The freeness problem for products of matrices defined on bounded languages

Émilie Charlier

(Joint work with Juha Honkala)

Département de Mathématique, Université de Liège

Journées montoises, Nancy, September 2014

Freeness problem

- Let S be a semigroup.
- $X \subseteq S$ is a code if

$$\text{for all } m, n \geq 1 \text{ and } x_1, \ldots, x_m, y_1, \ldots, y_n \in X,$$

$$x_1 x_2 \ldots x_m = y_1 y_2 \ldots y_n$$

$$\Downarrow$$

$$m = n \text{ and } \forall i,\ x_i = y_i.$$

- Decide if a given finite subset of S is a code.

Reformulating the problem

- Let S be a semigroup.
- Σ designates an alphabet (that is, a finite nonempty set).
- Decide if a given morphism $\mu\colon \Sigma^+ \to S$ is injective.
- In fact:

$$\mu \text{ is injective (on } \Sigma^+) \\ \Updownarrow \\ \mu(\Sigma) \text{ is a code and } \mu \text{ is injective on } \Sigma$$

Case of matrix semigroups

- Let R be a semiring and let $k \geq 1$ be an integer.
- The sets $R^{k \times k}$ and $R^{k \times k}_{\mathrm{uptr}}$ are monoids.
- Decide if a given morphism $\mu : \Sigma^* \to R^{k \times k}$ is injective.
- Most cases of this problem are undecidable.

Undecidability results

- Klarner, Birget, Satterfield (1991):

  The freeness problem over $\mathbb{N}^{3\times 3}$ is undecidable.

- Cassaigne, Harju, Karhumäki (1999):

  The problem remains undecidable for $\mathbb{N}^{3\times 3}_{\mathrm{uptr}}$.

- Both results use the Post correspondence problem.

Case of 2×2 matrices

- The freeness problem for $\mathbb{Q}^{2\times 2}$ is still open.
- Actually: still open even for $\mathbb{Q}^{2\times 2}_{\mathrm{uptr}}$.
- Partial decidability/undecidability results by Bell, Blondel, Cassaigne, Gawrychowski, Gutan, Harju, Honkala, Kisielewicz, Nicolas, Karhumäki, Potapov.

Our contribution

- A language $L \subseteq \Sigma^*$ is called bounded if there are $s \in \mathbb{N}$ and words $w_1, \ldots, w_s \in \Sigma^*$ such that

$$L \subseteq w_1^* w_2^* \ldots w_s^* .$$

- Decide if a given morphism $\mu : \Sigma^* \to \mathbb{Q}_{\mathrm{uptr}}^{k \times k}$ is injective on certain bounded languages.
- This approach is inspired by the well-known fact that many language theoretic problems which are undecidable in general become decidable when restricted to bounded languages.

Main results

First result: We can decide the injectivity of a given morphism

$$\mu : \{x, z_1, \ldots, z_{t+1}\}^* \to \mathbb{Q}_{\mathrm{uptr}}^{2\times 2}$$

on the language

$$z_1 x^* z_2 x^* z_3 \ldots z_t x^* z_{t+1}$$

(for any $t \geq 1$), provided that the matrices

$$\mu(z_i) \text{ are nonsingular for } 1 \leq i \leq t+1.$$

Main results

Second result: If we consider large enough matrices the problem becomes undecidable even if restricted to certain very special bounded languages.

- Hence, contrary to the common situation in language theory, the restriction of the freeness problem over bounded languages remains undecidable.
- We use a reduction to Hilbert's 10th problem (as for example in [1] and [2]).

[1] Kuich-Salomaa (1986): Semirings, Automata, Languages.

[2] Bell-Halava-Harju-Karhumäki (2007): Matrix equations and Hilbert's 10th problem.

Precise statements

Theorem 1 (C-Honkala 2014)

Let t be a positive integer. It is decidable whether a given morphism

$$\mu\colon \{x, z_1, \ldots, z_{t+1}\}^* \to \mathbb{Q}^{2\times 2}_{\mathrm{uptr}}$$

such that $\mu(z_i)$ is nonsingular for $i = 1, \ldots, t+1$, is injective on $z_1 x^* z_2 x^* z_3 \cdots z_t x^* z_{t+1}$.

