

The Equivalence Problem for Finite Structures

Vera Vértési

University Eötvös Loránd

2007

Beginning

Syracuse, early 90's

Beginning

Syracuse, early 90's

- synchronizing chemical experiments

Beginning

Syracuse, early 90's

- synchronizing chemical experiments
- decide whether two experiments will give the same result or not

Beginning

Syracuse, early 90's

- synchronizing chemical experiments
- decide whether two experiments will give the same result or not

Syracuse, meantime

The Computer Scientist showed that this problem traces back to equivalences of terms over commutative rings.

Beginning

Finite Automata, Formal Languages,
Montreal, Brno, Ekaterinburg

Finite Automata, Formal Languages,
Montreal, Brno, Ekaterinburg

- Syntactic Monoids

Finite Automata, Formal Languages, Montreal, Brno, Ekaterinburg

- Syntactic Monoids
- recognition of formal languages

Finite Automata, Formal Languages, Montreal, Brno, Ekaterinburg

- Syntactic Monoids
- recognition of formal languages

It was shown that this problem traces back to equivalences of terms over monoids.

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

- $x^p \overset{?}{\equiv} x$ in $\mathbb{Z}_p$

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

- $x^p \overset{?}{\equiv} x$ in $\mathbb{Z}_p$
- Yes, Fermat's theorem

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

- $x^p \overset{?}{\equiv} x$ in $\mathbb{Z}_p$
- Yes, Fermat's theorem

Example

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

- $x^p \stackrel{?}{\equiv} x$ in $\mathbb{Z}_p$
- Yes, Fermat's theorem

Example

- $AB \stackrel{?}{\equiv} BA$ over $M_n(\mathbb{F})$

Some Definitions and Examples

Definition

Let $\mathbf{A}$ be an algebra and let t and s be two terms over $\mathbf{A}$.

- We say that t and s are equivalent over $\mathbf{A}$ if $t(\bar{a}) = s(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Example

- $x^p \stackrel{?}{\equiv} x$ in $\mathbb{Z}_p$
- Yes, Fermat's theorem

Example

- $AB \stackrel{?}{\equiv} BA$ over $M_n(\mathbb{F})$
- No, $M_n(\mathbb{F})$ is not commutative

Some Definitions and Examples

Example

Some Definitions and Examples

Example

- $[(AB - BA)^2, C] \stackrel{?}{=} 0$ over $M_2(\mathbb{F})$

Some Definitions and Examples

Example

- $[(AB - BA)^2, C] \stackrel{?}{=} 0$ over $M_2(\mathbb{F})$
- Yes, $\text{tr}(AB - BA) = 0 \Rightarrow (AB - BA)^2$ is scalar matrix, hence commutes with C .

Some Definitions and Examples

Example

- $[(AB - BA)^2, C] \stackrel{?}{=} 0$ over $M_2(\mathbb{F})$
- Yes, $\text{tr}(AB - BA) = 0 \Rightarrow (AB - BA)^2$ is scalar matrix, hence commutes with C .

Example

Some Definitions and Examples

Example

- $[(AB - BA)^2, C] \stackrel{?}{\equiv} 0$ over $M_2(\mathbb{F})$
- Yes, $\text{tr}(AB - BA) = 0 \Rightarrow (AB - BA)^2$ is scalar matrix, hence commutes with C .

Example

- $[[x, y], [x, z]]^2 \stackrel{?}{\equiv} 1$ over S_4

Some Definitions and Examples

Example

- $[(AB - BA)^2, C] \stackrel{?}{=} 0$ over $M_2(\mathbb{F})$
- Yes, $\text{tr}(AB - BA) = 0 \Rightarrow (AB - BA)^2$ is scalar matrix, hence commutes with C .

Example

- $[[x, y], [x, z]]^2 \stackrel{?}{=} 1$ over S_4
- Yes, $[x, y] \in A_4 \implies [[x, y], [x, z]] \in A'_4$
 $A'_4 \simeq Z_2 \times Z_2$

The Equivalence Problem

Definition

TERM-EQ(**A**)

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

- What is the complexity of TERM-EQ?

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

- What is the complexity of TERM-EQ?
- Always in coNP.

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

- What is the complexity of TERM-EQ?
- Always in coNP.
- What is the complexity of the problem for certain class of structures?

The Equivalence Problem

Definition

TERM-EQ(**A**)

- Let **A** be an algebra
- Input: t and s two terms over **A**
- Question: are t and s equivalent over **A**

Always decidable: check every substitution

- What is the complexity of TERM-EQ?
- Always in coNP.
- What is the complexity of the problem for certain class of structures?
- Goal: Prove dichotomy: TERM-EQ is either in P or coNP-complete

Theorem

Goldmann, Russel (1999)

For nilpotent groups TERM-EQ is in P.

Results – Groups

Theorem

Goldmann, Russel (1999)

For nilpotent groups TERM-EQ is in P.

Theorem

Horváth, Mérai, Lawrence, Szabó (2005)

TERM-EQ is coNP-complete for non-solvable groups.

Results – Groups

Theorem

Goldmann, Russel (1999)

For nilpotent groups TERM-EQ is in P.

Theorem

Horváth, Mérai, Lawrence, Szabó (2005)

TERM-EQ is coNP-complete for non-solvable groups.

Theorem

Horváth, Szabó (2003)

TERM-EQ is in P for metacyclic groups (semidirect product of cyclic groups).

