Membership problems in groups

Markus Lohrey

University of Siegen

June 18, 2026

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L (the set of all products $a_1 a_2 \cdots a_n$ with $a_i \in L$).

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L (the set of all products $a_1 a_2 \cdots a_n$ with $a_i \in L$).

The set $\mathrm{Rat}(M) \subseteq 2^M$ of all rational subsets of M is the smallest set such that:

- Every finite subset of M belongs to $\mathrm{Rat}(M)$.

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L
(the set of all products $a_1 a_2 \cdots a_n$ with $a_i \in L$).

The set $\mathrm{Rat}(M) \subseteq 2^M$ of all rational subsets of M is the smallest set such that:

- Every finite subset of M belongs to $\mathrm{Rat}(M)$.
- If $L_1, L_2 \in \mathrm{Rat}(M)$, then also $L_1 \cup L_2,\ L_1 L_2 \in \mathrm{Rat}(M)$.

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L (the set of all products $a_1 a_2 \cdots a_n$ with $a_i \in L$).

The set $\mathrm{Rat}(M) \subseteq 2^M$ of all rational subsets of M is the smallest set such that:

- Every finite subset of M belongs to $\mathrm{Rat}(M)$.
- If $L_1, L_2 \in \mathrm{Rat}(M)$, then also $L_1 \cup L_2,\ L_1 L_2 \in \mathrm{Rat}(M)$.
- If $L \in \mathrm{Rat}(M)$, then also $L^* \in \mathrm{Rat}(M)$.

Rational sets in arbitrary monoids: Definition 2

A finite automaton over M is a tuple $A = (Q, \delta, q_0, F)$ where

- Q is a finite set of states,
- $q_0 \in Q$, $F \subseteq Q$, and
- $\delta : Q \times M \times Q$ is finite.

Rational sets in arbitrary monoids: Definition 2

A finite automaton over M is a tuple $A = (Q, \delta, q_0, F)$ where

- Q is a finite set of states,
- $q_0 \in Q$, $F \subseteq Q$, and
- $\delta : Q \times M \times Q$ is finite.

The subset $L(A) \subseteq M$ is the set of all products $m_1 m_2 \cdots m_k$ such that there exist $q_1, \ldots, q_k \in Q$ with

$$(q_{i-1}, m_i, q_i) \in \delta \text{ for } 1 \leq i \leq k \text{ and } q_k \in F.$$

Rational sets in arbitrary monoids: Definition 2

A finite automaton over M is a tuple $A = (Q, \delta, q_0, F)$ where

- Q is a finite set of states,
- $q_0 \in Q$, $F \subseteq Q$, and
- $\delta : Q \times M \times Q$ is finite.

The subset $L(A) \subseteq M$ is the set of all products $m_1 m_2 \cdots m_k$ such that there exist $q_1, \ldots, q_k \in Q$ with

$$(q_{i-1}, m_i, q_i) \in \delta \text{ for } 1 \leq i \leq k \text{ and } q_k \in F.$$

Then: $L \in \mathrm{Rat}(M) \iff \exists$ finite automaton A over M : $L(A) = L$.

Rational sets in groups

In this talk: M will be always a finitely generated (f.g.) group G.

Rational sets in groups

In this talk: M will be always a finitely generated (f.g.) group G.

The group G is called finitely generated if there exists a finite subset $\Sigma \subseteq G$ such that $G = (\Sigma \cup \Sigma^{-1})^* =: \langle \Sigma \rangle$.

Rational sets in groups

In this talk: M will be always a finitely generated (f.g.) group G.

The group G is called finitely generated if there exists a finite subset $\Sigma \subseteq G$ such that $G = (\Sigma \cup \Sigma^{-1})^* =: \langle \Sigma \rangle$.

Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

Rational sets in groups

In this talk: M will be always a finitely generated (f.g.) group G.

The group G is called finitely generated if there exists a finite subset $\Sigma \subseteq G$ such that $G = (\Sigma \cup \Sigma^{-1})^* =: \langle \Sigma \rangle$.

Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

The rational subset membership problem for G (RatMP(G)) is the following computational problem:

INPUT: A finite automaton A over G and $g \in G$

QUESTION: $g \in L(A)$?

Rational sets in groups

In this talk: M will be always a finitely generated (f.g.) group G.

The group G is called finitely generated if there exists a finite subset $\Sigma \subseteq G$ such that $G = (\Sigma \cup \Sigma^{-1})^* =: \langle \Sigma \rangle$.

Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

The rational subset membership problem for G (RatMP(G)) is the following computational problem:

INPUT: A finite automaton A over G and $g \in G$

QUESTION: $g \in L(A)$?

Decidability/complexity does not depend on the chosen generating set.

Membership in submonoids/subgroups

The submonoid membership problem for G (SubmonoidMP(G)) is the following computational problem:

INPUT: A finite subset $A \subseteq G$ and $g \in G$

QUESTION: $g \in A^*$?

Membership in submonoids/subgroups

The submonoid membership problem for G (SubmonoidMP(G)) is the following computational problem:

INPUT: A finite subset $A \subseteq G$ and $g \in G$

QUESTION: $g \in A^*$?

The subgroup membership problem for G (SubgroupMP(G)) is the following computational problem:

INPUT: A finite subset $A \subseteq G$ and $g \in G$

QUESTION: $g \in \langle A \rangle$?

Membership in submonoids/subgroups

The submonoid membership problem for G (SubmonoidMP(G)) is the following computational problem:

INPUT: A finite subset $A \subseteq G$ and $g \in G$

QUESTION: $g \in A^*$?

The subgroup membership problem for G (SubgroupMP(G)) is the following computational problem:

INPUT: A finite subset $A \subseteq G$ and $g \in G$

QUESTION: $g \in \langle A \rangle$?

The subgroup membership problem is a widely studied problem in combinatorial group theory.

Simple implications

Clearly, for a f.g. group G we have:

$$\begin{aligned} & \text{RatMP}(G) \text{ decidable} \\ \Rightarrow\quad & \text{SubmonoidMP}(G) \text{ decidable} \\ \Rightarrow\quad & \text{SubgroupMP}(G) \text{ decidable} \end{aligned}$$

Simple implications

Clearly, for a f.g. group G we have:

$$\begin{aligned} & \text{RatMP}(G) \text{ decidable} \\ \Rightarrow\ & \text{SubmonoidMP}(G) \text{ decidable} \\ \Rightarrow\ & \text{SubgroupMP}(G) \text{ decidable} \end{aligned}$$

What about the reverse implications?

Simple implications

Clearly, for a f.g. group G we have:

$$\begin{array}{ll} & \mathsf{RatMP}(G) \text{ decidable} \\ \Rightarrow & \mathsf{SubmonoidMP}(G) \text{ decidable} \\ \Rightarrow & \mathsf{SubgroupMP}(G) \text{ decidable} \end{array}$$

What about the reverse implications?

We will come back to this latter.

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \ldots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \ldots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \dots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \dots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

This is the membership problem for products of cyclic subgroups.

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \ldots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \ldots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

This is the membership problem for products of cyclic subgroups.

Alternative: restrict the x_i to $\mathbb{N}$ (membership in cyclic submonoids).

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \ldots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \ldots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

This is the membership problem for products of cyclic subgroups.

Alternative: restrict the x_i to $\mathbb{N}$ (membership in cyclic submonoids).

$\mathbb{Z}$-knapsack reduces to $\mathbb{N}$-knapsack:

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \ldots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \ldots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

This is the membership problem for products of cyclic subgroups.

Alternative: restrict the x_i to $\mathbb{N}$ (membership in cyclic submonoids).

