Solvability of Matrix-Exponential Equations

Joël Ouaknine [*] [†]
University of Oxford
joel@cs.ox.ac.uk

Amaury Pouly [†]
University of Oxford
amaury.pouly@cs.ox.ac.uk

João Sousa-Pinto [⋆] [‡]
University of Oxford
jspinto@cs.ox.ac.uk

James Worrell [⋆]
University of Oxford
jbw@cs.ox.ac.uk

Abstract

We consider a continuous analogue of (Babai et al. 1996)'s and (Cai et al. 2000)'s problem of solving multiplicative matrix equations. Given $k+1$ square matrices $A_1, \ldots, A_k, C$, all of the same dimension, whose entries are real algebraic, we examine the problem of deciding whether there exist non-negative reals $t_1, \ldots, t_k$ such that

$$\prod_{i=1}^{k} \exp(A_i t_i) = C.$$

We show that this problem is undecidable in general, but decidable under the assumption that the matrices $A_1, \ldots, A_k$ commute. Our results have applications to reachability problems for linear hybrid automata.

Our decidability proof relies on a number of theorems from algebraic and transcendental number theory, most notably those of Baker, Kronecker, Lindemann, and Masser, as well as some useful geometric and linear-algebraic results, including the Minkowski-Weyl theorem and a new (to the best of our knowledge) result about the uniqueness of strictly upper triangular matrix logarithms of upper unitriangular matrices. On the other hand, our undecidability result is shown by reduction from Hilbert's Tenth Problem.

Keywords exponential matrices, matrix reachability, matrix logarithms, commuting matrices, hybrid automata

Categories and Subject Descriptors F.2 [*Analysis of Algorithms and Problem Complexity*]: Miscellaneous

1. Introduction

Reachability problems are a fundamental staple of theoretical computer science and verification, one of the best-known examples being the Halting Problem for Turing machines. In this paper, our motivation originates from systems that evolve continuously subject to linear differential equations; such objects arise in the analysis of a range of models, including linear hybrid automata, continuous-time Markov chains, linear dynamical systems and cyber-physical systems as they are used in the physical sciences and engineering—see, e.g., (Alur 2015).

More precisely, consider a system consisting of a finite number of discrete locations (or control states), having the property that the continuous variables of interest evolve in each location according to some linear differential equation of the form $\dot{\boldsymbol{x}} = A\boldsymbol{x}$; here $\boldsymbol{x}$ is a vector of continuous variables, and A is a square 'rate' matrix of appropriate dimension. As is well-known, in each location the closed form solution $\boldsymbol{x}(t)$ to the differential equation admits a matrix-exponential representation of the form $\boldsymbol{x}(t) = \exp(At)\boldsymbol{x}(0)$. Thus if a system evolves through a series of k locations, each with rate matrix A_i, and spending time $t_i \geq 0$ in each location, the overall effect on the initial continuous configuration is given by the matrix

$$\prod_{i=1}^{k} \exp(A_i t_i)\,,$$

viewed as a linear transformation on $\boldsymbol{x}(0)$.[1]

A particularly interesting situation arises when the matrices A_i commute; in such cases, one can show that the order in which the locations are visited (or indeed whether they are visited only once or several times) is immaterial, the only relevant data being the total time spent in each location. Natural questions then arise as to what kinds of linear transformations can thus be achieved by such systems.

1.1 Related Work

Consider the following problems, which can be seen as discrete analogues of the question we deal with in this paper.

DEFINITION 1 (Matrix Semigroup Membership Problem). *Given $k+1$ square matrices $A_1, \ldots, A_k, C$, all of the same dimension, whose entries are algebraic, does the matrix C belong to the multiplicative semigroup generated by $A_1, \ldots, A_k$?*

DEFINITION 2 (Solvability of Multiplicative Matrix Equations). *Given $k+1$ square matrices $A_1, \ldots, A_k, C$, all of the same di-*

[*] Supported by the EPSRC

[†] Supported by the ERC grant AVS-ISS

[‡] Supported by the ERC grant ALGAME

[1] In this motivating example, we are assuming that there are no discrete resets of the continuous variables when transitioning between locations.

mension, whose entries are algebraic, does the equation

$$\prod_{i=1}^{k} A_i^{n_i} = C$$

admit any solution $n_1, \dots, n_k \in \mathbb{N}$*?*

In general, both problems have been shown to be undecidable, in (Paterson 1970) and (Bell et al. 2008), by reductions from Post's Correspondence Problem and Hilbert's Tenth Problem, respectively.

When the matrices $A_1, \dots, A_k$ commute, these problems are identical, and known to be decidable, as shown in (Babai et al. 1996), generalising the solution of the matrix powering problem, shown to be decidable in (Kannan and Lipton 1986), and the case with two commuting matrices, shown to be decidable in (Cai et al. 2000).

See (Halava 1997) for a relevant survey, and (Choffrut and Karhumäki 2005) for some interesting related problems.

The following continuous analogue of (Kannan and Lipton 1986)'s Orbit Problem was shown to be decidable in (Hainry 2008):

DEFINITION 3 (Continuous Orbit Problem). *Given an* $n \times n$ *matrix* A *with algebraic entries and two* n*-dimensional vectors* $\boldsymbol{x}, \boldsymbol{y}$ *with algebraic coordinates, does there exist a non-negative real* t *such that* $\exp(At)\boldsymbol{x} = \boldsymbol{y}$*?*

The paper (Chen et al. 2015) simplifies the argument of (Hainry 2008) and shows polynomial-time decidability. Moreover, a continuous version of the Skolem-Pisot problem was dealt with in (Bell et al. 2010), where a decidability result is presented for some instances of the problem.

As mentioned earlier, an important motivation for our work comes from the analysis of hybrid automata. In addition to (Alur 2015), excellent background references on the topic are (Henzinger et al. 1995; Henzinger 1996).

1.2 Decision Problems

We start by defining three decision problems that will be the main object of study in this paper: the *Matrix-Exponential Problem*, the *Linear-Exponential Problem*, and the *Algebraic-Logarithmic Integer Programming* problem.

DEFINITION 4. *An instance of the Matrix-Exponential Problem (MEP) consists of square matrices* $A_1, \dots, A_k$ *and* C*, all of the same dimension, whose entries are real algebraic numbers. The problem asks to determine whether there exist real numbers* $t_1, \dots, t_k \geq 0$ *such that*

$$\prod_{i=1}^{k} \exp(A_i t_i) = C\,. \tag{1}$$

We will also consider a generalised version of this problem, called the *Generalised MEP*, in which the matrices $A_1, \dots, A_k$ and C are allowed to have complex algebraic entries and in which the input to the problem also mentions a polyhedron $\mathcal{P} \subseteq \mathbb{R}^{2k}$ that is specified by linear inequalities with real algebraic coefficients. In the generalised problem we seek $t_1, \dots, t_k \in \mathbb{C}$ that satisfy (1) and such that the vector $(\mathrm{Re}(t_1), \dots, \mathrm{Re}(t_k), \mathrm{Im}(t_1), \dots, \mathrm{Im}(t_k))$ lies in $\mathcal{P}$.

In the case of commuting matrices, the Generalised Matrix Exponential Problem can be analysed block-wise, which leads us to the following problem:

DEFINITION 5. *An instance of the Linear-Exponential Problem (LEP) consists of a system of equations*

$$\exp\left(\sum_{i \in I} \lambda_i^{(j)} t_i\right) = c_j \exp(d_j) \quad (j \in J), \tag{2}$$

where I *and* J *are finite index sets, the* $\lambda_i^{(j)}$*,* c_j *and* d_j *are complex algebraic constants, and the* t_i *are complex variables, together with a polyhedron* $\mathcal{P} \subseteq \mathbb{R}^{2k}$ *that is specified by a system of linear inequalities with algebraic coefficients. The problem asks to determine whether there exist* $t_1, \dots, t_k \in \mathbb{C}$ *that satisfy the system (2) and such that* $(\mathrm{Re}(t_1), \dots, \mathrm{Re}(t_k), \mathrm{Im}(t_1), \dots, \mathrm{Im}(t_k))$ *lies in* $\mathcal{P}$.

To establish decidability of the Linear-Exponential Problem, we reduce it to the following *Algebraic-Logarithmic Integer Programming* problem. Here a *linear form in logarithms of algebraic numbers* is a number of the form $\beta_0 + \beta_1 \log(\alpha_1) + \dots + \beta_m \log(\alpha_m)$, where $\beta_0, \alpha_1, \beta_1, \dots, \alpha_m, \beta_m$ are algebraic numbers and log denotes a fixed branch of the complex logarithm function.

