Semialgebraic Model Checking for Linear Dynamical Systems

Toghrul Karimov[1], Engel Lefaucheux[1], Joël Ouaknine[1], David Purser[1], Anton Varonka[1,2], Markus A. Whiteland[1], and James Worrell[3]

[1] Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany
[2] Saarbrücken Graduate School of Computer Science, Saarland Informatics Campus, Germany
[3] Department of Computer Science, University of Oxford, UK

Abstract. We consider the MSO model-checking problem for discrete-time linear dynamical systems in arbitrary ambient dimension, with semialgebraic predicates. We establish decidability provided that each semialgebraic predicate *either* has intrinsic dimension 1, *or* is contained within some three-dimensional subspace.

1 Introduction

Dynamical systems are a fundamental modelling paradigm in many branches of science, and have been the subject of extensive research for many decades. In this paper, we focus on model-checking problems for orbits of *discrete-time linear dynamical systems*. Such a system is given by a square $d \times d$ matrix M with rational entries, together with a starting point $x \in \mathbb{Q}^d$. The *orbit* of (M, x) is the infinite trajectory $\mathcal{O} = \langle x, Mx, M^2x, \dots \rangle$.

Within the field of computer science, one of the earliest achievements concerning the analysis of linear dynamical systems is a celebrated result by Kannan and Lipton from the 1980s, the (polynomial-time) decidability of the *Orbit Problem* [15,16]: given (M, x) such a system, together with a point target $y \in \mathbb{Q}^d$, does the orbit of the system ever hit y?

Kannan and Lipton's paper answered an open problem of Harrisson from the 1960s on the reachability for linear sequential machines [14]. However, a secondary motivation was to propose an approach to attack the well-known Skolem Problem, which had itself been famously open since the 1930s (and remains unsolved to this day); phrased in the language of linear dynamical systems, the Skolem Problem asks whether it is decidable, given (M, x) as above, together with a $(d-1)$-dimensional subspace H of $\mathbb{R}^d$, to determine if the orbit of (M, x) ever hits H. This problem is known to be decidable in dimensions $d \leq 4$, and is otherwise open—for a more detailed discussion on the topic, we refer the reader to [28]. Kannan and Lipton suggested that, in ambient space $\mathbb{R}^d$ of arbitrary dimension, the problem of hitting a low-dimensional subspace might be decidable. Indeed, this was eventually substantiated by Chonev *et al.* for linear subspaces of dimension at most 3 [9,10].

Subsequent research focussed on the decidability of hitting targets of increasing complexity, such as half-spaces [12,18,26,25,27], polytopes [30,11,3], and semialgebraic sets [4,5]. Since discrete-time linear dynamical systems can equivalently be viewed as simple deterministic while loops with affine assignments, many of the questions considered above also have immediate bearing on corresponding halting problems for such loops.

In recent years, motivated in part by verification problems for stochastic systems and linear loops, researchers have begun investigating more sophisticated specification formalisms than mere reachability: for example, the paper [1] studies approximate LTL model checking of Markov chains (which themselves can be viewed as particular kinds of linear dynamical systems), whereas [17] focuses on LTL model checking of low-dimensional linear dynamical systems with semi-algebraic

predicates. In [2], the authors investigate the model-checking problem for diagonalisable linear dynamical systems in arbitrary dimension against prefix-independent MSO properties; both are significant restrictions—in particular, reachability queries are *not* prefix independent and therefore do not fall within the scope of the problems considered in [2].

Main contributions. In the present paper, we consider full MSO model checking of discrete-time linear dynamical systems of arbitrary dimension, only placing restrictions on the dimension of our semialgebraic predicates. More precisely, given a linear dynamical system (M, x) in ambient dimension d, together with a finite collection of (not necessarily disjoint) semialgebraic sets $\pi = \{\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_k\}$ (with each $\mathcal{T}_i \subseteq \mathbb{R}^d$), we associate an infinite *characteristic word* $w(\mathcal{O}, \pi)$ over the 2^k-letter alphabet 2^π with the orbit: writing $w(\mathcal{O}, \pi)[n]$ to denote the nth letter of this word, we require that

$$\mathcal{T}_i \in w(\mathcal{O}, \pi)[n] \text{ if and only if } M^n x \in \mathcal{T}_i \,.$$

In other words, $w(\mathcal{O}, \pi)$ keeps track at each discrete time step of the sub-collection of semialgebraic sets that the orbit is currently visiting.

In order to define our specification formalism, we formally associate to each subset $S \subseteq \pi$ of semialgebraic sets a unary predicate P_S, and require that $P_S(n)$ hold if and only if $w(\mathcal{O}, \pi)[n] = S$.

Our main result is as follows: provided that each of the semialgebraic sets in π *either* has intrinsic dimension 1, *or* is contained within some three-dimensional subspace of $\mathbb{R}^d$, the attendant MSO model-checking problem for discrete-time linear dynamical is decidable.[4]

Note that since we have a single starting point, the orbit consists of a single trajectory. The problem we are solving is sometimes referred to in the literature as "path checking", although typical applications in runtime verification and online monitoring involve finite traces, *e.g.*, [19]. Path checking ultimately periodic infinite traces is considered in [20], but the traces arising from linear dynamical systems need not be ultimately periodic (see [1]).

To the best of our knowledge, our model-checking result goes substantially farther than existing work in the literature. Moreover, allowing arbitrary three-dimensional semialgebraic sets (even those contained within a four-dimensional subspace) seems highly problematic; indeed, the decidability of mere reachability of a 3D polytope in four-dimensional ambient space presents formidable mathematical difficulties [11]. However, whether semialgebraic sets of intrinsic dimension 2 could be allowed remains an open question.

Our decidability result rests primarily on the following:

Theorem 1. *[29, Theorem 1] For any effectively almost periodic word w, the MSO theory of $(\mathbb{N}, <)$ expanded with unary predicates that define w is decidable.*

Our approach therefore consists in establishing that the characteristic word associated with the orbit of a linear dynamical system, given our dimensional constraints on the semialgebraic predicates, is always 'effectively almost periodic' (the precise definition is provided later in the paper). In order to achieve this, we make extensive use of spectral techniques, as well tools recently developed in [6] for handling parametric linear dynamical systems.

[4] The result is precisely stated in Theorem 6. The intrinsic dimension of a semialgebraic set is formally defined via cell decomposition; intuitively, one-dimensional semialgebraic sets can be viewed as 'strings' or 'curves'.

2 Preliminaries

2.1 Words

Given a finite alphabet Σ, let Σ^* be the set of finite words over Σ and $\Sigma^{\mathbb{N}}$ be the infinite words. Given a word w, let $w[i]$ be the i'th character in w, indexed from 0, i.e. $w = w[0]w[1]w[2]\cdots$. We say that a non-empty word $u = u_0 \cdots u_j$ *occurs at position* k in w if $w[k]w[k+1]\cdots w[k+j] = u$.

2.2 Monadic Second Order Logic (MSO)

Monadic Second Order Logic (MSO) is the second order logic, where second-order quantification is restricted to quantification over sets. Essentially this is a restriction on second order logic where predicates are unary, not relations. The grammar of a monadic second order specification is as follows[5]:

$\psi := P(i)$	(where $P(i)$ is a predicate on position i of the word)
$\psi := \exists X \subseteq \mathbb{N} : \psi \mid \forall X \subseteq \mathbb{N} : \psi$	(subset quantification)
$\psi := \exists i \in \mathbb{N} : \psi \mid \forall i \in \mathbb{N} : \psi$	(first order quantification)
$\psi := i \in X \mid i \notin X$	(subset membership testing)
$\psi := i < j \mid i = j$	(index comparison)
$\psi := \neg\psi \mid \psi \vee \psi \mid \psi \wedge \psi \mid \psi \implies \psi$	(standard logical operations)
$\psi := i = 0 \mid i = 1 \mid i = 2 \mid \ldots$	(fixed values)

We are interested in model checking words, and here the natural numbers represent positions in the word, and the predicates indicate properties of the character of the word at a particular position, for example, $P_S(i)$ could be defined to indicate whether $w(\mathcal{O}, \pi)[i] = S$.

Example 2. Examples of MSO formulas for model checking LDS:

- Reachability of target $\mathcal{T}_i$: $\exists n : P_{\mathcal{T}_i}(n)$.
- Eventually trapped inside $\mathcal{T}_i$: $\exists n \forall m : m > n \implies P_{\mathcal{T}_i}(m)$.
- Every alternate position is in target $\mathcal{T}_i$: (Here O is the set of odd natural numbers) $\exists O \subseteq \mathbb{N} : 1 \in O \wedge \forall x \in O, \exists y, z : (y \notin O \wedge z \in O \wedge x < y < z \wedge \nexists t : x < t < y \vee y < t < z) \wedge \forall x : x \in O \implies P_{\mathcal{T}_i}(x)$.
- Whenever $\mathcal{T}_i$ is visited $\mathcal{T}_j$ is visited some point later: $\forall n : P_{\mathcal{T}_i}(n) \implies \exists m > n : P_{\mathcal{T}_j}(m)$.
- Any linear temporal logic (LTL) formula over predicates $P_{\mathcal{T}_1}, \ldots, P_{\mathcal{T}_m}$.

Decomposing the predicates Suppose $P_{\mathcal{T}}(i)$ is the predicate to describe the target $\mathcal{T}$ as position i. Suppose a target $\mathcal{T}$ is decomposed further into $\mathcal{T}_1, \ldots, \mathcal{T}_\ell$ and replaced with predicates $P_{\mathcal{T}_1}, \ldots, P_{\mathcal{T}_\ell}$. Then its clear that $P_{\mathcal{T}}(i)$ can also be expressed as $P_{\mathcal{T}_1}(i) \vee \cdots \vee P_{\mathcal{T}_\ell}(i)$. Similarly, where a $\mathcal{T}$ is defined as $\mathcal{T}_1 \cap \mathcal{T}_2$, we can describe $P_{\mathcal{T}}(i) = P_{\mathcal{T}_1}(i) \wedge P_{\mathcal{T}_2}(i)$ in MSO. For these reasons it is equivalent to consider predicates corresponding to individual targets, rather than sets of targets, as indicated in the introduction.

Implicitly, at several points we consider the targets π to be decomposed further into $\tilde{\pi}$, where it is clear targets of π can be expressed in terms of targets of $\tilde{\pi}$ at the MSO level. Hence, it is sufficient to model check $w(\mathcal{O}, \tilde{\pi})$.

[5] some expressions can be expressed by a combination of the others, but are included to make the expressivity clear

2.3 Algebraic numbers and eigenvalues

Our linear dynamical systems are defined using rational matrices, however our techniques rely on the analysis of eigenvalues and the Jordan normal form of a matrix. Given a matrix M, the roots of the characteristic equation $\det(M - \lambda I) = 0$ are the eigenvalues. In particular the eigenvalues of a rational matrix may be algebraic. In general the eigenvalues and the entries of the Jordan normal form are not necessarily rational, but algebraic. The algebraic numbers $\overline{\mathbb{Q}}$ are the complex numbers which can be defined as some root of a univariate polynomial in $\mathbb{Q}[s]$. In particular, the rational numbers are algebraic numbers. For every $\alpha \in \overline{\mathbb{Q}}$ there exists a unique monic univariate polynomial $p_\alpha \in \mathbb{Q}[s]$ of minimum degree for which $p_\alpha(\alpha) = 0$. We call p_α the *minimal polynomial* of α. An algebraic number α is represented as a tuple (p, a, ε), where $p \in \mathbb{Q}[s]$ is its minimal polynomial, $a = a_1 + a_2 i$, with $a_1, a_2 \in \mathbb{Q}$, is an approximation of α, and $\varepsilon \in \mathbb{Q}$ is sufficiently small such that α is the unique root of p within distance ε of a (such ε can be computed by the root-separation bound, due to Mignotte [22]). This is referred to as the *standard* or *canonical representation* of an algebraic number. Given canonical representations of algebraic numbers α and β, one can compute canonical representations of $\alpha + \beta$, $\alpha\beta$, and α/β, all in polynomial time (see e.g., [24, Section 2.4]).

