# Generic complexity of the identity problem over finite groups and monoids

Alexander Rybalov

Mathematical Center in Akademgorodok, Omsk

3 december 2020

# Identity problem for finite groups

Let $G$ be a finite group. $X = \{x_1, x_2, \ldots\}$, $X^{-1} = \{x_1^{-1}, x_2^{-1}, \ldots\}$, $X_n = \{x_1, \ldots, x_n\}$ and $X_n^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$.

# Identity problem for finite groups

Let $G$ be a finite group. $X = \{x_1, x_2, \ldots\}$, $X^{-1} = \{x_1^{-1}, x_2^{-1}, \ldots\}$, $X_n = \{x_1, \ldots, x_n\}$ and $X_n^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$.

**Definition**

A **term** over group $G$ is a finite word $t$ over alphabet $\{X_n \cup X_n^{-1}\}$, where $n = |t|$.

# Identity problem for finite groups

Let $G$ be a finite group. $X = \{x_1, x_2, \ldots\}$, $X^{-1} = \{x_1^{-1}, x_2^{-1}, \ldots\}$, $X_n = \{x_1, \ldots, x_n\}$ and $X_n^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$.

**Definition**

A **term** over group $G$ is a finite word $t$ over alphabet $\{X_n \cup X_n^{-1}\}$, where $n = |t|$.

**Definition**

A term $t$ of size $n$ is **identity** over group $G$ if for all $(a_1, \ldots, a_n) \in G^n$ it holds $t(a_1, \ldots, a_n) = 1$.

# Identity problem for finite groups

Let $G$ be a finite group. $X = \{x_1, x_2, \ldots\}$, $X^{-1} = \{x_1^{-1}, x_2^{-1}, \ldots\}$, $X_n = \{x_1, \ldots, x_n\}$ and $X_n^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$.

**Definition**

A **term** over group $G$ is a finite word $t$ over alphabet $\{X_n \cup X_n^{-1}\}$, where $n = |t|$.

**Definition**

A term $t$ of size $n$ is **identity** over group $G$ if for all $(a_1, \ldots, a_n) \in G^n$ it holds $t(a_1, \ldots, a_n) = 1$.

**Definition**

**The identity problem over group** $G$ is the following:

- Given a term $t$.
- Is $t = 1$ an identity over $G$?

# Identity problem for finite semigroups

Let $S$ be a finite semigroup. Let $X = \{x_1, x_2, \ldots\}$ be a countable alphabet of variables. Denote $X_n = \{x_1, \ldots, x_n\}$.

# Identity problem for finite semigroups

Let $S$ be a finite semigroup. Let $X = \{x_1, x_2, \ldots\}$ be a countable alphabet of variables. Denote $X_n = \{x_1, \ldots, x_n\}$.

**Definition**

A **term** over semigroup $S$ is a finite word $t$ over alphabet $X_n$, where $n = |t|$.

# Identity problem for finite semigroups

Let $S$ be a finite semigroup. Let $X = \{x_1, x_2, \ldots\}$ be a countable alphabet of variables. Denote $X_n = \{x_1, \ldots, x_n\}$.

**Definition**

A **term** over semigroup $S$ is a finite word $t$ over alphabet $X_n$, where $n = |t|$.

**Definition**

A pair of terms $p, q$ of size $n = |p| + |q|$ is **identity** over semigroup $S$ if for all $(a_1, \ldots, a_n) \in S^n$ it holds $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$.

# Identity problem for finite semigroups

Let $S$ be a finite semigroup. Let $X = \{x_1, x_2, \ldots\}$ be a countable alphabet of variables. Denote $X_n = \{x_1, \ldots, x_n\}$.

**Definition**

A **term** over semigroup $S$ is a finite word $t$ over alphabet $X_n$, where $n = |t|$.

**Definition**

A pair of terms $p, q$ of size $n = |p| + |q|$ is **identity** over semigroup $S$ if for all $(a_1, \ldots, a_n) \in S^n$ it holds $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$.

**Definition**

**The identity problem over semigroup** $S$ is the following:

- Given a pair of terms $p, q$.
- Is $p = q$ an identity over $S$?

# Examples of identities

1. $G$ – finite group of order $n$.

# Examples of identities

1. $G$ – finite group of order $n$. **Identity**: $x^n = 1$.

# Examples of identities

1. $G$ – finite group of order $n$. **Identity**: $x^n = 1$.
2. $G$ – finite abelian group.

