Multiple Reachability in Linear Dynamical Systems

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

Edon Kelmendi ✉
School of Electronic Engineering and Computer Science, Queen Mary University of London, UK

Joël Ouaknine ✉
Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany

James Worrell ✉
Department of Computer Science, University of Oxford, UK

Abstract

We consider reachability problems for linear dynamical systems. Such a system in dimension d is specified by respective semialgebraic sets $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$ of source and target states and a matrix $M \in \mathbb{Q}^{d\times d}$. The task is to determine whether there is a point in $\mathbf{S}$ whose orbit under M intersects the target $\mathbf{T}$ in at least m distinct points. The case $m = 1$ (mere reachability) can be reduced to mild generalisations of the Skolem and Positivity Problems for linear recurrence sequences, whose decidability has been open for many decades. The situation is markedly different for *multiple reachability*, where m can be greater than one. In this paper, we prove that multiple reachability is undecidable already in dimension $d = 10$ with fixed multiplicity $m = 9$. Since our undecidability construction also shows that decision procedures for dimension $d \in \{3, \dots, 9\}$ would entail significant new results on effective solutions of Diophantine equations, we subsequently focus on the case $d = 2$, that is, multiple reachability in the plane. Here we obtain two positive results. We show that multiple reachability is decidable if the matrix M is a rotation and it is also decidable without restriction on M for halfplane targets. The former result relies on a deep theorem in arithmetic geometry, due to Bombieri and Zannier, concerning intersections of algebraic subgroups with subvarieties.

2012 ACM Subject Classification Theory of computation → Models of computation; Theory of computation → Logic and verification; Theory of computation → Verification by model checking

Keywords and phrases Linear Dynamical Systems, Linear Recurrence Sequences, Reachability, Multiple Reachability

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

1 Introduction

A *linear dynamical system* in dimension d is specified by respective semialgebraic sets (defined by boolean combinations of polynomial inequalities) $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$ of source and target states and a matrix $M \in \mathbb{Q}^{d\times d}$. We are interested in deciding properties of the *orbit* $\mathcal{O}_M(\mathbf{p}) \stackrel{\text{def}}{=} \{\mathbf{p} \cdot M^n : n \in \mathbb{N}\}$, where $\mathbf{p}$ ranges over the set $\mathbf{S}$ of initial points. Specifically, the *Multiple Reachability Problem* asks, given a linear dynamical system as above and a multiplicity $m \in \mathbb{N}$, whether there exists $\mathbf{p} \in \mathbf{S}$ such that $|\mathcal{O}_M(\mathbf{p}) \cap \mathbf{T}| \geq m$.

The above is best viewed as problem schema that can be specialised in different ways. There is an extensive literature treating the case $m = 1$, the *Reachability Problem*, which asks to determine whether $\mathcal{O}_M(\mathbf{p}) \cap \mathbf{T} \neq \emptyset$ for some $\mathbf{p} \in \mathbf{S}$. A celebrated paper of Kannan and Lipton [11] showed that point-to-point reachability (where both the source and target sets are singletons) is decidable in polynomial time, but for many variants of the Reachability Problem, decidability is open. Notably, point-to-hyperplane reachability (also known as Skolem's Problem) and point-to-halfspace reachability (also known as the Positivity Problem) have been studied extensively in relation to linear recurrence sequences, weighted automata, formal power series, model checking, and loop termination, but remain unsolved in general. The

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

current state of the art (see [1]) is that the Reachability Problem is decidable in dimension $d = 3$, Skolem's Problem is decidable in dimension $d = 4$, and the Positivity Problem is decidable in dimension $d = 5$. In Theorem 4 we note that the Reachability Problem can be reduced to its point-to-polytope variant. This last result suggests that the Skolem and Positivity Problems already capture much of the difficulty of the general (set-to-set) Reachability Problem.

In this paper we embark on a study of multiple reachability. Our first result is:

▶ **Theorem 1.** *The Multiple Reachability Problem is undecidable in general and is already undecidable in dimension $d = 10$ with multiplicity $m = 9$.*

The proof of Theorem 1 is by reduction from Hilbert's Tenth Problem (determine whether a given multivariate polynomial has an integer root) and uses in an essential way the quantification over the set $\mathbf{S}$ of source states in the Multiple Reachability Problem. This is in stark contrast with the Reachability Problem—no natural variants of which are known to be undecidable and which, as remarked above, can be reduced to its point-to-set variant.

The proof of Theorem 1 shows that decidability of multiple reachability in dimension d implies that one can solve Diophantine equations in $d - 1$ variables—a major open problem already for $d = 3$. Consequently, we focus on the case $d = 2$ (multiple reachability in the plane) where we show:

▶ **Theorem 2.** *In dimension $d = 2$ the Multiple Reachability Problem is decidable (i) when $\mathbf{T}$ is a halfspace (with $\mathbf{S}$ and M arbitrary) or (ii) when M is a rotation (with $\mathbf{S}$ and $\mathbf{T}$ arbitrary).*

Theorem 2(i) is proved using Kronecker's Theorem on Diophantine approximation and quantifier-elimination for the first-order theory of real-closed fields. Theorem 2(ii), is the main contribution of the present paper. The proof makes crucial use of bounds, due to Bombieri and Zannier, on the height of algebraic points in the set of intersections between a variety and algebraic subgroups of low dimension. To the best of our knowledge this is the first use of such tools in the analysis of linear dynamical systems and it is intriguing that they are apparently needed to handle even special cases of multiple reachability in the plane. The general case of the Multiple Reachability Problem in the plane remains open.

▶ **Example 3.** Consider the program in Figure 1. We ask whether there is some initialisation of the variables $x, y \in \mathbb{R}$ satisfying the equation $x^3 + xy^2 = 2y^2$ of the cissoid shown on the right such that the program terminates, Let us reinterpret this question as follows. First we remark that the loop body performs a linear transformation that rotates the vector (x, y) clockwise around the origin by the angle $\theta = -\cos^{-1}(4/5)$. So our problem can be reformulated as asking whether there is some point $\mathbf{p}$ in the cissoid that can be rotated into at least two points on the line $y = x - 1$. The latter is an instance of the Multiple Reachability Problem that falls within the purview of Theorem 2(ii). It so happens that the answer is "no" in this case.

Related Work

Closely related to *multiple* reachability is the question of multiplicity in linear recurrence sequences. A consequence of the Skolem-Mahler-Lech theorem is that for any integer k, and any nondegenerate linear recurrence sequence $\langle u_n \rangle_{n \in \mathbb{N}}$ the set $\{n \in \mathbb{N} : u_n = k\}$ is finite. Explicit upper bounds on the cardinality of this set in terms of the order of the recurrence are the subject of much study, see [7, Chapter 2.2] and references therein.

(x, y) satisfying $x^3 + xy^2 = 2y^2$
$m \leftarrow 2$
while $m \neq 0$ **do**
  $\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 4/5 & -3/5 \\ 3/5 & 4/5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$
  if $x = y + 1$ **then**
    $m \leftarrow m - 1$
  end if
end while

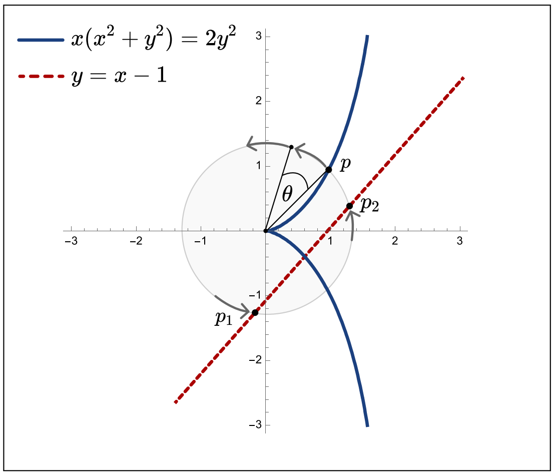

Figure 1 Instance of the Multiple Reachability Problem

The questions that we consider in this paper are generalisations of the Skolem Problem. There is another interesting generalisation in a different direction, which happens to be undecidable for nontrivial reasons. Namely, given k linear recurrence sequences over algebraic numbers: $\langle u_n^{(1)} \rangle_{n\in\mathbb{N}}, \langle u_n^{(2)} \rangle_{n\in\mathbb{N}}, \ldots, \langle u_n^{(k)} \rangle_{n\in\mathbb{N}}$, we are asked to decide whether there are natural numbers $n_1, \ldots, n_k$ such that $u_{n_1}^{(1)} + u_{n_2}^{(2)} + \cdots + u_{n_k}^{(k)} = 0$. This problem was conjectured to be undecidable by Cerlienco, Mignotte, and Piras in [5]. The conjecture was proved by Derksen and Masser recently in [6], for $k = 557844$. Similarly to the present paper, they reduce from Hilbert's Tenth Problem, and their proof requires that the sequences not be diagonalisable.

