Verification of Linear Dynamical Systems via O-Minimality of the Real Numbers

Toghrul Karimov
Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany

Abstract

A discrete-time linear dynamical system (LDS) is given by an update matrix $M \in \mathbb{R}^{d\times d}$, and has the trajectories $\langle s, Ms, M^2s, \ldots\rangle$ for $s \in \mathbb{R}^d$. Reachability-type decision problems of linear dynamical systems, most notably the Skolem Problem, lie at the forefront of decidability: typically, sound and complete algorithms are known only in low dimensions, and these rely on sophisticated tools from number theory and Diophantine approximation. Recently, however, o-minimality has emerged as a counterpoint to these number-theoretic tools that allows us to decide certain modifications of the classical problems of LDS without any dimension restrictions. In this paper, we first introduce the Decomposition Method, a framework that captures all applications of o-minimality to decision problems of LDS that are currently known to us. We then use the Decomposition Method to show decidability of the Robust Safety Problem (restricted to bounded initial sets) in arbitrary dimension: given a matrix M, a bounded semialgebraic set S of initial points, and a semialgebraic set T of unsafe points, it is decidable whether there exists $\varepsilon > 0$ such that all orbits that begin in the ε-ball around S avoid T.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Linear dynamical systems, formal verification, o-minimality, reachability problems

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

1 Introduction

Linear dynamical systems (LDS) are mathematical models widely used in engineering and sciences to describe systems that evolve over time. A *discrete-time* LDS is given by an update matrix M. The *orbit* of a point s under M is the infinite sequence of vectors $(M^n s)_{n\in\mathbb{N}}$. In formal verification, the most prominent decision problem of linear dynamical systems is the (point-to-set) Reachability Problem: given $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, and a *semialgebraic* target set T, decide whether there exists $n \in \mathbb{N}$ such that $M^n s \in T$. In terms of program verification, this is equivalent to the *Termination Problem* for linear loops: given a program fragment of the form

initialise $x = (x_1, \ldots, x_d)$
while $\neg \mathrm{P}(x)$ **do** $x = M \cdot x$

where M is a linear update and P is a Boolean combination of polynomial inequalities, decide whether the loop terminates. The restriction of the Termination Problem to P defined by a single linear equality (i.e., the Reachability Problem where T is restricted to hyperplanes) is Turing-equivalent to the famously open *Skolem Problem* of linear recurrence sequences (LRS): given an LRS $(u_n)_{n\in\mathbb{N}}$ defined by a recurrence relation

$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n$$

as well as the initial values $u_0, \ldots, u_{d-1}$, decide whether there exists n such that $u_n = 0$. The Skolem Problem is known to be decidable[1] only for LRS with $d \leq 4$ [17]. Consequently, the Termination Problem for linear loops with a linear guard is currently open for 5 or more program variables. Similarly to the above, the Termination Problem with P defined by a single linear inequality (i.e., the Reachability Problem with halfspace targets) is Turing-equivalent to the *Positivity Problem*: given an LRS $(u_n)_{n\in\mathbb{N}}$, decide whether $u_n \geq 0$. The Positivity Problem subsumes the Skolem Problem and is decidable for LRS with $d \leq 5$, but is also known to be hard with respect to certain long-standing open problems in Diophantine approximation [19]: a resolution (in either direction) of the decidability of the Positivity Problem would entail major breakthroughs regarding approximabiliity of *Lagrange constants* for a large class of transcendental numbers, which are currently believed to be out of reach.

Decidability of the Reachability Problem, which is formidably difficult in full generality, has also been studied under various geometric restrictions on T. The state of the art in this direction is that the Reachability Problem is decidable in arbitrary dimension for T restricted to the class of *tame* targets [12], i.e. for T that can be constructed through the usual set operations from semialgebraic sets that either (i) have dimension one (i.e. are "string-like"), or (ii) are contained in a three-dimensional subspace of $\mathbb{R}^d$. In particular, the Reachability Problem is decidable for arbitrary T in dimension $d \leq 3$. These decidability results rely on Baker's theorem [24] as well its p-adic analogue [25], and are tight in the sense that allowing T to be two-dimensional or contained in a four-dimensional subspace yields a decision problem that is Diophantine-hard similarly to the Positivity Problem [11, Chap. 8].

As discussed above, the Reachability Problem is intimately related to number theory, and, mathematically speaking, becomes harder and harder as we increase the dimension d. Recently, however, a string of results have emerged that show decidability of various reachability-type problems of LDS in arbitrary dimension. First, Akshay et al. [2] showed that the robust variants of the Skolem Problem as well as the Positivity Problem are decidable: given a matrix M, an initial point s, and a hyperplane or a halfspace T, we can decide whether there exists $\varepsilon > 0$ such that for all s' in the ε-ball around s, the orbit $(M^n s')_{n\in\mathbb{N}}$ avoids T. The proof is based on classical analyses of LRS. A second interesting result was given by Kelmendi in [13], who showed that given M, an initial point s, and a semialgebraic target T, the *frequency* of visits

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{1}(M^k s \in T)$$

exists and can be effectively compared against 0. The proof is variation on the fundamental result [20] that *ultimate positivity* is decidable for *simple* (also known as *diagonalisable*) linear recurrence sequences. Finally [9], showed that the Pseudo-Orbit Reachability Problem is decidable for diagonalisable M and a single starting point s: given such M, s and a semialgebraic target T, we can decide whether for every $\varepsilon > 0$ there exists $(x_n)_{n\in\mathbb{N}}$ such that (i) $x_0 = s$, (ii) $\|x_{n+1} - Mx_n\| < \varepsilon$ for all n, and (iii) $x_n \in T$ for some T. Such $(x_n)_{n\in\mathbb{N}}$ is called an *ε-pseudo-orbit* of s under M. The proof of decidability uses geometry of pseudo-orbits of diagonalisable M and the classical tools of linear dynamical systems in combination with *o-minimality*. Briefly, o-minimality of real numbers equipped with arithmetic and exponentiation tell us that every subset of $\mathbb{R}^d$ definable using first-order logic and the aforementioned operations has finitely many connected components. We will use

[1] Decidability for $d \leq 4$ applies to LRS over real algebraic numbers. For LRS over algebraic numbers, decidability is known for $d \leq 3$.

o-minimality to show that any sequence of subsets of $\mathbb{R}^d$ that can be defined using arithmetic and exponentiation must converge to a *limit shape* in a strong sense (Section 3.3). Although a concept originating in model theory, a branch of mathematical logic, o-minimality has recently had spectacular applications to Diophantine geometry, including counting rational points in algebraic varieties as well as the proofs of Mordell-Lang and André-Oort conjectures [21].

The thesis of this paper is that every single variant of the Reachability Problem that is decidable in an arbitrary dimension d can be explained using o-minimality (Section 5). Specifically, we introduce the Decomposition Method, a framework in which all decidability results mentioned above (and more) can be proven. As an application of the Decomposition Method, we study the Robust Safety Problem, which is motivated by situations in which a system must remain in a safe set forever, even when an adversarial perturbation is applied to the initial state. For effectiveness reasons, we work with real algebraic numbers[2], denoted by $\mathbb{R} \cap \overline{\mathbb{Q}}$, which subsume rationals and can be effectively represented and manipulated in computer memory. For $s \in \mathbb{R}^d$ and $\varepsilon > 0$, denote by $B(s, \varepsilon)$ the open ε-ball around s. Further write $B(S, \varepsilon)$ for $\bigcup_{s \in S} B(s, \varepsilon)$. The Robust Safety Problem is to decide, given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$, a semialgebraic set S of initial points, and a semialgebraic set T of unsafe points, whether the sequence $(M^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ *avoids* T: that is, whether $M^n \cdot B(s, \varepsilon)$ does not intersect T for all $s \in S$ and $n \in \mathbb{N}$. Our main result is the following, which, for bounded S, (i) characterises the largest $\varepsilon > 0$ such that $(M^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ avoids T, and (ii) shows decidability of the Robust Safety Problem.

▶ **Theorem 1.** *Let $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$, $S \subseteq \mathbb{R}$ be non-empty, semialgebraic and bounded, and $T \subseteq \mathbb{R}^d$ be semialgebraic. Further let*

$$\mu_1 = \sup\{\varepsilon \geq 0 \colon M^n \cdot B(S, \varepsilon) \text{ does not intersect } T \text{ for all } n\},$$
$$\mu_2 = \sup\{\varepsilon \geq 0 \colon M^n \cdot B(S, \varepsilon) \text{ does not intersect } T \text{ for all sufficiently large } n\}.$$

Then $\mu_1 \in \mathbb{R} \cap \overline{\mathbb{Q}}$, $\mu_2 \in (\mathbb{R} \cap \overline{\mathbb{Q}}) \cup \{\infty\}$ and is effectively computable, μ_1 can be approximated (both from above and below) to arbitrary precision, and it is decidable whether $\mu_1 = 0$. Moreover, for every $\varepsilon \in (0, \mu_2) \cap \overline{\mathbb{Q}}$ we can effectively compute N such that $(M^n \cdot B(S, \varepsilon))_{n \geq N}$ avoids T.