DEFINITION 6. *An instance of the Algebraic-Logarithmic Integer Programming Problem (ALIP) consists of a finite system of equations of the form*

$$A\boldsymbol{x} \leq \frac{1}{\pi}\boldsymbol{b}$$

where A *is an* $m \times n$ *matrix with real algebraic entries and where the coordinates of* $\boldsymbol{b}$ *are real linear forms in logarithms of algebraic numbers. The problem asks to determine whether such a system admits a solution* $\boldsymbol{x} \in \mathbb{Z}^n$.

1.3 Paper Outline

After introducing the main mathematical techniques that are used in the paper, we present a reduction from the Generalised Matrix Exponential Problem with commuting matrices to the Linear-Exponential Problem, as well as a reduction from the Linear-Exponential Problem to the Algebraic-Logarithmic Integer Programming Problem, before finally showing that the Algebraic-Logarithmic Integer Programming Problem is decidable. By way of hardness, we will prove that the Matrix Exponential Problem is undecidable (in the non-commutative case), by reduction from Hilbert's Tenth Problem.

2. Mathematical Background

2.1 Number Theory and Diophantine Approximation

A number $\alpha \in \mathbb{C}$ is said to be *algebraic* if there exists a non-zero polynomial $p \in \mathbb{Q}[x]$ for which $p(\alpha) = 0$. A complex number that is not algebraic is said to be *transcendental*. The monic polynomial $p \in \mathbb{Q}[x]$ of smallest degree for which $p(\alpha) = 0$ is said to be the minimal polynomial of α. The set of algebraic numbers, denoted by $\overline{\mathbb{Q}}$, forms a field. Note that the complex conjugate of an algebraic number is also algebraic, with the same minimal polynomial. It is possible to represent and manipulate algebraic numbers effectively, by storing their minimal polynomial and a sufficiently precise numerical approximation. An excellent course (and reference) in computational algebraic number theory can be found in (Cohen 1993). Efficient algorithms for approximating algebraic numbers were presented in (Pan 1996).

Given a vector $\boldsymbol{\lambda} \in \overline{\mathbb{Q}}^m$, its *group of multiplicative relations* is defined as

$$L(\boldsymbol{\lambda}) = \{\boldsymbol{v} \in \mathbb{Z}^m : \boldsymbol{\lambda}^{\boldsymbol{v}} = 1\}.$$

Moreover, letting log represent a fixed branch of the complex logarithm function, note that $\log(\alpha_1), \dots, \log(\alpha_m)$ are linearly independent over $\mathbb{Q}$ if and only if

$$L(\alpha_1,\ldots,\alpha_m)=\{\mathbf{0}\}.$$

Being a subgroup of the free abelian group $\mathbb{Z}^m$, the group $L(\boldsymbol{\lambda})$ is also free and admits a finite basis.

The following theorem, due to David Masser, allows us to effectively determine $L(\boldsymbol{\lambda})$, and in particular decide whether it is equal to $\{\mathbf{0}\}$. This result can be found in (Masser 1988).

THEOREM 1 (Masser). *The free abelian group $L(\boldsymbol{\lambda})$ has a basis $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_l\in\mathbb{Z}^m$ for which*

$$\max_{1\le i\le l,1\le j\le m}|v_{i,j}|\le (D\log H)^{O(m^2)}$$

where H and D bound respectively the heights and degrees of all the λ_i.

We will need the following results of Baker (Baker 1975). The first one, together with Masser's theorem, allows us to eliminate all algebraic relations in the description of linear forms in logarithms of algebraic numbers.

THEOREM 2 (Baker). *Let $\alpha_1,\ldots,\alpha_m\in\overline{\mathbb{Q}}\setminus\{0\}$. If*

$$\log(\alpha_1),\ldots,\log(\alpha_m)$$

are linearly independent over $\mathbb{Q}$, then

$$1,\log(\alpha_1),\ldots,\log(\alpha_m)$$

are linearly independent over $\overline{\mathbb{Q}}$.

The next result essentially implies that one can effectively check whether a linear form in logarithms of algebraic numbers equals zero. Noting that the set of linear forms in logarithms of algebraic numbers is closed under addition and multiplication by algebraic numbers, it easily follows that one can effectively compare two linear forms in logarithms of algebraic numbers. It is also closed under complex conjugation. See (Baker 1975) and (Baker and Wüstholz 1993).

THEOREM 3 (Baker). *Let $\alpha_1,\ldots,\alpha_m$ be non-zero algebraic numbers with degrees at most d and heights at most A. Further, let $\beta_0,\ldots,\beta_m$ be algebraic numbers with degrees at most d and heights at most B, where $B\ge 2$. Write*

$$\Lambda=\beta_0+\beta_1\log(\alpha_1)+\cdots+\beta_m\log(\alpha_m).$$

Then either $\Lambda=0$ or $|\Lambda|>B^{-C}$, where C is an effectively computable number depending only on m, d, A, and the chosen branch of the complex logarithm.

The theorem below was proved by Ferdinand von Lindemann in 1882, and later generalised by Karl Weierstrass in what is now known as the Lindemann-Weierstrass theorem. As a historical note, this result was behind the first proof of transcendence of π, which immediately follows from it.

THEOREM 4 (Lindemann). *If $\alpha\in\overline{\mathbb{Q}}\setminus\{0\}$, then e^α is transcendental.*

We will also need the following result, due to Leopold Kronecker, on simultaneous Diophantine approximation, which generalises Dirichlet's Approximation Theorem. We denote the *group of additive relations* of $\boldsymbol{v}$ by

$$A(\boldsymbol{v})=\{\boldsymbol{z}\in\mathbb{Z}^d:\boldsymbol{z}\cdot\boldsymbol{v}\in\mathbb{Z}\}.$$

Throughout this paper, dist refers to the l_1 distance.

THEOREM 5 (Kronecker). *Let $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_{\boldsymbol{k}}\in\mathbb{R}^d$ and $\boldsymbol{\beta}\in\mathbb{R}^d$. The following are equivalent:*

1. *For any $\varepsilon>0$, there exists $\boldsymbol{n}\in\mathbb{N}^k$ such that*

$$\operatorname{dist}(\boldsymbol{\beta}+\sum_{i=1}^{k}n_i\boldsymbol{\alpha}_i,\mathbb{Z}^d)\le\varepsilon.$$

2. *It holds that*

$$\bigcap_{i=1}^{k}A(\boldsymbol{\alpha}_i)\subseteq A(\boldsymbol{\beta}).$$

Many of these results, or slight variations thereof, can be found in (Hardy and Wright 1938) and (Cassels 1965).

2.2 Lattices

Consider a matrix $K\in\overline{\mathbb{Q}}^{r\times d}$ and vector $\boldsymbol{k}\in\overline{\mathbb{Q}}^r$. The following proposition shows how to compute a representation of the affine lattice $\{\boldsymbol{x}\in\mathbb{Z}^d:K\boldsymbol{x}=\boldsymbol{k}\}$. Further information about lattices can be found in (Micciancio and Goldwasser 2002) and (Cohen 1993).