2 Undecidability of Multiple Reachability

A *basic semialgebraic subset* of $\mathbb{R}^d$ is the set of solutions of a system of constraints

$$P_0(x_1, \ldots, x_d) = 0 \wedge \bigwedge_{i=1}^{k} P_i(x_1, \ldots, x_d) > 0\,, \tag{1}$$

where $P_i \in \mathbb{Z}[x_1, \ldots, x_d]$. Note that a conjunction of several polynomial equations can be rewritten to a single equation since $x = 0 \wedge y = 0$ if and only if $x^2 + y^2 = 0$ for reals x and y. Semialgebraic sets are unions of basic semialgebraic sets and are precisely the definable sets in first-order logic over the structure $\langle \mathbb{R}, 0, 1, +, \times \rangle$, since the latter admits quantifier elimination. An *algebraic set* is the set of zeros of a polynomial with integer coefficients. A *hyperplane* is the set of solutions of a linear equation, while a *halfspace* is the set of solutions of a linear *inequality*, and a *polytope* is the intersection of finitely many halfspaces. If the polynomials in (1) all have zero constant term, then we say that the constraints are *homogeneous*.

As noted in the Introduction, our proof of undecidability of the Multiple Reachability Problem uses in a critical way the quantification over the set $\mathbf{S}$ of source states in the problem statement. Before entering into the details, we draw a contrast with the Reachability Problem, where we can assume without loss of generality that $\mathbf{S}$ is a singleton:

▶ **Theorem 4.** *The full Reachability Problem reduces to the point-to-polytope variant.*

The full proof of Theorem 4 is in Appendix A; the main idea appears implicitly in the proof of [1, Theorem 11].

The following is a (undecidable) variant of Hilbert's Tenth Problem (cf. Appendix A).

▶ **Problem 5.** *Given a polynomial $P(x_1, \ldots, x_9)$ with integer coefficients, determine whether there are distinct positive integers $n_1, n_2, \ldots, n_9$ such that $P(n_1, \ldots, n_9) = 0$.*

We reduce Problem 5 to the Multiple Reachability Problem. A sketch of this reduction has already appeared in [12]. The key idea is to construct for each $d \in \mathbb{N}$ a single "universal" linear dynamical system whose orbits are in one-to-one correspondence with integer polynomials of degree at most d:

▶ **Lemma 6.** *Given $d \in \mathbb{N}$, write $\mathbf{h}_d := (1, 0, \ldots, 0) \in \mathbb{R}^{d+1}$. Then there is a square matrix M_d of dimension $d + 1$ such that for every polynomial $P \in \mathbb{Z}[x]$ of degree at most d we have*

$$\big(P(1), P(2), \ldots, P(d + 1)\big)\ M_d^n\ \mathbf{h}_d^\top = P(n), \qquad \textit{for all } n \in \mathbb{N}.$$

Given an arbitrary polynomial $F \in \mathbb{Z}[y_1, \ldots, y_n]$, we define a linear dynamical system in dimension $2n+1$ as follows. The source set $\mathbf{S}$ comprises all $(x_1, \ldots, x_{n+1}, y_1, \ldots, y_n) \in \mathbb{R}^{2n+1}$ such that

$$F(y_1, \ldots, y_n) = 0 \wedge \bigwedge_{k=1}^{n+1} x_k = (k - y_1)(k - y_2) \cdots (k - y_n)\,.$$

The matrix M has M_n from Lemma 6 as its top-left $(n + 1) \times (n + 1)$ block and all other entries 0. The target set $\mathbf{T}$ is the hyperplane containing the origin and normal to $\mathbf{h} := \mathbf{h}_{2n}$. The idea is that the orbit of $\mathbf{p} := (x_1, \ldots, x_{n+1}, y_1, \ldots, y_n) \in \mathbf{S}$ intersects the target set $\mathbf{T}$ in n points if and only if the $(y_1, \ldots, y_k)$ is integer valued and thereby an integer root of F:

▶ **Lemma 7.** *The following two statements are equivalent:*

- *The polynomial F has a solution in distinct positive integers.*
- *There is some $\mathbf{p} := (x_1, \ldots, x_{n+1}, y_1, \ldots, y_n) \in \mathbf{S}$ and distinct positive integers $r_1, \ldots, r_n$ such that $\mathbf{p}\ M^{r_i}\ \mathbf{h}^\top = 0$, for $1 \le i \le n$.*

It follows from Lemma 7 that algebraic-to-hyperplane multiple reachability is undecidable. More precisely, we have shown that a procedure to decide algebraic-to-hyperplane multiple reachability in dimension $2n + 1$ can be used to effectively solve Diophantine equations with n variables. By projecting away the coordinates $y_1, \ldots, y_n$ in the definition of $\mathbf{S}$ above, we obtain a semialgebraic set. Hence a procedure to decide *semialgebraic*-to-hyperplane multiple reachability in dimension $n + 1$ can be used to effectively solve Diophantine equations with n variables. By the undecidability of Problem 5 we have:

▶ **Theorem 8.** *Algebraic-to-hyperplane multiple reachability is undecidable in dimension* 19, *and semialgebraic-to-hyperplane multiple reachability is undecidable in dimension* 10.

In the above undecidability proof, the matrix M is not diagonalisable. It would be interesting to explore the multiple reachability problem for diagonalisable matrices.

3 Algorithms on the Affine Plane

This section is devoted to proving Theorem 2, concerning multiple reachability in the plane. In this variant, the matrix M has dimension 2 and its eigenvalues are either: (a) a pair of complex conjugates $\lambda, \overline{\lambda} \in \overline{\mathbb{Q}}$, (b) two real algebraic roots $\rho_1, \rho_2 \in \overline{\mathbb{Q}} \cap \mathbb{R}$, or (c) a repeated real root $\rho \in \mathbb{Q}$. When the eigenvalues are a pair of complex conjugates and furthermore $|\lambda| = 1$ we say that the matrix is a *rotation*. In Case (a) we assume that $\lambda/\overline{\lambda}$ is not a root of unity, because this case is essentially the same as the case that the eigenvalues are real. Matrices whose ratios of distinct eigenvalues are not roots of unity, we call *nondegenerate*.

We begin by noting the first difference between arbitrary dimension and the affine plane, as regards the Multiple Reachability Problem: when the target is a homogeneous hyperplane (in this case a line passing through the origin), it cannot be reached more than once, unless the matrix has a very special form. A consequence of this fact and the work in [1], which gives an algorithm for deciding single reachability in dimension 2, is that multiple reachability is decidable for such targets. This is not the case in dimension 10 or higher.

▶ **Proposition 9.** *Let $\mathbf{p} \in \mathbb{R}^2$ be non-zero, h the line containing the origin and orthogonal to $\mathbf{h} \in \mathbb{R}^2$, and $M \in \mathbb{R}^{2\times 2}$ a nondegenerate matrix. If there are distinct positive integers $n, m \in \mathbb{N}$ such that both M^n and M^m map $\mathbf{p}$ into h, i.e.,*

$$\mathbf{p}M^n\mathbf{h}^\top = \mathbf{p}M^m\mathbf{h}^\top = 0, \tag{2}$$

then $\mathbf{p}M^k\mathbf{h}^\top = 0$ for all $k \in \mathbb{N}$. Moreover, in this case, either one of the eigenvalues of M is zero, or $M = \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$, for some $s \in \mathbb{R}$.

In case the target is a line that does *not* pass through the origin, the above proposition fails and multiple reachability becomes more difficult.[1] In general, the effect of a linear map on a point consists of (a) a dilation (a shrinking or stretching), and (b) a rotation. When both these effects are relevant, the multiple reachability problem becomes difficult. The positive results that we provide in this section solve decision problems where just one of the effects is at play. For example, the proposition above is about a target that passes through the origin, so the stretching effect of the linear map is not relevant.

3.1 Halfplane Targets

A semialgebraic set $\mathbf{S}$ is said to be *bounded* if there exists a real $\rho > 0$ such that $\mathbf{S}$ is contained in the open disk $x^2 + y^2 < \rho$. We call the infimum among such ρ the *radius* of the set $\mathbf{S}$. The infimum among $\rho \geq 0$ such that the set $\mathbf{S}$ intersects the open disk of radius ρ is called the *distance to the origin*. Clearly, boundedness is expressible in first-order logic, and the radius and distance to the origin are real algebraic by quantifier elimination.

We prove Theorem 2(i), by giving an algorithm that decides multiple reachability for halfplanes. To this end, let $\mathbf{S}$ be the initial semialgebraic set, $\mathbf{T}$ the target halfplane, M a 2×2 matrix with rational entries and $m \in \mathbb{N}$ the minimum number of times we wish to enter the target. We consider, separately, the case that M has complex conjugate eigenvalues $\lambda, \overline{\lambda}$, and the case that it has real eigenvalues. We begin with the former.

Let $\mathbf{p} \in \mathbb{R}^2$ have polar coordinates (r, φ), i.e., $\mathbf{p} = (r\cos\varphi, r\sin\varphi)$. By putting M into Jordan normal form (or similarly by using the polar decomposition), and applying some trigonometric identities, we can show that there exist real numbers $s, \vartheta, \vartheta_0$ such that for all $n \in \mathbb{N}$ the polar coordinates of $\mathbf{p}M^n$ are

$$(sr|\lambda|^n, n\vartheta + \vartheta_0 + \varphi). \tag{3}$$

[1] There is some work characterising when a line that does not pass through the origin is reached at most once. For example, if the initial point is in $\mathbb{Z}^2$ and the eigenvalue $|\lambda| > 1$, then for all but finitely many such integral initial points the target can be reached at most once [3].

