Computing polycyclic quotients of finitely (L-)presented groups via Gröbner bases

Max Horn

joint work with Bettina Eick

Technische Universität Braunschweig

ICMS 2010, Kobe, Japan

Overview

Overview

Quotient Algorithms

- A quotient algorithm takes a group G (e.g. given via a finite presentation) and computes a quotient H.
- An *effective* quotient map $\pi : G \to H$ is also computed, i.e., allowing computation of images and preimages.
- H is ideally more tractable than G (e.g. finite or nilpotent), yet should share interesting features of G.
- Development and implementation of quotients methods for finitely presented groups have a long history.

Quotient Algorithms

- A quotient algorithm takes a group G (e.g. given via a finite presentation) and computes a quotient H.
- An *effective* quotient map $\pi : G \to H$ is also computed, i.e., allowing computation of images and preimages.
- H is ideally more tractable than G (e.g. finite or nilpotent), yet should share interesting features of G.
- Development and implementation of quotients methods for finitely presented groups have a long history.

Quotient Algorithms

- A quotient algorithm takes a group G (e.g. given via a finite presentation) and computes a quotient H.
- An *effective* quotient map $\pi : G \to H$ is also computed, i.e., allowing computation of images and preimages.
- H is ideally more tractable than G (e.g. finite or nilpotent), yet should share interesting features of G.
- Development and implementation of quotients methods for finitely presented groups have a long history.

Quotient Algorithms

- A quotient algorithm takes a group G (e.g. given via a finite presentation) and computes a quotient H.
- An *effective* quotient map $\pi : G \to H$ is also computed, i.e., allowing computation of images and preimages.
- H is ideally more tractable than G (e.g. finite or nilpotent), yet should share interesting features of G.
- Development and implementation of quotients methods for finitely presented groups have a long history.

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group
$\Leftrightarrow$ H is solvable and all subgroups are finitely generated
$\Leftrightarrow$ $\exists$ series $H = H_1 \rhd \ldots \rhd H_n \rhd 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group
$\Leftrightarrow$ H is solvable and all subgroups are finitely generated
$\Leftrightarrow$ $\exists$ series $H = H_1 \triangleright \ldots \triangleright H_n \triangleright 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing . . .

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group
$\Leftrightarrow$ H is solvable and all subgroups are finitely generated
$\Leftrightarrow$ $\exists$ series $H = H_1 \triangleright \ldots \triangleright H_n \triangleright 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group
$\Leftrightarrow$ H is solvable and all subgroups are finitely generated
$\Leftrightarrow$ $\exists$ series $H = H_1 \triangleright \ldots \triangleright H_n \triangleright 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group

$\Leftrightarrow$ H is solvable and all subgroups are finitely generated

$\Leftrightarrow$ $\exists$ series $H = H_1 \triangleright \ldots \triangleright H_n \triangleright 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group

$\Leftrightarrow$ H is solvable and all subgroups are finitely generated

$\Leftrightarrow$ $\exists$ series $H = H_1 \rhd \ldots \rhd H_n \rhd 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group

$\Leftrightarrow$ H is solvable and all subgroups are finitely generated

$\Leftrightarrow$ $\exists$ series $H = H_1 \rhd \ldots \rhd H_n \rhd 1$ with H_i / H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing . . .

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group

$\Leftrightarrow$ H is solvable and all subgroups are finitely generated

$\Leftrightarrow$ $\exists$ series $H = H_1 \rhd \ldots \rhd H_n \rhd 1$ with H_i/H_{i+1} cyclic

Types of Quotient Algorithms

Let G be a finitely presented group. Various quotient algorithms exist for such groups. They allow computing ...

- maximal abelian quotients, i.e., G/G'
- finite p-group quotients (Newman and O'Brien)
- finite solvable quotients (Niemeyer; Brückner and Plesken)
- nilpotent quotients (Nickel)
- polycyclic quotients (Lo; most general in this sequence)

H is a polycyclic group
$\Leftrightarrow$ H is solvable and all subgroups are finitely generated
$\Leftrightarrow$ $\exists$ series $H = H_1 \triangleright \ldots \triangleright H_n \triangleright 1$ with H_i/H_{i+1} cyclic

Our contribution

We implemented a polycyclic quotient algorithm for L-presented groups, partially based on the work by Eddie Lo.

