The Polyhedral Escape Problem is Decidable

Joël Ouaknine*, João Sousa Pinto**, and James Worrell

University of Oxford

Abstract. The Polyhedral Escape Problem for continuous linear dynamical systems consists of deciding, given an affine function $f : \mathbb{R}^d \to \mathbb{R}^d$ and a convex polyhedron $\mathcal{P} \subset \mathbb{R}^d$, whether, for some initial point $\boldsymbol{x}_0$ in $\mathcal{P}$, the trajectory of the unique solution to the differential equation $\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t)), \boldsymbol{x}(0) = \boldsymbol{x}_0, t \geq 0$, is entirely contained in $\mathcal{P}$. We show that this problem is decidable, by reducing it in polynomial time to the decision version of linear programming with real algebraic coefficients, thus placing it in $\exists\mathbb{R}$, which lies between *NP* and *PSPACE*. Our algorithm makes use of spectral techniques and relies among others on tools from Diophantine approximation.

1 Introduction

In ambient space $\mathbb{R}^d$, a **continuous linear dynamical system** is a trajectory $\boldsymbol{x}(t)$, where t ranges over the non-negative reals, defined by a differential equation $\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t))$ in which the function f is *affine* or *linear*. If the initial point $\boldsymbol{x}(0)$ is given, the differential equation uniquely defines the entire trajectory. (Linear) dynamical systems have been extensively studied in Mathematics, Physics, and Engineering, and more recently have played an increasingly important role in Computer Science, notably in the modelling and analysis of cyber-physical systems; a recent and authoritative textbook on the matter is [2].

In the study of dynamical systems, particularly from the perspective of control theory, considerable attention has been given to the study of *invariant sets*, i.e., subsets of $\mathbb{R}^d$ from which no trajectory can escape; see, e.g., [9, 4, 3, 15]. Our focus in the present paper is on sets with the dual property that *no trajectory remains trapped*. Such sets play a key role in analysing *liveness* properties in cyber-physical systems (see, for instance, [2, Chap. 9]): discrete progress is ensured by guaranteeing that all trajectories (i.e., from any initial starting point) must eventually reach a point at which they 'escape' (temporarily or permanently) the set in question.

Given an affine function $f : \mathbb{R}^d \to \mathbb{R}^d$ and a convex polyhedron $\mathcal{P} \subset \mathbb{R}^d$, both specified using rational number coefficients encoded in binary, we consider the **Polyhedral Escape Problem** which asks whether there is some point $\boldsymbol{x}_0$ in $\mathcal{P}$ for which the corresponding trajectory of the solution to the differential equation $\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t)), \boldsymbol{x}(0) = \boldsymbol{x}_0, t \geq 0$, is entirely contained in $\mathcal{P}$. Our main result is to show that this problem is decidable, by reducing it in polynomial time to the decision version of linear programming with real algebraic coefficients, which itself reduces to deciding the truth of a sentence in the first-order theory of the reals, a problem whose complexity is known to lie between *NP* and *PSPACE*. Our algorithm makes use of spectral techniques and relies among others on tools from Diophantine approximation.

2 Mathematical Background

2.1 Groups of additive relations

The s-dimensional **torus**, usually denoted by $\mathbb{T}^s$, is defined as the quotient $\mathbb{R}^s/\mathbb{Z}^s$ of the additive group $\mathbb{R}^s$, therefore inheriting its additive group structure.

Given $\boldsymbol{\theta} \in \mathbb{T}^s$, its **group of additive relations** is defined as

$$\mathcal{A}(\boldsymbol{\theta}) = \{\boldsymbol{z} \in \mathbb{Z}^s : \boldsymbol{z} \cdot \boldsymbol{\theta} = 0 \mod \mathbb{Z}\}.$$

* Supported by the EPSRC and by the ERC grant AVS-ISS

** Supported by the EPSRC and by the ERC grant ALGAME

Moreover, $\mathcal{A}(\boldsymbol{\theta})$ induces the following subgroup on the s-dimensional torus:

$$\mathcal{T}(\boldsymbol{\theta}) = \{\boldsymbol{\lambda} \in \mathbb{T}^s : \forall \boldsymbol{z} \in \mathcal{A}(\boldsymbol{\theta}), \boldsymbol{z} \cdot \boldsymbol{\lambda} = 0 \mod \mathbb{Z}\}\,.$$

Let $[\cdot] : \mathbb{R}^s \to \mathbb{T}^s$ denote the canonical quotient map. Note that the real numbers $\theta_1, \ldots, \theta_s, 1$ are linearly independent over $\mathbb{Q}$ if and only if $\mathcal{A}([(\theta_1, \ldots, \theta_s)]) = \{\boldsymbol{0}\}$.

