Knapsack Problems in Hyperbolic Groups

Markus Lohrey

September 30, 2018

Knapsack problem

Our setting

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

Knapsack problem

Our setting

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

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

- INPUT: Group elements $g, g_1, g_2, \ldots, g_k \in G$
- 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 generating set Σ for G with $a \in \Sigma \Leftrightarrow a^{-1} \in \Sigma$.
- Elements of G are represented by finite words over Σ.

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

- INPUT: Group elements $g, g_1, g_2, \ldots, g_k \in G$
- 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 Σ.
- 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 Σ.
- 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 Σ.
- 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 $g, g_1, \dots g_k$
- QUESTION: $\exists x_1, \dots, x_k \in \mathbb{Z} : g = g_1^{x_1} \cdots g_k^{x_k}$?

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

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

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. $5 \mathrel{\widehat{=}} 101$): 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. $5 \mathrel{\widehat{=}} 101$): 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 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 $1 \leq i \leq 4, \quad A_5 \to b, \quad A_6 \to a$

In compressed knapsack the group elements $g, g_1, \ldots, g_k$ are encoded by SLPs that produce words over Σ.

Some known results

Knapsack is decidable for

- all virtually special groups
  $=$ finite extensions of subgroups of right-angled Artin groups
- all co-context-free groups
  $=$ groups where complement of word problem is context-free
- all Baumslag-Solitar groups $\mathrm{BS}(1, q) = \langle a, t \mid t^{-1}at = a^q \rangle$
- the discrete Heisenberg group $H_3(\mathbb{Z})$

Knapsack is undecidable for

- $H_3(\mathbb{Z})^k$ where k is a fixed large enough number.

Cayley graph

The Cayley graph $\Gamma = \Gamma(G, \Sigma)$ of G (w.r.t. Σ) is the graph with

- node set G and
- edge set $E = \{(g, ga) \mid g \in G, a \in \Sigma\}$.

Cayley graph

The Cayley graph $\Gamma = \Gamma(G, \Sigma)$ of G (w.r.t. Σ) is the graph with

- node set G and
- edge set $E = \{(g, ga) \mid g \in G, a \in \Sigma\}$.

With $d_\Gamma(g, h)$ we denote the distance in Γ (length of a shortest path) between $g \in G$ and $h \in G$.

Hyperbolic groups

Cayley graph

The Cayley graph $\Gamma = \Gamma(G, \Sigma)$ of G (w.r.t. Σ) is the graph with

- node set G and
- edge set $E = \{(g, ga) \mid g \in G, a \in \Sigma\}$.

With $d_\Gamma(g, h)$ we denote the distance in Γ (length of a shortest path) between $g \in G$ and $h \in G$.

Geodesic triangles and slim triangles

A geodesic triangle Δ consists of points $p, q, r \in G$ and paths $P_{p,q}$, $P_{p,r}$, $P_{q,r}$ (the sides of the triangle), where $P_{x,y}$ is a path between x and y of length $d_\Gamma(x, y)$ (a geodesic path).

Hyperbolic groups

Cayley graph

The Cayley graph $\Gamma = \Gamma(G, \Sigma)$ of G (w.r.t. Σ) is the graph with

- node set G and
- edge set $E = \{(g, ga) \mid g \in G, a \in \Sigma\}$.

With $d_\Gamma(g, h)$ we denote the distance in Γ (length of a shortest path) between $g \in G$ and $h \in G$.

Geodesic triangles and slim triangles

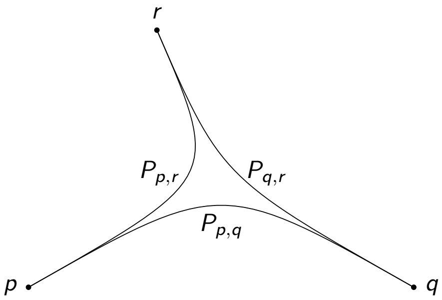
A geodesic triangle Δ consists of points $p, q, r \in G$ and paths $P_{p,q}$, $P_{p,r}$, $P_{q,r}$ (the sides of the triangle), where $P_{x,y}$ is a path between x and y of length $d_\Gamma(x, y)$ (a geodesic path).

Δ is δ-slim for $\delta \geq 0$ if every point on a side $P_{x,y}$ has distance at most δ from a point belonging to one of the two opposite sides.

Hyperbolic groups (Gromov 1987)

A group is hyperbolic if there is a constant δ such that every geodesic triangle is δ-slim.

