Invariants for Continuous Linear Dynamical Systems

Shaull Almagor
Computer Science Department, Technion, Israel
shaull@cs.technion.ac.il

Edon Kelmendi
Department of Computer Science, Oxford University, UK
edon.kelmendi@cs.ox.ac.uk

Joël Ouaknine
Max Planck Institute for Software Systems, Germany
Department of Computer Science, Oxford University, UK
joel@mpi-sws.org

James Worrell
Department of Computer Science, Oxford University, UK
jbw@cs.ox.ac.uk

Abstract

Continuous linear dynamical systems are used extensively in mathematics, computer science, physics, and engineering to model the evolution of a system over time. Yet, fundamental reachability problems for this class of systems are not known to be decidable. In this paper we study invariant synthesis for continuous linear dynamic systems. This is the task of finding a set that contains the orbit of the system, is itself invariant under the dynamics, and is disjoint from the a given set of error configurations. Assuming Schanuel's conjecture in transcendental number theory, we establish effective synthesis for o-minimal invariants and semi-algebraic error sets. Without Schanuel's conjecture, we give a procedure for synthesizing semi-algebraic invariants that contain all but a bounded initial segment of the orbit and are disjoint from the error set. We further prove that unconditional effective synthesis of semi-algebraic invariants that contain the whole orbit, is at least as hard as a certain open problem in transcendental number theory.

2012 ACM Subject Classification Theory of computation → Logic and verification; Computing methodologies → Algebraic algorithms; Mathematics of computing → Continuous mathematics; Mathematics of computing → Continuous functions; Theory of computation → Logic and verification; Theory of computation → Finite Model Theory; Software and its engineering → Formal software verification

Keywords and phrases Invariants, continuous linear dynamical systems, continuous Skolem problem, non-reachability, o-minimality

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Funding *Shaull Almagor*: Supported by a European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 837327.
Joël Ouaknine: Supported by ERC grant AVS-ISS (648701)
James Worrell: Supported by EPSRC Fellowship EP/N008197/1

42nd Conference on Very Important Topics (CVIT 2016).
Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:21
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

A *continuous linear dynamical system* (CDS) is a system whose evolution is governed by a differential equation of the form $\dot{\mathbf{x}}(t) = A\mathbf{x}(t)$, where A is a matrix with real entries. CDSs are ubiquitous in mathematics, physics, and engineering, they have been extensively studied as they describe the evolution of many types of systems (or abstractions thereof) over time. More recently, CDSs have become central in the study of cyber-physical systems; a recent authoritative textbook on the matter is [3].

In the study of CDSs, particularly from the perspective of control theory, a fundamental problem is *reachability* – namely whether the orbit $\mathbf{x}(t)$, $t \geq 0$, intersects a given set $Y \subseteq \mathbb{R}^d$. For example, when $\mathbf{x}(t)$ describes the state of an autonomous car (i.e., its location, velocity, etc.) Y may describe situations where the car is not able to stop in time to respond to a hazard.

The simplest case of Y a singleton set, has decidable reachability problem [14, Theorem 2]. However, even for Y that is a half-space, the reachability problem is not known to be decidable. This open problem is known in the literature as the *continuous Skolem-Pisot problem.* Some partial positive results were given in [4] and [7]. The continuous Skolem problem is related to notoriously difficult problems in the theory of Diophantine approximations, a procedure for the continuous Skolem problem would yield one for computing the Diophantine-approximation types of all real algebraic numbers [7]. The latter is an attribute of irrational numbers that is not well understood, yet it is central in this field.

A different approach to the direct reachability problem, is to ask whether the orbit can be separated from Y by a set X that has certain structure. In order for this scheme to be useful, this structure should make it easy to verify that X contains the orbit, and that it is disjoint from Y (indeed, if we give up either requirement, we can use as X either the orbit itself, or $\mathbb{R}^d \setminus Y$, neither of which makes the problem any easier).

Sensible candidates for such structured sets are *inductive invariants.* These are sets that, in addition to containing the orbit, are also invariant under the dynamics of the system. If X is invariant, proving that the orbit is contained in X amounts to proving that the starting point $\mathbf{x}(0)$ belongs to X, which is typically easy. Further restricting the class of sets under consideration (e.g., polyhedra, semi-algebraic sets, etc.), testing whether X intersects Y becomes, likewise, easy.

In [1, 2], a non-empty intersection of the authors studied o-minimal invariants for *discrete* linear dynamical systems. There it is proved that when Y is a semi-algebraic set, the question of whether there exists a o-minimal invariant disjoint from Y is decidable. Moreover, on the positive instances a semi-algebraic invariant exists and it can be constructed effectively. The present paper follows along similar ideas, although continuous linear dynamical systems reveal new difficulties.

Main Contributions. We treat the following problem. We are given a CDS and a semi-algebraic set Y as input. The CDS is given in the form $\langle A, \mathbf{x}_0 \rangle$, where A is a matrix with rational entries and $\mathbf{x}_0 = \mathbf{x}(0)$ is the starting point. Decide whether there exists a semi-algebraic invariant that is disjoint from Y. Assuming Schanuel's conjecture (a unifying conjecture in transcendental number theory that generalises many of the classical results of that subject), we prove that this problem is decidable and for the positive instances, the invariant can be effectively constructed.

Unconditionally, we can decide a slightly weaker problem, namely the question of whether there exists a semi-algebraic set disjoint from Y that is: (1) invariant under the dynamics of the system, and (2) contains *all but a finite part* of the orbit. Likewise, when the answer is positive, the set can be effectively constructed. Such an invariant is a compact certificate that the orbit does not enter a semi-algebraic set infinitely often. The latter is a very difficult problem even when the given set is a half-space [6].

We give a reason for this discrepancy with the discrete systems studied in [1, 2], by way of a reduction from a seemingly difficult problem that highlights the complications of the continuous systems. The problem that we reduce from, asks whether a given exponential polynomial of the form

$$f(t) = a_1 e^{b_1 t} + \cdots + a_n e^{b_n t}$$

has zeros in a bounded interval, where a_i, b_i are real algebraic numbers. Deciding whether f has zeros in a bounded region, without Schanuel's conjecture, seems to be hard because the zeros have to be transcendental and moreover they can be tangential.

The rest of the paper is organised as follows. In Section 2 we give the necessary definitions and terminology. In Section 3 we define *cones* which are over-approximations of the orbit, and prove that they are in a certain sense canonical. The positive results assuming Schanuel's conjecture are subsequently given in this section. Section 4 is devoted to the effective construction of the semi-algebraic invariants which allows us to state and prove the unconditional positive results. In Section 5 we give the aforementioned reduction.

Related Work. Invariant synthesis is a central technique for establishing safety properties of hybrid systems. For the class of CDS considered in this paper, i.e., those specified by a single linear differential equation, it has long been known how to compute strongest *algebraic* invariants [20]. Here an algebraic invariant is one that is specified by a conjunction of polynomial equalities. If one moves to the more general setting of semi-algebraic invariants, which allow inequalities, then there is typically no longer a strongest (or smallest) invariant, but one can still ask to decide the existence of an invariant that avoids a given target set of configurations. To the best of our knowledge the present paper is the first to address this problem in the context of continuous dynamical systems. A popular approach in previous work has been to seek invariants that match a given syntactic *template*, which allows to reduce invariant synthesis to constraint solving [13, 22, 15]. While this technique can be applied to much richer classes of systems than those considered here (e.g., with discrete control modes and non-linear differential equations), it does not appear to offer a way to decide the existence of arbitrary semi-algebraic invariants. An alternative to the template approach for invariant generation involves obtaining candidate invariants from semi-algebraic abstractions of a system [21]. Another active area of current research lies in developing powerful techniques to check whether a given semi-algebraic set is actually an invariant [12].

2 Preliminaries

A continuous-time linear dynamical system is a pair

$$\langle A, \mathbf{x}_0 \rangle$$

where $A \in \mathbb{Q}^{d \times d}$ and $\mathbf{x}_0 \in \mathbb{Q}^d$. The system evolves in time according the function $x(t)$ which is the unique solution to the differential equation $\dot{\mathbf{x}}(t) = A\mathbf{x}(t)$ with $\mathbf{x}(0) = \mathbf{x}_0$. Explicitly this solution can be written as:

$$\mathbf{x}(t) = e^{At}\mathbf{x}_0.$$

The *orbit of* $\langle A, \mathbf{x}_0 \rangle$ *from time* t_0 is the set $\mathcal{O}(t_0) = \{e^{At}\mathbf{x}_0 \;:\; t \geq t_0\}$ (we will simply write $\mathcal{O}$ for $\mathcal{O}(0)$). An *invariant for* $\langle A, \mathbf{x}_0 \rangle$ *from time* t_0 is a set $\mathcal{I} \subseteq \mathbb{R}^d$ that contains $e^{At_0}\mathbf{x}_0$ and is stable under applications of e^{At}, i.e., $e^{At}\mathcal{I} \subseteq \mathcal{I}$ for every $t \geq 0$. Note that an invariant from time t_0 contains $\mathcal{O}(t_0)$. Given a set $Y \subseteq \mathbb{R}^d$ (referred hence as an *error set*), we say that the invariant $\mathcal{I}$ *avoids* Y if the two sets are disjoint.

We denote by $\mathfrak{R}_0$ the structure $\langle \mathbb{R}, 0, 1, +, \cdot, < \rangle$. This is the ordered field of real numbers with constants 0 and 1. A sentence in the corresponding first-order language is a quantified Boolean combination of atomic propositions of the form $P(x_1, \ldots, x_n) > 0$, where P is a polynomial with integer coefficients and $x_1, \ldots, x_n$ are variables. In addition to $\mathfrak{R}_0$, we also consider its following expansions:

- $\mathfrak{R}_{\exp}$, obtained by expanding $\mathfrak{R}_0$ with the real exponentiation function $x \mapsto e^x$.
- $\mathfrak{R}^{\mathrm{RE}}$, obtained by expanding $\mathfrak{R}_0$ with the *restricted elementary functions*, namely $x \mapsto e^x|_{[0,1]}$, $x \mapsto \sin x|_{[0,1]}$, and $x \mapsto \cos x|_{[0,1]}$.
- $\mathfrak{R}^{\mathrm{RE}}_{\exp}$, obtained by expanding $\mathfrak{R}_{\exp}$ with the restricted elementary functions.

Tarski famously showed that the first-order theory of $\mathfrak{R}_0$ admits quantifier elimination, moreover the elimination is effective and therefore the theory is decidable [23, Theorem 37].

It is an open question whether the theory of the reals with exponentiation ($\mathfrak{R}_{\exp}$) is decidable; however decidability was established subject to Schanuel's conjecture by MacIntyre and Wilkie [17, Theorem 1.1]. MacIntyre and Wilkie further showed in [17, Section 5] that decidability of the theory of $\mathfrak{R}_{\exp}$ implies a weak form of Schanuel's conjecture.

Similarly, it is an open question whether $\mathfrak{R}^{\mathrm{RE}}$ and $\mathfrak{R}^{\mathrm{RE}}_{\exp}$ are decidable, but they are also known to be decidable subject to Schanuel's conjecture [16, Theorem 3.1][1].

Let $\mathfrak{R}$ be an expansion of the structure $\mathfrak{R}_0$. A set $S \subseteq \mathbb{R}^d$ is *definable* in $\mathfrak{R}$ if there exists a formula $\phi(x_1, \ldots, x_d)$ in $\mathfrak{R}$ with free variables $x_1, \ldots, x_d$ such that $S = \{(c_1, \ldots, c_d) \in \mathbb{R}^d \mid \mathfrak{R} \models \phi(c_1, \ldots, c_d)\}$. For $\mathfrak{R} = \mathfrak{R}_0$, the ordered field of real numbers, $\mathfrak{R}_0$-definable sets are known as *semi-algebraic* sets.