$\mathbb{Z}$-knapsack reduces to $\mathbb{N}$-knapsack: replace $g_i^{x_i}$ to $g_i^{y_i}(g_i^{-1})^{z_i}$ $(y_i, z_i \in \mathbb{N})$.

Knapsack problem (Myasnikov, Nikolaev, Ushakov 2015)

The knapsack problem for G is the following computational problem:

INPUT: A finite list $g_1, \ldots, g_n, g$ of elements from G.

QUESTION: Are there integers $x_1, \ldots, x_n \in \mathbb{Z}$ with $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$?

This is the membership problem for products of cyclic subgroups.

Alternative: restrict the x_i to $\mathbb{N}$ (membership in cyclic submonoids).

$\mathbb{Z}$-knapsack reduces to $\mathbb{N}$-knapsack: replace $g_i^{x_i}$ to $g_i^{y_i} (g_i^{-1})^{z_i}$ $(y_i, z_i \in \mathbb{N})$.

Open problem: Is there a group, for which $\mathbb{N}$-knapsack is undecidable and $\mathbb{Z}$-knapsack is decidable?

Uniform versus non-uniform membership problems

Theorem (Bodart 2025)

There is a finitely generated group G with the following properties:

- SubgroupMP(G) is undecidable.
- For every fixed finitely generated subgroup $H \leq G$, it is decidable whether a given element of G belongs to H.
- For every fixed finitely generated submonoid $M \subseteq G$, it is decidable whether a given element of G belongs to M.

Bodart's group G is a central extension of the lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}$ by $\mathbb{Z}_2$: $G/\mathbb{Z}_2 \cong \mathbb{Z}_2 \wr \mathbb{Z}$ with $\mathbb{Z}_2$ central in G.

Open problem: Is there a group G with RatMP(G) undecidable but membership in every fixed rational subset of G is decidable?

Extreme cases: abelian groups

Theorem

If G is a f.g. abelian group then $\mathrm{RatMP}(G)$ can be decided in polynomial time.

Extreme cases: abelian groups

Theorem

If G is a f.g. abelian group then $\mathrm{RatMP}(G)$ can be decided in polynomial time.

- Decidability (in **NP**) follows by a reduction to integer linear programming (Grunschlag 1999).

Extreme cases: abelian groups

Theorem

If G is a f.g. abelian group then RatMP(G) can be decided in polynomial time.

- Decidability (in **NP**) follows by a reduction to integer linear programming (Grunschlag 1999).
- For a fixed f.g. abelian group G, membership in **P** follows from the fact that integer programming in a fixed dimension is in **P** (Lenstra 1983).

Extreme cases: free groups

Let Σ be a finite alphabet and let $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ be a set of formal inverses.

Extreme cases: free groups

Let Σ be a finite alphabet and let $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ be a set of formal inverses.

The free group $F(\Sigma)$ consists of all words over the alphabet $\Sigma \cup \Sigma^{-1}$, where a and a^{-1} cancel for all $a \in \Sigma$.

Extreme cases: free groups

Let Σ be a finite alphabet and let $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ be a set of formal inverses.

The free group $F(\Sigma)$ consists of all words over the alphabet $\Sigma \cup \Sigma^{-1}$, where a and a^{-1} cancel for all $a \in \Sigma$.

Example: $ab^{-1}aa^{-1}ba = aa$

Extreme cases: free groups

Let Σ be a finite alphabet and let $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ be a set of formal inverses.

The free group $F(\Sigma)$ consists of all words over the alphabet $\Sigma \cup \Sigma^{-1}$, where a and a^{-1} cancel for all $a \in \Sigma$.

Example: $ab^{-1}aa^{-1}ba = aa$

Every word $w \in (\Sigma \cup \Sigma^{-1})^*$ has a unique normal form obtained by applying the reduction rules $aa^{-1} \to \varepsilon$, $a^{-1}a \to \varepsilon$ $(a \in \Sigma)$ as long as possible.

Extreme cases: free groups

Let Σ be a finite alphabet and let $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ be a set of formal inverses.

The free group $F(\Sigma)$ consists of all words over the alphabet $\Sigma \cup \Sigma^{-1}$, where a and a^{-1} cancel for all $a \in \Sigma$.

Example: $ab^{-1}aa^{-1}ba = aa$

Every word $w \in (\Sigma \cup \Sigma^{-1})^*$ has a unique normal form obtained by applying the reduction rules $aa^{-1} \to \varepsilon$, $a^{-1}a \to \varepsilon$ $(a \in \Sigma)$ as long as possible.

Nielsen 1921, Stallings 1983, Avenhaus and Madlener 1984

SubgroupMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

Stallings' folding

is a simple algorithm for SubgroupMP(F).

Stallings' folding

is a simple algorithm for SubgroupMP(F).

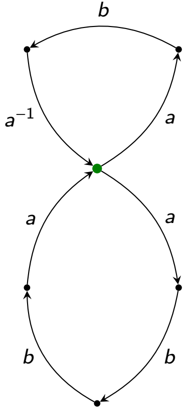
Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Start with a dual bouquet graph.

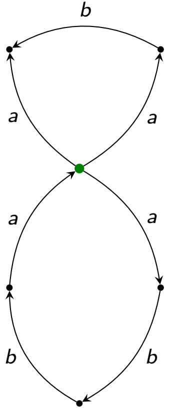


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a, b)$.

Start with a dual bouquet graph.

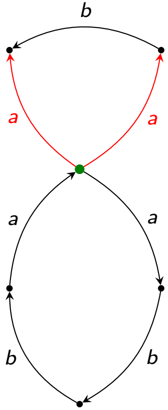


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a, b)$.

Fold edges with the same source (or target) node and the same label.

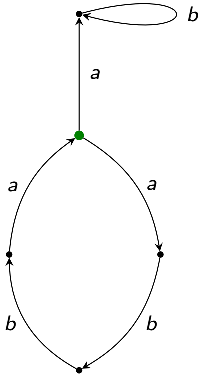


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Fold edges with the same source (or target) node and the same label.

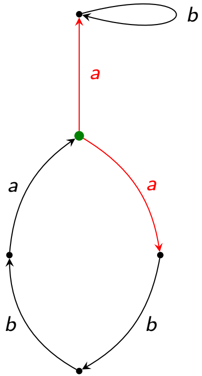


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a, b)$.

Fold edges with the same source (or target) node and the same label.

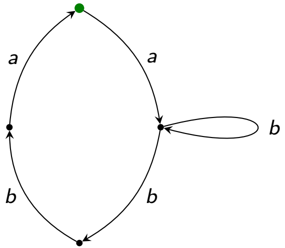


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Fold edges with the same source (or target) node and the same label.

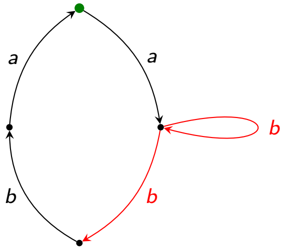


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Fold edges with the same source (or target) node and the same label.

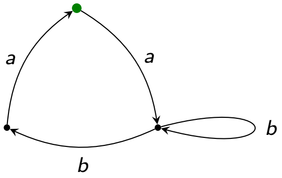


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Fold edges with the same source (or target) node and the same label.

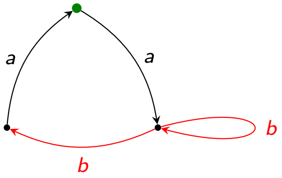


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

Fold edges with the same source (or target) node and the same label.