The supremum norm on $\mathbb{R}^s$ induces the following quotient norm in $\mathbb{T}^s$:

$$\mathcal{N}(\boldsymbol{\theta}) = \min\{\|\boldsymbol{u}\|_\infty : \boldsymbol{u} \in \mathbb{R}^s, [\boldsymbol{u}] = \boldsymbol{\theta}\}\,.$$

The following result on simultaneous Diophantine approximation, due to Kronecker, can be found in [11].

Theorem 1 (Kronecker). *Let $\boldsymbol{\theta} \in \mathbb{T}^s$. If $\mathcal{A}(\boldsymbol{\theta}) = \{\boldsymbol{0}\}$, then $\{n\boldsymbol{\theta} : n \in \mathbb{N}\}$ is dense in $\mathbb{T}^s$ with respect to $\mathcal{N}$.*

More generally, the topological closure of $\{n\boldsymbol{\theta} : n \in \mathbb{N}\}$ with respect to $\mathcal{N}$ is precisely $\mathcal{T}(\boldsymbol{\theta})$ (cf. [5]). We shall, however, only make use of the weaker statement.

2.2 Laurent polynomials

A **self-conjugate Laurent polynomial** in variables $z_1, \ldots, z_s$ is an expression of the form

$$g = \sum_{j=1}^{k} c_j {z_1}^{n_{1,j}} \ldots {z_s}^{n_{s,j}} + \overline{c_j} {z_1}^{-n_{1,j}} \ldots {z_s}^{-n_{s,j}}\,,$$

where $c_1, \ldots, c_k \in \mathbb{C}$ and $n_{1,1}, \ldots, n_{s,k} \in \mathbb{Z}$. We say that g is **simple** if g has no constant term and each monomial in g mentions only a single variable.

The following proposition extends a result of [6]:

Proposition 1. *If g is a self-conjugate Laurent polynomial whose constant term is zero and $\boldsymbol{\theta} \in \mathbb{R}^s$ satisfies $\mathcal{A}([\boldsymbol{\theta}]) = \{\boldsymbol{0}\}$, then $g(\exp(2\pi i\boldsymbol{\theta}t))$ is either identically zero for $t \in \mathbb{R}$ or*

$$\liminf_{t\to\infty} g(\exp(2\pi i\boldsymbol{\theta}t)) < 0\,,$$

where exp *is applied component-wise. This holds even when t ranges over* $\mathbb{N}$.

Proof. In what follows, we identify $\mathbb{T}$ with $[0, 1)$. We use an averaging argument to establish that either $g(\exp(2\pi i\boldsymbol{x}))$ is identically zero on $\mathbb{T}^s$ or there must exist a point $\boldsymbol{\nu} \in \mathbb{T}^s$ such that $g(\exp(2\pi i\boldsymbol{\nu})) < 0$. In fact,

$$\int_{\mathbb{T}^s} g(\exp(2\pi i\boldsymbol{x}))d\boldsymbol{x} = 0\,.$$

If $g(\exp(2\pi i\boldsymbol{x}))$ is identically zero on $\mathbb{T}^s$, the result follows. Otherwise, as the integral over a set with positive measure of a non-negative continuous function that is not identically zero must be strictly positive, such $\boldsymbol{\nu}$ must exist.

Since, by assumption, $\mathcal{A}([\boldsymbol{\theta}]) = \{\boldsymbol{0}\}$, it follows from Kronecker's Theorem that $\boldsymbol{\nu}$ is a limit point of $\{t[\boldsymbol{\theta}] : t \in \mathbb{N}\}$. Thus there are arbitrarily large $t \in \mathbb{N}$ for which $g(\exp(2\pi i\boldsymbol{\theta}t)) \leq \frac{1}{2}g(\exp(2\pi i\boldsymbol{\nu})) < 0$, due to continuity of g, which proves the result.

The following consequence of Proposition 1 will be key to proving decidability of the problem at hand.