Complex numbers, thus also algebraic numbers can also be represented in polar-representation, i.e. of the form $Ae^{i\theta}$, for $A \in \mathbb{R}_+, \theta \in [0, 2\pi)$. Then the modulus, $|Ae^{i\theta}|$, is A and the argument, $\arg(Ae^{i\theta})$, is θ. We say an angle θ is algebraic if $e^{i\theta}$ is an algebraic number.

2.4 Linear recurrence sequences

An order-k Linear recurrence sequence (LRS) $\langle u_n \rangle_{n \in \mathbb{N}}$ is computed by $u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k}$, for fixed $a_1, \ldots, a_k \in \mathbb{R}$ and initial values $u_1, \ldots, u_k \in \mathbb{R}$. Its characteristic polynomial is $p(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k$, and further the roots of p are called the *characteristic roots* of the LRS. An LRS with characteristic roots $\lambda_1, \ldots, \lambda_t$ can be expressed in closed form $u_n = p_1(n)\lambda_1^n + \cdots + p_t(n)\lambda_t^n$, for polynomials $p_1, \ldots, p_t$ with degrees depending on the multiplicities of the roots and coefficients on the initial values $u_1, \ldots, u_k$.

2.5 Almost periodic words and sets

Definition 3. *An infinite word $w \in \Sigma^{\mathbb{N}}$ over the alphabet Σ is called periodic if there exists $p \in \mathbb{N}$ such that $w[n] = w[n + p]$ for all $n \geq 0$. An infinite word w is eventually periodic if there exists a suffix of w with the same property, that is, $w[n] = w[n + p]$ for all $n \geq N$.*

Eventually periodic words can be represented by a finite directed graph, where each node has exactly one successor and each edge is labelled by a character. However, in some cases we must generalise this notion as follows:

Definition 4. *An infinite word $w \in \Sigma^{\mathbb{N}}$ is* almost periodic *if for any finite word $u \in \Sigma^*$, either u occurs finitely many times in w, or there exists $B_u \in \mathbb{N}$ such that the gap between any two consecutive occurrences of u is at most B_u.*

The word w is effectively almost periodic *if B_u can be computed for any given word u.*

Our goal is to show that the characteristic word is almost periodic. To do this we will represent sets using arcs on circles to represent the almost periodic words that we require.

Definition 5. *A set $\mathcal{Z} \subseteq \mathbb{N}$ is represented by an* arc-hitting model *if there exists an algebraic number λ with $|\lambda| = 1$ but not a root of unity, an open semialgebraic subset $I \subseteq \mathbb{T}$ of the unit*

circle[6]*, $N \in \mathbb{N}$ and a finite set $F \subseteq \{0, \ldots, N-1\}$. Then $n \in \mathcal{Z}$ if and only if either $\lambda^n \in I$ and $n \geq N$, or $n \in F$.*

The indicator word $w \in \{0,1\}^{\mathbb{N}}$ ($w[n] = 1$ if and only if $n \in \mathcal{Z}$) of a set $\mathcal{Z}$ represented by an arc-hitting model is known to be almost periodic [23, Theorem 15]. The arc-hitting model doesn't capture all almost periodic words, but is sufficient for our purposes; for example, because we exclude roots of unity, they do not capture eventually periodic set. Arc-hitting models can also represent finite and cofinite sets (X is cofinite if there exists $N \in \mathbb{N}$ such that $X \cup \{0, \ldots, N\} = \mathbb{N}$)—here $I = \emptyset$ or $\mathbb{T}$ respectively, with F taking care of the finite part.

2.6 The point target case

Let us first observe that if $\mathcal{T}$ is a single point, then $\mathcal{Z}(\mathcal{T})$ is either finite or eventually periodic. In fact, if a point $\mathcal{T}$ is repeated then the whole orbit is eventually periodic, since the dynamics of the system between the two occurrences will repeat indefinitely, and we can revert to model checking an eventually periodic word. Two applications of the Kannan-Lipton orbit problem can detect this case: first ask if (M, x) reaches $\mathcal{T}$ (if not, $\mathcal{Z}(\mathcal{T})$ is empty), and if the first hitting time is n, then ask if $(M, M^{n+1}x)$ hits $\mathcal{T}$, if so the system is eventually periodic and other wise $\mathcal{Z}(\mathcal{T}) = \{n\}$.

Henceforth, we assume the targets are not single points. However, our analysis will show that for some 1D semialgebraic targets, only a finite number of the points from the target can be reached—in which case these targets reduce to a finite union of points.

3 Degeneracy

For the sake of further analysis, we account for degeneracy. A LDS is *degenerate* if there exist two distinct eigenvalues λ_i, λ_j of matrix M such that their quotient λ_i/λ_j is a root of unity.

It is possible to decompose the orbit of degenerate linear dynamical system into subsequences described by non-degenerate systems. We take this approach, and so will need to put the sequences back together again—we do this in Section 6.

We take a short detour towards the Jordan normal form to discuss the eigenvalues of matrix M and its powers. It is well-known that there exists a nonsingular matrix S such that $M = S^{-1}JS$, where $J = \mathrm{diag}(J_1, \ldots, J_t)$ is a block diagonal matrix. Each block of it has the following form:

$$J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}, \tag{1}$$

where $\lambda_1, \ldots, \lambda_t$ are (not necessarily distinct) eigenvalues of M. A block J_i is referred to as a *Jordan block* of λ_i. Matrix J is the *Jordan normal form*, or simply *Jordan form*, of M. Since J is block diagonal, so is any power of it: $J^m = \mathrm{diag}(J_1^m, \ldots, J_t^m)$. As a matter of fact, the diagonal entries of a Jordan block power J_i^m are all λ_i^m. Hence, $\lambda_1^m, \ldots, \lambda_t^m$ are all eigenvalues of J^m. Since $M^m = S^{-1}J^mS$, we conclude that the eigenvalues of M^m are the same as eigenvalues of J^m.

Define the set of all eigenvalue quotients which are roots of unity:

$$\Omega = \{\lambda_i/\lambda_j : \lambda_1, \ldots, \lambda_t \text{ eigenvalues of } M \text{ and } \lambda_i/\lambda_j \text{ is a root of unity}\}.$$

[6] An open semialgebraic subset of the unit circle is a union of intervals. Closed intervals can also be represented, since the end points of intervals can only be hit finitely many times, which can be shifted to the finite set F.

Given a root of unity ω, let order(ω) be the smallest positive integer such that $\omega^{\text{order}(\omega)} = 1$, and let $L = \text{lcm}\{\text{order}(\omega) : \omega \in \Omega\}$. We note that every power of M that is a multiple of L has no degenerate eigenvalues. Moreover, for any fixed positive integer k, the matrix M^{kL} is not only non-degenerate; each of its non-real eigenvalue is not a real multiple of a root of unity. To see that, let λ be an eigenvalue of M such that $\lambda^{kL} = Ae^{i\theta}$, where $A \in \mathbb{R}$ and $e^{i\theta}$ is a root of unity. Since λ^{kL} is non-real, its conjugate $\overline{\lambda^{kL}}$ is an eigenvalue of M^{kL} as well. Then, however, their ratio $\lambda^{kL}/\overline{\lambda^{kL}} = Ae^{i\theta}/Ae^{-i\theta} = e^{2i\theta}$ would be a root of unity, contradicting non-degeneracy. Finally, by setting $L := \text{lcm}\{L, 2\}$, we can assume that all multiples of roots of unity among eigenvalues of M^L are *positive* reals.

We can then consider L subsequences $(M^L)^n M^r x \in \mathcal{T}$, for each $r \in \{0, \ldots, L-1\}$. Notice that each instance uses the same matrix M^L, but the starting points differs.

Our approach is to describe, for every target $\mathcal{T}$ and every $r \in \{0, \ldots, L-1\}$ the set $\mathcal{Z}_r(\mathcal{T})$ of n such that $(M^L)^n M^r x \in \mathcal{T}$. We will show that $\mathcal{Z}_r(\mathcal{T})$ can be represented with arc-hitting models (including possibly because $\mathcal{Z}_r(\mathcal{T})$ is finite or cofinite).

From the sets $\mathcal{Z}_r(\mathcal{T})$, we will be able to reconstruct the characteristic word $w(\mathcal{O}, \pi)$ in an effectively almost periodic way (Theorem 16), and hence apply Theorem 1 to prove our main theorem:

Theorem 6. *Take input a linear dynamical system (M, x), a collection π of semialgebraic targets each of which either has intrinsic dimension at most one or linear dimension at most three, and an MSO formula ψ. Let $w(\mathcal{O}, \pi)$ be the characteristic word. It is decidable whether $w(\mathcal{O}, \pi)$ satisfies ψ.*

Here the *intrinsic dimension* of a semialgebraic set is the usual dimension of a semialgebraic set (see [7] and Subsection A.1). The *linear dimension* of a semialgebraic set S is the dimension of the subspace spanned by the points in S.

Henceforth, when constructing $\mathcal{Z}_r(\mathcal{T})$ in Section 5 and Section 4 we consider only the non-degenerate matrix M^L.

4 Semialgebraic targets contained in 3D subspaces

In this section, we show that given an update matrix M, a starting point x and a semialgebraic target set $\mathcal{T}$ contained inside a 3D subspace, it is possible to partition the orbit $\langle x, Mx, M^2x, \ldots \rangle$ into L subsequences in a way that the time steps each of the L suborbits enters $\mathcal{T}$ can be described using an arc-hitting model. We then use this result in Theorem 16, which shows effective almost-periodicity of infinite words obtained by interleaving words that can be described using arc-hitting models.

Theorem 7. *Let $M \in \mathbb{Q}^{d\times d}$ and $x \in \mathbb{Q}^d$. For every semialgebraic target set $\mathcal{T} \subseteq \mathbb{R}^d$ contained inside a 3D subspace V of $\mathbb{R}^d$, there exists $L > 0$ such that for $0 \le r < L$, $\mathcal{Z}_r(\mathcal{T}) = \{n \in \mathbb{N} : M^{nL+r}x \in \mathcal{T}\} = \{n \in \mathbb{N} : (M^L)^n(M^r x) \in \mathcal{T}\}$ can be described by an arc-hitting model.*

That is, the sequence $(M^n x)_{n\in\mathbb{N}}$ can be written as interleaving of L sequences that can be described using arc-hitting models. Observe that it suffices to prove Theorem 7 for non-degenerate matrices M. To see this, suppose that the theorem holds for non-degenerate systems and let M be an arbitrary matrix and D be such that M^D is non-degenerate. Define sequences $x^0, \ldots, x^{D-1}$, $(x_i^k) = M^{iD+k}x$. Since M^D is non-degenerate, each x^i can be written as an interleaving of L_i sequences described by arc-hitting models. Observing that if a sequence can be described using L_i arc-hitting models, then it can be described using L_i' arc-hitting models for every multiple L_i' of L_i, we can take the least common multiple of $L_0, \ldots, L_{D-1}$ and assume that $L_i = L_j = L'$ for every i, j. Next, define $L = L'D$ and consider the subsequences $y^0, \ldots, y^{L-1}$,where $y_i^k = M^{iL+k}x$.