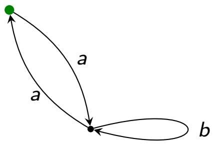


Stallings' folding

is a simple algorithm for SubgroupMP(F).

Example: check $abaaa \in \langle aba^{-1}, ab^2a \rangle \leq F(a,b)$.

When the graph is completely folded, test membership of $abaaa$.



Compressed Stallings' folding

A power word over Σ is an expression $w = u_1^{n_1} u_2^{n_2} \cdots u_k^{n_k}$, where

- $u_1, u_2, \ldots, u_k \in \Sigma^*$ are explicitly given words, and
- $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are binary encoded numbers.

Compressed Stallings' folding

A power word over Σ is an expression $w = u_1^{n_1} u_2^{n_2} \cdots u_k^{n_k}$, where

- $u_1, u_2, \ldots, u_k \in \Sigma^*$ are explicitly given words, and
- $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are binary encoded numbers.

Lohrey 21

SubgroupMP$(F(\Sigma))$ can be decided in polynomial time if all input words are given as power words.

Compressed Stallings' folding

A power word over Σ is an expression $w = u_1^{n_1} u_2^{n_2} \cdots u_k^{n_k}$, where

- $u_1, u_2, \ldots, u_k \in \Sigma^*$ are explicitly given words, and
- $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are binary encoded numbers.

Lohrey 21

SubgroupMP$(F(\Sigma))$ can be decided in polynomial time if all input words are given as power words.

$\mathrm{GL}_2(\mathbb{Z})$ is virtually free, i.e., has a free subgroup of finite index.

Compressed Stallings' folding

A power word over Σ is an expression $w = u_1^{n_1} u_2^{n_2} \cdots u_k^{n_k}$, where

- $u_1, u_2, \ldots, u_k \in \Sigma^*$ are explicitly given words, and
- $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are binary encoded numbers.

Lohrey 21

SubgroupMP($F(\Sigma)$) can be decided in polynomial time if all input words are given as power words.

$\mathrm{GL}_2(\mathbb{Z})$ is virtually free, i.e., has a free subgroup of finite index.

Corollary (Lohrey 21)

SubgroupMP($\mathrm{GL}_2(\mathbb{Z})$) can be decided in polynomial time if all input matrices are given in binary notation.

Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

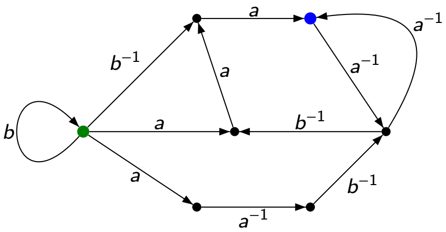
It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

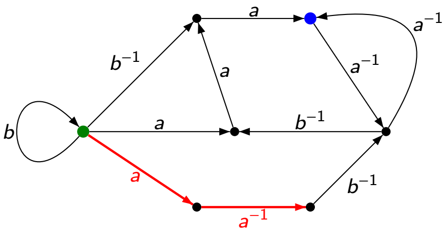


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

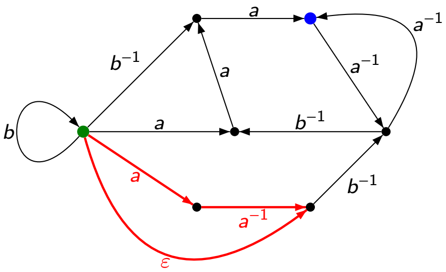


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

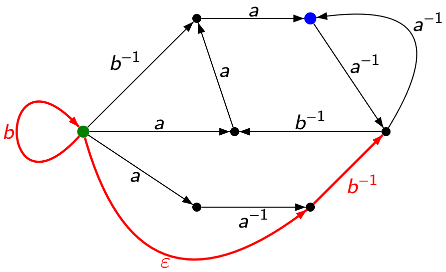


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

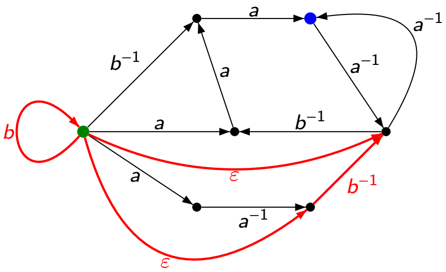


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

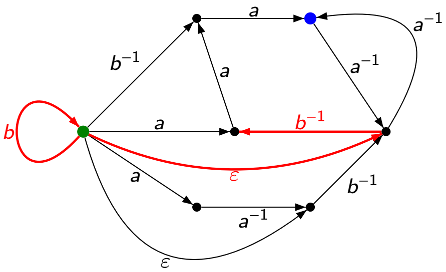


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

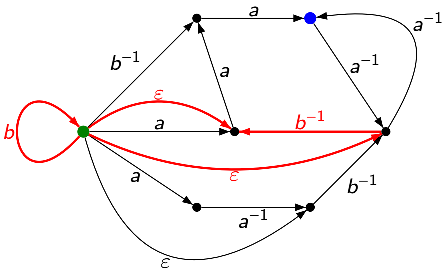


Benois' algorithm

Benois 1969

$\mathrm{RatMP}(F(\Sigma))$ can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

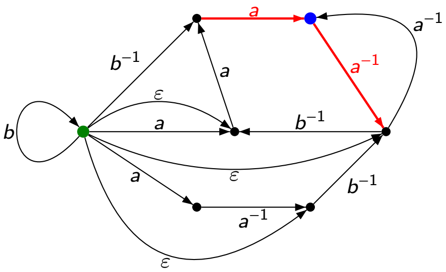


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

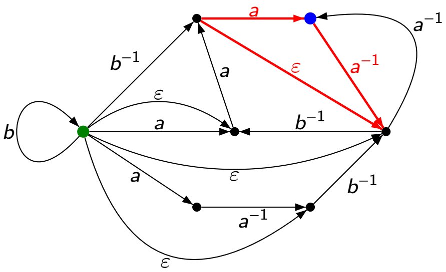


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

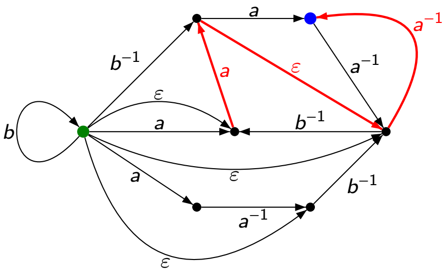


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

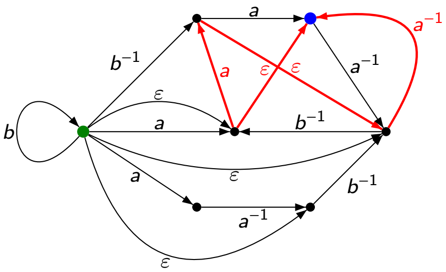


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.

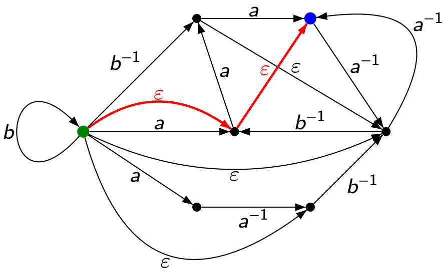


Benois' algorithm

Benois 1969

RatMP($F(\Sigma)$) can be decided in polynomial time for every finite Σ.

It suffices to check whether a finite automaton A over the alphabet $\Sigma \cup \Sigma^{-1}$ accepts a word w whose normal form is the empty word ε.



Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

In other words: take the free group $F(A)$ but allow the commutations $ab = ba$ whenever $(a, b) \in E$.

Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

In other words: take the free group $F(A)$ but allow the commutations $ab = ba$ whenever $(a, b) \in E$.

Extreme case:

Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

In other words: take the free group $F(A)$ but allow the commutations $ab = ba$ whenever $(a, b) \in E$.

Extreme case:

- $G(A, \emptyset) = F(A)$

Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

In other words: take the free group $F(A)$ but allow the commutations $ab = ba$ whenever $(a, b) \in E$.

Extreme case:

- $G(A, \emptyset) = F(A)$
- $G\big(A, \binom{A}{2}\big) = \mathbb{Z}^{|A|}$

Interpolating between free and abelian: graph groups

With a finite undirected graph (A, E) we associate the graph group

$$G(A, E) = \langle A \mid ab = ba \text{ for all } (a, b) \in E \rangle.$$

In other words: take the free group $F(A)$ but allow the commutations $ab = ba$ whenever $(a, b) \in E$.

Extreme case:

- $G(A, \emptyset) = F(A)$
- $G\big(A, \binom{A}{2}\big) = \mathbb{Z}^{|A|}$

Every graph group is linear (a subgroup of $\mathrm{GL}_d(\mathbb{F})$ for a field $\mathbb{F}$).

Graph groups: SubgroupMP

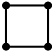
Kapovich, Myasnikov, Weidmann 2005:

SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Graph groups: SubgroupMP

Kapovich, Myasnikov, Weidmann 2005:

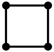
SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Two important graphs: P4:  C4: 

Graph groups: SubgroupMP

Kapovich, Myasnikov, Weidmann 2005:

SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Two important graphs: P4:  C4: 

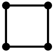
Mikhailova 1966

SubgroupMP($G(\text{C4})$) is undecidable.

Graph groups: SubgroupMP

Kapovich, Myasnikov, Weidmann 2005:

SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Two important graphs: P4:  C4: 

Mikhailova 1966

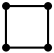
SubgroupMP(G(C4)) is undecidable.

Note: $G(\text{C4}) = F(\{a, b\}) \times F(\{c, d\}) \leq \text{SL}_4(\mathbb{Z})$

Graph groups: SubgroupMP

Kapovich, Myasnikov, Weidmann 2005:

SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Two important graphs: P4:  C4: 

Mikhailova 1966

SubgroupMP($G(\mathrm{C4})$) is undecidable.

Note: $G(\mathrm{C4}) = F(\{a, b\}) \times F(\{c, d\}) \leq \mathrm{SL}_4(\mathbb{Z})$

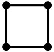
Big open problems:

- For which graph groups is the subgroup membership problem decidable? In particular, what about a cycle of length 5?

Graph groups: SubgroupMP

Kapovich, Myasnikov, Weidmann 2005:

SubgroupMP($G(A, E)$) is decidable if (A, E) is a chordal graph (does not contain an induced cycle of length ≥ 4).

Two important graphs: P4:  C4: 

Mikhailova 1966

SubgroupMP(G(C4)) is undecidable.

Note: $G(\text{C4}) = F(\{a, b\}) \times F(\{c, d\}) \leq \text{SL}_4(\mathbb{Z})$

Big open problems:

- For which graph groups is the subgroup membership problem decidable? In particular, what about a cycle of length 5?
- Is SubgroupMP($\text{SL}_3(\mathbb{Z})$) decidable?

Graph groups: SubmonoidMP and RatMP

L, Steinberg 2006

The following are equivalent for every finite undirected graph (A, E):

- RatMP$(G(A, E))$ is decidable.
- SubmonoidMP$(G(A, E))$ is decidable.
- The graph (A, E) neither contains P4 nor C4 as an induced subgraph.

Graph groups: SubmonoidMP and RatMP

L, Steinberg 2006

The following are equivalent for every finite undirected graph (A, E):

- RatMP$(G(A, E))$ is decidable.
- SubmonoidMP$(G(A, E))$ is decidable.
- The graph (A, E) neither contains P4 nor C4 as an induced subgraph.

The graphs that neither contain an induced P4 or C4 are exactly the graphs that can be constructed from the single-node graphs • using

- disjoint union and
- adding a new vertex • and connecting it to all other vertices.

Graph groups: SubmonoidMP and RatMP

Consequence: The graph groups $G(A, E)$, where (A, E) neither contains an induced P4 nor an induced C4, form the smallest class C of groups with:

- $\mathbb{Z} \in \mathsf{C}$,
- if $G, H \in \mathsf{C}$ then $G * H \in \mathsf{C}$ ($G * H$ is the free product)
- if $G \in \mathsf{C}$ then $G \times \mathbb{Z} \in \mathsf{C}$

Graph groups: SubmonoidMP and RatMP

Consequence: The graph groups $G(A, E)$, where (A, E) neither contains an induced P4 nor an induced C4, form the smallest class C of groups with:

- $\mathbb{Z} \in \mathsf{C}$,
- if $G, H \in \mathsf{C}$ then $G * H \in \mathsf{C}$ ($G * H$ is the free product)
- if $G \in \mathsf{C}$ then $G \times \mathbb{Z} \in \mathsf{C}$

Haase, Zetzsche 2019

Let (A, E) be a finite graph that neither contains an induced P4 nor an induced C4.

- RatMP($G(A, E)$) is **NP**-complete if (A, E) contains an induced P3.
- RatMP($G(A, E)$) is in **P** if (A, E) contains no induced P3.

Submonoids versus subgroups

Note: The graph group $G(\mathsf{P4})$ has the following properties:

- SubgroupMP(G(P4)) is decidable (P4 is chordal).
- SubmonoidMP(G(P4)) is undecidable.

Submonoids versus subgroups

Note: The graph group $G(\text{P4})$ has the following properties:

- SubgroupMP($G(\text{P4})$) is decidable (P4 is chordal).
- SubmonoidMP($G(\text{P4})$) is undecidable.

Another example can be found in the class of metabelian groups.

Submonoids versus subgroups

Note: The graph group $G(\text{P4})$ has the following properties:

- SubgroupMP($G(\text{P4})$) is decidable (P4 is chordal).
- SubmonoidMP($G(\text{P4})$) is undecidable.

Another example can be found in the class of metabelian groups.

G is metabelian if it has normal subgroup H such that H and G/H are abelian.

Submonoids versus subgroups

Note: The graph group $G(\text{P4})$ has the following properties:

- SubgroupMP(G(P4)) is decidable (P4 is chordal).
- SubmonoidMP(G(P4)) is undecidable.

Another example can be found in the class of metabelian groups.

G is metabelian if it has normal subgroup H such that H and G/H are abelian.

- SubgroupMP(G) is decidable for every metabelian group G (Romanovskii 1980).

Submonoids versus subgroups

Note: The graph group $G(\mathrm{P4})$ has the following properties:

- SubgroupMP($G(\mathrm{P4})$) is decidable (P4 is chordal).
- SubmonoidMP($G(\mathrm{P4})$) is undecidable.

Another example can be found in the class of metabelian groups.

G is metabelian if it has normal subgroup H such that H and G/H are abelian.

- SubgroupMP(G) is decidable for every metabelian group G (Romanovskii 1980).
- SubmonoidMP($\mathbb{Z} \wr \mathbb{Z}$) is undecidable (L, Steinberg, Zetzsche 2013). ($\mathbb{Z} \wr \mathbb{Z}$ is metabelian).

Submonoids versus subgroups

Note: The graph group $G(\mathrm{P4})$ has the following properties:

- SubgroupMP($G(\mathrm{P4})$) is decidable (P4 is chordal).
- SubmonoidMP($G(\mathrm{P4})$) is undecidable.

