Knapsack and the power word problem in solvable Baumslag-Solitar groups

Markus Lohrey, Georg Zetzsche

October 15, 2020

Baumslag-Solitar groups

For $p, q \in \mathbb{N} \setminus \{0\}$ let $\mathrm{BS}(p, q) = \langle a, t \mid t^{-1} a^p t = a^q \rangle$.

Baumslag-Solitar groups

For $p, q \in \mathbb{N} \setminus \{0\}$ let $\mathrm{BS}(p, q) = \langle a, t \mid t^{-1} a^p t = a^q \rangle$.

Weiß 2015

The word problem for $\mathrm{BS}(p, q)$ can be solved on a deterministic Turing machine whose work tape has length log(input length), i.e., it belongs to the complexity class logarithmic space.

Baumslag-Solitar groups

For $p, q \in \mathbb{N} \setminus \{0\}$ let $\mathrm{BS}(p, q) = \langle a, t \mid t^{-1} a^p t = a^q \rangle$.

Weiß 2015

The word problem for $\mathrm{BS}(p, q)$ can be solved on a deterministic Turing machine whose work tape has length log(input length), i.e., it belongs to the complexity class logarithmic space.

$\mathrm{BS}(1, q) = \langle a, t \mid t^{-1} a t = a^q \rangle$ is solvable and linear.

Baumslag-Solitar groups

For $p, q \in \mathbb{N} \setminus \{0\}$ let $\mathrm{BS}(p,q) = \langle a, t \mid t^{-1}a^p t = a^q \rangle$.

Weiß 2015

The word problem for $\mathrm{BS}(p,q)$ can be solved on a deterministic Turing machine whose work tape has length log(input length), i.e., it belongs to the complexity class logarithmic space.

$\mathrm{BS}(1,q) = \langle a, t \mid t^{-1}at = a^q \rangle$ is solvable and linear.

$\mathrm{BS}(1,q)$ is the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ generated by the two matrices

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}.$$

Baumslag-Solitar groups

For $p, q \in \mathbb{N} \setminus \{0\}$ let $\mathrm{BS}(p,q) = \langle a, t \mid t^{-1} a^p t = a^q \rangle$.

Weiß 2015

The word problem for $\mathrm{BS}(p,q)$ can be solved on a deterministic Turing machine whose work tape has length log(input length), i.e., it belongs to the complexity class logarithmic space.

$\mathrm{BS}(1,q) = \langle a, t \mid t^{-1} a t = a^q \rangle$ is solvable and linear.

$\mathrm{BS}(1,q)$ is the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ generated by the two matrices

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}.$$

Corollary

The word problem for $\mathrm{BS}(1,q)$ is in TC^0.

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size poly(n),

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size poly(n),
- the depth of the circuit is bounded by a constant.

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size poly(n),
- the depth of the circuit is bounded by a constant.

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size poly(n),
- the depth of the circuit is bounded by a constant.

Uniformity: given n it should be "very easy" to construct C_n.

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size poly(n),
- the depth of the circuit is bounded by a constant.

Uniformity: given n it should be "very easy" to construct C_n.

Details are quite technical! Implicitly we work with the strongest reasonable uniformity assumption (DLOGTIME-uniformity).

Excurse to TC^0

Formal definition of TC^0

A language $L \subseteq \{0,1\}^*$ belongs to TC^0 if for every $n \geq 0$ there is a Boolean circuit C_n such that:

- C_n accepts $L \cap \{0,1\}^n$,
- C_n consists of AND-gates, OR-gates, NOT-gates and majority gates,
- the fan-in of the gates is not restricted,
- the number of gates of C_n is of size $\mathrm{poly}(n)$,
- the depth of the circuit is bounded by a constant.

Uniformity: given n it should be "very easy" to construct C_n.

Details are quite technical! Implicitly we work with the strongest reasonable uniformity assumption (DLOGTIME-uniformity).

TC^0 is the smallest complexity class that allows to do arithmetic.

