An L_2-quotient algorithm for finitely presented groups

Wilhelm Plesken and Anna Fabiańska

Second Killing and Weierstrass Colloquium
Braniewo, 24-26.03.2010

RWTH AACHEN UNIVERSITY

Motivation

- deciding triviality/infiniteness of finitely presented groups
- computing certain types of factor groups:
  - abelian factor groups
  - nilpotent factor groups
  - soluble factor groups
- PROBLEM: perfect groups (i.e. no abelian quotients)

Starting point

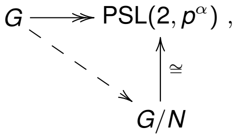
INPUT: a finitely presented group:

$$G := \langle a_1, a_2, \ldots, a_n \mid w_i(a_1, \ldots, a_n), i = 1, \ldots, k \rangle$$

e.g.

$$G := \langle a, b \mid a^2, b^3, (ab)^7, [a, b]^{21} \rangle, \text{ where } [a, b] = a^{-1} b^{-1} ab.$$

AIM: all epimorphisms:



i.e. all factor groups $G/N \cong \mathrm{PSL}(2, p^\alpha)$ for p prime and $\alpha, \beta \in \mathbb{N}$.

Problems

Given a f. p. group $G := \langle a_1, a_2, \ldots, a_n \mid w_i(a_1, \ldots, a_n), i = 1, \ldots, k \rangle$:

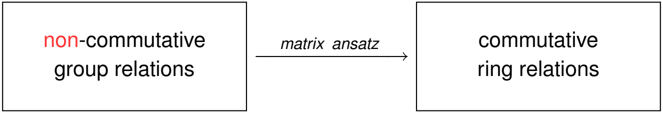
- decide if the set

  $$N_{L_2}(G) := \{N \trianglelefteq G \mid G/N \cong L_2(q) \text{ for some prime power } q\}$$

  is finite.

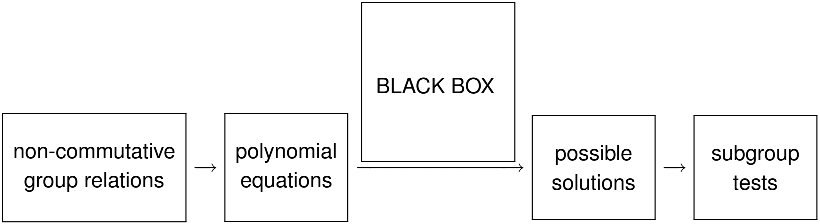
  - in case $|N_{L_2}(G)| < \infty$: give for each $N \in N_{L_2}(G)$ a representation Δ with $N = \ker \Delta$.
  - in case $|N_{L_2}(G)|$ is infinite: give one of the representations and a proof that the set $N_{L_2}(G)$ is infinite.

Main idea: matrix ansatz

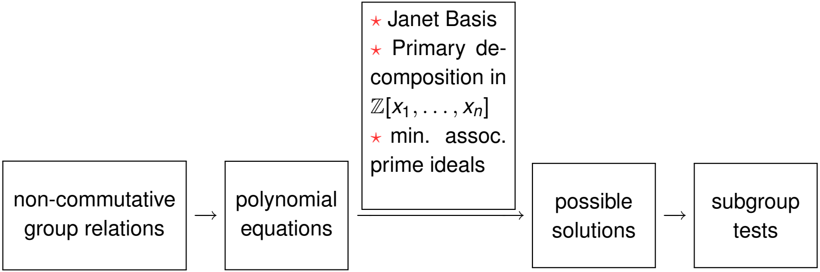


Similar problems:
Plesken, Souvignier (1997)
Plesken, Robertz (2006)

Main idea


non-commutative group relations
polynomial equations
BLACK BOX
possible solutions
subgroup tests

Main idea


non-commutative group relations
polynomial equations
⋆ Janet Basis
⋆ Primary decomposition in $\mathbb{Z}[x_1, \ldots, x_n]$
⋆ min. assoc. prime ideals
possible solutions
subgroup tests

Example: a “naive approach”

Example

$G := \langle a, b \mid a^2, b^3, (ab)^7, [a, b]^{21} \rangle$, where $[a, b] = a^{-1}b^{-1}ab$.