The numbers s, r and $|\lambda|$ are real algebraic, while ϑ and ϑ_0 are logarithms of algebraic numbers. We will make use of the following fact from Diophantine approximation (cf. [4, Theorem 1 in Page 11]). For $x \in \mathbb{R}$, denote by $\{x\}_{2\pi}$ the unique real number in $[0, 2\pi)$ such that, for some integer m, $x = 2\pi m + \{x\}_{2\pi}$.

▶ **Lemma 10.** *If ϑ is an irrational multiple of 2π, then $\{\{n\vartheta\}_{2\pi} : n \in \mathbb{N}\}$ is dense in $[0, 2\pi]$.*

Proof of Theorem 2(i) for complex eigenvalues. If $|\lambda| > 1$, the algorithm answers *yes*. The justification is as follows. When $\mathbf{T}$ is a halfplane, there exist positive real numbers α_0, ϕ_1, ϕ_2, with $\phi_1 < \phi_2$, such that for all $\alpha > \alpha_0$ and $\phi_1 < \phi < \phi_2$, the point with polar coordinates (α, ϕ) is in $\mathbf{T}$. In other words, the halfplane contains a cone minus a bounded set.

The matrix M is assumed to be nondegenerate, which implies that the rotation angle ϑ in (3) is an irrational multiple of 2π. Applying Lemma 10, we see that the the set

$$\{n\vartheta + \vartheta_0 + \phi \mod 2\pi : n \in \mathbb{N}\} \tag{4}$$

has infinite intersection with the interval (ϕ_1, ϕ_2). From $|\lambda| > 1$, it follows that the sequence of points $\mathbf{p}M^n$ enters the cone mentioned above, which is a subset of $\mathbf{T}$, infinitely often.

The case $|\lambda| = 1$ is handled in the next subsection, so we proceed to the case $|\lambda| < 1$. When the halfplane $\mathbf{T}$ has distance zero to the origin, or when the source $\mathbf{S}$ is unbounded, the algorithm answers *yes*, with justification symmetric to the one above. Assume that $\mathbf{T}$ has distance $\delta > 0$ to the origin and let $\mathbf{S}$ be bounded with radius ρ. Choose some $N \in \mathbb{N}$ such that $\rho|\lambda|^N < \delta$; then for any source point $\mathbf{p} \in \mathbf{S}$, and all $n > N$, $\mathbf{p}M^n$ is not in the target $\mathbf{T}$. To decide the multiple reachability problem, consider the semialgebraic sets, defined for $n \in \{0, 1, \dots, N\}$ as $\mathbf{S}_n \stackrel{\text{def}}{=} \{\mathbf{p} \in \mathbf{S} : \mathbf{p}M^n \in \mathbf{T}\}$, and decide whether there are m among them that have nonempty common intersection. ◀

We turn our attention now to the case where the eigenvalues of the matrix M are real. We spell out the case of distinct positive real eigenvalues $\rho_1 > \rho_2 > 0$, relegating the other cases (which are based on similar reasoning) to the Appendix. In Jordan normal form the matrix M is BDB^{-1} where D is a diagonal matrix and B is an invertible matrix with real algebraic entries. We can replace $\mathbf{S}$ by $\mathbf{S} \cdot B$, and the target set by $B^{-1} \cdot \mathbf{T}$. As a consequence we can assume that $M = \begin{pmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{pmatrix}$. We will also assume without loss of generality that $\rho_1 > \rho_2 > 0$. The algorithm rests on the following lemma.

▶ **Lemma 11.** *Let M be as above, H a halfplane, $\mathbf{p} \in \mathbb{R}^2$ a point, and $\mathbf{p}_0, \mathbf{p}_1, \dots$ its orbit under M. The orbit can switch from H to $\mathbb{R}^2 \setminus H$, or conversely, at most twice. In particular, the orbit is either ultimately in H or ultimately in $\mathbb{R}^2 \setminus H$.*

From the proof of the lemma we also see that when the halfplane is given by a homogeneous inequality, the orbit cannot leave the halfplane and come back.

The version of Lemma 11 in case M has a repeated eigenvalue ρ follows by an analogous argument. In this case, by a change of basis, we can assume that $M = \begin{pmatrix} \rho & 1 \\ 0 & \rho \end{pmatrix}$. Then the expression corresponding to (11) is $(nxc_2\rho^{-1} + c_2y + c_1x)\rho^n + c_3$, which likewise changes sign at most twice.

Proof of Theorem 2(i) for M with real eigenvalues. Lemma 11 and Appendix A entail, via a simple case analysis, that any orbit that enters H at least m times must harbour a segment of m visits to H whose gaps between consecutive visits is at most 4. In other words, the orbit of $\mathbf{p}$ enters $\mathbf{T}$ at least m times if and only if there exist $n_1, \ldots, n_m \in \mathbb{N}$ such that $\mathbf{p}M^{n_i} \in \mathbf{T}$ and $0 < n_{i+1} - n_i \leq 4$ for all n_i. The latter (contiguous) multiple reachability question can easily be reduced to a number of reachability queries. Indeed, an orbit contains a pattern (of visits and non-visits to H) of length $4m$ if and only if it reaches a certain polytopic subset $\mathbf{P}$ of $\mathbb{R}^2$; A formula defining P can be constructed by considering the sets $\{x \in \mathbb{R}^2 : xM^k \in H\}$ and$\{x \in \mathbb{R}^2 : xM^k \notin H\}$ for $0 \leq k \leq 4m$. Thus multiple reachability is reduced to at most 2^{4m} instances of single reachability from $\mathbf{S}$ to $\mathbf{P}$, which can be solved by invoking the algorithm from [1]. ◀

3.2 Rotations

Now we prove Theorem 2(ii), which says that multiple reachability is decidable for rotations on the plane. To this end, let $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^2$ be the source and target semialgebraic sets, given by respective first-order formulas $\Phi_{\mathbf{S}}, \Phi_{\mathbf{T}}$; M a matrix whose eigenvalues are the pair $\lambda, \overline{\lambda}$ on the unit circle, that is $|\lambda| = 1$, and let $m \in \mathbb{N}$. Our goal is to determine whether there exists some $\mathbf{p} \in \mathbf{S}$ and distinct positive integers $x_1, \ldots, x_m \in \mathbb{N}$ such that $\mathbf{p}M^{x_i} \in \mathbf{T}$, for each $i \in \{1, 2, \ldots, m\}$.

We begin our proof by treating an easier problem, namely the question of entering the target set infinitely often.

▶ **Proposition 12.** *For any $\mathbf{p} \in \mathbb{R}^2$, exactly one of the following holds:*

1. *There are infinitely many positive integers and infinitely many negative integers x such that $\mathbf{p}M^x \in \mathbf{T}$.*
2. *There are only finitely many positive integers and finitely many negative integers x such that $\mathbf{p}M^x \in \mathbf{T}$.*

Furthermore, we can decide whether there exists some $\mathbf{p} \in \mathbf{S}$ for which the first case holds.

If the first alternative in the proposition holds for some point in the source set, then clearly we have a positive instance of the Multiple Reachability Problem. We therefore assume in the rest of this section that from every point in the source set the target can be reached only finitely many times. More precisely, we work under:

▶ **Assumption 13.** *The linear dynamical system is such that for every point $\mathbf{p} \in \mathbf{S}$ there are only finitely many integers x such that $\mathbf{p}M^x \in \mathbf{T}$. In other words, the second alternative of Proposition 12 holds for all points in the source set.*

We proceed by eliminating the existential quantifier in the decision question. To this end, let $\mathbf{v} = (v_1, v_2)$ be a tuple of variables, let $V_1, \ldots, V_m$ be 2×2 matrices of fresh variables, and consider the formula: $\Gamma(\mathbf{v}, V_1, \ldots, V_m) \stackrel{\text{def}}{=} \Phi_{\mathbf{S}}(\mathbf{v}) \wedge \bigwedge_{i=1}^{m} \Phi_T(\mathbf{v}\ V_i)$. Then the Multiple Reachability Problem asks whether there exist $\mathbf{p} \in \mathbb{R}^2$ and distinct positive integers $x_1, \ldots, x_m$ such that

$$\Gamma(\mathbf{p}, M^{x_1}, \ldots, M^{x_m}) \tag{5}$$

holds. Eliminating the existential quantification over $\mathbf{v}$ from Γ, we obtain another formula $\Gamma'(V_1, \ldots, V_m)$ such that (5) holds for some point $\mathbf{p}$ if and only if $\Gamma'(M^{x_1}, \ldots, M^{x_m})$ is true. Tuples of reals that satisfy Γ' form a semialgebraic set; which can be written as a finite union of sets of the form (1), that is a system of one polynomial equality and a finite number of polynomial inequalities. Each set in this union can be treated separately, so let $P_0, \ldots, P_\ell$ be polynomials (with integer coefficients) of one of the sets:

$$\Psi(V_1, \ldots, V_m) \stackrel{\text{def}}{=} P_0(V_1, \ldots, V_m) = 0 \wedge \bigwedge_{i=1}^{\ell} P_i(V_1, \ldots, V_m) > 0\,.$$

Our goal is to decide whether there are distinct positive integers $x_1, \ldots, x_m$ such that $\Psi(M^{x_1}, \ldots, M^{x_m})$ holds. We will call any such tuple $(x_1, \ldots, x_m)$ a *solution.*

By diagonalisation there are algebraic numbers $c_1, \ldots, c_4 \in \overline{\mathbb{Q}}$ such that for all $n \in \mathbb{N}$

$$M^n = \begin{pmatrix} c_1\lambda^n + \overline{c_1\lambda^n} & c_2\lambda^n + \overline{c_2\lambda^n} \\ c_3\lambda^n + \overline{c_3\lambda^n} & c_4\lambda^n + \overline{c_4\lambda^n} \end{pmatrix}.$$

It follows that given the polynomials $P_0, \ldots, P_\ell$ appearing in Φ we can compute polynomials $Q_0, \ldots, Q_\ell$ with algebraic coefficients such that

$$P_i(M^{x_1}, \ldots, M^{x_m}) = Q_i(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}),$$

for $0 \le i \le \ell$ and all tuples of integers $(x_1, \ldots, x_m) \in \mathbb{Z}^m$.