We have to construct an arc-hitting model for each y^i. Wlog consider y^0. Observe that y^0 is a subsequence of x^0: in fact, $y^0_i = x^0_{iL'}$ for $i \geq 0$. By assumption, x^0 can be described (more precisely, the set $\{n \in \mathbb{N} : x^0_n \in \mathcal{T}\}$ can be described) using an arc-hitting model with parameters N, λ, I. Then y^0 can be described by the "L'-times accelerated" arc-hitting model with parameters NL', $\lambda^{L'}$ and I.

To prove Theorem 7, we begin by investigating $\mathcal{Z}(V)$ where V is a subspace.

Theorem 8. *Let V be a subspace of $\mathbb{R}^d$ and (M, x) a linear dynamical system. Then $\mathcal{Z}(V)$ is semilinear, that is, of the form $F \cup \bigcup_{i=1}^{s}(r_i + N\mathbb{N})$ for finite F and arithmetic progressions $r_i + N\mathbb{N}$ for $1 \leq i \leq s$.*

Proof. If $V = \mathbb{R}^d$, then $\mathcal{Z}(V) = \mathbb{N}$, which is semilinear. Otherwise, V can be written as an intersection $V_1 \cap \ldots \cap V_m$ of m hyperplanes of dimension $d-1$. By the Skolem-Mahler-Lech Theorem [13], $\mathcal{Z}(V_i)$ is semilinear for each i, and intersection of semilinear sets remains semilinear. □

Skolem-Mahler-Lech Theorem, however, is not constructive in the sense that it does not give us a way to construct the semilinear sets $\mathcal{Z}(V_1), \ldots, \mathcal{Z}(V_m)$. In fact, the famously open Skolem Problem boils down to deciding whether the finite set F is empty. We first show that it is possible to write down the set $\mathcal{Z}(V)$ if $\dim(V) \leq 3$. To do this later in Theorem 11, we will need the following lemmata. First, Lemma 9 which combines the results of [10, Lemmata G.1, G.3-G.4]:

Lemma 9. *Let $(u_i)_{i\in\mathbb{N}}$ be a non-zero non-degenerate LRS of order at most 4. If*

1. $u_n = A\lambda_1^n + \overline{A\lambda_1^n} + B\lambda_2^n + \overline{B\lambda_2^n}$, *or*
2. $u_n = (A + Bn)\lambda_1^n + (\overline{A} + \overline{B}n)\overline{\lambda_1^n}$

for $A, B, \lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$, then there exists a computable bound N on the zeros of $(u_i)_{i\in\mathbb{N}}$.

Lemma 10. *Let $\lambda, c \in \overline{\mathbb{Q}}$ with $|\lambda| = 1$, λ not a root of unity and $B \in \mathbb{R} \cap \overline{\mathbb{Q}}$. There exist computable values $D, N > 0$ such that for all $n > N$, $|c\lambda^n + \overline{c\lambda^n} + B| > \frac{1}{n^D}$.*

Proof. It suffices to only consider the case where $|c| = 1$, as one can show that D, N satisfy the statement of the lemma for λ, c, B if and only if D', N satisfies the statement of the lemma for $\lambda, \frac{c}{|c|}, B$ where $D' > 0$ is sufficiently large with respect to $|c|$.

Since $c\lambda^n + \overline{c\lambda^n}$ takes values in $[-2, 2]$, if $|B| > 2$, then $|c\lambda^n + \overline{c\lambda^n} + B| = \Omega(1)$ and the conclusion follows immediately. Henceforth we assume that $B \in [-2, 2]$.

Define $f(z) = |z + \overline{z} + B| = |2\operatorname{Re}(z) + B|$. Then $|c\lambda^n + \overline{c\lambda^n} + B| = f(c\lambda^n)$.

Given the restriction $B \in [-2, 2]$, $f(z)$ will have exactly two conjugate zeroes in the unit circle $\mathbb{T}$, which we denote with w and $\overline{w}$. Using [25, Corollary 8] we can compute D, N such that for all $n > N$, $|c\lambda^n - w|, |c\lambda^n - \overline{w}| > \frac{1}{n^D}$. We show that this implies that for all $n > N$, $|f(c\lambda^n)| > \frac{1}{n^D}$. We begin by writing

$$|f(c\lambda^n)| = |f(c\lambda^n) - f(w)| = |c\lambda^n + \overline{c\lambda^n} - w - \overline{w}| = 2|\operatorname{Re}(c\lambda^n) - \operatorname{Re}(w)|.$$

Recall that for all $n > N$, $|c\lambda^n - w|, |c\lambda^n - \overline{w}| > \frac{1}{n^D}$. This implies that all $n > N$, $|\arg(c\lambda^n) - \arg(w)|, |\arg(c\lambda^n) - \arg(\overline{w})| > \frac{1}{n^D}$. By considering the geometry of the unit circle, we hence obtain that for all $n > N$,

$$2|\operatorname{Re}(c\lambda^n) - \operatorname{Re}(w)| > 2|(1 - \cos\frac{1}{n^D})| = 2\sin\frac{1}{n^D} > \frac{1}{n^D}.$$ □

We are now ready to analyse $\mathcal{Z}(V)$ where V is a linear subspace of dimension at most three.

Theorem 11. *Let V be a linear subspace of $\mathbb{R}^d$ with $\dim V \leq 3$, and (M, x) a non-degenerate linear dynamical system with $M \in \mathbb{Q}^{d\times d}$ and $x \in \mathbb{Q}^d$. Either*

- *$\mathcal{Z}(V) = \mathbb{N}$, or*
- *$\mathcal{Z}(V)$ is finite with an effectively computable upper bound N on the elements of $\mathcal{Z}(V)$.*

Proof. Observe that whether $\mathcal{Z}(V) = \mathbb{N}$ can be determined by simply checking whether the first three elements x, Mx, M^2x of the orbit are in V. Otherwise, we show how to compute the bound N on $\mathcal{Z}(V)$.

In this proof we exploit the *real* Jordan normal form to streamline the arguments. Let $\lambda_1, \ldots, \lambda_k$ be the real eigenvalues of M, while $\lambda_{k+1}, \ldots, \lambda_s$ are complex and grouped into conjugate pairs. The real Jordan normal form, or real Jordan form, is a block diagonal matrix as in the definition given in Section 3. A *real Jordan block* R_i corresponding to $\lambda_i, i = 1, \ldots, k$ is defined as in (1), whereas the Jordan blocks $J_1, \ldots, J_\ell$ of complex eigenvalues are redefined. Every *complex Jordan block* of the form J_j corresponds to a pair of conjugate complex eigenvalues $\lambda_j = a_j + b_j i$, $\overline{\lambda_j} = a_j - b_j i$ and has the following form:

$$J_j = \begin{bmatrix} \Lambda_j & I & & \\ & \Lambda_j & \ddots & \\ & & \ddots & I \\ & & & \Lambda_j \end{bmatrix}, \ \Lambda_j = \begin{bmatrix} a_j & -b_j \\ b_j & a_j \end{bmatrix}$$

for $1 \leq j \leq l$, where $a_j, b_j \in \mathbb{R} \cap \overline{\mathbb{Q}}$. The benefit of working with the real Jordan form $J = \operatorname{diag}(R_1, \ldots, R_k, J_1, \ldots, J_\ell)$ is that all matrices involved are over $\mathbb{R} \cap \overline{\mathbb{Q}}$ rather than $\overline{\mathbb{Q}}$.

We can assume that M is in real Jordan form since any problem instance can be translated to real Jordan form by observing that for any S, J such that $M = S^{-1}JS$, $M^n x \in V$ if and only if $J^n(Sx) \in S(V)$ where $S(V)$ is the image of V under the coordinate transform S with $\dim S(V) = \dim V$. It will also be convenient to assume that for $1 \leq i \leq k$, the entry of x that corresponds to the bottom coordinate (row) of R_i is non-zero, and for $1 \leq j \leq l$, the two coordinates of x that correspond to the bottom two rows of J_j are not both zero. Any given instance with M, x and V can be transformed into this form by removing equations corresponding to certain coordinates that are always zero and modifying V accordingly. For example, suppose $M = \begin{bmatrix} \Lambda & I & 0 \\ 0 & \Lambda & I \\ 0 & 0 & \Lambda \end{bmatrix} \in \mathbb{R}^{6\times 6}$ and $x = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & 0 & 0 \end{bmatrix}^\top \in \mathbb{R}^6$. Then $M^n x \in V$ if and only if $\begin{bmatrix} \Lambda & I \\ 0 & \Lambda \end{bmatrix}^n \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \end{bmatrix}^\top \in W$, where $W = \{v \in \mathbb{R}^4 : (v, 0, 0) \in V\}$. In particular, $\dim(W) \leq \dim V$.

Next we show how to compute the bound N on $\mathcal{Z}(V)$ by a case analysis on the structure of J.

Case I. Suppose M has four distinct non-real eigenvalues, i.e. there exist blocks J_i and J_j with eigenvalues $\lambda_i, \overline{\lambda_i}, \lambda_j, \overline{\lambda_j}$ and $\Lambda_i \neq \Lambda_j$. We denote the entries of x corresponding to the bottom two rows of J_i and J_j by x_1, x_2 and x_3, x_4 respectively, with $(x_1, x_2) \neq \mathbf{0}$ and $(x_3, x_4) \neq \mathbf{0}$. Let W be the projection of V onto the coordinates that correspond to $x_1, \ldots, x_4$ and $H = \{x \in \mathbb{R}^4 : c^\top x = 0\}$, $c^\top = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 \end{bmatrix} \neq \mathbf{0}$ a hyperplane that contains W; such H must exist as $\dim W \leq 3$. We have

$$M^n x \in V \implies \begin{bmatrix} a_i & -b_i & 0 & 0 \\ b_i & a_i & 0 & 0 \\ 0 & 0 & a_j & -b_j \\ 0 & 0 & b_j & a_j \end{bmatrix}^n \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \in W \implies \begin{bmatrix} c_1 & c_2 & c_3 & c_4 \end{bmatrix} \begin{bmatrix} a_i & -b_i & 0 & 0 \\ b_i & a_i & 0 & 0 \\ 0 & 0 & a_j & -b_j \\ 0 & 0 & b_j & a_j \end{bmatrix}^n \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0.$$

By analysing the powers of Λ_i and Λ_j, the rightmost condition can be written as

$$A\lambda_i^n + \overline{A\lambda_i^n} + B\lambda_j^n + \overline{B\lambda_j^n} = 0$$

where $\lambda_i = a_i + b_i i$, $\lambda_j = a_j + b_j i$, $A = c_1(x_1 - x_2 i) + c_2(x_1 i + x_2)$ and $B = c_3(x_3 - x_4 i) + c_4(x_3 i + x_4)$. Since all the variables are real-valued, $c \neq \mathbf{0}$, and at least one of (x_1, x_2) and (x_3, x_4) is not equal to $\mathbf{0}$, A and B both cannot be zero. Hence $u_n = A\lambda_i^n + \overline{A\lambda_i^n} + B\lambda_j^n + \overline{B\lambda_j^n}$ is a real-valued, non-degenerate linear recurrence sequence, and by Lemma 9, it has finitely many zeros with a computable bound N such that $u_n \neq 0$ for $n > N$. Going back to (M, x) and V, we can conclude that $\mathcal{Z}(V)$ is also bounded by N.