▶ Remark 2.1. There is a natural first-order interpretation of the field of complex numbers $\mathbb{C}$ in the field of real numbers $\mathbb{R}$. We shall say that a set $S \subseteq \mathbb{C}^d$ is $\mathfrak{R}$*-definable* if the image $\{(x, y) \in \mathbb{R}^d \times \mathbb{R}^d \mid x + iy \in S\}$ of S under this interpretation is $\mathfrak{R}$-definable.

A totally ordered structure $\langle M, <, \ldots \rangle$ is said to be *o-minimal* if every definable subset of M is a finite union of intervals. Tarski's result on quantifier elimination implies that $\mathfrak{R}_0$ is o-minimal. The o-minimality of $\mathfrak{R}_{\exp}$ and $\mathfrak{R}^{\mathrm{RE}}$ is shown in [26], and the o-minimality of $\mathfrak{R}^{\mathrm{RE}}$ and $\mathfrak{R}^{\mathrm{RE}}_{\exp}$ is due to [24, 25].

A *semi-algebraic invariant* is one that is definable in $\mathfrak{R}_0$. An *o-minimal invariant* is one that is definable in an o-minimal expansion of $\mathfrak{R}_{\exp}$.

3 Orbit Cones

In this section we define orbit cones, an object that plays a central role in the subsequent results. They can be thought of as over-approximations of the orbit that has certain desirable properties, and moreover it is canonical in the sense that any other invariant must contain a cone.

[1] More precisely, the decidability of $\mathfrak{R}_{\exp}$ requires Schanuel's conjecture over $\mathbb{R}$, whereas that of $\mathfrak{R}^{\mathrm{RE}}_{\exp}$ requires it over $\mathbb{C}$.

3.1 Jordan Normal Form

Let $\langle A, \mathbf{x}_0 \rangle$ be a continuous linear dynamical system. The exponential of a square matrix A is defined by its formal power series as

$$e^A \overset{\text{def}}{=} \sum_{n=0}^{\infty} \frac{A^n}{n!}.$$

Let $\lambda_1, \dots, \lambda_k$ be the eigenvalues of A, and recall that when $A \in \mathbb{Q}^{d\times d}$, all the eigenvalues are algebraic. We can write A in *Jordan Normal Form* as $A = PJP^{-1}$ where $P \in \mathbb{C}^{d\times d}$ is an invertible matrix with algebraic entries, and $J = \operatorname{diag}(B_1, \dots, B_k)$ is a block-diagonal matrix where each block B_l is a Jordan block that corresponds to eigenvalue λ_l, and it has the form

$$B_l = \begin{pmatrix} \lambda_l & 1 & 0 & \cdots & 0 \\ 0 & \lambda_l & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_l \end{pmatrix} \in \mathbb{C}^{d_l \times d_l}$$

with $\sum_{l=1}^{k} d_l = d$.

From the power series, we can write $e^{At} = Pe^{Jt}P^{-1}$. Further, $e^{Jt} = \operatorname{diag}(e^{B_1}, \dots, e^{B_k})$. For each $1 \le l \le k$, write $B_l = \Lambda_l + N_l$, where Λ_l is the $d_l \times d_l$ diagonal matrix $\operatorname{diag}(\lambda_l, \dots, \lambda_l)$ and N_l is the $d_l \times d_l$ matrix $\operatorname{diag}_2(1, \dots, 1)$; where $\operatorname{diag}_j(\cdot)$ is the j-th diagonal matrix, with other entries zero.

The matrices Λ_l and N_l commute, since the former is a diagonal matrix. A fundamental property of matrix exponentiation is that if matrices A, B commute, then $e^{A+B} = e^A e^B$. Thus, we have

$$e^{Jt} = e^{\operatorname{diag}(\Lambda_1 t + N_1 t, \dots, \Lambda_k t + N_k t)} = \operatorname{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_k t}) e^{\operatorname{diag}(N_1 t, \dots, N_k t)},$$

where by $\operatorname{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_k t})$ we mean the $d \times d$ diagonal matrix that has the entry $e^{\lambda_1 t}$ written d_1 times, the entry $e^{\lambda_2 t}$ written d_2 times and so on. It will always be clear from the context whether we repeat the entries because of their multiplicity or not.

Matrices N_l are nilpotent, so its power series expansion is a finite sum, i.e. a polynomial in $N_l t$. More precisely, one can verify that:

$$e^{N_l t} = I + \operatorname{diag}_2(t, \dots, t) + \operatorname{diag}_3(\frac{t^2}{2}, \dots, \frac{t^2}{2}) + \dots + \operatorname{diag}_{d_l}\left(\frac{t^{(d_l-1)}}{(d_l-1)!}\right).$$

Set $Q(t) \overset{\text{def}}{=} \operatorname{diag}(e^{N_1 t}, \dots, e^{N_k t})$. From the equation above, the entries of $Q(t)$ are polynomials in t with rational coefficients.

Write the eigenvalues as $\lambda_l = \rho_l + \mathrm{i}\omega_l$, so that

$$\operatorname{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_k t}) = \underbrace{\operatorname{diag}(e^{\rho_1 t}, \dots, e^{\rho_k t})}_{E(t)} \cdot \underbrace{\operatorname{diag}(e^{\omega_1 \mathrm{i} t}, \dots, e^{\omega_k \mathrm{i} t})}_{R(t)}$$

We have in this manner decomposed the orbit

$$\mathcal{O}(t_0) = \{P \quad E(t) \; R(t) \; Q(t) \quad P^{-1}\mathbf{x}_0 \;:\; t \ge t_0\},$$

into an exponential $E(t)$, a rotation $R(t)$, and a simple polynomial $Q(t)$ matrices that commute with one another. Having the orbit in such a form will facilitate the analysis done in the sequel.

3.2 Cones as Canonical Invariants

In a certain sense, the rotation matrix $R(t)$ is the most complicated, because of it, the orbit is not even definable in $\mathfrak{R}_{\exp}$. The purpose of cones is to abstract away this matrix by a much simpler subgroup of the complex torus

$$\mathbb{T} \overset{\text{def}}{=} \{\mathbf{z} \in \mathbb{C}^k \ : \ |z_i| = 1, 1 \leq i \leq k\}.$$

To this end, consider the group of additive relations among the frequencies $\omega_1, \dots, \omega_k$:

$$S \overset{\text{def}}{=} \{\mathbf{a} \in \mathbb{Z}^k \ : \ a_1\omega_1 + \cdots + a_k\omega_k = 0\}.$$

The subgroup of the torus of interest respects the additive relations as follows:

$$\mathbb{T}_\omega \overset{\text{def}}{=} \{(\tau_1, \dots, \tau_k) \in \mathbb{T} \ : \ \text{for all } \mathbf{a} \in S,\ \tau_1^{a_1} \cdots \tau_k^{a_k} = 1\}.$$

Its desirable properties are summarised in the following proposition:

▶ **Proposition 3.1.** *For algebraic numbers $\omega_1, \dots, \omega_k$,*

1. *$\mathbb{T}_\omega$ is semi-algebraic,*
2. *diagonals of $\{R(t) \ : \ t \geq 0\}$ form a dense subset of $\mathbb{T}_\omega$.*

Proof. Being an Abelian subgroup of $\mathbb{Z}^k$, S has a finite basis, moreover this basis can be computed because of effective bounds, [18, Section 3]. To check that $(\tau_1, \dots, \tau_k)$ belongs to $\mathbb{T}_\omega$, it suffices to check that $\tau_1^{a_1} \cdots \tau_k^{a_k} = 1$ for $(a_1, \dots, a_k)$ in the finite basis. This forms a finite number of equations, therefore $\mathbb{T}_\omega$ is semi-algebraic. The fact that this is a subset of vectors of complex numbers is not problematic in this case because of the simple first-order interpretation in the theory of reals, see Remark 2.1.

The second statement of the proposition is a consequence of Kronecker's theorem on inhomogeneous simultaneous Diophantine approximations, see [5, Page 53, Theorem 4]. The proof of a slightly stronger statement can also be found in [6, Lemma 4]. Examples can be found where the set of diagonals of $\{R(t) \ : \ t \geq 0\}$ is a strict subset of $\mathbb{T}_\omega$. □

The orbit cone can now be defined by replacing the rotations with the subgroup of the torus. As it turns out, for our purposes this approximation is not too rough.

▶ **Definition 3.2.** *The* orbit cone *from $t_0 \geq 0$ is*

$$\mathcal{C}_{t_0} \overset{\text{def}}{=} \left\{P \ E(t) \ \mathrm{diag}(\boldsymbol{\tau}) \ Q(t) \ P^{-1}\mathbf{x}_0 \ : \ \boldsymbol{\tau} \in \mathbb{T}_\omega, t \geq t_0\right\}.$$

We prove that the cone is an inductive invariant and also a subset of $\mathbb{R}^d$.

▶ **Lemma 3.3.** *For all $\delta, t_0 \geq 0$, $e^{A\delta}\mathcal{C}_{t_0} \subseteq \mathcal{C}_{t_0}$.*

Proof. Fix $t \geq t_0$ and $\boldsymbol{\tau} \in \mathbb{T}_\omega$, and consider the point

$$\mathbf{v} = P \ E(t) \ \mathrm{diag}(\boldsymbol{\tau}) \ Q(t) \ P^{-1}\mathbf{x}_0 \in \mathcal{C}_{t_0},$$

then we can write $e^{A\delta}\mathbf{v}$ as

$$\begin{aligned} e^{A\delta}\mathbf{v} &= P \ E(\delta)R(\delta)Q(\delta) \cdot E(t)\mathrm{diag}(\boldsymbol{\tau})Q(t) \ P^{-1}\mathbf{x}_0 \\ &= P \ E(\delta + t) \ R(\delta)\mathrm{diag}(\boldsymbol{\tau}) \ Q(\delta)Q(t) \ P^{-1}\mathbf{x}_0. \end{aligned}$$

The matrix $R(\delta)\mathrm{diag}(\boldsymbol{\tau})$ is equal to $\mathrm{diag}(\boldsymbol{\tau}')$ for some $\boldsymbol{\tau}' \in \mathbb{T}_\omega$. Otherwise said, the vector $(e^{\delta\omega_1 \mathrm{i}}\tau_1, \dots, e^{\delta\omega_k \mathrm{i}}\tau_k)$ belongs to $\mathbb{T}_\omega$. Indeed this is the case because for any $\mathbf{a} \in S$ we have

$$e^{a_1\delta\omega_1\mathrm{i}}\tau_1^{a_1} \cdots e^{a_k\delta\omega_k\mathrm{i}}\tau_k^{a_k} = e^{\delta\mathrm{i} \ (a_1\omega_1 + \cdots + a_k\omega_k)} \cdot \tau_1^{a_1} \cdots \tau_k^{a_k} = 1.$$

Finally, by induction on the dimension d one can verify that $Q(\delta)Q(t) = Q(\delta + t)$. □

The fact that cones are subsets of $\mathbb{R}^d$ comes as a corollary of the following proposition which is proved in Appendix A.

▶ **Proposition 3.4.** *Let $A = PJP^{-1}$ as above, and let $C_i \in \mathbb{C}^{d_i \times d_i}$ for $i = 1, \ldots, k$, with dimensions compatible to the Jordan blocks of A, and such that for every i_1, i_2, if $B_{i_1} = \overline{B_{i_2}}$, then $C_{i_1} = \overline{C_{i_2}}$. Then $P\mathrm{diag}(C_1, \ldots, C_k)P^{-1}$ has real entries.*

The matrix $E(t)\mathrm{diag}(\tau)Q(t)$ can be written as $\mathrm{diag}(C_1, \ldots, C_k)$ where the C_i matrices satisfy the conditions of Proposition 3.4, hence the following corollary.

