Complexity of Reachability, Mortality and Freeness Problems for Matrix Semigroups

Paul C. Bell
Department of Computer Science
Loughborough University
P.Bell@lboro.ac.uk

Co-authors for todays topics:
V. Halava, T. Harju, M. Hirvensalo, J. Karhumäki (Turku University, Finland)
I. Potapov (University of Liverpool)

North British Semigroups and Applications Network (2015)
University of St Andrews
Outline of the talk

- Introduction
  - Complexity classes P, NP, PSPACE & hardness
  - Computability and undecidability
- Algorithmic problems for matrix semigroups
  - Reachability (membership)
    - Mortality
    - Identity
  - Freeness
- Open Problems
- Connections between semigroup theory, combinatorics on words and matrix problems
Computability & Complexity

- **Decidable**
  - P
  - NP (NP-hard, NP-complete, ...)
  - PSPACE

- **Undecidable**

- **Decidability**: giving an algorithm which always halts and gives the correct answer in a finite time.

- **Complexity**: showing equivalence of existing NP-hard, PSPACE-hard problems or analysing properties of the problem.

- **Undecidability**: simulation (reduction) of a Turing or Minsky machine, Post’s Correspondence Problem (PCP), Hilbert’s tenth problem, other undecidable problem, etc.
Marix Semigroups (Example 1)

Given a set of finite matrices $G = \{M_1, M_2, \ldots, M_k\} \subseteq K^{n \times n}$, we are interested in algorithmic decision questions regarding the semigroup $S$ generated by $G$, denoted $S = \langle G \rangle$.
Decision Problems for Matrix Semigroups

- Given a matrix semigroup $S$ generated by a finite set
  $G = \{M_1, M_2, \ldots, M_k\} \subseteq K^{n \times n}$ (where $K \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}\}$):
  - Decide whether the semigroup $S$
    - contains the zero matrix (Mortality Problem)
    - contains the identity matrix (Identity Problem)
    - is free (Freeness Problem)
    - is bounded, finite, etc.

- Vector reachability problems:
  - Given two vectors $x$ and $y$. Decide whether the semigroup $S$
    contains a matrix $M$ such that $Mx = y$
  - Variants of such problems are important for probabilistic and quantum automata models
Early Reachability Results

- The Mortality Problem was one of the earliest undecidability results of reachability for matrix semigroups

**Theorem ([Paterson 70])**

The Mortality Problem is undecidable over \( \mathbb{Z}^{3 \times 3} \)

- holds even when the semigroup is generated by just 6 matrices over \( \mathbb{Z}^{3 \times 3} \), or for 2 matrices over \( \mathbb{Z}^{15 \times 15} \) [Cassaigne et al., 14]

- The undecidability results use a reduction of Post’s Correspondence Problem (PCP).
Post’s Correspondence Problem

- Posts Correspondence Problem (PCP) is a useful tool for proving undecidability.

**Theorem**

- **PCP(2) is decidable**
  [Ehrenfeucht, Karhumäki, Rozenberg, 82]

- **PCP(7) is undecidable**
  [Matiyasevich, Sénizergues, 96]

- **PCP(5) is undecidable**
  [Neary 15].

**Figure:** An instance of PCP(3)
Post’s Correspondence Problem

- Posts Correspondence Problem (PCP) is a useful tool for proving undecidability.

**Theorem**

- **PCP(2) is decidable**
  
  \[\text{Ehrenfeucht, Karhumäki, Rozenberg, 82}\]

- **PCP(7) is undecidable**
  
  \[\text{Matiyasevich, Sénizergues, 96}\]

- **PCP(5) is undecidable**
  
  \[\text{Neary 15}\]

**Figure**: A solution - aabbaabba
Word Encodings

- Words over a binary alphabet can be encoded into $2 \times 2$ matrices.
- Given a binary alphabet $\Sigma = \{a, b\}$, let $\gamma : \Sigma^* \mapsto \mathbb{Z}^{2 \times 2}$ be defined by:
  $$\gamma(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \gamma(b) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
- Then $\gamma$ is a monomorphism (injective homomorphism).
- This gives us a way to embed problems on words into problems for semigroups (for example with the direct sum).
Word Encodings (2)

- Let $\sigma(a) = 1$, $\sigma(b) = 2$ and $\sigma(uv) = 3|v|\sigma(u) + \sigma(v)$ for every $u, v \in \Sigma^*$. Then $\sigma$ is a monomorphism $\Sigma^* \to \mathbb{N}$.
- We may then define a mapping $\tau : \Sigma^* \times \Sigma^* \mapsto \mathbb{Z}^{3 \times 3}$

\[
\tau(u, v) = \begin{pmatrix}
1 & \sigma(v) & \sigma(u) - \sigma(v) \\
0 & 3|v| & 3|u| - 3|v| \\
0 & 0 & 3|u|
\end{pmatrix}
\]

- We can prove that $\tau(u_1, v_1) \cdot \tau(u_2, v_2) = \tau(u_1u_2, v_1v_2)$ for all $u_1, u_2, v_1, v_2 \in \Sigma^*$, thus $\tau$ is a monomorphism.
- Note that $\tau(u, v)_{1,3} = 0$ if and only if $u = v$.
- With some more work this technique can be used to show the undecidability of the Mortality Problem via a reduction of PCP, see [Cassaigne et al. 14] for example.
An aside - Skolem’s Problem

- Determining if a matrix in a finitely generated matrix semigroup contains a zero in the top right element is referred to as the ZRUC (zero-in-the-right-upper-corner problem).