What is new?

- Extended input: L-presented, generalizing f.p.
- Flexibility: can compute polycylic, nilpotent, and "intermediate" quotients (note: a nilpotent quotient algorithm for L-presented due to Bartholdi, Eick and Hartung already exists)
- Effectivity: new ideas to improve algorithm

Moreover, it can be used everywhere GAP 4 runs. In contrast, Lo's algorithm is difficult to use on modern computers (compilation issues, relies on GAP 3).

Our contribution

We implemented a polycyclic quotient algorithm for L-presented groups, partially based on the work by Eddie Lo.

What is new?

- Extended input: L-presented, generalizing f.p.
- Flexibility: can compute polycylic, nilpotent, and "intermediate" quotients (note: a nilpotent quotient algorithm for L-presented due to Bartholdi, Eick and Hartung already exists)
- Effectivity: new ideas to improve algorithm

Moreover, it can be used everywhere GAP 4 runs. In contrast, Lo's algorithm is difficult to use on modern computers (compilation issues, relies on GAP 3).

Our contribution

We implemented a polycyclic quotient algorithm for L-presented groups, partially based on the work by Eddie Lo.

What is new?

- Extended input: L-presented, generalizing f.p.
- Flexibility: can compute polycylic, nilpotent, and "intermediate" quotients (note: a nilpotent quotient algorithm for L-presented due to Bartholdi, Eick and Hartung already exists)
- Effectivity: new ideas to improve algorithm

Moreover, it can be used everywhere GAP 4 runs. In contrast, Lo's algorithm is difficult to use on modern computers (compilation issues, relies on GAP 3).

Overview

L-presentations

Let X be a finite set of abstract generators, let F be the free group on X. Let R and Q be finite subsets of F and ϕ a finite set of endomorphisms of F. Then

$$\langle X \mid Q \mid \phi \mid R \rangle$$

is called a (finite) L-presentation.

Denote by ϕ^* the monoid generated by ϕ. Then the finite L-presentation defines a group F/K, where

$$K = \langle Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R) \rangle^F \trianglelefteq F.$$

F/K is a (finitely) L-presented group.

Examples of L-presented groups

- Every finitely presented group $\langle X \mid S \rangle$ is finitely L-presented, e.g. as $\langle X \mid S \mid \emptyset \mid \emptyset \rangle$ or as $\langle X \mid \emptyset \mid \emptyset \mid S \rangle$.
- There are interesting groups which are not finitely presented but admit finite L-presentations.
- The Grigorchuk group arose as a counterexample to the Burnside problem and has very interesting properties.

  ...2-group, amenable, automatic, intermediate growth, just infinite, residually finite...
- The Basilica group is an example with easy description.

  ...amenable, automatic, exponential growth, just non-solvable ...

$$\left\langle a, b \mid \emptyset \mid (a, b) \mapsto (b^2, a) \mid [a, b^{-1}ab] \right\rangle$$

Examples of L-presented groups

- Every finitely presented group $\langle X \mid S \rangle$ is finitely L-presented, e.g. as $\langle X \mid S \mid \emptyset \mid \emptyset \rangle$ or as $\langle X \mid \emptyset \mid \emptyset \mid S \rangle$.
- There are interesting groups which are not finitely presented but admit finite L-presentations.
- The Grigorchuk group arose as a counterexample to the Burnside problem and has very interesting properties.

  …2-group, amenable, automatic, intermediate growth, just infinite, residually finite…
- The Basilica group is an example with easy description.