Case II. There exists a a block J_j with multiplicity at least 2 (i.e. with at least 4 rows). Similarly to the preceding case, considering only the four coordinates corresponding to the bottom four rows of J_j, define x_1, x_2, x_3, x_4 and project V onto the 4 relevant coordinates to obtain W. Let $H = \{x \in \mathbb{R}^4 : c^\top x = 0\}$, $c \neq \mathbf{0}$ be a hyperplane that contains W. We have

$$M^n x \in V \implies \begin{bmatrix} a_i & -b_i & 1 & 0 \\ b_i & a_i & 0 & 1 \\ 0 & 0 & a_i & -b_i \\ 0 & 0 & b_i & a_i \end{bmatrix}^n \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \in W \implies \begin{bmatrix} c_1 & c_2 & c_3 & c_4 \end{bmatrix} \begin{bmatrix} a_i & -b_i & 1 & 0 \\ b_i & a_i & 0 & 1 \\ 0 & 0 & a_i & -b_i \\ 0 & 0 & b_i & a_i \end{bmatrix}^n \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0.$$

The last equation can be written as

$$C(n)\lambda_i^n + \overline{C(n)\lambda_i^n} = 0 \tag{2}$$

where $\lambda_i = a_i + b_i i$ and

$$C(n) = c_1(x_1 + x_2 i) + c_2(x_1 i + x_2) + c_3(x_3 + x_4 i) + c_4(x_3 i + x_4) + \frac{c_1(x_3 + i x_4) + c_2(-x_3 i + x_4)}{\lambda_i} n.$$

Recalling that x_3, x_4 are not both zero and that all variables are real-valued, we observe that $c_1(x_3 + i x_4) + c_2(-x_3 i + x_4) \neq 0$ and conclude that $C(n)$ is not identically zero. We can therefore write Equation 2 as $(A + Bn)\lambda_i^n + (\overline{A} + \overline{B}n)\overline{\lambda_i^n} = 0$, $A, B \in \overline{\mathbb{Q}}$, which by Lemma 9, has a computable upper bound on the solutions in n.

Case III. $J_i = \Lambda = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for every i. In this case, M has at most one pair of non-real eigenvalues, $\lambda = a + bi$ and $\overline{\lambda} = a - bi$, and all blocks with non-real eigenvalues have multiplicity 1. We show that for every hyperplane $H = \{x \in \mathbb{R}^d : c^\top x = 0\}$, $c \neq \mathbf{0}$, $\mathcal{Z}(H)$ is finite and can be effectively bounded. Hence either $V = \mathbb{R}^d$, in which case $\mathcal{Z}(V) = \mathbb{N}$, or V is contained in a hyperplane H and $\mathcal{Z}(V) \subset \mathcal{Z}(H)$ can be effectively bounded.

By considering powers of Λ and the blocks $R_1, \ldots, R_k$,

$$c^\top M^n x = C\lambda^n + \overline{C\lambda^n} + \sum_{i=1}^{k} p_i(n)\rho_i^n$$

where $C \in \overline{\mathbb{Q}}$, $\rho_1, \ldots, \rho_k$ are the real eigenvalues of M with $\rho_1 > \cdots > \rho_k > 0$ (recall that from Section 3 we can assume that all real eigenvalues are positive and distinct), and $p_i(n)$ are polynomials with non-zero real algebraic coefficients for $1 \leq i \leq k$.

Let $\sigma = \max\{|\lambda|, \rho_1\}$ be the spectral radius of M, $\gamma = \frac{\lambda}{\sigma}$ and $\delta_i = \frac{\rho_i}{\sigma}$ for $1 \leq i \leq k$. Observe that either $|\gamma| = 1$, or $\delta_1 = 1$ and $|\gamma|, \delta_2, \ldots, \delta_k < 1$. Define

$$v_n = \frac{c^\top M^n x}{\sigma^n} = C\gamma^n + \overline{C\gamma^n} + \sum_{i=1}^{k} p_i(n)\delta_i^n.$$

We have that $M^n x \in H \iff c^\top M^n x = 0 \iff v_n = 0$. Hence it suffices to show that the set of all zeros of v_n can be effectively bounded.

- If $|\gamma| < 1$ (in which case, $\delta_1 = 1$), then $|p_1(n)\delta_1^n| = \Omega(1)$, whereas $|C\gamma^n + \overline{C\gamma^n}|$ and $|\sum_{i=2}^{k} p_i(n)\delta_i^n|$ decrease exponentially to 0. Hence we can compute N such that for all $n > N$, $|p_1(n)\delta_1^n| > |C\gamma^n + \overline{C\gamma^n} + \sum_{i=2}^{k} p_i(n)\delta_i^n|$ and hence $v_n \neq 0$.
- Similarly, if $\delta_1 < 1$ (in which case, $|\lambda| = 1$), then $|\sum_{i=1}^{k} p_i(n)\delta_i^n|$ decreases exponentially to 0 with n, whereas by Lemma 10 we can compute a constant D and a bound N such that for all $n > N$, $|C\gamma^n + \overline{C\gamma^n}| > \frac{1}{n^D}$. Hence we can compute a bound N' such that for all $n > N'$, $|C\gamma^n + \overline{C\gamma^n}| > \frac{1}{n^D} > \left|\sum_{i=1}^{k} p_i(n)\right|$ and hence $v_n \neq 0$.
- If $\delta_1 = |\gamma| = 1$ and $p_1(n)$ is not constant, then $|p_1(n)\delta_1^n|$ goes to infinity with n, whereas $|C\gamma^n + \overline{C\gamma^n}|$ is bounded by a constant and $|\sum_{i=2}^{k} p_i(n)\delta_i^n|$ decreases exponentially. Hence we can compute N such that for all $n > N$, $|p_1(n)\delta_1^n| > |C\gamma^n + \overline{C\gamma^n} + \sum_{i=2}^{k} p_i(n)\delta_i^n|$ and hence $v_n \neq 0$.
- If $\delta_1 = |\gamma| = 1$ and $p_1(n) = B$ is constant, then by Lemma 10 we can compute a constant D and a bound N such that for all $n > N$, $|C\gamma^n + \overline{C\gamma^n} + B| > \frac{1}{n^D}$. Hence we deduce that for all $n > N$, $|C\gamma^n + \overline{C\gamma^n} + p_1(n)\delta_1^n| = |C\gamma^n + \overline{C\gamma^n} + B| > \frac{1}{n^D}$. Since $|\sum_{i=2}^{k} p_i(n)\delta_i^n|$ decreases exponentially to 0, we can then compute a bound $N' > N$ such that for all $n > N'$, $|C\gamma^n + \overline{C\gamma^n} + p_1(n)\delta_1^n| > \frac{1}{n^D} > \left|\sum_{i=2}^{k} p_i(n)\right|$ and hence $v_n \neq 0$. □

The preceding theorem describes $\mathcal{Z}(V)$ for a 3D subspace V. Recall that we are interested in understanding $\mathcal{Z}(\mathcal{T})$ for $\mathcal{T}$ contained inside such a subspace. To this end, we will combine Theorem 11 with the following result about three-dimensional dynamical systems from [17].

Lemma 12. *Let $\mathcal{T} \subseteq \mathbb{R}^3$ be a semialgebraic set in three dimensions and (M, x) a non-degenerate dynamical system with $M \in \overline{\mathbb{Q}}^{3\times 3}$ and $x \in \overline{\mathbb{Q}}^3$. $\mathcal{Z}(\mathcal{T})$ can be described by an arc-hitting model.*

Proof. Let $p : \mathbb{R}^3 \to \mathbb{R}$ be a polynomial in three variables. Our approach is to show that

- the set $\{n : p(M^n x) = 0\}$ is either finite or equal to $\mathbb{N}$, and
- the sets $\{n : p(M^n x) > 0\}$ and $\{n : p(M^n x) > 0\}$ are either finite or cofinite.

This suffices because as the semialgebraic set $\mathcal{T}$ is defined as a Boolean combination of sets of the form $\mathcal{T}_1, \ldots, \mathcal{T}_k$, where for $1 \leq i \leq k$, $\mathcal{T}_i = \{(x_1, x_2, x_3) : p_i(x_1, x_2, x_3) \sim_i 0\}$ and $\sim_i \in \{<, =, >\}$. Hence $\mathcal{Z}(\mathcal{T})$ is a Boolean combination of $\mathcal{Z}(\mathcal{T}_1), \ldots, \mathcal{Z}(\mathcal{T}_k)$, which are either finite or cofinite. It remains to observe that a Boolean combination of sets that are finite or cofinite is itself finite or cofinite. Finally, both finite and cofinite sets can be represented as arc-hitting models.

First consider the case where M has only real eigenvalues $\rho_1, \rho_2, \rho_3 \in \mathbb{R}$ and let $J = SMS^{-1}$ be the Jordan form of M. Let $x_1(n), x_2(n), x_3(n)$ denote the three coordinates of $M^n x$. By analysing the powers $M^n x = S^{-1}J^n S x$, we can observe that for $1 \leq i \leq 3$, $x_i(n)$ is of the form

$$\sum_{j=1}^{3} q_j(n)\rho_j^n$$

where for $1 \leq j \leq 3$, q_j is a polynomial with real algebraic coefficients. Since $p(M^n x)$ is obtained from $x_1(n), x_2(n), x_3(n)$ through multiplication and addition, $p(M^n x)$ will be of the form

$$\sum_{i,j,k<K} q_{i,j,k}(n)\rho_1^n \rho_2^n \rho_3^n = \sum_{i,j,k<K} q_{i,j,k}(n)\rho_{i,j,k}^n.$$

The expression above is either identically zero, ultimately positive or ultimately negative.

Now suppose M has a complex eigenvalue λ. [17, Section 4] shows, again by writing M in Jordan form and considering powers of M, that there exists a computable N such that for all $n > N$,

$$\text{sign}(p(M^n x)) = \text{sign}\left(\sum_{m=0}^{K} \beta_m \gamma^{nm} + \overline{\beta_m \gamma^{nm}} + r(n)\right)$$

where $\gamma = \frac{\lambda}{|\lambda|}$, $\beta_m \in \overline{\mathbb{Q}}$ for all m and $r(n)$ decreases exponentially to 0 as $n \to \infty$. From this one can deduce that either $\text{sign}(p(M^n x))$ is always 0 (in case $\beta_m = 0$ for all m), or [17, Theorem 5] that there exist a computable open subsets $I_>$ and $I_<$ of $\mathbb{T}$ (that are finite unions of open intervals) such that for all $n > N$, $p(M^n x) \neq 0$ and $p(M^n x) \sim 0$ if and only if $\gamma^n \in I_\sim$. This gives us arc-hitting models with parameters N, γ and $I_>$ or $I_<$. □

Proof of Theorem 7. Recall that it suffices to prove Theorem 7 for non-degenerate M. Let $M \in \mathbb{Q}^{d\times d}$, $x \in \mathbb{Q}^d$, V be a 3D subspace of $\mathbb{R}^d$ and $\mathcal{T} \subseteq V$ a semialgebraic target. Consider $\mathcal{Z}(V)$. By Theorem 11, there are two possibilities. If $\mathcal{Z}(V)$ is finite with an effectively computable upper bound, then so is $\mathcal{Z}(\mathcal{T})$ and we can describe $\mathcal{Z}(\mathcal{T})$ using a single arc-hitting model (i.e. $L = 1$).

