Knapsack problems in groups

Daniel König, Markus Lohrey, Georg Zetzsche

March 7, 2016

Knapsack problem

Our setting

- Let G be a finitely generated (f.g.) group.
- Fix a finite (group) generating set Σ for G.
- Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

Knapsack problem

Our setting

- Let G be a finitely generated (f.g.) group.
- Fix a finite (group) generating set Σ for G.
- Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

Knapsack problem for G (Myasnikov, Nikolaev, Ushakov 2013)

- INPUT: Group elements $g, g_1, \ldots g_k$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : g = g_1^{e_1} \cdots g_k^{e_k}$?

Knapsack problem

Our setting

- Let G be a finitely generated (f.g.) group.
- Fix a finite (group) generating set Σ for G.
- Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

Knapsack problem for G (Myasnikov, Nikolaev, Ushakov 2013)

- INPUT: Group elements $g, g_1, \ldots g_k$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : g = g_1^{e_1} \cdots g_k^{e_k}$?

Decidability/complexity of knapsack does not depend on the chosen generating set for G.

Related problems

Rational subset membership problem for G

- INPUT: Group element $g \in G$ and a finite automaton with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

Related problems

Rational subset membership problem for G

- INPUT: Group element $g \in G$ and a finite automaton with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

Harder than knapsack: Take a finite automaton for $g_1^* g_2^* \cdots g_k^*$.

Related problems

Rational subset membership problem for G

- INPUT: Group element $g \in G$ and a finite automaton with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

Harder than knapsack: Take a finite automaton for $g_1^* g_2^* \cdots g_k^*$.

Knapsack problem for G with integer exponents

- INPUT: Group elements $g, g_1, \ldots g_k$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{Z} : g = g_1^{e_1} \cdots g_k^{e_k}$?

Related problems

Rational subset membership problem for G

- INPUT: Group element $g \in G$ and a finite automaton with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

Harder than knapsack: Take a finite automaton for $g_1^* g_2^* \cdots g_k^*$.

Knapsack problem for G with integer exponents

- INPUT: Group elements $g, g_1, \ldots g_k$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{Z} : g = g_1^{e_1} \cdots g_k^{e_k}$?

Easier than knapsack: Replace g^e (with $e \in \mathbb{Z}$) by $g^{e_1}(g^{-1})^{e_2}$ (with $e_1, e_2 \in \mathbb{N}$).

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \ldots a_k \in \mathbb{Z}$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : a = e_1 \cdot a_1 + \cdots + e_k \cdot a_k$?

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \ldots a_k \in \mathbb{Z}$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : a = e_1 \cdot a_1 + \cdots + e_k \cdot a_k$?

This problem is known to be decidable and the complexity depends on the encoding of the integers $a, a_1, \ldots a_k \in \mathbb{Z}$:

- Binary encoding of integers (e.g. $5 \widehat{=} 101$): NP-complete
- Unary encoding of integers (e.g. $5 \widehat{=} 11111$): P

  Exact complexity is TC^0 (Elberfeld, Jakoby, Tantau 2011).

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \ldots a_k \in \mathbb{Z}$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : a = e_1 \cdot a_1 + \cdots + e_k \cdot a_k$?

This problem is known to be decidable and the complexity depends on the encoding of the integers $a, a_1, \ldots a_k \in \mathbb{Z}$:

- Binary encoding of integers (e.g. $5 \mathrel{\widehat{=}} 101$): NP-complete
- Unary encoding of integers (e.g. $5 \mathrel{\widehat{=}} 11111$): P
  Exact complexity is TC^0 (Elberfeld, Jakoby, Tantau 2011).

Complexity bounds carry over to $\mathbb{Z}^m$ for every fixed m.

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \ldots a_k \in \mathbb{Z}$
- QUESTION: $\exists e_1, \ldots e_k \in \mathbb{N} : a = e_1 \cdot a_1 + \cdots + e_k \cdot a_k$?

This problem is known to be decidable and the complexity depends on the encoding of the integers $a, a_1, \ldots a_k \in \mathbb{Z}$:

- Binary encoding of integers (e.g. $5 \mathrel{\widehat{=}} 101$): NP-complete
- Unary encoding of integers (e.g. $5 \mathrel{\widehat{=}} 11111$): P
  Exact complexity is TC^0 (Elberfeld, Jakoby, Tantau 2011).

