

 $PAMs \rightarrow Matrix Problems \rightarrow Linear Recurrences$

Reachability problems in linear maps and matrix semigroups

Igor Potapov University of Liverpool

MIR@W day, 11 March 2024 Mathematical Interdisciplinary Research at Warwick Computation in Mathematics and Mathematics in Computation



20

Reachability Problems

Given: An initial state X, a target state Y and a set of transformations F

Question: Does a state Y is **reachable** from X following a sequence of transformations from F?





RP24: INTERNATIONAL CONFERENCE ON REACHABILITY PROBLEMS 2024

Overview Submission Dates CFP PC Invited Venue Travel Accommodation PROGRAM

The 18th International Conference on Reachability Problems - RP 2024

September 25-27, TU Wien, Vienna, Austria

The 18th International Conference on Reachability Problems (RP'24) is being organised as a *phyical meeting* by the <u>Formal Methods in Systems</u> <u>Engineering Research Unit</u> of the <u>Faculty of Informatics</u> at the <u>TU Wien</u>.

The conference is aimed at gathering together scholars from diverse disciplines and backgrounds interested in reachability problems that appear in

- Algebraic structures
- Automata theory and formal languages
- · Computational game theory
- · Concurrency and distributed computation
- · Decision procedures in computational models
- Hybrid dynamical systems
- Logic and model checking
- Verification of finite and infinite-state systems





Abstracts: May 27, 2024 Original full papers: May 30, 2024

From affine maps to Matrix Semigroups



- If N = 3 and $\rho_i = 1/3$, the above dynamics it is equivalent to studying the movement of a particle inside the equilateral triangle
- Every time the particle touches one of the edges the direction of its trajectory changes following the vector (in the above case perpendicular to that edge).

Theorem. Pseudo-Billiard System (PBS) is equivalent to Piecewise Affine Map (PAM) [SKP, IJFCS 2008]

Pseudo billiard dynamics ("strange billiard")











Reachability for PAMs

Piecewise affine maps (PAMs) are frequently used as a reference model to show the openness of the reachability questions in other systems. $map(x) \\ \{ if x=y then halt \\ if x \in I_1 then \\ map(ax+b) \\ else map(cx+d) \end{cases}$

OPEN PROBLEM even in case of two intervals

$$f(x) = \begin{cases} ax+b, & cx+d \\ I_1 & I_2 \\ ax+b, & x \in I_1 \\ cx+d, & x \in I_2 \end{cases}$$
 rational numbers

<u>Given</u>: some initial point x_0 and PAM f(x)<u>Question</u>: Is y is reachable from x_0 after a finite number of iterations?

$$f(x_0): x_0 \longrightarrow x_1 \longrightarrow x_2 \longrightarrow x_3 \longrightarrow \dots \longrightarrow x_i \longrightarrow \dots$$

Known to be undecidable in dimension two.





- The Bernoulli shift is a simple example of chaotic map
- orbits are dense;
- the system is sensitive to initial conditions.

However the **reachability problem** for it is trivially decidable.

x₀=1.0101010101011

i.e. starting from any rational number in binary representation 2x - shift of the number and 2x-1 - shift and removal of one.

$$\beta \text{-expansion} \quad x = \sum_{i=1}^{\infty} w(i) \frac{1}{\beta^{i}}$$

$$w: \mathbb{N} \to \{0, 1, \dots, \lceil \beta \rceil - 1\}$$

Any number can be written in any nonintegral base $\beta > 1$

For example $0.102_{[5/2]} = 66/125_{[5/2]} = 1 \cdot (2/5) + 0 \cdot (2/5)^2 + 2 \cdot (2/5)^3$



Fig. 1. A non-deterministic PAM for $\frac{5}{2}$ -expansion

The Target Discounted-Sum 0-1 problem (TDS_{01}) Given a rational non-integer $\beta > 1$ and a rational number $x \in [0,1]$ decide whether there is a sequence $w : \mathbb{N} \to \{0,1\}$ of zeros and ones such that $x = \sum_{i=1}^{\infty} w(i) \frac{1}{\beta^i}$. In this sum a factor $\frac{1}{\beta}$ is called as discounted factor.