Intuitively, μ_1 is the best possible margin of safety. From Theorem 1 it follows that the Robust Safety Problem is decidable: we simply check whether $\mu_1 = 0$. For positive instances, i.e. when $\mu_1 > 0$, we can compute $\varepsilon \geq 0$ that is arbitrarily close to the best possible safety margin by approximating μ_1 from below. Finally, for every positive $\varepsilon \neq \mu_2$ we can decide whether $(M^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ avoids T: for $\varepsilon > \mu_2$, the answer is immediately negative. For $\varepsilon \in (0, \mu_2)$, we can compute N and then check whether $M^n \cdot B(S, \varepsilon)$ intersects T for some $n < N$. For $\varepsilon = \mu_2$, however, we do not know how to decide whether $(M^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ avoids T: in this case we have to contend with the hard Diophantine approximation problems that also arise in the classical Reachability Problem.

Related work

At the time of writing, to the best of our knowledge, there are only two published works that apply o-minimality to verification of (discrete-time) linear dynamical systems: [3] studies o-minimal and semialgebraic *invariants* of LDS (see Section 5), and [9] studies the

[2] If we move from the reals to the complex numbers, i.e. consider the Robust Safety Problem in $\overline{\mathbb{Q}}^d$, all of our results still apply. In this setting semialgebraic sets are defined by identifying $\mathbb{C}^d$ with $\mathbb{R}^{2d}$.

Pseudo-Orbit Reachability Problem for LDS. In the unpublished extension [8] of [9], it is described how the decidability of the Pseudo-Orbit Reachability Problem can be adapted to study the Robust Safety Problem for singleton S. The latter problem, however, is much simpler, and can be solved more generally and directly using the Decomposition Method.

Theorem 1 is a generalisation of the aforementioned results of Akshay et al. [2] to bounded S and semialgebraic T. A similar result is [7], which shows the Pseudo-Orbit Reachability Problem is decidable for hyperplane/halfspace targets, without any restrictions on M. Both of these heavily rely on the fact that T is defined by a single linear (in)equality, and their approach does not generalise to targets defined by non-linear or multiple inequalities.

Some other connections between o-minimality and dynamical (or, more generally, cyber-physical) systems have already been established. In [14], Lafferriere et al. show that *o-minimal hybrid systems* always admit a finite bisimulation; these do not include linear dynamical systems. In [18], Miller studies expansions of the field of real numbers with trajectories of LDS from the perspective of definability and o-minimality.

2 Preliminaries

2.1 Notation and conventions

We denote by $\boldsymbol{i}$ the imaginary number and by $\mathbb{T}$ the unit circle in $\mathbb{C}$. We write $\mathbf{0}$ for a vector of all zeros as well as a zero matrix. In both cases, the dimensions will be clear from the context. For $x \in \mathbb{R}^d$ and $\varepsilon > 0$, we define $B(x, \varepsilon) = \{y \in \mathbb{R}^d \colon \|x - y\| < \varepsilon\}$ where $\|\cdot\|$ is the ℓ_2-norm. We work exclusively with open ℓ_2-balls. We abbreviate $B(\mathbf{0}, \varepsilon)$ to $B(\varepsilon)$. For $x \in \mathbb{R}^d$ and $Y \subseteq \mathbb{R}^d$, we define $d(x, Y) = \inf\{\|y - x\| \colon y \in Y\} \in \mathbb{R} \cup \{\infty\}$. For a set Y and $\varepsilon > 0$, we let $B(Y, \varepsilon) = \{x \colon d(x, Y) < \varepsilon\}$.

For sets of vectors X, Y, we write $X + Y$ for $\{x + y \colon x \in X, y \in Y\}$. For a matrix M and a set X of vectors, we write $M \cdot X$ to mean $\{Mx \colon x \in X\}$. Finally, for a set $\mathcal{M}$ of matrices and a set X of vectors we define $\mathcal{M} \cdot X = \{Mx \colon M \in \mathcal{M}, x \in X\}$. For a (not necessarily invertible) matrix $C \in \mathbb{R}^{d \times d}$ and $X \subseteq \mathbb{R}^d$, we define $C^{-1} \cdot X$ to be $\{y \in \mathbb{R}^d \colon Cy \in X\}$. We write C^{-n} for $(C^n)^{-1}$.

We denote by $\mathrm{Cl}(X)$ the closure of X in a topological space that will be either explicit or clear from the context. We will only be working with Euclidean topology and induced subset topologies. When we say that an object X is effectively computable, we mean that a representation of X in a scheme that will be clear from the context is effectively computable.

2.2 Linear algebra

For a matrix $A \in \mathbb{R}^{d \times d}$, $\|A\| = \max_{x \neq \mathbf{0}} \|Ax\|/\|x\|$. The matrix norm is sub-multiplicative: for all A, B of matching dimensions, $\|AB\| \leq \|A\| \cdot \|B\|$.

Let $X_i \in \mathbb{R}^{d_i \times d_i}$ for $1 \leq i \leq k$. We write $\mathrm{diag}(X_1, \ldots, X_k)$ for the block-diagonal matrix in $\mathbb{R}^{d \times d}$, where $d = d_1 + \cdots + d_k$, constructed from $X_1, \ldots, X_k$ respecting the order. For $a, b \in \mathbb{R}$, let $\Lambda(a, b) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, and for $\theta \in \mathbb{R}$, let $R(\theta) = \Lambda(\sin(\theta), \cos(\theta))$. A *real Jordan block* is a matrix

$$J = \begin{bmatrix} \Lambda & I & & \\ & \Lambda & \ddots & \\ & & \ddots & I \\ & & & \Lambda \end{bmatrix} \in \mathbb{R}^{d \times d} \tag{1}$$

where I is an identity matrix, and either (i) $\Lambda, I \in \mathbb{R}^{1\times 1}$, or (ii) $\Lambda = \rho R(\theta)$ with $I \in \mathbb{R}^{2\times 2}$, $\rho \in \mathbb{R}_{>0}$, and $\theta \in \mathbb{R}$. A matrix J is in *real Jordan form* if $J = \operatorname{diag}(J_1, \dots, J_l)$ where each J_i is a real Jordan block. Given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, we can compute $P, J \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ such that J is in real Jordan form and $M = P^{-1}JP$ [6].

2.3 Logical theories

A *structure* $\mathbb{M}$ consists of a universe U, constants $c_1, \dots, c_k \in U$, predicates $P_1, \dots, P_l$ where each $P_i \subseteq U^{\mu(i)}$ for some $\mu(i) \geq 1$, and functions $f_1, \dots, f_m$ where each f_i has the type $f_i \colon U^{\delta(i)} \to U$ for some $\delta(i) \geq 1$. By the *language* of the structure $\mathbb{M}$, written $\mathcal{L}_{\mathbb{M}}$, we mean the set of all well-formed first-order formulas constructed from symbols denoting the constants $c_1, \dots, c_k$, predicates $P_1, \dots, P_l$, functions $f_1, \dots, f_m$, as well as the equality symbol $=$, the quantifier symbols $\forall, \exists$ and the connectives $\wedge, \vee, \neg$. A *theory* is simply a set of sentences, i.e. formulas without free variables. The theory of the structure $\mathbb{M}$, written $\operatorname{Th}(\mathbb{M})$, is the set of all sentences in the language of $\mathbb{M}$ that are true in $\mathbb{M}$. A theory $\mathcal{T}$

- is *decidable* if there exists an algorithm that takes a sentence φ and decides whether $\varphi \in \mathcal{T}$, and
- admits *quantifier elimination* if for every formula φ with free variables $x_1, \dots, x_n$, there exists a quantifier-free formula ψ with the same free variables such that the formula

  $$\forall x_1, \dots, x_n \colon (\varphi(x_1, \dots, x_n) \Leftrightarrow \psi(x_1, \dots, x_n))$$

  belongs to $\mathcal{T}$.

We will be working with the following structures and their theories.

- Let $\mathbb{R}_0 = \langle \mathbb{R}; 0, 1, <, +, \cdot \rangle$, which is the ordered ring of real numbers. We will denote the language of this structure by $\mathcal{L}_{or}$, called the *language of ordered rings*. Observe that using the constants $0, 1$ and the addition, we can obtain any constant $c \in \mathbb{N}$. Hence every atomic formula in $\mathcal{L}_{or}$ with k free variables is equivalent to $p(x_1, \dots, x_k) \sim 0$, where p is a polynomial with integer coefficients and $\sim$ is either $>$ or the equality. By the Tarski-Seidenberg theorem, $\operatorname{Th}(\mathbb{R}_0)$ admits quantifier elimination and is decidable [4].
- Let $\mathbb{R}_{\exp} = \langle \mathbb{R}; 0, 1, <, +, \cdot, \exp \rangle$, the real numbers augmented with $x \mapsto e^x$. The theory of this structure is *model-complete*, meaning that quantifiers in any formula can be eliminated down to a single block of existential quantifiers, and decidable assuming Schanuel's conjecture [22, 15].