When P_0 is identically zero, we will argue that there cannot be any solutions, due to Assumption 13. In fact, we prove a more general statement that will be useful later on:

▶ **Lemma 14.** *Let $\Lambda \subseteq \mathbb{Z}^m$ be a non-trivial additive subgroup such that for all $(x_1, \ldots, x_m) \in \Lambda$ we have $Q_0(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}) = 0$. Then there is no solution in Λ.*

For the case in which P_0 (and hence Q_0) is identically zero, we take $\Lambda = \mathbb{Z}^m$ in the lemma above, and conclude that there are no solutions. The idea is to use a general version of Kronecker's theorem in Diophantine approximation to prove that if there is some element of the subgroup $(x_1, \ldots, x_m) \in \Lambda$ such that $Q_i(\lambda^{x_1}, \ldots, \lambda^{-x_m}) > 0$, then there are infinitely many such elements—contradicting Assumption 13; See Appendix A for the proof.

The rest of this section is devoted to proving the following lemma:

▶ **Lemma 15.** *There exists an effective bound $B \in \mathbb{N}$ depending only on Q_0, such that if there is a solution in $\mathbb{N}^m$, then there is one, call it $\mathbf{x}$, with $\|\mathbf{x}\| \stackrel{\text{def}}{=} \sum |x_i| \le B$.*

Since both λ and the coefficients of the polynomials are algebraic numbers, we can use Tarski's algorithm to check whether each of $\mathbf{x}$, $\|\mathbf{x}\| \le B$, is a solution. Therefore as a consequence of Lemma 15 and Proposition 12, multiple reachability for rotations is decidable, i.e., Theorem 2(ii) holds.

For the proof of Lemma 15, we will use deep results of Zannier, Bombieri, and Schmidt concerning the intersection of varieties with algebraic subgroups of dimension 1. In order to state these, we need a few definitions. More more details see [15], [14], and especially [2, Chapter 3]. We borrow from the latter freely.

It is convenient in the rest of this section to set $n := 2m$, where m is the number of times we want to enter the target set. A *variety* Y in affine n-dimensional space $\overline{\mathbb{Q}}^n$ is defined to be the set of tuples $(y_1, \ldots, y_n)$ which satisfy a system of polynomial equations $f_i(y_1, \ldots, y_n) = 0$, where f_i is from a family of polynomials with algebraic coefficients. We say that a variety is *irreducible* if it cannot be written as the union of two proper subvarieties.

We define $\mathbb{G}^n$ to be the set of tuples $(z_1, \ldots, z_n)$ of nonzero algebraic numbers. In other words it is the subset of $\overline{\mathbb{Q}}^n$ satisfying $z_1 \cdots z_n \neq 0$. It is a group under component-wise multiplication.

We define the variety $X_0 \subseteq \mathbb{G}^n$ to be the zero set of the polynomial Q_0 and the polynomials $z_j z_{j+1} - 1$, where $1 \le j \le n$ is an odd number, to ensure that the conjugate relations hold. We assume that X_0 is irreducible, for otherwise, we can factorize the polynomials and treat the irreducible components in turn. We will effectively find points in the intersection of this variety and all algebraic subgroups of dimension 1, which we now define.

An *algebraic subgroup* is a subvariety of $\mathbb{G}^n$ that is also a subgroup. As an example, given an additive subgroup $\Lambda \subseteq \mathbb{Z}^n$, we can see that it determines an algebraic subgroup

$$H_\Lambda \stackrel{\text{def}}{=} \{(z_1,\ldots,z_n) \in \mathbb{G}^n : z_1^{a_1} z_2^{a_2} \cdots z_n^{a_n} = 1 \text{ for all } \mathbf{a} \in \Lambda\}.$$

In fact every algebraic subgroup is of this type, [2, Corollary 3.2.15]. Further, if Λ is a subgroup of $\mathbb{Z}^n$ of rank $n-r$ then H_Λ is an algebraic subgroup of dimension r. By dimension here we mean the dimension of the variety, see for example [8, Definition on Page 5].

▶ **Lemma 16.** *For all $(a_1,\ldots,a_k) \in \mathbb{Z}^k$, the point $(\lambda^{a_1},\ldots,\lambda^{a_k})$ belongs to an algebraic subgroup of dimension 1.*

We denote by $\mathcal{H}_1(n)$ the union of all algebraic subgroups of $\mathbb{G}^n$ that have dimension 1; the parameter n will be omitted when the ambient dimension is understood. We are interested in the intersection $\mathcal{H}_1 \cap X_0$, as, by the lemma above, this contains all points $(\lambda^{x_1},\lambda^{-x_1},\ldots,\lambda^{x_m},\lambda^{-x_m})$ for which $Q_0(\lambda^{x_1},\lambda^{-x_1},\ldots,\lambda^{x_m},\lambda^{-x_m}) = 0$, where x_i are integers. Equipped with these definitions, we next give an overview of the proof of the crucial Lemma 15.

Overview of the Proof

The proof is by induction on a certain structure of the set X_0, leading to an increasing sequence $b_0 \leq b_1 \leq \cdots \leq b_n = B$ of bounds, with B the bound appearing in Lemma 15. As a first step, the set X_0 is partitioned into the disjoint union of two subsets X_0° and $X_0^\bullet$, defined below. The latter is Zariski closed, i.e., it is the solution of a collection of polynomial equations. Bombieri and Zannier's theorem tells us that there are only finitely many points in $\mathcal{H}_1 \cap X_0^\circ$ —we call these the short points—and moreover gives an effective upper bound on their height, which is immediately translated into a bound b_0.

We call the remaining points in $\mathcal{H}_1 \cap X_0^\bullet$ the tall points. Fortunately, the set $X_0^\bullet$ also has a very pleasant form: it is isomorphic to $X_1 \times \mathbb{G}^r$ for some $r \geq 1$, where X_1 is now another (smaller) variety. We repeat, by decomposing X_1 into disjoint sets X_1° and $X_1^\bullet$. Again, in the former set the size of the points intersecting $\mathcal{H}_1$ is upper bounded. Going through the isomorphism such points define some linear space, in which, by integer programming we obtain a new bound $b_1 \geq b_0$. This process eventually terminates because the variety $X_{i+1}^\bullet$ lives in an ambient space whose dimension is strictly smaller than that of the ambient space of the variety $X_i^\bullet$. ◀

We proceed with a sequence of definitions and lemmas that form the proof Lemma 15, which is concluded in the last subsection. A *linear torus* is an algebraic subgroup that is irreducible. A *torus coset* is a coset of the form gH where H is a linear torus and $g \in \mathbb{G}^n$.

Given any subvariety $X \subseteq \mathbb{G}^n$ we denote by $X^\bullet$ the union of all nontrivial torus cosets that are contained entirely in X, in other words:

$$X^\bullet \stackrel{\text{def}}{=} \bigcup \{gH \text{ a torus coset } : gH \subseteq X \text{ and nontrivial}\}.$$

Define $X^\circ \stackrel{\text{def}}{=} X \setminus X^\bullet$. We will analyse the points in $X_0^\bullet \cap \mathcal{H}_1$ (*i.e.* $(X_0)^\bullet \cap \mathcal{H}_1$) and $X_0^\circ \cap \mathcal{H}_1$ in the next two subsections, calling them respectively the *tall points* and the *short points*.

