Identities in Algebras

Vera Vértesi

Joint work with Csaba Szabó

2005

Basic Notions

- Algebra $\mathbf{A}(A, \mathcal{F})$, where

  A is the *underlying* set of $\mathbf{A}$,

  $\mathcal{F} = \{f_1, \ldots, f_n\}$ is the set of *fundamental operations*

  E.g.: $\mathbf{G}(G, \{1, \cdot, ^{-1}\})$

- term is an expression containing *variables*, connected with fundamental operations.

  E.g.: $x_1 x_2^{-1} x_3 1 x_4 x_9$ is a term over any group

The Identity Checking Problem

- TERM-EQ($\mathbf{A}$)

  Given: $\mathbf{A}$ a finite and finitely typed algebra

  Input: $t \overset{?}{\equiv} s$ identity, where t and s are terms

  Question: Is $t = s$ for every substitution over $\mathbf{A}$?

  (i.e. Is $t \equiv s$ is an identity of $\mathbf{A}$?)

- E.g. $x^p \overset{?}{\equiv} x$ in $\mathbb{Z}_p$
- E.g. $AB \not\equiv BA$ over $M_n(\mathbb{F})$
- E.g. $[(AB - BA)^2, C] \equiv 0$ over $M_2(\mathbb{F})$

Complexity of the Identity Checking Problem

- Always decidable (by substituting)
- ? Computational Complexity:

  P, NP, coNP, NP-complete, coNP-complete
- It is in coNP

  Given: A variety (rings, groups, lattices, semigroups,. . .)

  Goal: Prove duality! (TERM-EQ is either in P or coNP-complete)

Groups

- Theorem: *Lawrence*, *Willard* (1993)
  TERM-EQ is coNP-complete for G finite non-solvable groups.

- Theorem: *Goldmann*, *Russel* (2001)
  For nilpotent groups TERM-EQ is in P.

- Theorem: *Horváth*, *Kun*, *Szabó*, *W* (2003)
  TERM-EQ is in P for metacyclic groups (semidirect product of cyclic groups).

- The question is open for other finite groups.

Rings

- Theorem: *Burris*, *Lawrence* (1993)
  For a finite ring $\mathcal{R}$ $\mathrm{TERM\text{-}EQ}(\mathcal{R})$ is in P, if $\mathcal{R}$ is nilpotent, $\mathrm{TERM\text{-}EQ}(\mathcal{R})$ is coNP-complete otherwise

- E.g. $\mathbb{Z}_2$
  Boole-ring: identity element, $x^2 = x$

  Boole-algebra:
  $$\begin{aligned} x \wedge y &\leftrightarrow x \cdot y \\ x \vee y &\leftrightarrow x + y + xy \\ \bar{x} &\leftrightarrow 1 + x \end{aligned}$$

  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 Identity Checking Problem over Rings

TERM:

- any
  E.g. $(x + y)^n$

- TERM_Σ (sum of monomials)
  E.g. $x_1 x_2^3 x_3 + x_1 + x_2 x_1 x_3 + x_{19}$
  TERM_Σ-$\mathrm{EQ}(\mathcal{R})$ problem

- monomial
  just in the multiplicative semigroup
  TERM-EQ problem for the multiplicative semigroup

Matrix Rings

- Theorem: *Lawrence*, *Willard* (1997)
  If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple matrix ring whose invertible elements form a nonsolvable group, then $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(\mathcal{R})$ is coNP-complete.

- Theorem: *Szabó*, *W* (2002-2003)
  TERM-EQ is in P for the multiplicative semigroup of a finite simple matrix ring, $M_n(\mathbb{F})$ if it is commutative;
  Otherwise it is coNP-complete.

$\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$

- Theorem: *Szabó*, *W* Let $M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$ a non-commutative direct sum of matrix rings (i.e. $\exists n_i \geq 1$) then $\text{TERM}_\Sigma\text{-EQ}$ is coNP-complete.

  Let $\mathcal{R}$ be a finite ring,
  $\mathcal{J}(\mathcal{R})$ denotes its Jacobson-radical.
  Then $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$

- Theorem: *Szabó*, *W* For a finite ring $\mathcal{R}$ $\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ is in P if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative;
  Otherwise it is coNP-complete.

Semigroups

Are there any semigroups so that TERM-EQ is coNP-complete?

- *Volkov* (2002)
  #elements $\approx \mathbf{2^{1700}}$
- *Kisielewicz* (2002)
  few thousand
- *Szabó*, *W* (2002)
  13
- *Klima* (2003)
  6

Other semigroups?

Combinatorial 0-simple semigroups

$\mathbf{M}$ – a 0–1 matrix.