We say that a structure $\mathbb{S}$ *expands* $\mathbb{M}$ if $\mathbb{S}$ and $\mathbb{M}$ have the same universe and every constant, function, and relation of $\mathbb{M}$ is also present in $\mathbb{S}$. We will only need structures expanding $\mathbb{R}_0$. A set $X \subseteq U^d$ is *definable* in a structure $\mathbb{M}$ if there exist $k \geq 0$, a formula φ in the language of $\mathbb{M}$ with $d + k$ free variables, and $a_1, \dots, a_k \in U$ such that for all $x_1, \dots, x_d \in U$, $\varphi(x_1, \dots, x_d, a_1, \dots, a_k)$ holds in $\mathbb{M}$ if and only if $(x_1, \dots, x_d) \in X$. We say that X is *definable in* $\mathbb{M}$ *without parameters* if we can take $k = 0$ above. Similarly, a function is definable (without parameters) in $\mathbb{M}$ if its graph is definable (without parameters) in $\mathbb{M}$.

A structure $\mathbb{M}$ expanding $\mathbb{R}_0$ is *o-minimal* if every set definable in $\mathbb{M}$ has finitely many connected components. The structures $\mathbb{R}_0$ and $\mathbb{R}_{\exp}$, as well as the expansion of $\mathbb{R}_{\exp}$ with bounded trigonometric functions [22], are o-minimal.

2.4 Semialgebraic sets and algebraic numbers

A set $X \subseteq \mathbb{R}^d$ is *semialgebraic* if it is definable in $\mathbb{R}_0$ without parameters. By quantifier elimination, every semialgebraic set can be written as a Boolean combination of polynomial

equalities and inequalities with integer coefficients. We say that $Z \subseteq \mathbb{C}^d$ is semialgebraic if $\widetilde{Z} = \{(x_1, y_1, \ldots, x_d, y_d) \colon (x_1 + \boldsymbol{i}y_1, \ldots, x_d + \boldsymbol{i}y_d) \in Z\}$ is a semialgebraic subset of $\mathbb{R}^{2d}$. We represent Z by a formula defining $\tilde{Z}$. A function $f \colon X \to Y$ is semialgebraic if its graph $\{(x, f(x)) \colon x \in X\} \subseteq X \times Y$ is semialgebraic. We also identify $\mathbb{R}^{a \times b}$ with $\mathbb{R}^{ab}$, and define semialgebraic subsets of $\mathbb{R}^{a \times b}$ accordingly.

A number $z \in \mathbb{C}$ is algebraic if there exists a polynomial $p \in \mathbb{Z}[x]$ such that $p(z) = 0$. The set of all algebraic numbers is denoted by $\overline{\mathbb{Q}}$. Computationally, we will be working with *real algebraic* numbers. The number $x \in \mathbb{R} \cap \overline{\mathbb{Q}}$ will be represented by a formula $\varphi \in \mathcal{L}_{or}$ defining the singleton set $\{x\}$. In this representation, arithmetic on real algebraic numbers is straightforward, and first-order properties of a given number can be verified using the decision procedure for $\mathrm{Th}(\mathbb{R}_0)$.

3 The Decomposition Method

We say that a matrix M is a *scaling matrix* if all eigenvalues of M belong to $\mathbb{R}_{\geq 0}$, and a *rotation matrix* if M is diagonalisable and all eigenvalues of M have modulus 1. A decomposition of $M \in \mathbb{R}^{d \times d}$ is a pair of matrices (C, D) such that C is a scaling matrix, D is a rotation matrix, and $M = CD = DC$.

▶ **Lemma 2.** *Every $M \in \mathbb{R}^{d \times d}$ has a decomposition (C, D). If $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$, then $C, D \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ and can be effectively computed.*

Proof. Write $M = P^{-1}JP$, where J is in real Jordan form. Once we construct a decomposition (C_J, D_J) of J, we have the decomposition $(P^{-1}C_JP, P^{-1}D_JP)$ of M. Suppose $J = \mathrm{diag}(J_1, \ldots, J_m)$, where each J_i is a real Jordan block. It suffices to construct decompositions (C_i, J_i) of J_i for $1 \leq i \leq m$: then $(\mathrm{diag}(C_1, \ldots, C_m), \mathrm{diag}(D_1, \ldots, D_m))$ is a decomposition of J.

If J_i has a single real eigenvalue, then we simply take $D = I$ and $C = J_i$. Now suppose J is of the form (1), where $\Lambda = \rho\Lambda(a, b) = \rho R(\theta)$ for some $\rho > 0$ and I is the 2×2 identity matrix. Note that the entries of $\Lambda(a, b)$ as well as ρ are real algebraic in case $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$. Let N be the nilpotent matrix satisfying $J_i = \mathrm{diag}(\Lambda(a, b), \ldots, \Lambda(a, b)) + N$. We compute the decomposition (C_i, D_i) with $D_i = aI$ and $C_i = \mathrm{diag}(\Lambda(0, b), \ldots, \Lambda(0, b)) + N$. The only eigenvalue of C_i is ρ, and the eigenvalues of D_i are $e^{\boldsymbol{i}\theta}, e^{-\boldsymbol{i}\theta} \in \mathbb{T} \cap \overline{\mathbb{Q}}$. Since D_i is diagonal, it commutes with C_i. ◀

We will apply the Decomposition Method to the Robust Safety Problem as follows. Let $M \in \mathbb{R}^{d \times d}$ and $S, T \subseteq \mathbb{R}^d$. We have that for every $\varepsilon > 0$, $M^n \cdot B(S, \varepsilon)$ does not intersect T for all $n \in \mathbb{N}$ if and only if

$$D^n \cdot B(S, \varepsilon) \text{ does not intersect } C^{-n} \cdot T$$

for all $n \in \mathbb{N}$. We will study the sequences $(D^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ and $(C^{-n} \cdot T)_{n \in \mathbb{N}}$ separately. The sequence $(D^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ is, in the parlance of dynamical systems theory, "uniformly recurrent"; this is proven using Kronecker's theorem in Diophantine approximation. The sequence $(C^{-n} \cdot T)_{n \in \mathbb{N}}$, on the other hand, converges to a limit shape in a strong sense thanks to o-minimality. We will then combine our analyses of the two sequences to prove Theorem 1.

3.1 Applications of Kronecker's theorem

We next develop the tools necessary for analysing the sequence $(D^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ where D is a rotation matrix and S is bounded and semialgebraic. Our main tool is Kronecker's classical

theorem in simultaneous Diophantine approximation. For $x, y \in \mathbb{R}$ define $[\![x]\!]_y$ to be the closest distance from x to a multiple of y, and write $[\![x]\!] = [\![x]\!]_1$.

▶ **Theorem 3** (Kronecker, see [5, Chap. 7, Sec. 1.3, Prop. 1.7]). *Let $\lambda_1, \dots, \lambda_l$ and $x_1, \dots, x_l$ be real numbers such that for all $u_1, \dots, u_l \in \mathbb{Z}$,*

$$u_1\lambda_1 + \cdots + u_l\lambda_l \in \mathbb{Z} \Rightarrow u_1x_1 + \cdots + u_lx_l \in \mathbb{Z}.$$

Then for every $\varepsilon > 0$ there exist infinitely many $n \in \mathbb{N}$ such that $[\![n\lambda_i - x_i]\!] < \varepsilon$ for all i.

Let $\beta_1, \dots, \beta_l \in \mathbb{T} \cap \overline{\mathbb{Q}}$, which in our case will be the eigenvalues of a rotation matrix D. Write $\beta = (\beta_1, \dots, \beta_l) \in \mathbb{T}^l$ and $\beta^n = (\beta_1^n, \dots, \beta_l^n)$ for $n \in \mathbb{N}$. We will use Kronecker's theorem to analyse the orbit $(\beta^n)_{n\in\mathbb{N}}$ in $\mathbb{T}^l$, from which, in the following section, we will deduce various properties of the sequence $(D^n)_{n\in\mathbb{N}}$ in $\mathbb{R}^{d\times d}$. Let

$$G(\beta) = \{(k_1, \dots, k_l) \in \mathbb{Z}^l \colon \beta_1^{k_1} \cdots \beta_l^{k_l} = 1\}$$

which is called the *group of multiplicative relations* of $(\beta_1, \dots, \beta_l)$. Observe that $G(\beta)$ is an abelian subgroup of $\mathbb{Z}^l$ and thus has a finite basis of at most l elements. Such a basis can be computed using the result [16] of Masser, which places an effective upper bound $M(\beta)$ on the smallest bit length of a basis of $G(\beta)$ in terms of the description length of β. To compute a basis, it remains to enumerate all linearly independent subsets of $\mathbb{Z}^l$ of bit length at most $M(\beta)$, and select a maximal one that only contains multiplicative relations satisfied by β.

Let $X(\beta) = \{z \in \mathbb{T}^l \colon G(\beta) \subseteq G(z)\} \subseteq \mathbb{T}^l$. We next prove that $(\beta^n)_{n\in\mathbb{N}}$ is uniformly recurrent in $X(\beta)$.