Proposition 2. *If g is a simple self-conjugate Laurent polynomial, then either*

$$g(\exp(2\pi i\boldsymbol{\theta}t)) \equiv 0 \quad \text{or} \quad \liminf_{t\to\infty} g(\exp(2\pi i\boldsymbol{\theta}t)) < 0$$

where exp *is applied component-wise. This holds even when t ranges over* $\mathbb{N}$.

Proof. If $\mathcal{A}([\boldsymbol{\theta}]) = \{\mathbf{0}\}$, the result follows from the previous proposition. Suppose instead that $\mathcal{A}([\boldsymbol{\theta}]) \neq \{\mathbf{0}\}$, and that $\theta_1, \ldots, \theta_k$ is a maximal subset of coordinates of $\boldsymbol{\theta}$ such that $\mathcal{A}([(\theta_1, \ldots, \theta_k)]) = \{\mathbf{0}\}$. Then, for some $N \in \mathbb{N}$ and each $j \geq k+1$, one can write

$$\theta_j = \frac{1}{N}\left(m + \sum_{i=1}^{k} n_i \theta_i\right)$$

where $m, n_1, \ldots, n_k$ are integers that depend on j, whilst N does not depend on j.

Letting $\boldsymbol{\gamma} = (\theta_1, \ldots, \theta_k)$, one can see that there exists a self-conjugate Laurent polynomial h with zero constant term such that $h(\exp(2\pi i \boldsymbol{\gamma} t)) = g(\exp(2\pi i \boldsymbol{\theta} N t))$, which can be obtained by substituting the formulas for each θ_j ($j \geq k+1$) in $g(\exp(2\pi i \boldsymbol{\theta} N t))$. The result follows from the previous proposition, as $\mathcal{A}([\boldsymbol{\gamma}]) = \{\mathbf{0}\}$.

2.3 Generalised Eigenvectors and Jordan Canonical Forms

Let $A \in \mathbb{Q}^{d \times d}$ be a square matrix with rational entries. The **minimal polynomial** of A is the unique monic polynomial $m(x) \in \mathbb{Q}[x]$ of least degree such that $m(A) = 0$. By the Cayley-Hamilton Theorem the degree of m is at most the dimension of A. The set $\sigma(A)$ of eigenvalues is the set of roots of m. The **index** of an eigenvalue λ, denoted by $\nu(\lambda)$, is defined as its multiplicity as a root of m. We use $\nu(A)$ to denote the maximum index across all eigenvalues of A. Given an eigenvalue $\lambda \in \sigma(A)$, we say that $\boldsymbol{v} \in \mathbb{C}^d$ is a **generalised eigenvector** if $\boldsymbol{v} \in \ker(A - \lambda I)^k$, for some $k \in \mathbb{N}$.

We denote the subspace of $\mathbb{C}^d$ spanned by the set of generalised eigenvectors associated with some eigenvalue λ by $\mathcal{V}_\lambda$. We denote the subspace of $\mathbb{C}^d$ spanned by the set of generalised eigenvectors associated with some real eigenvalue by $\mathcal{V}^r$. We likewise denote the subspace of $\mathbb{C}^d$ spanned by the set of generalised eigenvectors associated to eigenvalues with non-zero imaginary part by $\mathcal{V}^c$.

It is well known that each vector $\boldsymbol{v} \in \mathbb{C}^d$ can be written uniquely as $\sum_{\lambda \in \sigma(A)} \boldsymbol{v}_\lambda$, where $\boldsymbol{v}_\lambda \in \mathcal{V}_\lambda$, and also as $\boldsymbol{v}^r + \boldsymbol{v}^c$, where $\boldsymbol{v}^r \in \mathcal{V}^r$ and $\boldsymbol{v}^c \in \mathcal{V}^c$.

Moreover, we can write any matrix A as $A = Q^{-1} J Q$ for some invertible matrix Q and block diagonal Jordan matrix $J = diag(J_1, \ldots, J_N)$, with each block J_i having the following form:

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

Given a rational matrix A, the factorisation $A = Q^{-1} J Q$ can be computed in polynomial time, as shown in [7].

Note that each vector $\boldsymbol{v}$ appearing as a column of the matrix Q^{-1} is a generalised eigenvector. We also note that the index $\nu(\lambda)$ of some eigenvalue λ corresponds to the dimension of the largest Jordan block associated with it.