$\boldsymbol{\Lambda}$ – the index set of rows

$\boldsymbol{I}$ – the index set of columns

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

Multiplication:

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

and

$$0 \cdot s = 0 = s \cdot 0 \qquad \forall s \in S_{\mathrm{M}}$$

Example

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

and

$$0 \cdot s = 0 = s \cdot 0 \qquad \forall s \in S_{\mathrm{M}}$$

E.g.

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

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

$$\langle 2, \underbrace{3 \rangle \langle 1}_{M(3,1)=1}, 2 \rangle = \langle 2, 2 \rangle$$

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

Example

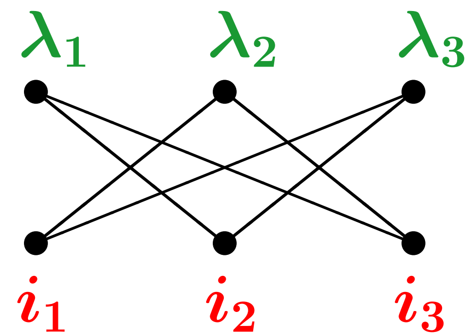
$$\langle i,\lambda\rangle\langle j,\mu\rangle = \begin{cases} \langle i,\mu\rangle, & \text{if } \mathrm{M}(\lambda,j)=1 \\ 0, & \text{if } \mathrm{M}(\lambda,j)=0 \end{cases}$$

and

$$0\cdot s = 0 = s\cdot 0 \qquad \forall s\in S_{\mathrm{M}}$$

E.g.

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



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

$$\langle 2,3\rangle\underbrace{\rangle\langle}_{M(3,1)=1}1,2\rangle = \langle 2,2\rangle$$

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

Translating to Graphs

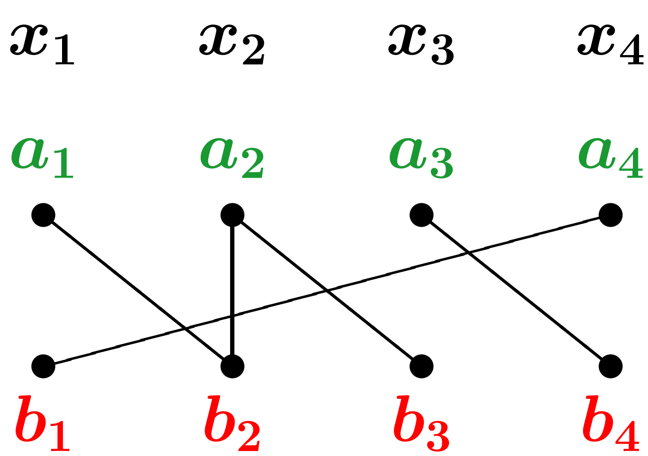
$t = x_1 \cdots x_n$, $X := \{x_1, \ldots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$

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

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

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

E.g.: $t = x_1 x_2^2 x_3 x_4 x_1 x_2$



Evaluating

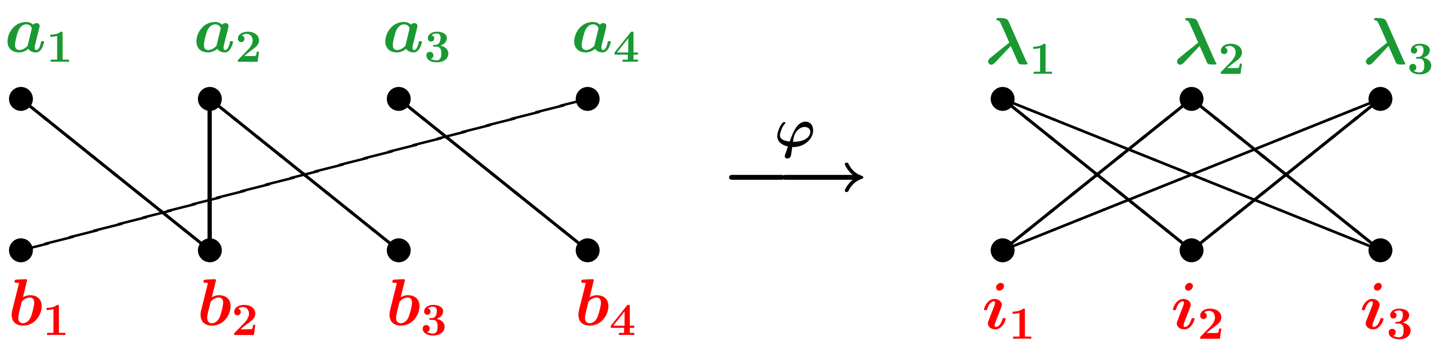
$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \overset{\varepsilon}{\longmapsto} \langle 1, 2 \rangle \qquad x_2 \overset{\varepsilon}{\longmapsto} \langle 3, 2 \rangle \qquad x_3 \overset{\varepsilon}{\longmapsto} \langle 2, 1 \rangle \qquad x_4 \overset{\varepsilon}{\longmapsto} \langle 2, 2 \rangle$$