Excurse to TC^0

Problems in TC^0

- computing sum, product, or integer quotient of two binary encoded integers (Hesse, Allender, Barrington 2002)

Excurse to TC^0

Problems in TC^0

- computing sum, product, or integer quotient of two binary encoded integers (Hesse, Allender, Barrington 2002)
- word problem for finitely generated solvable linear groups (L, König 2018)

Excurse to TC^0

Problems in TC^0

- computing sum, product, or integer quotient of two binary encoded integers (Hesse, Allender, Barrington 2002)
- word problem for finitely generated solvable linear groups (L, König 2018)
- conjugacy problem for free solvable groups and iterated wreath products of abelian groups (Miasnikov, Vassileva, Weiß2017)

Excurse to TC^0

Problems in TC^0

- computing sum, product, or integer quotient of two binary encoded integers (Hesse, Allender, Barrington 2002)
- word problem for finitely generated solvable linear groups (L, König 2018)
- conjugacy problem for free solvable groups and iterated wreath products of abelian groups (Miasnikov, Vassileva, Weiß2017)
- Subgroup membership for finitely generated nilpotent groups (Miasnikov, Weiß2017)

Power word problem

G a finitely generated group with finite generating set Σ.

Power word problem

G a finitely generated group with finite generating set Σ.

Power word problem of G

INPUT: Words $w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$, binary encoded $n_1, \ldots, n_k \in \mathbb{N}$.

QUESTION: $w_1^{n_1} \cdots w_k^{n_k} = 1$ in G?

Power word problem

G a finitely generated group with finite generating set Σ.

Power word problem of G

INPUT: Words $w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$, binary encoded $n_1, \ldots, n_k \in \mathbb{N}$.
QUESTION: $w_1^{n_1} \cdots w_k^{n_k} = 1$ in G?

Special case of the so-called compressed word problem for G.

Power word problem

G a finitely generated group with finite generating set Σ.

Power word problem of G

INPUT: Words $w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$, binary encoded $n_1, \ldots, n_k \in \mathbb{N}$.
QUESTION: $w_1^{n_1} \cdots w_k^{n_k} = 1$ in G?

Special case of the so-called compressed word problem for G.

Ge 1993

For given algebraic numbers $\alpha_1, \ldots, \alpha_k$ and binary encoded $n_1, \ldots, n_k \in \mathbb{N}$ one can check in polynomial time whether $\alpha_1^{n_1} \cdots \alpha_k^{n_k} = 1$ holds.

Power word problems for groups

Some complexity results for power word problems:

	computational complexity of power word problem

Power word problems for groups

Some complexity results for power word problems:

	computational complexity of power word problem
f.g. nilpotent groups free solvable groups	TC^0 (L, Weiß 2019, Figelius, Ganardi, L, Zetzsche 2020)

Power word problems for groups

Some complexity results for power word problems:

	computational complexity of power word problem
f.g. nilpotent groups free solvable groups	TC^0 (L, Weiß 2019, Figelius, Ganardi, L, Zetzsche 2020)
f.g. free groups Grigorchuk group	logspace (L, Weiß 2019)

Power word problems for groups

Some complexity results for power word problems:

	computational complexity of power word problem
f.g. nilpotent groups free solvable groups	TC^0 (L, Weiß 2019, Figelius, Ganardi, L, Zetzsche 2020)
f.g. free groups Grigorchuk group	logspace (L, Weiß 2019)
Thompson's group F	coNP-complete (Figelius, Ganardi, L, Zetzsche 2020)

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.
  (so-called super-sparse or lacunary representation).

Power word problem for BS$(1, q)$

Theorem 1

The power word problem for BS$(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for BS$(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.
  (so-called super-sparse or lacunary representation).

  QUESTION: Does $P(q) = 0$ hold?

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.
  (so-called super-sparse or lacunary representation).

  QUESTION: Does $P(q) = 0$ hold?

- H.W. Lenstra Jr. 1999: The above problem is in polynomial time.

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.
  (so-called super-sparse or lacunary representation).

  QUESTION: Does $P(q) = 0$ hold?

- H.W. Lenstra Jr. 1999: The above problem is in polynomial time.
  (for every algebraic number in the place of q).

Power word problem for $\mathrm{BS}(1, q)$

Theorem 1

The power word problem for $\mathrm{BS}(1, q)$ is in TC^0.

Proof strategy:

- Main step: Reduce the power word problem for $\mathrm{BS}(1, q)$ to the following problem:

  INPUT: Polynomial $P(x) = a_1 x^{e_1} + \cdots + a_k x^{e_k} \in \mathbb{Z}[x]$ represented by the list of binary encoded numbers $a_1, e_1, \ldots, a_k, e_k$.
  (so-called super-sparse or lacunary representation).