Matrix ansatz:

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \; B := \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$$

Matrix equations:

$$A^2 = \pm I_2, \;\; B^3 = \pm I_2, \;\; (AB)^7 = \pm I_2, \;\; (A^{-1}B^{-1}AB)^{21} = \pm I_2$$

and $\det(A) = 1, \det(B) = 1$.

Example

Example

$G := \langle a, b \mid a^2, b^3, (ab)^7, [a,b]^{21} \rangle$, where $[a,b] = a^{-1}b^{-1}ab$.

Matrix ansatz (w.l.o.g):

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} \\ 0 & a_{2,2} \end{pmatrix}, \; B := \begin{pmatrix} 0 & -1 \\ 1 & b_{2,2} \end{pmatrix}$$

Matrix equations:

$$A^2 = \pm I_2, \;\; B^3 = \pm I_2, \;\; (AB)^7 = \pm I_2, \;\; (A^{-1}B^{-1}AB)^{21} = \pm I_2,$$

and $\det(A) = 1, \det(B) = 1$.

Consider one of the 2^4 possibilities, e.g. $\epsilon = (+,+,+,+)$, then

$$A^2 = \begin{pmatrix} {a_{1,1}}^2 & a_{1,1}a_{1,2} + a_{1,2}a_{2,2} \\ 0 & {a_{2,2}}^2 \end{pmatrix} \text{ and}$$

$$I(G, \Delta, \epsilon) = \langle {a_{1,1}}^2 - 1, \; a_{1,1}a_{1,2} + a_{1,2}a_{2,2}, \; {a_{2,2}}^2 - 1, \ldots, \det(A) - 1 \rangle \trianglelefteq \mathbb{Z}[a_{1,1}, \ldots b_{2,2}]$$

Example

given:

$$I(G, \Delta, \epsilon) \trianglelefteq \mathbb{Z}[a_{1,1}, \ldots b_{2,2}]$$

a solution of corresp. polyn. system $\longrightarrow$ max. ideal $\mathcal{M} \in \mathbb{Z}[a_{1,1}, \ldots b_{2,2}]$ with $I \subset \mathcal{M}$

a solution of corresp. polyn. system $\longrightarrow$ max. ideal $\mathcal{M} \in \mathbb{Z}[a_{1,1}, \ldots b_{2,2}]$ with $P \subset \mathcal{M}$ where P a min. ass. prime of I

Example

Example

$G := \langle a, b \mid a^2, b^3, (ab)^7, [a,b]^{21} \rangle$, where $[a,b] = a^{-1}b^{-1}ab$.

All corresponding minimal associated prime ideals:

$$
\begin{aligned}
P_1 &= \langle 13,\ b_{2,2}+1, a_{2,2}+5, a_{1,2}+8, a_{1,1}+8 \rangle,\\
P_2 &= \langle 13,\ b_{2,2}+1, a_{2,2}+8, a_{1,2}+11, a_{1,1}+5 \rangle,\\
P_3 &= \langle 41,\ b_{2,2}+1, a_{2,2}+9, a_{1,2}+36, a_{1,1}+32 \rangle,\\
P_4 &= \langle 41,\ b_{2,2}+1, a_{2,2}+32, a_{1,2}+18, a_{1,1}+9 \rangle,\\
P_5 &= \langle 43,\ b_{2,2}+1, a_{1,2}+42\,a_{2,2}+35, a_{1,1}+a_{2,2}, a_{2,2}b_{2,2}+a_{2,2}, {a_{2,2}}^2+1 \rangle.
\end{aligned}
$$

Example: Subgroup tests

1. $P_1 = \langle 13,\ b_{2,2}+1, a_{2,2}+5, a_{1,2}+8, a_{1,1}+8\rangle$

   Do the matrices

   $$A := \begin{pmatrix} -8 & -8 \\ 0 & -5 \end{pmatrix},\ B := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

   generate PSL(2, 13) or a subgroup of it?