▶ **Lemma 4.** *The set $X(\beta)$ is compact, semialgebraic, and effectively computable. Moreover, for every open subset O of $\mathbb{T}^l$ containing some $\alpha \in X(\beta)$ there exist infinitely many $n \in \mathbb{N}$ such that $\beta^n \in O$.*

Proof. To compute a representation of $X(\beta)$, first compute a basis $V = \{v_1, \dots, v_m\}$ of $G(\beta)$ as described above. Write $v_i = (v_{i,1}, \dots, v_{i,l})$ for $1 \le i \le m$. Then $G(\beta) = \bigcap_{i=1}^{l} G_i$ where

$$G_i = \{(z_1, \dots, z_l) \in \mathbb{T}^l \colon z_1^{v_{i,1}} \cdots z_l^{v_{i,l}} = 1\}.$$

It remains to observe that each G_i is closed and semialgebraic.

To prove the second claim, let $\alpha = (e^{\boldsymbol{i}a_1}, \dots, e^{\boldsymbol{i}a_l})$ where $a_i \in \mathbb{R}$ for all i. Write $\beta_i = e^{\boldsymbol{i}b_i}$ where $b_i \in \mathbb{R}$ for all i. For all $n \in \mathbb{N}$,

$$\|\beta^n - \alpha\|_\infty = \max_{1\le i\le l} |e^{\boldsymbol{i}nb_i} - e^{\boldsymbol{i}a_i}| \le \max_{1\le i\le l} [\![nb_i - a_i]\!]_{2\pi} = 2\pi \cdot \max_{1\le i\le l} [\![nb_i/(2\pi) - a_i/(2\pi)]\!].$$

We will apply Kronecker's theorem to the right-hand side of the last equality and to show that it can be made arbitrarily small for infinitely many n. To do this, first we need to show that for all $u_1, \dots, u_l \in \mathbb{Z}$,

$$\frac{u_1b_1}{2\pi} + \cdots + \frac{u_lb_l}{2\pi} \in \mathbb{Z} \Rightarrow \frac{u_1a_1}{2\pi} + \cdots + \frac{u_la_l}{2\pi} \in \mathbb{Z}.$$

Suppose $\frac{u_1b_1}{2\pi} + \cdots + \frac{u_lb_l}{2\pi} \in \mathbb{Z}$, and observe that this is equivalent to $e^{\boldsymbol{i}u_1b_1} \cdots e^{\boldsymbol{i}u_lb_l} = 1$. Since $\alpha \in X(\beta)$, $G(\beta) \subseteq G(\alpha)$ and hence $e^{\boldsymbol{i}u_1a_1} \cdots e^{\boldsymbol{i}u_la_l} = 1$. The latter, in turn, is equivalent to $\frac{u_1a_1}{2\pi} + \cdots + \frac{u_la_l}{2\pi} \in \mathbb{Z}$. Applying Theorem 3 we obtain that for every $\varepsilon > 0$ there exist infinitely many $n \in \mathbb{N}$ such that $[\![nb_i/(2\pi) - a_i/(2\pi)]\!] < \varepsilon$. Hence for every $\varepsilon > 0$ there exist infinitely many $n \in \mathbb{N}$ such that $\|\beta^n - \alpha\|_\infty < \varepsilon$. It remains to construct, for the given open set O, a value $\varepsilon > 0$ such that $\{z \in \mathbb{T}^l \colon \|z - \alpha\|_\infty < \varepsilon\} \subseteq O$. ◀

▶ **Corollary 5.** *The set $X(\beta)$ is the topological closure*[3] *of $\{\beta^n : n \in \mathbb{N}\}$.*

Proof. For every $n \in \mathbb{N}$, $G(\beta) \subseteq G(\beta^n)$ and hence $\beta^n \in X(\beta)$. From the density of $(\beta^n)_{n\in\mathbb{N}}$ in $X(\beta)$ (Lemma 4) it follows that $X(\beta)$ is the closure of $(\beta^n)_{n\in\mathbb{N}}$ in $\mathbb{T}^l$. ◀

3.2 Dynamics of rotation matrices

In this section, let $D \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ be a rotation matrix and $\mathcal{D} \subseteq \mathbb{R}^{d\times d}$ be the closure of $\{D^n : n \in \mathbb{N}\}$ in $\mathbb{R}^{d\times d}$. We will study the dynamics of the LDS governed by D, and the set $\mathcal{D}$ will play a critical role therein.

▶ **Lemma 6.** *We have the following.*

(a) The set $\mathcal{D}$ is compact, semialgebraic, and effectively computable.

(b) For every $A \in \mathcal{D}$, $\det(A) = 1$. Moreover, there exists $b > 0$ such that $\|A\|, \|A^{-1}\| \leq b$ for all $A \in \mathcal{D}$.

(c) For every non-empty open subset O of $\mathcal{D}$ there exist infinitely many $n \in \mathbb{N}$ such that $D^n \in O$.

Proof. Let $\beta_1, \ldots, \beta_l \in \mathbb{T} \cap \overline{\mathbb{Q}}$ be the eigenvalues of D. Write $\beta_i = e^{\boldsymbol{i}b_i}$ for all i with $b_i \in \mathbb{R}$ and $\beta^n = (\beta_1^n, \ldots, \beta_m^n)$ for $n \in \mathbb{N}$. Define $f : \mathbb{T}^m \to \mathbb{R}^{d\times d}$ by

$$f(e^{\boldsymbol{i}\theta_1}, \ldots, e^{\boldsymbol{i}\theta_m}) = \operatorname{diag}(R(\theta_1), \ldots, R(\theta_m), I),$$

where I is the identity matrix of the suitable dimensin, and let $U = f(\mathbb{T}^m)$. We have that f is a continuous bijection (i.e. a homomorphism) between $\mathbb{T}^m$ and U. Next, write $D = P^{-1}JP$, where $P \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ and $J = f(\beta_1, \ldots, \beta_m) \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$. Observe that for all $n \in \mathbb{N}$, $J^n = f(\beta^n)$. Denote by $\mathcal{J}$ the closure of $\{J^n : n \in \mathbb{N}\}$. Since f is a homeomorphism, $\mathcal{J} = f(X(\beta))$, where $X(\beta)$ is the closure of $\{\beta^n : n \in \mathbb{N}\}$ (Corollary 5). Because f is a semialgebraic function (Section 2.4) and $X(\beta)$ is semialgebraic and effectively computable (Lemma 4), we conclude the same for $\mathcal{J}$. To prove (a) it remains to observe that $\mathcal{D} = P^{-1}\mathcal{J}P$ and hence $\mathcal{D}$ is semialgebraic and effectively computable. Since $X(\beta)$ is compact, $\mathcal{J}$ and hence $\mathcal{D}$ are also compact.

Due to the structure of J, for every $n \in \mathbb{N}$ and $x \in \mathbb{R}^d$, $\det(J^n) = 1$ and

$$\left\|J^n x\right\| = \left\|J^{-n} x\right\| = \|x\|$$

which implies that $\left\|J^n\right\| = \left\|J^{-n}\right\| = 1$. Choose $b = \|P^{-1}\| \cdot \|P\|$. We have that for every $n \in \mathbb{N}$, $\det(D^n) = \det(P^{-1})\det(J^n)\det(P) = 1$, $\left\|D^n\right\| \leq \|P^{-1}\| \cdot \left\|J^n\right\| \cdot \|P\| \leq b$, and similarly $\left\|D^{-n}\right\| \leq b$. Statement (b) then follows from the continuity of the determinant, the matrix norm, and the matrix inverse. Finally, by Lemma 4, for every non-empty open subset O of $X(\beta)$ there exist infinitely many $n \in \mathbb{N}$ such that $\beta^n \in O$. Statement (c) then follows from the fact that f is a homeomorphism. ◀

We can now give the main result of this section, which is about the orbit of an open set in a dynamical system defined by a rotation matrix.

▶ **Lemma 7.** *Let $O \subseteq \mathbb{R}^d$ be open.*

(a) For all $n \in \mathbb{N}$, $D^n \cdot O \subseteq \mathcal{D} \cdot O$.

(b) For every $y \in \mathcal{D} \cdot O$ there exists $\varepsilon > 0$ such that $D^n \cdot O \supset B(y, \varepsilon)$ for infinitely many $n \in \mathbb{N}$.

[3] This holds both in $\mathbb{T}^l$ and $\mathbb{C}^l$, since the former is itself closed in the latter.

Proof. Statement (a) follows immediately from the fact that $D^n \in \mathcal{D}$ for all $n \in \mathbb{N}$. To prove (b), consider $y \in \mathcal{D} \cdot O$. By definition of $\mathcal{D}$, there exist $A \in \mathcal{D}$ and $z \in O$ such that $y = Az$. Let $\varepsilon_1, \varepsilon_2 > 0$ be such that $O \supseteq B(z, \varepsilon_1 + \varepsilon_2)$. We choose $\varepsilon = \varepsilon_1 / b$, where b is such that $\|X\|, \|X^{-1}\| \leq b$ for all $X \in \mathcal{D}$ (Lemma 6 (b)). Recalling that every $X \in \mathcal{D}$ is invertible, construct $\delta > 0$ be such that for all $X \in \mathcal{D}$ with $\|X - A\| < \delta$, we have that $y \in X \cdot B(z, \varepsilon_2)$.