# Examples of identities

1. $G$ – finite group of order $n$. **Identity**: $x^n = 1$.
2. $G$ – finite abelian group. **Identity**: $[x, y] = xyx^{-1}y^{-1} = 1$.

# Examples of identities

1. $G$ – finite group of order $n$. **Identity**: $x^n = 1$.
2. $G$ – finite abelian group. **Identity**: $[x, y] = xyx^{-1}y^{-1} = 1$.
3. Brandt semigroup

$$B_2 = \langle a, b \mid a^2 = b^2 = 0, aba = a, bab = b \rangle.$$

# Examples of identities

1. $G$ – finite group of order $n$. **Identity**: $x^n = 1$.
2. $G$ – finite abelian group. **Identity**: $[x, y] = xyx^{-1}y^{-1} = 1$.
3. Brandt semigroup

$$B_2 = \langle a, b \mid a^2 = b^2 = 0, aba = a, bab = b \rangle.$$

**Identity**: $xyx = xyxyx$.

# Finite basis problem

**Finite basis problem (Lyndon, Higman, 1960s)**

Let $G$ be a finite group (semigroup). Can all identities over $G$ be deduced from a finite set (basis) of identities?

# Finite basis problem

**Finite basis problem (Lyndon, Higman, 1960s)**

Let $G$ be a finite group (semigroup). Can all identities over $G$ be deduced from a finite set (basis) of identities?

**Oates, Powell (1964)**: For every finite group there is a finite basis of identities.

# Finite basis problem

**Finite basis problem (Lyndon, Higman, 1960s)**

Let $G$ be a finite group (semigroup). Can all identities over $G$ be deduced from a finite set (basis) of identities?

**Oates, Powell (1964)**: For every finite group there is a finite basis of identities.

**Perkins (1968)**: For the Brandt monoid $B_2^1$ there is no finite basis of identities!

# Finite basis problem

**Finite basis problem (Lyndon, Higman, 1960s)**

Let $G$ be a finite group (semigroup). Can all identities over $G$ be deduced from a finite set (basis) of identities?

**Oates, Powell (1964)**: For every finite group there is a finite basis of identities.

**Perkins (1968)**: For the Brandt monoid $B_2^1$ there is no finite basis of identities!

**Trahtman (1981)**: For Brandt semigroup $B_2$ the finite basis is

$$x^2 = x^3, xyx = xyxyx, x^2y^2 = y^2x^2.$$

# Finite basis problem

**Finite basis problem (Lyndon, Higman, 1960s)**

Let $G$ be a finite group (semigroup). Can all identities over $G$ be deduced from a finite set (basis) of identities?

**Oates, Powell (1964)**: For every finite group there is a finite basis of identities.

**Perkins (1968)**: For the Brandt monoid $B_2^1$ there is no finite basis of identities!

**Trahtman (1981)**: For Brandt semigroup $B_2$ the finite basis is

$$x^2 = x^3, xyx = xyxyx, x^2y^2 = y^2x^2.$$

**Volkov (1985)** found finite bases for more general classes of Brandt semigroups.

# Complexity of the problem

Let $S$ be a fixed finite group (semigroup).

# Complexity of the problem

Let $S$ be a fixed finite group (semigroup).
It is easy to see, that the identity problem over $S$ is in the co-NP class (class of complements of problems from NP).

# Complexity of the problem

Let $S$ be a fixed finite group (semigroup).
It is easy to see, that the identity problem over $S$ is in the co-NP class (class of complements of problems from NP).
Dichotomy: it can be decidable in polynomial time, or hard (co-NP-complete).

# Complexity of the problem

Let $S$ be a fixed finite group (semigroup).
It is easy to see, that the identity problem over $S$ is in the co-NP class (class of complements of problems from NP).
Dichotomy: it can be decidable in polynomial time, or hard (co-NP-complete).

**Sapir (1994)**

Let $S$ be a fixed finite group (semigroup). What is the computational complexity of the identity problem over $S$?

# Feasible problems

In class P:

- Nilpotent groups (Burris and Lawrence, Horvath and Szabo).

# Feasible problems

In class P:

- Nilpotent groups (Burris and Lawrence, Horvath and Szabo).
- Commutative semigroups (Kisielewicz).

# Feasible problems

In class P:

- Nilpotent groups (Burris and Lawrence, Horvath and Szabo).
- Commutative semigroups (Kisielewicz).
- Aperiodic finite 0-simple semigroups (Seif and Szabo). Including $B_n$.