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- *Volkov, Popov (2002)* #elements $\approx 2^{1700}$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$
$$(= P_0P_2P_1 \quad) = P_0P_3P_1$$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \ 0 \leq j \leq 14 \quad \begin{array}{ll} (= P_0P_2P_1 &) = P_0P_3P_1 \\ \neg = P_0P_4P_1 & \vee = P_0P_5P_1 \quad \wedge = P_0P_6P_1 \end{array}$$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$

$(= P_0P_2P_1$	$) = P_0P_3P_1$		
$\neg = P_0P_4P_1$	$\vee = P_0P_5P_1$	$\wedge = P_0P_6P_1$	
$1 = P_0P_{10}P_1$	$0 = P_0P_{11}P_1$		

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$

$(= P_0P_2P_1$	$) = P_0P_3P_1$		
$\neg = P_0P_4P_1$	$\vee = P_0P_5P_1$	$\wedge = P_0P_6P_1$	
$1 = P_0P_{10}P_1$	$0 = P_0P_{11}P_1$		

Expressions

$(0), (1), (\neg 0), (\neg 1)$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$

$(= P_0P_2P_1$	$) = P_0P_3P_1$		
$\neg = P_0P_4P_1$	$\vee = P_0P_5P_1$	$\wedge = P_0P_6P_1$	
$1 = P_0P_{10}P_1$	$0 = P_0P_{11}P_1$		

Expressions

$(0), (1), (\neg 0), (\neg 1)$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$
$$\begin{array}{llll} (= P_0P_2P_1 &) = P_0P_3P_1 \\ \neg = P_0P_4P_1 & \vee = P_0P_5P_1 & \wedge = P_0P_6P_1 \\ 1 = P_0P_{10}P_1 & 0 = P_0P_{11}P_1 \end{array}$$

Expressions

$(0), (1), (\neg 0), (\neg 1)$

$(V_1 \wedge V_2 \wedge \cdots \wedge V_k)$, where $V_i \in \{0, 1, \neg 0, \neg 1\}$

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$
$$\begin{array}{llll} (= P_0P_2P_1 &) = P_0P_3P_1 \\ \neg = P_0P_4P_1 & \vee = P_0P_5P_1 & \wedge = P_0P_6P_1 \\ 1 = P_0P_{10}P_1 & 0 = P_0P_{11}P_1 \end{array}$$

Expressions

$(0), (1), (\neg 0), (\neg 1)$

$(V_1 \wedge V_2 \wedge \cdots \wedge V_k)$, where $V_i \in \{0, 1, \neg 0, \neg 1\}$

$W_1 \vee W_2 \vee \cdots \vee W_l$, where W_j is defined by the previous forms

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$

$(= P_0P_2P_1$	$) = P_0P_3P_1$		
$\neg = P_0P_4P_1$	$\vee = P_0P_5P_1$	$\wedge = P_0P_6P_1$	
$1 = P_0P_{10}P_1$	$0 = P_0P_{11}P_1$		

Expressions

$(0), (1), (\neg 0), (\neg 1)$

$(V_1 \wedge V_2 \wedge \cdots \wedge V_k)$, where $V_i \in \{0, 1, \neg 0, \neg 1\}$

$W_1 \vee W_2 \vee \cdots \vee W_l$, where W_j is defined by the previous forms

Relations

$U = W$, whenever U, W is not an expression

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$
$$\begin{array}{ll} (= P_0P_2P_1 &) = P_0P_3P_1 \\ \neg = P_0P_4P_1 & \vee = P_0P_5P_1 \quad \wedge = P_0P_6P_1 \\ 1 = P_0P_{10}P_1 & 0 = P_0P_{11}P_1 \end{array}$$

Expressions

$(0), (1), (\neg 0), (\neg 1)$

$(V_1 \wedge V_2 \wedge \cdots \wedge V_k)$, where $V_i \in \{0, 1, \neg 0, \neg 1\}$

$W_1 \vee W_2 \vee \cdots \vee W_l$, where W_j is defined by the previous forms

Relations

$U = W$, whenever U, W is not an expression

Volkov's Example

$\langle a, b \rangle$ — the free semigroup generated by two elements

$$P_j = ab^{15+j}a^2, \quad 0 \leq j \leq 14$$
$$\begin{array}{llll} (= P_0P_2P_1 &) = P_0P_3P_1 \\ \neg = P_0P_4P_1 & \vee = P_0P_5P_1 & \wedge = P_0P_6P_1 \\ 1 = P_0P_{10}P_1 & 0 = P_0P_{11}P_1 \end{array}$$

Expressions

$$(0), (1), (\neg 0), (\neg 1)$$

$$(V_1 \wedge V_2 \wedge \cdots \wedge V_k), \text{ where } V_i \in \{0, 1, \neg 0, \neg 1\}$$

$$W_1 \vee W_2 \vee \cdots \vee W_l, \text{ where } W_j \text{ is defined by the previous forms}$$

Relations

$U = W$, whenever U, W is not an expression

$$\begin{array}{llll} \neg 0 = 1 & \neg 1 = 0 & (0 \wedge 0 = (0 & (0 \wedge 1 = (0 \\ (1 \wedge 0 = (0 & (1 \wedge 1 = (1 & \wedge 0 \wedge 0 = \wedge 0 & \wedge 0 \wedge 1 = \wedge 0 \\ \wedge 1 \wedge 0 = \wedge 0 & \wedge 1 \wedge 1 = \wedge 1 & (0) \vee (0) = (0) & (0) \vee (1) = (1) \\ (1) \vee (0) = (1) & (1) \vee (1) = (1) & & \end{array}$$

Volkov's Example

Need to be checked

Volkov's Example

Need to be checked

- does not collapse

Volkov's Example

Need to be checked

- does not collapse
- finite

Volkov's Example

Need to be checked

- does not collapse
- finite
- size $\approx 2^{1700}$

Volkov's Example

Need to be checked

- does not collapse
- finite
- size $\approx 2^{1700}$

SAT can be formulated

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- *Volkov, Popov (2002)* #elements $\approx 2^{1700}$