Another example can be found in the class of metabelian groups.

G is metabelian if it has normal subgroup H such that H and G/H are abelian.

- SubgroupMP(G) is decidable for every metabelian group G (Romanovskii 1980).
- SubmonoidMP($\mathbb{Z} \wr \mathbb{Z}$) is undecidable (L, Steinberg, Zetzsche 2013). ($\mathbb{Z} \wr \mathbb{Z}$ is metabelian).

What about submonoids versus rational subsets?

Slightly non-abelian: nilpotent groups

A group G is nilpotent if the lower central series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ with $G_{i+1} = [G_i, G]$ finally reaches the trivial group 1.

Slightly non-abelian: nilpotent groups

A group G is nilpotent if the lower central series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ with $G_{i+1} = [G_i, G]$ finally reaches the trivial group 1.

G is nilpotent of class k if k is the smallest number with $G_k = 1$.

Slightly non-abelian: nilpotent groups

A group G is nilpotent if the lower central series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ with $G_{i+1} = [G_i, G]$ finally reaches the trivial group 1.

G is nilpotent of class k if k is the smallest number with $G_k = 1$.

In particular: G is nilpotent of class 2 if every commutator $aba^{-1}b^{-1}$ commutes with every $c \in G$:

$$\forall a, b, c \in G : aba^{-1}b^{-1}c = caba^{-1}b^{-1}$$

Slightly non-abelian: nilpotent groups

A group G is nilpotent if the lower central series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ with $G_{i+1} = [G_i, G]$ finally reaches the trivial group 1.

G is nilpotent of class k if k is the smallest number with $G_k = 1$.

In particular: G is nilpotent of class 2 if every commutator $aba^{-1}b^{-1}$ commutes with every $c \in G$:

$$\forall a, b, c \in G : aba^{-1}b^{-1}c = caba^{-1}b^{-1}$$

Malcev 1958

SubgroupMP(G) is decidable for every f.g. nilpotent group.

Slightly non-abelian: nilpotent groups

A group G is nilpotent if the lower central series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ with $G_{i+1} = [G_i, G]$ finally reaches the trivial group 1.

G is nilpotent of class k if k is the smallest number with $G_k = 1$.

In particular: G is nilpotent of class 2 if every commutator $aba^{-1}b^{-1}$ commutes with every $c \in G$:

$$\forall a, b, c \in G : aba^{-1}b^{-1}c = caba^{-1}b^{-1}$$

Malcev 1958

SubgroupMP(G) is decidable for every f.g. nilpotent group.

The problem is actually in $\mathbf{TC}^0$ (Myasnikov and Weiß 2022).

Heisenberg groups: decidability

The discrete n-dimensional Heisenberg group ($n \geq 3$) is

$$\mathsf{H}_n(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a^\top & c \\ 0 & I_{n-2} & b \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}^{n-2},\ c \in \mathbb{Z} \right\}.$$

Heisenberg groups: decidability

The discrete n-dimensional Heisenberg group $(n \geq 3)$ is

$$\mathrm{H}_n(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a^\top & c \\ 0 & I_{n-2} & b \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}^{n-2},\ c \in \mathbb{Z} \right\}.$$

All $\mathrm{H}_n(\mathbb{Z})$ $(n \geq 3)$ are nilpotent of class two.

Heisenberg groups: decidability

The discrete n-dimensional Heisenberg group $(n \geq 3)$ is

$$\mathsf{H}_n(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a^\top & c \\ 0 & I_{n-2} & b \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}^{n-2},\ c \in \mathbb{Z} \right\}.$$

All $\mathsf{H}_n(\mathbb{Z})$ $(n \geq 3)$ are nilpotent of class two.

Remark: The group $\mathsf{UT}_n(\mathbb{Z})$ groups of all upper unitriangular n-dimensional integer matrices is nilpotent of class $n-1$.

Heisenberg groups: decidability

The discrete n-dimensional Heisenberg group $(n \geq 3)$ is

$$\mathsf{H}_n(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a^\top & c \\ 0 & I_{n-2} & b \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}^{n-2},\ c \in \mathbb{Z} \right\}.$$

All $\mathsf{H}_n(\mathbb{Z})$ $(n \geq 3)$ are nilpotent of class two.

Remark: The group $\mathsf{UT}_n(\mathbb{Z})$ groups of all upper unitriangular n-dimensional integer matrices is nilpotent of class $n-1$.

Colcombet, Ouaknine, Semukhin, Worrell 2019

SubmonoidMP($\mathsf{H}_n(\mathbb{Z})$) is decidable for every $n \geq 3$.

Heisenberg groups: decidability

König, L, Zetzsche 2014

Knapsack is decidable for every Heisenberg group $\mathsf{H}_n(\mathbb{Z})$ ($n \geq 3$).

Heisenberg groups: decidability

König, L, Zetzsche 2014

Knapsack is decidable for every Heisenberg group $\mathsf{H}_n(\mathbb{Z})$ ($n \geq 3$).

Proof (for $n = 3$): Take matrixes $A, A_1, \ldots, A_k \in \mathsf{H}_3(\mathbb{Z})$ and let

$$A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_i = \begin{pmatrix} 1 & a_i & c_i \\ 0 & 1 & b_i \\ 0 & 0 & 1 \end{pmatrix}$$

Heisenberg groups: decidability

König, L, Zetzsche 2014

Knapsack is decidable for every Heisenberg group $\mathsf{H}_n(\mathbb{Z})$ ($n \geq 3$).

Proof (for $n = 3$): Take matrixes $A, A_1, \ldots, A_k \in \mathsf{H}_3(\mathbb{Z})$ and let

$$A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_i = \begin{pmatrix} 1 & a_i & c_i \\ 0 & 1 & b_i \\ 0 & 0 & 1 \end{pmatrix}$$

We get:

$$A_i^n = \begin{pmatrix} 1 & a_i \cdot n & c_i \cdot n + a_i b_i \frac{(n-1)n}{2} \\ 0 & 1 & b_i \cdot n \\ 0 & 0 & 1 \end{pmatrix}$$

Heisenberg groups

There is a solution $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ of $A = A_1^{x_1} \cdots A_k^{x_k}$ iff the following system of three Diophantine equations has a solution over $\mathbb{Z}$:

$$a = \sum_{i=1}^{k} a_i \cdot x_i$$

$$b = \sum_{i=1}^{k} b_i \cdot x_i$$

$$c = \sum_{i=1}^{k} c_i \cdot x_i + \sum_{i=1}^{k} a_i b_i \frac{(x_i - 1)x_i}{2} + \sum_{1 \le i < j \le k} a_i b_j x_i x_j$$

This is a Diophantine system with a single quadratic equation and two linear equations.

Decidability follows by results from Duchin, Liang, and Shapiro 2015 (based on Grunewald and Segal 2004). □

Heisenberg groups: decidability

Bodart 2024

$\mathsf{RatMP}(\mathsf{H}_3(\mathbb{Z}))$ is decidable.

Heisenberg groups: decidability

Bodart 2024

$\mathsf{RatMP}(\mathsf{H}_3(\mathbb{Z}))$ is decidable.

Bodart reduces the $\mathsf{RatMP}(\mathsf{H}_3(\mathbb{Z}))$ to the knapsack problem for $\mathsf{H}_3(\mathbb{Z})$:

Heisenberg groups: decidability

Bodart 2024

$\mathrm{RatMP}(\mathrm{H}_3(\mathbb{Z}))$ is decidable.