A Case of $\beta < 2$ is decidable and $\beta > 2$ is open .

Reachability in full PAMs => Reachability in Matrix semigroups



Reachability in PAM = > Point-to-point reachability in Nondeterministic map $f_1^{-1}(x), f_2^{-1}(x), f_3^{-1}(x)$

Reachability for full PAMS with two intervals is decidable

Olivier Bournez, Oleksiy Kurganskyy, Igor Potapov: Reachability Problems for One-Dimensional Piecewise Affine Maps. Int. J. Found. Comput. Sci. 29(4): 529-549 (2018)

Decision Problems in Matrix Semigroups



II. A Memoir on the Theory of Matrices. By ARTHUR CAYLEY, Esq., F.R.S.

Received December 10, 1857,-Read January 14, 1858.

The term matrix might be used in a more general sense, but in the present memoir I consider only square and rectangular matrices, and the term matrix used without qualification is to be understood as meaning a square matrix; in this restricted sense, a set of quantities arranged in the form of a square, e. g.

$$\left(\begin{array}{c} a \;,\; b \;,\; c \\ a' \;,\; b' \;,\; c' \\ a'' \;,\; b'' \;,\; c'' \end{array}
ight)$$

is said to be a matrix. The notion of such a matrix arises naturally from an abbreviated notation for a set of linear equations, viz. the equations

$$X = ax + by + cz,$$

$$Y = a'x + b'y + c'z,$$

$$Z = a''x + b''y + c''z,$$

may be more simply represented by

$$(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = (a, b, c) (x, y, z) \begin{vmatrix} a', b', c' \\ a'', b'', c'' \end{vmatrix}$$

and the consideration of such a system of equations leads to most of the fundamental notions in the theory of matrices. It will be seen that matrices (attending only to those of the same order) comport themselves as single quantities; they may be added, multiplied or compounded together, &c.: the law of the addition of matrices is precisely similar to that for the addition of ordinary algebraical quantities; as regards their multiplication (or composition), there is the peculiarity that matrices are not in general convertible; it is nevertheless possible to form the powers (positive or negative, integral or fractional) of a matrix, and thence to arrive at the notion of a rational and integral function, or generally of any algebraical function, of a matrix. I obtain the remarkable theorem that any matrix whatever satisfies an algebraical equation of its own order, the coefficient of the highest power being unity, and those of the other



Definitions

Let F be a finite collection of matrices. Then $\langle F \rangle$ denotes the multiplicative semigroup (with identity) generated by F, i.e, $M \in \langle F \rangle$ iff M = I or there are $M_1, \ldots, M_n \in F$ such that $M = M_1 \cdots M_n$.

Membership problem

Let M be an $n \times n$ matrix and F be a finite collection of $n \times n$ matrices. Determine whether $M \in \langle F \rangle$, that is, whether M can be presented as a product of matrices from F.

Other problems:

Decide whether a semigroup S

- contains the zero matrix (Mortality Problem)
- contains the identity matrix (Identity Problem)
- is free, bounded, finite, etc.

Variants of parametrized membership

- Vector reachability (Decide for given vectors u and v whether there exists a matrix M in S such that $M \cdot u = v$)
- **Polyhedron-hitting** (Decide for a given polyhedron V and vector u whether there exists a matrix M such that $M \cdot u \in V$)
- Scalar reachability (Decide for a given vectors u, v and a scalar λ whether exists $M \in S$ such that $u^{\mathsf{T}} \cdot M \cdot v = \lambda$)
- Freeness (Decide whether every matrix product in *S* is unique, i.e. whether it is a code).

The Mortality problem over $\mathbb{Q}^{d \times d}$



Identity Problem



Identity problem: Decide whether the identity matrix belongs to a matrix semigroup S.

- Undecidable for SL(4,Z)
- Open for 3x3 matrices over Z,Q,C
- NP-complete for GL(2,Z)

Identity Correspondence Problem

• The Identity Correspondence Problem: Given a set of pairs of words over a binary group alphabet, can they simultaneously equal the empty (identity) word?