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- Volkov, Popov (2002) #elements $\approx 2^{1700}$
- Kisielewicz (2002) few thousand

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- Volkov, Popov (2002) #elements $\approx 2^{1700}$
- Kisielewicz (2002) few thousand
- Szabó, VV (2002) 13

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- Volkov, Popov (2002) #elements $\approx 2^{1700}$
- Kisielewicz (2002) few thousand
- Szabó, VV (2002) 13
- Klíma (2003) 6

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- Volkov, Popov (2002) #elements $\approx 2^{1700}$
- Kisielewicz (2002) few thousand
- Szabó, VV (2002) 13
- Klíma (2003) 6
- for every at most 5 element monoid the problem is in P

Results – Semigroups

Theorem

Seif, Szabó (2001)

TERM-EQ is P for combinatorial 0-simple semigroups.

Is there any semigroup with coNP-complete TERM-EQ?

- Volkov, Popov (2002) #elements $\approx 2^{1700}$
- Kisielewicz (2002) few thousand
- Szabó, VV (2002) 13
- Klíma (2003) 6
- for every at most 5 element monoid the problem is in P
- for almost every at most 6 element monoid the problem is in P

Combinatorial 0-simple semigroups



Combinatorial 0-simple semigroups

- M – a 0–1 matrix.

Combinatorial 0-simple semigroups

- M – a 0–1 matrix.
- Λ – the index set of rows

Combinatorial 0-simple semigroups

- $\mathbf{M}$ – a 0–1 matrix.
- Λ – the index set of rows
- I – the index set of columns

Combinatorial 0-simple semigroups

- $\mathbf{M}$ – a 0–1 matrix.
- Λ – the index set of rows
- I – the index set of columns

Underlying set

$$S_{\mathbf{M}} := \{\langle i, \lambda \rangle : i \in I, \lambda \in \Lambda\} \cup \{0\}$$

Combinatorial 0-simple semigroups

- $\mathbf{M}$ – a 0–1 matrix.
- Λ – the index set of rows
- I – the index set of columns

Underlying set

$$S_{\mathbf{M}} := \{\langle i, \lambda \rangle : i \in I, \lambda \in \Lambda\} \cup \{0\}$$

Multiplication:

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } \mathbf{M}(\lambda, j) = 1 \\ 0, & \text{if } \mathbf{M}(\lambda, j) = 0 \end{cases}$$

and

$$0 \cdot s = 0 = s \cdot 0 \quad \forall s \in S_{\mathbf{M}}$$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 2, 3 \rangle \langle 1, 2 \rangle =$$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 2, 3 \rangle \langle 1, 2 \rangle =$$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 2, 3 \rangle \langle 1, 2 \rangle =$$

$\underbrace{\hspace{1.5cm}}$

$$M(3, 1) = 1$$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 2, 3 \rangle \langle 1, 2 \rangle = \langle 2, 2 \rangle$$

$M(3, 1) = 1$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = 0 \iff \lambda = j$$

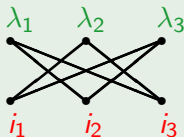
Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

where $\Lambda = I = \{1, 2, 3\}$



Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = 0 \iff \lambda = j$$

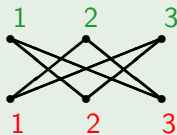
Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle, & \text{if } M(\lambda, j) = 1 \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

Example

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

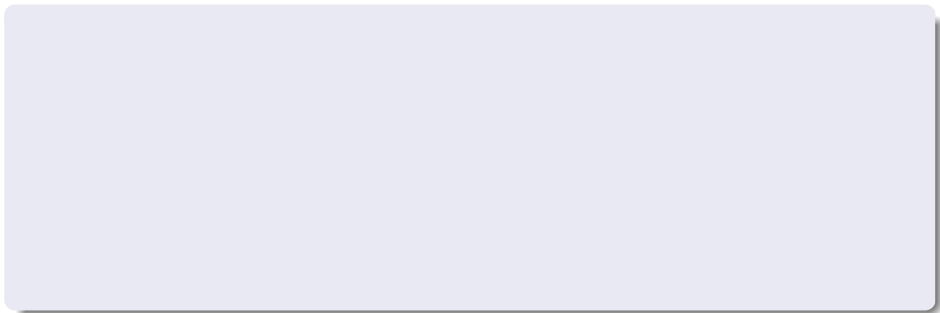
where $\Lambda = I = \{1, 2, 3\}$



Example

$$\langle i, \lambda \rangle \langle j, \mu \rangle = 0 \iff \lambda = j$$

Translating to Graphs



Translating to Graphs

- $t = x_1 \cdots x_n$ a term

Translating to Graphs

- $t = x_1 \cdots x_n$ a term
- $X := \{x_1, \dots, x_n\}$ the set of variables in t

Translating to Graphs

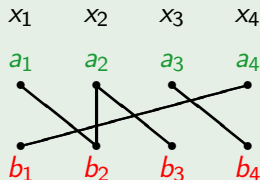
- $t = x_1 \cdots x_n$ a term
- $X := \{x_1, \dots, x_n\}$ the set of variables in t
- Define $G_t(A_t, B_t, E_t)$
where
 - $A_t = \{a_x \mid x \in X\}$
 - $B_t = \{b_x \mid x \in X\}$
 - $(a_x, b_y) \in E_t \iff xy$ is subword of t