▶ **Corollary 3.5.** *For all $t_0 \geq 0$,*

$$\mathcal{C}_{t_0} \subseteq \mathbb{R}^d.$$

It is surprising that, already, the cones are a complete characterisation of o-minimal inductive invariants in the following sense.

▶ **Theorem 3.6.** *Let $\mathcal{I}$ be an o-minimal invariant that contains the orbit $\mathcal{O}(u)$ from some time $u \geq 0$, then there exists $t_0 \geq u$ such that:*

$$\mathcal{C}_{t_0} \subseteq \mathcal{I}.$$

Proof sketch. Conceptually, the proof follows along the lines of its analogue in [2]. There are a few differences, namely that the entries of the matrix A in [2] are assumed to be algebraic, while this is not true for the entries of e^A.

We define rays of the cone, which are subsets where $\boldsymbol{\tau} \in \mathbb{T}_\omega$ is fixed. Then we prove that for every ray, all but a finite part of it, is contained in the invariant. This is done by contradiction: if a ray is not contained in the invariant, a whole dense subset of the cone can be shown not to be contained in the invariant, leading to a contradiction, since the invariant is assumed to contain the orbit. We achieve this using some results on the topology of o-minimal sets.

The complete proof deferred to Appendix B.

◻

Another desirable property of cones is that they are $\mathfrak{R}_{\exp}$-definable. Also, one can observe that for every t_0, the set $\{e^{At}\mathbf{x}_0 : 0 \leq t \leq t_0\}$ is definable in $\mathfrak{R}_{\exp}^{\mathrm{RE}}$ (as we only need bounded restrictions of sin and cos to capture e.g. $e^{\mathrm{i}\omega_i}$ up to time t_0). As an immediate corollary of Theorem 3.6, we have the following theorems.

▶ **Theorem 3.7.** *Let $\langle A, \mathbf{x}_0 \rangle$ be a CDS. For every $t_0 \geq 0$, the set $\mathcal{C}_{t_0} \cup \{e^{At}\mathbf{x}_0 : 0 \leq t \leq t_0\}$ is an invariant that contains the whole orbit of $\langle A, \mathbf{x}_0 \rangle$. Moreover, this invariant is definable in $\mathfrak{R}_{\exp}^{\mathrm{RE}}$ (and in particular is o-minimal).*

▶ **Theorem 3.8.** *Let $\langle A, \mathbf{x}_0 \rangle$ be a CDS and let $Y \subseteq \mathbb{R}^d$ be an error set. There exists an o-minimal invariant $\mathcal{I}$ that contains the orbit and is disjoint from Y if and only if there exists t_0 such that $\mathcal{C}_{t_0} \cup \{e^{At}\mathbf{x}_0 : 0 \leq t \leq t_0\}$ is such an invariant.*

Theorem 3.8 now allows us to provide an algorithm for deciding the existence of an invariant, subject to Schanuel's conjecture:

▶ **Theorem 3.9.** *Assuming Schanuel's conjecture, given a CDS $\langle A, \mathbf{x}_0 \rangle$ and an $\mathfrak{R}_{\exp}^{\mathrm{RE}}$ definable error set Y, it is decidable whether there exists an o-minimal invariant for $\langle A, \mathbf{x}_0 \rangle$ that avoids Y. Moreover, if such an invariant exists, we can compute a representation of it.*

Proof. By Theorem 3.7, there exists an o-minimal invariant $\mathcal{I}$ that avoids Y if and only if there exists some $t_0 \in \mathbb{R}$ such that $\mathcal{C}_{t_0} \cup \{e^{At}\mathbf{x}_0 : 0 \le t \le t_0\}$ is such an invariant. Thus, the problem reduces to deciding the truth value of the following $\mathfrak{R}_{\exp}^{\mathrm{RE}}$ sentence:

$$\exists t_0 \;:\; (\mathcal{C}_{t_0} \cup \{e^{At}\mathbf{x}_0 : 0 \le t \le t_0\}) \cap Y = \emptyset$$

The theory of $\mathfrak{R}_{\exp}^{\mathrm{RE}}$ is decidable subject to Schanuel's conjecture, and therefore we can decide the existence of an invariant. Moreover, if an invariant exists, we can compute a representation of it by iterating over increasing values of t_0, until we find a value for which the sentence $\big(\mathcal{C}_{t_0} \cup \{e^{At}\mathbf{x}_0 : 0 \le t \le t_0\}\big) \cap Y = \emptyset$ is true. ◻

4 Semi-algebraic Error Sets and Fat Trajectory Cones

In this section, we restrict attention to semi-algebraic invariants and semi-algebraic error sets, in order to regain unconditional decidability.

Substitute $s = e^t$ in the definition of the cone to get:

$$\mathcal{C}_{t_0} = \big\{P\ E(\log s)\ \mathrm{diag}(\boldsymbol{\tau})\ Q(\log s)\ P^{-1}\mathbf{x}_0 \;:\; \boldsymbol{\tau} \in \mathbb{T}_\omega,\ s \ge e^{t_0}\big\}\,.$$

Written this way, observe that $E(\log s) = \mathrm{diag}(s^{\rho_1}, \ldots, s^{\rho_k})$, which is almost semi-algebraic, apart from the fact that the exponents need not be rational.

4.1 Unconditional Decidability

We give the final, yet crucial property of the cones. When the error set is semi-algebraic, it is possible to decide, unconditionally, whether there exists some cone that avoids the error set. Moreover the proof is constructive, it will produce the cone for which this property holds.

▶ **Theorem 4.1.** *For a semi-alegbraic error set Y, it is (unconditionally) decidable whether there exists $t_0 \ge 0$ such that $\mathcal{C}_{t_0} \cap Y = \emptyset$. Moreover, such a t_0 can be computed.*

Proof. Define the set

$$U \overset{\text{def}}{=} \big\{\mathcal{V} \in \mathbb{R}^{d\times d} \;:\; \forall \boldsymbol{\tau} \in \mathbb{T}_\omega,\;\; P\ \mathcal{V}\ \mathrm{diag}(\boldsymbol{\tau})\ P^{-1}\mathbf{x}_0 \in \mathbb{R}^d \setminus Y\big\}\,.$$

The set U can be seen to be semi-algebraic and thus is expressed by a quantifier-free formula that is a finite disjunction of formulas of the form $\bigwedge_{l=1}^{m} R_l(\mathcal{V}) \sim_l 0$, where each R_l is a polynomial with integer coefficients, over $d \times d$ variables of the entries of the matrix $\mathcal{V}$, and$\sim_l \in \{>, =\}$. Define the matrix

$$\Lambda(s) \overset{\text{def}}{=} \mathrm{diag}(s^{\rho_1}, \ldots, s^{\rho_k}) Q(\log s) \in \mathbb{R}^{d\times d},$$

and notice that $\mathcal{C}_{t_0} \cap Y = \emptyset$ if and only if $\Lambda(s) \in U$ for every $s \ge e^{t_0}$. Thus, it is enough to decide whether there exists $s_0 \ge 1$ such that for every $s \ge s_0$, at least one of the disjuncts $\bigwedge_{l=1}^{m} R_l(\Lambda(s)) \sim_l 0$ is satisfied.

Since $R_l(\Lambda(s))$ are polynomials in entries of the form s^{ρ_i} and $\log(s)$, there is an effective bound s_0 such that for all $s \ge s_0$, none of the values $R_l(\Lambda(s))$ change sign for any $1 \le l \le m$. Hence we only need to decide whether there exists some $s_0' \ge s_0$ such that for all $s \ge s_0'$ we have $R_l(\Lambda(s)) \sim_l 0$ for every $1 \le l \le m$.

Fix some l. The polynomial $R_l(v_1, \ldots, v_D)$ has the form $\sum_i a_i v_1^{n_{i,1}} \cdots v_D^{n_{i,D}}$. After identifying the matrix $\Lambda(s)$ with a vector in $\mathbb{R}^D$ for $D = d^2$, we see that $R_l(\Lambda(s))$ is a sum of terms of the form

$$a_i s^{n'_{i,1}\rho_1 + \ldots n'_{i,k}\rho_k} \cdot Q_{i,1}(\log s) \cdots Q_{i,D}(\log s)$$

where the $n'_{i,j}$ are aggregations of the $n_{i,j}$ for identical entries of $\mathrm{diag}(s_1^\rho, \dots, s_k^\rho)$, and $Q_{i,j}(\log s)$ are polynomials obtained from the entries of $Q(\log s)$ under R_l. We can join the polynomials $Q_1, \dots, Q_D$ into a single polynomial f_i, which would also absorb a_i. Thus, we rewrite R_l in the form $\sum_i s^{n'_{i,1}\rho_1 + \dots n'_{i,k}\rho_k} f_i(\log s)$ where each f_i is a polynomial with rational coefficients (as the coefficients in $Q(\log s)$ are rational).

In order to reason about the sign of this expression as $s \to \infty$, we need to find the leading term of $R_l(\Lambda(s))$. This, however, is easy: the exponents $n'_{i,1}\rho_1 + \dots + n'_{i,k}\rho_k$ are algebraic numbers, and are therefore susceptible to effective comparison. Thus, we can order the terms by magnitude. Then, we can determine the asymptotic sign of each coefficient $f_i(\log s)$ by looking at the leading term in f_i.

We can thus determine the asymptotic behaviour of each $R_l(\Lambda(s))$, to conclude whether $\bigwedge_{l=1}^m R_l(\Lambda(s)) \sim_l 0$ eventually holds. Moreover, for rational s, every quantity above can be computed to arbitrary precision, therefore it is possible to compute a threshold s'_0, after which, for all $s \geq s'_0$, $\bigwedge_{l=1}^m R_l(\Lambda(s)) \sim_l 0$ holds. This completes the proof. ◻

▶ **Theorem 4.2.** *For a semi-algebraic set Y, it is decidable whether there exists a o-minimal invariant, disjoint from Y, that contains the orbit $\mathcal{O}(u)$ after some time $u \geq 0$. Moreover in the positive instances an invariant that is $\mathfrak{R}_{\exp}$-definable can be constructed.*

Proof. If there is an invariant $\mathcal{I}$ that contains $\mathcal{O}(u)$, for some $u \geq 0$, then Theorem 3.6 implies that there exists some $t_0 \geq u$ such that $\mathcal{C}_{t_0}$ is contained in $\mathcal{I}$. Consequently, the question that we want to decide is equivalent to the question of whether there exists a t_0, such that $\mathcal{C}_{t_0} \cap Y = \emptyset$. The latter is decidable thanks to Theorem 4.1. The effective construction follows from the fact that such a t_0 is computable and that the cone is $\mathfrak{R}_{\exp}$-definable. ◻

4.2 Effectively Constructing the Semi-algebraic Invariant

We now turn to show that in fact, for semi-algebraic error sets Y, we can approximate $\mathcal{C}_{t_0}$ with a semi-algebraic set such that if $\mathcal{C}_{t_0}$ avoids Y, so does the approximation. Intuitively, this is done by relaxing the "non semi-algebraic" parts of $\mathcal{C}_{t_0}$ in order to obtain a *fat cone*. This relaxation has two parts: one is to "rationalize" the (possibly irrational) exponents $\rho_1, \dots, \rho_k$, and the other is to approximate the polylogs in $Q(\log s)$ by polynomials.

Relaxing the exponents. We start by approximating the exponents $\rho_1, \dots, \rho_k$ with rational numbers. We remark that naively taking rational approximations is not sound, as the approximation must also adhere to the additive relationships of the exponents.