Complexity bounds carry over to $\mathbb{Z}^m$ for every fixed m.

Note: Our definition of knapsack corresponds to the unary variant.

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Represent the group elements $g, g_1, \ldots, g_k$ by compressed words over the generators.

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Represent the group elements $g, g_1, \ldots, g_k$ by compressed words over the generators.

Compressed words: straight-line programs (SLP) $=$ context-free grammars that produce a single word.

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Represent the group elements $g, g_1, \ldots, g_k$ by compressed words over the generators.

Compressed words: straight-line programs (SLP) $=$ context-free grammars that produce a single word.

Example: An SLP for a^{16}: $S \to AA$, $A \to BB$, $B \to CC$, $C \to DD$, $D \to a$.

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Represent the group elements $g, g_1, \ldots, g_k$ by compressed words over the generators.

Compressed words: straight-line programs (SLP) = context-free grammars that produce a single word.

Example: An SLP for a^{16}: $S \to AA$, $A \to BB$, $B \to CC$, $C \to DD$, $D \to a$.

In compressed knapsack the group elements $g, g_1, \ldots, g_k$ are encoded by SLPs that produce words over $\Sigma \cup \Sigma^{-1}$.

Compressed knapsack problem

Is there a knapsack variant for arbitrary groups that corresponds to the binary knapsack version for $\mathbb{Z}$?

Represent the group elements $g, g_1, \dots, g_k$ by compressed words over the generators.

Compressed words: straight-line programs (SLP) = context-free grammars that produce a single word.

Example: An SLP for a^{16}: $S \to AA$, $A \to BB$, $B \to CC$, $C \to DD$, $D \to a$.

In compressed knapsack the group elements $g, g_1, \dots, g_k$ are encoded by SLPs that produce words over $\Sigma \cup \Sigma^{-1}$.

More details: Next talk by Georg Zetzsche.

Decidability: hyperbolic groups, virtually special groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Decidability: hyperbolic groups, virtually special groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

L, Zetzsche 2015 (See the next talk by Georg Zetzsche)

For every virtually special group (finite extension of subgroup of a right-angled Artin group), compressed knapsack is in NP.

Decidability: hyperbolic groups, virtually special groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

L, Zetzsche 2015 (See the next talk by Georg Zetzsche)

For every virtually special group (finite extension of subgroup of a right-angled Artin group), compressed knapsack is in NP.

In particular, compressed knapsack is in NP for:

- Coxeter groups,
- one-relator groups with torsion
- fully residually free groups
- fundamental groups of hyperbolic 3-manifolds.

Decidability: hyperbolic groups, virtually special groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

L, Zetzsche 2015 (See the next talk by Georg Zetzsche)

For every virtually special group (finite extension of subgroup of a right-angled Artin group), compressed knapsack is in NP.

In particular, compressed knapsack is in NP for:

- Coxeter groups,
- one-relator groups with torsion
- fully residually free groups
- fundamental groups of hyperbolic 3-manifolds.

Ordinary knapsack for $F_2 \times F_2$ is NP-complete.

Decidability results: Heisenberg groups

The discrete Heisenberg group:

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

Decidability results: Heisenberg groups

The discrete Heisenberg group:

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z} \right\}.$$

It is the free nilpotent group of class 2 and rank 2.

Decidability results: Heisenberg groups

The discrete Heisenberg group:

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

It is the free nilpotent group of class 2 and rank 2.

König, L, Zetzsche 2015

Knapsack for $H(\mathbb{Z})$ is decidable.

Decidability results: Heisenberg groups

The discrete Heisenberg group:

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, c \in \mathbb{Z} \right\}.$$

It is the free nilpotent group of class 2 and rank 2.

König, L, Zetzsche 2015

Knapsack for $H(\mathbb{Z})$ is decidable.

Proof: An equation $A = A_1^{x_1} A_2^{x_2} \cdots A_n^{x_n}$ $(A, A_1, \ldots, A_n \in H(\mathbb{Z}))$ translates into a system of

- two linear equations and
- a single quadratic Diophantine equation.