Bodart reduces the $\mathrm{RatMP}(\mathrm{H}_3(\mathbb{Z}))$ to the knapsack problem for $\mathrm{H}_3(\mathbb{Z})$:

- Every rational subset of $\mathrm{H}_3(\mathbb{Z})$ is effectively the image of a bounded regular language L.

Heisenberg groups: decidability

Bodart 2024

$\mathrm{RatMP}(\mathrm{H}_3(\mathbb{Z}))$ is decidable.

Bodart reduces the $\mathrm{RatMP}(\mathrm{H}_3(\mathbb{Z}))$ to the knapsack problem for $\mathrm{H}_3(\mathbb{Z})$:

- Every rational subset of $\mathrm{H}_3(\mathbb{Z})$ is effectively the image of a bounded regular language L.

  $L \subseteq \Sigma^*$ is bounded iff $L \subseteq w_1^* w_2^* \cdots w_k^*$ for $w_1, \ldots, w_k \in \Sigma^*$.

Heisenberg groups: decidability

Bodart 2024

RatMP($H_3(\mathbb{Z})$) is decidable.

Bodart reduces the RatMP($H_3(\mathbb{Z})$) to the knapsack problem for $H_3(\mathbb{Z})$:

- Every rational subset of $H_3(\mathbb{Z})$ is effectively the image of a bounded regular language L.

  $L \subseteq \Sigma^*$ is bounded iff $L \subseteq w_1^* w_2^* \cdots w_k^*$ for $w_1, \dots, w_k \in \Sigma^*$.

- A regular language is bounded iff it is a finite union of languages $v_0 w_1^* v_1 w_2^* \cdots v_{k-1} w_k^* v_k$.

Heisenberg groups: decidability

Bodart 2024

RatMP($H_3(\mathbb{Z})$) is decidable.

Bodart reduces the RatMP($H_3(\mathbb{Z})$) to the knapsack problem for $H_3(\mathbb{Z})$:

- Every rational subset of $H_3(\mathbb{Z})$ is effectively the image of a bounded regular language L.

  $L \subseteq \Sigma^*$ is bounded iff $L \subseteq w_1^* w_2^* \cdots w_k^*$ for $w_1, \dots, w_k \in \Sigma^*$.

- A regular language is bounded iff it is a finite union of languages $v_0 w_1^* v_1 w_2^* \cdots v_{k-1} w_k^* v_k$.
- One directly obtains a finite number of knapsack equations.

Heisenberg groups: decidability

Bodart 2024

RatMP($H_3(\mathbb{Z})$) is decidable.

Bodart reduces the RatMP($H_3(\mathbb{Z})$) to the knapsack problem for $H_3(\mathbb{Z})$:

- Every rational subset of $H_3(\mathbb{Z})$ is effectively the image of a bounded regular language L.

  $L \subseteq \Sigma^*$ is bounded iff $L \subseteq w_1^* w_2^* \cdots w_k^*$ for $w_1, \dots, w_k \in \Sigma^*$.

- A regular language is bounded iff it is a finite union of languages $v_0 w_1^* v_1 w_2^* \cdots v_{k-1} w_k^* v_k$.

- One directly obtains a finite number of knapsack equations.

Open problem: Does this generalize to every $H_n(\mathbb{Z})$ for $n \geq 3$?

Nilpotent groups: undecidability

König, L, Zetzsche 2014

There exist nilpotent groups of class 2 with undecidable knapsack problem.

Nilpotent groups: undecidability

König, L, Zetzsche 2014

There exist nilpotent groups of class 2 with undecidable knapsack problem.

Proof: Reduction from Hilbert's 10th problem.

Nilpotent groups: undecidability

König, L, Zetzsche 2014

There exist nilpotent groups of class 2 with undecidable knapsack problem.

Proof: Reduction from Hilbert's 10th problem.

There is a fixed polynomial $P(X_1, \ldots, X_k) \in \mathbb{Z}[X_1, \ldots, X_k]$ such that the following problem is undecidable:

- INPUT: $a \in \mathbb{N}$.
- QUESTION: $\exists (x_1, \ldots, x_k) \in \mathbb{Z}^k : P(x_1, \ldots, x_k) = a$?

Nilpotent groups: undecidability

König, L, Zetzsche 2014

There exist nilpotent groups of class 2 with undecidable knapsack problem.

Proof: Reduction from Hilbert's 10th problem.

There is a fixed polynomial $P(X_1, \dots, X_k) \in \mathbb{Z}[X_1, \dots, X_k]$ such that the following problem is undecidable:

- INPUT: $a \in \mathbb{N}$.
- QUESTION: $\exists (x_1, \dots, x_k) \in \mathbb{Z}^k : P(x_1, \dots, x_k) = a$?

Write $P(X_1, \dots, X_k) = a$ as a system $\mathcal{S}$ of equations of the form

$$X \cdot Y = Z, \ X + Y = Z, \ X = c \ (c \in \mathbb{Z})$$

with a distinguished equation $X_0 = a$.

Nilpotent groups: undecidability

Toy example: $\mathcal{S} = \{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$

Nilpotent groups: undecidability

Toy example: $\mathcal{S} = \{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$

Work in the direct product $\mathsf{H}_3(\mathbb{Z})^3$ ($3 =$ number of equations).

Nilpotent groups: undecidability

Toy example: $\mathcal{S} = \{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$

Work in the direct product $\mathsf{H}_3(\mathbb{Z})^3$ ($3 =$ number of equations).

For $A \in \mathsf{H}_3(\mathbb{Z})$ let $A_1 = (A, \mathsf{Id}, \mathsf{Id})$, $A_2 = (\mathsf{Id}, A, \mathsf{Id})$, $A_3 = (\mathsf{Id}, \mathsf{Id}, A)$.

Nilpotent groups: undecidability

The solutions of $\{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$ are the solutions of

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1^a =$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1^{X_0} \cdot$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}_2^X \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2^Y \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}_2^X \cdot \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2^Y \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2^{X_0} \cdot$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3^X \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3^Z \cdot \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3^Y$$

Nilpotent groups: undecidability

The solutions of $\{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$ are the solutions of

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 =$$

$$\begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 \cdot$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & X \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & Y & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -X \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & -Y & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot$$

$$\begin{pmatrix} 1 & 0 & X \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3 \cdot \begin{pmatrix} 1 & 0 & Z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3 \cdot \begin{pmatrix} 1 & 0 & -Y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3$$

Nilpotent groups: undecidability

The solutions of $\{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$ are the solutions of

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 =$$

$$\begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 \cdot$$

$$\begin{pmatrix} 1 & Y & 0 \\ 0 & 1 & X \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & -Y & 0 \\ 0 & 1 & -X \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot$$

$$\begin{pmatrix} 1 & 0 & X + Z - Z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3$$

Nilpotent groups: undecidability

The solutions of $\{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$ are the solutions of

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 =$$

$$\begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 \cdot$$

$$\begin{pmatrix} 1 & 0 & -XY \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot \begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot$$

$$\begin{pmatrix} 1 & 0 & X + Z - Y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3$$

Nilpotent groups: undecidability

The solutions of $\{X_0 = a,\ X_0 = X \cdot Y,\ Y = X + Z\}$ are the solutions of

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 =$$

$$\begin{pmatrix} 1 & 0 & X_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_1 \cdot$$

$$\begin{pmatrix} 1 & 0 & X_0 - XY \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_2 \cdot$$

$$\begin{pmatrix} 1 & 0 & X + Z - Y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_3$$

Nilpotent groups: undecidability

How to achieve synchronization?

Nilpotent groups: undecidability

How to achieve synchronization?