PROPOSITION 1. *There exist $\boldsymbol{x}_0\in\mathbb{Z}^d$ and $M\in\mathbb{Z}^{d\times s}$, where $s\le r$, such that*

$$\{\boldsymbol{x}\in\mathbb{Z}^d:K\boldsymbol{x}=\boldsymbol{k}\}=\boldsymbol{x}_0+\{M\boldsymbol{y}:\boldsymbol{y}\in\mathbb{Z}^s\}.$$

Proof. Let θ denote a primitive element of the number field generated by the entries of K and $\boldsymbol{k}$. Let the degree of this extension, which equals the degree of θ, be D. Then for $\boldsymbol{x}\in\mathbb{Z}^d$ one can write

$$\begin{aligned}K\boldsymbol{x}=\boldsymbol{k}&\Leftrightarrow\left(\sum_{i=0}^{D-1}N_i\theta^i\right)\boldsymbol{x}=\sum_{i=0}^{D-1}\boldsymbol{k}_i\theta^i\\&\Leftrightarrow N_i\boldsymbol{x}=\boldsymbol{k}_i,\forall i\in\{0,\ldots,D-1\},\end{aligned}$$

for some integer matrices $N_0,\ldots,N_{D-1}\in\mathbb{Z}^{r\times d}$ and integer vectors $\boldsymbol{k}_0,\ldots,\boldsymbol{k}_{D-1}\in\mathbb{Z}^r$. The solution of each of these equations is clearly an affine lattice, and therefore so is their intersection. □

2.3 Matrix exponentials

Given a matrix $A\in\mathbb{C}^{n\times n}$, its exponential is defined as

$$\exp(A)=\sum_{i=0}^{\infty}\frac{A^i}{i!}.$$

The series above always converges, and so the exponential of a matrix is always well defined. The standard way of computing $\exp(A)$ is by finding $P\in GL_n(\mathbb{C})$ such that $J=P^{-1}AP$ is in Jordan Canonical Form, and by using the fact that $\exp(A)=P\exp(J)P^{-1}$, where $\exp(J)$ is easy to compute. When $A\in\overline{\mathbb{Q}}^{n\times n}$, P can be taken to be in $GL_n(\overline{\mathbb{Q}})$; note that

$$\text{if } J=\begin{pmatrix}\lambda&1&0&\cdots&0\\0&\lambda&1&\cdots&0\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&\lambda&1\\0&0&\cdots&0&\lambda\end{pmatrix}\text{ then}$$

$$\exp(Jt)=\exp(\lambda t)\begin{pmatrix}1&t&\frac{t^2}{2}&\cdots&\frac{t^{k-1}}{(k-1)!}\\0&1&t&\cdots&\frac{t^{k-2}}{(k-2)!}\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&1&t\\0&0&\cdots&0&1\end{pmatrix}.$$

Then $\exp(J)$ can be obtained by setting $t=1$, in particular $\exp(J)_{ij}=\frac{\exp(\lambda)}{(j-i)!}$ if $j\ge i$ and 0 otherwise.

When A and B commute, so must $\exp(A)$ and $\exp(B)$. Moreover, when A and B have algebraic entries, the converse also holds, as shown in (Wermuth 1989). Also, when A and B commute, it holds that $\exp(A)\exp(B) = \exp(A + B)$.

2.4 Matrix logarithms

The matrix B is said to be a logarithm of the matrix A if $\exp(B) = A$. It is well known that a logarithm of a matrix A exists if and only if A is invertible. However, matrix logarithms need not be unique. In fact, there exist matrices admitting uncountably many logarithms. See, for example, (Culver 1966) and (Helton 1968).

A matrix is said to be unitriangular if it is triangular and all its diagonal entries equal 1. Crucially, the following uniqueness result holds:

THEOREM 6. *Given an upper unitriangular matrix $M \in \mathbb{C}^{n\times n}$, there exists a unique strictly upper triangular matrix L such that $\exp(L) = M$. Moreover, the entries of L lie in the number field $\mathbb{Q}(M_{i,j} : 1 \le i, j \le n)$.*

Proof. Firstly, we show that, for any strictly upper triangular matrix T and for any $1 < m < n$ and $i < j$, the term $(T^m)_{i,j}$ is polynomial on the elements of the set $\{T_{r,s} : s - r < j - i\}$. This can be seen by induction on m, as each T^m is strictly upper triangular, and so

$$(T^m)_{i,j} = \sum_{l=1}^{n} (T^{m-1})_{i,l} T_{l,j} = \sum_{l=i+1}^{j-1} (T^{m-1})_{i,l} T_{l,j}.$$

Finally, we show, by induction on $j - i$, that each $L_{i,j}$ is polynomial on the elements of the set

$$\{M_{i,j}\} \cup \{M_{r,s} : s - r < j - i\}.$$

If $j - i \le 0$, then $L_{i,j} = 0$, so the claim holds. When $j - i > 0$, as L is nilpotent,

$$M_{i,j} = \exp(L)_{i,j} = L_{i,j} + \sum_{m=2}^{n-1} \frac{1}{m!} (L^m)_{i,j}$$

$$\Rightarrow L_{i,j} = M_{i,j} - \sum_{m=2}^{n-1} \frac{1}{m!} (L^m)_{i,j}.$$

The result now follows from the induction hypothesis and from our previous claim, as this argument can be used to both construct such a matrix L and to prove that it is uniquely determined. □

2.5 Properties of commuting matrices

We will now present a useful decomposition of $\mathbb{C}^n$ induced by the commuting matrices $A_1, \ldots, A_k \in \mathbb{C}^{n\times n}$. Let $\sigma(A_i)$ denote the spectrum of the matrix A_i. In what follows, let

$$\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \sigma(A_1) \times \cdots \times \sigma(A_k).$$

We remind the reader that $\ker(A_i - \lambda_i)^n$ corresponds to the generalised eigenspace of λ_i of A_i. Moreover, we define the following subspaces:

$$\mathcal{V}_{\boldsymbol{\lambda}} = \bigcap_{i=1}^{k} \ker(A_i - \lambda_i I)^n.$$

Also, let $\Sigma = \{\boldsymbol{\lambda} \in \sigma(A_1) \times \cdots \times \sigma(A_k) : \mathcal{V}_{\boldsymbol{\lambda}} \ne \{\mathbf{0}\}\}$.

THEOREM 7. *For all $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \Sigma$ and for all $i \in \{1, \ldots, k\}$, the following properties hold:*

1. *$\mathcal{V}_{\boldsymbol{\lambda}}$ is invariant under A_i.*
2. *$\sigma(A_i \restriction_{\mathcal{V}_{\boldsymbol{\lambda}}}) = \{\lambda_i\}$.*
3. *$\mathbb{C}^n = \bigoplus_{\boldsymbol{\lambda}\in\Sigma} \mathcal{V}_{\boldsymbol{\lambda}}$.*

Proof. We show, by induction on k, that the subspaces $\mathcal{V}_{\boldsymbol{\lambda}}$ satisfy the properties above.

When $k = 1$, the result follows from the existence of Jordan Canonical Forms. When $k > 1$, suppose that $\sigma(A_k) = \{\mu_1, \ldots, \mu_m\}$, and let $\mathcal{U}_j = \ker(A_k - \mu_j I)^n$, for $j \in \{1, \ldots, m\}$. Again, it follows from the existence of Jordan Canonical Forms that

$$\mathbb{C}^n = \bigoplus_{j=1}^{m} \mathcal{U}_m.$$

In what follows, $i \in \{1, \ldots, k-1\}$ and $j \in \{1, \ldots, m\}$. Now, as A_k and A_i commute, so do $(A_k - \mu_j I)$ and A_i. Therefore, for all $\boldsymbol{v} \in \mathcal{U}_j$, $(A_k - \mu_j I)^n A_i \boldsymbol{v} = A_i (A - \mu_j I)^n \boldsymbol{v} = \mathbf{0}$, so $A_i \boldsymbol{v} \in \mathcal{U}_j$, that is, $\mathcal{U}_j$ is invariant under A_i. The result follows from applying the induction hypothesis to the commuting operators $A_i \restriction_{\mathcal{U}_j}$. □

We will also make use of the following well-known result on simultaneous triangularisation of commuting matrices. See, for example, (Newman 1967).

THEOREM 8. *Given k commuting matrices $A_1, \ldots, A_k \in \overline{\mathbb{Q}}^{n\times n}$, there exists a matrix $P \in GL_n(\overline{\mathbb{Q}})$ such that $P^{-1} A_i P$ is upper triangular for all $i \in \{1, \ldots, k\}$.*

2.6 Convex Polyhedra and Semi-Algebraic Sets

A convex polyhedron is a subset of $\mathbb{R}^n$ of the form $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} \le \boldsymbol{b}\}$, where A is a $d \times n$ matrix and $\boldsymbol{b} \in \mathbb{R}^d$. When all the entries of A and coordinates of $\boldsymbol{b}$ are algebraic numbers, the convex polyhedron $\mathcal{P}$ is said to have an algebraic description.

A set $S \subseteq \mathbb{R}^n$ is said to be semi-algebraic if it is a Boolean combination of sets of the form $\{\boldsymbol{x} \in \mathbb{R}^n : p(\boldsymbol{x}) \ge 0\}$, where p is a polynomial with integer coefficients. Equivalently, the semi-algebraic sets are those definable by the quantifier-free first-order formulas over the structure $(\mathbb{R}, <, +, \cdot, 0, 1)$.

If was shown by Alfred Tarski in (Tarski 1951) that the first-order theory of reals admits quantifier elimination. Therefore, the semi-algebraic sets are precisely the first-order definable sets.

