *The Edmonton notes on nilpotent groups.* Queen Mary College Mathematics Notes. Mathematics Department, Queen Mary College, London, 1969.

[5] C. R. Leedham-Green and L. H. Soicher. Symbolic collection using Deep Thought. *LMS J. Comput. Math.*, 1:9 – 24, 1998.

[6] C. C. Sims. *Computation with finitely presented groups.* Cambridge University Press, Cambridge, 1994.