2. $P_5 = \langle 43,\ b_{2,2}+1, a_{1,2}+42\, a_{2,2}+35, a_{1,1}+a_{2,2}, a_{2,2}b_{2,2}+a_{2,2}, {a_{2,2}}^2+1\rangle$

   Do matrices

   $$A := \begin{pmatrix} -a_{2,2} & a_{2,2}+8 \\ 0 & a_{2,2} \end{pmatrix},\ B := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

   generate $\mathrm{PSL}(2, 43^2)$, PSL(2, 43), or a subgroup of one of them?

→ Subgroup tests, Dickson’s Classification Theorem (1901)

→ Galois descent

Example: summary

Example

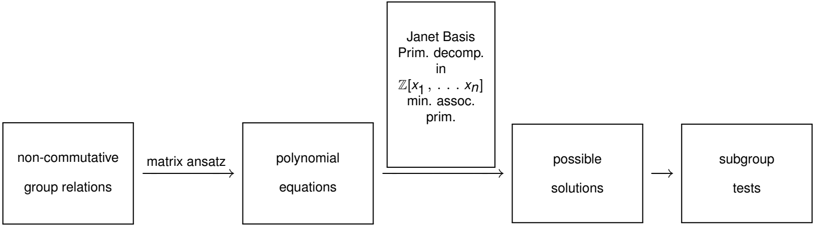
$G := \langle a, b \mid a^2, b^3, (ab)^7, [a, b]^{21} \rangle$, where $[a, b] = a^{-1}b^{-1}ab$.

Five minimal associated primes:

$$
\begin{aligned}
P_1 &= \langle 13,\ b_{2,2}+1, a_{2,2}+5, a_{1,2}+8, a_{1,1}+8 \rangle,\\
P_2 &= \langle 13,\ b_{2,2}+1, a_{2,2}+8, a_{1,2}+11, a_{1,1}+5 \rangle,\\
P_3 &= \langle 41,\ b_{2,2}+1, a_{2,2}+9, a_{1,2}+36, a_{1,1}+32 \rangle,\\
P_4 &= \langle 41,\ b_{2,2}+1, a_{2,2}+32, a_{1,2}+18, a_{1,1}+9 \rangle,\\
P_5 &= \langle 43,\ b_{2,2}+1, a_{1,2}+42\, a_{2,2}+35, a_{1,1}+a_{2,2}, a_{2,2}b_{2,2}+a_{2,2}, {a_{2,2}}^2+1 \rangle.
\end{aligned}
$$

and finitely many epimorphic images of L_2-type:
PSL(2, 13), PSL(2, 41), and PSL(2, 43)

Main problems



Main problems:

1. multiplication of matrices (long words)
2. subgroup tests

New idea: properties of traces

1. Let X be a 2×2 matrix of determinant 1.

   Is it possible to compute $\mathrm{tr}(X^n), \ldots, \mathrm{tr}(w(X))$ knowing only $\mathrm{tr}(X)$?

2. Let $X_1, \ldots, X_n$ be 2×2 matrices of determinat 1.

   Is it possible to compute $\mathrm{tr}(w(X_1, \ldots, X_n))$ knowing only $\mathrm{tr}(X_1), \ldots, \mathrm{tr}(X_n)$?

Example

What is the trace

$$\mathrm{tr}(w(A, B)) \text{ for } w = [a, b] \in F_2,$$

where A, B are 2×2-matrices of determinant 1?