Consider $D^n \in \mathcal{D}$ such that $\|D^n - A\| < \delta$. By Lemma 6 (c), there exist infinitely many such n. We have that

$$D^n \cdot O \supseteq D^n \cdot B(z, \varepsilon_1) + D^n \cdot B(\varepsilon_2) \supseteq y + D^n \cdot B(\varepsilon_1).$$

Since $\|D^{-n}\| \leq b$, we have that $D^n \cdot B(\varepsilon_1) \supseteq B(\varepsilon_1 / b) = B(\varepsilon)$. Therefore, $D^n \cdot O \supseteq B(y, \varepsilon)$. ◀

3.3 Real exponentiation and o-minimality

We now develop the tools necessary for studying dynamics of scaling matrices. The main results of this section are certain (effective) convergence arguments in o-minimal structures.

We say that a sequence $(Z_n)_{n \in \mathbb{N}}$ of subsets of $\mathbb{R}^d$ is *definable* in a structure $\mathbb{S}$ expanding $\mathbb{R}_0$ if there exist $k \geq 0$, $a_1, \ldots, a_m \in \mathbb{R}$, and $\varphi \in \mathcal{L}_{\mathbb{S}}$ with $d + m + 1$ free variables such that for all $n \in \mathbb{N}$ and $x = (x_1, \ldots, x_d) \in \mathbb{R}^d$, $x \in Z_n$ if and only if $\varphi(x_1, \ldots, x_d, n, a_1, \ldots, a_m)$ holds in $\mathbb{S}$. The following form of convergence is also known as *Kuratowski convergence*, and captures the kind of set-to-set convergence with which we will work.

▶ **Definition 8.** *Let $(Z_n)_{n \in \mathbb{N}}$ be a sequence of subsets of $\mathbb{R}^d$, and*

$$L = \{x \in \mathbb{R}^d \colon \liminf_{n \to \infty} d(x, Z_n) = 0\}.$$

We say that $(Z_n)_{n \in \mathbb{N}}$ converges if $L = \{x \in \mathbb{R}^d \colon \lim_{n \to \infty} d(x, Z_n) = 0\}$, in which case L is called the limit shape of $(Z_n)_{n \in \mathbb{N}}$.

We immediately have the following.

▶ **Lemma 9.** *Suppose L is the limit shape of $(Z_n)_{n \in \mathbb{N}}$. Then*

(a) L is closed,

(b) $L = \varnothing$ if and only if for every compact X, there exists N such that $Z_n \cap X = \varnothing$ for all $n \geq N$, and

(c) for every compact $X \subseteq \mathbb{R}^d$ and $\varepsilon > 0$, there exists N such that for all $n \geq N$,

$$Z_n \cap X \subseteq B(L \cap X, \varepsilon).$$

Proof. Statement (a) is immediate from the definition, and (b) follows from the Bolzano-Weierstraß theorem. To prove (c), fix compact X and $\varepsilon > 0$. The set $Y \coloneqq X \setminus B(L \cap X, \varepsilon)$ is compact. For every $y \in Y$, since $Y \notin L$, there exist $N_y \in \mathbb{N}$ and an open subset $B_y \ni y$ of Y such that $Z_n \cap B_y = \varnothing$ for all $n \geq N_y$. Hence $\mathcal{C} = \{B_y \colon y \in Y\}$ is an open cover of Y. Let $\mathcal{F}$ be a finite sub-cover. We can then take $N = \max\{N_y \colon y \in \mathcal{F}\}$. ◀

We mention that by the properties above, for $(Z_n)_{n \in \mathbb{N}}$ contained in a compact set X our notion of convergence coincides with convergence with respect to the Hausdorff metric. Next, we recall that a function definable in an o-minimal structure is ultimately monotonic [23, Sec. 4.1]. The following is an immediate consequence, but we give a little more detail to illustrate the role of o-minimality.

▶ **Theorem 10.** *Every $(Z_n)_{n \in \mathbb{N}}$ definable in an o-minimal expansion $\mathbb{S}$ of $\mathbb{R}_0$ converges.*

Proof. Let $a_1, \ldots, a_m \in \mathbb{R}$ and $\varphi \in \mathcal{L}_{\mathbb{S}}$ be a formula with $d+m+1$ free variables such that

$$(x_1, \ldots, x_d) \in Z_n \Leftrightarrow \varphi(x_1, \ldots, x_d, n, a_1, \ldots, a_m) \text{ holds in } \mathbb{S}$$

for all $(x_1, \ldots, x_d) \in \mathbb{R}^d$ and $n \in \mathbb{N}$. Consider $x \in \mathbb{R}^k$ with $\liminf_{n\to\infty} d(x, Z_n) = 0$ and $\Delta > 0$. Let

$$T = \{t \geq 0 \mid \exists y = (y_1, \ldots, y_d) \colon d(x, y) < \Delta \wedge \varphi(y_1, \ldots, y_d, t, a_1, \ldots, a_m)\}$$

which is definable in $\mathbb{S}$. By o-minimality, T is a finite union of interval subsets of $\mathbb{R}_{\geq 0}$. Since $\liminf_{t\to\infty} d(x, Z_n) = 0$, T must be unbounded. Therefore, T must enclose an interval of the form $[N, \infty)$. That is, $d(x, Z_n) < \Delta$ for all sufficiently large n. It follows that $\lim_{n\to\infty} d(x, Z_n) = 0$. ◀

In the cases we will encounter, the limit shape L will be a semialgebraic set whose representation can be computed effectively. To show this, we first need a lemma.

▶ **Lemma 11.** *Let $k > 0$, $\varphi \in \mathcal{L}_{or}$ with $k+m+1$ free variables, and $\rho_1, \ldots, \rho_m \in \mathbb{R}_{>0} \cap \overline{\mathbb{Q}}$. Define*

$$A = \{(x_1, \ldots, x_k) \in \mathbb{R}^k \mid \exists N. \forall n \geq N \colon \varphi(x_1, \ldots, x_k, n, \rho_1^n, \ldots, \rho_m^n)\}$$

and

$$B = \{(x_1, \ldots, x_k) \in \mathbb{R}^k \mid \exists N. \forall n \geq N \colon \neg\varphi(x_1, \ldots, x_k, n, \rho_1^n, \ldots, \rho_m^n)\}.$$

We have the following.

(a) $A \cup B = \mathbb{R}^k$.

(b) Both A and B are semialgebraic sets whose representations can be computed effectively.

(c) Given $(x_1, \ldots, x_k) \in B \cap \mathbb{Q}^k$, we can effectively compute $N \in \mathbb{N}$ such that for all $n \geq N$, $\varphi(x_1, \ldots, x_k, n, \rho_1^n, \ldots, \rho_m^n)$ does not hold.

Proof. Let $(x_1, \ldots, x_k) \in \mathbb{R}^k$, and define $T = \{t \geq 0 \colon \varphi(x_1, \ldots, x_k, t, \rho_1^t, \ldots, \rho_m^t)\}$. By o-minimality of $\mathbb{R}_{\exp}$, either T is bounded, or it encloses an interval of the form $[N, \infty)$. That is, $(x_1, \ldots, x_k)$ belongs to either A or B. This proves (a).

Next, using quantifier elimination in $\mathrm{Th}(\mathbb{R}_0)$, compute a formula

$$\bigvee_{i\in I} \bigwedge_{j\in J} p_{i,j}(x_1, \ldots, x_k, y_0, \ldots, y_m) \; \Delta_{i,j} \; 0 \tag{2}$$

in $\mathcal{L}_{or}$ equivalent to $\varphi(x_1, \ldots, x_k, y_0, \ldots, y_m)$, where each $p_{i,j}$ is a polynomial with rational coefficients and $\Delta_{i,j} \in \{>, =\}$. For $i \in I$ and $j \in J$, write

$$p_{i,j}(x_1, \ldots, x_k, n, \rho_1^n, \ldots, \rho_m^n) = \sum_{l=1}^{d} h_l(x_1, \ldots, x_k) q_l(n) R_l^n$$

where $R_1 > \ldots > R_d > 0$, each R_i real algebraic, and h_l, q_l are non-zero polynomials. Without loss of generality we can further assume that $q_l(n) > 0$ for all sufficiently large n. Let

$$A_{i,j} = \{(x_1, \ldots, x_k) \in \mathbb{R}^k \colon p_{i,j}(x_1, \ldots, x_k, n, \rho_1^n, \ldots, \rho_m^n) \; \Delta_{i,j} \; 0 \text{ for all sufficiently large } n\}.$$

Observe that whether $(x_1, \dots, x_k) \in A_{i,j}$ only depends on the sign of $h_l(x_1, \dots, x_k)$ for $1 \leq l \leq d$. In particular, if $\Delta_{i,j}$ is $=$, then $A_{i,j}$ is defined by $\bigwedge_{l=1}^{d} h_l(x_1, \dots, x_k) = 0$. If $\Delta_{i,j}$ is $>$, then $A_{i,j}$ defined by

$$\bigvee_{l=1}^{d} \Big(h_l(x_1, \dots, x_k) > 0 \wedge \bigwedge_{s=1}^{l-1} h_s(x_1, \dots, x_k) = 0 \Big).$$

Hence $A_{i,j}$ is semialgebraic with an effectively computable representation. It remains to observe that $A = \bigvee_{i \in I} \bigwedge_{j \in J} A_{i,j}$.