  …amenable, automatic, exponential growth, just non-solvable …

$$\langle a, b \mid \emptyset \mid (a, b) \mapsto (b^2, a) \mid [a, b^{-1}ab] \rangle$$

Examples of L-presented groups

- Every finitely presented group $\langle X \mid S \rangle$ is finitely L-presented, e.g. as $\langle X \mid S \mid \emptyset \mid \emptyset \rangle$ or as $\langle X \mid \emptyset \mid \emptyset \mid S \rangle$.
- There are interesting groups which are not finitely presented but admit finite L-presentations.
- The Grigorchuk group arose as a counterexample to the Burnside problem and has very interesting properties.

  ...2-group, amenable, automatic, intermediate growth, just infinite, residually finite...
- The Basilica group is an example with easy description.

  ...amenable, automatic, exponential growth, just non-solvable ...

$$\langle a, b \mid \emptyset \mid (a, b) \mapsto (b^2, a) \mid [a, b^{-1}ab] \rangle$$

Examples of L-presented groups

- Every finitely presented group $\langle X \mid S \rangle$ is finitely L-presented, e.g. as $\langle X \mid S \mid \emptyset \mid \emptyset \rangle$ or as $\langle X \mid \emptyset \mid \emptyset \mid S \rangle$.
- There are interesting groups which are not finitely presented but admit finite L-presentations.
- The Grigorchuk group arose as a counterexample to the Burnside problem and has very interesting properties.

  ... 2-group, amenable, automatic, intermediate growth, just infinite, residually finite...
- The Basilica group is an example with easy description.

  ... amenable, automatic, exponential growth, just non-solvable ...

$$\left\langle a, b \mid \emptyset \mid (a, b) \mapsto (b^2, a) \mid [a, b^{-1}ab] \right\rangle$$

Overview

Quotient algorithm: Overview

Steps of polycyclic quotient algorithm:

- Input: group G, positive integer c
- Output: polycyclic pres. of $G/G^{(c)}$ if it exists, or an error (recall $G^{(0)} := G$, $G^{(i+1)} := [G^{(i)}, G^{(i)}]$)
- Also computes *effective* epimorphism $\psi_c : G \to G/G^{(c)}$.

Use an inductive approach:

- Start with the trivial epimorphism $\psi_0 : G \to 1 = G/G^{(0)}$.
- Repeatedly run extension algorithm: Extend effective epimorphism $\psi_i : G \to G/G^{(i)}$, to $\psi_{i+1} : G \to G/G^{(i+1)}$ and determine polycyclic presentation of $G/G^{(i+1)}$, if any, or an error.

Extension algorithm: Overview

Input:

- An L-presented G and a polycyclic presented H;
- An effective epimorphism $\psi : G \to H$ with kernel N;
- A description for a subgroup $U \trianglelefteq H$.

Set $M := [\psi^{-1}(U), N]$.
$U = 1 \implies M = N' \rightsquigarrow$ polycyclic quotients.
$U = H \implies M = [G, N] \rightsquigarrow$ nilpotent quotients.
From now on $U = 1$ and $M = N'$.

Output:

- Check whether G/M is polycyclic, and, if so, then
- an effective epimorphism $\nu : G \to K$ with kernel M and polycyclic presentation for K.

Extension algorithm: Overview

Input:

- An L-presented G and a polycyclic presented H;
- An effective epimorphism $\psi : G \to H$ with kernel N;
- A description for a subgroup $U \trianglelefteq H$.

Set $M := [\psi^{-1}(U), N]$.

$U = 1 \implies M = N' \rightsquigarrow$ polycyclic quotients.

$U = H \implies M = [G, N] \rightsquigarrow$ nilpotent quotients.

From now on $U = 1$ and $M = N'$.

Output:

- Check whether G/M is polycyclic, and, if so, then
- an effective epimorphism $\nu : G \to K$ with kernel M and polycyclic presentation for K.

Extension algorithm: Overview

Input:

- An L-presented G and a polycyclic presented H;
- An effective epimorphism $\psi : G \to H$ with kernel N;
- A description for a subgroup $U \trianglelefteq H$.

Set $M := [\psi^{-1}(U), N]$.
$U = 1 \implies M = N' \rightsquigarrow$ polycyclic quotients.
$U = H \implies M = [G, N] \rightsquigarrow$ nilpotent quotients.
From now on $U = 1$ and $M = N'$.