  QUESTION: Does $P(q) = 0$ hold?

- H.W. Lenstra Jr. 1999: The above problem is in polynomial time.
  (for every algebraic number in the place of q).
- Lenstra's algorithm can be implemented in TC^0.

Power word problems for some matrix groups

Hence, we get:

Theorem 2

For every $\alpha \in \mathbb{C} \setminus \{0\}$ the power word problem for the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

belongs to DLOGTIME-uniform TC^0.

Power word problems for some matrix groups

Hence, we get:

Theorem 2

For every $\alpha \in \mathbb{C} \setminus \{0\}$ the power word problem for the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

belongs to DLOGTIME-uniform TC^0.

For α transcendental, the above group is isomorphic to $\mathbb{Z} \wr \mathbb{Z}$, for which the power word problem is in TC^0 (L, Weiß 2019).

The knapsack problem for groups

The knapsack problem for groups

Knapsack problem for group $G = \langle \Sigma \rangle$ (Miasnikov, Nikolaev, Ushakov 2014)

INPUT: Words $w_0, w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$

QUESTION: Are there $x_1, \ldots, x_k \in \mathbb{N}$ with $w_1^{x_1} \cdots w_k^{x_k} = w_0$ in G?

The knapsack problem for groups

Knapsack problem for group $G = \langle \Sigma \rangle$ (Miasnikov, Nikolaev, Ushakov 2014)

INPUT: Words $w_0, w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$

QUESTION: Are there $x_1, \ldots, x_k \in \mathbb{N}$ with $w_1^{x_1} \cdots w_k^{x_k} = w_0$ in G?

Note: knapsack = rational subset membership for sets $w_1^* w_2^* \cdots w_k^*$.

The knapsack problem for groups

Knapsack problem for group $G = \langle \Sigma \rangle$ (Miasnikov, Nikolaev, Ushakov 2014)

INPUT: Words $w_0, w_1, \ldots, w_k \in (\Sigma \cup \Sigma^{-1})^*$

QUESTION: Are there $x_1, \ldots, x_k \in \mathbb{N}$ with $w_1^{x_1} \cdots w_k^{x_k} = w_0$ in G?

Note: knapsack = rational subset membership for sets $w_1^* w_2^* \cdots w_k^*$.

Babai, Beals, Cai, Ivanyos, Luks 1996

The following problem can be solved in polynomial time:

INPUT: Non-singluar commuting matrixes $A_1, \ldots, A_k, B$ over an algebraic number field.

QUESTION: Are there $x_1, \ldots, x_k \in \mathbb{Z}$ with $A_1^{x_1} \cdots A_k^{x_k} = B$?

Problem becomes NP-complete if $x_1, \ldots, x_k \in \mathbb{N}$

Knapsack problems

	knapsack problem

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)
Heisenberg group	decidable (König, L, Zetzsche 2015)

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)
Heisenberg group	decidable (König, L, Zetzsche 2015)
co-context-free groups	decidable (König, L, Zetzsche 2015)

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)
Heisenberg group	decidable (König, L, Zetzsche 2015)
co-context-free groups	decidable (König, L, Zetzsche 2015)
hyperbolic groups	in P (Miasnikov, Nikolaev, Ushakov 2014)

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)
Heisenberg group	decidable (König, L, Zetzsche 2015)
co-context-free groups	decidable (König, L, Zetzsche 2015)
hyperbolic groups	in P (Miasnikov, Nikolaev, Ushakov 2014)
virtually special groups	in NP (L, Zetzsche 2015)

Knapsack problems

	knapsack problem
f.g. 2-step nilpotent groups	undecidable in general (L 2014, Mishchenko, Treyer 2016)
Heisenberg group	decidable (König, L, Zetzsche 2015)
co-context-free groups	decidable (König, L, Zetzsche 2015)
hyperbolic groups	in P (Miasnikov, Nikolaev, Ushakov 2014)
virtually special groups	in NP (L, Zetzsche 2015)
free solvable groups	in NP (Figelius, Ganardi, L, Zetzsche 2020)

Knapsack for BS$(1, q)$

Theorem

The knapsack problem for BS$(1, q) = \langle a, t \mid t^{-1}at = a^q \rangle$ is NP-complete.