THEOREM 9 (Tarski). *The first-order theory of reals is decidable.*

See (Renegar 1992) and (Basu et al. 2006) for more efficient decision procedures for the first-order theory of reals.

DEFINITION 7 (Hilbert's Tenth Problem). *Given a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_k]$, decide whether $p(\boldsymbol{x}) = 0$ admits a solution $\boldsymbol{x} \in \mathbb{N}^k$. Equivalently, given a semi-algebraic set $S \subseteq \mathbb{R}^k$, decide whether it intersects $\mathbb{Z}^k$.*

The following celebrated theorem, due to Yuri Matiyasevich, will be used in our undecidability proof; see (Matiyasevich 1993) for a self-contained proof.

THEOREM 10 (Matiyasevich). *Hilbert's Tenth Problem is undecidable.*

On the other hand, our proof of decidability of ALIP makes use of some techniques present in the proof of the following result, shown in (Khachiyan and Porkolab 1997):

THEOREM 11 (Khachiyan and Porkolab). *It is decidable whether a given* convex *semi-algebraic set $S \subseteq \mathbb{R}^k$ intersects $\mathbb{Z}^k$.*

2.7 Fourier-Motzkin Elimination

Fourier-Motzkin elimination is a simple method for solving systems of inequalities. Historically, it was the first algorithm used in solving linear programming, before more efficient procedures such as the simplex algorithm were discovered. The procedure consists in isolating one variable at a time and matching all its lower and upper bounds. Note that this method preserves the set of solutions on the remaining variables, so a solution of the reduced system can always be extended to a solution of the original one.

THEOREM 12. *By using Fourier-Motzkin elimination, it is decidable whether a given convex polyhedron $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^n : \pi A\boldsymbol{x} < \boldsymbol{b}\}$, where the entries of A are all real algebraic numbers and those of $\boldsymbol{b}$ are real linear forms in logarithms of algebraic numbers, is empty. Moreover, if $\mathcal{P}$ is non-empty one can effectively find a rational vector $\boldsymbol{q} \in \mathcal{P}$.*

Proof. When using Fourier-Motzkin elimination, isolate each term πx_i, instead of just isolating the variable x_i. Note that the coefficients of the terms πx_i will always be algebraic, and the loose constants will always be linear forms in logarithms of algebraic numbers, which are closed under multiplication by algebraic numbers, and which can be effectively compared by using Baker's Theorem. □

3. Example

Let $\lambda_1, \lambda_2 \in \mathbb{R} \cap \bar{\mathbb{Q}}$ such that $\lambda_1 > \lambda_2$ and consider the following commuting matrices $A_1, A_2 \in (\mathbb{R} \cap \bar{\mathbb{Q}})^{2\times 2}$:

$$A_i = \begin{pmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{pmatrix}, i \in \{1,2\}.$$

One can easily see that

$$\begin{aligned} \exp(A_i t_i) &= \exp(\lambda_i t_i I)\exp(t_i(A_i - \lambda_i I)) \\ &= \exp(\lambda_i t_i)\exp\begin{pmatrix} 0 & t_i \\ 0 & 0 \end{pmatrix} \\ &= \exp(\lambda_i t_i)\begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}, i \in \{1,2\}. \end{aligned}$$

Let $c_1, c_2 \in \mathbb{R} \cap \bar{\mathbb{Q}}$ such that $c_1, c_3 > 0$, and let

$$C = \begin{pmatrix} c_1 & c_2 \\ 0 & c_1 \end{pmatrix}.$$

Note that, in this case, we are searching for a solution in an unbounded polyhedron, which we can do in this particular case, but not in general.

We would like to determine whether there exists a solution $t_1, t_2 \in \mathbb{R}$, $t_1, t_2 \geq 0$ to

$$\exp(A_1 t_1)\exp(A_2 t_2) = C$$

This amounts to solving the following system of equations:

$$\begin{cases} \exp(\lambda_1 t_1 + \lambda_2 t_2) = c_1 \\ (t_1 + t_2)\exp(\lambda_1 t_1 + \lambda_2 t_2) = c_2 \end{cases} \Leftrightarrow$$

$$\begin{cases} \exp(t_1(\lambda_1 - \lambda_2) + \frac{c_2}{c_1}\lambda_2) = c_1 \\ t_2 = \frac{c_2}{c_1} - t_1 \end{cases} \Leftrightarrow$$

$$\begin{cases} t_1 = \frac{\log(c_1) - \frac{c_2}{c_1}\lambda_2}{\lambda_1 - \lambda_2} \\ t_2 = \frac{\frac{c_2}{c_1}\lambda_1 - \log(c_1)}{\lambda_1 - \lambda_2} \end{cases}$$

Then $t_1, t_2 \geq 0$ holds if and only if

$$\lambda_2 \leq \frac{c_1}{c_2}\log(c_1) \leq \lambda_1.$$

Whether these inequalities hold can be decided by making use of Baker's theorem and taking sufficiently precise finite numerical approximations of these values.

4. Decidability in the Commutative Case

We start this section by reducing the Generalised MEP with commuting matrices to LEP. The intuition behind it is quite simple: perform a change of basis so that the matrices $A_1, \dots, A_k$, as well as C, become block-diagonal matrices, with each block being upper triangular; we can then separate the problem into several subinstances, corresponding to the diagonal blocks, and finally make use of our uniqueness result concerning strictly upper triangular logarithms of upper unitriangular matrices.

THEOREM 13. *The Generalised MEP with commuting matrices reduces to LEP.*

Proof. Consider an instance of the generalised MEP, as given in Definition 4, with commuting $n \times n$ matrices $A_1, \dots, A_k$ and target matrix C.

We first show how to define a matrix P such that each matrix $P^{-1}A_iP$ is block diagonal, $i = 1, \dots, k$, with each block being moreover upper triangular.

By Theorem 7 we can write $\mathbb{C}^n$ as a direct sum of subspaces $\mathbb{C}^n = \oplus_{j=1}^{b}\mathcal{V}_j$ such that for every subspace $\mathcal{V}_j$ and matrix A_i, $\mathcal{V}_j$ is an invariant subspace of A_i on which A_i has a single eigenvalue $\lambda_i^{(j)}$.

Define a matrix Q by picking an algebraic basis for each $\mathcal{V}_j$ and successively taking the vectors of each basis to be the columns of Q. Then, each matrix $Q^{-1}A_iQ$ is block-diagonal, where the j-th block is a matrix $B_i^{(j)}$ that represents $A_i \restriction \mathcal{V}_j$, $j = 1, \dots, b$.

Fixing $j \in \{1, \dots, b\}$, note that the matrices $B_1^{(j)}, \dots, B_k^{(j)}$ all commute. Thus we may apply Theorem 8 to obtain an algebraic matrix M_j such that each matrix $M_j^{-1}B_i^{(j)}M_j$ is upper triangular, $i = 1, \dots, k$. Thus we can write

$$M_j^{-1}B_i^{(j)}M_j = \lambda_i^{(j)}I + N_i^{(j)}$$

for some strictly upper triangular matrix $N_i^{(j)}$.

We define M to be the block-diagonal matrix with blocks $M_1, \dots, M_b$. Letting $P = QM$, it is then the case that $P^{-1}A_iP$ is block-diagonal, with the j-th block being $\lambda_i^{(j)}I + N_i^{(j)}$ for $j = 1, \dots, b$. Now

$$\prod_{i=1}^{k}\exp(A_it_i) = C \Leftrightarrow \prod_{i=1}^{k}\exp(P^{-1}A_iPt_i) = P^{-1}CP. \quad (3)$$

If $P^{-1}CP$ is not block-diagonal, with each block being upper triangular and with the same entries along the diagonal, then Equation (3) has no solution and the problem instance must be negative. Otherwise, denoting the blocks $P^{-1}CP$ by $D^{(j)}$ for $j \in \{1, \dots, b\}$, our problem amounts to simultaneously solving the system of matrix equations

$$\prod_{i=1}^{k}\exp\big((\lambda_i^{(j)}I + N_i^{(j)})t_i\big) = D^{(j)}, \quad j \in \{1, \dots, b\} \quad (4)$$

with one equation for each block.