3.2.1 Tall Points

Recall that for $\mathbf{a} \in \mathbb{Z}^n$ we write $\mathbf{z}^\mathbf{a} = z_1^{a_1} \cdots z_n^{a_n}$. Let A be an $n \times n$ matrix with integer entries, and denote by $A_1,\ldots,A_n$ its columns. We denote by $\varphi_A : \mathbb{G}^n \to \mathbb{G}^n$ the map $\varphi_A(\mathbf{z}) \stackrel{\text{def}}{=} (\mathbf{z}^{A_1},\ldots,\mathbf{z}^{A_n})$. One can show that $\varphi_{AB} = \varphi_B \circ \varphi_A$, and as a consequence for matrices A with determinant ± 1, φ_A is an isomorphism[2] with inverse $\varphi_{A^{-1}}$. Such an isomorphism is called a *monoidal transformation*. Recall that the group of $n \times n$ integer matrices with determinant ± 1 is the special linear group, denoted $\mathrm{SL}(n, \mathbb{Z})$.

We state here some basic results related to the structure of algebraic subgroups. Recall that we use the notation $\|\mathbf{a}\|$ for the ℓ^1 norm of a vector $\mathbf{a}$. For a matrrix A, we denote by $\|A\|$ the maximum of the ℓ^1 norms of its columns.

▶ **Proposition 17** ([2, Proposition 3.2.10 and Corollary 3.2.9]). *Let H_Λ be a linear torus, where Λ is a subgroup of $\mathbb{Z}^n$ of rank $n-r$ and suppose that Λ has $n-r$ independent vectors of norm at most N. Then there is a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$ with $\|A\| \le n^3 N^{n-r}$ and $\|A^{-1}\| \le n^{2n-1} N^{(n-1)^2}$, such that $\varphi_A(\mathbf{1}_{n-r} \times \mathbb{G}^r) = H_\Lambda$, where $\mathbf{1}_{n-r} \subseteq \mathbb{G}^r$ is the subgroup $\mathbf{1}_{n-r} = \{(1, \dots, 1)\}$.*

We can effectively compute A given $n-r$ independent vectors of Λ, using the Smith normal form.

Let $X \subseteq \mathbb{G}^n$ be a subvariety. We say that an algebraic subgroup H of $\mathbb{G}^n$ is *maximal* in X if $H \subseteq X$ and H is not properly contained in any subgroup $H' \subseteq \mathbb{G}^n$ with $H' \subseteq X$.

▶ **Proposition 18** ([2, Proposition 3.2.14]). *Let $X \subseteq \mathbb{G}^n$ be a subvariety, defined by polynomial equations $f_i(\mathbf{x}) := \sum c_{i,\mathbf{a}} \mathbf{x}^{\mathbf{a}} = 0$, $1 \le i \le k$, and let E_i be the set of exponents appearing in the monomials of f_i. Let H be a maximal algebraic subgroup of $\mathbb{G}^n$ contained in X. Then $H = H_\Lambda$ where Λ is generated by vectors of type $\mathbf{a}'_i - \mathbf{a}_i$, with $\mathbf{a}'_i, \mathbf{a}_i \in E_i$, for $i = 1, \dots, k$.*

The first proposition says that linear tori of dimension r are isomorphic to $\mathbb{G}^r$, and that the isomorphism is given in terms of a monoidal transformation that we can compute. (An analogous statement holds also for general algebraic subgroups; however the component $\mathbf{1}_{n-r}$ is replaced by a finite subgroup of $\mathbb{G}^{n-r}$ in the general case.) The second proposition tells us that maximal algebraic subgroups contained in a variety X are defined by the exponents of monomials appearing in the polynomial that define X.

The two propositions above have the following important consequence. If $gH \subseteq X$ is a maximal torus coset (meaning that it is not contained in another torus coset), then H is one of the components of a maximal algebraic subgroup H' of the variety $g^{-1}X$. Proposition 18 implies that there are finitely many such H', that we can effectively compute them, and further that they are independent of g—note that only the exponents matter in the proposition, not the coefficients. Since it is possible to compute the equations of each component of H' by factoring in the number field $\mathbb{Q}(\lambda)$, we have:

▶ **Lemma 19.** *Given a variety X, we can effectively construct a (possibly empty) finite set $\mathcal{T}_X$ of positive-dimensional tori, such that if $gH \subseteq X$ is a maximal torus coset, then $H \in \mathcal{T}_X$, and for every $H \in \mathcal{T}_X$ there is some torus coset $gH \subseteq X$ which is maximal.*

From this lemma, given a variety X, another way of defining the subset $X^\bullet$ is

$$X^\bullet = \bigcup \{gH : g \in \mathbb{G}^n, H \in \mathcal{T}_X, \text{ and } gH \subseteq X\}.$$

Finally we give another way of expressing all torus cosets gH for fixed H that are contained in X.

[2] This means that it is a group homomorphism that is also a morphism of algebraic varieties.

▶ **Lemma 20.** *([2, Theorem 3.3.9]). Let $X \subseteq \mathbb{G}^n$ be a subvariety and H a linear torus of dimension $r \geq 1$. Then there exists a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$, which can be computed, such that*

$$\bigcup_{gH \subseteq X} gH = \varphi_A(X_1 \times \mathbb{G}^r),$$

where $X_1 \subseteq \mathbb{G}^{n-r}$ is a subvariety, whose defining polynomials can be computed.

The end goal of this subsection was to show that $X^\bullet$ is composed of finitely many sets which essentially are subvarieties of strictly smaller dimension. Since all the objects are effective, this lends itself to a recursive procedure. Before explaining how all of this comes together in the proof of Lemma 15, we first discuss the points in X°.

3.2.2 Short Points

The height of a point $\mathbf{z}$ in $\overline{\mathbb{Q}}^n$ is a central notion in Diophantine geometry. It is used to measure the arithmetic complexity of $\mathbf{z}$. For more details the reader should consult, for example, Chapter 1 of [2]. For our purposes, it suffices to define the height as follows. Let $K := \mathbb{Q}(\lambda)$ be the number field that we work in. There is a way of choosing absolute values M_K in this field, such that the product formula holds. Writing $\log^+ t := \max(0, \log t)$, the the (absolute logarithmic Weil) *height* of a point $\mathbf{z} = (z_1, \ldots, z_n) \in K^n$ is defined as:

$$h(\mathbf{z}) \stackrel{\text{def}}{=} \sum_{v \in M_K} \max_j \log^+ |z_j|_v.$$

We are interested in specific points of the form $(\lambda^{x_1}, \ldots, \lambda^{x_n})$, where $x_i \in \mathbb{Z}$. The height of such points has the following properties:

▶ **Lemma 21.** *Let $\mathbf{x} \in \mathbb{Z}^n$, and denote by $M = \max_j |x_j|$. Then*

$$Mh(\lambda) \leq h\big((\lambda^{x_1}, \ldots, \lambda^{x_n})\big) \leq 2Mh(\lambda).$$

The main fact that allows for a procedure to decide multiple reachability for rotations is the following theorem on heights of points in $X^\circ \cap \mathcal{H}_1$, due to Bombieri and Zannier:

▶ **Theorem 22** ([14, Theorem 1, Page 524])**.** *Let $X \subseteq \mathbb{G}^n$ be a subvariety. Then there exists an effective bound $b \in \mathbb{N}$ depending only on X such that for all $\mathbf{z} \in \mathbb{G}^n$, if $\mathbf{z} \in X^\circ \cap \mathcal{H}_1$ then $h(\mathbf{z}) \leq b$.*

The theorem cited in [14] does not explicitly state that the bound is effective, but upon a closer inspection of the proof one can see that all steps are explicit, with the sole exception of points $(c_1^*, \ldots, c_h^*) \in \mathbb{Z}^h$ that are chosen to be outside a finite number of linear subspaces of $\mathbb{Q}^h$ with effective descriptions. It is plain that we can effectively construct such points.

Now we can describe the algorithm that computes the bound of Lemma 15.

3.2.3 The Algorithm

Consider vectors $\mathbf{x} \in \mathbb{Z}^m$ such that $(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}) \in X_0$. From Lemma 16 such points also belong to $\mathcal{H}_1 \cap X_0$. From Theorem 22 we compute a bound $b_0 \in \mathbb{N}$ such that if $\|x\| > b_0$ then $(\lambda^{x_1}, \ldots, \lambda^{-x_m})$ does not belong to $\mathcal{H}_1 \cap X_0^\circ$.

Next, for points in $\mathcal{H}_1 \cap X_0^\bullet$, we use Lemma 19 to construct the set $\mathcal{T}_{X_0}$ of tori, which have a maximal coset contained in X_0. If $\mathcal{T}_{X_0}$ is empty, so is the set $X_0^\bullet$, and we are done because the bound b_0 suffices. Otherwise let $H \in \mathcal{T}_{X_0}$ be a linear torus of dimension $r \geq 1$.

If $r = n$, using Lemma 20 we can compute a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$ such that

$$\bigcup_{gH \subseteq X_0} gH = \varphi_A(\mathbb{G}^n).$$

In this case, we take the image of A, $\mathrm{Im}(A) \subseteq \mathbb{Q}^n$, which is a linear subspace, and intersect it with the subspace generated by the equations $x_1 + x_2 = 0$, $x_3 + x_4 = 0$, up to $x_{n-1} + x_n = 0$, to get linear subspace V of $\mathbb{Q}^m$. This is a subspace of $\mathbb{Q}^m$, because the odd coordinates determine the even ones. The set $V \cap \mathbb{Z}^m$ is a subgroup of $\mathbb{Z}^m$, and it satisfies the conditions of Lemma 14, so for all $\mathbf{x} \in \mathbb{Z}^m$, and $g \in \mathbb{G}^n$ such that $(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}) \in gH$, the vector $\mathbf{x}$ cannot be a solution.