Theorem 2 (C-Honkala 2014)

There exist two positive integers k and t such that there is no algorithm to decide whether a given morphism

$$\mu\colon \{x, y, z_1, z_2\}^* \to \mathbb{Z}^{k\times k}_{\mathrm{uptr}}$$

is injective on $z_1 (x^* y)^{t-1} x^* z_2$.

Some more comments on our results

- The languages
$$z_1(x^*y)^{t-1}x^*z_2$$
are the simplest bounded languages for which we are able to show undecidability while the languages
$$z_1x^*z_2x^*z_3\cdots z_tx^*z_{t+1}$$
are the most general ones for which we can show decidability.
- While bounded languages have a simple structure the induced matrix products can be used to represent very general sets.
- Our proof gives a method to compute the integers k and t in the second theorem.

Some examples

Example ($t = 2$)

Let

$$\mu(x) = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mu(z_2) = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}.$$

Then

$$\mu(x^m z_2 x^n) = \begin{pmatrix} 2 \cdot 3^{m+n} & 3^m \\ 0 & 3 \end{pmatrix} \quad \text{for all } m, n \in \mathbb{N}\,.$$

Hence μ is injective on $z_1 x^* z_2 x^* z_3$.

Recall that $\mu(z_1)$ and $\mu(z_3)$ are nonsingular.

Example ($t = 1$)

Let

$$\mu(x) = c\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{where } b, c \in \mathbb{Q} \text{ and } c \neq 0.$$

Then

$$\mu(x^n) = c^n\begin{pmatrix} 1 & nb \\ 0 & 1 \end{pmatrix} \quad \text{for all } n \in \mathbb{N}\,.$$

It follows that there exist different $m, n \in \mathbb{N}$ such that

$$\mu(x^m) = \mu(x^n)$$

if and only if

$$c \in \{-1, 1\} \quad \text{and} \quad b = 0.$$

Hence μ is injective on $z_1 x^* z_2$ iff $c \notin \{-1, 1\}$ or $b \neq 0$.

Example ($t = 2$)

Let

$$\mu(x) = c\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{where } b, c \in \mathbb{Q} \text{ and } c \neq 0,$$

and

$$\mu(z_2) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \in \mathbb{Q}^{2\times 2}_{\mathrm{uptr}}\,.$$

Then, for all $m, n \in \mathbb{N}$,

$$\mu(x^m z_2 x^n) = c^{m+n}\begin{pmatrix} A & Cbm + Abn + B \\ 0 & C \end{pmatrix}.$$

Hence μ is injective on $z_1 x^* z_2 x^* z_3$ iff $c \notin \{-1, 1\}$ and $Ab \neq Cb$.

Example ($t \geq 3$)

Let $\mu(x) = c\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b, c \in \mathbb{Q}$ and $c \neq 0$,

and $\mu(z_2) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, $\mu(z_3) = \begin{pmatrix} D & E \\ 0 & F \end{pmatrix} \in \mathbb{Q}^{2\times 2}_{\mathrm{uptr}}$.

Then, for all $\ell, m, n \in \mathbb{N}$,

$$\mu(x^\ell z_2 x^m z_3 x^n) = c^{\ell+m+n}\begin{pmatrix} AD & CFb\ell + AFbm + ADbn + AE + BF \\ 0 & CF \end{pmatrix}.$$

Then we can find different (ℓ, m, n), $(\ell', m', n') \in \mathbb{N}^3$ such that

$$\begin{aligned} \ell + m + n &= \ell' + m' + n', \text{ and} \\ CF\ell + AFm + ADn &= CF\ell' + AFm' + ADn'. \end{aligned}$$

This implies that μ is not injective on $z_1 x^* z_2 x^* \cdots z_t x^* z_{t+1}$.