Translating to Graphs

- $t = x_1 \cdots x_n$ a term
- $X := \{x_1, \dots, x_n\}$ the set of variables in t
- Define $G_t(A_t, B_t, E_t)$
where
- $A_t = \{a_x \mid x \in X\}$
- $B_t = \{b_x \mid x \in X\}$
- $(a_x, b_y) \in E_t \iff xy$ is subword of t

Example

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$



Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$a_1 \mapsto 2$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

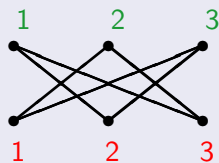
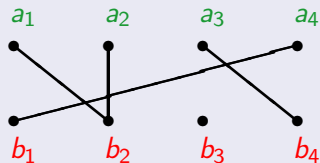
$$a_2 \mapsto 2$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

$$a_3 \mapsto 1$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

$$a_4 \mapsto 2$$



Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$a_1 \mapsto 2$$

$$b_1 \mapsto 1$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

$$a_2 \mapsto 2$$

$$b_2 \mapsto 3$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

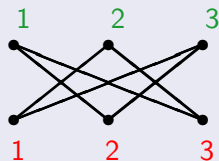
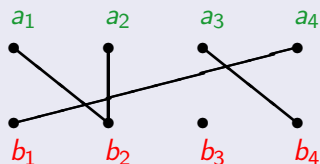
$$a_3 \mapsto 1$$

$$b_3 \mapsto 2$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

$$a_4 \mapsto 2$$

$$b_4 \mapsto 2$$



Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$a_1 \mapsto 2$$

$$b_1 \mapsto 1$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

$$a_2 \mapsto 2$$

$$b_2 \mapsto 3$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

$$a_3 \mapsto 1$$

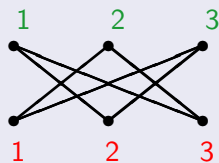
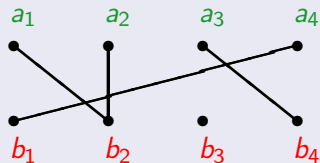
$$b_3 \mapsto 2$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

$$a_4 \mapsto 2$$

$$b_4 \mapsto 2$$

$$t(\vec{a}) = \langle 1, 2 \rangle \langle 3, 2 \rangle \langle 3, 2 \rangle \langle 2, 1 \rangle \langle 2, 2 \rangle \langle 1, 2 \rangle \langle 3, 2 \rangle = 0$$



Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$a_1 \mapsto 2$$

$$b_1 \mapsto 1$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

$$a_2 \mapsto 2$$

$$b_2 \mapsto 3$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

$$a_3 \mapsto 1$$

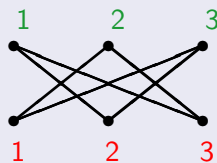
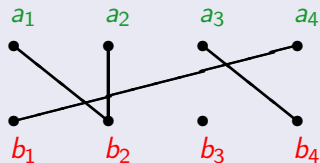
$$b_3 \mapsto 2$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

$$a_4 \mapsto 2$$

$$b_4 \mapsto 2$$

$$t(\vec{a}) = \langle 1, 2 \rangle \langle 3, 2 \rangle \underbrace{\langle 3, 2 \rangle \langle 2, 1 \rangle}_{A(2,2)=0} \langle 2, 2 \rangle \langle 1, 2 \rangle \langle 3, 2 \rangle = 0$$



Evaluating

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \mapsto \langle 1, 2 \rangle$$

$$a_1 \mapsto 2$$

$$b_1 \mapsto 1$$

$$x_2 \mapsto \langle 3, 2 \rangle$$

$$a_2 \mapsto 2$$

$$b_2 \mapsto 3$$

$$x_3 \mapsto \langle 2, 1 \rangle$$

$$a_3 \mapsto 1$$

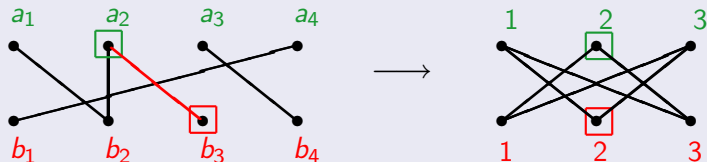
$$b_3 \mapsto 2$$

$$x_4 \mapsto \langle 2, 2 \rangle$$

$$a_4 \mapsto 2$$

$$b_4 \mapsto 2$$

$$t(\vec{a}) = \langle 1, 2 \rangle \langle 3, 2 \rangle \underbrace{\langle 3, 2 \rangle \langle 2, 1 \rangle}_{A(2,2)=0} \langle 2, 2 \rangle \langle 1, 2 \rangle \langle 3, 2 \rangle = 0$$



Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

$$A_t = \{a_x \mid x \in X\},$$

$$B_t = \{b_x \mid x \in X\} \text{ and}$$

$$(a_x, b_y) \in E_t \iff xy \text{ is subword of } t$$

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

$$A_t = \{a_x \mid x \in X\},$$

$$B_t = \{b_x \mid x \in X\} \text{ and}$$

$$(a_x, b_y) \in E_t \iff xy \text{ is subword of } t$$

$$\text{for an evaluation } X \rightarrow S_A \setminus \{0\}, \quad x_j \mapsto \langle i_j, \lambda_j \rangle$$

$$G_t \rightarrow \text{diagram} \quad a_x \mapsto \lambda, b_x \mapsto i \text{ if } x = \langle i, \lambda \rangle$$

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

$$A_t = \{a_x \mid x \in X\},$$

$$B_t = \{b_x \mid x \in X\} \text{ and}$$

$$(a_x, b_y) \in E_t \iff xy \text{ is subword of } t$$

$$\text{for an evaluation } X \rightarrow S_A \setminus \{0\}, \quad x_j \mapsto \langle i_j, \lambda_j \rangle$$

$$G_t \rightarrow \text{diagram} \quad a_x \mapsto \lambda, b_x \mapsto i \text{ if } x = \langle i, \lambda \rangle$$