Now suppose $\mathcal{Z}(V) = \mathbb{N}$, i.e. the orbit of (M, x) always remains inside V. In this case, we essentially have a three-dimensional dynamical system. More formally, let $D \leq 3$ be the maximal number of independent vectors in $\{x, Mx, M^2x\}$. We can then define a D-dimensional dynamical system (M_p, x_p) and a semialgebraic set $\mathcal{T}_p \subseteq \mathbb{R}^D$ such that $M^n x \in \mathcal{T} \iff M_p^n x_p \in \mathcal{T}_p$. For example, if $D = 3$, then we use $\{x, Mx, M^2x\}$ as a basis for $\mathbb{R}^3$ and write $x_p = \begin{bmatrix}1 & 0 & 0\end{bmatrix}$, $M_p = \begin{bmatrix}Mx \mid M^2x \mid M^3x\end{bmatrix}$ and $\mathcal{T}_p = \{(a, b, c) : ax + bMx + cM^2x \in \mathcal{T}\}$. But now observe that we can characterize the set of all n such that $M_p^n x_p \in \mathcal{T}_p$ using Lemma 12. Let L be such that M_p^L is non-degenerate. Then, by Lemma 12, we have that $\mathcal{Z}_r(\mathcal{T}_p)$ (and hence $\mathcal{Z}_r(\mathcal{T})$) can be described by an arc-hitting model for $0 \leq r < L$. □

5 1D semialgebraic targets

In this section we consider semialgebraic target sets that have (intrinsic) dimension 1 but need not stay within a 3D subspace of $\mathbb{R}^d$. Such sets are essentially finite unions of curves, and in Appendix A.1 we argue that a 1D semialgebraic target $\mathcal{T}$ can be represented as union $\mathcal{T} = \bigcup_{i=1}^{\ell} \{v_i(s) : s \in \mathbb{R}\}$ of sets parametrized by an algebraic function of a single variable.

Let M be an update matrix, $L > 0$ such that M^L is non-degenerate, x a starting point and $\mathcal{T}$ a semialgebraic target of dimension 1. Similarly to the main theorem of Section 4, we will show that for $0 \leq r < L$, $\mathcal{Z}_r(\mathcal{T}) = \{n \in \mathbb{N} : M^{nL+r}x \in \mathcal{T}\}$ can be described by an arc-hitting model. We extend the work of [6], which (implicitly) showed whether $\mathcal{Z}(\mathcal{T})$ is empty or not, by fully characterising the set using arc-hitting models:

Theorem 13. *Given a non-degenerate $(M, \tilde{x})$ and a semialgebraic target $\mathcal{T}$ of dimension 1, the set $\mathcal{Z}(\mathcal{T})$ can be effectively represented with arc-hitting models.*

Now assuming non-degenerate matrices, we further observe that we can assume the problem to be given in Jordan form, as defined in Section 3. Suppose $M = S^{-1}JS$ with J in Jordan form and that $\mathcal{T} = \{v(s) : s \in \mathbb{R}\}$. Then $M^n x \in \mathcal{T} \iff J^n(Sx) = Sv(s)$ for some s. Let $\tilde{x} = Sx$ and $\tilde{v}(s) = Sv(s)$. Here $\tilde{v}(s)$ is a linear transformation on $v(s)$ and so remains an algebraic function. Notice that the entries of $J, \tilde{x}$ and $\tilde{v}$ may be complex due to J being the complex Jordan form. The following section proves Theorem 13 with the translation to JNF in mind.

5.1 Non-diagonalisable

Let $J = (J_1, \ldots, J_t)$ be the Jordan form of the non-degenerate matrix, where J_i is a Jordan block of dimension d_i corresponding to an eigenvalue λ_i. We index $\tilde{x}$ by $\tilde{x}_{i,1}, \ldots, \tilde{x}_{i,d_i}$ for the coordinates corresponding to J_i (where $\tilde{x}_{i,1}$ corresponds to the bottom row), similarly for $\tilde{v}(s)$. For example:

$$J = \begin{bmatrix} J_1 & & \\ & J_2 & \\ & & J_3 \end{bmatrix} \quad \tilde{x} = \begin{bmatrix} \tilde{x}_{1,1} \\ \tilde{x}_{2,d_2} \\ \vdots \\ \tilde{x}_{2,1} \\ \tilde{x}_{3,d_3} \\ \tilde{x}_{3,1} \end{bmatrix} \quad \tilde{v}(s) = \begin{bmatrix} \tilde{v}_{1,1}(s) \\ \tilde{v}_{2,d_2}(s) \\ \vdots \\ \tilde{v}_{2,1}(s) \\ \tilde{v}_{3,d_3}(s) \\ \tilde{v}_{3,1}(s) \end{bmatrix}$$

Lemma 14. *Given non-degenerate J, if there exists a non-diagonal Jordan block J_i with eigenvalue λ_i, then $\mathcal{Z}(\mathcal{T})$ is effectively finite or cofinite.*

Proof. Recall, either λ_i is not a root of unity or $\lambda_i = 1$.

If λ_i is not a root of unity, we can apply [6, Lemma 18] which shows there is an effective bound on n for which $\lambda_i^n \tilde{x}_{i,1} = \tilde{v}_{i,1}(s)$ and $\lambda_i^n \tilde{x}_{i,2} + n\lambda_i^{n-1} \tilde{x}_{i,1} = \tilde{v}_{i,2}(s)$ can both hold. This entails that $\mathcal{Z}(\mathcal{T})$ is finite.

Now let us turn to the case when $\lambda_i = 1$, we will still conclude $\mathcal{Z}(\mathcal{T})$ is finite or cofinite. We consider polynomial equations in variable n, formed by $J_i^n \tilde{x}_i = \tilde{v}_i(s)$, for all Jordan blocks with $\lambda_i = 1$. For J_i, this leads to constraints on (n, s) in the following form:

$$\tilde{x}_{i,1} = \tilde{v}_{i,1}(s), \quad n\tilde{x}_{i,1} + \tilde{x}_{i,2} = \tilde{v}_{i,2}(s), \quad \ldots, \quad \sum_{j=1}^{d_i} \binom{n}{d_i - j} \tilde{x}_{i,j} = \tilde{v}_{i,d_i}(s).$$

Equations which do not depend on n, for example $\tilde{v}_{i,1} = \tilde{x}_{i,1}(s)$ must either hold for all s, or there are finitely many choices of s (reducing the problem to single point targets).

For the remaining equations, there is an equation of the form $n = (\tilde{v}_{i,2}(s) - \tilde{x}_s)/\tilde{x}_{i,1}$, which can be used to replace n in all other equations. Again we test whether the constraint system is satisfied for all s or only finitely many s (in which case we again reduce to single point targets).

If the constraints hold for all s, we have the equation $n = (\tilde{v}_{i,2}(s) - \tilde{x}_s)/\tilde{x}_{i,1}$. If the range $\{(\tilde{v}_{i,2}(s) - \tilde{x}_s)/\tilde{x}_{i,1} \mid s \in R\}$ is bounded then we conclude that $\mathcal{Z}(\mathcal{T})$ is finite.

Finally we take an equation of the form $\lambda_j^n \tilde{x}_{j,1} = \tilde{v}_{j,1}(s)$ from some Jordan block with eigenvalue different from 1 (if it exists) and can again apply [6, Lemma 18] to bound n such that $\lambda_j^n \tilde{x}_{j,1} = \tilde{v}_{j,1}(s)$ and $n = (\tilde{v}_{i,2}(s) - \tilde{x}_s)/\tilde{x}_{i,1}$ both hold, concluding that $\mathcal{Z}(\mathcal{T})$ is finite. If no such equation exists (because all Jordan blocks have eigenvalue 1) then n is unbounded, and $\mathcal{Z}(\mathcal{T})$ is cofinite. □

5.2 Diagonalisable

In the remainder, we complete the proof of Theorem 13 when the matrix is diagonalisable, and so we have constraints of the form $\lambda_i^n \tilde{x}_i = \tilde{v}(s)_i$, $i = 1, \ldots, t$. Henceforth, we rewrite this as $\lambda_i^n = \gamma_i(s)$, where $\gamma_i(s) = \tilde{v}(s)_i/\tilde{x}_i$. In order to do this, we must assume that $\tilde{x}_i \neq 0$. Observe that if $\tilde{x}_i = 0$ (or indeed $\lambda_i = 0$), then the constraint can be dropped: either all n satisfy the constraint if there exists $s : \tilde{v}(s)_i = 0$, or otherwise no n satisfy the constraint and $\mathcal{Z}(\mathcal{T})$ is empty.

Eigenvalues can either be real or complex. We recall, due to our non-degeneracy assumption, that no complex eigenvalue has rational argument (that is a rational multiple of 2π). That is there are no real multiples of roots of unity, except the positive reals.

Hence, if any eigenvalues λ_i is a root of unity then $\lambda_i = 1$, forming the constraint $1^n = 1 = \gamma_i(s)$, this holds either at finitely many s (reducing $\mathcal{T}$ to point targets), or $\gamma_i(s) = 1$ identically in which case the constraint holds for all n. Thus we may assume that no λ_i is a root of unity.

In the remainder of this section, we assume that no eigenvalue $\lambda_1, \ldots, \lambda_t$ is 0 or 1 by removing such equations as described above.

We split our case analysis depending on whether there exist two *multiplicatively independent* eigenvalues, that is, whether there exists i, j such that $\lambda_i^a \neq \lambda_j^b$ for all $a, b \in \mathbb{Z}$ not both zero.[7] Indeed, if there are two multiplicatively independent eigenvalues, then the following lemma of [6] entails that $\mathcal{Z}(\mathcal{T})$ is finite.

Lemma 15 ([6, Lemma 20]). *Suppose λ_1, λ_2 are constant, not roots of unity, and are multiplicatively independent. Assume further that γ_1, γ_2 are non-constant algebraic functions. Then the system $\lambda_1^n = \gamma_1(s)$, $\lambda_2^n = \gamma_2(s)$ has only finitely many solutions, and there is an effectively computable upper bound on such n.*

It remains that all pairs of eigenvalues are multiplicatively dependent. In particular, for each pair λ_i, λ_j, we have $\lambda_i^{a_2} = \lambda_j^{a_1}$ for some integers a_1, a_2 not both zero. In fact, since we assume that no eigenvalue of interest is a root of unity, we have that neither a_1 nor a_2 equals 0.

We observe that we cannot have both reals and complex numbers because we have eliminated the case where λ_i's may be (real multiples of) roots of unity. Suppose λ_i is complex and λ_j is real, but then $\lambda_i^{a_1} = \lambda_j^{a_2}$ implies $\lambda_i^{a_1}$ is real (thus λ_i is a (real multiple of a) root of unity).