Identity Correspondence Problem is undecidable [Bell, Potapov, Int. J. Found. Comput. Sci. 21(6): 963-978 (2010)]

Identity problem

- Identity Correspondence Problem is Undecidable for 48 pairs of words over a group alphabet.
- Identity problems for SL(4,Z) is Undecidable, e.g. to check whether a given finitely generated matrix semigroup contains an identity matrix.

Given a semigroup S generated by **eight** 4 × 4 integer matrices with a determinant one(e.g. from SL(4,Z) , determining whether the identity matrix belongs to S is undecidable. [ICALP 2018]

GL(2,Z)

GL(2,Z)

GL(2,Q)

GL(2,Z)

GL(2,Q)

- The identity problem is
 - open for SL(3,Z), but
 - decidable and NP-complete from SL(2,Z) [SODA 2017]
 - decidable for Flat Rational Subsets of GL(2,Q) [ISSAC 2020]
 - decidable for unitriangular UT(4,Z). [Dong, MFCS 2022]

Open problem: Membership/Identity problem for matrix semigroup with generators from GL(2,Q)

$\mathsf{SL}(2,\mathbb{Z}) \leq \mathsf{SA}(2,\mathbb{Z}) \leq \mathsf{SL}(3,\mathbb{Z})$

• Ruiwen Dong shown that the Identity problem is NP-complete for SA(2,Z) [LICS 2023]

$$\mathsf{SA}(2,\mathbb{Z}) \coloneqq \left\{ \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix} \middle| A \in \mathsf{SL}(2,\mathbb{Z}), \boldsymbol{a} \in \mathbb{Z}^2 \right\}$$

Special Affine group $SA(2, \mathbb{Z}) = \mathbb{Z}^2 \rtimes SL(2, \mathbb{Z})$

Ruiwen Dong. The Identity Problem in the special affine group of Z², LICS 2023

SL(2,Z) vs SL(3,Z)

 $SL(2, \mathbb{Z}) = \langle S, T \mid S^4 = I_2, (ST)^6 = I_2 \rangle$ $SL(3, \mathbb{Z}) = \langle X, Y, Z \mid X^3 = Y^3 = Z^2 = (XZ)^3 =$ $(YZ)^3 = (X^{-1}ZXY)^2 = (Y^{-1}ZYX)^2 = (XY)^6 = I_3 \rangle$

$$x = \left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{array}\right), y = \left(\begin{array}{ccc} 1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{array}\right), \ z = \left(\begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -1 & -1 \end{array}\right)$$



Heisenberg group

In <u>mathematics</u>, the **Heisenberg group** H, named after <u>Werner Heisenberg</u>, is the <u>group</u> of 3×3 <u>upper triangular</u> <u>matrices</u> of the form

$$M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

under the operation of matrix multiplication,



The Heisenberg subgroup of SL(3,Z) is generated by

$$(zy^{2}zx^{2})^{2} = y^{2}xzy^{2}x^{2} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ (xy^{2}z)^{2} = z(xy)^{2}zy = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$(x^{2}zy^{2}z)^{2} = x^{2}y^{2}xzy^{2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Identity for Heisenberg Matrices over Gaussian rational Q(i)

Problem 1 (Identity Problem). Let S be a matrix semigroup generated by a finite set of $n \times n$ matrices over $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{A}, \mathbb{Q}(i), \ldots$ Is the identity matrix I in the semigroup, i.e., does $I \in S$ hold?

Theorem 1. Let $G \subseteq H(n, \mathbb{Q}(i))$ be a finite set of matrices. Then it is decidable in polynomial time if $I \in \langle G \rangle$.

Corollary 1. It is decidable in polynomial time whether a finite set of matrices $G \subseteq H(n, \mathbb{Q}(i))$ forms a group.

In the three-dimensional case, the product of two Heisenberg matrices is given by:

$$egin{pmatrix} 1 & a & c \ 0 & 1 & b \ 0 & 0 & 1 \end{pmatrix} egin{pmatrix} 1 & a' & c' \ 0 & 1 & b' \ 0 & 0 & 1 \end{pmatrix} = egin{pmatrix} 1 & a+a' & c+ab'+c' \ 0 & 1 & b+b' \ 0 & 0 & 1 \end{pmatrix}.$$

We define the commutator [M₁, M₂] of M1 and M2 by [M₁, M₂] = $a_1^T b_2 - a_2^T b_1 \in Q(i)$.