Output:

- Check whether G/M is polycyclic, and, if so, then
- an effective epimorphism $\nu : G \to K$ with kernel M and polycyclic presentation for K.

Extension algorithm: Overview

Input:

- An L-presented G and a polycyclic presented H;
- An effective epimorphism $\psi : G \to H$ with kernel N;
- A description for a subgroup $U \trianglelefteq H$.

Set $M := [\psi^{-1}(U), N]$.
$U = 1 \implies M = N' \leadsto$ polycyclic quotients.
$U = H \implies M = [G, N] \leadsto$ nilpotent quotients.
From now on $U = 1$ and $M = N'$.

Output:

- Check whether G/M is polycyclic, and, if so, then
- an effective epimorphism $\nu : G \to K$ with kernel M and polycyclic presentation for K.

Extension algorithm: Overview

Input:

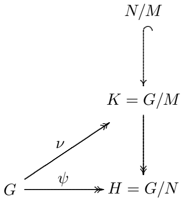
- An L-presented G and a polycyclic presented H;
- An effective epimorphism $\psi : G \to H$ with kernel N;
- A description for a subgroup $U \trianglelefteq H$.

Set $M := [\psi^{-1}(U), N]$.
$U = 1 \implies M = N' \rightsquigarrow$ polycyclic quotients.
$U = H \implies M = [G, N] \rightsquigarrow$ nilpotent quotients.
From now on $U = 1$ and $M = N'$.

Output:

- Check whether G/M is polycyclic, and, if so, then
- an effective epimorphism $\nu : G \to K$ with kernel M and polycyclic presentation for K.

Extension algorithm: Overview (cont.)

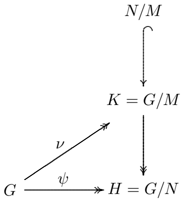


- N/M is a (right) $\mathbb{Z}H$-module.
- K is an extension of N/M by H.

Steps:

1. Compute finite $\mathbb{Z}H$-module presentation for N/M.
2. Check whether N/M has finite $\mathbb{Z}$-rank ($\Leftrightarrow$ K is polycyclic), and, if so, then
3. determine generators for N/M as abelian group; extend N/M by H to K and ψ to ν.

Extension algorithm: Overview (cont.)

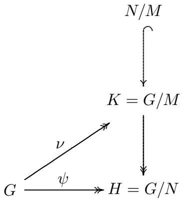


- N/M is a (right) $\mathbb{Z}H$-module.
- K is an extension of N/M by H.

Steps:

1. Compute finite $\mathbb{Z}H$-module presentation for N/M.
2. Check whether N/M has finite $\mathbb{Z}$-rank ($\Leftrightarrow K$ is polycyclic), and, if so, then
3. determine generators for N/M as abelian group; extend N/M by H to K and ψ to ν.

Extension algorithm: Overview (cont.)

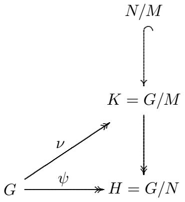


- N/M is a (right) $\mathbb{Z}H$-module.
- K is an extension of N/M by H.

Steps:

1. Compute finite $\mathbb{Z}H$-module presentation for N/M.
2. Check whether N/M has finite $\mathbb{Z}$-rank ($\Leftrightarrow$ K is polycyclic), and, if so, then
3. determine generators for N/M as abelian group; extend N/M by H to K and ψ to ν.

Extension algorithm: Overview (cont.)



- N/M is a (right) $\mathbb{Z}H$-module.
- K is an extension of N/M by H.

Steps:

1. Compute finite $\mathbb{Z}H$-module presentation for N/M.
2. Check whether N/M has finite $\mathbb{Z}$-rank ($\Leftrightarrow$ K is polycyclic), and, if so, then
3. determine generators for N/M as abelian group; extend N/M by H to K and ψ to ν.

Extension algorithm: Step 1

Step 1: Compute a finite $\mathbb{Z}H$-module presentation for N/M.