# Feasible problems

In class P:

- Nilpotent groups (Burris and Lawrence, Horvath and Szabo).
- Commutative semigroups (Kisielewicz).
- Aperiodic finite 0-simple semigroups (Seif and Szabo). Including $B_n$.
- Monoids with less than 6 elements (Klima).

# Hard problems

co-NP-complete:

- Non-solvable finite groups (Horvath, Lawrence, Merai, Szabo).

# Hard problems

co-NP-complete:

- Non-solvable finite groups (Horvath, Lawrence, Merai, Szabo).
- Some classes of matrix semigroups (Szabo and Vertesi).

# Hard problems

co-NP-complete:

- Non-solvable finite groups (Horvath, Lawrence, Merai, Szabo).
- Some classes of matrix semigroups (Szabo and Vertesi).
- 6-element Brand monoid $B_2^1$ (Klima, Seif).

# Hard problems

co-NP-complete:

- Non-solvable finite groups (Horvath, Lawrence, Merai, Szabo).
- Some classes of matrix semigroups (Szabo and Vertesi).
- 6-element Brand monoid $B_2^1$ (Klima, Seif).
- Finite semigroups with non-solvable subgroups (Almeida, Volkov, Goldberg).

# Hard problems

co-NP-complete:

- Non-solvable finite groups (Horvath, Lawrence, Merai, Szabo).
- Some classes of matrix semigroups (Szabo and Vertesi).
- 6-element Brand monoid $B_2^1$ (Klima, Seif).
- Finite semigroups with non-solvable subgroups (Almeida, Volkov, Goldberg).
- Some 0-simple semigroups (Plescheva, Vertesi).

# Generic-case approach

Kapovich, Myasnikov, Schupp and Shpilrain in 2003 developed generic approach to algorithmic problems, which considers an algorithmic problem on "most"of the inputs (i.e., on a generic set) instead of the entire domain and ignores it on the rest of inputs (a negligible set). It turned out, that many famous undecidable problems are easily decidable on most inputs.

# Generic sets

Let $I$ be the set of all inputs and $I_n$ be the set of all inputs of size $n$ (sphere of radius $n$). For a subset $S \subseteq I$ define the following sequence

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|}, \ n = 1, 2, 3, \ldots$$

**The asymptotic density** of set $S$ is the following limit (if it exists)

$$\rho(S) = \lim_{n \to \infty} \rho_n(S).$$

$S$ is called **generic** if $\rho(S) = 1$ and **negligible** if $\rho(S) = 0$.

# Generic sets

Let $I$ be the set of all inputs and $I_n$ be the set of all inputs of size $n$ (sphere of radius $n$). For a subset $S \subseteq I$ define the following sequence

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|}, \ n = 1, 2, 3, \ldots$$

**The asymptotic density** of set $S$ is the following limit (if it exists)

$$\rho(S) = \lim_{n \to \infty} \rho_n(S).$$

$S$ is called **generic** if $\rho(S) = 1$ and **negligible** if $\rho(S) = 0$.
We will deal with words and pairs of words over a finite alphabets. Let $A$ be a finite alphabet. Denote by $A^*$ the set of all finite words in alphabet $A$. For every word $w \in A^*$ we will denote by $|w|$ the length of word $w$. The size of pair $(w_1, w_2) \in A^* \times A^*$ is $|w_1| + |w_2|$.

# Generic algorithms

Algorithm $\mathcal{A} : I \to I \cup \{?\}$ is called **generic** if

1. $\mathcal{A}$ halts on all inputs from $I$,
2. set $\{x \in I : \mathcal{A}(x) = ?\}$ is negligible.

# Generic algorithm for groups

**Theorem**

Let $G$ be a finite group. Then the identity problem over $G$ is generically decidable in polynomial time.

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.

Suppose $|G| > 1$. Then we can find an element $a$ of group $G$ of order $N > 1$.

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.
Suppose $|G| > 1$. Then we can find an element $a$ of group $G$ of order $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $t \in \{X \cup X^{-1}\}^*$ in the following way.

1. Compute $d_i(t)$, $i = 1, \ldots, |t|$.

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.
Suppose $|G| > 1$. Then we can find an element $a$ of group $G$ of order $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $t \in \{X \cup X^{-1}\}^*$ in the following way.

1. Compute $d_i(t)$, $i = 1, \ldots, |t|$.
2. Check is $d_i(t)$ divided by $N$ for all $i = 1, \ldots, |t|$.

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.
Suppose $|G| > 1$. Then we can find an element $a$ of group $G$ of order $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $t \in \{X \cup X^{-1}\}^*$ in the following way.