From matrices to representations of rational numbers

- For any $m \in \mathbb{Q}$, we introduce a corresponding letter $\overline{m}$.
- We regard the elements of the set $\mathbb{Q}_1 = \{\overline{m} \mid m \in \mathbb{Q}\}$ as digits.
- For any $r \in \mathbb{Q} \setminus \{0\}$, we define

$$\mathsf{val}_r(\overline{w_{n-1}} \cdots \overline{w_1}\,\overline{w_0}) = \sum_{i=0}^{n-1} w_i\, r^i$$

where the $\overline{w_i}$'s belong to $\mathbb{Q}_1$.

A decidability method for Theorem 1

To prove Theorem 1 we study representations of rational numbers in a rational base.

Lemma

Let $s \in \mathbb{N} \setminus \{0\}$, *let* $M = c\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ *with* $a, b, c \in \mathbb{Q}$ *and,*

for $i = 1, \ldots, s+1$, *let* $N_i = \begin{pmatrix} A_i & B_i \\ 0 & C_i \end{pmatrix} \in \mathbb{Q}^{2\times 2}_{\mathrm{uptr}}$.

Then we can compute $d_1, d_2, q_1, \ldots, q_{s+1}, p_1, \ldots, p_s \in \mathbb{Q}$ *such that for all* $m_1, \ldots, m_s \in \mathbb{N} \setminus \{0\}$,

$$N_1 M^{m_1} N_2 \cdots N_s M^{m_s} N_{s+1}$$

$$= c^{\sum_{j=1}^{s} m_j} \begin{pmatrix} d_1 a^{\sum_{j=1}^{s} m_j} & \mathrm{val}_a(\overline{q_1}\,\overline{p_1}^{m_s - 1}\,\overline{q_2} \cdots \overline{q_s}\,\overline{p_s}^{m_1 - 1}\,\overline{q_{s+1}}) \\ 0 & d_2 \end{pmatrix}.$$

Comparison of the representations

If Σ is an alphabet, we let $\hat{\Sigma}$ be the alphabet defined by

$$\hat{\Sigma} = \left\{ \left[\begin{array}{c} \sigma_1 \\ \sigma_2 \end{array} \right] : \sigma_1, \sigma_2 \in \Sigma \right\}.$$

For convenience, we write

$$\left[\begin{array}{c} \sigma_{i_1} \\ \sigma_{j_1} \end{array} \right] \left[\begin{array}{c} \sigma_{i_2} \\ \sigma_{j_2} \end{array} \right] \cdots \left[\begin{array}{c} \sigma_{i_\ell} \\ \sigma_{j_\ell} \end{array} \right] = \left[\begin{array}{c} \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_\ell} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_\ell} \end{array} \right].$$

Lemma

Let $S \subseteq \mathbb{Q}$ be a finite nonempty set, let $S_1 = \{\overline{s} : s \in S\}$ and let $X = \hat{S_1}$. Let $r \in \mathbb{Q} \setminus \{-1, 0, 1\}$. Then the language

$$L = \left\{ \left[\begin{array}{c} w_1 \\ w_2 \end{array} \right] \in X^* : \ \mathrm{val}_r(w_1) = \mathrm{val}_r(w_2) \right\}$$

is effectively regular.

Sketch of the proof of Theorem 2

Main idea: use the undecidability of Hilbert's 10th problem combined with the following result.

Lemma

Let t be any positive integer and $p(x_1, \ldots, x_t)$ be any polynomial with integer coefficients. Then there effectively exists a positive integer k and matrices $A, M, N, B \in \mathbb{Z}_{\mathrm{uptr}}^{k\times k}$ such that

$$AM^{a_1}NM^{a_2}N\cdots NM^{a_t}B = \begin{pmatrix} 0 & \cdots & 0 & p(a_1, \ldots, a_t) \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

for all $a_1, \ldots, a_t \in \mathbb{N}$.

Strong version of the undecidability of Hilbert's 10th problem

Theorem 3.20 in [3]

There exists a polynomial $P(x_1, x_2, \ldots, x_m)$ with integer coefficients such that no algorithm exists for the following problem:

Given $a \in \mathbb{N} \setminus \{0\}$, decide if there exist $b_2, \ldots, b_m \in \mathbb{N}$ such that

$$P(a, b_2, \ldots, b_m) = 0.$$

[3] Rozenberg-Salomaa (1994): Cornerstones of undecidability.