Secondly observe that complex λ_i's have modulus 1. Suppose we have complex λ_i, then since M is real we also have the complex conjugate $\lambda_j = \overline{\lambda_i}$. As λ_i and $\overline{\lambda_i}$ are multiplicatively dependent, we have $\lambda_i^{a_1} = \overline{\lambda_i^{a_2}}$ for $a_1, a_2 \neq 0$. Then $\lambda_i^{a_1+a_2} = \lambda_i^{a_2}\overline{\lambda_i^{a_2}} = (|\lambda_i|^2)^{a_2}$. Hence either $|\lambda| = 1$ or $a_1 = a_2$. However if $a_1 = a_2$ then $\lambda_i^{a_1} = \overline{\lambda_i^{a_1}}$ is real and so λ_i is a (real multiple of a) root of unity, which we have already excluded.

All real First we suppose $\lambda_i's$ are all real; as mentioned in Section 3 we may further assume that all λ_i's are positive real. We will show that $\mathcal{Z}(\mathcal{T})$ is either finite or cofinite.

We have for any two eigenvalues $\lambda_i^{a_i} = \lambda_j^{a_j}$ and require $\lambda_i^n = \gamma_i(s)$ and $\lambda_j^n = \gamma_j(s)$. Since we require that $\lambda_i = \lambda_j^{a_j/a_i}$, we have $\gamma_i(s) = \lambda_i^n = (\lambda_j^{a_j/a_i})^n = (\lambda_j^n)^{a_j/a_i} = \gamma_j(s)^{a_j/a_i}$. We either have $\gamma_i(s) = \gamma_j(s)^{a_j/a_i}$ holds identically, in which case we can drop one of the equations, or there are finitely many such s. In which case this reduces to the single point target problem. Hence we only need to worry about a single equation, let us assume this is $\lambda_i^n = \gamma(s)$.

Further since $\gamma(s)$ only crosses 0 finitely many times, some can partition $\mathcal{T}$ by splitting into regions of R where $\gamma(s)$ is of constant sign. We have $\mathcal{Z}(\mathcal{T}) = \emptyset$ whenever $\lambda_i > 0$ and $\gamma(s) \leq 0$, so we assume $\gamma(s) > 0$.

Hence we solve $\lambda^n = \gamma(s)$ for $\lambda, \gamma > 0$. Now, suppose $\lambda = 1$, either we have $\gamma = 1$, in which case $\mathcal{Z}(\mathcal{T}) = \mathbb{N}$. Or $\gamma(s) = 1$ for finitely many s, in which case we partition $\mathcal{T}$ into finitely many point targets.

The case where $\lambda > 1$ reduces to $\lambda < 1$ by taking $\frac{1}{\lambda}$. Thus $\lambda < 1$. Then if $\inf_{s\in R} \gamma(s) > 0$, we have $\lambda^n < \inf$ for some n and so $\mathcal{Z}(\mathcal{T})$ is finite. If $\inf_{s\in R} \gamma(s) = 0$ we reach $\mathcal{T}$ for every $n \geq m$ where $\lambda^m < \sup_{s\in R} \gamma(s)$. Hence $\mathcal{Z}(\mathcal{T})$ is cofinite.

[7] Given a collection $Y = \{\lambda_1, \ldots, \lambda_t\}$ of algebraic numbers consider the set $L = \{(a_1, \ldots, a_t) \in \mathbb{Z}^t \colon \lambda_1^{a_1} \cdots \lambda_t^{a_t} = 1\}$. It forms an abelian group under component-wise addition, and a deep result of Masser [21] shows that a basis of L can be computed (in polynomial time, see, e.g., [8]). In particular, it is decidable whether any two of the eigenvalues λ_i are multiplicatively independent.

Some non-real Let us first work under the assumption there is a single equation $\lambda^n = \gamma(s)$, where λ is a complex number of modulus one, but not a root of unity. Therefore λ^n takes on values in the unit circle. In the case $\gamma(s)$ intersects the unit circle only at finitely many s and we reduce to the finitely many targets case. Otherwise $\gamma(s)$, by continuity, results in arcs on the unit circle. Thus we have an arc-hitting word with angle $\arg(\lambda)$.

However, we may not necessarily have a single equation. We show they must all be related, and reduce to the single equation case (or finitely many point targets). In the complex case we would again like to conclude that there is a single equation. However, here we cannot simply take $\lambda_i^{a_i/a_j}$ or $\gamma_i(s)^{a_i/a_j}$, as these are multivalued functions over complex numbers.

Let a_j, b_j, $j = 2, \ldots, t$, be non-zero integers such that $\lambda_1^{a_j} = \lambda_j^{b_j}$, $j = 2, \ldots, t$. Let $\ell = \operatorname{lcm}\{b_2, \ldots, b_t\}$. Fix μ to be one of the ℓ numbers in the set $\lambda_1^{1/\ell}$. Take then an algebraic function η satisfying $\eta^\ell = \gamma$ identically, with η continuous over D (e.g., a suitable root of the polynomial obtained by replacing y with y^ℓ in the minimal polynomial of γ).

The aim is to show that, for each $0 \leq r < \ell$, the set of solutions (n, s), with $n = r \mod \ell$, to the original system of equations is exactly the union of solutions to the equations $\mu^n = \omega\eta(s)$, where ω ranges over a suitable subset (depending on r) of the ℓth roots of unity.

Now $\mu^{\ell a_j} = \lambda_1^{a_j} = \lambda_j^{b_j}$ so we have $\omega_j \mu^{\ell a_j / b_j} = \lambda_j$ for some b_jth root of unity ω_j. Notice that $c_j := \ell a_j / b_j$ is an integer. Similarly we have $\eta^{\ell a_j}(s) = \gamma_1^{a_j}(s) = \gamma_j^{b_j}(s)$ for all $s \in D$, so we have $\gamma_j(s) = \omega'_{s,j}\eta^{c_j}(s)$ for each s and some b_jth root of unity $\omega'_{s,j}$. In fact, $\omega'_{s,j}$ is constant in s since η and γ are continuous. Thus we may write $\gamma_j = \omega'_j \eta^{c_j}$.

We then look at taking powers to n. The equations are not "constant" in n as ω_j^n varies with n, but we can take arithmetic progressions with period ℓ to get "constant" equations. That is to say, for each r, $0 \leq r < \ell$, and for each $n = r \mod \ell$, we have $\lambda_j^n = \omega_j^n \mu^{c_j n} = \omega_j^r \mu^{c_j n}$. The equation $\lambda_j^n = \gamma_j(s)$ is then equivalent to $\mu^{c_j n}\omega_j^r = \omega'_j \eta_j^{c_j}(s)$. Writing $\omega''_j = \omega'_j / \omega_j^r$ for each j (with r fixed), we obtain the following equivalent system of equations

$$\begin{cases} \mu^{\ell n} & = \eta^\ell(s) \\ \mu^{c_j n} & = \eta_j^{c_j}(s)\omega''_j, \quad j = 2, \ldots, t, \end{cases} \tag{3}$$

where $\omega''_j = \omega'_j / \omega_j^r$ is yet another fixed c_jth root of unity (assuming r is fixed).

For (n, s) a solution to the equation $\mu^{\ell n} = \eta^\ell(s)$ implies that (n, s) is a solution to the equation $\mu^n = w\eta(s)$ for some ℓth root of unity ω. Conversely, any such solution is a solution to $\mu^{\ell n} = \eta^\ell(s)$. Therefore, to satisfy the first equation, we must have $\mu^n = \omega\eta(s)$ for some ω an ℓth root of unity. So assume (n, s) is a solution to the first equation. Then $\mu^{c_j n} = (\omega\eta_j)^{c_j} = \omega^{c_j}\eta^{c_j}(s)$. We conclude that (n, s) is a solution to (3) if and only if (n, s) is a solution to $\mu^n = \omega\eta(s)$ with ω an ℓth root of unity such that $\omega^{c_j} = \omega''_j$ for each $j = 2, \ldots, t$. In (3), we need $\omega^{c_j} = \omega''_j$ for each j. We compute the set S_r of ℓth roots of unity ω which satisfy $\omega^{c_j} = \omega''_j$ for all j. Then the set of solutions (n, s) to (3) with $n = r \mod \ell$ is exactly the union of the solutions to the equations $\mu^n = \omega\eta(s)$, $\omega \in S_r$.

We claim that the characteristic sequences of the union of the solutions to the equations $\mu^n = \omega\eta(s)$, $w \in S_r$ can be expressed as an arc-hitting word. Indeed, as η describes an arc on the unit circle, the union of the arcs given by $\omega\eta$, $\omega \in S_r$, gives a set $\mathcal{I}$ of arcs on the unit circle, such that $\mu^n \in \mathcal{I}$ if and only if $\mu^n = \omega\eta(s)$ for some $\omega \in S_r$. The arc-hitting model has angle $\arg(\lambda_1)/\ell$.

6 Putting Humpty together again

In this section, we prove the main result of this paper, Theorem 6. From Theorem 7 and Theorem 13 we know that for a single semialgebraic target $\mathcal{T}$ that is either contained inside a 3D subspace or has intrinsic dimension 1, there exists computable $L > 0$ such that $\mathcal{Z}(\mathcal{T})$ is equal to interleaving

of $\mathcal{Z}_0(\mathcal{T}), \ldots, \mathcal{Z}_{L-1}(\mathcal{T})$ where for each r, $\mathcal{Z}_r(\mathcal{T}) = \{n \mid M^{nL+r}x \in \mathcal{T}\}$ can be represented by an arc-hitting model. Let us consider what happens when we have multiple targets $\mathcal{T}_1, \ldots, \mathcal{T}_m$ that either have linear dimension 3 or intrinsic dimension 1. Suppose for $1 \leq i \leq m$, $\mathcal{Z}(\mathcal{T}_i)$ can be written as a union of L_i sets each of which can be represented by an arc-hitting model. Observe that if a set can be represented as a union of L_i arc-hitting models, then for any positive integer multiple L of L_i, it can be represented as a union of L arc-hitting models. Hence by taking the least common multiple of $L_1, \ldots, L_m$, we can assume that $L_i = L_j = L$ for every i, j. That is, we can assume that for all of the targets it suffices to consider the same number L of subsequences.

From Subsection 2.5 we already know that the characteristic word of $\mathcal{Z}_r(\mathcal{T}_i)$ is effectively almost periodic for $0 \leq r \leq L-1$ and $1 \leq i \leq m$ (because it can be represented by an arc-hitting model), and next we show that the overall word $w(\mathcal{O}, \pi)$ with respect to targets $\mathcal{T}_1, \ldots, \mathcal{T}_m$, which is obtained by combining the sets $\mathcal{Z}_r(\mathcal{T}_i)$, is also effectively almost periodic.