- $N/M \cong V/W$ for a free $\mathbb{Z}H$-module V of finite rank and a submodule W.
- W is determined by the relations of G, plus $\psi : G \to H$.
- Problem: Infinitely many relators: $Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R)$.
- But we can filter the relators by length of σ, this yields an ascending chain of submodules $W_1 \subseteq W_2 \subseteq \ldots \subseteq W$.
- $\mathbb{Z}H$-modules are Noetherian (as H is polycyclic), hence $\exists n \in \mathbb{N}$, such that $W_n = W_{n+1} = W_{n+2} = \ldots = W$.

Extension algorithm: Step 1

Step 1: Compute a finite $\mathbb{Z}H$-module presentation for N/M.

- $N/M \cong V/W$ for a free $\mathbb{Z}H$-module V of finite rank and a submodule W.
- W is determined by the relations of G, plus $\psi : G \to H$.
- Problem: Infinitely many relators: $Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R)$.
- But we can filter the relators by length of σ, this yields an ascending chain of submodules $W_1 \subseteq W_2 \subseteq \ldots \subseteq W$.
- $\mathbb{Z}H$-modules are Noetherian (as H is polycyclic), hence $\exists n \in \mathbb{N}$, such that $W_n = W_{n+1} = W_{n+2} = \ldots = W$.

Extension algorithm: Step 1

Step 1: Compute a finite $\mathbb{Z}H$-module presentation for N/M.

- $N/M \cong V/W$ for a free $\mathbb{Z}H$-module V of finite rank and a submodule W.
- W is determined by the relations of G, plus $\psi : G \to H$.
- Problem: Infinitely many relators: $Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R)$.
- But we can filter the relators by length of σ, this yields an ascending chain of submodules $W_1 \subseteq W_2 \subseteq \ldots \subseteq W$.
- $\mathbb{Z}H$-modules are Noetherian (as H is polycyclic), hence $\exists n \in \mathbb{N}$, such that $W_n = W_{n+1} = W_{n+2} = \ldots = W$.

Extension algorithm: Step 1

Step 1: Compute a finite $\mathbb{Z}H$-module presentation for N/M.

- $N/M \cong V/W$ for a free $\mathbb{Z}H$-module V of finite rank and a submodule W.
- W is determined by the relations of G, plus $\psi : G \to H$.
- Problem: Infinitely many relators: $Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R)$.
- But we can filter the relators by length of σ, this yields an ascending chain of submodules $W_1 \subseteq W_2 \subseteq \ldots \subseteq W$.
- $\mathbb{Z}H$-modules are Noetherian (as H is polycyclic), hence $\exists n \in \mathbb{N}$, such that $W_n = W_{n+1} = W_{n+2} = \ldots = W$.

Extension algorithm: Step 1

Step 1: Compute a finite $\mathbb{Z}H$-module presentation for N/M.

- $N/M \cong V/W$ for a free $\mathbb{Z}H$-module V of finite rank and a submodule W.
- W is determined by the relations of G, plus $\psi : G \to H$.
- Problem: Infinitely many relators: $Q \cup \bigcup_{\sigma \in \phi^*} \sigma(R)$.
- But we can filter the relators by length of σ, this yields an ascending chain of submodules $W_1 \subseteq W_2 \subseteq \ldots \subseteq W$.
- $\mathbb{Z}H$-modules are Noetherian (as H is polycyclic), hence $\exists n \in \mathbb{N}$, such that $W_n = W_{n+1} = W_{n+2} = \ldots = W$.

Extension algorithm: Steps 2 & 3

Step 2: Is N/M finitely generated as abelian group?

- Compute Gröbner basis of W, use this to determine $\mathbb{Z}$-rank of V/W.
- For this, adapt methods by Lo and Madlener-Reinert.

Step 3: Finding group generators for $N/M \cong V/W$ and extending N/M by H to K and ψ to ν.

- Generators can be extracted from the Gröbner basis.
- Rest is tedious, but doable (linear algebra over integers).

Extension algorithm: Steps 2 & 3

Step 2: Is N/M finitely generated as abelian group?