Now suppose that $0 < r < n$. Using Lemma 20, we compute a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$, and the subvariety $X_1 \subseteq \mathbb{G}^{n-r}$, such that

$$\bigcup_{gH \subseteq X_0} gH = \varphi_A(X_1 \times \mathbb{G}^r).$$

Since $\mathcal{H}_1$, which is the union of all subgroups of dimension 1, is invariant under monoidal transformations, we have

$$\mathcal{H}_1 \cap \varphi_A(X_1 \times \mathbb{G}^r) = \varphi_A\big(\mathcal{H}_1 \cap (X_1 \times \mathbb{G}^r)\big).$$

Let b_1' be the bound we get from Theorem 22 when applied to the intersection

$$X_1^\circ \cap \mathcal{H}_1(n-r). \tag{6}$$

Let $(y_1, \ldots, y_{n-r}) \in \mathbb{Z}^{n-r}$, and denote by $\widetilde{y}$ the maximal value among $|y_1|, \ldots, |y_{n-r}|$. Then the bound in Lemma 21, implies that if $\widetilde{y} > b_1'/h(\lambda)$, $(\lambda^{y_1}, \ldots, \lambda^{y_{n-r}})$ does not belong to the intersection in (6). We can enumerate the finitely many vectors $(y_1, \ldots, y_{n-r}) \in \mathbb{Z}^{n-r}$ such that $\widetilde{y} \leq \lceil b_1'/h(\lambda) \rceil$, and test for each using Tarski's algorithm whether $(\lambda^{y_1}, \ldots, \lambda^{y_{n-r}})$ belongs to X_1, and collect those vectors for which the inclusion holds in a finite set $E \subseteq \mathbb{Z}^{n-r}$. If $E = \emptyset$ then clearly there are no solutions in $\varphi_A(X_1^\circ \times \mathbb{G}^r)$, otherwise the set $(E \times \mathbb{Z}^r) \cdot A$, is a finite union of sets of the form $V + \mathbf{h}$ where V is a linear subspace of $\mathbb{Q}^n$. When we intersect these translated subspaces with requirements that odd coordinates must be strictly positive and distinct, we get a set of linear (in)equalities, for which an integer solution $\mathbf{x}$ can be found using a variation of integer linear programming (see, e.g., [9]). If $\|\mathbf{x}\| > b_0$, then set $b_1 = \lceil \|\mathbf{x}\| \rceil$. In this way we have shown that if there is a point $(\lambda^{y_1}, \lambda^{-y_1}, \ldots, \lambda^{y_m}, \lambda^{-y_m})$ belonging either to X_0° or to $\varphi_A(X_1^\circ \times \mathbb{G}^r)$, then there is one with exponents $\mathbf{x}$ such that $\|\mathbf{x}\| \leq b_1$.

We then proceed recursively for $X_1^\bullet$ to construct the set $\mathcal{T}_{X_1}$, and repeat the process. Similarly for other tori in $\mathcal{T}_{X_0}$, either by showing that there are no solutions or computing bounds $b_2 < b_3 < \cdots < B$. The procedure terminates because in Lemma 20 the dimension of the subvariety X_1 is strictly smaller than that of X, and because the set of tori $\mathcal{T}_X$ in Lemma 19 is finite.

This concludes the proof of Lemma 15, and that of Theorem 2(ii).

Finally, let us briefly comment about why we are limited to rotations on the plane. If the given matrix is not a rotation, then the relevant points do not all belong to $\mathcal{H}_1$, but rather to $\mathcal{H}_2$, in subgroups of dimension 2. Intuitively this is because the matrix changes vectors over two dimensions: scaling and rotating. What we lack is an effective bound, akin to Theorem 22, for subgroups of dimension 2. There are finiteness results, often as special cases of the Mordell-Lang conjecture, see, e.g., [13], but to our knowledge, no effective bounds are known.

References

1. Shaull Almagor, Joël Ouaknine, and James Worrell. The semialgebraic orbit problem. In Rolf Niedermeier and Christophe Paul, editors, *36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019, March 13-16, 2019, Berlin, Germany*, volume 126 of *LIPIcs*, pages 6:1–6:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.STACS.2019.6.
2. Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry.* Number 4. Cambridge university press, 2007.
3. W. B. Brindza, A Pintér, and W. M. Schmidt. Multiplicities of binary recurrences. *Canadian Mathematical Bulletin*, 44(1):19–21, 2001.
4. J. W. S. Cassels. *An Introduction To Diophantine Approximation.* 1959.
5. L Cerlienco, M Mignotte, and F Piras. Linear recurrent sequences: algebraic and arithmetical properties. *Enseign. Math.(2)*, 33(1-2):67–108, 1987.
6. H. Derksen and D. Masser. Linear equations over multiplicative groups, recurrences, and mixing ii. *Indagationes Mathematicae*, 26(1):113–136, Jan 2015. URL: http://dx.doi.org/10.1016/j.indag.2014.08.002, doi:10.1016/j.indag.2014.08.002.
7. Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. Recurrence sequences, 2003. URL: http://dx.doi.org/10.1090/surv/104, doi:10.1090/surv/104.
8. Robin Hartshorne. *Algebraic Geometry.* 1977. doi:10.1007/978-1-4757-3849-0.
9. Rui-Juan Jing and Marc Moreno Maza. Computing the integer points of a polyhedron, i: algorithm. In *International Workshop on Computer Algebra in Scientific Computing*, pages 225–241. Springer, 2017.
10. James P. Jones. Universal diophantine equation. *The Journal of Symbolic Logic*, 47(3):549–571, 1982. URL: http://www.jstor.org/stable/2273588.
11. R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, 1986. doi:10.1145/6490.6496.
12. Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. *What's Decidable About Discrete Linear Dynamical Systems?*, pages 21–38. Springer Nature Switzerland, Cham, 2022. doi:10.1007/978-3-031-22337-2_2.
13. Michel Laurent. Equations diophantiennes exponentielles. *Inventiones mathematicae*, 78:299–327, 1984.
14. Andrzej Schinzel. *Polynomials with special regard to reducibility. With an Appendix by Umberto Zannier.*, volume 77. Cambridge University Press, 2000.
15. W.M. Schmidt. Heights of points on subvarieties of $\mathfrak{G}_m^n$. *Number Theory (Paris, 1993– 1994), London Math. Soc. Lecture Note Ser. 235*, pages 157–187, 1996.

A Missing Proofs

A *linear recurrence sequence* is a sequence $\langle u_n \rangle_{n\in\mathbb{N}}$ of rational numbers that satisfies a linear recurrence relation $u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$ for all $n > d$, where a_i are rational numbers. Here d is the order of the recurrence. We consider linear recurrence sequences and linear dynamical systems as interchangeable. Indeed if $M \in \mathbb{Q}^{d\times d}$ is a matrix with rational entries, and $1 \le i, j \le d$ then $\langle (M^n)_{i,j} \rangle_{n\in\mathbb{N}}$ satisfies a linear recurrence of order d and conversely every sequence satisfying an order-d linear recurrence admits such a matrix-power representation. A consequence of this fact is that if $\langle u_n \rangle_{n\in\mathbb{N}}$ and $\langle v_n \rangle_{n\in\mathbb{N}}$ are two linear recurrence sequences, then so is their pointwise sum $\langle u_n + v_n \rangle_{n\in\mathbb{N}}$ and pointwise product $\langle u_n \cdot v_n \rangle_{n\in\mathbb{N}}$. The *characteristic polynomial* of the above linear recurrence is $x^d - a_1 x^{d-1} - a_2 x^{d-2} - \cdots - a_d$. Denote by $\Lambda_1, \ldots, \Lambda_k$ the distinct roots of this polynomial and by $m_1, \ldots, m_k$ their respective multiplicities. A linear recurrence sequence $\langle u_n \rangle_{n\in\mathbb{N}}$ can also be written as a *generalized power sum* $u_n = \sum_{i=1}^k P_i(n)\ \Lambda_i^n$, where $P_i \in \overline{\mathbb{Q}}[n]$ are polynomials of degree at most $m_i - 1$

with algebraic coefficients. All such generalized power sums satisfy linear recurrence relations with algebraic coefficients.

▶ **Theorem 4.** *The full Reachability Problem reduces to the point-to-polytope variant.*

Proof. Suppose that we are given an instance of the Reachability Problem in dimension $d \in \mathbb{N}$, with source and target sets $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$, and matrix M. Denote by $\Phi_\mathbf{S}$, $\Phi_\mathbf{T}$, the formulas defining $\mathbf{S}$ and $\mathbf{T}$ respectively. Write $\mathbf{x}$ for the tuple of variables $(x_1, \dots, x_d)$ and A for the $d \times d$ matrix of variables $(A_{1,1}, \dots, A_{d,d})$, and define the formula: $\Gamma(\mathbf{x}, A) \stackrel{\text{def}}{=} \Phi_\mathbf{S}(\mathbf{x}) \wedge \Phi_\mathbf{T}(\mathbf{x} \cdot A)$.