Let $\boldsymbol{\ell} = (\ell_1, \dots, \ell_k)$ and $\mathbf{u} = (u_1, \dots, u_k)$ be tuples of rational numbers such that $\ell_i \leq \rho_i \leq u_i$ for $i = 1, \dots, k$. Define $\mathbb{S} \subseteq \mathbb{R}^k$ as:

$$\mathbb{S} \overset{\text{def}}{=} \left\{ (q_1, \dots, q_k) \in \mathbb{R}^k \ : \ \forall n_1, \dots, n_k \in \mathbb{Z}, \ \left(\sum_{i=1}^k n_i \rho_i = 0 \Rightarrow \sum_{i=1}^k n_i q_i = 0 \right) \right\}$$

Thus, $\mathbb{S}$ captures the integer additive relationships among the ρ_i. Define

$$\mathrm{Box}(\boldsymbol{\ell}, \mathbf{u}) \overset{\text{def}}{=} \{\mathrm{diag}(\mathbf{q}) \ : \ \boldsymbol{\ell} \leq \mathbf{q} \leq \mathbf{u}, \mathbf{q} \in \mathbb{S}\}.$$

Approximating polylogs. Let $\epsilon, \delta > 0$. We simply replace $\log s$ by r such that $\delta \leq r \leq s^\epsilon$. Note that it is not necessarily the case that $\delta \leq \log s \leq s^\epsilon$, so this replacement is a-priori not sound. However, for large enough s the inequalities do hold, which will suffice for our purposes.

We can now define the fat cone. Let $\epsilon, \delta > 0$ and $\boldsymbol{\ell} = (\ell_1, \dots, \ell_k)$ and $\mathbf{u} = (u_1, \dots, u_k)$ as above, the fat orbit cone $\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}}$ is the set:

$$\left\{ P \ \mathrm{diag}(s^{q_1}, \dots, s^{q_k})\mathrm{diag}(\boldsymbol{\tau}) \ Q(r)P^{-1}\mathbf{x}_0 \ : \ \boldsymbol{\tau} \in \mathbb{T}_\omega, \ s \geq s_0, \ \delta \leq r \leq s^\epsilon, \ \mathbf{q} \in \mathrm{Box}(\boldsymbol{\ell}, \mathbf{u}) \right\}.$$

That is, the fat cone is obtained from $\mathcal{C}_{t_0}$ with the following changes:

- $R(\log s) = \mathrm{diag}(s^{\rho_1}, \dots, s^{\rho_k})$ is replaced with $\mathrm{diag}(s^{q_1}, \dots, s^{q_k})$, where the q_i are rational approximations of the ρ_i, and maintain the additive relationships.
- $Q(\log s)$ is replaced with $Q(r)$ where $\delta \leq r \leq s^\epsilon$.
- The variable s starts from s_0 (as opposed to e^{t_0}).

We first show that the fat cone is semi-algebraic (the proof is in Appendix C), then proceed to prove that if there is a cone that avoids the error set, then there is a fat one that avoids it as well.

▶ **Lemma 4.3.** *$\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}}$ is definable in $\mathfrak{R}_0$, and we can compute a representation of it.*

▶ **Lemma 4.4.** *Let $Y \subseteq \mathbb{R}^d$ be a a semi-algebraic error set such that $\mathcal{C}_{t_0} \cap Y = \emptyset$ for some $t_0 \in \mathbb{R}$, then there exists $\delta, \epsilon, s_0, \boldsymbol{\ell}, \boldsymbol{u}$ as above such that*

1. *$\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\boldsymbol{u}} \cap Y = \emptyset$, and*
2. *for every $t \geq 0$ it holds that $e^{At} \cdot \mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\boldsymbol{u}} \subseteq \mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\boldsymbol{u}}$.*

The result is constructive, so when t_0 is given, the constants $s_0, \epsilon, \delta, \boldsymbol{\ell}, \mathbf{u}$ can be computed. It follows that a corollary of this lemma, and Lemma 4.3, is a stronger statement than that of Theorem 4.2, namely one where $\mathfrak{R}_{\exp}$ is replaced by $\mathfrak{R}_0$. We state it here before moving on with the proof of Lemma 4.4.

▶ **Theorem 4.5.** *For a semi-algebraic set Y, it is decidable whether there exists a o-minimal invariant, disjoint from Y, that contains the orbit $\mathcal{O}(u)$ after some time $u \geq 0$. Moreover in the positive instances an invariant that is $\mathfrak{R}_0$-definable can be constructed.*

The proof of Lemma 4.4 is given by the two corresponding steps. The second step, proving the invariance of the fat cone, is Lemma C.1 in Appendix C. We turn our attention to the first step.

▶ **Lemma 4.6.** *Let $Y \subseteq \mathbb{R}^d$ be a semi-algebraic error set, and let $t_0 \in \mathbb{R}$ be such that $\mathcal{C}_{t_0} \cap Y = \emptyset$, then there exists $\delta, \epsilon, s_0, \boldsymbol{\ell}, \mathbf{u}$ as above such that $\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}} \cap Y = \emptyset$.*

Proof. We use the same analysis and definitions of U, R_l, $\sim_l$, $\Lambda(s)$ as in the proof of Theorem 4.1 and focus on a single polynomial R_l. Recall that we had

$$R_l(\Lambda(s)) = \sum_i s^{n_{i,1}\rho_1 + \dots n_{i,k}\rho_k} f_i(\log s) \tag{1}$$

where each f_i is a polynomial with rational coefficients.

Denote $\boldsymbol{\rho} = (\rho_1, \dots, \rho_k)$. We show, first, how to replace the exponents vector $\boldsymbol{\rho}$ by any exponents vector in $\mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$ for appropriate $\boldsymbol{\ell}, \mathbf{u}$, and second, how to replace $\log s$ by r where $\delta \leq r \leq s^\epsilon$ for some appropriate δ and ϵ, while maintaining the inequality or equality prescribed by $\sim_l$.

Denote by N the set of vectors $\mathbf{n_i} = (n_{i,1}, \dots, n_{i,k})$ of exponents in (1). Let $\mu > 0$, such that for every $\mathbf{n}, \mathbf{n'} \in N$, if $\boldsymbol{\rho} \cdot (\mathbf{n} - \mathbf{n'}) \neq 0$ then $|\boldsymbol{\rho} \cdot (\mathbf{n} - \mathbf{n'})| > \mu$. That is, μ is a lower bound on the minimal difference between distinct exponents in (1). Observe that we can compute a description of μ, as the exponents are algebraic numbers.

Let $M = \max_{\mathbf{n},\mathbf{n'} \in N} \|\mathbf{n} - \mathbf{n'}\|$ (where $\|\cdot\|$ is the Euclidean norm in $\mathbb{R}^k$).

▷ Claim 4.7. Let $\mathbf{c} \in \mathbb{R}^k$ be such that $\|\boldsymbol{\rho} - \mathbf{c}\| \leq \frac{\mu}{2M}$, then, for all $\mathbf{n}, \mathbf{n'} \in N$, if $\boldsymbol{\rho}\cdot(\mathbf{n}-\mathbf{n'}) > 0$ then $\mathbf{c} \cdot (\mathbf{n} - \mathbf{n'}) > \frac{\mu}{2}$.

Proof of Claim 4.7. Suppose that $\boldsymbol{\rho}\cdot(\mathbf{n}-\mathbf{n'}) > 0$, then by the above we have $\boldsymbol{\rho}\cdot(\mathbf{n}-\mathbf{n'}) > \mu$, and hence

$$\begin{aligned}\mathbf{c} \cdot (\mathbf{n} - \mathbf{n'}) &= \boldsymbol{\rho} \cdot (\mathbf{n} - \mathbf{n'}) + (\mathbf{c} - \boldsymbol{\rho}) \cdot (\mathbf{n} - \mathbf{n'}) \\ &\geq \mu - \|\mathbf{c} - \boldsymbol{\rho}\| \cdot \|\mathbf{n} - \mathbf{n'}\| \\ &\geq \mu - \frac{\mu}{2M} M = \frac{\mu}{2}.\end{aligned}$$

□

We can now choose $\boldsymbol{\ell}$ and $\mathbf{u}$ such that $u_i - \ell_i \leq \frac{\mu}{2M\sqrt{k}}$ and for all $\mathbf{c} \in \mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$ we have

$$\|\boldsymbol{\rho} - \mathbf{c}\| \leq \sqrt{\sum_{i=1}^{k}(u_i - \ell_i)^2} \leq \sqrt{\frac{\mu^2}{(2M)^2}} = \frac{\mu}{2M}.$$

It follows from Claim 4.7 and from the definition of $\mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$ that, intuitively, every $\mathbf{c} \in \mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$ maintains the order of magnitude of the monomials $s^{n_{i,1}\cdot\rho_1+\ldots+n_{i,k}\cdot\rho_k}$ in $R_l(\Lambda(s))$.

More precisely, let $\Lambda'(s) = \mathrm{diag}(s^{c_1}, \ldots, s^{c_k})Q(\log s)$ for some $\mathbf{c} \in \mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$, then the exponent of the ratio of every two monomials in $R_l(\Lambda'(s))$ has the same (constant) sign as the corresponding exponent in $R_l(\Lambda(s))$. Moreover, the exponents of distinct monomials in $R_l(\Lambda(s))$ differ by at least $\frac{\mu}{2}$ in $R_l(\Lambda'(s))$.

We now turn our attention to the $\log s$ factor. First, let s_0 be large enough that $f_i(\log s)$ has constant sign for every $s \geq s_0$. We can now let δ be large enough such that for every $r \geq \delta$, the sign of $f_i(\log s)$ coincides with the sign of $f_i(r)$ for every $s \geq s_0$. It remains to give an upper bound on r of the form s^ϵ such that plugging $f_i(r)$ instead of $f_i(\log s)$ does not change the ordering of the terms (by their magnitude) in $R_l(\Lambda'(s))$.

Let B be the maximum degree of all polynomials f_i in (1), and define $\epsilon = \frac{\mu}{3B}$ (in fact, any $\epsilon < \frac{\mu}{2B}$ would suffice), then we have that, for $s \geq s_0$, $f_i(r)$ has the same sign as $f_i(\log s)$ for every $\delta \leq r \leq s^\epsilon$ (by our choice of δ), and guarantees that plugging s^ϵ instead of s does not change the ordering of the terms (by their magnitude) in R_l. Since the exponents of the monomials in $R_l(\Lambda'(s))$ differ by at least $\frac{\mu}{2}$, it follows that their order is maintained when replacing $\log s$ by $\delta \leq r \leq s^\epsilon$.

Let $\Lambda''(s) = \mathrm{diag}(s^{c_1}, \ldots, s^{c_k})Q(r)$ for some $\mathbf{c} \in \mathrm{Box}(\boldsymbol{\ell}, \mathbf{u})$ and $\delta \leq r \leq s^\epsilon$, then by our choice of ϵ, the dominant term in $R_l(\Lambda''(s))$ is the same as that in $R_l(\Lambda(s))$. Therefore, for large enough s, the signs of $R_l(\Lambda''(s))$ and $R_l(\Lambda(s))$ are the same.

Note that since $\mathcal{C}_{t_0} \cap Y = \emptyset$, then w.l.o.g. $R_l(\Lambda(s)) \sim_l 0$ for every l. Thus, by repeating the above argument for each R_l, we can compute $s_0 \in \mathbb{R}$, $\epsilon > 0$, $\delta \in \mathbb{R}$, and $\boldsymbol{\ell}, \mathbf{u} \in \mathbb{Q}^k$ such that $\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}} \cap Y = \emptyset$, and we are done. □

5 A Reduction from Zeros of an Exponential Polynomial

In Theorem 4.5, we showed unconditional decidability for the question of whether there exists an invariant containing the orbit $\mathcal{O}(u)$, for some $u \geq 0$. Even though we construct such an invariant, it cannot be used as a certificate proving that the orbit never enters the error set; however it is a certificate that the orbit of the system does not enter Y *after* time u.

In this section we give indications that deciding whether there exists an invariant that takes into account the orbit $\leq u$ is difficult. More precisely, we will reduce a problem about zeros of a certain exponential polynomial to the question of whether there exists a semi-algebraic invariant disjoint from Y containing $\mathcal{O}(0)$.