For each fixed j, the matrices $N_i^{(j)}$ inherit commutativity from the matrices $B_i^{(j)}$, so we have

$$\begin{aligned} \prod_{i=1}^{k}\exp((\lambda_i^{(j)}I + N_i^{(j)})t_i) &= \exp\big(\sum_{i=1}^{k}(\lambda_i^{(j)}I + N_i^{(j)})t_i\big) \\ &= \exp\big(\sum_{i=1}^{k}\lambda_i^{(j)}t_i\big) \cdot \exp\big(\sum_{i=1}^{k}N_i^{(j)}t_i\big). \end{aligned}$$

Hence the system (4) is equivalent to

$$\exp\big(\sum_{i=1}^{k} \lambda_i^{(j)} t_i\big) \cdot \exp\big(\sum_{i=1}^{k} N_i^{(j)} t_i\big) = D^{(j)} \qquad (5)$$

for $j = 1, \dots, b$.

By assumption, the diagonal entries of each matrix $D^{(j)}$ are equal to a unique value, say $c^{(j)}$. Since the diagonal entries of $\exp\left(\sum_{i=1}^{k} N^{(j)} t_i\right)$ are all 1, the equation system (5) is equivalent to:

$$\exp\big(\sum_{i=1}^{k} \lambda_i^{(j)} t_i\big) = c^{(j)} \text{ and } \exp\big(\sum_{i=1}^{k} N_i^{(j)} t_i\big) = \frac{1}{c^{(j)}} D^{(j)}$$

for $j = 1, \dots, b$.

Applying Theorem 6, the above system can equivalently be written

$$\exp\big(\sum_{i=1}^{k} \lambda_i^{(j)} t_i\big) = c^{(j)} \text{ and } \sum_{i=1}^{k} N_i^{(j)} t_i = S^{(j)}$$

for some effectively computable matrix $S^{(j)}$ with algebraic entries, $j = 1, \dots, b$.

Except for the additional linear equations, this has the form of an instance of LEP. However we can eliminate the linear equations by performing a linear change of variables, i.e., by computing the solution of the system in parametric form. Thus we finally arrive at an instance of LEP. □

In the following result, we essentially solve the system of equations 2, reducing it to the simpler problem that really lies at its heart.

THEOREM 14. *LEP reduces to ALIP.*

Proof. Consider an instance of LEP, comprising a system of equations

$$\exp\left(\sum_{\ell=1}^{k} \lambda_\ell^{(j)} t_\ell\right) = c_j \exp(d_j) \quad j = 1, \dots, b, \qquad (6)$$

and polyhedron $\mathcal{P} \subseteq \mathbb{R}^{2k}$, as described in Definition 5.

Throughout this proof, let log denote a fixed logarithm branch that is defined on all the numbers $c_j, \exp(d_j)$ appearing above, and for which $\log(-1) = i\pi$. Note that if any $c_j = 0$ for some j then (6) has no solution. Otherwise, by applying log to each equation in (6), we get:

$$\sum_{\ell=1}^{k} \lambda_\ell^{(j)} t_\ell = d_j + \log(c_j) + 2i\pi n_j \quad j = 1, \dots, b, \qquad (7)$$

where $n_j \in \mathbb{Z}$.

The system of equations (7) can be written in matrix form as

$$A\boldsymbol{t} \in \boldsymbol{d} + \log(\boldsymbol{c}) + 2i\pi\mathbb{Z}^b \,,$$

where A is the $b \times k$ matrix with $A_{j,\ell} = \lambda_\ell^{(j)}$ and log is applied pointwise to vectors. Now, defining the convex polyhedron $\mathcal{Q} \subseteq \mathbb{R}^{2b}$ by

$$\mathcal{Q} = \{(\mathrm{Re}(A\boldsymbol{y}), \mathrm{Im}(A\boldsymbol{y})) : \boldsymbol{y} \in \mathbb{C}^k, (\mathrm{Re}(\boldsymbol{y}), \mathrm{Im}(\boldsymbol{y})) \in \mathcal{P}\} \,,$$

it suffices to decide whether the affine lattice $\boldsymbol{d} + \log(\boldsymbol{c}) + 2i\pi\mathbb{Z}^b$ intersects $\{\boldsymbol{x} \in \mathbb{C}^b : (\mathrm{Re}(\boldsymbol{x}), \mathrm{Im}(\boldsymbol{x})) \in \mathcal{Q}\}$.

Define $f : \mathbb{R}^b \to \mathbb{C}^b$ by $f(\boldsymbol{v}) = \boldsymbol{d} + \log(\boldsymbol{c}) + 2i\pi\boldsymbol{v}$, and define a convex polyhedron $\mathcal{T} \subseteq \mathbb{R}^b$ by

$$\mathcal{T} = \{\boldsymbol{v} \in \mathbb{R}^b : (\mathrm{Re}(f(\boldsymbol{v})), \mathrm{Im}(f(\boldsymbol{v}))) \in \mathcal{Q}\} \,.$$

The problem then amounts to deciding whether the convex polyhedron $\mathcal{T}$ intersects contains an integer point. Crucially, the description of the convex polyhedron $\mathcal{T}$ is of the form $\pi B\boldsymbol{x} \leq \boldsymbol{b}$, for some matrix B and vector $\boldsymbol{b}$ such that the entries of B are real algebraic and the components of $\boldsymbol{b}$ are real linear forms in logarithms of algebraic numbers. But this is the form of an instance of ALIP. □

We are left with the task of showing that ALIP is decidable. The argument essentially consists of reducing to a lower-dimensional instance whenever possible, and eventually either using the fact that the polyhedron is bounded to test whether it intersects the integer lattice or using Kronecker's theorem to show that, by a density argument, it must intersect the integer lattice.

THEOREM 15. *ALIP is decidable.*

Proof. We are given a convex polyhedron $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : \pi A\boldsymbol{x} \leq \boldsymbol{b}\}$, where the coordinates $\boldsymbol{b}$ are linear forms in logarithms of algebraic numbers, and need to decide whether this polyhedron intersects $\mathbb{Z}^d$. Throughout this proof, log denotes the logarithm branch picked at the beginning of the proof of Theorem 14. We start by eliminating linear dependencies between the logarithms appearing therein, using Masser's Theorem. For example, suppose that

$$b_i = r_0 + r_1 \log(s_1) + \cdots + r_k \log(s_k), r_0, r_1, s_1, \dots, r_k, s_k \in \overline{\mathbb{Q}}.$$

Due to Baker's theorem, there exists a non-trivial linear relation with algebraic coefficients amongs $\log(-1), \log(s_1), \dots, \log(s_k)$ if and only if there is one with integer coefficients. But such relations can be computed, since

$$n_0 \log(-1) + n_1 \log(s_1) + \cdots + n_k \log(s_k) = 0 \Leftrightarrow$$
$$(-1)^{n_0} s_1^{n_1} \cdots s_k^{n_k} = 1$$

and since the group of multiplicative relations $L(-1, s_1, \dots, s_k)$ can be effectively computed. Whenever it contains a non-zero vector, we use it to eliminate an unnecessary $\log(s_i)$ term, although never eliminating $\log(-1)$. When this process is over, we can see whether each term b_i/π is algebraic or transcendental: it is algebraic if $b_i = \alpha \log(-1), \alpha \in \overline{\mathbb{Q}}$, and transcendental otherwise.

Now, when $\boldsymbol{x} \in \mathbb{Z}^d$, $A\boldsymbol{x}$ is a vector with algebraic coefficients, so whenever b_i/π is transcendental we may alter $\mathcal{P}$ by replacing $\leq$ by $<$ in the i-th inequality, preserving its intersection with $\mathbb{Z}^d$. On the other hand, whenever b_i/π is algebraic, we split our problem into two: in the first one, $\mathcal{P}$ is altered to force equality on the i-th constraint (that is, replacing $\leq$ by $=$), and in the second we force strict inequality (that is, replacing $\leq$ by $<$). We do this for all i, so that no $\leq$ is left in any problem instance, leaving us with finitely many polyhedra, each defined by equations of the form

$$\begin{aligned} K\boldsymbol{x} &= \boldsymbol{k} & (\boldsymbol{k} \in \overline{\mathbb{Q}}^{d_1}) \\ M\boldsymbol{x} &< \boldsymbol{m} & (\boldsymbol{m} \in \overline{\mathbb{Q}}^{d_2}) \\ F\boldsymbol{x} &< \boldsymbol{f} & (\boldsymbol{f} \in \mathbb{R} \setminus \overline{\mathbb{Q}}^{d_3}) \end{aligned}$$

where K, M, F are matrices with algebraic entries. Before proceeding, we eliminate all such empty polyhedra; note that emptiness can be decided via Fourier-Motzkin elimination.