One can obtain a closed-form expression for powers of block diagonal Jordan matrices, and use this to get a closed-form expression for exponential block diagonal Jordan matrices. In fact, if J_i is a $k \times k$ Jordan block associated with some eigenvalue λ, then

$$J_i^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-1} & \cdots & \binom{n}{k-1}\lambda^{n-k+1} \\ 0 & \lambda^n & n\lambda^{n-1} & \cdots & \binom{n}{k-2}\lambda^{n-k+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n\lambda^{n-1} \\ 0 & 0 & 0 & \cdots & \lambda^n \end{pmatrix} \quad \text{and} \quad \exp(J_i t) = \exp(\lambda t) \begin{pmatrix} 1 & t & \cdots & \frac{t^{k-1}}{(k-1)!} \\ 0 & 1 & \cdots & \frac{t^{k-2}}{(k-2)!} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

In the above, $\binom{n}{j}$ is defined to be 0 when $n < j$.

Proposition 3. *Every expression of the form* $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0$ *is a linear combination of terms of the form* $t^n \exp(\lambda t)$*.*

Proof. Note that, if $A = Q^{-1}JQ$ and $J = diag(J_1, \ldots, J_N)$ is a block diagonal Jordan matrix, then $\exp(At) = Q^{-1}\exp(Jt)Q$ and $\exp(Jt) = diag(\exp(J_1 t), \ldots, \exp(J_N t))$.

In order to compare the asymptotic growth of expressions of the form $t^n \exp(\lambda t)$ we define $\prec$ to be the lexicographic order on $\mathbb{R} \times \mathbb{N}_0$, that is,

$$(\eta, j) \prec (\rho, m) \quad \text{iff} \quad \eta < \rho \text{ or } (r = s \text{ and } j < m)\,.$$

Then $\exp(\eta t)t^j = o(\exp(\rho t)t^m)$ as $t \to \infty$ if and only if $(\eta, j) \prec (\rho, m)$.

If $\boldsymbol{b}^T \exp(At)\boldsymbol{v}$ is not identically zero, the maximal $(\rho, m) \in \mathbb{R} \times \mathbb{N}_0$ with respect to $\prec$ for which there is a term $t^m \exp(\lambda t)$ with $\Re(\lambda) = \rho$ in the closed-form expression for $\boldsymbol{b}^T \exp(At)\boldsymbol{v}$ is called dominant for $\boldsymbol{b}^T \exp(At)\boldsymbol{v}$.

Before we can proceed, we shall need the following auxiliary result:

Proposition 4. *Suppose that* $\boldsymbol{v} \in \mathbb{R}^d$ *and that* $\boldsymbol{v} = \sum_{\lambda \in \sigma(A)} \boldsymbol{v}_\lambda$*, where* $\boldsymbol{v}_\lambda \in \mathcal{V}_\lambda$*. Then* $\boldsymbol{v}_{\overline{\lambda}}$ *and* $\boldsymbol{v}_\lambda$ *are component-wise complex conjugates.*

Proof. Note that $\boldsymbol{v}_\lambda \in \ker(A - \lambda I)^k$ implies that $\overline{\boldsymbol{v}_\lambda} \in \ker(A - \overline{\lambda} I)^k$. The result follows from the fact that

$$\boldsymbol{0} = \boldsymbol{v} - \overline{\boldsymbol{v}} = \sum_{\lambda \in \sigma(A)} (\boldsymbol{v}_\lambda - \overline{\boldsymbol{v}_{\overline{\lambda}}})$$

and from uniqueness of the above decomposition.

Proposition 5. *Consider a function of the form* $h(t) = \boldsymbol{b}^T \exp(At)\boldsymbol{v}^c$*, where* $\boldsymbol{v}^c \in \mathcal{V}^c$*, with* $(\rho, m) \in \mathbb{R} \times \mathbb{N}_0$ *dominant. If* $h(t) \not\equiv 0$*, then we have*

$$-\infty < \liminf_{t \to \infty} \frac{h(t)}{\exp(\rho t)t^m} < 0\,.$$

Proof. Let $\Re(\sigma(A)) = \{\eta \in \mathbb{R} : \eta + i\theta \in \sigma(A), \text{ for some } \theta \in \mathbb{R}\}$. Moreover, for $\eta \in \Re(\sigma(A))$, we define $\boldsymbol{\theta}_\eta = \{\theta \in \mathbb{R}^+ : \eta + i\theta \in \sigma(A)\}$. By abuse of notation, we also use $\boldsymbol{\theta}_\eta$ to refer to the vector whose coordinates are exactly the members of this set, ordered in an increasing way. We note that, due to Proposition 4, the following holds:

$$\begin{aligned}
\boldsymbol{b}^T \exp(At)\boldsymbol{v}^c &= \boldsymbol{b}^T \exp(At) \sum_{\eta \in \Re(\sigma(A))} \sum_{\theta \in \boldsymbol{\theta}_\eta} \boldsymbol{v}_{\eta + i\theta} + \boldsymbol{v}_{\eta - i\theta} \\
&= \sum_{\eta \in \Re(\sigma(A))} \sum_{\theta \in \boldsymbol{\theta}_\eta} \boldsymbol{b}^T \exp(At)\boldsymbol{v}_{\eta + i\theta} + \overline{\boldsymbol{b}^T \exp(At)\boldsymbol{v}_{\eta + i\theta}} \\
&= \sum_{\eta \in \Re(\sigma(A))} \sum_{j=0}^{\nu(A)-1} t^j \exp(\eta t) g_{(\eta,j)}(\exp(i\boldsymbol{\theta}_\eta t))
\end{aligned}$$

for some simple self-conjugate Laurent polynomials $g_{(\eta,j)}$. Note that

$$(\rho, m) = \max_{\prec}\{(\eta, j) \in \mathbb{R} \times \mathbb{N}_0 : g_{(\eta,j)}(\exp(i\boldsymbol{\theta}_\eta t)) \not\equiv 0\}\,.$$

The result then follows from the fact that

$$\liminf_{t \to \infty} \frac{h(t)}{\exp(\rho t)t^m} = \liminf_{t \to \infty} g_{(\rho,m)}(\exp(i\boldsymbol{\theta}_\rho t))\,.$$

2.4 Computation with Algebraic Numbers

In this section, we briefly explain how one can represent and manipulate algebraic numbers efficiently.

Any given algebraic number α can be represented as a tuple (p, a, ε), where p is its minimal polynomial, $a \in \mathbb{Q}(i)$ is an approximation of α, and $\varepsilon \in \mathbb{Q}$ is suitably chosen so that α is the unique root of p within distance ε of a. This is referred to as the standard or canonical representation of an algebraic number.

The following separation bound, due to Mignotte [13], entails that such a representation is unambiguous provided that the error term is sufficiently small:

Proposition 6. *Let $f \in \mathbb{Z}[x]$. If α_1 and α_2 are distinct roots of f, then*

$$|\alpha_1 - \alpha_2| > \frac{\sqrt{6}}{d^{(d+1)/2} H^{d-1}}$$

where d and H are respectively the degree and height (maximum absolute value of the coefficients) of f.

One can efficiently perform arithmetic operations on standard representations of algebraic numbers, as one can:

- factor an arbitrary polynomial with rational coefficients as a product of irreducible polynomials in polynomial time using the LLL algorithm, described in [12];
- compute an approximation of an arbitrary algebraic number accurate up to polynomially many bits in polynomial time, due to the work in [14];
- use the sub-resultant algorithm (see Algorithm 3.3.7 in [10]) and the two aforementioned procedures to compute canonical representations of sums, differences, multiplications, and divisions of canonically represented algebraic numbers.

3 Existential First-Order Theory of the Reals

Let $\boldsymbol{x} = (x_1, \ldots, x_m)$ be a list of m real-valued variables, and let $\sigma(\boldsymbol{x})$ be a Boolean combination of atomic predicates of the form $g(\boldsymbol{x}) \sim 0$, where each $g(\boldsymbol{x})$ is a polynomial with integer coefficients in the variables $\boldsymbol{x}$, and $\sim$ is either $>$ or $=$. Tarski has famously shown that we can decide the truth over the field $\mathbb{R}$ of sentences of the form $\phi = Q_1 x_1 \cdots Q_m x_n \sigma(\boldsymbol{x})$, where Q_i is either $\exists$ or $\forall$. He did so by showing that this theory admits quantifier elimination (Tarski-Seidenberg theorem [16]). The set of all true sentences of such form is called the first-order theory of the reals, and the set of all true sentences where only existential quantification is allowed is called the existential first-order theory of the reals. The complexity class $\exists\mathbb{R}$ is defined as the set of problems having a polynomial-time many-one reduction to the existential theory of the reals. It was shown in [8] that $\exists\mathbb{R} \subseteq PSPACE$.