To prove (c), fix $x = (x_1, \dots, x_k) \in B \cap \mathbb{Q}^k$. Let $\varphi \in \mathcal{L}_{or}$ be the formula obtained by substituting the values of $x_1, \dots, x_k$ into (2), which will be of the form

$$\psi(y_0, \dots, y_m) \coloneqq \bigvee_{i \in I} \bigwedge_{j \in J} v_{i,j}(y_0, \dots, y_m) \; \Delta_{i,j} \; 0$$

for non-zero polynomials $v_{i,j}$ with rational coefficients and $\Delta_{i,j} \in \{>, =\}$. We have to construct N such that for all $n \geq N$, $\psi(n, \rho_1^n, \dots, \rho_m^n)$ does not hold. To do this, it suffices to construct, for each $i \in I$ and $j \in J$, an integer $N_{i,j}$ such that either $v_{i,j}(n, \rho_1^n, \dots, \rho_m^n) \; \Delta_{i,j} \; 0$ holds for all $n \geq N_{i,j}$, or it does not hold for all $n \geq N_{i,j}$. We can then take $N = \max_{i,j} N_{i,j}$.

Fix i, j, and write $v_{i,j}(n, \rho_1^n, \dots, \rho_m^n) = \sum_{l=1}^{d} q_l(n) R_l^n$ where $R_1 > \dots > R_d > 0$, and each q_l is a non-zero polynomial with rational coefficients. Compute rationals $M_1, M_2, c > 0$ and $N_{i,j} \in \mathbb{N}$ such that

- $R_1 > M_1 > M_2 > R_2$,
- for all $t \geq N_{i,j}$, $|q_1(t)| > c$, and
- $cM_1^n > (d-1) q_l(n) M_2^n$ for all $n \geq N_{i,j}$.

The sign of $v_{i,j}(n, \rho_1^n, \dots, \rho_m^n)$ is stable for $n \geq N_{i,j}$ and the same as the sign of $q_1(n)$. ◀

The following is our main effective convergence result.

▶ **Lemma 12.** *Let $(Z_n)_{n \in \mathbb{N}}$ be a sequence of subsets of $\mathbb{R}^d$. Suppose there exist $\varphi \in \mathcal{L}_{or}$ and $\rho_1, \dots, \rho_m \in \mathbb{R}_{>0} \cap \overline{\mathbb{Q}}$ such that for all $x = (x_1, \dots, x_d) \in \mathbb{R}^d$ and $n \in \mathbb{N}$,*

$$x \in Z_n \Leftrightarrow \varphi(x_1, \dots, x_d, n, \rho_1^n, \dots, \rho_m^n). \tag{3}$$

Then $(Z_n)_{n \in \mathbb{N}}$ converges, and the limit shape L of $(Z_n)_{\geq 0}$ is semialgebraic and can be effectively computed from $\varphi, \rho_1, \dots, \rho_m$.

Proof. The sequence $(Z_n)_{n \in \mathbb{N}}$ is definable in $\mathbb{R}_{\exp}$ and thus converges by Theorem 10. Let

$$X = \{(\varepsilon, x_1, \dots, x_d) \mid \varepsilon > 0 \text{ and } \exists N. \, \forall n \geq N \colon d((x_1, \dots, x_d), Z_n) < \varepsilon\}.$$

Invoking Lemma 11 with $k = d_1$ we conclude that X is semialgebraic and effectively computable. It remains to observe that the limit shape is

$$L = \{(x_1, \dots, x_d) \mid \forall \varepsilon > 0 \colon (\varepsilon, x_1, \dots, x_d) \in X\}$$

which is semialgebraic and can be effectively computed from X. ◀

3.4 Dynamics of scaling matrices

Now consider a scaling matrix $C \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ and a semialgebraic set $T \subseteq \mathbb{R}^d$. In order to apply the Decomposition Method, one of the prerequisites is to understand the sequence of sets $(C^{-n} \cdot T)_{n \in \mathbb{N}}$. We have the following.

▶ **Lemma 13.** *Suppose the non-zero eigenvalues of C are $\rho_1, \ldots, \rho_m$. We can compute $\varphi \in \mathcal{L}_{or}$ such that for all $n \in \mathbb{N}$ and $(x_1, \ldots, x_d) \in \mathbb{R}^d$,*

$$x \in C^{-n} \cdot T \Leftrightarrow \varphi(x_1, \ldots, x_d, n, \rho_1^{-n}, \ldots, \rho_m^{-n}).$$

Proof. Note that $\rho_1, \ldots, \rho_m$ must be positive by the assumption that C is a scaling matrix. The proof follows immediately from the real Jordan form and the definition of $C^{-n} \cdot T$ (Section 2.1). ◀

▶ **Lemma 14.** *The sequence $(C^{-n} \cdot T)_{n \in \mathbb{N}}$ converges to a limit shape L that is semialgebraic and an effectively computable.*

Proof. Let $\rho_1, \ldots, \rho_m$ and φ be as above, and apply Lemma 12. ◀

4 Proof of Theorem 1

We now prove our main result. Given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$, non-empty and bounded semialgebraic S, and semialgebraic T, let (C, D) be a decomposition of M with $C, D \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$. Recall the definitions of μ_1, μ_2 from the statement of Theorem 1, and that for all n and ε,

$$M^n \cdot B(S, \varepsilon) \text{ intersects } T \Leftrightarrow D^n \cdot B(S, \varepsilon) \text{ intersects } C^{-n} \cdot T.$$

Let $\mathcal{D}$ be the closure of $\{D^n : n \in \mathbb{N}\}$ (Lemma 6) and L be the limit shape of $(C^{-n} \cdot T)_{n \in \mathbb{N}}$ (Lemma 14). Define $\mu_3 = \sup \{\varepsilon \geq 0 : \mathcal{D} \cdot B(S, \varepsilon) \text{ intersects } L\}$.

Figure 1 depicts our application of the Decomposition Method. The bounded initial set is the triangle S. We are interested in the sequences $(D^n \cdot B(S, \varepsilon))_{n \in \mathbb{N}}$ for various $\varepsilon \geq 0$: specifically, we want to understand the time steps n at which $D^n \cdot B(S, \varepsilon)$ intersects $C^{-n} \cdot T$. We see that $\varepsilon = \mu_3$ is the critical value: in this case $\mathcal{D} \cdot B(S, \varepsilon)$, which envelopes $D^n \cdot B(S, \varepsilon)$ for all n, just about touches the limit shape L. We have that for $\varepsilon \in (0, \mu_3)$, for all sufficiently large n, $C^{-n} \cdot T$ is very close to L and thus is well-separated from $D^n \cdot B(S, \varepsilon)$. On the other hand, for $\varepsilon > \mu_3$, once again $C^{-n} \cdot B(S, \varepsilon)$ stabilises around L for large values of n, and by uniform recurrence of $D^n \cdot B(S, \varepsilon)$ in $\mathcal{D} \cdot B(S, \varepsilon)$ (Lemma 7), $D^n \cdot B(S, \varepsilon)$ intersects $C^{-n} \cdot T$ for infinitely many n. We next formalise these arguments.

▷ Claim. $\mu_2 = \mu_3$.

Proof. Suppose $\varepsilon > 0$ is such that $\varepsilon < \mu_3$. Then there exists $\varepsilon' \in (\varepsilon, \mu_3)$ such that $\mathcal{D} \cdot B(S, \varepsilon')$ is disjoint from L. Let $\varepsilon'' > 0$ be such that $B(L, \varepsilon'')$ is disjoint from $B(S, \varepsilon')$. Further let X be a compact subset of $\mathbb{R}^d$ containing $B(S, \varepsilon')$, and, applying Lemma 9 (c), N be such that for all $n \geq N$, $(C^{-n} \cdot T) \cap X \subseteq B(L \cap X, \varepsilon'')$. We have that for $n \geq N$, $\mathcal{D} \cdot B(S, \varepsilon)$ is disjoint from $C^{-n} \cdot T$, which implies the same for $D^n \cdot B(S, \varepsilon)$. Therefore, $\varepsilon \leq \mu_2$. Since the choice of ε was arbitrary, it follows that $\mu_3 \leq \mu_2$.

Now suppose $\varepsilon > 0$ is such that $\varepsilon > \mu_3$. Take $x \in L \cap (\mathcal{D} \cdot B(S, \varepsilon))$, and, invoking Lemma 7 (with $O = B(S, \varepsilon)$), let $\varepsilon' > 0$ be such that $D^n \cdot B(S, \varepsilon) \supseteq B(x, \varepsilon')$ for infinitely many $n \in \mathbb{N}$. Since $x \in L$, by definition of convergence, there exists N such that for all $n \geq N$, $C^{-n} \cdot T$ intersects $B(x, \varepsilon')$. Therefore, for infinitely many $n \geq N$, $D^n \cdot B(S, \varepsilon)$ intersects $C^{-n} \cdot T$. Therefore, $\varepsilon \geq \mu_2$. It follows that $\mu_2 \leq \mu_3$. ◁

Observe that the time step n does not appear in the definition of μ_3, which we now know to be equal to μ_2. Since both $\mathcal{D}$ and L are semialgebraic, we can use a decision procedure for the theory of $\mathbb{R}_0$ to check whether μ_2 is finite. If this is the case, we can compute a formula $\varphi \in \mathcal{L}_{or}$ that defines the set $\{\mu_2\}$. Thus μ_2 must be algebraic.