Lemma

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$$

$$A_t = \{a_x \mid x \in X\},$$

$$B_t = \{b_x \mid x \in X\} \text{ and}$$

$$(a_x, b_y) \in E_t \iff xy \text{ is subword of } t$$

$$\text{for an evaluation } X \rightarrow S_A \setminus \{0\}, \quad x_j \mapsto \langle i_j, \lambda_j \rangle$$

$$G_t \rightarrow \text{diagram} \quad a_x \mapsto \lambda, b_x \mapsto i \text{ if } x = \langle i, \lambda \rangle$$

Lemma

$$\bullet \quad t(\vec{a}) \neq 0 \iff G_t \rightarrow \text{diagram} \text{ is a homomorphism;}$$

Evaluating Terms

$$t = x_1 \cdots x_n, X := \{x_1, \dots, x_n\} \rightsquigarrow G_t(\mathbf{A}_t, \mathbf{B}_t, E_t)$$

$$\mathbf{A}_t = \{a_x \mid x \in X\},$$

$$\mathbf{B}_t = \{b_x \mid x \in X\} \text{ and}$$

$$(a_x, b_y) \in E_t \iff xy \text{ is subword of } t$$

$$\text{for an evaluation } X \rightarrow S_A \setminus \{0\}, \quad x_j \mapsto \langle i_j, \lambda_j \rangle$$

$$G_t \rightarrow \text{diagram} \quad a_x \mapsto \lambda, b_x \mapsto i \text{ if } x = \langle i, \lambda \rangle$$

Lemma

- $t(\vec{a}) \neq 0 \iff G_t \rightarrow \text{diagram}$ is a homomorphism;
- If $\neq 0$, then $t(\vec{a}) = \langle i_1, \lambda_n \rangle$

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{diagram} \text{ is a homomorphism} \iff G_s \rightarrow \text{diagram} \text{ is a homomorphism;}$

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{Diagram}$ is a homomorphism $\iff G_s \rightarrow \text{Diagram}$ is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $i_{x_1} = i_{y_1}$ and $\lambda_{x_n} = \lambda_{y_m}$

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{diagram}$ is a homomorphism $\iff G_s \rightarrow \text{diagram}$ is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $i_{x_1} = i_{y_1}$ and $\lambda_{x_n} = \lambda_{y_m}$

Theorem

$t \equiv s$ if and only if:

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{diagram}$ is a homomorphism $\iff G_s \rightarrow \text{diagram}$ is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $i_{x_1} = i_{y_1}$ and $\lambda_{x_n} = \lambda_{y_m}$

Theorem

$t \equiv s$ if and only if:

- $G_t = G_s$; and

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{diagram}$ is a homomorphism $\iff G_s \rightarrow \text{diagram}$ is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $i_{x_1} = i_{y_1}$ and $\lambda_{x_n} = \lambda_{y_m}$

Theorem

$t \equiv s$ if and only if:

- $G_t = G_s$; and
- $x_1 = y_1$ and $x_n = y_m$

Identities of S_A

$$t = x_1 \cdots x_n \quad s = y_1 \cdots y_m, \quad X = \{x_1, \dots, x_n, y_1, \dots, y_m\}$$

Let us consider an evaluation $X \rightarrow S_A \setminus \{0\}$, then $t(\vec{a}) = s(\vec{a})$ iff:

- $G_t \rightarrow \text{Diagram}$ is a homomorphism $\iff G_s \rightarrow \text{Diagram}$ is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $i_{x_1} = i_{y_1}$ and $\lambda_{x_n} = \lambda_{y_m}$

Theorem

$t \equiv s$ if and only if:

- $G_t = G_s$; and
- $x_1 = y_1$ and $x_n = y_m$

Theorem

Seif, Szabó (2001) $TERM-EQ(S_A) \in P$

0-simple semigroups



0-simple semigroups

- G finite group

0-simple semigroups

- G finite group
- $M - G \cup \{0\}$ matrix.

0-simple semigroups

- G finite group
- $M - G \cup \{0\}$ matrix.
- Λ – the index set of rows

0-simple semigroups

- G finite group
- $M - G \cup \{0\}$ matrix.
- Λ – the index set of rows
- I – the index set of columns

0-simple semigroups

- G finite group
- $M - G \cup \{0\}$ matrix.
- Λ – the index set of rows
- I – the index set of columns

Underlying set

$$S_M := \{\langle i, g, \lambda \rangle : i \in I, g \in G, \lambda \in \Lambda\} \cup \{0\}$$

0-simple semigroups

- G finite group
- $M - G \cup \{0\}$ matrix.
- Λ – the index set of rows
- I – the index set of columns

Underlying set

$$S_M := \{\langle i, g, \lambda \rangle : i \in I, g \in G, \lambda \in \Lambda\} \cup \{0\}$$

Multiplication:

$$\langle i, g, \lambda \rangle \langle j, h, \mu \rangle = \begin{cases} \langle i, gM(\lambda, j)h, \mu \rangle, & \text{if } M(\lambda, j) \in G \\ 0, & \text{if } M(\lambda, j) = 0 \end{cases}$$

and

$$0 \cdot s = 0 = s \cdot 0 \quad \forall s \in S_M$$

Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle =$$

Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle = \langle \quad, \quad, \quad \rangle$$

Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle = \langle 1, \quad, \quad \rangle$$