The shape of a geodesic triangle in a hyperbolic group:



Some facts about hyperbolic groups

- Let G be hyperbolic. Then, either
  1. $F_2 \leq G$ (nonelementary hyperbolic groups) or
  2. $\mathbb{Z} \leq G$ with $[G : \mathbb{Z}]$ finite (elementary hyperbolic groups)

Some facts about hyperbolic groups

- Let G be hyperbolic. Then, either
  1. $F_2 \leq G$ (nonelementary hyperbolic groups) or
  2. $\mathbb{Z} \leq G$ with $[G : \mathbb{Z}]$ finite (elementary hyperbolic groups)
- The word problem for a hyperbolic group can be solved in
  1. linear time and
  2. belongs to the complexity class LogCFL $\subseteq \mathsf{NC}^2$.

  LogCFL = closure of context-free languages under logspace reductions.

Complexity of knapsack in hyperbolic groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Complexity of knapsack in hyperbolic groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Theorem 1

Let G be a hyperbolic group. Knapsack for G is

- in LogCFL and is
- LogCFL-complete if G is nonelementary.

Complexity of knapsack in hyperbolic groups

Myasnikov, Nikolaev, Ushakov 2013

Knapsack for every hyperbolic group belongs to P.

Theorem 1

Let G be a hyperbolic group. Knapsack for G is

- in LogCFL and is
- LogCFL-complete if G is nonelementary.

Theorem 2

For every infinite hyperbolic group, compressed knapsack is NP-complete.

Some proof ingredients

Myasnikov, Nikolaev, Ushakov 2013

Let G be hyperbolic, $g, g_1, \dots, g_k$, and $N = |g| + |g_1| + \cdots + |g_k|$.

Some proof ingredients

Myasnikov, Nikolaev, Ushakov 2013

Let G be hyperbolic, $g, g_1, \ldots, g_k$, and $N = |g| + |g_1| + \cdots + |g_k|$.

If there exist $x_1, \ldots, x_k \in \mathbb{N}$ with $g = g_1^{x_1} \cdots g_k^{x_k}$ then there exists such $x_1, \ldots, x_k \leq p(N)$ for a polyomial p only depending on G.

Some proof ingredients

Myasnikov, Nikolaev, Ushakov 2013

Let G be hyperbolic, $g, g_1, \ldots, g_k$, and $N = |g| + |g_1| + \cdots + |g_k|$.

If there exist $x_1, \ldots, x_k \in \mathbb{N}$ with $g = g_1^{x_1} \cdots g_k^{x_k}$ then there exists such $x_1, \ldots, x_k \le p(N)$ for a polyomial p only depending on G.

Grunschlag 1999 / Buntrock, Otto 1998

The word problem for a hyperbolic group is

1. growing context-sensitive and hence
2. can be recognized by a one-way logspace-bounded AuxPDA in polynomial time.

Some proof ingredients

Myasnikov, Nikolaev, Ushakov 2013

Let G be hyperbolic, $g, g_1, \dots, g_k$, and $N = |g| + |g_1| + \cdots + |g_k|$.

If there exist $x_1, \dots, x_k \in \mathbb{N}$ with $g = g_1^{x_1} \cdots g_k^{x_k}$ then there exists such $x_1, \dots, x_k \le p(N)$ for a polyomial p only depending on G.

Grunschlag 1999 / Buntrock, Otto 1998

The word problem for a hyperbolic group is

1. growing context-sensitive and hence
2. can be recognized by a one-way logspace-bounded AuxPDA in polynomial time.

Holt, L, Schleimer 2018

The compressed word problem for a hyperbolic group belongs to P.

Hyperbolic groups are knapsack-semilinear

(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.

Hyperbolic groups are knapsack-semilinear

(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

A finitely generated group G is knapsack-semilinear if for all $g, g_1, g_2, \ldots, g_k \in G$ the following set is semilinear:

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

Hyperbolic groups are knapsack-semilinear

(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

A finitely generated group G is knapsack-semilinear if for all $g, g_1, g_2, \ldots, g_k \in G$ the following set is semilinear:

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

Theorem 3

Every hyperbolic group is knapsack-semilinear.

Open problems

- Knapsack in braid groups:
  Is it decidable?

Open problems

- Knapsack in braid groups:

  Is it decidable?

- Knapsack in co-context-free groups.

  It can be solved in exponential time.

  Is there a better upper bound?

Open problems

- Knapsack in braid groups:

  Is it decidable?

- Knapsack in co-context-free groups.

  It can be solved in exponential time.

  Is there a better upper bound?

- Knapsack for automaton groups:

  There are automaton groups with undecidable knapsack problem (powers of Heisenberg group).

  For which automaton groups is knapsack decidable?