We also remark that our standard representation of algebraic numbers allows us to write them explicitly in the first-order theory of the reals, that is, given $\alpha \in \mathbb{A}$, there exists a sentence $\sigma(x)$ such that $\sigma(x)$ is true if and only if $x = \alpha$. Thus, we allow their use when writing sentences in the first-order theory of the reals, for simplicity.

The decision version of linear programming with canonically-defined algebraic coefficients is in $\exists\mathbb{R}$, as the emptiness of a convex polyhedron can easily be described by a sentence of the form $\exists x_1 \cdots \exists x_n \sigma(\boldsymbol{x})$.

Finally, we note that even though the decision version of linear programming with rational coefficients is in P, allowing algebraic coefficients makes things more complicated. While it has been shown in [1] that this is solvable in time polynomial in the size of the problem instance and on the degree of the smallest number field containing all algebraic numbers in each instance, it turns out that in the problem at hand the degree of that extension can be exponential in the size of the input. In other words, the splitting field of the characteristic polynomial of a matrix can have a degree which is exponential in the degree of the characteristic polynomial.

4 The Polyhedral Escape Problem

The Polyhedral Escape Problem for continuous linear dynamical systems consists of deciding whether, given an affine function $f : \mathbb{R}^d \to \mathbb{R}^d$ and a convex polyhedron $\mathcal{P} \subset \mathbb{R}^d$, whether, for some initial point $\boldsymbol{x}_0 \in \mathcal{P}$, the trajectory of the unique solution to the differential equation $\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t)), \boldsymbol{x}(0) = \boldsymbol{x}_0, t \geq 0$, is entirely contained in $\mathcal{P}$. A starting point $\boldsymbol{x}_0 \in \mathcal{P}$ is said to be **trapped** if the trajectory of the corresponding solution is contained in $\mathcal{P}$, and **eventually trapped** if the trajectory of the corresponding solution contains a trapped point. Therefore, the Polyhedral Escape Problem amounts to deciding whether a trapped point exists, which in turn is equivalent to deciding whether an eventually trapped point exists.

The goal of this section is to prove the following result:

Theorem 2. *The Polyhedral Escape Problem is polynomial-time reducible to the decision version of linear programming with algebraic coefficients.*

A d-dimensional instance of the Polyhedral Escape Problem is a pair $(f, \mathcal{P})$, where $f : \mathbb{R}^d \to \mathbb{R}^d$ is an affine function and $\mathcal{P} \subseteq \mathbb{R}^d$ is a convex polyhedron. In this formulation we assume that all numbers involved in the definition of f and $\mathcal{P}$ are rational.[1]

An instance $(f, \mathcal{P})$ of the Polyhedral Escape Problem is said to be **homogeneous** if f is a linear function and $\mathcal{P}$ is a convex polyhedral cone (in particular, $\boldsymbol{x} \in \mathcal{P}, \alpha > 0 \Rightarrow \alpha\boldsymbol{x} \in \mathcal{P}$).

The restriction of the Polyhedral Escape Problem to homogeneous instances is called the homogeneous Polyhedral Escape Problem.

Lemma 1. *The Polyhedral Escape Problem is polynomial-time reducible to the homogeneous Polyhedral Escape Problem.*

Proof. Let $(f, \mathcal{P})$ be an arbitrary instance of the Polyhedral Escape Problem. Write

$$f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{a} \text{ and } \mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : B_1\boldsymbol{x} > \boldsymbol{b}_1 \wedge B_2\boldsymbol{x} \geq \boldsymbol{b}_2\}$$

Also write

$$A' = \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 0 \end{pmatrix}, B_1' = \begin{pmatrix} B_1 & -\boldsymbol{b}_1 \\ 0 & 0 \end{pmatrix}, B_2' = \begin{pmatrix} B_2 & -\boldsymbol{b}_2 \\ 0 & 0 \end{pmatrix}, \text{ and } \mathcal{P}' = \{\boldsymbol{x} \in \mathbb{R}^{d+1} : B_1'\boldsymbol{x} > 0 \wedge B_2'\boldsymbol{x} \geq 0\}.$$

It then follows that $(f, \mathcal{P})$ is a positive instance if and only if so is $(A', \mathcal{P}')$.