Example

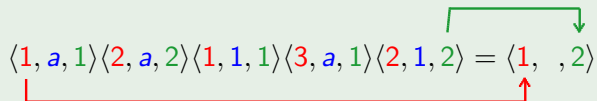
Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle = \langle 1, \quad, 2 \rangle$$


Example

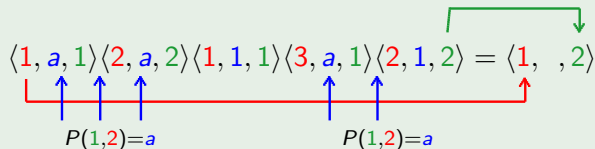
Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example



Example

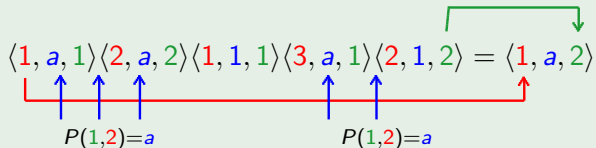
Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example



Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle = \langle 1, a, 2 \rangle$$

$P(1,2)=a$ $P(1,2)=a$

Theorem

Pletscheva, VV (2005) TERM-EQ(S_P) is coNP-complete

Example

Example

$$Z_2 = \langle a \rangle$$

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

where $\Lambda = I = \{1, 2, 3\}$

Example

$$\langle 1, a, 1 \rangle \langle 2, a, 2 \rangle \langle 1, 1, 1 \rangle \langle 3, a, 1 \rangle \langle 2, 1, 2 \rangle = \langle 1, a, 2 \rangle$$

$P(1,2)=a$ $P(1,2)=a$

Theorem

Goldberg, VV (2005) $TERM-EQ(S_P)$ is coNP-complete

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{array}{c} h^{-1} \\ \downarrow \\ \begin{pmatrix} 0 & g \\ h & k \end{pmatrix} \end{array}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & g \\ 1 & k \end{pmatrix} \leftarrow g^{-1}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & k \end{pmatrix} \xleftarrow{k^{-1}}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & g_1 & g_2 \\ g_4 & 0 & g_3 \\ g_5 & g_6 & 0 \end{pmatrix}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{matrix} g_5^{-1} \\ \downarrow \\ \begin{pmatrix} 0 & g_1 & g_2 \\ g_4 & 0 & g_3 \\ g_5 & g_6 & 0 \end{pmatrix} \end{matrix}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & g_1 & g_2 \\ g'_4 & 0 & g_3 \\ 1 & g_6 & 0 \end{pmatrix} \leftarrow g'^{-1}_4$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & g_1 & g_2 \\ 1 & 0 & g'_3 \\ 1 & g_6 & 0 \end{pmatrix}$$

$g_3'^{-1}$
↓

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & g_1 & g'_2 \\ 1 & 0 & 1 \\ 1 & g_6 & 0 \end{pmatrix} \leftarrow g_2'^{-1}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{matrix} g_6^{-1} \\ \downarrow \\ \begin{pmatrix} 0 & g_1 & 1 \\ 1 & 0 & 1 \\ 1 & g_6 & 0 \end{pmatrix} \end{matrix}$$

Example

Fact

Multiplying a row or column of the matrix by a group-element doesn't change the semigroup

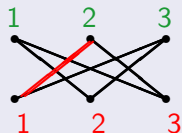
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & g & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Translating to Graphs

For the semigroup S_P we define a bipartite graph:

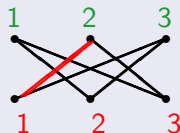
$$P = \begin{pmatrix} 0 & a & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$



Translating to Graphs

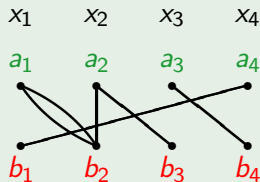
For the semigroup S_P we define a bipartite graph:

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



Example

$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$



The Equivalence Problem over S_P

2HOM(H)

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph
- Question: $\forall \varphi : G \rightarrow H$ homomorphism $2 \mid |\varphi^{-1}(e)|$

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph
- Question: $\forall \varphi : G \rightarrow H$ homomorphism $2 \mid |\varphi^{-1}(e)|$

Lemmata

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph
- Question: $\forall \varphi : G \rightarrow H$ homomorphism $2 \mid |\varphi^{-1}(e)|$

Lemmata

- 2HOM() $\stackrel{\text{poly}}{\iff}$ TERM-EQ(S_P)

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph
- Question: $\forall \varphi : G \rightarrow H$ homomorphism $2 \mid |\varphi^{-1}(e)|$

Lemmata

- 2HOM() $\stackrel{\text{poly}}{\iff}$ TERM-EQ(S_P)
- 2HOM() coNP-complete.

The Equivalence Problem over S_P

2HOM(H)

- Given: H a finite bipartite graph
- Input: G a finite bipartite graph
- Question: $\forall \varphi : G \rightarrow H$ homomorphism $2 \mid |\varphi^{-1}(e)|$

Lemmata

- $2\text{HOM}\left(\begin{array}{c} \bullet & & \bullet \\ \diagdown & & \diagup \\ \bullet & & \bullet \\ \diagup & & \diagdown \\ \bullet & & \bullet \end{array}\right) \stackrel{\text{poly}}{\iff} \text{TERM-EQ}(S_P)$
- $2\text{HOM}\left(\begin{array}{c} \bullet & & \bullet \\ \diagdown & & \diagup \\ \bullet & & \bullet \\ \diagup & & \diagdown \\ \bullet & & \bullet \end{array}\right)$ coNP-complete.

Theorem

Goldberg, VV

$\text{TERM-EQ}(S_P)$ is coNP-complete.