1. Compute $d_i(t)$, $i = 1, \ldots, |t|$.
2. Check is $d_i(t)$ divided by $N$ for all $i = 1, \ldots, |t|$.
3. If YES, then output the answer "?".

# Generic algorithm for groups

One can define for every term $t \in \{X \cup X^{-1}\}^*$ and for every $i = 1, \ldots, n$, where $n = |t|$, $d_i(t)$ as sum of powers of letter $x_i$ in word $t$.
Suppose $|G| > 1$. Then we can find an element $a$ of group $G$ of order $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $t \in \{X \cup X^{-1}\}^*$ in the following way.

1. Compute $d_i(t)$, $i = 1, \ldots, |t|$.
2. Check is $d_i(t)$ divided by $N$ for all $i = 1, \ldots, |t|$.
3. If YES, then output the answer "?".
4. If NO, then output the answer "NO".

# Generic algorithm for monoids

**Theorem**

Let $S$ be a finite monoid such that there is an element $a \in S$ of period greater than 1. Here period of $a$ is a minimal natural $m$ such that $a^k = a^{k+m}$ for some $k$. Then the identity problem over $S$ is generically decidable in polynomial time.

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.
Let $a \in S$ be an element of period $N > 1$.

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.
Let $a \in S$ be an element of period $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $(p, q) \in X^*$ in the following way.

1. Compute $d_i(p, q)$, $i = 1, \ldots, |p| + |q|$.

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.
Let $a \in S$ be an element of period $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $(p, q) \in X^*$ in the following way.

1. Compute $d_i(p, q)$, $i = 1, \ldots, |p| + |q|$.
2. Check is $d_i(p, q)$ divided by $N$ for all $i = 1, \ldots, |p| + |q|$.

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.
Let $a \in S$ be an element of period $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $(p, q) \in X^*$ in the following way.

1. Compute $d_i(p, q)$, $i = 1, \ldots, |p| + |q|$.
2. Check is $d_i(p, q)$ divided by $N$ for all $i = 1, \ldots, |p| + |q|$.
3. If YES, then output the answer "?".

# Generic algorithm for monoids

One can define for every pair of terms $p, q \in X^*$ and for every $i = 1, \ldots, n$, where $n = |p| + |q|$, $d_i(p, q)$ as the number of letter $x_i$ in word $p$ minus the number of letter $x_i$ in word $q$.
Let $a \in S$ be an element of period $N > 1$.

## Algorithm

Algorithm $\mathcal{A}$ works on an input $(p, q) \in X^*$ in the following way.

1. Compute $d_i(p, q)$, $i = 1, \ldots, |p| + |q|$.
2. Check is $d_i(p, q)$ divided by $N$ for all $i = 1, \ldots, |p| + |q|$.
3. If YES, then output the answer "?".
4. If NO, then output the answer "NO".

# Gromyko type algorithms

Andrei Andreyevich Gromyko – Soviet Minister of Foreign Affairs, known as «Mister No».

# Brandt semigroups

Let $G$ be a group, $I$ a set with at least 2 elements, and $0 \notin G \cup I$. Define a multiplication operation on the set $B(G, I) = I \times G \times I \cup \{0\}$ as follows:

$$(i, g, j)(k, h, l) = \begin{cases} (i, gh, l), & \text{if } j = k, \\ 0, & \text{otherwise,} \end{cases}$$

for all $i, j, k, l \in I$ and all $g, h \in G$. Also $0x = 0$ and $x0 = 0$ for all $x \in B(G, I)$. The set $B(G, I)$ with defined multiplication is called the **Brandt semigroup over the group** $G$ with **index set** $I$.

# Brandt semigroups

Let $G$ be a group, $I$ a set with at least 2 elements, and $0 \notin G \cup I$. Define a multiplication operation on the set $B(G, I) = I \times G \times I \cup \{0\}$ as follows:

$$(i, g, j)(k, h, l) = \begin{cases} (i, gh, l), & \text{if } j = k, \\ 0, & \text{otherwise,} \end{cases}$$

for all $i, j, k, l \in I$ and all $g, h \in G$. Also $0x = 0$ and $x0 = 0$ for all $x \in B(G, I)$. The set $B(G, I)$ with defined multiplication is called the **Brandt semigroup over the group** $G$ with **index set** $I$.
We are interested in finite Brandt semigroup $B_n = B(E, \{1, \ldots, n\})$ over the trivial one-element group $E$, which elements are just pairs $(i, j)$ of natural numbers.