We remind the reader that the unique solution to the differential equation $\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t)), \boldsymbol{x}(0) = \boldsymbol{x}_0, t \geq 0$, where $f(\boldsymbol{x}) = A\boldsymbol{x}$, is given by

$$\boldsymbol{x}(t) = \exp(At)\boldsymbol{x}_0 .$$

In this setting, the sets of trapped and eventually trapped points are, respectively:

$$T = \{\boldsymbol{x}_0 \in \mathbb{R}^d : \forall t \geq 0, \exp(At)\boldsymbol{x}_0 \in \mathcal{P}\}$$
$$ET = \{\boldsymbol{x}_0 \in \mathbb{R}^d : \exists t \geq 0, \exp(At)\boldsymbol{x}_0 \in T\}$$

Note that both T and ET are convex subsets of $\mathbb{R}^d$.

Lemma 2. *The homogeneous Polyhedral Escape Problem is polynomial-time reducible to the decision version of linear programming with algebraic coefficients.*

[1] The assumption of rationality is required to justify some of our complexity claims (e.g., Jordan Canonical Forms are only known to be polynomial-time computable for matrices with rational coordinates). Nevertheless, our procedure remains valid in a more general setting, and in fact, the overall $\exists\mathbb{R}$ complexity of our algorithm would not be affected if one allowed real algebraic numbers when defining problem instances.

Proof. Let $\boldsymbol{x}_0 = \boldsymbol{x}_0^r + \boldsymbol{x}_0^c$, where $\boldsymbol{x}_0^r \in \mathcal{V}^r$ and $\boldsymbol{x}_0^c \in \mathcal{V}^c$. We start by showing that if $\boldsymbol{x}_0$ lies in the set T of trapped points then its component $\boldsymbol{x}_0^r$ in the real eigenspace $\mathcal{V}^r$ lies in the set ET of eventually trapped points. It suffices to prove this claim for the case when $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{b}^T \boldsymbol{x} \triangleright 0\}$ (where $\triangleright$ is either $>$ or $\geq$).

Moreover, we assume that neither $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0$ nor $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^c$ are identically zero, as in that case $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0 \equiv \boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^r$ and our claim holds trivially. Also, if $\boldsymbol{x}_0 \in T$, it cannot hold that $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^r \equiv 0$, since $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^c$ is negative infinitely often.

Suppose that $\boldsymbol{x}_0 \in T$ and let (ρ, m) and (η, j) be the dominant indices for $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^r$ and $\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^c$ respectively. Also, we define

$$c = \lim_{t \to \infty} \frac{\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^r}{\exp(\rho t)t^m} .$$

It must hold that $(\eta, j) \preceq (\rho, m)$. Indeed, if $(\eta, j) \succ (\rho, m)$, then, as $t \to \infty$:

$$\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0 = \exp(\eta t)t^j \left(\frac{\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^c}{\exp(\eta t)t^j} + o(1) \right)$$

but the limit inferior of the right-hand term is strictly negative by Proposition 5, contradicting the fact that $\boldsymbol{x}_0 \in T$.

If $(\eta, j) = (\rho, m)$, then, as $t \to \infty$:

$$\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0 = \exp(\rho t)t^m \left(c + \frac{\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^c}{\exp(\rho t)t^m} + o(1) \right)$$

and by invoking Proposition 5 as above, it follows that $c > 0$, from which we conclude that $\boldsymbol{x}_0^r \in ET$, since, as $t \to \infty$:

$$\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0^r = \exp(\rho t)t^m \left(c + o(1)\right) .$$

Finally, if $(\eta, j) \prec (\rho, m)$, then, as $t \to \infty$:

$$\boldsymbol{b}^T \exp(At)\boldsymbol{x}_0 = \exp(\rho t)t^m \left(c + o(1)\right)$$

where $c > 0$, implying that $\boldsymbol{x}_0^r \in ET$.

Having argued that $ET \neq \emptyset$ iff $ET \cap \mathcal{V}^r \neq \emptyset$, we will now show that the set $ET \cap \mathcal{V}^r$ is a convex polyhedron that we can efficiently compute. As before, it suffices to prove this claim for the case when $\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{b}^T \boldsymbol{x} \triangleright 0\}$ (where $\triangleright$ is either $>$ or $\geq$), due to the simple fact that the intersection of finitely many convex polyhedra is still a convex polyhedron.