Theorem 16. *Let (M, x) be a linear dynamical system such that $\mathcal{Z}_r(\mathcal{T}_1), \ldots, \mathcal{Z}_r(\mathcal{T}_m)$, for $r \in \{0, \ldots, L-1\}$, are represented by arc-hitting models. Let $w = w(\mathcal{O}, \pi) \in \left(2^{\{\mathcal{T}_1, \ldots, \mathcal{T}_m\}}\right)^{\mathbb{N}}$ be the characteristic word of the LDS with respect to the m targets. Then w is effectively almost periodic.*

Proof Sketch. Let $\lambda_{i,r}, N_{i,r}, F_{i,r}, I_{i,r}$ be the parameters of the arc-hitting model corresponding to $\mathcal{Z}_r(\mathcal{T}_i)$. Recall that these arc-hitting models are used in the following way. There exists large enough N such that for all $n > N$, $n = qL + r$, $\mathcal{T}_i \in w[n]$ if and only if $\lambda_{i,r}^q \in I_{i,r}$, where $I_{i,r}$ is an open subsets of $\mathbb{T}$. We first lift this result from $\mathbb{T}$ to $\mathbb{T}^{L \cdot m}$ and from $\mathcal{T}_i \in w[n]$ to "the finite word u occurs at position n of w" in the following sense. We show that there exists a large enough N such that for every finite word u and residue $0 \leq r < L$, there exists an open subset $O_{u,r}$ of $\mathbb{T}^{L \cdot m}$ such that for all $n > N$, $n = qL + r$, the word u occurs at position n of w if and only if $\lambda^n \in O_{u,r}$, where $\lambda^n = (\lambda_{1,0}^n, \ldots, \lambda_{1,L-1}^n, \ldots, \lambda_{m,0}^n, \ldots, \lambda_{m,L-1}^n)$. Finally, using Kronecker's theorem from Diophantine approximation we show how, given $\lambda = (\lambda_{1,0}, \ldots, \lambda_{1,L-1}, \ldots, \lambda_{m,0}, \ldots, \lambda_{m,L-1})$ and $O_{u,r} \subseteq \mathbb{T}^{L \cdot m}$ for each $0 \leq r < L$, to compute a bound on consecutive visits of $(\lambda^n)_{n \in \mathbb{N}}$ to $O_{u,r}$. □

Together with Theorem 1, Theorem 16 completes the proof of the main result of this paper.

References

1. Agrawal, M., Akshay, S., Genest, B., Thiagarajan, P.S.: Approximate verification of the symbolic dynamics of markov chains. J. ACM 62(1), 2:1–2:34 (2015)
2. Almagor, S., Karimov, T., Kelmendi, E., Ouaknine, J., Worrell, J.: Deciding ω-regular properties on linear recurrence sequences. Proc. ACM Program. Lang. 5(POPL), 1–24 (2021)
3. Almagor, S., Ouaknine, J., Worrell, J.: The polytope-collision problem. In: ICALP. LIPIcs, vol. 80, pp. 24:1–24:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2017)
4. Almagor, S., Ouaknine, J., Worrell, J.: The semialgebraic orbit problem. In: STACS. LIPIcs, vol. 126, pp. 6:1–6:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2019)
5. Almagor, S., Ouaknine, J., Worrell, J.: First-order orbit queries (2020)
6. Baier, C., Funke, F., Jantsch, S., Lefaucheux, E., Luca, F., Ouaknine, J., Purser, D., Whiteland, M.A., Worrell, J.: The Orbit Problem for Parametric Linear Dynamical Systems (2021), https://arxiv.org/abs/2104.10634
7. Bochnak, J., Coste, M., Roy, M.F.: Real algebraic geometry, vol. 36. Springer-Verlag Berlin Heidelberg (1998)
8. Cai, J., Lipton, R.J., Zalcstein, Y.: The complexity of the A B C problem. SIAM J. Comput. 29(6), 1878–1888 (2000)
9. Chonev, V., Ouaknine, J., Worrell, J.: The orbit problem in higher dimensions. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013. pp. 941–950. ACM (2013)

10. Chonev, V., Ouaknine, J., Worrell, J.: On the complexity of the orbit problem. J. ACM 63(3), 23:1–23:18 (2016)
11. Chonev, V., Ouaknine, J., Worrell, J.: The polyhedron-hitting problem. Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms 2015 (07 2014)
12. Halava, V., Harju, T., Hirvensalo, M.: Positivity of second order linear recurrent sequences. Discret. Appl. Math. 154(3), 447–451 (2006)
13. Hansel, G.: A simple proof of the Skolem-Mahler-Lech theorem. In: ICALP. Lecture Notes in Computer Science, vol. 194, pp. 244–249. Springer (1985)
14. Harrison, M.A.: Lectures on Linear Sequential Machines. Academic Press, New York (1969)
15. Kannan, R., Lipton, R.J.: The orbit problem is decidable. In: Miller, R.E., Ginsburg, S., Burkhard, W.A., Lipton, R.J. (eds.) Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA. pp. 252–261. ACM (1980)
16. Kannan, R., Lipton, R.J.: Polynomial-time algorithm for the orbit problem. J. ACM 33(4), 808–821 (1986)
17. Karimov, T., Ouaknine, J., Worrell, J.: On LTL model checking for low-dimensional discrete linear dynamical systems. In: MFCS. LIPIcs, vol. 170, pp. 54:1–54:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2020)
18. Laohakosol, V., Tangsupphathawat, P.: Positivity of third order linear recurrence sequences. Discret. Appl. Math. 157(15), 3239–3248 (2009)
19. Leucker, M., Schallhart, C.: A brief account of runtime verification. J. Log. Algebraic Methods Program. 78(5), 293–303 (2009)
20. Markey, N., Schnoebelen, P.: Model checking a path. In: Amadio, R.M., Lugiez, D. (eds.) CONCUR 2003 - Concurrency Theory, 14th International Conference, Marseille, France, September 3-5, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2761, pp. 248–262. Springer (2003)
21. Masser, D.W.: Linear relations on algebraic groups, pp. 248–262. Cambridge University Press (1988)
22. Mignotte, M.: Some Useful Bounds, pp. 259–263. Springer Vienna, Vienna (1982)
23. Muchnik, A.A., Semenov, A.L., Ushakov, M.: Almost periodic sequences. Theor. Comput. Sci. 304(1-3), 1–33 (2003)
24. Ouaknine, J., Pinto, J.S., Worrell, J.: On the polytope escape problem for continuous linear dynamical systems. In: Frehse, G., Mitra, S. (eds.) HSCC 2017. pp. 11–17. ACM (2017)
25. Ouaknine, J., Worrell, J.: On the positivity problem for simple linear recurrence sequences,. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds.) Automata, Languages, and Programming. pp. 318–329. Springer Berlin Heidelberg, Berlin, Heidelberg (2014), extended version with proofs https://arxiv.org/abs/1309.1550
26. Ouaknine, J., Worrell, J.: Positivity problems for low-order linear recurrence sequences. In: SODA. pp. 366–379. SIAM (2014)
27. Ouaknine, J., Worrell, J.: Ultimate positivity is decidable for simple linear recurrence sequences. In: ICALP (2). Lecture Notes in Computer Science, vol. 8573, pp. 330–341. Springer (2014)
28. Ouaknine, J., Worrell, J.: On linear recurrence sequences and loop termination. ACM SIGLOG News 2(2), 4–13 (2015)
29. Semenov, A.L.: Logical theories of one-place functions on the set of natural numbers. Mathematics of the USSR-Izvestiya 22(3), 587 (1984)
30. Tarasov, S.P., Vyalyi, M.N.: Orbits of linear maps and regular languages. In: CSR. Lecture Notes in Computer Science, vol. 6651, pp. 305–316. Springer (2011)

A Additional material for Section 5

A.1 Reformulating semialgebraic targets in the parametric models

Consider a 1D semialgebraic target $\mathcal{T} \subseteq \mathbb{R}^d$. We show that $\mathcal{T}$ can be written as a finite union of sets parametrized by an algebraic function over $\mathbb{R}$ (i.e. sets of the form $\{f(s) : s \in \mathbb{R}\}$ where $f : \mathbb{R} \mapsto \mathbb{R}^d$ is an algebraic function) and points in $\mathbb{R}^d$. One way to define the dimension of a semialgebraic set is through Cell Decomposition (see, e.g., [7, Chapter 2]). In particular, we know that a semialgebraic set of dimension one (in our case, the target $\mathcal{T}$) is a union of cells $C_1, \ldots, C_k$ of dimension one in $\mathbb{R}^d$, which can be defined inductively as follows.

- Cells of dimension one in $\mathbb{R}$ are open intervals with endpoints in $\overline{\mathbb{Q}} \cup \{-\infty, \infty\}$ and points in $\overline{\mathbb{Q}}$;
- A cell C of dimension one in $\mathbb{R}^{k+1}$ with $k > 0$ can be written as $C = \{(x, g(x)) : x \in D\}$, where D is a cell of dimension one in $\mathbb{R}^k$ and $g(x)$ is the unique value of y satisfying the system $p_1(x, y) = 0$, $q_1(x, y) > 0, \ldots, q_m(x, y) > 0$ where $p_1, q_1, \ldots, q_m$ are polynomials in $k+1$ variables with rational coefficients. In other words, $C \subseteq \mathbb{R}^{k+1}$ is the image of the semialgebraic function g over the cell $D \subseteq \mathbb{R}^k$ of dimension one.

We show, by induction, that each cell of dimension one can be written as a union of sets parametrized by an algebraic function over $\mathbb{R}$. For the base case, observe that a point $p \in \overline{\mathbb{Q}}$ can be characterized using the algebraic function $f(s) = p$, the interval $(0, 1]$ as $\{\frac{1}{1+s^2} : s \in \mathbb{R}\}$ and the interval $(0, \infty)$ as $\{\frac{1}{s^2} : s \in \mathbb{R}\}$. We can characterize other intervals using these characterizations. For example, $(a, b] = \{a + \frac{b-a}{1+s^2}\}$, $[b, a) = \{a - \frac{a-b}{1+s^2} : s \in \mathbb{R}\}$ and an open interval (a, b) can be written as $(a, b) = (a, \frac{a+b}{2}] \cup [\frac{a+b}{2}, b)$.

Next, let C be a cell of dimension 1 in $\mathbb{R}^{k+1}$. Recall that

$$C = \{(x, y) : x \in D, p_1(x, y) = 0, q_1(x, y) > 0, \ldots, q_m(x, y) > 0\}$$

where D is a cell of dimension 1 in $\mathbb{R}^k$. By induction hypothesis, D must be a union of sets $D_1, \ldots, D_\ell$ parametrized by $f_1(s), \ldots, f_\ell(s)$, respectively. Hence $C = \bigcup_{i=1}^{\ell} C_i$, where for $1 \leq i \leq \ell$,

$$C_i = \{(f_i(s), y) : s \in \mathbb{R},\ p_1(f_i(s), y) = 0,\ q_1(f_i(s), y) > 0,\ \ldots,\ q_m(f_i(s), y) > 0\}$$

is the part of C that is obtained from D_i. We need to show that each C_i can be parametrized by an algebraic function. Viewing $p_1(f_i(s), y)$ and $q_j(f_i(s), y)$, $1 \leq j \leq m$, as polynomials in y with coefficients that are algebraic functions of s, we can factorise to obtain the system

$$\begin{cases} p_1(f_i(s), y) = (y - h_1^0(s)) \cdot \ldots \cdot (y - h_{\kappa(0)}^0(f_1(s))) = 0 \\ q_1(f_i(s), y) = (y - h_1^1(s)) \cdot \ldots \cdot (y - h_{\kappa(1)}^1(f_1(s))) > 0 \\ \ldots \\ q_m(f_i(s), y) = (y - h_1^m(s)) \cdot \ldots \cdot (y - h_{\kappa(m)}^m(f_1(s))) > 0 \end{cases}$$

where h_r^i is an algebraic function for every $0 \leq i \leq m$ and $1 \leq r \leq \kappa(i)$. Next we will show how to compute $\kappa(0)$ subsets $I_1, \ldots, I_{\kappa(0)}$ of $\mathbb{R}$ that have the following properties.

- $\bigcup_{j=1}^{\kappa(0)} I_j = \mathbb{R}$;
- Each I_j is a finite union of intervals;
- For $1 \leq j \leq \kappa(0)$, the value of y for each $s \in I_j$ is equal to $h_j^0(s)$, the jth root of $p_1(f_i(s))$.