Results – Rings

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

Results – Rings

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

- *in P , if the ring is nilpotent,*

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

- *in P , if the ring is nilpotent,*
- *coNP-complete otherwise.*

Results – Rings

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

- *in P , if the ring is nilpotent,*
- *coNP-complete otherwise.*

Theorem

Burris, Lawrence (1993)

For a finite ring the equivalence problem is

Results – Rings

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

- *in P , if the ring is nilpotent,*
- *coNP-complete otherwise.*

Theorem

Burris, Lawrence (1993)

For a finite ring the equivalence problem is

- *in P , if the ring is nilpotent,*

Results – Rings

Theorem

Hunt, Stearnes (1990)

For a finite commutative ring the equivalence problem is

- *in P , if the ring is nilpotent,*
- *coNP-complete otherwise.*

Theorem

Burris, Lawrence (1993)

For a finite ring the equivalence problem is

- *in P , if the ring is nilpotent,*
- *is coNP-complete otherwise.*

Example

Example

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$
 - $x \vee y \leftrightarrow x + y + xy$

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$
 - $x \vee y \leftrightarrow x + y + xy$
 - $\bar{x} \leftrightarrow 1 + x$

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$
 - $x \vee y \leftrightarrow x + y + xy$
 - $\bar{x} \leftrightarrow 1 + x$
- 3-SAT can be formulated:

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$
 - $x \vee y \leftrightarrow x + y + xy$
 - $\bar{x} \leftrightarrow 1 + x$
- 3-SAT can be formulated:
- $(x_1 \vee x_2 \vee \bar{x}_3) \wedge \cdots \wedge (x_{n_1} \vee x_{n_2} \vee x_{n_3}) \rightsquigarrow$

Example

Example

- $\mathbb{Z}_2$ is a Boolean ring:
 - identity element
 - $x^2 = x$
- form a Boolean algebra:
 - $x \wedge y \leftrightarrow x \cdot y$
 - $x \vee y \leftrightarrow x + y + xy$
 - $\bar{x} \leftrightarrow 1 + x$
- 3-SAT can be formulated:
 - $(x_1 \vee x_2 \vee \bar{x}_3) \wedge \cdots \wedge (x_{n_1} \vee x_{n_2} \vee x_{n_3}) \rightsquigarrow$
 - $((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2)) \cdots$

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

expand $\Rightarrow$ exponentially many monoms

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

expand $\Rightarrow$ exponentially many monoms

Restriction for TERMS

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

expand $\Rightarrow$ exponentially many monoms

Restriction for TERMS

- any

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

expand $\Rightarrow$ exponentially many monoms

Restriction for TERMS

- any
- TERM_Σ (sum of monomials)
 $x_1x_2^3x_3 + x_1 + x_2x_1x_3 + x_{19}$
 $\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ problem

Different approaches of the Equivalence Problem over Rings

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2))(x_5 + x_2 \cdots) \cdots$$

expand $\Rightarrow$ exponentially many monoms

Restriction for TERMS

- any
- TERM_Σ (sum of monomials)
 $x_1x_2^3x_3 + x_1 + x_2x_1x_3 + x_{19}$
 $\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ problem
- monomial
just in the multiplicative semigroup TERM-EQ problem for the multiplicative semigroup

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

- *in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative.*

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

- *in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative.*
- *If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple non-commutative matrix ring, then $TERM_{\Sigma}\text{-}EQ(\mathcal{R})$ is coNP-complete.*

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

- in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative.*
- If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple non-commutative matrix ring, then $TERM_{\Sigma}\text{-}EQ(\mathcal{R})$ is coNP-complete.*

Theorem

Szabó, VV (2004)

The Σ -version of the equivalence problem is

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

- in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative.*
- If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple non-commutative matrix ring, then $TERM_{\Sigma}\text{-}EQ(\mathcal{R})$ is coNP-complete.*

Theorem

Szabó, VV (2004)

The Σ -version of the equivalence problem is

- in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative;*

The Σ -version for Rings

Theorem

Lawrence, Willard (1997), Szabó, VV (2004)

The Σ -version of the equivalence problem is

- *in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative.*
- *If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple non-commutative matrix ring, then $TERM_{\Sigma}\text{-}EQ(\mathcal{R})$ is coNP-complete.*

Theorem

Szabó, VV (2004)

The Σ -version of the equivalence problem is

- *in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative;*
- *coNP-complete otherwise.*

Step 1. – Reduction to the Group case

Search for a big N such that

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

- $\exists B \in \mathrm{SL}_n(q)$ with $B^N \neq 1$.

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

- $\exists B \in \mathrm{SL}_n(q)$ with $B^N \neq 1$.

Zsigmondy's Theorem

For almost all $1 < a, n \in \mathbb{Z}$ there exists a prime p such that:

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

- $\exists B \in \text{SL}_n(q)$ with $B^N \neq 1$.

Zsigmondy's Theorem

For almost all $1 < a, n \in \mathbb{Z}$ there exists a prime p such that:

- $p \mid a^n - 1$

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

- $\exists B \in \text{SL}_n(q)$ with $B^N \neq 1$.

Zsigmondy's Theorem

For almost all $1 < a, n \in \mathbb{Z}$ there exists a prime p such that:

- $p \mid a^n - 1$
- $p \nmid a^i - 1, \quad 0 < i < n$

Step 1. – Reduction to the Group case

Search for a big N such that

- for every non invertible matrix $A \in M_n(\mathbb{F})$: A^N is idempotent

Everything can disappear!!

- $\exists B \in \text{SL}_n(q)$ with $B^N \neq 1$.