The Reachability Problem asks whether there exists $\mathbf{p} \in \mathbb{R}^d$ and $n \in \mathbb{N}$ such that $\Gamma(\mathbf{p}, M^n)$ holds. Using quantifier elimination for the first-order theory of reals we obtain a quantifier-free formula $\Gamma'(A)$ that is equivalent to the projection $\exists \mathbf{x}\ \Gamma(\mathbf{x}, A)$. Now the reachability problem is equivalent to the question of whether there is some n such that $\Gamma'(M^n)$ holds. Since Γ' is quantifier-free, it can be written as a disjunction of formulas $\varphi_1, \dots, \varphi_m$, for some $m \in \mathbb{N}$, such that each φ_i is of the form (1). For each φ_i we construct an instance of the point-to-polytope reachability problem, with the property that $\varphi_i(M^n)$ holds for some n if and only if the respective polytope can be reached. To this end, let φ be one of the disjuncts, defined as:

$$P_0(A_{1,1}, \dots, A_{d,d}) = 0 \wedge \bigwedge_{i=1}^{k} P_i(A_{1,1}, \dots, A_{d,d}) > 0\,.$$

For all $i \in \{0, \dots, k\}$ define the linear recurrence sequence

$$u_{i,n} \stackrel{\text{def}}{=} P_i\left((M^n)_{1,1}, \dots, (M^n)_{d,d}\right),\ n \in \mathbb{N}.$$

Note that we can effectively construct a matrix N_i such that $u_{i,n} = (N_i)_{1,2}$.

Unravelling the definitions, we see that for all $n \in \mathbb{N}$, $\varphi(M^n)$ holds if and only if the upper-right corner of N_0^n is 0, and the upper-right corners of N_i^n, $1 \leq i \leq k$ are strictly positive. The latter can be interpreted as a point-to-polytope reachability problem as follows. Let $D := \sum d_i$, and construct a block diagonal matrix whose blocks are $N_0, \dots, N_k$, and whose size is $D \times D$. Then the equivalent instance of the point-to-polytope problem has as initial point $\mathbf{p}_0 := (1, \dots, 1) \in \mathbb{R}^D$, the matrix is N and the polytope is the intersection of the following halfspaces. The closed halfspaces characterised by the normal vectors $\Delta(d_0)$ and $-\Delta(d_0)$ (where by $\Delta(i) \in \mathbb{R}^D$ we denote the vector whose components are all zero except the component in position i whose value is 1), and the open halfspaces with normal vectors $\Delta(d_1), \dots, \Delta(d_k)$. ◀

The above proof idea does not appear to extend to Multiple Reachability. The critical difference is that after we obtain the projection Γ'. If there are two distinct integers n_1, n_2 such that $\Gamma'(M^{n_1})$ and $\Gamma'(M^{n_2})$ hold, it does not necessarily mean that there is a *single* $\mathbf{p}$ for which both $\Gamma(\mathbf{p}, M^{n_1})$ and $\Gamma(\mathbf{p}, M^{n_2})$ hold. Indeed, it is unlikely that such a reduction is possible for multiple reachability, in light of the result of the next section.

▶ **Lemma 6.** *Given $d \in \mathbb{N}$, write $\mathbf{h}_d := (1, 0, \dots, 0) \in \mathbb{R}^{d+1}$. Then there is a square matrix M_d of dimension $d+1$ such that for every polynomial $P \in \mathbb{Z}[x]$ of degree at most d we have*

$$\big(P(1), P(2), \dots, P(d+1)\big)\ M_d^n\ \mathbf{h}_d^\top = P(n), \qquad \text{for all } n \in \mathbb{N}.$$

Proof. Let P be a univariate polynomial of degree d. We claim that the unique sequence that satisfies the recurrence

$$\sum_{i=0}^{d+1} (-1)^i \binom{d+1}{i} v_{n-i} = 0, \qquad n > d+1. \tag{7}$$

and whose first $d+1$ entries are $P(1), P(2), \ldots, P(d+1)$ is the sequence $\langle P(n)\rangle_{n\in\mathbb{N}}$.

The proof of the claim is as follows. The characteristic polynomial of the recurrence (7) is $(x-1)^{d+1}$, as one can see by expanding the latter product using the Binomial theorem. In other words, the recurrence has a single characteristic root 1, with multipliciity $d+1$. It follows from standard results (see, e.g., [7, Section 1.1.6]) that the set of solutions of (7) is spanned by the $d+1$ sequences $\langle n^k\rangle_{n=0}^{\infty}$, where $k=0,\ldots,d$. Equivalently, a sequence $\langle v_n\rangle_{n=0}^{\infty}$ satisfies (7) if and only if for some polynomial $P(x)$ of degree at most d we have $v_n = P(n)$ for all $n\in\mathbb{N}$. For uniqueness, notice that if one fixes the $d+1$ first entries of a sequence, the remainder is determined from the recurrence relation of that order.

We next reformulate the claim in terms of matrix powers. Denote the $d+1$ coefficients of the recurrence (7) by

$$q_i \stackrel{\text{def}}{=} (-1)^{i+1}\binom{k+1}{i}, \qquad 1\le i\le d+1.$$

Let $\mathbf{h}_d := (1,0,\ldots,0)\in\mathbb{R}^{d+1}$ and define the matrix

$$M_d \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 & \cdots & 0 & q_{d+1} \\ 1 & 0 & \cdots & 0 & q_d \\ 0 & 1 & \cdots & 0 & q_{d-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & q_1 \end{pmatrix},$$

where the shaded block is the $d\times d$ identity matrix. It follows from the discussion above that for all univariate polynomials P of degree d, we have

$$\big(P(1), P(2), \ldots, P(d+1)\big)\; M_d^n\; \mathbf{h}_d^\top = P(n), \qquad \text{for all } n\in\mathbb{N}. \tag{8}$$

◀

▶ **Proposition 23.** *Problem 5 is undecidable.*

Proof. Recall that Hilbert's Tenth Problem is known to be undecidable even when the number of variables is fixed, equal to 9 [10]. In other words, there is no algorithm that decides whether a given polynomial with integer coefficients and nine variables has a zero in positive integers.

Now let $Q(x_1,\ldots,x_9)$ be an arbitrary polynomial with integer coefficients. For any partition $\mathcal{P}$ of $\{1,\ldots,9\}$, define $Q_{\mathcal{P}}$ to be the polynomial that one obtains by taking Q and for every $A\in\mathcal{P}$, replacing all variables x_i, for $i\in A$, by a single fresh variable x. It is plain that Q has a zero in positive integers $x_1,\ldots,x_9$ if and only if one of the polynomials $Q_{\mathcal{P}}$ has a zero in *distinct* positive integers. We conclude that Problem Proposition 23 is undecidable. ◀

▶ **Lemma 7.** *The following two statements are equivalent:*

- *The polynomial F has a solution in distinct positive integers.*
- *There is some $\mathbf{p} := (x_1,\ldots,x_{n+1},y_1,\ldots,y_n)\in\mathbf{S}$ and distinct positive integers $r_1,\ldots,r_n$ such that $\mathbf{p}\; M^{r_i}\; \mathbf{h}^\top = 0$, for $1\le i\le n$.*

Proof. ($\Rightarrow$) Let $y_1,\ldots,y_n$ be distinct positive integers comprising a root of F. Set $x_i := (i-y_1)(i-y_2)\cdots(i-y_n)$, for all $i\in\{1,\ldots,n+1\}$. Then $\mathbf{p} := (x_1,\ldots,x_{n+1},y_1,\ldots,y_n)\in S$

by definition. The definition of the matrix M above (that has nonzero entries only in the first $(n+1)\times(n+1)$ block) and (8) imply that for all $r \in \mathbb{N}$ we have

$$\mathbf{p}M^r\ \mathbf{h}^\top = (r-y_1)(r-y_2)\cdots(r-y_n). \tag{9}$$

Hence the second statement of the lemma holds for the distinct positive integers $r_i = y_i$.
($\Leftarrow$) Let $\mathbf{p}$ and distinct positive integers $r_1,\dots,r_n$ be such that the second statement holds. Then (9) implies that the tuple $(y_1,\dots,y_n)$ is a permutation of the tuple of distinct positive integers $(r_1,\dots,r_n)$. It then follows from the definition of S that the same permutation is also a root of F. ◀

▶ **Proposition 9.** *Let $\mathbf{p} \in \mathbb{R}^2$ be non-zero, h the line containing the origin and orthogonal to $\mathbf{h} \in \mathbb{R}^2$, and $M \in \mathbb{R}^{2\times 2}$ a nondegenerate matrix. If there are distinct positive integers $n, m \in \mathbb{N}$ such that both M^n and M^m map $\mathbf{p}$ into h, i.e.,*

$$\mathbf{p}M^n\mathbf{h}^\top = \mathbf{p}M^m\mathbf{h}^\top = 0, \tag{2}$$

then $\mathbf{p}M^k\mathbf{h}^\top = 0$ for all $k \in \mathbb{N}$. Moreover, in this case, either one of the eigenvalues of M is zero, or $M = \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$, for some $s \in \mathbb{R}$.