Example: Consider an equation

$$g = a^Y b^Z c^Y d^Z$$

with $g, a, b, c, d \in G$ (any group).

Nilpotent groups: undecidability

How to achieve synchronization?

Example: Consider an equation

$$g = a^Y b^Z c^Y d^Z$$

with $g, a, b, c, d \in G$ (any group).

It has a solution (with $Y, Z \in \mathbb{Z}$ if and only if the following equation (over the group $G \times \mathbb{Z}^4$) has a solution:

$$\begin{aligned}&(g,0,0,0,0) = \\ &\quad (\mathbf{1},1,0,1,0)^Y (\mathbf{1},0,1,0,1)^Z \\ &\quad (a,-1,0,0,0)^U (b,0,-1,0,0)^V (c,0,0,-1,0)^W (d,0,0,0,-1)^X\end{aligned}$$

Nilpotent groups: undecidability

How to achieve synchronization?

Example: Consider an equation

$$g = a^Y b^Z c^Y d^Z$$

with $g, a, b, c, d \in G$ (any group).

It has a solution (with $Y, Z \in \mathbb{Z}$ if and only if the following equation (over the group $G \times \mathbb{Z}^4$) has a solution:

$$\begin{aligned}&(g, 0, 0, 0, 0) = \\ &\quad (\mathbf{1}, 1, 0, 1, 0)^Y (\mathbf{1}, 0, 1, 0, 1)^Z \\ &\quad (a, -1, 0, 0, 0)^U (b, 0, -1, 0, 0)^V (c, 0, 0, -1, 0)^W (d, 0, 0, 0, -1)^X\end{aligned}$$

In our example: Work in $\mathsf{H}_3(\mathbb{Z})^3 \times \mathbb{Z}^9 \leq \mathsf{H}_3(\mathbb{Z})^{12}$ (still nilpotent of class 2).

Nilpotent groups: undecidability

What we actually proved:

Nilpotent groups: undecidability

What we actually proved:

König, L 2014

There is a fixed class-2 nilpotent group G and a fixed sequence of elements $g_1, g_2, \ldots, g_n \in G$ such that membership in the product

$$\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$$

is undecidable.

Nilpotent groups: undecidability

What we actually proved:

König, L 2014

There is a fixed class-2 nilpotent group G and a fixed sequence of elements $g_1, g_2, \ldots, g_n \in G$ such that membership in the product

$$\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$$

is undecidable.

Most of the g_i are central, which allows to write $\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$ as a product $G_1 G_2 G_3 G_4$ of four abelian subgroups of G.

Nilpotent groups: undecidability

What we actually proved:

König, L 2014

There is a fixed class-2 nilpotent group G and a fixed sequence of elements $g_1, g_2, \ldots, g_n \in G$ such that membership in the product

$$\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$$

is undecidable.

Most of the g_i are central, which allows to write $\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$ as a product $G_1 G_2 G_3 G_4$ of four abelian subgroups of G.

König, L 2014

There is a class-2 nilpotent group G with four abelian subgroups G_1, G_2, G_3, G_4 such that membership in $G_1 G_2 G_3 G_4$ is undecidable.

Nilpotent groups: undecidability

This result has been recently improved:

Nilpotent groups: undecidability

This result has been recently improved:

Shafrir 2025

There is a class-2 nilpotent group G with three abelian subgroups G_1, G_2, G_3 such that membership in $G_1 G_2 G_3$ is undecidable.

Nilpotent groups: undecidability

This result has been recently improved:

Shafrir 2025

There is a class-2 nilpotent group G with three abelian subgroups G_1, G_2, G_3 such that membership in $G_1 G_2 G_3$ is undecidable.

On the other hand:

Lennox, Wilson 1979

For every f.g. nilpotent (in fact, every polycyclic) group G the following problem is decidable:

INPUT: Two f.g. subgroups $G_1, G_2 \leq G$ and $g \in G$

QUESTION: $g \in G_1 G_2$?

Nilpotent groups: undecidability

Romankov 2023

There is a f.g. nilpotent group G of class 2 with SubmonoidMP(G) undecidable.

Nilpotent groups: undecidability

Romankov 2023

There is a f.g. nilpotent group G of class 2 with SubmonoidMP(G) undecidable.

Romankov's proof is also based on a reduction from Hilbert 10 (quite technical).

Nilpotent groups: undecidability

Romankov 2023

There is a f.g. nilpotent group G of class 2 with SubmonoidMP(G) undecidable.

Romankov's proof is also based on a reduction from Hilbert 10 (quite technical).

Lefaucheux (unpublished work) gave a relatively direct reduction from knapsack in $\mathsf{H}_3(\mathbb{Z})^d$ to SubmonoidMP($\mathsf{H}_3(\mathbb{Z})^e$) for some $e > d$.

Nilpotent groups: undecidability

Submonoids versus rational subsets

Bodart 2024

There is a f.g. nilpotent group of class 2 with the following properties:

- RatMP(G) is undecidable.
- SubmonoidMP(G) is decidable.

Another group with decidable SubmonoidMP and undecidable RatMP was found bei Shafrir:

Submonoids versus rational subsets

Bodart 2024

There is a f.g. nilpotent group of class 2 with the following properties:

- $\mathrm{RatMP}(G)$ is undecidable.
- $\mathrm{SubmonoidMP}(G)$ is decidable.

Another group with decidable SubmonoidMP and undecidable RatMP was found bei Shafrir:

Shafrir 2018

Every wreath product $G = A \wr (\mathbb{Z} \times \mathbb{Z})$ with A finite and abelian has the following properties:

- $\mathrm{RatMP}(G)$ is undecidable.
- $\mathrm{SubmonoidMP}(G)$ is decidable.

Groups, where SubmonoidMP and RatMP are equivalent

For a f.g. group G (finitely generated by $A \subseteq G$) define the Cayley-graph $C(G, A)$ as the graph

$$C(G, A) = (G, \{(g, ga) \mid a \in A \cup A^{-1}\}).$$

Groups, where SubmonoidMP and RatMP are equivalent

For a f.g. group G (finitely generated by $A \subseteq G$) define the Cayley-graph $C(G,A)$ as the graph

$$C(G,A) = (G, \{(g,ga) \mid a \in A \cup A^{-1}\}).$$

The number of ends of G is the supremum of the set

$$\{\text{number of infinite connected components of } C(G,A) \setminus E \mid E \text{ is a finite set of edges of } C(G,A)\}.$$

It belongs to $\mathbb{N} \cup \{\infty\}$.

Groups, where SubmonoidMP and RatMP are equivalent

For a f.g. group G (finitely generated by $A \subseteq G$) define the Cayley-graph $C(G, A)$ as the graph

$$C(G, A) = (G, \{(g, ga) \mid a \in A \cup A^{-1}\}).$$

The number of ends of G is the supremum of the set

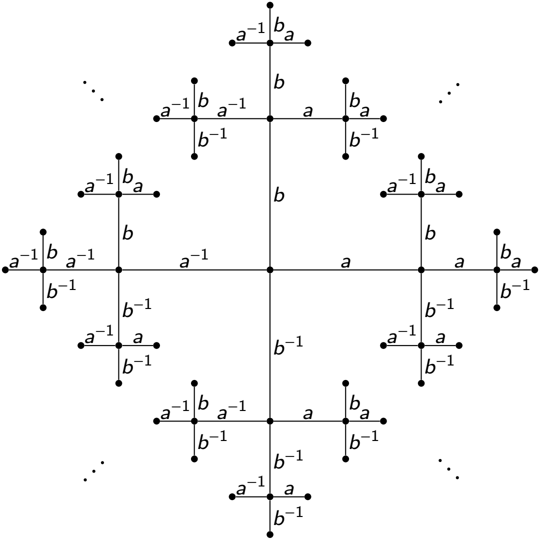
$$\{\text{number of infinite connected components of } C(G, A) \setminus E \mid \\ E \text{ is a finite set of edges of } C(G, A)\}.$$

It belongs to $\mathbb{N} \cup \{\infty\}$.