H(n, Q(i)), it is clear that
$$M_1M_2 - M_2M_1 = \begin{pmatrix} 0 \ \mathbf{0}^T \ \mathbf{a}_1^T \mathbf{b}_2 - \mathbf{a}_2^T \mathbf{b}_1 \\ \mathbf{0} \ \mathbf{0} & \mathbf{0} \\ 0 \ \mathbf{0}^T & \mathbf{0} \end{pmatrix}$$
,
a + bi = r exp(iy), where r \in R and y $\in [0, \pi)$

 γ is the angle of the commutator if [M1,M2] = r exp(i γ)

The identity matrix can always be constructed using a solution that contains four particular matrices.

Let M1, M2, M3 and M4 be such that

- [M1, M2] = r exp(iγ)
- [M3, M4] = r' exp(iγ')

where pairs M1,M2 and M3,M4 have different commutator angles.

This difference in order and the different commutator angles ensures that we can control the top right corner elements to construct the identity matrix.



$$a_n = 5_{n-1} - 6a_{n-2}$$

Linear Recurrences vs Matrix Equations

$$A_1^{m_1}A_2^{m_2}\ldots A_t^{m_t}=\mathbf{O}_{k,k}$$

Matrix Equations

Given integral matrices $X_1, X_2, ..., X_k \in \mathbb{Z}^{n \times n}$, 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.



 $A^{x}B^{y=C}$ is decidable even if A and B do not commute

Skolem-Pisot Problem

A LRS may be written in the form:

 $u_k = a_{n-1}u_{k-1} + a_{n-2}u_{k-2} + \dots + a_0u_{k-n},$

for $k \ge n$ where $u_0, u_1, \ldots, u_{n-1} \in \mathbb{Z}$ are the initial inputs and $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ are the recurrence coefficients.

Skolem's Problem - Given a LRS $(u_k)_{k=0}^{\infty} \subseteq \mathbb{Z}$, is it algorithmically decidable if there exists some $j \ge 0$ such that $u_j = 0$?

Define the matrix $A \in \mathbb{Z}^{n \times n}$ by:

 $A = \left(egin{array}{cccccccccc} 0 & 1 & 0 & \cdots & 0 \ 0 & 0 & 1 & \cdots & 0 \ dots & dots & \ddots & \ddots & dots \ 0 & 0 & 0 & \cdots & 1 \ a_0 & a_1 & a_2 & \cdots & a_{n-1} \end{array}
ight)$

This is the companion matrix of the (characteristic) polynomial of the linear recurrent sequence. If $u = (u_0, u_1, \ldots, u_{n-1})^T$ then $A^k u = (u_k, u_{k+1}, \ldots, u_{k+n-1})^T$.

Linear Recurrent Sequences (LRS)

Now we shall extend this matrix by 1 dimension to give:

$$B = \begin{pmatrix} A & Au \\ \overline{0} & 0 \end{pmatrix} \in \mathbb{Z}^{(n+1) \times (n+1)},$$

where $\overline{0}$ is the zero vector of appropriate size. It is not difficult to now see that $u_k = B_{1,n}^k$ for $k \ge 1$. This can be proven directly with the Cayley-Hamilton theorem. Matrix Equations to Skolem: A^xB^yC^z=0

Theorem. [Inf. Comput. 281]

Let F be the ring of integers Z (Q or A). Then the ABC problem for matrices from $F^{k\times k}$ is Turing reducible to the **Skolem problem** of depth k over F.

Х

B

=

1

Theorem. *The ABC problem is decidable for*

- 3 × 3 matrices over algebraic numbers and
- 4 × 4 matrices over real algebraic numbers.
- The same kind of ABCD problem may have non-semilinear set of solutions.