# Brandt semigroups

Let $G$ be a group, $I$ a set with at least 2 elements, and $0 \notin G \cup I$. Define a multiplication operation on the set $B(G, I) = I \times G \times I \cup \{0\}$ as follows:

$$(i, g, j)(k, h, l) = \begin{cases} (i, gh, l), & \text{if } j = k, \\ 0, & \text{otherwise,} \end{cases}$$

for all $i, j, k, l \in I$ and all $g, h \in G$. Also $0x = 0$ and $x0 = 0$ for all $x \in B(G, I)$. The set $B(G, I)$ with defined multiplication is called the **Brandt semigroup over the group** $G$ with **index set** $I$.
We are interested in finite Brandt semigroup $B_n = B(E, \{1, \ldots, n\})$ over the trivial one-element group $E$, which elements are just pairs $(i, j)$ of natural numbers.
Monoid $B_n^1$ is semigroup $B_n$ with jointed unit 1.

# Identity problem over Brandts monoids

Klima and Seif: The identity problem over $B_n^1$, $n \geq 2$, is co-NP-complete.

# Identity problem over Brandts monoids

Klima and Seif: The identity problem over $B_n^1$, $n \geq 2$, is co-NP-complete.

Our generic algorithm does not work for $B_n^1$! Because for every $a \in B_n^1$ either $a^2 = a$ or $a^2 = 0$.

# Identity problem over Brandts monoids

Klima and Seif: The identity problem over $B_n^1$, $n \geq 2$, is co-NP-complete.
Our generic algorithm does not work for $B_n^1$! Because for every $a \in B_n^1$ either $a^2 = a$ or $a^2 = 0$.

**Theorem**

The problem of identity checking over the Brandt monoid $B_n^1$ is decidable generically in polynomial time.

# Identity problem over Brandts monoids

Klima and Seif: The identity problem over $B_n^1$, $n \geq 2$, is co-NP-complete.
Our generic algorithm does not work for $B_n^1$! Because for every $a \in B_n^1$ either $a^2 = a$ or $a^2 = 0$.

**Theorem**

The problem of identity checking over the Brandt monoid $B_n^1$ is decidable generically in polynomial time.

**Theorem**

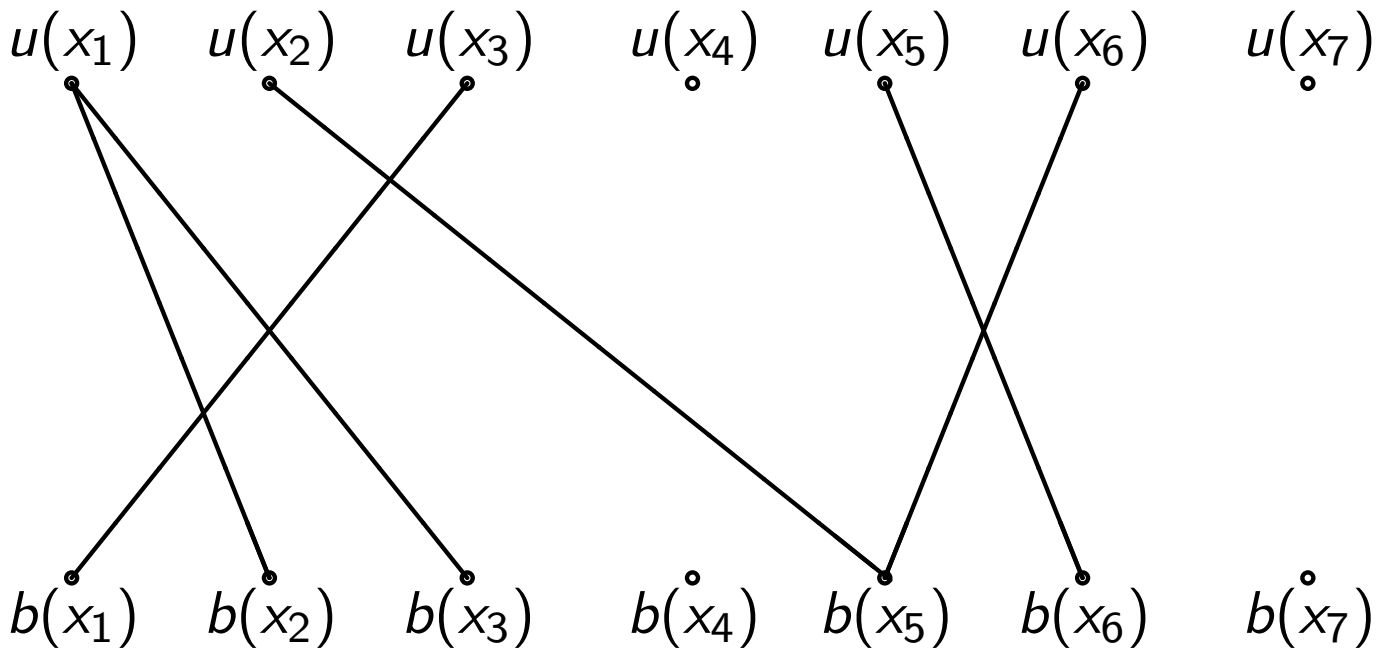
The problem of identity checking over Plescheva-Vertesi semigroup is decidable generically in polynomial time.

