Knapsack Problems in Non-Commutative Groups

Moses Ganardi, Daniel König, Markus Lohrey, Georg Zetzsche

February 10, 2018

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 $g, g_1, g_2, \ldots, g_k$
- QUESTION: $\exists x_1, \ldots x_k \in \mathbb{N} : g = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k}$?

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 $g, g_1, g_2, \ldots, g_k$
- QUESTION: $\exists x_1, \ldots x_k \in \mathbb{N} : g = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k}$?

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 A 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 A with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

At least as difficult as 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 A with transitions labelled by elements from $\Sigma \cup \Sigma^{-1}$.
- QUESTION: Does $g \in L(A)$ hold?

At least as difficult as 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: $\exists x_1, \ldots, x_k \in \mathbb{Z} : g = g_1^{x_1} \cdots g_k^{x_k}$?

Related problems

Rational subset membership problem for G

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

At least as difficult as 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: $\exists x_1, \ldots, x_k \in \mathbb{Z} : g = g_1^{x_1} \cdots g_k^{x_k}$?

Easier than knapsack:
Replace g^x (with $x \in \mathbb{Z}$) by $g^{x_1}(g^{-1})^{x_2}$ (with $x_1, x_2 \in \mathbb{N}$).

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \ldots a_k \in \mathbb{Z}$
- QUESTION: $\exists x_1, \ldots x_k \in \mathbb{N} : a = x_1 \cdot a_1 + \cdots + x_k \cdot a_k$?

Knapsack over $\mathbb{Z}$

The classical knapsack problem

- INPUT: Integers $a, a_1, \dots a_k \in \mathbb{Z}$
- QUESTION: $\exists x_1, \dots x_k \in \mathbb{N} : a = x_1 \cdot a_1 + \cdots + x_k \cdot a_k$?

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

- 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: $\exists x_1, \ldots x_k \in \mathbb{N} : a = x_1 \cdot a_1 + \cdots + x_k \cdot a_k$?

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: $\exists x_1, \ldots x_k \in \mathbb{N} : a = x_1 \cdot a_1 + \cdots + x_k \cdot a_k$?

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).

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 1: An SLP for a^{32}:
$S \to AA, \quad A \to BB, \quad B \to CC, \quad C \to DD, \quad D \to EE, \quad E \to a.$

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 1: An SLP for a^{32}:
$S \to AA, \quad A \to BB, \quad B \to CC, \quad C \to DD, \quad D \to EE, \quad E \to a.$

Example 2: An SLP for *babbabab*:
$A_i \to A_{i+1}A_{i+2}$ for $1 \leq i \leq 4, \quad A_5 \to b, \quad A_6 \to a$

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 1: An SLP for a^{32}:
$S \to AA, \quad A \to BB, \quad B \to CC, \quad C \to DD, \quad D \to EE, \quad E \to a.$

Example 2: An SLP for *babbabab*:
$A_i \to A_{i+1}A_{i+2}$ for $1 \le i \le 4, \quad A_5 \to b, \quad A_6 \to a$

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

Decidability: hyperbolic groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Decidability: hyperbolic groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Conjecture: Compressed knapsack for every infinite hyperbolic group is NP-complete.

Decidability: graph groups = right-angled Artin groups

Let (Σ, I) be a finite undirected simple graph.

$\rightharpoonup$ graph group $G(\Sigma, I) = \langle \Sigma \mid ab = ba \text{ for } (a,b) \in I \rangle$.

Decidability: graph groups = right-angled Artin groups

Let (Σ, I) be a finite undirected simple graph.

$\rightsquigarrow$ graph group $G(\Sigma, I) = \langle \Sigma \mid ab = ba \text{ for } (a,b) \in I \rangle$.

Formally: $G(\Sigma, I) = F(\Sigma)/N$, where

- $F(\Sigma)$ is the free group generated by Σ and
- $N \leq F(\Sigma)$ is the smallest normal subgroup containing all commutators $aba^{-1}b^{-1}$ for $(a,b) \in I$.

Decidability: graph groups = right-angled Artin groups

Let (Σ, I) be a finite undirected simple graph.

$\rightsquigarrow$ graph group $G(\Sigma, I) = \langle \Sigma \mid ab = ba \text{ for } (a,b) \in I \rangle$.

Formally: $G(\Sigma, I) = F(\Sigma)/N$, where

- $F(\Sigma)$ is the free group generated by Σ and
- $N \leq F(\Sigma)$ is the smallest normal subgroup containing all commutators $aba^{-1}b^{-1}$ for $(a,b) \in I$.