**Definition (Linear Recurrence Sequence)**

Given a sequence of recurrence coefficients \(a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}\) and a sequence of initial values \(u_0, u_1, \ldots, u_{n-1} \in \mathbb{Z}\), a linear recurrence sequence (of depth \(n\)) may be written in the form (for \(k \geq n\)):

\[ u_k = a_{n-1}u_{k-1} + a_{n-2}u_{k-2} + \cdots + a_0u_{k-n}. \]
(Very difficult) **Open Problem 1:** For a linear recurrence sequence $u = (u_k)_{k=0}^\infty \subseteq \mathbb{Z}$, the zero set of $u$ is given by $Z(u) = \{ i \in \mathbb{N} \mid u_i = 0 \}$. Determine if $Z(u)$ is an empty set.

It is known that $Z(u)$ is a semilinear set [Skolem, 34], [Mahler, 35], [Lech, 53], and that the problem is decidable when the depth is 4 or below [Vereshchagin, 85].

It is not difficult to show that this problem is equivalent to the following: given a matrix $M \in \mathbb{Z}^{(n+2)\times(n+2)}$, determine if there exists $k > 0$, such that $M_{1,(n+2)}^k = 0$

i.e. the ZRUC problem for a semigroup generated by a single matrix.
Mortality over Bounded Languages

Theorem (B., Halava, Harju, Karhumäki, Potapov, 2008)

Given integral matrices $X_1, X_2, \ldots, X_k \in \mathbb{Z}^{n \times n}$, it is algorithmically undecidable to determine whether there exists a solution to the equation:

$$X_1^{i_1}X_2^{i_2}\cdots X_k^{i_k} = Z,$$

where $Z$ denotes the zero matrix and $i_1, i_2, \ldots, i_k \in \mathbb{N}$ are unknowns.

To prove this theorem, an encoding of Hilbert’s tenth problem was used (next slide).
Hilbert’s Tenth Problem - Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.
Semigroup Freeness

Definition (Code)

Let $S$ be a semigroup and $G$ a subset of $S$. We call $G$ a code if the property

$$u_1 u_2 \cdots u_m = v_1 v_2 \cdots v_n$$

for $u_i, v_i \in G$, implies that $m = n$ and $u_i = v_i$ for each $1 \leq i \leq n$.

Definition (Semigroup freeness)

A semigroup $S$ is called free if there exists a code $G \subseteq S$ such that $S = G^+.$

- For example, consider the semigroup $\{0, 1\}^+$ under concatenation. Then the set $\{00, 01, 10, 11\}$ is a code, but $\{01, 10, 0\}$ is not (since $0 \cdot 10 = 01 \cdot 0$ for example).
Matrix Freeness

Problem (Matrix semigroup freeness)

**SEMIGROUP FREENESS PROBLEM** - Given a finite set of matrices $G \subseteq \mathbb{Z}^{n \times n}$ generating a semigroup $S$, does every element $M \in S$ have a single, unique factorisation over $G$? Alternatively, is $G$ a code?

- The semigroup freeness problem is *undecidable* over $\mathbb{N}^{3 \times 3}$ [Klarner, Birget and Satterfield, 91]
- In fact, the undecidability result holds even over $\mathbb{N}^{3 \times 3}_{uptr}$ [Cassaigne, Harju and Karhumäki, 99]
Matrix Freeness in Dimension 2

- Let \( A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \) and \( B = \begin{pmatrix} 3 & 5 \\ 0 & 5 \end{pmatrix} \), is \( \{A, B\} \) a code?

- Two groups of authors independently showed that in fact the following equation holds and thus the generated semigroup is not free [Gawrychowskia et al. 2010], [Cassaigne et al. 2012]:

\[
\]

and no shorter non-trivial equation exists.

- **Open Problem 2** - Determine the decidability of the **Freeness Problem** over \( \mathbb{N}^{2\times2} \) (even for two matrices, or when all matrices are upper triangular).
The Identity Problem

Problem (The Identity Problem)

Given a matrix semigroup $S$ generated by a finite set $G = \{M_1, M_2, \ldots, M_k\} \subseteq \mathbb{Z}^{n \times n}$, determine if $I_n \in \langle G \rangle$, where $I_n$ is the $n$-dimensional multiplicative identity matrix.

- The Identity Problem is undecidable over $\mathbb{Z}^{4 \times 4}$ [B., Potapov, 2011].
- To show the undecidability of the Identity Problem, we introduced the Identity Correspondence Problem (next slide).
The Identity Problem - undecidability

Problem (Identity Correspondence Problem (ICP))

Identity Correspondence Problem (ICP) - Let \( \Gamma = \{ a, b, a^{-1}, b^{-1} \} \) generate a free group on a binary alphabet and \( \Pi = \{(s_1, t_1), (s_2, t_2), \ldots, (s_m, t_m)\} \subseteq \Gamma^* \times \Gamma^* \).