Properties of traces

For 2×2 matrices X, Y of determinant 1:

1. $\mathrm{tr}(XY) - \mathrm{tr}(X)\,\mathrm{tr}(Y) = \det(X) + \det(Y) - \det(X + Y)$
2. $\mathrm{tr}(XY) = \mathrm{tr}(YX)$
3. $\mathrm{tr}(XXY) = \mathrm{tr}(X)\,\mathrm{tr}(XY) - \mathrm{tr}(Y)$
4. $\mathrm{tr}(X^{-1}) = \mathrm{tr}(X)$

Theorem

Let X be a 2×2 matrix of determinant 1 and trace $\operatorname{tr}(X) = x$.
Let $T_n(x)$ be the trace of X^n. Then,

$$\begin{aligned} T_0(x) &= 2, \\ T_1(x) &= x \\ \textit{and} \quad T_{n+1}(x) &= xT_n(x) - T_{n-1}(x). \end{aligned}$$

Chebyshev polynomials
of the first kind

$$\begin{aligned} C_0(x) &= 2 \\ C_1(x) &= x \\ C_{n+1}(x) &= 2\,x\,C_n(x) - C_{n-1}(x) \end{aligned}$$

$\longrightarrow$

$$\begin{aligned} T_0(x) &= 2 \\ T_1(x) &= x \\ T_{n+1}(x) &= x\,T_n(x) - T_{n-1}(x) \end{aligned}$$

i.e. $T_n(x) = 2\,C_n(\frac{x}{2})$ for $n > 1$.

Generalized Chebyshev polynomials

Definition (Plesken, F., 2009)

Multivariate polynomials p_w, satisfying

$$\begin{aligned} p_1 &= 2 \\ p_{wv} &= p_{vw} \\ p_{wwv} &= p_w p_{wv} - p_v \end{aligned}$$

are called the *generalized Chebyshev polynomials*.

Example

What is the trace

$$\operatorname{tr}(w(A,B)) \text{ for } w = [a,b] \in F_2,$$

where A, B are 2×2-matrices of determinant 1?

Generalized Chebyshev polynomials: Example

Rules: $p_1 = 2 \qquad p_{wv} = p_{vw} \qquad p_{wwv} = p_w p_{wv} - p_v.$

Then:

1. $p_{a^2} = p_{aa} = p_{aaa^{-1}a} = p_a\, p_{a^{-1}} - p_{a^{-1}a} = p_a\, p_a - 2 = p_a^2 - 2$
2. $p_{baab} = p_{aabb} = p_a\, p_{abb} - p_{bb} = p_a\,(p_b\, p_{ba} - p_a) - p_{bb} =$
   $= p_a\, p_b\, p_{ba} - {p_a}^2 - {p_b}^2 + 2$
3. $p_{a^{-1}b^{-1}ab} = p_{a^{-1}b^{-1}a^{-1}b^{-1}baab} = p_{a^{-1}b^{-1}}\, p_{ab} - p_{baab} = p_{(ab)^{-1}}\, p_{ab} - p_{baab} =$
   $= {p_{ab}}^2 - (p_a\, p_b\, p_{ba} - {p_a}^2 - {p_b}^2 + 2) = {p_a}^2 + {p_b}^2 + {p_{ab}}^2 - p_a\, p_b\, p_{ba} - 2$

Thus finally:

$$\operatorname{tr}(A^{-1}B^{-1}AB) = \operatorname{tr}(A)^2 + \operatorname{tr}(B)^2 + \operatorname{tr}(AB)^2 - \operatorname{tr}(A)\operatorname{tr}(B)\operatorname{tr}(AB) - 2$$

Theorem (Plesken, F., 2009)

For every $w = w(g_1, g_2) \in F_2$ there exists a unique polynomial

$$p_w(x_1, x_2, x_{12}) \in \mathbb{Z}[x_1, x_2, x_{12}]$$

satisfying for every $\Delta : F_2 \to \mathrm{SL}(2, R) : g_i \mapsto X_i$ (for any integral domain R) the property

$$\mathrm{tr}(\Delta(w)) = p_w(\mathrm{tr}(X_1), \mathrm{tr}(X_2), \mathrm{tr}(X_1\ X_2)).$$

Similarly for $w \in F_3$:

$$\mathrm{tr}(\Delta(w)) = p_w(\mathrm{tr}(X_1),\ \mathrm{tr}(X_2),\ \mathrm{tr}(X_3),\ \mathrm{tr}(X_1\,X_2),\ \mathrm{tr}(X_1\,X_3),\ \mathrm{tr}(X_2\,X_3),\ \mathrm{tr}(X_1\,X_2\,X_3)).$$