In what follows, we let $[K]$ denote the set $\{1, \ldots, K\}$. We can write

$$\boldsymbol{b}^T \exp(At) = \sum_{(\eta,j) \in \sigma(A) \times [\nu(A)]} \exp(\eta t) t^j \boldsymbol{u}_{(\eta,j)}^T ,$$

where $\boldsymbol{u}_{(\eta,j)}^T$ is the vector of coefficients of $t^j \exp(\eta t)$ in $\boldsymbol{b}^T \exp(At)$.

Noting that, if $\boldsymbol{x} \in \mathcal{V}^r$ and $(\eta, j) \in (\sigma(A) \setminus \mathbb{R}) \times \mathbb{N}_0$, then $\boldsymbol{u}_{(\eta,j)}^T \boldsymbol{x} = 0$, and

$$ET \cap \mathcal{V}^r = (\mathcal{B} \cap \mathcal{C}) \cup \begin{cases} \{\boldsymbol{0}\} & \text{if } \triangleright \text{ is } \geq \\ \emptyset & \text{if } \triangleright \text{ is } > \end{cases}$$

where

$$\mathcal{B} = \bigcap_{(\eta,j) \in (\sigma(A) \setminus \mathbb{R}) \times [\nu(A)]} \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{u}_{(\eta,j)}^T \boldsymbol{x} = 0\}$$

$$\mathcal{C} = \bigcup_{(\eta,j) \in (\sigma(A) \cap \mathbb{R}) \times [\nu(A)]} \left[\{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{u}_{(\eta,j)}^T \boldsymbol{x} > 0\} \cap \bigcap_{(\rho,m) \succ (\eta,j)} \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{u}_{(\rho,m)}^T \boldsymbol{x} = 0\} \right]$$

The set $ET \cap \mathcal{V}^r$ can be seen to be convex from the above characterisation. Alternatively, note that ET can be shown to be convex from its definition and that $\mathcal{V}^r$ is convex, therefore so must be their intersection. Thus $ET \cap \mathcal{V}^r$ must be a convex polyhedron whose definition possibly involves canonically-represented real algebraic numbers, and this problem amounts to testing it for emptiness.

5 Conclusion

We have shown that the polyhedral escape problem for continuous-time linear dynamical systems is decidable. This was done by analysing the real eigenstructure of the linear operator $f - f(\mathbf{0})$. In fact, we showed that all other eigenvalues could essentially be ignored for purposes of deciding this problem. Deciding whether the trajectory of the dynamical system from a given starting point is trapped or eventually trapped in $\mathcal{P}$ is an interesting related problem, for which one cannot simply discard the influence of the complex eigenstructure.

References

1. I. Adler and P. A. Beling. Polynomial algorithms for linear programming over the algebraic numbers. *Algorithmica*, 12(6):436–457, 1994.
2. R. Alur. *Principles of Cyber-Physical Systems.* MIT Press, 2015.
3. A. Bacciotti and L. Mazzi. Stability of dynamical polysystems via families of Lyapunov functions. *Jour. Nonlin. Analysis*, 67:2167–2179, 2007.
4. V. Blondel and J. Tsitsiklis. A survey of computational complexity results in systems and control. *Automatica*, 36(9):1249–1274, 2000.
5. N. Bourbaki. *Elements of Mathematics: General Topology (Part 2).* Addison-Wesley, 1966.
6. M. Braverman. Termination of integer linear programs. In *Proc. Intern. Conf. on Computer Aided Verification (CAV)*, volume 4144 of *LNCS*. Springer, 2006.
7. J.-Y. Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. *Int. J. Found. Comput. Sci.*, 5(3/4):293–302, 1994.
8. J. Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of STOC'88*, pages 460–467. ACM, 1988.
9. E. B. Castelan and J.-C. Hennet. On invariant polyhedra of continuous-time linear systems. *IEEE Transactions on Automatic Control*, 38(11):1680–85, 1993.
10. H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.
11. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1938.
12. A.K. Lenstra, H.W. Lenstra Jr., and Lászlo Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
13. M. Mignotte. Some useful bounds. In *Computer Algebra*, 1982.
14. V. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12), 1996.
15. S. Sankaranarayanan, T. Dang, and F. Ivancic. A policy iteration technique for time elapse over template polyhedra. In *Proceedings of HSCC*, volume 4981 of *LNCS*. Springer, 2008.
16. A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, 1951.