- Compute Gröbner basis of W, use this to determine $\mathbb{Z}$-rank of V/W.
- For this, adapt methods by Lo and Madlener-Reinert.

Step 3: Finding group generators for $N/M \cong V/W$ and extending N/M by H to K and ψ to ν.

- Generators can be extracted from the Gröbner basis.
- Rest is tedious, but doable (linear algebra over integers).

Extension algorithm: Steps 2 & 3

Step 2: Is N/M finitely generated as abelian group?

- Compute Gröbner basis of W, use this to determine $\mathbb{Z}$-rank of V/W.
- For this, adapt methods by Lo and Madlener-Reinert.

Step 3: Finding group generators for $N/M \cong V/W$ and extending N/M by H to K and ψ to ν.

- Generators can be extracted from the Gröbner basis.
- Rest is tedious, but doable (linear algebra over integers).

Extension algorithm: Steps 2 & 3

Step 2: Is N/M finitely generated as abelian group?

- Compute Gröbner basis of W, use this to determine $\mathbb{Z}$-rank of V/W.
- For this, adapt methods by Lo and Madlener-Reinert.

Step 3: Finding group generators for $N/M \cong V/W$ and extending N/M by H to K and ψ to ν.

- Generators can be extracted from the Gröbner basis.
- Rest is tedious, but doable (linear algebra over integers).

Extension algorithm: Steps 2 & 3

Step 2: Is N/M finitely generated as abelian group?

- Compute Gröbner basis of W, use this to determine $\mathbb{Z}$-rank of V/W.
- For this, adapt methods by Lo and Madlener-Reinert.

Step 3: Finding group generators for $N/M \cong V/W$ and extending N/M by H to K and ψ to ν.

- Generators can be extracted from the Gröbner basis.
- Rest is tedious, but doable (linear algebra over integers).

Overview

Towards Gröbner bases in group rings

Group ring elements of $\mathbb{K}G$ are similar to polynomials.
Which properties are crucial for Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials. $\rightsquigarrow$ Well partial order $\preceq$ on group elements.

(P2) Finite monomial set have a *unique* least common multiple $\rightsquigarrow$ finite subsets of G with a common upper bound have a unique least common upper bound

(P3) A total order $\leq$ linearizaing $\preceq$ (necessarily a well-order).

(P4) $g \preceq xg$ and $f \leq g \implies xf \leq xg$.

Allows reduction, syzygies, finiteness of Gröbner bases ...

Towards Gröbner bases in group rings

Group ring elements of $\mathbb{K}G$ are similar to polynomials.
Which properties are crucial for Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials. $\rightsquigarrow$ Well partial order $\preceq$ on group elements.

(P2) Finite monomial set have a *unique* least common multiple $\rightsquigarrow$ finite subsets of G with a common upper bound have a unique least common upper bound

(P3) A total order $\leq$ linearizaing $\preceq$ (necessarily a well-order).

(P4) $g \preceq xg$ and $f \leq g \implies xf \leq xg$.

Allows reduction, syzygies, finiteness of Gröbner bases ...

Towards Gröbner bases in group rings

Group ring elements of $\mathbb{K}G$ are similar to polynomials.
Which properties are crucial for Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

- (P1) Divisibility of monomials. $\rightsquigarrow$ Well partial order $\preceq$ on group elements.
- (P2) Finite monomial set have a *unique* least common multiple $\rightsquigarrow$ finite subsets of G with a common upper bound have a unique least common upper bound
- (P3) A total order $\leq$ linearizaing $\preceq$ (necessarily a well-order).
- (P4) $g \preceq xg$ and $f \leq g \implies xf \leq xg$.

Allows reduction, syzygies, finiteness of Gröbner bases ...

Towards Gröbner bases in group rings

Group ring elements of $\mathbb{K}G$ are similar to polynomials.
Which properties are crucial for Gröbner bases in $\mathbb{K}[x_1, \dots, x_n]$?

(P1) Divisibility of monomials. $\rightsquigarrow$ Well partial order $\preceq$ on group elements.