Matrix ansatz

Matrix ansatz in case of two generators:

$$A := \begin{pmatrix} \alpha & x_2\alpha - x_1x_2 + x_{12} \\ 0 & -\alpha + x_1 \end{pmatrix},\; B := \begin{pmatrix} 0 & -1 \\ 1 & x_2 \end{pmatrix},$$

where

$$\mathrm{tr}(A) = x_1,\; \mathrm{tr}(B) = x_2 \text{ and } \mathrm{tr}(AB) = x_{12}.$$

Example (finitely many primes, infinitely many L_2-quotients)

$$G := \langle a, b, c \mid a^3,\ b^3,\ c^2,\ (ca)^3,\ [a, b] \rangle$$

- only one prime ideal passes the subgroup tests:

$$P_1 := \langle 3,\ x_{23} + 2\,x_{123} + 2,\ x_{13} + 1,\ x_{12} + 1,\ x_3,\ x_2 + 1,\ x_1 + 1 \rangle$$

- the Krull dimension of P_1 is one (in $\mathbb{Z}[x_1, \ldots x_{123}]$)
- x_{123} is a free variable
- thus for any $\alpha \in \mathbb{N}$ one gets $\mathrm{PSL}(2, 3^\alpha)$ as an epimorphic image of G (by specifying x_{123} by an irreducible polynomial of degree α)

Example (infinitely many primes infinitely many L_2-quotients for every prime)

$$G := \langle a, b, c \mid a^2, b^2, c^2, (ab)^3, (ac)^4, (bc)^5 \rangle.$$

- only one prime ideal passes the subgroup tests

$$P_1 := \langle 1 - 7\,x_{123}{}^4 + 2\,x_{123}{}^2 + 2\,x_{123}{}^6 + x_{123}{}^8, 1 - 5\,x_{123}{}^4 + 3\,x_{23} + 10\,x_{123}{}^2 - 2\,x_{123}{}^6, x_{23}x_{123}{}^2 + 1 - 3\,x_{123}{}^4 + x_{23} + 5\,x_{123}{}^2 - x_{123}{}^6, x_{23}{}^2 + x_{23} - 1, x_{12} + 1, x_3, x_2, x_1 \rangle$$

- $\mathbb{Q}P_1$ of Krull dim. 0 in $\mathbb{Q}[x_1, x_2, x_3, x_{12}, x_{13}, x_{23}, x_{123}]$,
- for every prime p: finitely many (from 1 to 8) max. ideals in char. p containing P_1, e.g.

$p = 7$:	$\mathrm{PGL}(2, p^2)$ twice
$p = 13$:	$\mathrm{PSL}(2, p^2)$ four times
$p = 31$:	$\mathrm{PSL}(2, p)$ four times and $\mathrm{PGL}(2, p)$ twice
$p = 241$:	$\mathrm{PSL}(2, p)$ as epimorphic image of G eight times

Summary

L_2-quotient algorithm: enumeration of all epimorphic images of L_2-type

Applications:

- examination of f. p. groups
- in certain cases: proof of infiniteness of a group

Implementation:

- Maple-package PSL
  `http://wwwb.math.rwth-aachen.de/projekte.php`

Tools:

- Janet Basis (special Groebner basis) of an ideal in a polynomial ring, INVOLUTIVE (Y. Blinkov, C. Cid, V. Gerdt, W. Plesken, D. Robertz)
- minimal associated primes for ideals in $\mathbb{Z}[x_1, \ldots, x_n]$, PRIMDECOMP (M. Lange-Hegermann)
- generalized Chebyshev polynomials

Further problems

1. finitely presented groups given on $n > 3$ generators
2. other epiomorphic images, e.g. PSL$(3, q)$, PSL$(4, q)$, (S. Jambor)

Anna Fabiańska
fabianska@momo.math.rwth-aachen.de

Lehrstuhl B für Mathematik, RWTH Aachen University, Germany.
http://wwwb.math.rwth-aachen.de