The idea of the next step is to reduce the dimension of all the problem instances at hand until we are left with a number of new instances with full-dimensional open convex polyhedra, of the same form as the original one, apart from the fact that all inequalities in their definitions will be strict. To do that, we use the equations $K\boldsymbol{x} = \boldsymbol{k}$ to eliminate variables: note that, whenever there is an integer solution,

$$K\boldsymbol{x} = \boldsymbol{k}, \boldsymbol{x} \in \mathbb{Z}^d \Leftrightarrow \boldsymbol{x} = \boldsymbol{x}_0 + M\boldsymbol{z},$$

where M is a matrix with integer entries, $\boldsymbol{x}_0$ is an integer vector and $\boldsymbol{z}$ ranges over integer vectors over a smaller dimension space, wherein we also define the polyhedron

$$\mathcal{Q} = \{\boldsymbol{y} : \boldsymbol{x}_0 + M\boldsymbol{y} \in \mathcal{P}\}.$$

Having now eliminated all equality constraints, we are left with a finite set of polyhedra of the form $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : \pi A\boldsymbol{x} < \boldsymbol{b}\}$ that are either empty or full-dimensional and open, and wish to decide whether they intersect the integer lattice of the corresponding space (different instances may lie in spaces of different dimensions, of course). Note that, when $\mathcal{P}$ is non-empty, we can use Fourier-Motzkin elimination to find a vector $\boldsymbol{q} \in \mathbb{Q}^d$ in its interior, and $\varepsilon > 0$ such that the l_1 closed ball of radius ε and centre $\boldsymbol{q}$, which we call $\mathcal{B}$, is contained in $\mathcal{P}$.

The next step is to consider the Minkowski-Weyl decomposition of $\mathcal{P}$, namely $\mathcal{P} = \mathcal{H} + \mathcal{C}$, where $\mathcal{H}$ is the convex hull of finitely many points of $\mathcal{P}$ (which we need not compute) and $\mathcal{C} = \{\boldsymbol{x} \in \mathbb{R}^d : A\boldsymbol{x} \leq \boldsymbol{0}\}$ is a cone with an algebraic description. Note that $\mathcal{P}$ is bounded if and only if $\mathcal{C} = \{\boldsymbol{0}\}$, in which case the problem at hand is simple: consider the polyhedron $\mathcal{Q}$ with an algebraic description obtained by rounding up each coordinate of $\boldsymbol{b}/\pi$, which has the same conic part as $\mathcal{P}$ and which contains $\mathcal{P}$, and therefore is bounded; finally, compute a bound on $\mathcal{Q}$ (such a bound can be defined in the first-order theory of reals), which is also a bound on $\mathcal{P}$, and test the integer points within that bound for membership in $\mathcal{P}$. Otherwise,

$$\mathcal{C} = \{\lambda_1 \boldsymbol{c}_1 + \cdots + \lambda_k \boldsymbol{c}_k : \lambda_1, \ldots, \lambda_k \geq 0\},$$

where $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k \in \overline{\mathbb{Q}}^d$ are the extremal rays of $\mathcal{C}$. Note that $\boldsymbol{q} + \mathcal{C} \subseteq \mathcal{P}$ and that $\mathcal{B} + \mathcal{C} \subseteq \mathcal{P}$.

Now we consider a variation of an argument which appears in (Khachiyan and Porkolab 1997). Consider the computable set

$$\mathcal{L} = \mathcal{C}^{\perp} \cap \mathbb{Z}^d = \bigcap_{i=1}^{k} A(\boldsymbol{c}_i),$$

where $A(\boldsymbol{v})$ denotes the group of additive relations of $\boldsymbol{v}$.

If $\mathcal{L} = \{\boldsymbol{0}\}$ then due to Kronecker's theorem on simultaneous Diophantine approximation it must be the case that there exists a vector $(n_1, \ldots, n_k) \in \mathbb{N}^k$ such that

$$\operatorname{dist}\left(\boldsymbol{q} + \sum_{i=1}^{k} n_i \boldsymbol{c}_i, \mathbb{Z}^d\right) \leq \varepsilon,$$

and we know that $\mathcal{P} \cap \mathbb{Z}^d \neq \emptyset$ from the fact that the l_1 closed ball $\mathcal{B}$ of radius ε and centre $\boldsymbol{q}$ is contained in $\mathcal{P}$.

On the other hand, if $\mathcal{L} \neq \{\boldsymbol{0}\}$, let $\boldsymbol{z} \in \mathcal{L} \setminus \{\boldsymbol{0}\}$. Since $\mathcal{H}$ is a bounded subset of $\mathbb{R}^n$, the set

$$\{\boldsymbol{z}^T \boldsymbol{x} : \boldsymbol{x} \in \mathcal{P}\} = \{\boldsymbol{z}^T \boldsymbol{x} : \boldsymbol{x} \in \mathcal{H}\}$$

is a bounded subset of $\mathbb{R}$. Therefore there exist $a, b \in \mathbb{Z}$ such that

$$\forall \boldsymbol{x} \in \mathcal{P}, a \leq \boldsymbol{z}^T \boldsymbol{x} \leq b,$$

so we can reduce our problem to $b - a + 1$ smaller-dimensional instances by finding the integer points of $\{\boldsymbol{x} \in \mathcal{P} : \boldsymbol{z}^T \boldsymbol{x} = i\}$, for $i \in \{a, \ldots, b\}$. Note that we have seen earlier in the proof how to reduce the dimension of the ambient space when the polyhedron $\mathcal{P}$ is contained in an affine hyperplane. □

5. Undecidability of the Non-Commutative Case

In this section we show that the Matrix Exponentials Problem is undecidable in the case of non-commuting matrices. We show undecidability for the most fundamental variant of the problem, as given in Definition 4, in which the matrices have real entries and the variables t_i range over the non-negative reals. Recall that this problem is decidable in the commutative case by the results of the previous section.

5.1 Matrix Exponentials Problem with Constraints

The proof of undecidability in the non-commutative case is by reduction from Hilbert's Tenth Problem. The reduction proceeds via several intermediate problems. These problems are obtained by augmenting MEP with various classes of arithmetic constraints on the real variables that appear in the statement of the problem.

DEFINITION 8. *We consider the following three classes of arithmetic constraints over real variables $t_1, t_2, \ldots$:*

- *$\mathcal{E}_{\pi\mathbb{Z}}$ comprises constraints of the form $t_i \in \alpha + \beta\pi\mathbb{Z}$, where α and $\beta \neq 0$ are real-valued constants such that $\cos(2\alpha\beta^{-1})$, β are both algebraic numbers.*
- *$\mathcal{E}_+$ comprises linear equations of the form $\alpha_1 t_1 + \ldots + \alpha_n t_n = \alpha_0$, for $\alpha_0, \ldots, \alpha_n$ real algebraic constants.*
- *$\mathcal{E}_\times$ comprises equations of the form $t_\ell = t_i t_j$.*

A class of constraints $\mathcal{E} \subseteq \mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$ induces a generalisation of the MEP problem as follows:

DEFINITION 9 (MEP with Constraints). *Given a class of constraints $\mathcal{E} \subseteq \mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$, the problem MEP($\mathcal{E}$) is as follows. An instance consists of real algebraic matrices $A_1, \ldots, A_k, C$ and a finite set of constraints $E \subseteq \mathcal{E}$ on real variables $t_1, \ldots, t_k$. The question is whether there exist non-negative real values for $t_1, \ldots, t_k$ such that $\prod_{i=1}^{k} e^{A_i t_i} = C$ and the constraints E are all satisfied.*

Note that in the above definition of MEP($\mathcal{E}$) the set of constraints E only mentions real variables $t_1, \ldots, t_k$ appearing in the matrix equation $\prod_{i=1}^{k} e^{A_i t_i} = C$. However, without loss of generality, we can allow constraints to mention fresh variables t_i, for $i > k$, since we can always define a corresponding matrix $A_i = 0$ for such variables for then $e^{A_i t_i} = I$ has no effect on the matrix product. In other words, we effectively have constraints in $\mathcal{E}$ with existentially quantified variables. In particular, we have the following useful observations:

- We can express inequality constraints of the form $t_i \neq \alpha$ in $\mathcal{E}_+ \cup \mathcal{E}_\times$ by using fresh variables t_j, t_ℓ. Indeed $t_i \neq \alpha$ is satisfied whenever there exist values of t_j and t_ℓ such that $t_i = t_j + \alpha$ and $t_j t_\ell = 1$.
- By using fresh variables, $\mathcal{E}_+ \cup \mathcal{E}_\times$ can express polynomial constraints of the form $P(t_1, \ldots, t_n) = t$ for P a polynomial with integer coefficients.