Knapsack for BS$(1, q)$

Theorem

The knapsack problem for BS$(1, q) = \langle a, t \mid t^{-1}at = a^q \rangle$ is NP-complete.

Unusual:

- Solution sets not semilinear!

  Solution set of $(t^{-x}at^y = a^z) = \{(k, k, q^k) \mid k \in \mathbb{N}\}$

- Minimal solutions can be doubly exponential for BS$(1, 2)$!

  Hence, one cannot guess a solution with binary encoded exponents and then reduce to power word problem.

Previous result on knapsack for $\mathrm{BS}(1, q)$

Recall: $\mathrm{BS}(1, q) \cong \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{Z}, z \in \mathbb{Z}[1/q] \right\}$

Previous result on knapsack for BS$(1, q)$

Recall: $\mathrm{BS}(1, q) \cong \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{Z}, z \in \mathbb{Z}[1/q] \right\}$

Dudkin & Treyer 2018

Decidability for instances $g_1^{x_1} \cdots g_k^{x_k} = h$ where every $g_i = \begin{pmatrix} q^{d_i} & z_i \\ 0 & 1 \end{pmatrix}$ satisfies $d_i \neq 0$.

Previous result on knapsack for BS$(1, q)$

Recall: $\mathrm{BS}(1, q) \cong \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{Z}, z \in \mathbb{Z}[1/q] \right\}$

Dudkin & Treyer 2018

Decidability for instances $g_1^{x_1} \cdots g_k^{x_k} = h$ where every $g_i = \begin{pmatrix} q^{d_i} & z_i \\ 0 & 1 \end{pmatrix}$ satisfies $d_i \neq 0$.

Used decidability of $\mathrm{FO}(\mathbb{Z}, +, \geq, n \mapsto q^n)$ (Semënov 1979)

Previous result on knapsack for BS$(1, q)$

Recall: $\mathrm{BS}(1,q) \cong \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{Z}, z \in \mathbb{Z}[1/q] \right\}$

Dudkin & Treyer 2018

Decidability for instances $g_1^{x_1} \cdots g_k^{x_k} = h$ where every $g_i = \begin{pmatrix} q^{d_i} & z_i \\ 0 & 1 \end{pmatrix}$ satisfies $d_i \neq 0$.

Used decidability of $\mathrm{FO}(\mathbb{Z}, +, \geq, n \mapsto q^n)$ (Semënov 1979)

Cadilhac, Chistikov, Zetzsche 2020

Rational subset membership problem for BS$(1, q)$ is PSPACE-complete.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Fix a knapsack equation $g_1^{x_1} \cdots g_k^{x_k} = g_0$ over BS$(1, q)$.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Fix a knapsack equation $g_1^{x_1} \cdots g_k^{x_k} = g_0$ over BS$(1, q)$.

Key trick: Do not introduce variables in the logic for $x_1, \ldots, x_k$

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Fix a knapsack equation $g_1^{x_1} \cdots g_k^{x_k} = g_0$ over BS$(1, q)$.

Key trick: Do not introduce variables in the logic for $x_1, \ldots, x_k$

Instead: Variables for entries of matrices $g_1^{x_1} \cdots g_i^{x_i}$ for $i = 1, \ldots, k$.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Fix a knapsack equation $g_1^{x_1} \cdots g_k^{x_k} = g_0$ over BS$(1, q)$.

Key trick: Do not introduce variables in the logic for $x_1, \ldots, x_k$

Instead: Variables for entries of matrices $g_1^{x_1} \cdots g_i^{x_i}$ for $i = 1, \ldots, k$.

Let $\mathrm{BS}_{\mathbb{Z}}(1, q) = \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{N}, z \in \mathbb{Z} \right\} \subseteq \mathrm{BS}(1, q)$.

Knapsack problem for BS$(1, q)$

Büchi arithmetic

First-order logic over $(\mathbb{Z}, +, \geq, V_q)$ with $V_q(n) = \max\{q^k : q^k \mid n\}$.

Theorem (Guépin, Haase, Worrell 2019)

The existential fragment of Büchi arithmetic is NP-complete.

Fix a knapsack equation $g_1^{x_1} \cdots g_k^{x_k} = g_0$ over BS$(1, q)$.