Decidability results: Heisenberg groups

The discrete Heisenberg group:

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, c \in \mathbb{Z} \right\}.$$

It is the free nilpotent group of class 2 and rank 2.

König, L, Zetzsche 2015

Knapsack for $H(\mathbb{Z})$ is decidable.

Proof: An equation $A = A_1^{x_1} A_2^{x_2} \cdots A_n^{x_n}$ $(A, A_1, \ldots, A_n \in H(\mathbb{Z}))$ translates into a system of

- two linear equations and
- a single quadratic Diophantine equation.

By a result of Grunewald and Segal, solvability of such a system is decidable. □

Decidability results: co-context-free groups

A f.g. group G is co-context-free if the language

$$\mathrm{coWP}(G) := \{w \in (\Sigma \cup \Sigma^{-1})^* \mid w \neq 1 \text{ in } G\}$$

is context-free.

König, L, Zetzsche 2015

Knapsack for every co-context-free group G is decidable.

In particular, knapsack is decidable for $\mathbb{Z} \wr \mathbb{Z}$ and Higman-Thompson groups.

Decidability results: co-context-free groups

A f.g. group G is co-context-free if the language

$$\mathrm{coWP}(G) := \{w \in (\Sigma \cup \Sigma^{-1})^* \mid w \neq 1 \text{ in } G\}$$

is context-free.

König, L, Zetzsche 2015

Knapsack for every co-context-free group G is decidable.

In particular, knapsack is decidable for $\mathbb{Z} \wr \mathbb{Z}$ and Higman-Thompson groups.

Proof: Consider the knapsack instance

$$w = w_1^{e_1} \cdots w_k^{e_k}$$

with $w, w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$.

Decidability results: co-context-free groups

Define the alphabets $X = \{a_1, \dots, a_k\}$, $Y = X \cup \{a\}$ and the homomorphisms

$$\alpha : Y^* \to (\Sigma \cup \Sigma^{-1})^*, \qquad \beta : Y^* \to X^*$$

defined by

$$\alpha(a) = w^{-1}, \quad \alpha(a_i) = w_i, \quad \beta(a) = \varepsilon, \quad \beta(a_i) = a_i.$$

Decidability results: co-context-free groups

Define the alphabets $X = \{a_1, \ldots, a_k\}$, $Y = X \cup \{a\}$ and the homomorphisms

$$\alpha : Y^* \to (\Sigma \cup \Sigma^{-1})^*, \qquad \beta : Y^* \to X^*$$

defined by

$$\alpha(a) = w^{-1}, \quad \alpha(a_i) = w_i, \quad \beta(a) = \varepsilon, \quad \beta(a_i) = a_i.$$

For the language $M := \beta(\alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* a)$ we have:

- M is (effectively) context-free.
- $M = \{a_1^{e_1} \cdots a_k^{e_k} \mid w_1^{e_1} \cdots w_k^{e_k} \neq w \text{ in } G\}$

Decidability results: co-context-free groups

Define the alphabets $X = \{a_1, \ldots, a_k\}$, $Y = X \cup \{a\}$ and the homomorphisms

$$\alpha : Y^* \to (\Sigma \cup \Sigma^{-1})^*, \qquad \beta : Y^* \to X^*$$

defined by

$$\alpha(a) = w^{-1}, \quad \alpha(a_i) = w_i, \quad \beta(a) = \varepsilon, \quad \beta(a_i) = a_i.$$

For the language $M := \beta(\alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* a)$ we have:

- M is (effectively) context-free.
- $M = \{a_1^{e_1} \cdots a_k^{e_k} \mid w_1^{e_1} \cdots w_k^{e_k} \neq w \text{ in } G\}$

Hence, we have to check whether $M = a_1^* a_2^* \cdots a_k^*$.

Decidability results: co-context-free groups

Define the alphabets $X = \{a_1, \dots, a_k\}$, $Y = X \cup \{a\}$ and the homomorphisms

$$\alpha : Y^* \to (\Sigma \cup \Sigma^{-1})^*, \qquad \beta : Y^* \to X^*$$

defined by

$$\alpha(a) = w^{-1}, \quad \alpha(a_i) = w_i, \quad \beta(a) = \varepsilon, \quad \beta(a_i) = a_i.$$

For the language $M := \beta(\alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* a)$ we have:

- M is (effectively) context-free.
- $M = \{a_1^{e_1} \cdots a_k^{e_k} \mid w_1^{e_1} \cdots w_k^{e_k} \neq w \text{ in } G\}$

Hence, we have to check whether $M = a_1^* a_2^* \cdots a_k^*$.