Zsigmondy's Theorem

For almost all $1 < a, n \in \mathbb{Z}$ there exists a prime p such that:

- $p \mid a^n - 1$
- $p \nmid a^i - 1, \quad 0 < i < n$
- $p \nmid n$

Step 2. – Reduction to the Group case

Theorem

Horváth, Mérai, Lawrence, Szabó

TERM-EQ is coNP-complete for nonsolvable groups.

Step 2. – Reduction to the Group case

Theorem

Horváth, Mérai, Lawrence, Szabó

TERM-EQ is coNP-complete for nonsolvable groups.

(Gabor Horváth's talk)

Step 2. – Reduction to the Group case

Theorem

Horváth, Mérai, Lawrence, Szabó

TERM-EQ is coNP-complete for nonsolvable groups.

(Gabor Horváth's talk)

$\rightsquigarrow$ w a term that proves the coNP-completeness for $GL_n(q)$

Step 2. – Reduction to the Group case

Theorem

Horváth, Mérai, Lawrence, Szabó

TERM-EQ is coNP-complete for nonsolvable groups.

(Gabor Horváth's talk)

$\rightsquigarrow$ w a term that proves the coNP-completeness for $GL_n(q)$
 w^N will be a proof for $M_n(q)$

Step 3. – Direct Sum of Matrix Rings

Find a polynomial f such that

Step 3. – Direct Sum of Matrix Rings

Find a polynomial f such that

- $f(A) = 0$ in most of the coordinates but

Step 3. – Direct Sum of Matrix Rings

Find a polynomial f such that

- $f(A) = 0$ in most of the coordinates but
- $\exists B \in \mathrm{SL}_n(\mathbb{F})$ such that $f(B) \in \mathrm{GL}_n(\mathbb{F})$ for one coordinate

Step 3. – Direct Sum of Matrix Rings

Find a polynomial f such that

- $f(A) = 0$ in most of the coordinates but
- $\exists B \in \mathrm{SL}_n(\mathbb{F})$ such that $f(B) \in \mathrm{GL}_n(\mathbb{F})$ for one coordinate

Hilbert Theorem 90's

There exist an element of norm 1 in $\mathbb{F}_p^\alpha$ over $\mathbb{F}_p$.

Step 4. – From Direct Sum of Matrix Rings to Rings

Fact

$\mathcal{R}$ a finite ring ,
 $\mathcal{J}(\mathcal{R})$ its Jacobson-radical then

Step 4. – From Direct Sum of Matrix Rings to Rings

Fact

$\mathcal{R}$ a finite ring ,
 $\mathcal{J}(\mathcal{R})$ its Jacobson-radical then

- $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$

Step 4. – From Direct Sum of Matrix Rings to Rings

Fact

$\mathcal{R}$ a finite ring ,
 $\mathcal{J}(\mathcal{R})$ its Jacobson-radical then

- $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$
- $\mathcal{J}(\mathcal{R})$ is nilpotent, i.e. $\mathcal{J}(\mathcal{R})^n = 0$

Step 4. – From Direct Sum of Matrix Rings to Rings

Fact

$\mathcal{R}$ a finite ring ,
 $\mathcal{J}(\mathcal{R})$ its Jacobson-radical then

- $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$
- $\mathcal{J}(\mathcal{R})$ is nilpotent, i.e. $\mathcal{J}(\mathcal{R})^n = 0$

w is a word that proves coNP-completeness for $M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$
then
 w^n proves the coNP-completeness for $\mathcal{R}$

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)
- non-solvable ✓ (Horváth, Mérai, Lawrence, Szabó)

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)
- non-solvable ✓ (Horváth, Mérai, Lawrence, Szabó)
- metacyclic groups ✓ (Horváth, Szabó)

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)
- non-solvable ✓ (Horváth, Mérai, Lawrence, Szabó)
- metacyclic groups ✓ (Horváth, Szabó)
- S_4 ?

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)
- non-solvable ✓ (Horváth, Mérai, Lawrence, Szabó)
- metacyclic groups ✓ (Horváth, Szabó)
- S_4 ?
- ...

Problems

Rings

✓ (Burris, Hunt, Lawrence, Stearnes, Szabó, VV, Willard)

Groups

- nilpotent ✓ (Goldmann, Russel)
- non-solvable ✓ (Horváth, Mérai, Lawrence, Szabó)
- metacyclic groups ✓ (Horváth, Szabó)
- S_4 ?
- ...

Semigroups

Semigroups

Semigroups

- with constants (polynomials) $\equiv$ CSP

Problems

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups
 - S_P ✓ (Goldberg, VV)

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups
 - S_P ✓ (Goldberg, VV)
 - Hope: For any $CSP(B) \exists$ a 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$?

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups
 - S_P ✓ (Goldberg, VV)
 - Hope: For any $CSP(B) \exists$ a 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$?
- NP-complete for bands ✓ (Klima)

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups
 - S_P ✓ (Goldberg, VV)
 - Hope: For any $CSP(B) \exists$ a 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$?
- NP-complete for bands ✓ (Klima)
- NP-complete for the Brandt monoid ✓ (Klima, Seif)

Semigroups

- with constants (polynomials) $\equiv$ CSP

Theorem

*For any $CSP(B) \exists$ a combinatorial 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$*

- unfortunately TERM-EQ is in P for these structures (Seif, Szabó)
- 0-simple semigroups
 - S_P ✓ (Goldberg, VV)
 - Hope: For any $CSP(B) \exists$ a 0-simple semigroup S such that:
 $POL-EQ(S) \equiv CSP(B)$?
- NP-complete for bands ✓ (Klima)
- NP-complete for the Brandt monoid ✓ (Klima, Seif)
- Combinatorial semigroups ?

Vége = The End

What about your favorite structure?