▶ Remark 5.1. In the setting of discrete linear dynamical systems, the existence of a semi-algebraic invariant from time t_0 immediately implies the existence of one from time 0. This is because the system goes through finitely many points from 0 to t_0, which can be added one by one to the semi-algebraic set. In this respect CDSs are more complicated to analyse.

The problem that we reduce from, can be stated as follows. We are given as input real algebraic numbers $a_1, \dots, a_n, \rho_1, \dots, \rho_n$, and $t_0 \in \mathbb{Q}$, and asked to decide whether the function:

$$f(t) \stackrel{\text{def}}{=} a_1 e^{\rho_1 t} + \cdots + a_n e^{\rho_n t},$$

has any zeros in the interval $[0, t_0]$.

While there has been progress on characterising the asymptotic distribution of complex zeros of such systems, less is known about the real zeros, and we lack any effective characterisation, see [4] and the references therein. The difficulty of knowing whether f has a zero in the specified region is because (a) all the zeros have to be transcendental (a consequence the Hermite-Lindemann Theorem) and (b) there can be tangential zeros, that is f has a zero but it never changes its sign. See the discussion in [4, Section 6]. Finding the zeros of such a polynomial is a special case of the *bounded* continuous Skolem-Pisot problem. We note that when ρ_i are all rational the problem is equivalent to a sentence of $\mathfrak{R}_0$ (and hence decidable) by replacing $t = \log s$.

The rest of this section is devoted to the proof of the following theorem.

▶ **Theorem 5.2.** *For every exponential polynomial f we can construct a CDS $\langle A, \mathbf{x}_0 \rangle$ and semi-algebraic set Y such that the following two statements are equivalent:*

- *there exists a semi-algebraic invariant disjoint from Y that contains $\mathcal{O}(0)$,*
- *f does not have a zero in $[0, t_0]$.*

Fix the function f, *i.e.* real algebraic numbers $a_1, \dots, a_n, \rho_1, \dots, \rho_n$ and $t_0 \in \mathbb{Q}$. Without loss of generality we can assume that $\rho_1, \dots, \rho_n$ are all nonnegative, since $e^{\rho t} f(t) = 0$ if and only if $f(t) = 0$ where ρ is larger than all $\rho_1, \dots, \rho_n$.

Since every ρ_i is algebraic, there is a minimal polynomial p_i, that has ρ_i as a simple root. Let A be the $d \times d$ companion matrix of the polynomial $p_1(x) \cdots p_n(x) x^2$. The numbers ρ_i are eigenvalues A of multiplicity one, and the latter also has zero as an eigenvalue of multiplicity two. In addition to those, the matrix A generally has other (complex) eigenvalues as well. We put A in Jordan normal form, $P^{-1}AP = J$ where J is made of two block diagonals: $\tilde{A}$ and B, where

$$\tilde{A} \stackrel{\text{def}}{=} \begin{pmatrix} \operatorname{diag}(\rho_1, \dots, \rho_n) & & \\ & 0 & 1 \\ & 0 & 0 \end{pmatrix},$$

and B is some $(d - n - 2) \times (d - n - 2)$ matrix. Define:

$$\tilde{\mathbf{x}}_0 \stackrel{\text{def}}{=} (\underbrace{1, \dots, 1}_{n+2}, 0, \dots, 0),$$

the vector that has $n + 2$ ones and the rest, $d - (n + 2)$ zeros, whose purpose is to ignore the contribution of the eigenvalues in matrix B in the system. To simplify notation, since $\tilde{\mathbf{x}}_0$ is ignoring the contribution of the matrix B, the dynamics of the system $\langle J, \tilde{\mathbf{x}}_0\rangle$ can be assume to be the same as:

$$e^{\tilde{A}t}(1,\ldots,1) = (e^{\rho_1 t},\ldots,e^{\rho_n t},t).$$

Focus on a single eigenvalue, *i.e.* on the graph $\{(e^{\rho t},t) \ : \ t \geq 0\}$, as the analysis will easily generalise to the CDS in question. This is itself a CDS, so terminology such as orbits *etc.* make sense. The challenge is to find a family of *tubes* around this exponential curve such that (a) all the tubes together with $\{(y,t) \ : \ t \geq t_0\}$ are invariants and (b) then tubes are arbitrarily close approximations of the curve.

We achieve this by the following families of polynomials:

- under-approximations are given by the family indexed by $n \in \mathbb{N}$:

$$P_n(t) \overset{\text{def}}{=} \sum_{k=0}^{n} \frac{(\rho t)^k}{k!}.$$

- over-approximations are given by a family indexed by $n \in \mathbb{N}$ and $\mu > 1$:

$$Q_{n,\mu}(t) \overset{\text{def}}{=} P_n(\mu t).$$

Define:

$$\mathcal{I}_{n,\mu} \overset{\text{def}}{=} \{(y,t) \ : \ P_n(t) \leq y \leq Q_{n,\mu}(t) \text{ and } 0 \leq t \leq t_0\}\,.$$

It is clear from Taylor's theorem and the assumption that $\rho > 0$ that by taking $n \to \infty$, and $\mu \to 1^+$ the sets $\mathcal{I}_{n,\mu}$ are arbitrary precise approximations of the graph $\{(e^{\rho t},t) \ : \ t \geq 0\}$, what remains to show is that they are invariant.

▶ **Lemma 5.3.** *For every $\mu > 1$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ the set*

$$\mathcal{I}_{n,\mu} \cup \{(y,t) \ : \ t > t_0\}$$

is an invariant containing the whole orbit, i.e. $\{(e^{\rho t},t) \ : \ t \geq 0\}$.

The proof is in Appendix D.

We can construct such invariants for every curve $e^{\rho_i t}$, and thus build $\tilde{\mathcal{I}}_{n,\mu}$ for

$$\left\{(e^{\rho_1 t},\ldots,e^{\rho_n t},t) \ : \ t \geq 0\right\}.$$

To prove Theorem 5.2 we define $\tilde{Y}$ by the formula

$$\Phi(x_1,\ldots,x_n,x_{n+1}) \overset{\text{def}}{=} a_1x_1 + \cdots + a_nx_n = 0 \text{ and } 0 \leq x_{n+1} \leq t_0.$$

Since the analysis was done on the CDS $\langle J, \tilde{\mathbf{x}}_0\rangle$, whose entries are not rational in general, before proceeding with the proof of Theorem 5.2, we need the following lemma to say that changing basis does not have an effect in the decision problem at hand:

▶ **Lemma 5.4.** *For every $\tilde{Y}$ semi-algebraic, there exists another semi-algebraic set Y and $\mathbf{x}_0$ with rational entries such that the following two statements are equivalent:*

- *$\langle J, \tilde{\mathbf{x}}_0\rangle$ has a semi-algebraic invariant disjoint from $\tilde{Y}$, containing the whole orbit,*
- *$\langle PJP^{-1}, \mathbf{x}_0\rangle$ has a semi-algebraic invariant disjoint from Y, containing the whole orbit.*

The proof is postponed to Appendix D. Thanks to this lemma, we can prove Theorem 5.2 for the CDS $\langle J, \tilde{\mathbf{x}}_0\rangle$ and the set $\tilde{Y}$ instead. This is done as follows. The direct implication is trivial. For the converse, observe that $f(t)$ does not have a zero in $[0,t_0]$ if and only if the $\mathcal{O}(0)$ and $\tilde{Y}$ are disjoint. Since both $\mathcal{O}(0)$ and $\tilde{Y}$ are closed sets, we can find a tube that contains $\mathcal{O}(0)$ and is disjoint from $\tilde{Y}$, *i.e.* there exists some $\mu > 1$ and $n \in \mathbb{N}$ such that

$$\tilde{\mathcal{I}}_{n,\mu} \cup \{(y,t) \ : \ t > t_0\},$$

is an invariant that is disjoint from $\tilde{Y}$ but contains $\mathcal{O}(0)$.

References

1 Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for discrete-time dynamical systems. (preprint, submitted).

2 Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for linear loops. In *45th International Colloquium on Automata, Languages, and Programming ICALP*, pages 1–14. Schloss Dagstuhl, 2018.

3 Rajeev Alur. *Principles of cyber-physical systems.* MIT Press, 2015.

4 Paul C. Bell, Jean-Charles Delvenne, Raphaël M. Jungers, and Vincent D. Blondel. The continuous skolem-pisot problem. *Theor. Comput. Sci.*, 411(40–42):3625–3634, September 2010.

5 John W.S. Cassels. *An Introduction to Diophantine Approximation.* Cambridge University Press, 1965.

6 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On recurrent reachability for continuous linear dynamical systems. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 515–524, 2016.

7 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the skolem problem for continuous linear dynamical systems. In *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016).* Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

8 Patrick Cousot. Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In *Verification, Model Checking, and Abstract Interpretation, 6th International Conference, VMCAI 2005, Paris, France, January 17-19, 2005, Proceedings*, pages 1–24, 2005.

9 Patrick Cousot and Nicolas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth Annual ACM Symposium on Principles of Programming Languages, Tucson, Arizona, USA, January 1978*, pages 84–96, 1978.

10 L. P. D. van den Dries. *Tame Topology and O-minimal Structures.* London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

11 Nathanaël Fijalkow, Pierre Ohlmann, Joël Ouaknine, Amaury Pouly, and James Worrell. Semialgebraic invariant synthesis for the kannan-lipton orbit problem. In *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*, pages 29:1–29:13, 2017.

12 Khalil Ghorbal, Andrew Sogokon, and André Platzer. A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets. *Comput. Lang. Syst. Struct.*, 47:19–43, 2017.

13 Sumit Gulwani and Ashish Tiwari. Constraint-based approach for analysis of hybrid systems. In *Computer Aided Verification, 20th International Conference, CAV 2008, Proceedings*, volume 5123 of *Lecture Notes in Computer Science*, pages 190–203. Springer, 2008.

14 Emmanuel Hainry. Reachability in linear dynamical systems. In Arnold Beckmann, Costas Dimitracopoulos, and Benedikt Löwe, editors, *Logic and Theory of Algorithms*, pages 241–250, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

15 Jiang Liu, Naijun Zhan, and Hengjun Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. In *Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011*, pages 97–106. ACM, 2011.

16 Angus Macintyre. Turing meets schanuel. *Annals of Pure and Applied Logic*, 167(10):901–938, 2016.

17 Angus Macintyre and Alex J. Wilkie. On the decidability of the real exponential field. In Piergiorgio Odifreddi, editor, *Kreiseliana. About and Around Georg Kreisel*, pages 441–467. A K Peters, 1996.

18 David W Masser. Linear relations on algebraic groups. *New Advances in Transcendence Theory*, pages 248–262, 1988.

19 Enric Rodríguez-Carbonell and Deepak Kapur. Generating all polynomial invariants in simple loops. *J. Symb. Comput.*, 42(4):443–476, 2007.

20 Enric Rodríguez-Carbonell and Ashish Tiwari. Generating polynomial invariants for hybrid systems. In *Hybrid Systems: Computation and Control, 8th International Workshop, HSCC 2005, Proceedings*, volume 3414 of *Lecture Notes in Computer Science*, pages 590–605. Springer, 2005.

21 Andrew Sogokon, Khalil Ghorbal, Paul B. Jackson, and André Platzer. A method for invariant generation for polynomial continuous systems. In *Verification, Model Checking, and Abstract Interpretation - 17th International Conference, VMCAI, Proceedings*, volume 9583 of *Lecture Notes in Computer Science*, pages 268–288. Springer, 2016.

22 Thomas Sturm and Ashish Tiwari. Verification and synthesis using real quantifier elimination. In *Symbolic and Algebraic Computation, International Symposium, ISSAC 2011, Proceedings*, pages 329–336. ACM, 2011.

23 Alfred Tarski. A decision method for elementary algebra and geometry. *RAND Corporation, R-109*, 1951.

24 Lou van den Dries, Angus Macintyre, and David Marker. The elementary theory of restricted analytic fields with exponentiation. *Annals of Mathematics*, 140(1):183–205, 1994.