$$a_1 \overset{\varphi}{\longmapsto} \lambda_1 \qquad a_2 \overset{\varphi}{\longmapsto} \lambda_3 \qquad a_3 \overset{\varphi}{\longmapsto} \lambda_2 \qquad a_4 \overset{\varphi}{\longmapsto} \lambda_2$$

$$b_1 \overset{\varphi}{\longmapsto} i_2 \qquad b_2 \overset{\varphi}{\longmapsto} i_2 \qquad b_3 \overset{\varphi}{\longmapsto} i_1 \qquad b_4 \overset{\varphi}{\longmapsto} i_2$$

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



Evaluating

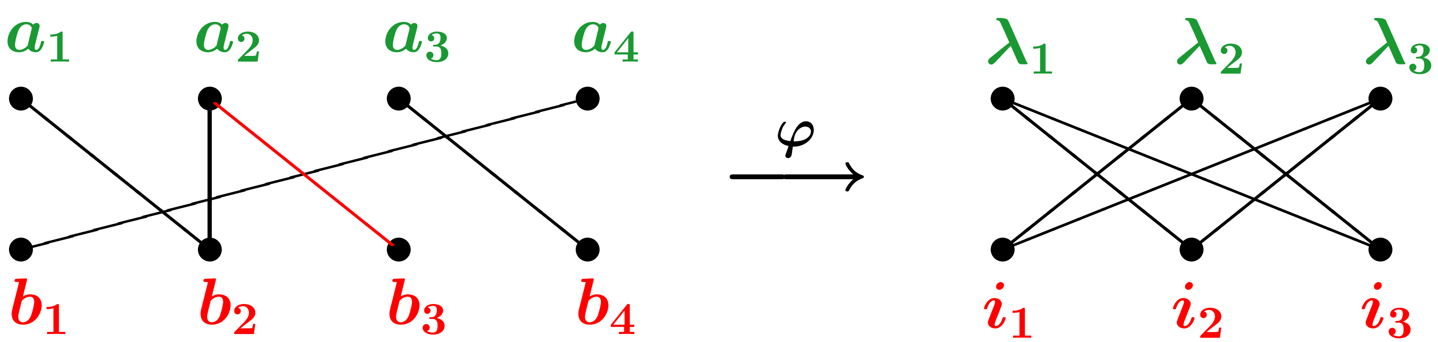
$$t = x_1 x_2^2 x_3 x_4 x_1 x_2$$

$$x_1 \overset{\varepsilon}{\longmapsto} \langle 1, 2\rangle \qquad x_2 \overset{\varepsilon}{\longmapsto} \langle 3, 2\rangle \qquad x_3 \overset{\varepsilon}{\longmapsto} \langle 2, 1\rangle \qquad x_4 \overset{\varepsilon}{\longmapsto} \langle 2, 2\rangle$$

$$a_1 \overset{\varphi}{\longmapsto} \lambda_1 \qquad a_2 \overset{\varphi}{\longmapsto} \lambda_3 \qquad a_3 \overset{\varphi}{\longmapsto} \lambda_2 \qquad a_4 \overset{\varphi}{\longmapsto} \lambda_2$$

$$b_1 \overset{\varphi}{\longmapsto} i_2 \qquad b_2 \overset{\varphi}{\longmapsto} i_2 \qquad b_3 \overset{\varphi}{\longmapsto} i_1 \qquad b_4 \overset{\varphi}{\longmapsto} i_2$$

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



Evaluating Terms

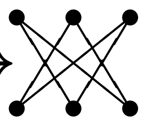
$t = x_1 \cdots x_n$, $X := \{x_1, \ldots, x_n\} \rightsquigarrow G_t(A_t, B_t, E_t)$

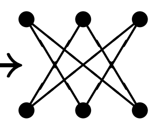
where $A_t = \{a_x \mid x \in X\}$,

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

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

$\varepsilon : X \longrightarrow S_A \setminus \{0\}$ an evaluation

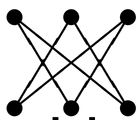
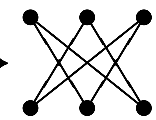
$\varphi^t_\varepsilon : G_t \rightarrow$  $\varphi^t_\varepsilon(a_x) = \lambda$, $\varphi^t_\varepsilon(b_x) = i$ if $\varepsilon(x) = \langle i, \lambda \rangle$