Key trick: Do not introduce variables in the logic for $x_1, \ldots, x_k$

Instead: Variables for entries of matrices $g_1^{x_1} \cdots g_i^{x_i}$ for $i = 1, \ldots, k$.

Let $\mathrm{BS}_{\mathbb{Z}}(1, q) = \left\{ \begin{pmatrix} q^d & z \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{N}, z \in \mathbb{Z} \right\} \subseteq \mathrm{BS}(1, q)$.

Represent elements of $\mathrm{BS}_{\mathbb{Z}}(1, q)$ in the logic by two integer variables.

Knapsack problem for BS$(1, q)$

Step 1

Knapsack problem for BS$(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

Knapsack problem for $\mathrm{BS}(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

- $X \cdot g = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$

Knapsack problem for $\mathrm{BS}(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

- $X \cdot g = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$
- $X \cdot g^* = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$

Knapsack problem for $\mathrm{BS}(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

- $X \cdot g = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$
- $X \cdot g^* = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$

The following are equivalent

Knapsack problem for $\mathrm{BS}(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

- $X \cdot g = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$
- $X \cdot g^* = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$

The following are equivalent

- $\exists x_1, \ldots, x_k \in \mathbb{N} : g_1^{x_1} \cdots g_k^{x_k} = g_0$

Knapsack problem for $\mathrm{BS}(1, q)$

Step 1

From $g \in \mathrm{BS}(1, q)$ we construct small formulae that express

- $X \cdot g = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$
- $X \cdot g^* = Y$ for variables $X, Y \in \mathrm{BS}_{\mathbb{Z}}(1, q)$

The following are equivalent

- $\exists x_1, \ldots, x_k \in \mathbb{N} : g_1^{x_1} \cdots g_k^{x_k} = g_0$
- $\exists X_0, \ldots, X_k \in \mathrm{BS}_{\mathbb{Z}}(1, q) : \bigwedge_{i=0}^{d-1} X_i \cdot g_i^* = X_{i+1} \ \wedge \ X_0 \cdot g_0 = X_k$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \, x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \, x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

$X \cdot g = Y$: can be expressed in existential Presburger logic.

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \, x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

$X \cdot g = Y$: can be expressed in existential Presburger logic.

$\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$: let $g = \begin{pmatrix} q^d & a \\ 0 & 1 \end{pmatrix}$ with $d \in \mathbb{Z}$ and $a \in \mathbb{Z}[1/q]$.

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

$X \cdot g = Y$: can be expressed in existential Presburger logic.

$\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$: let $g = \left(\begin{smallmatrix} q^d & a \\ 0 & 1 \end{smallmatrix}\right)$ with $d \in \mathbb{Z}$ and $a \in \mathbb{Z}[1/q]$.

Case 1. $d \neq 0$: Simple computation transforms $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ into

$$\exists s \in \mathbb{N} \; \exists z \in \mathbb{Z} : x = q^{d \cdot s} \cdot u \wedge a \cdot z + v = y \wedge (q^d - 1) \cdot z = x - u$$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

$X \cdot g = Y$: can be expressed in existential Presburger logic.

$\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$: let $g = \left(\begin{smallmatrix} q^d & a \\ 0 & 1 \end{smallmatrix}\right)$ with $d \in \mathbb{Z}$ and $a \in \mathbb{Z}[1/q]$.

Case 1. $d \neq 0$: Simple computation transforms $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ into

$$\exists s \in \mathbb{N} \; \exists z \in \mathbb{Z} : x = q^{d \cdot s} \cdot u \wedge a \cdot z + v = y \wedge (q^d - 1) \cdot z = x - u$$

Case 2. $d = 0$, i.e., $g = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ is equivalent to

$$u = x \wedge \exists s \in \mathbb{N} : y = v + a \cdot s \cdot u$$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : x = q^r \wedge y = q^{d \cdot s} x$.

Step 2. Express $X \cdot g = Y$ and $X \cdot g^* = Y$ in existential Presburger + S_d.

$X \cdot g = Y$: can be expressed in existential Presburger logic.

$\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$: let $g = \left(\begin{smallmatrix} q^d & a \\ 0 & 1 \end{smallmatrix}\right)$ with $d \in \mathbb{Z}$ and $a \in \mathbb{Z}[1/q]$.