25 Lou Van den Dries, Chris Miller, et al. Geometric categories and o-minimal structures. *Duke Math. J*, 84(2):497–540, 1996.

26 A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted pfaffian functions and the exponential function. *Journal of the American Mathematical Society*, 9(4):1051–1094, 1996.

A Proof of Proposition 3.4

▶ **Proposition 3.4.** *Let $A = PJP^{-1}$ as above, and let $C_i \in \mathbb{C}^{d_i \times d_i}$ for $i = 1, \dots, k$, with dimensions compatible to the Jordan blocks of A, and such that for every i_1, i_2, if $B_{i_1} = \overline{B_{i_2}}$, then $C_{i_1} = \overline{C_{i_2}}$. Then $P\mathrm{diag}(C_1, \dots, C_k)P^{-1}$ has real entries.*

Write $P = \begin{pmatrix} P_1 & \cdots & P_k \end{pmatrix}$ with P_i having dimension $d \times d_i$ for $i \in \{1, \dots, k\}$. The condition $A = PJP^{-1}$ is equivalent to $AP = PJ$, which in turn is equivalent to $AP_i = P_iJ_i$ for $i = \{1, \dots, k\}$. Now if $AP_i = P_iJ_i$ then $\overline{AP_i} = \overline{P_iJ_i}$ and hence we may assume without loss of generality that for $i_1, i_2 \in \{1, \dots, k\}$, if $\overline{J_{i_1}} = J_{i_2}$ then $\overline{P_{i_1}} = P_{i_2}$. Equivalently we may assume that $\overline{P} = PM$ for M a permulation matrix that interchanges column (i_1, j) of P with column (i_2, j) such that $\overline{J_{i_1}} = J_{i_2}$. Then we have

$$\begin{aligned}
\overline{P\,\mathrm{diag}(B_1, \dots, B_k)P^{-1}} &= \overline{P}\,\mathrm{diag}(\overline{B_1}, \dots, \overline{B_k})\overline{P}^{-1} \\
&= PM\mathrm{diag}(\overline{B_1}, \dots, \overline{B_k})M^{-1}P^{-1} \\
&= P\mathrm{diag}(B_1, \dots, B_k)P^{-1}\,.
\end{aligned}$$

Hence $P\,\mathrm{diag}(B_1, \dots, B_k)P^{-1}$ is real. □

B Proof of Theorem 3.6

▶ **Theorem 3.6.** *Let $\mathcal{I}$ be an o-minimal invariant that contains the orbit $\mathcal{O}(u)$ from some time $u \geq 0$, then there exists $t_0 \geq u$ such that:*

$$\mathcal{C}_{t_0} \subseteq \mathcal{I}.$$

Before proceeding with the proof, we give some useful definitions and properties of o-minimal theories. Consider an o-minimal theory $\mathfrak{R}$.

A function $f\colon B \to \mathbb{R}^m$ with $B \subseteq \mathbb{R}^n$ is *definable* in $\mathfrak{R}$ if its graph $\Gamma(f) = \{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in B\} \subseteq \mathbb{R}^{n+m}$ is an $\mathfrak{R}$-definable set.

O-minimal theories admit the following properties (see [10] for precise definitions and proofs).

1. For an $\mathfrak{R}$-definable set $S \subseteq \mathbb{R}^d$, its topological closure $\overline{S}$ is also $\mathfrak{R}$-definable.
2. For an $\mathfrak{R}$-definable function $f\colon S \to \mathbb{R}$, the number $\inf\{f(\mathbf{x}) \ : \ \mathbf{x} \in S\}$ is $\mathfrak{R}$-definable (as a singleton set).
3. O-minimal structures admit *cell decomposition*: every $\mathfrak{R}$-definable set $S \subseteq \mathbb{R}^d$ can be written as a finite union of connected components called *cells*. Moreover, each cell is $\mathfrak{R}$-definable and homeomorphic to $(0,1)^m$ for some $m \in \{0,1,\dots,d\}$ (where for $m=0$ we have that $(0,1)^0$ is a single point, namely $\{\mathbf{0}\} \subseteq \mathbb{R}^d$). The *dimension* of S is defined as the maximal such m occurring in the cell decomposition of S.
4. For an $\mathfrak{R}$-definable function $f\colon S \to \mathbb{R}^m$, the dimension of its graph $\Gamma(f)$ is the same as the dimension of S.

We recall the definition of the orbit cone:

$$\mathcal{C}_{t_0} \stackrel{\text{def}}{=} \left\{P\ E(t)\ \mathrm{diag}(\tau)\ Q(t)\ P^{-1}\mathbf{x}_0 \ : \ \tau \in \mathbb{T}_\omega, t \geq t_0\right\},$$

and define the *orbit rays* for $\tau \in \mathbb{T}_\omega$:

$$\mathrm{r}(\tau, t_0) \stackrel{\text{def}}{=} \left\{P\ E(t)\ \mathrm{diag}(\tau)\ Q(t)\ P^{-1}\mathbf{x}_0 \ : \ t \geq t_0\right\}.$$

Fix $\mathcal{I}$ to be an o-minimal invariant, with $\mathcal{O} \subseteq \mathcal{I}$ definable in $\mathfrak{R}$. To prove Theorem 3.6, we begin by making following claims of increasing strength:

▷ Claim B.1. For every $\boldsymbol{\tau} \in \mathbb{T}_\omega$ there exists $t_0 \geq 0$ such that $\mathrm{r}(\boldsymbol{\tau}, t_0) \subseteq \mathcal{I}$ or $\mathrm{r}(\boldsymbol{\tau}, t_0) \cap \mathcal{I} = \emptyset$.

▷ Claim B.2. For every $\boldsymbol{\tau} \in \mathbb{T}_\omega$ there exists $t_0 \geq 0$ such that $\mathrm{r}(\boldsymbol{\tau}, t_0) \subseteq \mathcal{I}$.

▷ Claim B.3. There exists $t_0 \geq 0$ such that for every $\boldsymbol{\tau} \in \mathbb{T}_\omega$ we have $\mathrm{r}(\boldsymbol{\tau}, t_0) \subseteq \mathcal{I}$.

Proof of Claim B.1. Fix $\boldsymbol{\tau} \in \mathbb{T}_\omega$. Then the set

$$\{t \geq 0 \ : \ P\ E(t)\ \mathrm{diag}(\boldsymbol{\tau})\ Q(t) P^{-1}\mathbf{x}_0 \in \mathcal{I}\}$$

is $\mathfrak{R}$-definable and hence comprises a finite union of intervals. If this set contains an unbounded interval then there exists t_0 such that $\mathrm{r}(\boldsymbol{\tau}, t_0) \subseteq \mathcal{I}$; otherwise there exists t_0 such that $\mathrm{r}(\boldsymbol{\tau}, t_0) \cap \mathcal{I} = \emptyset$. □

Proof of Claim B.2. We strengthen Claim B.1. Assume by way of contradiction that there exist $\boldsymbol{\tau} \in \mathbb{T}_\omega$ and $t_0 \in \mathbb{R}$ such that $\mathrm{r}(\boldsymbol{\tau}, t_0) \cap \mathcal{I} = \emptyset$. Without loss of generality assume that $t_0 > 1$, and consider $e^{-A} \cdot \mathrm{r}(\boldsymbol{\tau}, t_0)$. Recall from analysis of e^{At} the decomposition:

$$e^{-A} = P\ E(-1)\ R(-1)\ Q(-1)\ P^{-1},$$

and let $\boldsymbol{\tau}' \in \mathbb{T}_\omega$ be equal to $R(-1)\mathrm{diag}(\boldsymbol{\tau})$. In other words, $\mathrm{diag}(\boldsymbol{\tau}) = \mathrm{diag}(\boldsymbol{\tau}')R(1)$ and hence $e^A \mathrm{r}(\boldsymbol{\tau}', t_0 - 1) = \mathrm{r}(\boldsymbol{\tau}, t_0)$ (this is implicitly shown in the proof of Lemma 3.3). Since $\mathcal{I}$ is invariant we have $\mathrm{r}(\boldsymbol{\tau}', t_0 - 1) \cap \mathcal{I} = \emptyset$, and consequently $\mathrm{r}(\boldsymbol{\tau}', t_0)$ itself is disjoint from $\mathcal{I}$.

Repeating this argument, we get that for every $n \in \mathbb{N}$, the point $\mathrm{diag}(\boldsymbol{\sigma}) = R(-n)\mathrm{diag}(\boldsymbol{\tau})$ satisfies $\mathrm{r}(\boldsymbol{\sigma}, t_0) \cap \mathcal{I} = \emptyset$.

Let $U = \{R(-n)\mathrm{diag}(\boldsymbol{\tau}) \ : \ n \in \mathbb{N}\}$. Then diagonals of U are dense in $\mathbb{T}_\omega$, since the group of multiplicative relations defined by the $\{e^{-\mathrm{i}\omega_1}, \dots, e^{-\mathrm{i}\omega_k}\}$ is the same as the one defined by $\{e^{\mathrm{i}\omega_1}, \dots, e^{\mathrm{i}\omega_k}\}$. Set $U' = \{\boldsymbol{\sigma} \in \mathbb{T}_\omega \ : \ \mathrm{r}(\boldsymbol{\sigma}, t_0) \cap \mathcal{I} = \emptyset\}$ which is $\mathfrak{R}$-definable, and further, we have $U \subseteq U' \subseteq \mathbb{T}_\omega$. Moreover, $\overline{U} = \mathbb{T}_\omega$, so $\overline{U'} = \mathbb{T}_\omega$.

We now prove that, in fact, $U' = \mathbb{T}_\omega$. Assuming (again by way of contradiction) that there exists $\boldsymbol{\sigma} \in \mathbb{T}_\omega \setminus U'$, then by the definition of U' we have $\mathrm{r}(\boldsymbol{\sigma}, t_0) \cap \mathcal{I} \neq \emptyset$. It follows that for every $n \in \mathbb{N}$, the point $\mathrm{diag}(\boldsymbol{\sigma}') = R(n)\mathrm{diag}(\boldsymbol{\sigma})$ also satisfies $\mathrm{r}(\boldsymbol{\sigma}', t_0) \cap \mathcal{I} \neq \emptyset$. Define $V = \{R(n)q \ : \ n \in \mathbb{N}\}$, then the diagonals of V are dense in $\mathbb{T}_\omega$. Further the set $V' = \{\boldsymbol{\sigma}' \in \mathbb{T}_\omega \ : \ \mathrm{r}(\boldsymbol{\sigma}', t_0) \cap \mathcal{I} \neq \emptyset\}$ satisfies $V \subseteq V' \subseteq \mathbb{T}_\omega$ and $\overline{V'} = \mathbb{T}_\omega$. Now the sets U' and V' are both definable in $\mathfrak{R}$, and the topological closure of each of them is $\mathbb{T}_\omega$.

We employ [2, Lemma 10], which states that if $X, Y \subseteq \mathbb{T}_\omega$ are $\mathfrak{R}$-definable sets such that $\overline{X} = \overline{Y} = \mathbb{T}_\omega$, then $X \cap Y \neq \emptyset$.

It follows that $V' \cap U' \neq \emptyset$, which is clearly a contradiction. Therefore, there is no $\boldsymbol{\sigma} \in \mathbb{T}_\omega \setminus U'$; that is, $U' = \mathbb{T}_\omega$.