Claim:
- $\varepsilon(t) \neq 0 \iff \varphi^t_\varepsilon : G_t \rightarrow$  is a homomorphism;
- If $\varepsilon(t) \neq 0$, then $\varepsilon(t) = \langle \varphi^t_\varepsilon(b_{x_1}), \varphi^t_\varepsilon(a_{x_n}) \rangle$

Identities of S_A

$t = x_1 \cdots x_n \; s = y_1 \cdots y_m, \; X = \{x_1, \ldots, x_n, y_1, \ldots y_m\}$

Claim: Let $\varepsilon : X \to S_A \setminus \{0\}$ be an evaluation, then $\varepsilon(t) = \varepsilon(s)$ iff:

- $\varphi^t_\varepsilon : G_t \to$  is a homomorphism $\iff$ $\varphi^s_\varepsilon : G_s \to$  is a homomorphism;
- if $\varepsilon(t) \neq 0$ and $\varepsilon(s) \neq 0$, then $\varphi^t_\varepsilon(b_{x_1}) = \varphi^s_\varepsilon(b_{y_1})$ and $\varphi^t_\varepsilon(a_{x_n}) = \varphi^s_\varepsilon(a_{y_m})$

Theorem: $t \equiv s$ if and only if:
- $G_t = G_s$; and
- $x_1 = y_1$ and $x_n = x_m$

Theorem: *Seif*, *Szabó* (2001) $\text{TERM-EQ}(S_A) \in P$

Completely 0-simple Semigroups

G finite group

M is a $G \cup \{0\}$ matrix.

Λ – index set of rows

I – index set of columns

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

Multiplication:

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

and

$$0 \cdot s = 0 = s \cdot 0 \qquad \forall s \in S_{\mathrm{M}}$$

Example

E.g. $Z_2 = \langle a \rangle$

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

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

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

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

- Theorem: *Pletscheva*, *W* (2005) $\mathrm{TERM\text{-}EQ}(S_P)$ is coNP-complete

Sandwich Matrix

G finite group

$\mathbf{M} \in (G \cup \{0\})^{n \times m}$ matrix.

$S_M = \{$matrix of size $m \times n$ with at most one nonzero entry$\}$

Multiplication: $A, B \in S_M$

$$A \circ B = AMB$$

E.g.

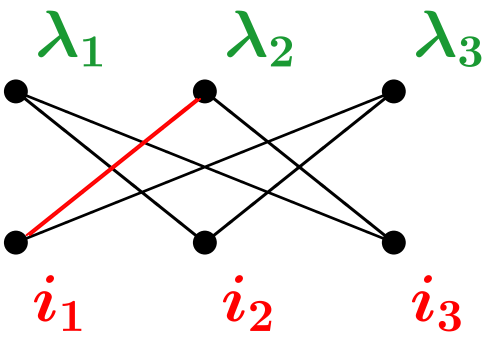
$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & a & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\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

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

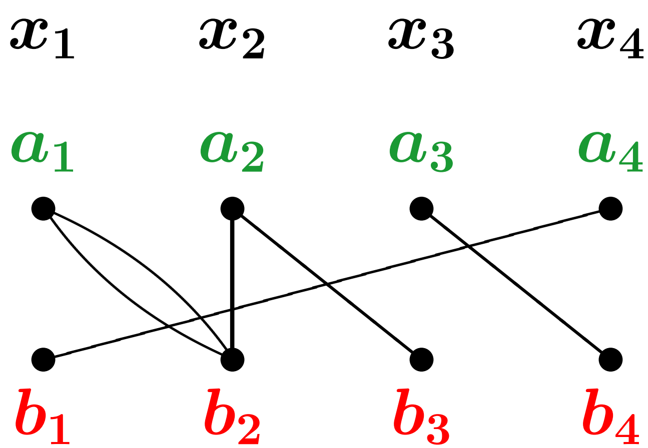
Translating to Graphs

For the semigroup S_P we define a bipartite graph:

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



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



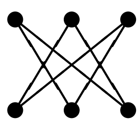
TERM-EQ(S_P)

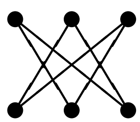
- $2HOM(H)$

Given: H a finite bipartite graph

Input: G a finite bipartite graph

Question: $\forall \varphi : G \to H$ homomorfism $2 \mid |\varphi^{-1}(e)|$

Lemma: 2HOM() $\overset{\text{poly}}{\Longleftrightarrow}$ TERM-EQ(S_P)

Lemma: 2HOM() coNP-complete.

Theorem: TERM-EQ(S_P) is coNP-complete.