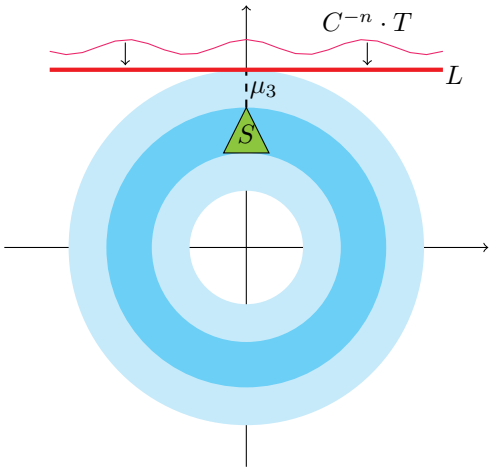

Figure 1 Illustration of the Decomposition Method. Here $\mathcal{D} = \{R(\theta) \colon \theta \in \mathbb{R}\} \subset \mathbb{R}^{2\times 2}$ is the group of all 2×2 matrices whose action is a rotation, the larger annulus (light blue) is $\mathcal{D} \cdot B(S, \mu_3)$, and the smaller one (blue) is $\mathcal{D} \cdot S$. The sequence $(C^{-n} \cdot T)_{n\in\mathbb{N}}$ converges to L. The length of the dashed line segment in μ_3.

Now consider $\varepsilon \in (0, \mu_2) \cap \mathbb{Q}$. We have to construct N such that $(M \cdot B(S, \varepsilon))_{n\in\mathbb{N}}$ avoids T. Using Lemma 13 we can construct a formula $\varphi \in \mathcal{L}_{or}$ such that for all n, $\varphi(\varepsilon, n, \rho_1^{-n}, \ldots, \rho_m^{-n})$ holds if and only if $\mathcal{D} \cdot B(S, \varepsilon)$ intersects $C^{-n} \cdot T$, where $\rho_1, \ldots, \rho_m$ are the non-zero eigenvalues of C. By construction of ε, $\varphi(\varepsilon, n, \rho_1^{-n}, \ldots, \rho_m^{-n})$ evaluates to false for all sufficiently large n. Therefore, we can compute the desired N using Lemma 11 (c).

We now move on to μ_1. For $n \in \mathbb{N}$, let

$$\varepsilon_n = \sup\{\varepsilon \geq 0 \colon D^n \cdot B(S, \varepsilon) \text{ does not intersect } C^{-n} \cdot T\}.$$

Each ε_n is algebraic and $\mu_1 = \inf_{n\in\mathbb{N}} \varepsilon_n$. Note that each ε_n is non-negative, but it is possible that $\varepsilon_n > \mu_2$. We perform a case analysis based on whether μ_2 is infinite.

Case I.

Suppose μ_2 is infinite, which is the case if and only if $L = \varnothing$. By Lemma 9 (b), for every compact X, $C^{-n} \cdot T$ does not intersect X for all sufficiently large n. Let $X = \mathrm{Cl}(\mathcal{D} \cdot B(S, \varepsilon_1))$ and N be such that $C^{-n} \cdot T$ does not intersect X for all $n \geq N$. It follows that $\varepsilon_n \geq \varepsilon_1$ for all $n \geq N$ and thus

$$\mu_1 = \inf_{n\in\mathbb{N}} \varepsilon_n = \sup\{\varepsilon_0, \ldots, \varepsilon_{N-1}\}.$$

In this case, we can explicitly compute μ_1, and it is algebraic. We can also decide whether $\mu_1 = 0$.

Case II.

Now suppose $\mu_2 \in \mathbb{R} \cap \overline{\mathbb{Q}}$, i.e. L is non-empty. We claim that $\liminf_{n\to\infty} \varepsilon_n = \mu_2$. This immediately implies that μ_1 is algebraic, since $\inf_{n\in\mathbb{N}} \varepsilon_n$ is either equal to ε_n for some n, or to $\liminf_{n\to\infty} \varepsilon_n$.

Let $X = \mathrm{Cl}(\mathcal{D} \cdot B(S, \mu_2))$, which is compact. By Lemma 9 (c), for every $\varepsilon > 0$ there exists N such that $(C^{-n} \cdot T) \cap X \subseteq B(L \cap X, \varepsilon)$ for all $n \geq N$. Thus for every $\delta > 0$, $\varepsilon_n > \mu_2 - \delta$

for sufficiently large n, and hence $\lim_{n\to\infty} \varepsilon_n \geq \mu_2$. On the other hand, by definition of μ_2, $\varepsilon_n \leq \mu_2$ for infinitely many n. It follows that $\lim_{n\to\infty} \varepsilon_n \leq \mu_2$.

It remains to show how to decide whether $\mu_1 = 0$ and approximate μ_1 to arbitrary precision. Let $\varepsilon \in (0, \mu_2) \in \overline{\mathbb{Q}}$ and X be as above. Using Lemma 9 (c), Lemma 13, and Lemma 11 compute $N \in \mathbb{N}$ such that for all $n \geq N$, $C^{-n} \cdot T$ is disjoint from $\mathcal{D} \cdot B(S, \varepsilon)$. Then $\varepsilon_n \geq \varepsilon$ for all $n \geq N$. Compute $\xi = \min\{\varepsilon_0, \ldots, \varepsilon_{N-1}\}$. We have that $\mu_1 = 0$ if and only if $\xi = 0$, which gives us the desired decision procedure. The approximation $\widetilde{\mu} = \min\{\xi, \varepsilon\}$, on the other hand satisfies $\widetilde{\mu} \leq \mu_1$ and, since $\mu_1 \leq \mu_2$, has the absolute error of at most $\mu_2 - \varepsilon$. Therefore, we can obtain arbitrarily good sandwiching approximations $(\widetilde{\mu}, \widetilde{\mu} + \mu_2 - \varepsilon)$ of μ_1 by taking $\varepsilon \to \mu_2$ from below.

The reason we are unable to determine μ_1 exactly is as follows. Suppose we compute $\varepsilon_0, \ldots, \varepsilon_N$ for some large N, and observe that $\varepsilon_0 > \cdots > \varepsilon_N > \mu_2$. There are two possibilities: either ε_n remains above μ_2 for all n, in which case the limit is μ_2, or $\varepsilon_n < \mu_2$ for some n, in which case the limit is an element of the sequence $(\varepsilon_n)_{n\in\mathbb{N}}$. But it is not possible to determine which is the case using the tools we currently have.

5 Other applications of o-minimality

In this section we briefly discuss how o-minimality and the Decomposition Method are related to various other problems of linear dynamical systems.[4] We first discuss semialgebraic and o-minimal *invariants*. An invariant of the LDS with update matrix $M \in \mathbb{R}^{d\times d}$ is a set $\mathcal{I} \subseteq \mathbb{R}^d$ such that $M \cdot \mathcal{I} \subseteq \mathcal{I}$. We say that an invariant $\mathcal{I}$ of M *separates* an initial set S from a target set T if $S \subseteq \mathcal{I}$ and $T \cap \mathcal{I} = \varnothing$. Intuitively, such $\mathcal{I}$ certifies that all trajectories starting at S are safe: for all $s \in S$ and $n \in \mathbb{N}$, $M^n s \notin T$. In [3], the authors prove the following. Let $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, T be semialgebraic, and $S = \{s\}$ be a singleton with $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$.

- It is decidable whether M has an invariant $\mathcal{I}$ definable in $\mathbb{R}_{\exp}$.
- If such $\mathcal{I}$ exists, then it can be taken to be semialgebraic.

Their arguments can be implemented in the framework of the Decomposition Method. We can moreover easily generalise from singleton to bounded S.

▶ **Proposition 15** (See [11, Chap. 9.5]). *Let $S \subseteq \mathbb{R}^d$ be bounded and semialgebraic, T be semialgebraic, and $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ with a decomposition (C, D) over $(\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$. Further let $\mathcal{D}$ be the closure of $\{D^n : n \in \mathbb{N}\}$ and L be the limit shape of $(C^{-n} \cdot T)_{n\in\mathbb{N}}$.*

1. *For all $n \in \mathbb{N}$, $M^n \cdot S$ intersects T if and only if $D^n \cdot S$ intersects $C^{-n} \cdot T$.*
2. *We can compute N such that either (i) for all $n \geq N$, $\mathcal{D} \cdot S$ intersects $C^{-n} \cdot T$, or (ii) $\mathcal{D} \cdot S$ does not intersect $C^{-n} \cdot T$ for all $n \geq N$.*
3. *There exists an $\mathbb{R}_{\exp}$-definable invariant $\mathcal{I}$ of M separating S from T if and only if (i) holds, in which case $\mathcal{I}$ can be taken to be semialgebraic.*

Statement (1) is immediate from the definition of a decomposition, and (2) is an application of Lemma 11: the dichotomy (i-ii), without effectiveness of N, can be shown using just o-minimality. Proving (3) requires retracing the arguments of [3]. Intuitively, Proposition 15 states that we can topologically separate $M^n \cdot S$ from T using an $\mathbb{R}_{\exp}$-definable set if and only if we can topologically separate $\mathcal{D} \cdot S$ (and hence $D^n \cdot S$) from $C^{-n} \cdot T$ for all sufficiently large n. Combining this with our analysis of the Robust Safety Problem yields the following.