Case 1. $d \neq 0$: Simple computation transforms $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ into

$$\exists s \in \mathbb{N} \; \exists z \in \mathbb{Z} : x = q^{d \cdot s} \cdot u \wedge a \cdot z + v = y \wedge (q^d - 1) \cdot z = x - u$$

Case 2. $d = 0$, i.e., $g = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \cdot g^* = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ is equivalent to

$$u = x \wedge \exists s \in \mathbb{N} : y = v + a \cdot s \cdot u$$

Morover, $\exists s \in \mathbb{N} : y = v + a \cdot s \cdot u$ can be expressed as

$$\exists w \in \mathbb{N} : y = v + a \cdot w \wedge V_q(w) \geq u$$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

- $P_q(x) \iff V_q(x) = x$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

- $P_q(x) \iff V_q(x) = x$
- $P_{q^d}(x) \iff P_q(x) \wedge q^d - 1$ divides $x - 1$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

- $P_q(x) \iff V_q(x) = x$
- $P_{q^d}(x) \iff P_q(x) \wedge q^d - 1$ divides $x - 1$

Express S_d and S_{-d} using P_{q^d}

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

- $P_q(x) \iff V_q(x) = x$
- $P_{q^d}(x) \iff P_q(x) \wedge q^d - 1$ divides $x - 1$

Express S_d and S_{-d} using P_{q^d}

- $x \, S_d \, y \iff y \geq x \wedge \bigvee_{i=0}^{d-1} P_{q^d}(q^i \cdot x) \wedge P_{q^d}(q^i \cdot y)$

Knapsack problem for BS$(1, q)$

For $d \in \mathbb{Z}$, $x, y \in \mathbb{N}$ let: $x \, S_d \, y \iff \exists r, s \in \mathbb{N} : \; x = q^r \wedge y = q^{d \cdot s} x$.

Step 3. For $d \in \mathbb{N}$ express S_d and S_{-d} using V_q:

For $m, x \in \mathbb{N}$ let $P_m(x) \iff x$ is a power of m.

- $P_q(x) \iff V_q(x) = x$
- $P_{q^d}(x) \iff P_q(x) \wedge q^d - 1$ divides $x - 1$

Express S_d and S_{-d} using P_{q^d}

- $x \, S_d \, y \iff y \geq x \wedge \bigvee_{i=0}^{d-1} P_{q^d}(q^i \cdot x) \wedge P_{q^d}(q^i \cdot y)$
- $x \, S_{-d} \, y \iff y \, S_d \, x$

Open Problems

Power word problem

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)
- The compressed word problem is the word problem for a given straight-line program (CFG that generates a single word).
  Best known upper bound for $\mathrm{BS}(1, q)$: coRP.

Open Problems

Power word problem

- BS$(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)
- The compressed word problem is the word problem for a given straight-line program (CFG that generates a single word).
  Best known upper bound for BS$(1, q)$: coRP.

Knapsack problem

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)
- The compressed word problem is the word problem for a given straight-line program (CFG that generates a single word).
  Best known upper bound for $\mathrm{BS}(1, q)$: coRP.

Knapsack problem

- The general case $\mathrm{BS}(p, q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$:

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)
- The compressed word problem is the word problem for a given straight-line program (CFG that generates a single word).
  Best known upper bound for $\mathrm{BS}(1, q)$: coRP.

Knapsack problem

- The general case $\mathrm{BS}(p, q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$:
  - Knapsack known decidable for $\gcd(p, q) = 1$ (Dudkin & Treyer 2018)
    But: the case $\gcd(p, q) > 1$ is still open.

Open Problems

Power word problem

- $\mathrm{BS}(1, q)$ is a f.g. solvable linear group.
  - Is power word problem in TC^0 for every f.g. solvable linear group?
  - The word problem is! (König & L 2018)
- The compressed word problem is the word problem for a given straight-line program (CFG that generates a single word).
  Best known upper bound for $\mathrm{BS}(1, q)$: coRP.

Knapsack problem

- The general case $\mathrm{BS}(p, q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$:
  - Knapsack known decidable for $\gcd(p, q) = 1$ (Dudkin & Treyer 2018)
    But: the case $\gcd(p, q) > 1$ is still open.
- Is knapsack decidable for $\mathrm{GL}(2, \mathbb{Q})$?