This will allow us to write

$$C_i = \bigcup_{j=1}^{\kappa(0)} \{(f_i(s), h_j^0(s)) : s \in I_j\}.$$

Recall that each I_j is a finite union of intervals, each of which can be parametrized by an algebraic function with domain $\mathbb{R}$. Since composition of two algebraic functions remains algebraic, we can characterize each component of C_i that comes from a single subinterval of I_j using an algebraic function with domain $\mathbb{R}$. Hence we can write C_i as a union of sets with the desired parametrization.

To construct I_j, we proceed as follows. By definition, $I_j = \{s : (f_i(s), h_j^0(s)) \in C_i\}$ and hence can be defined by the formula

$$\varphi(s) = p_1(f_i(s), h_j^0(s)) = 0 \wedge q_1(f_i(s), h_j^0(s)) > 0 \wedge \cdots \wedge q_m(f_i(s), h_j^0(s)) > 0.$$

Hence I_j is semialgebraic. Since semialgebraic sets have finitely many connected components, I_j must be a finite union of interval subsets of $\mathbb{R}$.

B Additional material for Section 6

Proof of Theorem 16. Let $\lambda_{i,r}, N_{i,r}, F_{i,r}, I_{i,r}$ be the parameters of the arc-hitting model corresponding to $\mathcal{Z}_r(\mathcal{T}_i)$. We will use these arc-hitting models in the following way. Let $n = qL + r$, $0 \le r < L$ be larger than $\max\{N_{i,r} : 1 \le i \le m, 0 \le r < L\}$. We have that for each i, $\mathcal{T}_i \in w[n]$ if and only if $\lambda_{i,r}^q \in I_{i,r}$, by the definition of the arc-hitting model. In other words, $\mathcal{T}_i \in w[n]$ if and only if $\lambda_{i,r}^{\lfloor \frac{n}{L} \rfloor} \in I_{i,r}$.

Next we compute large enough N such that for all $n > N$, $1 \le i \le m$ and $0 \le r < L$,

- $\lfloor \frac{n}{L} \rfloor > N_{i.r}$, and
- $\lambda_{i,r}^{\lfloor \frac{n}{L} \rfloor}$ is not an endpoint of $I_{i,r}$. To see that this is possible, observe that for every i and r, $I_{i,r}$ has a finite number of endpoints. Since $\lambda_{i,r}$ by definition cannot be a root of unity, for every point $p \in \mathbb{T}$ one can compute N_p such that for all $n > N_p$, $\lambda^n \neq p$. Hence for all n larger than $\max\{N_p : p \text{ is an endpoint of } I_{i.r}\}$, λ^n is not an enpoint of $I_{i,r}$.

The first condition means that for $n > N$, $n = qL + r$, in order to determine whether $\mathcal{T}_i \in w[n]$ we only need to consider $\lambda_{i,r}$ and $I_{i,r}$ and ignore the finite set $F_{i,r}$ of exceptions. The second condition is useful for determining whether $\mathcal{T}_i \notin w[n]$: for $n > N$, $\mathcal{T}_i \notin w[n]$ if and only if $\lambda_{i,r}^q \notin I_{i,r}$, which, by the second condition is equivalent to $\lambda_{i,r}^q \in \operatorname{Int} I_{i,r}$, the interior of $I_{i,r}$. But crucially, the interior $\operatorname{Int} I_{i,r}$ of $I_{i,r}$ is also an open set, and hence for $n > N$, $\mathcal{T}_i \in w[n]$ (or $\mathcal{T}_i \notin w[n]$) if and only if $\lambda_{i,r}$ is in a certain open semialgebraic subset of $\mathbb{T}$.

Let $\mathbb{T}^{L \cdot m}$ denote the $L \cdot m$-dimensional torus (one coordinate per arc-hitting model and semialgebraic target). We define $\lambda = (\lambda_{1,0}, \ldots, \lambda_{1,L-1}, \ldots, \lambda_{m,0}, \ldots, \lambda_{m,L-1}) \in \mathbb{T}^{L \cdot m}$ and write $\lambda^n = (\lambda_{1,0}^n, \ldots, \lambda_{1,L-1}^n, \ldots, \lambda_{m,0}^n, \ldots, \lambda_{m,L-1}^n)$. Arc-hitting models describe the structure of $\mathcal{Z}_r(\mathcal{T}_i)$ in terms of powers of $\lambda_{i,r}$ and the open subset $I_{i,r}$ of $\mathbb{T}$. Next, we show how to describe the structure of w in terms of powers of λ and semialgebraic open subsets of $\mathbb{T}^{L \cdot n}$.

Let $n = qL + r > N$, with $0 \le r < L$.

- For every target $\mathcal{T}_i$, $\mathcal{T}_i \in w[n]$ if and only if $\lambda_{i,r}^q \in I_{i,r}$ by definition of the arc-hitting model. Let $O_{i,r}$ be the preimage of the projection map $\mathbb{T}^{L \cdot m} \to \mathbb{T}$ onto the coordinate (i, r). We have that $O_{i,r}$ is open and $\mathcal{T}_i \in w[n]$ if and only if $\lambda^n \in O_{i,r}$.
- Similarly, for every target $\mathcal{T}_i$, let $O'_{i,r}$ be the preimage of $\operatorname{Int}(\mathbb{T} \setminus I_{i,r})$ in $\mathbb{T}^{L \cdot m}$ under the projection map onto (i, r). Recall that $\operatorname{Int}(\mathbb{T} \setminus I_{i,r})$ is the open set that is used to characterize when the orbit is not in $\mathcal{T}_i$. We have that $O'_{i,r}$ is open and $T_i \notin w[n]$ if and only if $\lambda^n \in O'_{i,r}$, for all $n > N$.

- Next, let $\ell \in 2^{\{\mathcal{T}_1,\ldots,\mathcal{T}_m\}}$, be a letter. For example, suppose $\ell = \{\mathcal{T}_1, \mathcal{T}_3\}$, i.e. ℓ describes the set $(\mathcal{T}_1 \cup \mathcal{T}_3) \setminus \mathcal{T}_2$, assuming there are three targets in total. Then $w[n] = \ell$ if and only if $\lambda^q \in O_{1,r}$ (λ^q as opposed to λ^n because we need $q = n \bmod L$) and $\lambda^q \in O'_{2,r}$ and $\lambda^q \in O_{3,r}$, which is equivalent to $\lambda^q \in O_{1,r} \cap O'_{2,r} \cap O_{3,r} =: O_{\ell,r}$. Observing that $O_{\ell,r}$ is open, we conclude that for any letter ℓ, we can define an open subset $O_{\ell,r}$ (that is obtained by taking intersections and unions of the sets $O_{i,r}$ and $O'_{i,r}$) such that $w[n] = \ell$ if and only if $\lambda^n \in O_{\ell,r}$.
- Finally, let $u = u_0 \cdots u_k$ be a finite word over $2^{\{\mathcal{T}_1,\ldots,\mathcal{T}_m\}}$. We characterize an occurrence of u at position n of w, that is, for $0 \le j \le k$, $w[n+j] = u_j$. Let us consider a single equality $w[n+j] = u_j$. By the preceding analysis, this is equivalent to $\lambda^{\lfloor \frac{n+j}{L} \rfloor} \in O_{u_j, n+j \bmod L}$. Observe that $\lambda^{\lfloor \frac{n+j}{L} \rfloor} = \lambda^{q+\delta_j} = \lambda^q \lambda^{\delta_j}$ for $\delta_j \ge 0$. Hence $w[n+j] = u_j$ if and only if $\lambda^q \in \lambda^{-\delta_j} O_{u_j, n+j \bmod L}$. Hence we obtain that the word u occurs at position n if and only if $\lambda^q \in O_{u,r}$ where

$$O_{u,r} = \bigcap_{0 \le j \le k} \lambda^{-\delta_j} O_{u_j, n+j \bmod L}$$

  is an open subset of $\mathbb{T}^{L \cdot m}$.

We now move onto proving effective almost periodicity. To this end, given a finite word u, we need to show how to compute a bound p_u such that either u does not occur in $w[u, \infty)$, or it occurs within every contiguous subword of w of length p_u. From the analysis above we can compute the open sets $O_{u,0}, \ldots, O_{u,L-1}$. Suppose all of these sets are empty. In this case, for $n > N$, the word u cannot occur in position $w[n]$. Hence we can choose $p_u = N$. Now suppose that not all of the open sets $O_{u,0}, \ldots, O_{u,L-1}$ are empty. Below we show how to compute an effective upper bound on the distance between consecutive occurrences.

Let $W = \{\lambda^n : n \in \mathbb{N}\}$, where $\lambda \in \mathbb{T}^{L \cdot m}$ is defined as above. First, compute an effective representation of the set $\overline{W}$. The closure of W, unlike W itself, is very well-understood and is semialgebraic; see [25, Appendix A] for how to compute a representation for it. It is also the case that, by Kronecker's theorem, the sequence $(\lambda^n)_{n \in \mathbb{N}}$ is dense in $\overline{W}$ [25, Theorem 5].

Next, let $O_u = \bigcup_{r=0}^{L-1} O_{u,r}$. If $O_u \cap \overline{W}$ is empty (this can be effectively checked as $O_{u,r}$ is semialgebraic for all u and r and $\overline{W}$ is semialgebraic too), then λ^n is never in O, and hence for $n > N$, the word u cannot occur at position n of w. Therefore, we can once again choose $p_u = N$. It only remains to consider the case where $O_u \cap \overline{W}$ is non-empty. We will prove that in this case, the word u occurs infinitely often in w and show how to compute p_u. Wlog assume that $O_{u,0} \cap \overline{W} := O \neq \emptyset$, and observe that O must be open.

Recall that for large enough q (i.e. $qL > N$), $\lambda^q \in O_{u,0}$ if and only if the word u occurs at position qL. By density of $(\lambda^n)_{n \in \mathbb{N}}$ in $\overline{W}$ and openness of O, the sequence $(\lambda^n)_{n \in \mathbb{N}}$ will visit O infinitely often. Hence the word u will occur at position qL of w. To compute the bound on p_u on the gap between consecutive occurrences of u in w, we will proceed as follows. Consider the sequence $\langle O, \lambda^{-1}O, \lambda^{-2}O, \ldots \rangle \bigcup_{j=1^\infty} \lambda^{-j} O$. By density of $(\lambda^n)_{n \in \mathbb{N}}$ in $\overline{W}$, from any point in $\overline{W}$ one can reach O in finitely many steps. Hence $\bigcup_{j=0}^{\infty} \lambda^{-j} O = \overline{W}$. By compactness of $\overline{W}$, there must exist a finite open cover, i.e. $\bigcup_{j=0}^{M} = \overline{W}$ for some $M > 0$. The value of M can be determined by guess and check: observe that for any prefix of $\langle O, \lambda^{-1}O, \lambda^{-2}O, \ldots \rangle$, whether it is a cover can be determined by manipulating the semialgebraic sets in the prefix and the semialgebraic set $\overline{W}$. In the end, we have that $(\lambda^n)_{n \in \mathbb{N}}$ visits O within every M steps and hence the word u must occur (at a position qL for some q) within every window of size $L \cdot M$ in $w[N, \infty]$. Hence we can choose $p_u = \max\{N, L \cdot M\}$. □