Determine if there exists a nonempty finite sequence of indices \( i_1, i_2, \ldots, i_k \) where \( 1 \leq i_j \leq m \) such that

\[
s_{i_1} s_{i_2} \cdots s_{i_k} = t_{i_1} t_{i_2} \cdots t_{i_k} = \varepsilon,
\]

where \( \varepsilon \) is the empty word (identity).

The Identity Correspondence can be shown to be undecidable (next slides).
The Identity Problem - encoding idea
Applications of the Identity Correspondence Problem

Problem (Group Problem)

Given a free binary group alphabet \( \Gamma = \{ a, b, a^{-1}, b^{-1} \} \), is the semigroup generated by a finite set of pairs of words \( P = \{ (u_1, v_1), (u_2, v_2), \ldots, (u_m, v_m) \} \subset \Gamma^* \times \Gamma^* \) a group?

Theorem (B., Potapov, 2010)

The Group Problem is undecidable for \( m = 8(n - 1) \) pairs of words where \( n \) is the minimal number of pairs for which PCP is known to be undecidable \( (n = 5) \).
Theorem (B., Potapov, 2010)

The Identity Problem is undecidable for a semigroup generated by 48 matrices from $\mathbb{Z}^{4 \times 4}$.

The proof uses the following injective homomorphism 

$$
\rho : \Gamma^* \rightarrow \mathbb{Z}^{2 \times 2}:
$$

\begin{align*}
\rho(a) &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \\
\rho(b) &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \\
\rho(a^{-1}) &= \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \\
\rho(b^{-1}) &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.
\end{align*}

Given an instance of the ICP - $W$, for each pair of words $(w_1, w_2) \in W$, define matrix $A_{w_1,w_2} = \rho(w_1) \oplus \rho(w_2)$.

Let $S$ be a semigroup generated by $\{A_{w_1,w_2}|(w_1, w_2) \in W\}$. Then the ICP instance $W$ has a solution iff $I \in S$.

Open Problem 3 - Determine the decidability of the Identity Problem over $\mathbb{Z}^{3 \times 3}$. 
The Identity Problem in Dimension 2

- The **Identity Problem** is decidable over $\mathbb{Z}^{2 \times 2}$ [Choffrut, Karhumäki, 2005] but it is at least NP-hard [B., Potapov, 2012]

- We shall see some details of the NP-hardness proof.

- A problem is said to be NP-hard if it is at least as difficult as all other problems in the class NP (the class of problems solvable in Non-deterministic Polynomial time).
The Subset Sum Problem (SSP)

The **Subset Sum Problem** is NP-hard and is a very useful tool to show other problems are also NP-hard.

**Problem (Subset Sum Problem)**

*Given a positive integer $x$ and a finite set of positive integer values $S = \{s_1, s_2, \ldots, s_k\}$, does there exist a (nonempty) subset of $S$ which sums to $x$?*

We shall now encode an instance of the subset sum problem into a set of matrices
The Structure of an Identity

Figure: The structure of a product which forms the identity.
The Subset Sum Problem

\[ W = \{ 1 \cdot a^{s_1} \cdot \bar{2}, \quad 2 \cdot a^{s_2} \cdot \bar{3}, \quad \ldots, \quad k \cdot a^{s_k} \cdot (k+1), \quad (k+1) \cdot \bar{a}^x \cdot (k+2), \quad (k+2) \cdot b^{s_1} \cdot (k+3), \quad (k+3) \cdot b^{s_2} \cdot (k+4), \quad \ldots, \quad (2k+1) \cdot b^{s_k} \cdot (2k+2), \quad (2k+2) \cdot \bar{b}^x \cdot \bar{1} \} \subseteq \Sigma^* , \]

where \( \Sigma = \{ 1, 2, \ldots, 2k+2, \bar{1}, \bar{2}, \ldots, (2k+2), a, b, \bar{a}, \bar{b} \} \) is an alphabet and \( \bar{z} \) denotes \( z^{-1} \) for all alphabet characters.
The Identity Problem in Dimension 2

- We then encode the set $W_2$ into a set of matrices over $\mathbb{N}^{2 \times 2}$ and ensure that the representation size of the matrices is polynomial in the size of the subset sum instance to complete the proof.
The Identity Problem in Dimension 2

As a corollary, the following problems are also therefore NP-hard:

1. Determining if the intersection of two finitely generated $2 \times 2$ integral matrix semigroups is empty.
2. Given a finite set of $2 \times 2$ integer matrices, determining if they form a group.
3. The ZRUC($k$, 2) (zero-in-the-right-upper-corner) problem.
4. Determining whether a finitely generated $2 \times 2$ integer matrix semigroup contains any diagonal matrix.
5. The **Scalar/Vector Reachability Problems** over $2 \times 2$ integer matrices.
We have seen a variety of problems on low dimensional, finitely generated matrix semigroups.

Connections between combinatorics on words, automata theory and matrix semigroups.
Selected References