We illustrate the above two observations in an example.

EXAMPLE 1. *Consider the problem, given matrices A_1, A_2 and C, to decide whether there exist $t_1, t_2 \geq 0$ such that*

$$e^{A_1 t_1} e^{A_2 t_2} = C \text{ and } t_1^2 - 1 = t_2, t_2 \neq 0\,.$$

This is equivalent to the following instance of MEP($\mathcal{E}_+ \cup \mathcal{E}_\times$): decide whether there exist $t_1, \ldots, t_5 \geq 0$ such that

$$\prod_{i=1}^{5} e^{A_i t_i} = C \text{ and } t_1 t_1 = t_3, t_3 - 1 = t_2, t_2 t_4 = t_5, t_5 = 1$$

where A_1, A_2 and C are as above and $A_3 = A_4 = A_5 = 0$.

We will make heavy use of the following proposition to combine several instances of the constrained MEP into a single instance by combining matrices block-wise.

PROPOSITION 2. *Given real algebraic matrices $A_1, \ldots, A_k, C$ and $A_1', \ldots, A_k', C'$, there exist real algebraic matrices $A_1'', \ldots, A_k'', C''$ such that for all $t_1, \ldots, t_k$:*

$$\prod_{i=1}^{k} e^{A_i'' t_i} = C'' \quad \Leftrightarrow \quad \prod_{i=1}^{k} e^{A_i t_i} = C \wedge \prod_{i=1}^{k} e^{A_i' t_i} = C'.$$

Proof. Define for any $i \in \{1, \ldots, k\}$:

$$A''_i = \begin{bmatrix} A_i & 0 \\ 0 & A'_i \end{bmatrix}, \qquad C'' = \begin{bmatrix} C & 0 \\ 0 & C' \end{bmatrix}.$$

The result follows because the matrix exponential can be computed block-wise (as is clear from its power series definition):

$$\prod_{i=1}^{k} e^{A''_i t_i} = \prod_{i=1}^{k} \begin{bmatrix} e^{A_i t_i} & 0 \\ 0 & e^{A'_i t_i} \end{bmatrix} = \begin{bmatrix} \prod_{i=1}^{k} e^{A_i t_i} & 0 \\ 0 & \prod_{i=1}^{k} e^{A'_i t_i} \end{bmatrix}.$$

□

We remark that in the statement of Proposition 2 the two matrix equations that are combined are over the same set of variables. However, we can clearly combine any two matrix equations for which the common variables appear in the same order in the respective products.

The core of the reduction is to show that the constraints in $\mathcal{E}_{\pi\mathbb{Z}}, \mathcal{E}_+$ and $\mathcal{E}_\times$ do not make the MEP problem harder: one can always encode them using the matrix product equation.

PROPOSITION 3. *MEP($\mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$) reduces to MEP($\mathcal{E}_+ \cup \mathcal{E}_\times$).*

Proof. Let $A_1, \ldots, A_k, C$ be real algebraic matrices and $E \subseteq \mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$ a finite set of constraints on $t_1, \ldots, t_k$. Since E is finite it suffices to show how to eliminate from E each constraint in $\mathcal{E}_{\pi\mathbb{Z}}$.

Let $t_j \in \alpha + \beta\pi\mathbb{Z}$ be a constraint in E. By definition of $\mathcal{E}_{\pi\mathbb{Z}}$ we have that $\cos(2\alpha\beta^{-1}), \sin(2\alpha\beta^{-1})$ and $\beta \neq 0$ are real algebraic. Now define the following extra matrices:

$$A'_j = \begin{bmatrix} 0 & 2\beta^{-1} \\ -2\beta^{-1} & 0 \end{bmatrix}, C' = \begin{bmatrix} \cos(2\alpha\beta^{-1}) & \sin(2\alpha\beta^{-1}) \\ -\sin(2\alpha\beta^{-1}) & \cos(2\alpha\beta^{-1}) \end{bmatrix}.$$

Our assumptions ensure that A'_j and C' are both real algebraic.

We now have the following chain of equivalences:

$$\begin{aligned} e^{A'_j t_j} = C' &\Leftrightarrow \begin{bmatrix} \cos(2t_j\beta^{-1}) & \sin(2t_j\beta^{-1}) \\ -\sin(2t_j\beta^{-1}) & \cos(2t_j\beta^{-1}) \end{bmatrix} = C' \\ &\Leftrightarrow \cos(2t_j\beta^{-1}) = \cos(2\alpha\beta^{-1}) \\ &\qquad \wedge \sin(2t_j\beta^{-1}) = \sin(2\alpha\beta^{-1}) \\ &\Leftrightarrow 2\beta^{-1}t_j = 2\alpha\beta^{-1} \mod 2\pi \\ &\Leftrightarrow t_j \in \alpha + \beta\pi\mathbb{Z}. \end{aligned}$$

Thus the additional matrix equation $e^{A'_j t_j} = C'$ is equivalent to the constraint $t_j \in \alpha + \beta\pi\mathbb{Z}$. Applying Proposition 2 we can thus eliminate this constraint. □

PROPOSITION 4. *MEP($\mathcal{E}_+ \cup \mathcal{E}_\times$) reduces to MEP($\mathcal{E}_+$).*

Proof. Let $A_1, \ldots, A_k, C$ be real algebraic matrices and $E \subseteq \mathcal{E} \cup \mathcal{E}_\times$ a finite set of constraints on variables $t_1, \ldots, t_k$. We proceed as above, showing how to remove from E each constraint from $\mathcal{E}_\times$. In so doing we potentially increase the number of matrices and add new constraints from $\mathcal{E}_+$.

Let $t_l = t_i t_j$ be an equation in E. To eliminate this equation the first step is to introduce fresh variables x, x', y, y', z and add the constraints

$$t_i = x,\ t_j = y,\ t_\ell = z,$$

which are all in $\mathcal{E}_+$. We now add a new matrix equation over the fresh variables x, x', y, y', z that is equivalent to the constraint $xy = z$. Since this matrix equation involves a new set of variables we are free to the set the order of the matrix products, which is crucial to express the desired constraint.

The key gadget is the following matrix product equation, which holds for any $x, x', y, y', z \geqslant 0$:

$$\begin{bmatrix} 1 & 0 & -z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -y' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x' & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x - x' & z - xy \\ 0 & 1 & y - y' \\ 0 & 0 & 1 \end{bmatrix}.$$

Notice that each of the matrices on the left-hand side of the above equation has a single non-zero off-diagonal entry. Crucially each matrix of this form can be expressed as an exponential. Indeed we can write the above equation as a matrix-exponential product

$$e^{B_1 z} e^{B_2 y'} e^{B_3 x} e^{B_4 y} e^{B_5 x'} = \begin{bmatrix} 1 & x - x' & z - xy \\ 0 & 1 & y - y' \\ 0 & 0 & 1 \end{bmatrix}$$

for matrices

$$B_1 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad B_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$
$$B_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad B_4 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$
$$B_5 = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Thus the constraint $xy = z$ can be expressed as

$$e^{B_1 z} e^{B_2 y'} e^{B_3 x} e^{B_4 y} e^{B_5 z'} = I. \tag{8}$$

Again, we can apply Proposition 2 to combine the equation (8) with the matrix equation from the original problem instance and thus encode the constraint $x = yz$.

□

PROPOSITION 5. *MEP($\mathcal{E}_+$) reduces to MEP.*

Proof. Let $A_1, \ldots, A_k, C$ be real algebraic matrices and $E \subseteq \mathcal{E} \cup \mathcal{E}_+$ a set of constraints. We proceed as above, showing how to eliminate each constraint from E that lies in $\mathcal{E}_+$, while preserving the set of solutions of the instance.