(P2) Finite monomial set have a *unique* least common multiple $\rightsquigarrow$ finite subsets of G with a common upper bound have a unique least common upper bound

(P3) A total order $\leq$ linearizaing $\preceq$ (necessarily a well-order).

(P4) $g \preceq xg$ and $f \leq g \implies xf \leq xg$.

Allows reduction, syzygies, finiteness of Gröbner bases ...

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x f) \neq x \, \mathrm{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- Integer coefficients $\rightsquigarrow$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x f) \neq x \,\mathrm{lm}(f)$)! $\leadsto$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- Integer coefficients $\leadsto$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\operatorname{lm}(xf) \neq x \operatorname{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- Integer coefficients $\rightsquigarrow$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x f) \neq x\,\mathrm{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- Integer coefficients $\rightsquigarrow$ complicates things further. ☹

Overview

Two examples

$G := \langle a, b \mid a^4, (a^{-2}b)^2, (babab)^{-1}aba \rangle$
$H := \langle a, b \mid \emptyset \mid (a, b) \mapsto (b^2, a) \mid [a, b^{-1}ab] \rangle$ (Basilica group)

(LC) $\rightsquigarrow$ lower central series: abelian invariants of $\gamma_{(i)}/\gamma_{(i+1)}$

(D) $\rightsquigarrow$ derived serives: abelian invariants of $G^{(i)}/G^{(i+1)}$

	G		H	
Step	(LC)	(D)	(LC)	(D)
1	(2,4)	(2,4)	(0,0)	(0,0)
2	(2)	(0,0)	(0)	(0,0,0)
3	(2)	()	(4)	(2,2,0,0,0,0,0,0,0,0)
4	(2)	()	(4)	?
5	(2)	()	(4,4)	?

Two examples

G: An f.p. group; (LC): lower central series; (D): derived series.

Reaches the maximal solvable quotient of G after 3 steps along the derived series: it is polycyclic of Hirsch length 2. Along the lower central series, we will never reach the maximal solvable quotient, since all nilpotent quotients of G are finite.

	G		H	
Step	(LC)	(D)	(LC)	(D)
1	(2,4)	(2,4)	(0,0)	(0,0)
2	(2)	(0,0)	(0)	(0,0,0)
3	(2)	()	(4)	(2,2,0,0,0,0,0,0,0,0)
4	(2)	()	(4)	?
5	(2)	()	(4,4)	?

Two examples

H: Basilica group; (LC): lower central series; (D): derived series.

We see that $H/H^{(3)}$ is polycyclic of Hirsch length 13.
On the other hand, $H/\gamma_{48}(H)$ has been determined by Bartholdi-Eick-Hartung: this has only Hirsch length 3.

	G		H	
Step	(LC)	(D)	(LC)	(D)
1	(2,4)	(2,4)	(0,0)	(0,0)
2	(2)	(0,0)	(0)	(0,0,0)
3	(2)	()	(4)	(2,2,0,0,0,0,0,0,0,0)
4	(2)	()	(4)	?
5	(2)	()	(4,4)	?

Outlook

- Many improvements and optimizations planned, especially for Gröbner basis computations:
  - Adapting improvements from F_4 algorithm. (And F_5?)
  - Exploit ideas from algorithms for $\mathbb{Z}$-lattice computations, such as Hermite-Normal-form algorithms, LLL-algorithm.
  - Take advantage of parallelization.
- We will make our implementation available as a GAP share package in the future.

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x f) = x \,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\operatorname{lm}(x f) = x \operatorname{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Gröbner bases in polynomial rings

Which properties are crucial Gröbner bases in $\mathbb{K}[x_1, \ldots, x_n]$?

(P1) Divisibility of monomials $\rightsquigarrow$ a well partial order $\preceq$.

(P2) Any finite monomial set has a *unique* least common multiple wrt. this partial order.

(P3) A total order $\leq$ on the monomials which is a linearization of $\preceq$ $\rightsquigarrow$ necessarily is a well-order.

(P4) If f, g, x are monomials, then $f \leq g$ implies $xf \leq xg$.