# Graphs

For a term $t(x_1, \ldots, x_n)$ define the following bipartite graph $B(t)$. It has $n$ upper vertices $u(x_1), \ldots, u(x_n)$ and $n$ bottom vertices $b(x_1), \ldots, b(x_n)$. Each variable $x_i$ corresponds to two vertices $u(x_i)$ and $b(x_i)$. Vertices $u(x_i)$ and $b(x_j)$ are connected by an edge in $B(t)$ if and only if there is a subword $x_i x_j$ in the term $t$.

# Example of graph

For example the following picture is the graph $B(t)$ of term $t = x_1x_3x_1x_2x_5x_6x_5$.



# Connected components

Denote by

$$C(B(t)) = \{C_1, C_2, \ldots, C_k\}$$

the set of all connected components (given by sets of vertices) of the graph $B(t)$.

# The identity problem over $B_n$

Seif and Szabo proved that $t_1 = t_2$ is identity over Brandt semigroup $B_n$ if and only if

1. $C(B(t_1)) = C(B(t_2))$,
2. connected component of $B(t_1)$, containing $u(x_i)$, where $x_i$ is the first letter of $t_1$, is the same as connected component of $B(t_2)$, containing $u(x_j)$, where $x_j$ is the first letter of $t_2$,
3. connected component of $B(t_1)$, containing $b(x_k)$, where $x_k$ is the last letter of $t_1$, is the same as connected component of $B(t_2)$, containing $b(x_l)$, where $x_l$ is the last letter of $t_2$.

# The identity problem over $B_n$

Seif and Szabo proved that $t_1 = t_2$ is identity over Brandt semigroup $B_n$ if and only if

1. $C(B(t_1)) = C(B(t_2))$,
2. connected component of $B(t_1)$, containing $u(x_i)$, where $x_i$ is the first letter of $t_1$, is the same as connected component of $B(t_2)$, containing $u(x_j)$, where $x_j$ is the first letter of $t_2$,
3. connected component of $B(t_1)$, containing $b(x_k)$, where $x_k$ is the last letter of $t_1$, is the same as connected component of $B(t_2)$, containing $b(x_l)$, where $x_l$ is the last letter of $t_2$.

Note that sets $C(B(t_1))$ and $C(B(t_2))$ can be constructed in polynomial time, therefore the problem of identity checking in Brandt semigroup $B_n$ is polynomial time decidable. But, as proved by Klima and Seif, the problem of identity checking over Brandt monoid $B_n^1$, $n \geq 2$, is co-NP-complete. Thus there is no effective polynomial algorithm for the problem of identity checking over Brandt monoid $B_n^1$, $n \geq 2$, provided P $\neq$ NP.

# Scetch of the proof

**Lemma**

The set

$$\mathcal{EPT} = \{(t_1, t_2) \in \mathcal{PT} \ : \ C(B(t_1)) = C(B(t_2))\}.$$

is negligible.

# Scetch of the proof

**Lemma**

The set

$$\mathcal{EPT} = \{(t_1, t_2) \in \mathcal{PT} \ : \ C(B(t_1)) = C(B(t_2))\}.$$

is negligible.

1. Construct $B(t_1)$ and $B(t_2)$.
2. If $B(t_1) = B(t_2)$ then output "YES".
3. If $C(B(t_1)) \neq C(B(t_2))$ then output "NO".
4. If $C(B(t_1)) = C(B(t_2))$ then output "?".

# The end

Thank you!