Let $\beta + \sum_{i=1}^{k} \alpha_i t_i = 0$ be an equation in E. Recall that $\beta, \alpha_1, \ldots, \alpha_k$ are real algebraic. Define the extra matrices $A'_1, \ldots, A'_k$ and C' as follows:

$$A'_i = \begin{bmatrix} 0 & \alpha_i \\ 0 & 0 \end{bmatrix}, \qquad C' = \begin{bmatrix} 1 & -\beta \\ 0 & 1 \end{bmatrix}.$$

Our assumptions ensure that $A'_1, \ldots, A'_k$ and C' are all real algebraic. Furthermore, the following extra product equation becomes:

$$\begin{aligned} \prod_{i=1}^{k} e^{A'_i t_i} = C &\Leftrightarrow \prod_{i=1}^{k} \begin{bmatrix} 1 & \alpha_i t_i \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -\beta \\ 0 & 1 \end{bmatrix} \\ &\Leftrightarrow \sum_{i=1}^{k} \alpha_i t_i = -\beta. \end{aligned}$$

□

Combining Propositions 3, 4, and 5 we have:

PROPOSITION 6. *MEP($\mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$) reduces to MEP.*

5.2 Reduction from Hilbert's Tenth Problem

THEOREM 16. *MEP is undecidable in the non-commutative case.*

Proof. We have seen in the previous section that the problem MEP($\mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$) reduces to MEP without constraints. Thus it suffices to reduce Hilbert's Tenth Problem to MEP($\mathcal{E}_{\pi\mathbb{Z}} \cup \mathcal{E}_+ \cup \mathcal{E}_\times$). In fact the matrix equation will not play a role in the target of this reduction, only the additional constraints.

Let P be an polynomial of total degree d in k variables with integer coefficients. From P we build a homogeneous polynomial Q as follows:

$$Q(\mathbf{x}, u, \lambda) = \lambda^d P\left(\frac{x_1}{\lambda}, \dots, \frac{x_k}{\lambda}\right) + \lambda^{d-1}(u - \lambda)P(0, \dots, 0).$$

Intuitively, we add an extra variable u for the constant term and we make the polynomial homogeneous using another extra variable λ. It is easy to see that Q is homogeneous and still has integer coefficients. Furthermore, we have the relationship

$$Q(\mathbf{x}, 1, 1) = P(\mathbf{x}).$$

As we have seen previously, it is easy to encode Q with constraints, in the sense that we can compute a finite set of constraints $E_Q \subseteq \mathcal{E}_+ \cup \mathcal{E}_\times$ mentioning variables $t_0, \dots, t_m, \lambda, u$ such that E is satisfied if and only if $t_0 = Q(t_1, \dots, t_k, u, \lambda)$. Note that E_Q may need to mention variables other than $t_1, \dots, t_k$ to do that. Another finite set of equations $E_{\pi\mathbb{Z}} \subseteq \mathcal{E}_{\pi\mathbb{Z}}$ is used to encode that $t_1, \dots, t_k, \lambda, u \in \pi\mathbb{Z}$. Finally, $E_= \subseteq \mathcal{E}_+ \cup \mathcal{E}_\times$ is used to encode $t_0 = 0$, $\lambda = u$ and $1 \leqslant u \leqslant 4$. The latter is done by adding the polynomial equations $u = 1 + \alpha^2$ and $u = 4 - \beta^2$ for some α and β. Finally we have the following chain of equivalences:

$$\begin{aligned}
&\exists t_0, \dots, \lambda, u \geqslant 0 \text{ s.t. } E_Q \cup E_{\pi\mathbb{Z}} \cup E_= \text{ is satisfied} \\
&\qquad \Leftrightarrow \exists t_1, \dots, \lambda, u \geqslant 0 \text{ s.t. } 0 = Q(t_1, \dots, t_k, \lambda, \lambda) \\
&\qquad\qquad \wedge\, t_1, \dots, t_k, \lambda \in \pi\mathbb{Z} \wedge 1 \leqslant \lambda \leqslant 4 \\
&\qquad \Leftrightarrow \exists n_1, \dots, n_k \in \mathbb{N} \text{ s.t. } 0 = Q(\pi n_1, \dots, \pi n_k, \pi, \pi) \\
&\qquad \Leftrightarrow \exists n_1, \dots, n_k \in \mathbb{N} \text{ s.t. } 0 = \pi^d Q(n_1, \dots, n_k, 1, 1) \\
&\qquad \Leftrightarrow \exists n_1, \dots, n_k \in \mathbb{N} \text{ s.t. } 0 = P(n_1, \dots, n_k).
\end{aligned}$$

□

6. Conclusion

We have shown that the Matrix-Exponential Problem is undecidable in general, but decidable when the matrices involved commute with eahc other. This is analogous to what was known for the discrete version of this problem, in which the matrix exponentials e^{At} are replaced by matrix powers A^n.

A natural problem that remains open is as follows:

Definition 10. *Given square matrices $A_1, \dots, A_k$ and C, all of the same dimension and all with real algebraic entries, is C a member of the matrix semigroup generated by*

$$\{\exp(A_i t_i) : t_i \geq 0, i = 1, \dots, k\}?$$

When the matrices $A_1, \dots, A_k$ all commute, the above problem is equivalent to the Matrix Exponential Problem. However decidability in the non-commutative case is open.

It would also be interesting to look at possibly decidable restrictions of the MEP, for example the case where $k = 2$ with a non-commuting pair of matrices, which was shown to be decidable for the discrete analogue of this problem in (Bell et al. 2008).

Acknowledgments

The author João Sousa-Pinto would like to thank Andrew Kaan Balin for a productive discussion during the early stages of this work.

References

R. Alur. *Principles of Cyber-Physical Systems*. MIT Press, 2015.

L. Babai, R. Beals, J. Cai, G. Ivanyos, and E. M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, 28-30 January 1996, Atlanta, Georgia.*, pages 498–507, 1996.

A. Baker. *Transcendental Number Theory*. Camb. Univ. Press, 1975.

A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *Jour. Reine Angew. Math.*, 442, 1993.

S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Springer, 2nd edition, 2006.

P. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. Matrix equations and Hilbert's Tenth Problem. *IJAC*, 18(8):1231–1241, 2008.

P. C. Bell, J. Delvenne, R. M. Jungers, and V. D. Blondel. The continuous Skolem-Pisot problem. *Theor. Comput. Sci.*, 411(40-42):3625–3634, 2010.

J.-Y. Cai, R. J. Lipton, and Y. Zalcstein. The complexity of the A B C problem. *SIAM J. Comput.*, 29(6), 2000.

J. W. S. Cassels. *An introduction to Diophantine approximation*. Camb. Univ. Pr., 1965.

T. Chen, N. Yu, and T. Han. Continuous-time orbit problems are decidable in polynomial-time. *Inf. Process. Lett.*, 115(1):11–14, 2015.

C. Choffrut and J. Karhumäki. Some decision problems on integer matrices. *ITA*, 39(1):125–131, 2005.

H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

W. J. Culver. On the existence and uniqueness of the real logarithm of a matrix. *Proc. Amer. Math. Soc.*, 17:1146–1151, 1966.

E. Hainry. Reachability in linear dynamical systems. In *Logic and Theory of Algorithms, 4th Conference on Computability in Europe, CiE 2008, Athens, Greece, June 15-20, 2008, Proceedings*, pages 241–250, 2008.

V. Halava. *Decidable and undecidable problems in matrix theory*. 1997.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1938.

B. W. Helton. Logarithms of matrices. *Proc. Amer. Math. Soc.*, 19:733–738, 1968.

T. A. Henzinger. The theory of hybrid automata. In *Proceedings, 11th Annual IEEE Symposium on Logic in Computer Science, New Brunswick, New Jersey, USA, July 27-30, 1996*, pages 278–292, 1996.

T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, 29 May-1 June 1995, Las Vegas, Nevada, USA*, pages 373–382, 1995.

R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *J. ACM*, 33(4):808–821, 1986.

L. Khachiyan and L. Porkolab. Computing integral points in convex semi-algebraic sets. In *FOCS*, pages 162–171, 1997.

D. W. Masser. Linear relations on algebraic groups. In *New Advances in Transcendence Theory*. Camb. Univ. Press, 1988.

Y. Matiyasevich. *Hilbert's 10th Problem*. MIT Press, 1993.

D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, 2002.

M. Newman. Two classical theorems on commuting matrices. *Journal of research of the National Bureau of Standards - B. Mathematics and Mathematical Physics*, 71 B(2, 3), 1967.

V. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12), 1996.

M. S. Paterson. Undecidability in 3 by 3 matrices. *J. of Math. and Physics*, 1970.

J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. *J. Symb. Comp.*, 1992.

A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.

E. Wermuth. Two remarks on matrix exponentials. *Linear Algebra and its Applications*, 117:127–132, 1989.