Linear Recurrence Automata

$$a_n = 5_{n-1} - 6a_{n-2}$$

A linear recurrence automaton $\mathcal{A} = (Q, E, a, q_0, Q_{acc})$ of depth $k \in \mathbb{N}$ over a ring \mathbb{F} consists of

- a (finite) directed graph (Q, E), possibly with self-loops and parallel edges, whose vertices are called *states*;
- for each edge $e \in E$, a k-tuple $a^{(e)} = (a_0^{(e)}, \dots, a_{k-1}^{(e)}) \in \mathbb{F}^k$;
- a vertex $q_0 \in Q$ called the *initial state*; and
- and a set $Q_{\text{acc}} \subseteq Q$ of final states.

This automaton \mathcal{A} is said to be *satisfied* by a sequence $(u_t)_{t\in\mathbb{N}}\in\mathbb{F}^{\mathbb{N}}$ if there is a walk $q_0e_0q_1e_1\ldots$ (starting at the initial state) such that

$$u_{t+k} = a_{k-1}^{(e_t)} u_{t+k-1} + \dots + a_0^{(e_t)} u_t \tag{1}$$

for each $t \in \mathbb{N}$.

Number of States - s Number of different linear recurrences - m

Depth (order) of Recurrences - k

Definition 1. The class of linear recurrence automata $\mathcal{A} = (Q, E, a, q_0, Q_{\text{acc}})$ of order k over \mathbb{F} with |Q| = s and $|\{a^{(e)} : e \in E\}| = m$ is denoted by $LRA_{\mathbb{F}}(s, m, k)$. **Theorem 1.** Let \mathcal{F} be a field and S be a matrix semigroup generated by $M_1, \ldots, M_r \in \mathcal{F}^{n \times n}$. The Scalar Reachability for a semgroup S can be reduced to to the 1-Subsequence Reachability Problem for a Linear Recurrence Automata

$$\mathcal{A} \in LRA_{\mathcal{F}}(r(n-1)+2, rn+1, 2n-1),$$

the Vector Reachability to the n-Subsequence Reachability for

$$\mathcal{A} \in LRA_{\mathcal{F}}(r(n-1)+1, rn, 2n-1)$$

and the Membership Problem for the n^2 -Subsequence Reachability

$$\mathcal{A} \in LRA_{\mathcal{F}}(r(n^2 - 1) + 1, n^2, 2n^2 - 1).$$

Finally the question about the scalar reachability can be now reduced to the questions whether a recurrent linear automata could generate the value λ in the final state s_f .

Theorem 2. 1-Subsequence Reachability Problem for a Linear Recurrence Automata $\mathcal{A} \in LRA_{\mathcal{F}}(s, m, k)$, can be reduced to the Scalar Reachability and *n*-Subsequence Reachability to the Vector Reachability.

Linear recurrence automata of low-order k

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \dots + a_k u_{n-k}$$

Theorem 3. 1-Subsequence Reachability Problem for a Linear Recurrence Automata $\mathcal{A} \in LRA_{\mathcal{F}}(s, m, 1)$, i.e. with linear recurrences of the order one is decidable in polynomial time.

Theorem 4. 1-Subsequence Reachability Problem for a Linear Recurrence Automata $\mathcal{A} \in LRA_{\mathcal{F}}(s, m, 2)$, i.e. with linear recurrences of the order two is *PSPACE-hard*.

Theorem 5. 2-Subsequence Reachability Problem for a Linear Recurrence Automata $\mathcal{A} \in LRA_{\mathcal{F}}(7,11,3)$, i.e. with linear recurrences of the order three is undecidable.

Chasing Butterflies



"Chasse aux Papillons" (Chasing Butterflies) by Berthe Morisot (1841-1895), oil on canvas, 1874 Membership, Vector Reachability Freeness in SL(3,Z), Q^{2x2},SL(2,Q), C^{2x2}, SL(2,C), H, Z^{2x2} A high-profile event with 80-100 participants. The audience consists of established academics running the UUKi projects with Ukraine, heads of international offices and global engagement of UK universities, PVC research, etc.

https://www.digital-ukraine.co.uk/ UK-Ukraine Research Twinning Showcase and Networking 26-27 March 2024



REMOTE * ScienceFor-Ukraine NOW!



scienceforukraine.eu