[4] A complete account of the claims in this section, as well as details of how the Pseudo-Orbit Reachability Problem can be solved using the Decomposition Method, will be given in a future paper.

▶ **Proposition 16.** *Let M, S, T be as above. If there exists $\varepsilon > 0$ such that $M^n \cdot B(S, \varepsilon)$ does not intersect T for all n, then there exists a semialgebraic invariant $\mathcal{I}$ separating S from T.*

The idea of the proof is that if $\langle M, S, T\rangle$ is a positive instance of the Robust Safety Problem, then there exists $\varepsilon > 0$ such that for all sufficiently large n, $\mathcal{D}\cdot B(S, \varepsilon)$ does not intersect $C^{-n}\cdot T$; this is even stronger than the topological separation described in (ii) of Proposition 15 (b). The converse of Proposition 16 does not hold already in dimension $d = 1$.

We next discuss the main result of [13] that, given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, an initial point $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$, and semialgebraic $T \subseteq \mathbb{R}^d$, the frequency

$$\mu = \lim_{n\to\infty} \frac{|\{0 \le k < n \colon M^k s \in T\}|}{n}$$

is well-defined, can be approximated to arbitrary precision, and can be effectively compared against zero. The method of [13] is to first use lower bounds on sums of S-units [10], a deep result from algebraic number theory, to express μ in terms $\lambda_1, \ldots, \lambda_m \in \mathbb{T} \cap \overline{\mathbb{Q}}$. The second step is to use Weyl's equidistribution theorem to write μ as an integral, which can be evaluated to arbitrary precision using numerical techniques. We can use o-minimality and the Decomposition Method to give a full geometric version of the first step.

▶ **Proposition 17.** *Let $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ with a decomposition (C, D) over $(\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, and $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$. Further let $\mathcal{D}$ be the closure of $\{D^n \colon n \in \mathbb{N}\}$ and L be the limit shape of $(C^{-n} \cdot T)_{n\in\mathbb{N}}$. Then*

$$\mu = \lim_{n\to\infty} \frac{|\{0 \le k < n \colon M^k s \in T\}|}{n} = \lim_{n\to\infty} \frac{|\{0 \le k < n \colon D^n s \in C^{-n} \cdot T\}|}{n}$$

is exactly equal to the measure of $L \cap (\mathcal{D} \cdot s)$ in a suitable probability space over $\mathcal{D} \cdot S$.

The aforementioned probability space is derived from the Haar measure on $\mathcal{D}$. We sketch the proof of Proposition 17. Write $X = \mathcal{D} \cdot s$. Because X is bounded, by Lemma 9, $(C^{-n} \cdot T) \cap X$ converges uniformly (with respect to the Hausdorff metric) to $L \cap X$ as $n \to \infty$. Thus when measuring the frequency μ, we can pass from the sequence $(C^{-n} \cdot T)_{n\in\mathbb{N}}$ to the limit shape $L \cap X$. We thus need to understand the frequency with which $(D^n s)_{n\in\mathbb{N}}$ intersects $L \cap X$, which, by Weyl's equidistribution theorem, can expressed as an integral over X. To check whether $\mu > 0$, we simply check, using tools from semialgebraic geometry, whether $L \cap X$ has full dimension in X.

It is now understood that o-minimality gives us strong ergodic properties of linear dynamical systems, despite the fact that they are typically not compact. This idea is pursued further in the recent work [1], where it shown how to compute an integral representation for the *mean payoff* $\mu = \frac{1}{n}\sum_{k=0}^{n-1} w(M^n)$, where $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ and $w \in \mathbb{R}^{d\times d} \to \mathbb{R}$ is a *weight function* definable in $\mathbb{R}_{\exp}$. Let (C, D) be a decomposition of M. The idea is to write

$$\mu = \frac{1}{n}\sum_{k=0}^{n-1} f(C^n D^n) = \frac{1}{n}\sum_{k=0}^{n-1} f_n(D^n)$$

where $f_n \colon \mathcal{D} \to \mathbb{R}$ with $f_n(X) = C^n \cdot X$. Then the sequence of functions $(f_n)_{n\in\mathbb{N}}$, when viewed as a sequence of subsets of $\mathcal{D} \times \mathbb{R}$, converges pointwise to a limit function $f \colon \mathcal{D} \to \mathbb{R}$ (Lemma 12). The next step is to argue that, in fact, $\mu = \lim_{n\to\infty} \frac{1}{n}\sum_{k=0}^{n-1} f(D^n)$, after which we can compute the integral representation of μ using the fact that $(D^n)_{n\in\mathbb{N}}$ is ergodic by Weyl's equidistribution theorem. We can also approximate μ to arbitrary precision using the aforementioned integral representation. This, however, requires assuming Schanuel's conjecture since in the most general setting all we know about f is that it is definable in $\mathbb{R}_{\exp}$.

References

1 Rajab Aghamov, Christel Baier, Toghrul Karimov, Joël Ouaknine, and Jakob Piribauer. Linear dynamical systems with weight functions. *arXiv preprint*, 2025.

2 S. Akshay, Hugo Bazille, Blaise Genest, and Mihir Vahanwala. On robustness for the Skolem, positivity and ultimate positivity problems. *Logical Methods in Computer Science*, 20, 2024.

3 Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for discrete-time dynamical systems. *ACM Transactions on Computational Logic (TOCL)*, 23(2):1–20, 2022.

4 Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36. Springer Science & Business Media, 2013.

5 Nicolas Bourbaki. *Elements of Mathematics: General Topology. Part 2*. Hermann, 1966.

6 Jin-Yi Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. *International Journal of Foundations of Computer Science*, 5(04):293–302, 1994.

7 Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, Sadegh Soudjani, and James Worrell. The pseudo-skolem problem is decidable. *LIPIcs*, 202, 2021.

8 Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, and James Worrell. The pseudo-reachability problem for diagonalisable linear dynamical systems. *arXiv preprint arXiv:2204.12253*, 2022.

9 Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, and James Worrell. The pseudo-reachability problem for diagonalisable linear dynamical systems. In *47th International Symposium on Mathematical Foundations of Computer Science*, 2022.

10 Jan-Hendrik Evertse. On sums of S-units and linear recurrences. *Compositio Mathematica*, 53(2):225–244, 1984.

11 Toghrul Karimov. *Algorithmic verification of linear dynamical systems*. PhD thesis, Saarland University, 2024.

12 Toghrul Karimov, Engel Lefaucheux, Joël Ouaknine, David Purser, Anton Varonka, Markus Whiteland, and James Worrell. What's decidable about linear loops? *Proceedings of the ACM on Programming Languages*, 6(POPL):1–25, 2022.

13 Edon Kelmendi. Computing the density of the positivity set for linear recurrence sequences. *Logical Methods in Computer Science*, 19, 2023.

14 Gerardo Lafferriere, George Pappas, and Shankar Sastry. O-minimal hybrid systems. *Mathematics of control, signals and systems*, 13:1–21, 2000.

15 A. Macintyre, A. Wilkie, and P. Odifreddi. On the decidability of the real exponential field. *Kreisel's Mathematics*, 115:451, 1996.

16 D. W. Masser. *Linear Relations on Algebraic Groups*, page 248–262. Cambridge University Press, 1988. doi:10.1017/CBO9780511897184.016.

17 M. Mignotte, T. N. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 349, 1984.

18 Chris Miller. Expansions of o-minimal structures on the real field by trajectories of linear vector fields. *Proceedings of the American Mathematical Society*, 139(1):319–330, 2011.

19 Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, 12 2013. doi:10.1137/1.9781611973402.27.

20 Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *International Colloquium on Automata, Languages, and Programming*, pages 330–341. Springer, 2014.

21 J. Pila, G. Jones, and A. Wilkie. O-minimality and Diophantine geometry. In *Proceedings ICM*, 2014.

22 Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel Journal of Mathematics*, 85:19–56, 1994.

23 Lou van den Dries and Chris Miller. Geometric categories and o-minimal structures. *Duke Mathematical Journal*, 84(2):497–540, 1996. doi:10.1215/S0012-7094-96-08416-1.

24 G. Wüstholz and A. Baker. Logarithmic forms and group varieties. *Journal für die reine und angewandte Mathematik*, 442:19–62, 1993.

25 Kunrui Yu. p-Adic logarithmic forms and group varieties II. *Acta Arithmetica*, 89(4):337–378, 1999. URL: http://eudml.org/doc/207276.