Compute the Parikh image $\Psi(M) \subseteq \mathbb{N}^k$ and check whether $\Psi(M) = \mathbb{N}^k$. $\square$

Undecidability: class-2 nilpotent groups

König, L, Zetzsche 2015

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

In particular, there are nilpotent groups of class 2 with undecidable knapsack problem.

Undecidability: class-2 nilpotent groups

König, L, Zetzsche 2015

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

In particular, there are nilpotent groups of class 2 with undecidable knapsack problem.

König, L, Zetzsche 2015

Decidability of knapsack is not preserved by direct products.

Undecidability: class-2 nilpotent groups

König, L, Zetzsche 2015

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

In particular, there are nilpotent groups of class 2 with undecidable knapsack problem.

König, L, Zetzsche 2015

Decidability of knapsack is not preserved by direct products.

König, L, Zetzsche 2015

There is a nilpotent group G of class 2 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.

Undecidability: class-2 nilpotent groups

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

Undecidability: class-2 nilpotent groups

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

Proof: Reduction from Hilbert's 10th problem.

Undecidability: class-2 nilpotent groups

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

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

Undecidability: class-2 nilpotent groups

There is an $m \geq 2$ such that knapsack is undecidable for $H(\mathbb{Z})^m$.

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

Write $P(X_1, \ldots, X_k) = a$ 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 $X_0 = a$.

Undecidability: class-2 nilpotent groups

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

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

Recall that $H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle|\ a, b, c \in \mathbb{Z} \right\}$.

Undecidability: class-2 nilpotent groups

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

Recall that $H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle|\ a, b, c \in \mathbb{Z} \right\}$.

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

Undecidability: class-2 nilpotent groups

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

Recall that $H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle|\ a, b, c \in \mathbb{Z} \right\}$.

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

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

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

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

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

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

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

Undecidability: class-2 nilpotent groups

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

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

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

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

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

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

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

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

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

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

Undecidability: class-2 nilpotent groups

How to achieve synchronization?

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).

Undecidability: class-2 nilpotent groups

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:

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

Undecidability: class-2 nilpotent groups

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:

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

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

What we actually proved:

Undecidability: class-2 nilpotent groups

What we actually proved:

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.

Undecidability: class-2 nilpotent groups

What we actually proved:

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.

Undecidability: class-2 nilpotent groups

What we actually proved:

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.

This 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.

Undecidability: class-2 nilpotent groups

What we actually proved:

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.

This 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 2015

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.

Open problems

- For every polycyclic group G and all finitely generated subgroups $G_1, G_2 \leq G$, membership in $G_1 G_2$ is decidable (Lennox, Wilson 1979).

  What about a product of 3 finitely generated subgroups?

Open problems

- For every polycyclic group G and all finitely generated subgroups $G_1, G_2 \leq G$, membership in $G_1 G_2$ is decidable (Lennox, Wilson 1979).

  What about a product of 3 finitely generated subgroups?

- Is compressed knapsack for a hyperbolic group in P?

Open problems

- For every polycyclic group G and all finitely generated subgroups $G_1, G_2 \leq G$, membership in $G_1 G_2$ is decidable (Lennox, Wilson 1979).

  What about a product of 3 finitely generated subgroups?

- Is compressed knapsack for a hyperbolic group in P?

- Complexity of knapsack for a co-context-free group.

  Our algorithm runs in exponential time.

Open problems

- For every polycyclic group G and all finitely generated subgroups $G_1, G_2 \leq G$, membership in $G_1 G_2$ is decidable (Lennox, Wilson 1979).

  What about a product of 3 finitely generated subgroups?

- Is compressed knapsack for a hyperbolic group in P?

- Complexity of knapsack for a co-context-free group.

  Our algorithm runs in exponential time.

- coC-groups for a language class C having:

  (i) effective closure under inverse homomorphisms,

  (ii) effective closure under intersection with regular languages,

  (iii) effective semilinear Parikh images