The number of ends is independent of the finite generating set A.

The ends of groups

A group with infinitely many ends: $F(a, b)$ (free group of rank 2)

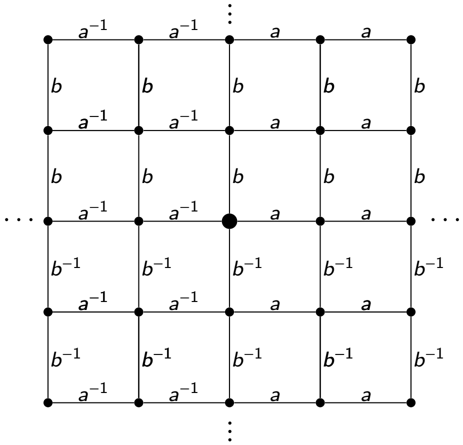


The ends of groups

A group with two ends: $\mathbb{Z}$

The ends of groups

A group with one end: $\mathbb{Z} \times \mathbb{Z}$



The ends of groups

Hopf 1942

The number of ends of a f.g. group is either 1, 2, or ∞.

The ends of groups

Hopf 1942

The number of ends of a f.g. group is either 1, 2, or ∞.

L, Steinberg 2009

If G has infinitely many ends then the following are equivalent:

- RatMP(G) is decidable.
- SubmonoidMP(G) is decidable.

The ends of groups

Hopf 1942

The number of ends of a f.g. group is either 1, 2, or ∞.

L, Steinberg 2009

If G has infinitely many ends then the following are equivalent:

- RatMP(G) is decidable.
- SubmonoidMP(G) is decidable.

Remarks:

- The proof uses the theory of groups acting on trees.

The ends of groups

Hopf 1942

The number of ends of a f.g. group is either 1, 2, or ∞.

L, Steinberg 2009

If G has infinitely many ends then the following are equivalent:

- $\mathrm{RatMP}(G)$ is decidable.
- $\mathrm{SubmonoidMP}(G)$ is decidable.

Remarks:

- The proof uses the theory of groups acting on trees.
- If G has exactly two ends, then $\mathbb{Z}$ is a finite index subgroup of G.
  It is then easy to show that $\mathrm{RatMP}(G)$ is decidable.

More groups with decidable RatMP

The Baumslag-Solitar group $\mathsf{BS}_{1,q}$ for $q \geq 2$ is

$$\mathsf{BS}_{1,q} = \langle a, t \mid t^{-1}at = a^q \rangle = \left\{ \begin{pmatrix} q^z & t \\ 0 & 1 \end{pmatrix} : z \in \mathbb{Z},\ t \in \mathbb{Z}[1/q] \right\}$$

Cadilhac, Chistikov, Zetzsche 2020

RatMP($\mathsf{BS}_{1,q}$) is decidable for every $q \geq 2$.

Remember that SubmonoidMP is undecidable for

$$\mathbb{Z} \wr \mathbb{Z} \cong \left\{ \begin{pmatrix} x^z & t \\ 0 & 1 \end{pmatrix} : z \in \mathbb{Z},\ t \in \mathbb{Z}[x, x^{-1}] \right\}.$$

L, Steinberg, Zetzsche 2015

RatMP($G \wr H$) is decidable for every finite group G and free group H.

Open problem

The context-free subset membership problem for a group G (CFMP(G)) can be defined analogously to the rational subset membership problem.

Open problem

The context-free subset membership problem for a group G (CFMP(G)) can be defined analogously to the rational subset membership problem.

Easy observations:

- If G contains a free submonoid $\{a, b\}^*$ then CFMP(G) is undecidable (reduction from Post correspondence problem).

Open problem

The context-free subset membership problem for a group G (CFMP(G)) can be defined analogously to the rational subset membership problem.

Easy observations:

- If G contains a free submonoid $\{a, b\}^*$ then CFMP(G) is undecidable (reduction from Post correspondence problem).
- If G is virtually abelian then CFMP(G) is decidable.

Open problem

The context-free subset membership problem for a group G (CFMP(G)) can be defined analogously to the rational subset membership problem.

Easy observations:

- If G contains a free submonoid $\{a, b\}^*$ then CFMP(G) is undecidable (reduction from Post correspondence problem).
- If G is virtually abelian then CFMP(G) is decidable.

What else can we say?

Open problem

The context-free subset membership problem for a group G (CFMP(G)) can be defined analogously to the rational subset membership problem.

Easy observations:

- If G contains a free submonoid $\{a, b\}^*$ then CFMP(G) is undecidable (reduction from Post correspondence problem).
- If G is virtually abelian then CFMP(G) is decidable.

What else can we say?

In particular: Is CFMP($H_3(\mathbb{Z})$) decidable?

Open problem

Why is $\mathsf{CFMP}(\mathsf{H}_3(\mathbb{Z}))$ is of particular interest?

Open problem

Why is $\mathsf{CFMP}(\mathsf{H}_3(\mathbb{Z}))$ is of particular interest?

Assume that G is a solvable group.

Open problem

Why is CFMP($\mathsf{H}_3(\mathbb{Z})$) is of particular interest?

Assume that G is a solvable group.

Rosenblatt 1974: G is either virtually nilpotent or contains a free monoid $\{a, b\}^*$.

Open problem

Why is $\mathrm{CFMP}(\mathrm{H}_3(\mathbb{Z}))$ is of particular interest?

Assume that G is a solvable group.

Rosenblatt 1974: G is either virtually nilpotent or contains a free monoid $\{a, b\}^*$.

If G contains a free monoid $\{a, b\}^*$ then $\mathrm{CFMP}(G)$ is undecidable.

Open problem

Why is CFMP($\mathsf{H}_3(\mathbb{Z})$) is of particular interest?

Assume that G is a solvable group.

Rosenblatt 1974: G is either virtually nilpotent or contains a free monoid $\{a, b\}^*$.

If G contains a free monoid $\{a, b\}^*$ then CFMP(G) is undecidable.

So, let G be virtually nilpotent.

Open problem

Why is $\mathrm{CFMP}(\mathrm{H}_3(\mathbb{Z}))$ is of particular interest?

Assume that G is a solvable group.

Rosenblatt 1974: G is either virtually nilpotent or contains a free monoid $\{a, b\}^*$.

If G contains a free monoid $\{a, b\}^*$ then $\mathrm{CFMP}(G)$ is undecidable.

So, let G be virtually nilpotent.

If G is virtually abelian then $\mathrm{CFMP}(G)$ is decidable.

Open problem

Why is $\mathsf{CFMP}(\mathsf{H}_3(\mathbb{Z}))$ is of particular interest?

Assume that G is a solvable group.

Rosenblatt 1974: G is either virtually nilpotent or contains a free monoid $\{a, b\}^*$.

If G contains a free monoid $\{a, b\}^*$ then $\mathsf{CFMP}(G)$ is undecidable.

So, let G be virtually nilpotent.

If G is virtually abelian then $\mathsf{CFMP}(G)$ is decidable.

If G is not virtually abelian then G contains a copy of $\mathsf{H}_3(\mathbb{Z})$.