- P4 $\rightsquigarrow$ if $\mathrm{lm}(x\,f) = x\,\mathrm{lm}(f)$
- P1+P4 $\rightsquigarrow$ reduction
- P1+P3 $\rightsquigarrow$ finiteness of Gröbner bases

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\mathrm{lm}(x\,g) = x\,\mathrm{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\mathrm{lm}(x\,g) = x\,\mathrm{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a *reduction group* if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\mathrm{lm}(x\,g) = x\,\mathrm{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\operatorname{lm}(x\,g) = x\operatorname{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\mathrm{lm}(x\,g) = x\,\mathrm{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\operatorname{lm}(x\,g) = x \operatorname{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\operatorname{lm}(x\,g) = x \operatorname{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\mathrm{lm}(x\,g) = x\,\mathrm{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Towards Gröbner bases in group rings

Definition (Lo; Madlener-Reinert (mid-90s))

A group G with a partial order $\preceq$ and a total order $\leq$ is a reduction group if

(R1) $\preceq$ is a well partial order,

(R2) finite subsets of G with a common upper bound have a unique least common upper bound,

(R3) $\leq$ extends $\preceq$ linearly, and

(R4) for all $x, f, g \in G$, if $g \preceq xg$ and $f \leq g$ then $xf \leq xg$.

- R4 $\rightsquigarrow$ if $g \preceq xg$ then $\operatorname{lm}(x\,g) = x\operatorname{lm}(g)$
- R1+R4 $\rightsquigarrow$ reduction
- R1+R3 $\rightsquigarrow$ finiteness of Gröbner bases

Polycyclic groups are reduction groups!

Gröbner bases in group rings

Definition

Let I be a left-ideal of a group ring. A Gröbner basis of I is a finite subset $B \subset I$ such that for any non-zero $f \in I$ there is $b \in B$ such that $\mathrm{lm}(b) \preceq \mathrm{lm}(f)$.

Theorem

Let B be a Gröbner basis of I. Then $f \in \mathbb{K}G$ is contained in I if and only if f reduces to zero modulo B.

Corollary

Let B be a Gröbner basis of I. Then I is generated by B.

Gröbner bases in group rings

Definition

Let I be a left-ideal of a group ring. A Gröbner basis of I is a finite subset $B \subset I$ such that for any non-zero $f \in I$ there is $b \in B$ such that $\operatorname{lm}(b) \preceq \operatorname{lm}(f)$.

Theorem

Let B be a Gröbner basis of I. Then $f \in \mathbb{K}G$ is contained in I if and only if f reduces to zero modulo B.

Corollary

Let B be a Gröbner basis of I. Then I is generated by B.

Gröbner bases in group rings

Definition

Let I be a left-ideal of a group ring. A Gröbner basis of I is a finite subset $B \subset I$ such that for any non-zero $f \in I$ there is $b \in B$ such that $\operatorname{lm}(b) \preceq \operatorname{lm}(f)$.

Theorem

Let B be a Gröbner basis of I. Then $f \in \mathbb{K}G$ is contained in I if and only if f reduces to zero modulo B.

Corollary

Let B be a Gröbner basis of I. Then I is generated by B.

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x f) \neq x \, \mathrm{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- So far, coefficients were from a field. But we need integer coefficients $\rightsquigarrow$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(xf) \neq x\,\mathrm{lm}(f)$)! $\leadsto$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- So far, coefficients were from a field. But we need integer coefficients $\leadsto$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x\,f) \neq x\,\mathrm{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- So far, coefficients were from a field. But we need integer coefficients $\rightsquigarrow$ complicates things further. ☹

Gröbner bases in group rings II

- How to compute a Gröbner basis? Adapt Buchberger's algorithm!
- But watch out: Lead monomials can change unexpectedly ($\mathrm{lm}(x f) \neq x \, \mathrm{lm}(f)$)! $\rightsquigarrow$ need to introduce additional "polynomials" during algorithm.
- One can adapt various improvements from the polynomial case, e.g. Gebauer-Möller criterion.
- So far, coefficients were from a field. But we need integer coefficients $\rightsquigarrow$ complicates things further. ☹