Extreme cases:

- $G(\Sigma, I) = \mathbb{Z}^{|\Sigma|}$ for $I = \{(a,b) \mid a \neq b\}$ (complete graph)

Decidability: graph groups = right-angled Artin groups

Let (Σ, I) be a finite undirected simple graph.

$\rightsquigarrow$ graph group $G(\Sigma, I) = \langle \Sigma \mid ab = ba \text{ for } (a,b) \in I \rangle$.

Formally: $G(\Sigma, I) = F(\Sigma)/N$, where

- $F(\Sigma)$ is the free group generated by Σ and
- $N \leq F(\Sigma)$ is the smallest normal subgroup containing all commutators $aba^{-1}b^{-1}$ for $(a,b) \in I$.

Extreme cases:

- $G(\Sigma, I) = \mathbb{Z}^{|\Sigma|}$ for $I = \{(a,b) \mid a \neq b\}$ (complete graph)
- $G(\Sigma, I) = F(\Sigma)$ for $I = \varnothing$.

Decidability: graph groups = right-angled Artin groups

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.

Decidability: graph groups = right-angled Artin groups

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.
- Prove that if $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$ has a solution, then it has a solution with $x_i \leq \lambda^{\mathrm{poly}(n)}$ for all i.

Decidability: graph groups = right-angled Artin groups

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.
- Prove that if $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$ has a solution, then it has a solution with $x_i \leq \lambda^{\mathrm{poly}(n)}$ for all i.
- Assume now that $g, g_1, \ldots, g_n$ are given by SLPs and let m be the maximal size of those SLPs. Hence, $\lambda \leq 2^{O(m)}$.

Decidability: graph groups = right-angled Artin groups

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.
- Prove that if $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$ has a solution, then it has a solution with $x_i \le \lambda^{\text{poly}(n)}$ for all i.
- Assume now that $g, g_1, \ldots, g_n$ are given by SLPs and let m be the maximal size of those SLPs. Hence, $\lambda \le 2^{O(m)}$.
- Guess binary encodings of numbers $x_i \le \lambda^{\text{poly}(n)} \le 2^{O(m \cdot \text{poly}(n))}$

Decidability: graph groups = right-angled Artin groups

L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.
- Prove that if $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$ has a solution, then it has a solution with $x_i \le \lambda^{\mathrm{poly}(n)}$ for all i.
- Assume now that $g, g_1, \ldots, g_n$ are given by SLPs and let m be the maximal size of those SLPs. Hence, $\lambda \le 2^{O(m)}$.
- Guess binary encodings of numbers $x_i \le \lambda^{\mathrm{poly}(n)} \le 2^{O(m \cdot \mathrm{poly}(n))}$
- Verify in polynomial time whether $g = g^{x_1} g^{x_2} \cdots g^{x_n}$ holds.

Decidability: graph groups = right-angled Artin groups

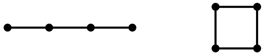
L, Zetzsche 2015

For every graph group, compressed knapsack is NP-complete.

- Consider a knapsack instance $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$, where $g, g_1, \ldots, g_n \in G(\Sigma, I)$ and $\lambda := \max\{|g|, |g_1|, \ldots, |g_n|\}$.
- Prove that if $g = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$ has a solution, then it has a solution with $x_i \leq \lambda^{\mathrm{poly}(n)}$ for all i.
- Assume now that $g, g_1, \ldots, g_n$ are given by SLPs and let m be the maximal size of those SLPs. Hence, $\lambda \leq 2^{O(m)}$.
- Guess binary encodings of numbers $x_i \leq \lambda^{\mathrm{poly}(n)} \leq 2^{O(m \cdot \mathrm{poly}(n))}$
- Verify in polynomial time whether $g = g^{x_1} g^{x_2} \cdots g^{x_n}$ holds.
  $\rightsquigarrow$ compressed word problem for $G(\Sigma, I)$.

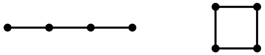
Decidability: graph groups = right-angled Artin groups

A graph (Σ, I) is a transitive forest if it does not contain one of the following two graphs (C4 and P4) as an induced subgraph:



Decidability: graph groups = right-angled Artin groups

A graph (Σ, I) is a transitive forest if it does not contain one of the following two graphs (C4 and P4) as an induced subgraph:



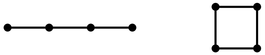
L, Zetzsche 2016

Let (Σ, I) be a finite simple undirected graph.