From this, however, it follows that $\mathcal{C}_{t_0} \cap \mathcal{I} = \emptyset$, which is again a contradiction, since $\mathcal{C}_{t_0} \cap \mathcal{O} \neq \emptyset$ and $\mathcal{O} \subseteq \mathcal{I}$, so we are done. □

Proof of Claim B.3. Consider the function $f : \mathbb{T}_\omega \to \mathbb{R}$ defined by $f(\boldsymbol{\tau}) = \inf\{t \in \mathbb{R} \ : \ \mathrm{r}(\boldsymbol{\tau}, t) \subseteq \mathcal{I}\}$. By Claim B.2 this function is well-defined. Since $\mathrm{r}(\boldsymbol{\tau}, t)$ is $\mathfrak{R}$-definable, then so is f. Moreover, its graph $\Gamma(f)$ has finitely many connected components, and the same dimension as $\mathbb{T}_\omega$. Thus, there exists an open set $K \subseteq \mathbb{T}_\omega$ (in the induced topology on $\mathbb{T}_\omega$) such that f is continuous on K. Furthermore, K is homeomorphic to $(0,1)^m$ for some $0 \leq m \leq k$, and thus we can find sets $K'' \subseteq K' \subseteq K$ such that K'' is open, and K' is closed.[2] Since f is continuous on K, it attains a maximum on K'. Consider the set $\{R(n) \cdot K'' \ : \ n \in \mathbb{N}\}$. By the density of the diagonals of $\{R(n) \ : \ n \in \mathbb{N}\}$ in $\mathbb{T}_\omega$, this is an open cover of $\mathbb{T}_\omega$, and hence there is a finite subcover $\{R(n_1)K'', \ldots, R(n_a)K''\}$. Since $K'' \subseteq K'$, it follows that $\{R(n_1)K', \ldots, R(n_a)K'\}$ is a finite closed cover of $\mathbb{T}_\omega$.

We now show that, for all $\boldsymbol{\tau} \in \mathbb{T}_\omega$, we have $f(R(1)\boldsymbol{\tau}) \leq f(\boldsymbol{\tau}) + 1$. Indeed, consider any $\boldsymbol{\tau} \in \mathbb{T}_\omega$ and $t > 0$ such that $\mathrm{r}(\boldsymbol{\tau}, t) \subseteq \mathcal{I}$. Applying e^A, we get $e^A \cdot \mathrm{r}(\boldsymbol{\tau}, t) \subseteq e^A \mathcal{I} \subseteq \mathcal{I}$. Similarly to the proof of Lemma 3.3, we have that $e^A \cdot \mathrm{r}(\boldsymbol{\tau}, t) = \mathrm{r}(R(1)\boldsymbol{\tau}, t+1)$, so we can conclude that $\mathrm{r}(R(1)\boldsymbol{\tau}, t+1) \subseteq \mathcal{I}$. This means that $\mathrm{r}(\boldsymbol{\tau}, t) \subseteq \mathcal{I}$ implies $\mathrm{r}(R(1)\boldsymbol{\tau}, t+1) \subseteq \mathcal{I}$; therefore, $f(R(1)\boldsymbol{\tau}) \leq 1 + f(\boldsymbol{\tau})$.

Now denote $s_0 = \max_{\boldsymbol{\tau} \in K'} f(\boldsymbol{\tau})$. Then for every $1 \leq i \leq m$ we have $\max_{\boldsymbol{\tau} \in R(n_i)K'} f(\boldsymbol{\tau}) \leq n_i + s_0$; so $f(\boldsymbol{\tau})$ is indeed bounded on $\mathbb{T}_\omega$. □

Finally, we conclude from Claim B.3 that there exists $t_0 \geq 0$ such that $\mathcal{C}_{t_0} \subseteq \mathcal{I}$. This completes the proof of Theorem 3.6.

C Proofs of Section 4

▶ **Lemma 4.3.** *$\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}}$ is definable in $\mathfrak{R}_0$, and we can compute a representation of it.*

Proof. The only part that is not immediately semi-algebraic is the $\mathrm{diag}(s^{q_1}, \ldots, s^{q_k})$ factor, as the exponents are not fixed.

Consider the group $L \overset{\mathrm{def}}{=} \{(n_1, \ldots, n_k) \in \mathbb{Z}^k \ : \ \sum_{i=1}^k n_i \rho_i = 0\}$. Similarly to the analysis in Section 3, we can compute a finite basis $\{\mathbf{z}^1, \ldots, \mathbf{z}^m\} \subseteq \mathbb{Z}^k$ for L. Then, we can rewrite $\mathbb{S}$ as $\mathbb{S} = \{(q_1, \ldots, q_k) \ : \ \bigwedge_{j=1}^m q_1 z_1^j + \ldots q_k z_k^j = 0\}$. Next, observe that

$$\{\mathrm{diag}(s^{q_1}, \ldots, s^{q_k}) \ : \ (q_1, \ldots, q_k) \in \mathbb{S}\} = \left\{ \mathrm{diag}(w_1, \ldots, w_k) \ : \ \bigwedge_{j=1}^m w_1^{z_1^j} \cdots w_k^{z_k^j} = 1 \right\}.$$

[2] In case $m = 0$, the proof actually follows immediately from Claim B.2, since $\mathbb{T}_\omega$ is finite.

Indeed, for every $\mathbf{z}^j$ and $(q_1,\ldots,q_k) \in \mathbb{S}$ we have $(s^{q_1})^{z_1^j}\cdots(s^{q_k})^{z_k^j} = s^{q_1 z_1^j+\ldots+q_k z_k^j} = s^0 = 1$, and conversely, if $w_1,\ldots,w_k$ satisfy the condition on the right hand set, then for every $(n_1,\ldots,n_k) \in L$ we have $w_1^{n_1}\cdots w_k^{n_k} = 1$, denote $q_i = \log_s w_i$, then this can be rewritten as $s^{q_1 n_1}\cdots s^{q_k n_k} = 1$, so $n_1 q_1 + \ldots + n_k q_k = 0$, and hence $(q_1,\ldots,q_k) \in \mathbb{S}$.

Furthermore, the requirement $(q_1,\ldots,q_k)$ can be restated in the above formulation as $\ell_i \le \log_s w_i \le u_i$, or equivalently, $s^{\ell_i} \le w_i \le s^{u_i}$ (where $\boldsymbol{\ell} = (\ell_1,\ldots,\ell_k)$ and $\mathbf{u} = (u_1,\ldots,u_k)$).

Thus, define

$$\mathbb{S}^{\text{diag}}(L,U) \overset{\text{def}}{=} \left\{ \text{diag}(w_1,\ldots,w_k) \ :\ \bigwedge_{j=1}^{m} w_1^{z_1^j}\cdots w_k^{z_k^j} = 1 \text{ and for all } i,\ L_i \le w_i \le U_i \right\},$$

then we can rewrite the fat cone as $\mathcal{F}_{s_0,\epsilon,\delta,\boldsymbol{\ell},\boldsymbol{u}}$ as the set

$$\left\{ P\ W\ \text{diag}(\tau)\ Q(r)\ P^{-1}\mathbf{x}_0\ :\ \boldsymbol{\tau} \in \mathbb{T}_\omega,\ s \ge s_0,\ \delta \le r \le s^\epsilon,\ W \in \mathbb{S}^{\text{diag}}(s^{\boldsymbol{\ell}}, s^{\mathbf{u}}) \right\}$$

which is clearly semi-algebraic, and is equivalent by the above. ◻

▶ **Lemma C.1.** *For every $\epsilon > 0$, there exists s_0 such that for every $s_1 \ge s_0$, $t \ge 0$ and $\delta, \boldsymbol{\ell}, \mathbf{u}$ we have that $e^{At}\mathcal{F}_{s_1,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}} \subseteq \mathcal{F}_{s_1,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}}$*

Proof. Consider a vector

$$\mathbf{v} \overset{\text{def}}{=} P\ \text{diag}(s^{q_1},\ldots s^{q_k})\ \text{diag}(\boldsymbol{\tau})\ Q(r)\ P^{-1}\mathbf{x}_0 \in \mathcal{F}_{s_1,\epsilon,\delta,\boldsymbol{\ell},\mathbf{u}},$$

where s_1 will be determined later, and let $t \ge 0$. Set $t = \log x$ and recall that

$$e^{At} = e^{A\log x} = P\ \text{diag}(x^{\rho_1},\ldots,x^{\rho_k})\ \text{diag}(e^{\mathrm{i}\omega_1 \log x},\ldots,e^{\mathrm{i}\omega_k \log x})\ Q(\log x)\ P^{-1},$$

whence

$$\begin{aligned} e^{At}v &= e^{A\log x}\mathbf{v} \\ &= P\ \text{diag}(x^{\rho_1}s^{q_1},\ldots,x^{\rho_k}s^{q_k})\text{diag}(e^{\mathrm{i}\omega_1\log x}\tau_1,\ldots,e^{\mathrm{i}\omega_k\log x}\tau_k)\ Q(\log x)\ Q(r)\ P^{-1}\mathbf{x}_0. \end{aligned}$$

We will now show that $e^{At}\mathbf{v} \in \mathcal{F}_{s_1,\epsilon,\delta,\boldsymbol{\ell},\boldsymbol{u}}$, by drawing some condition on s_1. First, we claim that $(e^{\mathrm{i}\omega_1\log x}\tau_1,\ldots,e^{\mathrm{i}\omega_k\log x}\tau_k) \in \mathbb{T}_\omega$. Indeed, for all j we have $|e^{\mathrm{i}\omega_j\log x}\tau_j| = 1$, and for all $\mathbf{z}$ such that $z_1\omega_1 + \ldots + z_k\omega_k = 0$, we have

$$(e^{\mathrm{i}\omega_1\log x}\tau_1)^{z_1}\cdots(e^{\mathrm{i}\omega_k\log x}\tau_k)^{z_k} = e^{\mathrm{i}\log x(z_1\omega_1+\ldots+z_k\omega_k)}\cdot\tau_1^{z_1}\cdots\tau_k^{z_k} = 1$$

since $\boldsymbol{\tau} \in \mathbb{T}_\omega$.

Next, it is also not hard to prove that $(x^{\rho_1}s^{q_1},\ldots,x^{\rho_k}s^{q_k})$ can be written as

$$((xs)^{p_1},\ldots,(xs)^{p_k})$$

for $(p_1,\ldots,p_k) \in \text{Box}(\boldsymbol{\ell},\boldsymbol{u})$. Indeed, take $p_i = \frac{\rho_i\log x + q_i\log s}{\log x+\log s}$, then for all i, $(xs)^{p_i} = \exp((\log x + \log s)p_i) = \exp(\rho_i\log x + q_i\log s) = x^{\rho_i}s^{q_i}$.

It remains to show that $Q(\log x)\cdot Q(r)$ can be written as $Q(y)$ for $\delta \le y \le (xs)^\epsilon$. Recall that $Q(\log x)\cdot Q(r) = Q(\log x + r)$, and that $\delta \le r \le s^\epsilon$ and $x \ge 1$. It immediately follows that $\delta < \log x + r$.

Now, observe that $\log x + r \le \log x + s^\epsilon$. We prove that if s_1 is large enough, then $\log x + s^\epsilon \le (xs)^\epsilon$. Let $x_0 \ge 1$ be such that for every $y \ge x_0$ we have $y^\epsilon \ge \max\{\log y, 2\}$. Clearly such x_0 exists. We now split the proof into two cases.

- If $x > x_0$, take s_1 to be large enough such that $s^\epsilon \geq 2$ for every $s \geq s_1$. Then by the condition on x_0 we have that

  $$\log x + s^\epsilon \leq x^\epsilon + s^\epsilon \leq (xs)^\epsilon$$

  where the last inequality follows since both summands are at least 2 (indeed, if $A, B \geq 2$ and w.l.o.g. $A \leq B$, then $A + B \leq 2B \leq AB$).
- If $x \leq x_0$, recall that $x \geq 1$, and thus $\log x \leq x - 1$. So it suffices to find s_1 such that for all $s \geq s_1$ we have $x - 1 + s^\epsilon \leq x^\epsilon s^\epsilon$. The latter is equivalent to $x - 1 \leq (x^\epsilon - 1)s^\epsilon$. Now, if $x = 1$, the inequality holds for any s, and we are done. Otherwise, let $x > 1$, then observe that the function $\frac{x-1}{x^\epsilon - 1}$ is increasing, and $\lim_{x\to 1^+} \frac{x-1}{x^\epsilon-1} = \frac{1}{\epsilon}$ (e.g., by L'Hôpital's rule). In particular, the function $\frac{x-1}{x^\epsilon-1}$ is bounded from above on the interval $(0, x_0]$. Set s_1 be large enough such that for every $s \geq s_1$ and for every $x \in (0, x_0]$ we have $\frac{x-1}{x^\epsilon-1} \leq s^\epsilon$, and we are done.