- (Σ, I) is a complete graph.
  $\rightsquigarrow$ knapsack for $G(\Sigma, I)$ is TC^0-complete.

Decidability: graph groups = right-angled Artin groups

A graph (Σ, I) is a transitive forest if it does not contain one of the following two graphs (C4 and P4) as an induced subgraph:



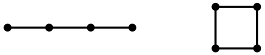
L, Zetzsche 2016

Let (Σ, I) be a finite simple undirected graph.

- (Σ, I) is a complete graph.
  $\leadsto$ knapsack for $G(\Sigma, I)$ is TC^0-complete.
- (Σ, I) is not complete but a transitive forest.
  $\leadsto$ knapsack for $G(\Sigma, I)$ is LogCFL-complete.

Decidability: graph groups = right-angled Artin groups

A graph (Σ, I) is a transitive forest if it does not contain one of the following two graphs (C4 and P4) as an induced subgraph:



L, Zetzsche 2016

Let (Σ, I) be a finite simple undirected graph.

- (Σ, I) is a complete graph.
  $\rightsquigarrow$ knapsack for $G(\Sigma, I)$ is TC^0-complete.
- (Σ, I) is not complete but a transitive forest.
  $\rightsquigarrow$ knapsack for $G(\Sigma, I)$ is LogCFL-complete.
- (Σ, I) is not a transitive forest.
  $\rightsquigarrow$ knapsack for $G(\Sigma, I)$ is NP-complete.

Decidability: graph groups = right-angled Artin groups

What's so special about transitive forests?

Decidability: graph groups = right-angled Artin groups

What's so special about transitive forests?

The class of graph groups $G(\Sigma, I)$ with (Σ, I) a transitive forest is the smallest class $\mathcal{C}$ with

- $\mathbb{Z} \in \mathcal{C}$

Decidability: graph groups = right-angled Artin groups

What's so special about transitive forests?

The class of graph groups $G(\Sigma, I)$ with (Σ, I) a transitive forest is the smallest class $\mathcal{C}$ with

- $\mathbb{Z} \in \mathcal{C}$
- $G \in \mathcal{C} \;\Rightarrow\; G \times \mathbb{Z} \in \mathcal{C}$

Decidability: graph groups = right-angled Artin groups

What's so special about transitive forests?

The class of graph groups $G(\Sigma, I)$ with (Σ, I) a transitive forest is the smallest class $\mathcal{C}$ with

- $\mathbb{Z} \in \mathcal{C}$
- $G \in \mathcal{C} \;\Rightarrow\; G \times \mathbb{Z} \in \mathcal{C}$
- $G, H \in \mathcal{C} \;\Rightarrow\; G * H \in \mathcal{C}$

Decidability: virtually special groups

A group G is virtually special if there is a subgroup $H \leq G$ of finite index such that H embeds into a graph product.

Decidability: virtually special groups

A group G is virtually special if there is a subgroup $H \leq G$ of finite index such that H embeds into a graph product.

L, Zetzsche 2015

For every virtually special group, compressed knapsack is in NP.

Decidability: virtually special groups

A group G is virtually special if there is a subgroup $H \leq G$ of finite index such that H embeds into a graph product.

L, Zetzsche 2015

For every virtually special group, compressed knapsack is in NP.

$\leadsto$ compressed knapsack is in NP for every

- Coxeter group,
- one-relator group with torsion,
- fully residually free group
- fundamental group of a hyperbolic 3-manifold.

Follows from result for graph groups:
If knapsack for G is in NP, then the same holds for
(i) every subgroup of G and (ii) every finite extension of G.

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

For every co-context-free group G, knapsack 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

For every co-context-free group G, knapsack is decidable.

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

Proof: Consider the knapsack instance

$$w = w_1^{x_1} w_2^{x_2} \cdots w_k^{x_k}$$

with $w, w_1, w_2, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$.

Decidability results: co-context-free groups

Define the homomorphism $\alpha : \{a_1, \ldots, a_k, b\}^* \to (\Sigma \cup \Sigma^{-1})^*$ by

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

Decidability results: co-context-free groups

Define the homomorphism $\alpha : \{a_1, \ldots, a_k, b\}^* \to (\Sigma \cup \Sigma^{-1})^*$ by

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

For the language

$$M := \alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* b$$

we have:

- M is (effectively) context-free.
- $M = \{a_1^{x_1} a_2^{x_2} \cdots a_k^{x_k} b \mid w_1^{x_1} w_2^{x_2} \cdots w_k^{x_k} \neq w \text{ in } G\}$

Decidability results: co-context-free groups

Define the homomorphism $\alpha : \{a_1, \ldots, a_k, b\}^* \to (\Sigma \cup \Sigma^{-1})^*$ by

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

For the language

$$M := \alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* b$$

we have:

- M is (effectively) context-free.
- $M = \{a_1^{x_1} a_2^{x_2} \cdots a_k^{x_k} b \mid w_1^{x_1} w_2^{x_2} \cdots w_k^{x_k} \neq w \text{ in } G\}$

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

Decidability results: co-context-free groups

Define the homomorphism $\alpha : \{a_1, \ldots, a_k, b\}^* \to (\Sigma \cup \Sigma^{-1})^*$ by

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

For the language

$$M := \alpha^{-1}(\mathrm{coWP}(G)) \cap a_1^* a_2^* \cdots a_k^* b$$

we have:

- M is (effectively) context-free.
- $M = \{a_1^{x_1} a_2^{x_2} \cdots a_k^{x_k} b \mid w_1^{x_1} w_2^{x_2} \cdots w_k^{x_k} \neq w \text{ in } G\}$

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

Compute the Parikh image $\Psi(M) \subseteq \mathbb{N}^{k+1}$ and check whether $\Psi(M) = \{(n_1, n_2, \ldots, n_k, 1) \mid n_i \in \mathbb{N}\}$. □

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 $P(X_1, \dots, X_k) \in \mathbb{Z}[X_1, \dots, X_k]$ 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 $X_0 = a$.

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

Undecidability: class-2 nilpotent groups

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

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

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 $A_1 = (A, \mathrm{Id}, \mathrm{Id})$, $A_2 = (\mathrm{Id}, A, \mathrm{Id})$, $A_3 = (\mathrm{Id}, \mathrm{Id}, A)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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:

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

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).

Undecidability: class-2 nilpotent groups

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 $g_1, g_2, \dots, g_n \in G$ 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.

Knapsack-semilinear groups

(semi-)linear sets

A subset $A \subseteq \mathbb{N}^k$ is linear if there exist $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ such that

$$A = \{v_0 + \lambda_1 v_1 + \cdots + \lambda_n v_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}.$$

A semilinear set is a finite union of linear sets.

Knapsack-semilinear groups

(semi-)linear sets

A subset $A \subseteq \mathbb{N}^k$ is linear if there exist $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ such that

$$A = \{v_0 + \lambda_1 v_1 + \cdots + \lambda_n v_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}.$$

A semilinear set is a finite union of linear sets.

knapsack-semilinear groups

The f.g. group G is knapsack-semilinear if for all $g, g_1, g_2, \ldots, g_k \in G$ the set

$$\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid g = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k}\}$$

is semilinear and the vectors in a semilinear representation of this set can be effectively computed from $g, g_1, \ldots, g_k$.

Obviously, knapsack is decidable for every knapsack-semilinear

Knapsack-semilinear groups

The class of knapsack-semilinear groups is very rich:

Ganardi, König, L, Zetzsche 2017

The following groups are knapsack-semilinear:

- virtually special groups
- hyperbolic groups
- co-context-free groups
- free solvable groups

Knapsack-semilinear groups

Ganardi, König, L, Zetzsche 2017

If G and H are knapsack-semilinear, then the following groups are knapsack-semilinear as well:

- every f.g. subgroup of G
- every finite extension of G
- $G \times H$ and $G * H$
- HNN-extension $\langle G, t \mid t^{-1}at = \varphi(a)(a \in A)\rangle$ with $A \leq G$ finite
- amalgamated free product $G *_A H$ where A is a finite subgroup of G and H.
- $G \wr H$ (restricted wreath product of G and H)

Knapsack-semilinear groups

Ganardi, König, L, Zetzsche 2017

If G and H are knapsack-semilinear, then the following groups are knapsack-semilinear as well:

- every f.g. subgroup of G
- every finite extension of G
- $G \times H$ and $G * H$
- HNN-extension $\langle G, t \mid t^{-1}at = \varphi(a) (a \in A)\rangle$ with $A \leq G$ finite
- amalgamated free product $G *_A H$ where A is a finite subgroup of G and H.
- $G \wr H$ (restricted wreath product of G and H)

But: there are f.g. groups, which are not knapsack-semilinear and for which knapsack is still decidable: Heisenberg group $H(\mathbb{Z})$.

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?

- 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?

- 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

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?

- 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

- Knapsack for automaton groups.