By taking the maximal s_1 from the conditions above, we conclude the lemma. □

D Proofs of Section 5

▶ **Lemma 5.3.** *For every $\mu > 1$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ the set*

$$\mathcal{I}_{n,\mu} \cup \{(y, t) \ : \ t > t_0\}$$

is an invariant containing the whole orbit, i.e. $\{(e^{\rho t}, t) \ : \ t \geq 0\}$.

To prove this lemma, we gather some properties of the under and over approximations. We recall their definitions here.

$$P_n(t) \stackrel{\text{def}}{=} \sum_{k=0}^{n} \frac{(\rho t)^k}{k!},$$

$$Q_{n,\mu}(t) \stackrel{\text{def}}{=} P_n(\mu t).$$

▶ **Proposition D.1.** *The under-approximations have the following properties:*

- ***Property 1:*** *for all $n \in \mathbb{N}$ and $0 \leq t \leq t_0$, we have $P_n(t) \leq e^{\rho t}$,*
- ***Property 2:*** *for all $n \in \mathbb{N}$ and $0 < t_1 \leq t \leq t_0$, we have ${P_n}'(t) \leq (P_n(t_1)e^{\rho(t-t_1)})'$,*
- ***Property 3:*** $\max_{0\leq t\leq t_0} \|P_n(t) - e^{\rho t}\| \to 0$ *as $n \to \infty$.*

Proof. Property 3 is satisfied by Taylor's theorem. Property 1 holds since $\rho > 0$ by our assumption, in which case every Taylor polynomial of $e^{\rho t}$ is an under-approximation.

We turn to establish Property 2, which is equivalent to $P'_n(t) \leq \rho P_n(t_1)e^{\rho(t-t1)}$. Note that it clearly holds for $n = 0$. Observe that $P'_n(t) = \rho P_{n-1}(t)$, thus we want to prove that $\rho P'_n(t) \leq \rho P_n(t_1)e^{\rho(t-t_1)}$. Since $\rho > 0$, we can cancel it from the inequality. Now consider the function $g_n(t) = P_n(t_1)e^{\rho(t-t_1)} - P_{n-1}(t)$, we prove that $g_n(t) \geq 0$ for all $t_1 \leq t \leq t_0$. First, we have that $g_n(t_1) = P_n(t_1) - P_{n-1}(t_1) = \frac{(\rho t_1)^n}{n!} \geq 0$. We now prove that $g'_n(t) \geq 0$ for $t_1 \leq t \leq t_0$. We have

$$g'_n(t) = \rho P_n(t_1)e^{\rho(t-t_1)} - P'_{n-1}(t) = \rho P_n(t_1)e^{\rho(t-t_1)} - \rho P_{n-2}(t) = \rho(P_n(t_1)e^{\rho(t-t_1)} - P_{n-2}(t))$$

Thus, $g'_n(t) \geq 0$ if and only if $P_n(t_1)e^{\rho(t-t_1)} - P_{n-2}(t) \geq 0$. Repeating this argument for $n - 1$ times, we end up with the condition $P_n(t_1)e^{\rho(t-t_1)} - P_0(t) \geq 0$, which is equivalent to $P_n(t_1)e^{\rho(t-t_1)} \geq 1$, and it holds since $P_n(t_1) \geq 1$ and $e^{\rho(t-t_1)} \geq 1$. □

Intuitively, Property 1 in Proposition D.1 ensures that the curve of $P_n(t)$ always is below that of $e^{\rho t}$, Property 3 says that the under-approximation can get arbitrarily close to the exponential function, and Property 2 is a condition on the derivative of $P_n(t)$ which ensures that the resulting set is invariant. Formally, we have the following:

▶ **Lemma D.2.** *For every $n \in \mathbb{N}$, the set*

$$\mathcal{L}_n \stackrel{\text{def}}{=} \left\{(y,t) : y \geq P_n(t), 0 \leq t \leq t_0\right\} \cup \left\{(y,t) : t > t_0\right\}$$

is a semi-algebraic invariant that contains the orbit from time 0.

Proof. Clearly the set $\mathcal{L}_n$ is semi-algebraic (recall that $t_0 \in \mathbb{Q}$). It thus remains to prove that for every $(y_1,t_1) \in \mathcal{L}_n$ and for every $\delta > 0$ it holds that $(e^{\rho\delta}y_1, t_1+\delta) \in \mathcal{L}_n$. Denote $t = t_1 + \delta$. If $t > t_0$, then the claim is trivial. Thus, assume $t_1 \leq t \leq t_0$, and we need to prove that $P_n^\rho(t) \leq e^{\rho(t-t_1)}y_1$. Since $(y_1,t_1) \in \mathcal{L}_n$, then $y_1 \geq P_n^\rho(t_1)$, and thus for $t = t_1$ the claim holds, and Property 2 in Proposition D.1 ensures that the inequality is maintained for all $t_1 \leq t \leq t_0$ (by taking derivative of both sides of the inequality). □

Proposition D.1 and Lemma D.2 provide us with an under-approximating invariant. We now turn our attention to the over-approximations.

▶ **Proposition D.3.** *The over-approximations have the following properties:*

- ***Property 1:*** *for every $\mu > 1$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ and $0 \leq t \leq t_0$, we have $Q_{n,\mu}(t) \geq e^{\rho t}$,*
- ***Property 2:*** *for every $\mu > 1$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ and $0 \leq t_1 \leq t \leq t_0$, we have ${Q_{n,\mu}}'(t) \geq (Q_{n,\mu}(t_1)e^{\rho(t-t_1)})'$,*
- ***Property 3:*** *for every $\epsilon > 0$ there exist $\mu > 1$ and $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $\max_{0\leq t\leq t_0}\|Q_{n,\mu}(t) - e^{\rho t}\| < \epsilon$.*

Proof. Property 3 clearly holds by Taylor's theorem and since $Q_{n,\mu} \to P_n$ uniformly as $\mu \to 1^+$. For Property 1, fix $\mu > 1$, and observe that $Q_{n,\mu}(t) \to e^{\mu\rho t}$ uniformly in $[0,t_0]$ as $n \to \infty$, and since $\mu > 1$, we have that $e^{\mu\rho t} \geq e^{\rho t}$.

We turn to establish Property 2. Plugging the definition of $Q_{n,\mu}$ and expanding the derivatives, rewrite the property as $\rho\mu P_{n-1}(\mu t) \geq \rho P_n(\mu t_1)e^{\rho(t-t_1)}$. Cancel ρ, and recall from Proposition D.1 that $P_n(t) \leq e^{\rho t}$, and thus $P_n(\mu t_1) \leq e^{\rho\mu t_1}$, so

$$P_n(\mu t_1)e^{\rho(t-t_1)} \leq e^{\rho\mu t_1}e^{\rho(t-t_1)} = e^{\rho((\mu-1)t_1+t)} \leq e^{\rho\mu t}$$

where the last inequality follows since $t_1 \leq t$.

Next, from Taylor's theorem, for every $\epsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that $P_{n-1}(\mu t) \geq e^{\mu\rho t} - \epsilon$ for all $t \in [0,t_0]$. Fix $0 < \epsilon < \frac{\mu-1}{\mu}$, and let n_0 be the corresponding threshold. By the above, it now suffices to prove that $\mu(e^{\rho\mu t} - \epsilon) \geq e^{\rho\mu t}$, which holds by our choice of ϵ for every $n \geq n_0$. □

We can now use Proposition D.3 to establish the following Lemma, whose proof follows, *mutatis mutandis*, the proof of Lemma D.2.

▶ **Lemma D.4.** *For every $\mu > 1$ there exists $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$, the set*

$$\mathcal{U}_n = \left\{(y,t) : y \leq Q_{n\mu}(t), 0 \leq t \leq t_0\right\} \cup \left\{(y,t) : t > t_0\right\}$$

is a semi-algebraic invariant that contains the orbit from time 0.

Combining Lemmas D.2 and D.4 and the properties in Propositions D.1 and D.3, we regain Lemma 5.3.

▶ **Lemma 5.4.** *For every $\tilde{Y}$ semi-algebraic, there exists another semi-algebraic set Y and $\mathbf{x}_0$ with rational entries such that the following two statements are equivalent:*

- *$\langle J, \tilde{\mathbf{x}}_0\rangle$ has a semi-algebraic invariant disjoint from $\tilde{Y}$, containing the whole orbit,*
- *$\langle PJP^{-1}, \mathbf{x}_0\rangle$ has a semi-algebraic invariant disjoint from Y, containing the whole orbit.*

Proof. Define $g : \mathbb{C}^d \to \mathbb{C}^d$ to be the injective linear map:

$$\mathbf{v} \mapsto P(\mathbf{v}P^{-1})^T,$$

and let

$$Y \overset{\text{def}}{=} g(\tilde{Y}) \qquad\qquad \mathbf{x}_0 \overset{\text{def}}{=} g(\tilde{\mathbf{x}}_0)^T.$$

Both Y and $\mathbf{x}_0$ can be seen to be subsets of $\mathbb{R}^d$ as follows. Without loss of generality, we can assume that $\pi_j(\tilde{Y}) = 0$ for all $n+2 < j \leq d$, that is the projection to the last $d-n-2$ entries is zero, since $\tilde{\mathbf{x}}_0$ ignores these entries. The first $n+2$ columns of P^{-1} are real numbers since they are eigenvectors that span the eigenspace corresponding to the real eigenvalues $\rho_1, \ldots, \rho_n, 0$. The same is true for the first $n+2$ rows of P. It follows now from the definitions that $Y, \mathbf{x}_0 \subset \mathbb{R}^d$. The set Y is semi-algebraic because semi-algebraic sets are closed under linear maps.

For the direct implication assume that $\tilde{\mathcal{I}}$ is an invariant of $\langle J, \tilde{\mathbf{x}}_0\rangle$ with the properties in the statement. Let $\mathcal{I} = g(\tilde{\mathcal{I}})$. We prove that $\mathcal{I}$ is an invariant for $\langle PJP^{-1}, \mathbf{x}_0\rangle$. Any point in $\mathcal{I}$ can be written as

$$P(\mathbf{x}P^{-1})^T, \text{ where } \mathbf{x} \in \tilde{\mathcal{I}},$$

hence, since $\tilde{\mathcal{I}}$ is invariant for all $\delta \geq 0$ we have:

$$Pe^{J\delta}P^{-1} \cdot P(\mathbf{x}P^{-1})^T = P(e^{J\delta}\mathbf{x}P^{-1})^T \in \mathcal{I}.$$

Moreover, by definition $\mathbf{x}_0 \in \mathcal{I}$ since $\tilde{\mathbf{x}}_0 \in \tilde{\mathcal{I}}$, so $\mathcal{I}$ contains the whole orbit. The set $\mathcal{I}$ can be further shown to be disjoint from Y, because the map g is injective. The inverse implication follows along the same lines.

This does not prove the lemma because $\mathbf{x}_0$ might have irrational entries. We can amend this by translating the whole system by some vector $\mathbf{v}$ such that $\mathbf{x}_0 + \mathbf{v} \in \mathbb{Q}^d$, which is feasible because the sets $Y + \mathbf{v}$, and $\mathcal{I} + \mathbf{v}$ are semi-algebraic. □