Proof. By assumption (2) the point $\mathbf{h}$ belongs to the two lines defined by $\mathbf{p}M^n$ and $\mathbf{p}M^m$, which pass through the origin. Since $\mathbf{h} \neq \mathbf{0}$, it follows that there is some $r \in \mathbb{R}$, $r \neq 0$, such that $r\mathbf{p}M^n = \mathbf{p}M^m$. If M is not invertible then one of the eigenvalues is 0, and by putting M into Jordan normal form, we can see that (2) cannot hold, unless M is the zero matrix, or the other eigenvalue is 1, in which case the conclusion holds. If M is invertible, $r\mathbf{p} = \mathbf{p}M^{m-n}$, so r is an eigenvalue of M^{m-n} and by nondegeneracy, the matrix M has eigenvalue $R := r^{1/(m-n)}$, which is real. The scaled matrix $\widetilde{M} = M/R$ has the property that for any $k \in \mathbb{N}$, $\widetilde{M}^k$ sends $\mathbf{p}$ to the line h if and only if M^k does as well. The matrix $\widetilde{M}$ has 1 as an eigenvalue, and for (2) to hold, $\widetilde{M}$ (and also M) has to be a stretching matrix, i.e., corresponding to multiplication by a scalar $s \in \mathbb{R}$. Consequently, $\mathbf{p}\mathbf{h}^\top = 0$ and hence $\mathbf{p}M^k\mathbf{h}^\top = \mathbf{p}s^k\mathbf{h}^\top = 0$ for all $k \in \mathbb{N}$. ◀

▶ **Lemma 11.** *Let M be as above, H a halfplane, $\mathbf{p} \in \mathbb{R}^2$ a point, and $\mathbf{p}_0, \mathbf{p}_1, \dots$ its orbit under M. The orbit can switch from H to $\mathbb{R}^2 \setminus H$, or conversely, at most twice. In particular, the orbit is either ultimately in H or ultimately in $\mathbb{R}^2 \setminus H$.*

Proof. We begin by observing that for all real numbers a_1, a_2, a_3, not all zero, and positive reals b_1, b_2, the function $f : \mathbb{R} \to \mathbb{R}$, defined as

$$x \mapsto a_1 b_1^x + a_2 b_2^x + a_3, \tag{10}$$

has at most two zeros. Indeed, since f is continuous, by Rolle's theorem, between any two zeros of f, f' has a zero. As a consequence, if f had more than two zeros, f' would have more than one zero. But since f' has the form $\alpha_1 b_1^x + \alpha_2 b_2^x$ for real numbers α_1, α_2, this is impossible.

Let c_1, c_2, c_3 be real numbers such that the point (x, y) belongs to the halfplane H if and only if $c_1 x + c_2 y + c_3 > 0$. The orbit of such a point under M is $(x\rho_1^n, y\rho_2^n)$. Consider now the expression

$$c_1 x \rho_1^n + c_2 y \rho_2^n + c_3. \tag{11}$$

From the observation about the zeros of (10) above, this expression as a function of n may change sign at most twice, which establishes the lemma. ◀

▶ **Proposition 12.** *For any $\mathbf{p} \in \mathbb{R}^2$, exactly one of the following holds:*

1. *There are infinitely many positive integers and infinitely many negative integers x such that $\mathbf{p}M^x \in \mathbf{T}$.*
2. *There are only finitely many positive integers and finitely many negative integers x such that $\mathbf{p}M^x \in \mathbf{T}$.*

Furthermore, we can decide whether there exists some $\mathbf{p} \in \mathbf{S}$ for which the first case holds.

Proof. If the target is of dimension ≤ 1, then by the Skolem-Mahler-Lech theorem for any $\mathbf{p} \in \mathbf{S}$, M^n sends $\mathbf{p}$ to $\mathbf{T}$ at most finitely many times. If the target has dimension 2, then using Tarski's algorithm we check whether there exists a circle, centered at the origin, of radius r such that (1) it intersects $\mathbf{S}$, and (2) writing its points in polar coordinates (r, θ), there exists $\theta_1 < \theta_2$ in $[0, 2\pi]$, such that for all θ in (θ_1, θ_2), the points (r, θ) are in $\mathbf{T}$.

If such a circle exists then an argument similar to that in the proof of Theorem 2(i) for complex eigenvalues can be used to show that there exists $\mathbf{p} \in \mathbf{S}$ whose orbit enters the target $\mathbf{T}$ infinitely often.

If no such circle exists then clearly all circles centered at the origin that intersect $\mathbf{S}$, intersect $\mathbf{T}$ at finitely many points, and therefore no orbit from $\mathbf{S}$ can hit the target infinitely often. ◀

▶ **Lemma 14.** *Let $\Lambda \subseteq \mathbb{Z}^m$ be a non-trivial additive subgroup such that for all $(x_1, \ldots, x_m) \in \Lambda$ we have $Q_0(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}) = 0$. Then there is no solution in Λ.*

Proof. Suppose that the subgroup Λ is given as the integer points in the kernel of a matrix A with integer entries, m rows, and $m' \leq m$ columns. We have: $\Lambda = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}\ A = \mathbf{0}\}$.

Denote by $\mathbb{T}$ the unit circle in the complex plane. We will write $\mathbf{z}$ for the vector $(z_1, \ldots, z_m)$ and for any vector $\mathbf{b} = (b_1, \ldots, b_m)$ of length m, we abbreviate $\mathbf{z}^{\mathbf{b}} = z_1^{b_1} \cdots z_m^{b_m}$. Denote by $\mathbf{a}_1, \ldots, \mathbf{a}_{m'}$ the columns of A, and define the following semialgebraic sets:

$$\mathbf{R} \stackrel{\text{def}}{=} \{\mathbf{z} \in \mathbb{T}^m : \mathbf{z}^{\mathbf{a}_i} = 1 \text{ for all } 1 \leq i \leq m'\},$$

$$\mathbf{R}' \stackrel{\text{def}}{=} \left\{\mathbf{z} \in \mathbf{R} : Q_i(z_1, z_1^{-1}, \ldots, z_m, z_m^{-1}) > 0 \text{ for all } 1 \leq i \leq \ell\right\}.$$

We are going to prove that $\mathbf{R}'$ is empty. Observe that this is sufficient to prove the lemma, for if there were a solution $(x_1, \ldots, x_m) \in \Lambda$, then $(\lambda^{x_1}, \ldots, \lambda^{x_m}) \in \mathbf{R}$, from the definition of the subgroup Λ and $\mathbf{R}$; and moreover, by definition of a solution, $(\lambda^{x_1}, \ldots, \lambda^{x_m})$ belongs to $\mathbf{R}'$.

We will prove that $\mathbf{R}' = \emptyset$ via the following claim:

▷ Claim 24. If $\mathbf{R}'$ is non-empty, there are infinitely many elements of $(x_1, \ldots, x_m) \in \Lambda$, for which $(\lambda^{x_1}, \ldots, \lambda^{x_m}) \in \mathbf{R}'$.

Indeed, if the claim holds, and $\mathbf{R}'$ is non-empty, there are infinitely many $(x_1, \ldots, x_m)$ for which $(\lambda^{x_1}, \ldots, \lambda^{x_m})$ is a zero of Q_0 and satisfies the polynomial inequalities $Q_i > 0$, for $1 \leq i \leq \ell$. This means that for infinitely many $(x_1, \ldots, x_m)$, the formula (5) holds which contradicts the assumption made in Assumption 13, namely that there can be only finitely many such tuples. It follows that $\mathbf{R}'$ is empty.

For the proof of the claim we will use the following theorem of Knonecker on Diophantine approximation [4, Theorem IV, Page 53]:

▶ **Theorem 25.** *For $1 \leq j \leq m$ let $L_j(\mathbf{y}) = L_j(y_1, \ldots, y_{m'})$ be m homogeneous linear forms in m' of variables y_i. Then the two following statements about a real vector $\alpha = (\alpha_1, \ldots, \alpha_m)$ are equivalent:*

1. *For all* $\epsilon > 0$ *there is an integral vector* $\mathbf{a} = (a_1, \ldots, a_{m'})$ *such that simultaneously*

$$|L_j(\mathbf{a}) - \alpha_j| < \epsilon, \quad 1 \le j \le m.$$

2. *If* $\mathbf{u} = (u_1, \ldots, u_m)$ *is any integral vector such that:* $u_1 L_1(\mathbf{y}) + \cdots + u_m L_m(\mathbf{y})$ *has integer coefficients, considered as a form in the indeterminates* y_i*, then* $u_1\alpha_1 + \cdots + u_m\alpha_m \in \mathbb{Z}$.

In order to apply this theorem, we define our linear forms L_i as follows. By putting A in a row-reduced echelon form, finding a basis and multiplying with a suitable scalar, we can compute a set of integral vectors $b_1, \ldots, b_{m'}$ that generate Λ. Write $\lambda = \exp(\vartheta 2\pi \mathbf{i})$, where the angle ϑ is not a rational number, because λ is not a root of 1. For $1 \le j \le m$ define:

$$L_j(y_1, \ldots, y_{m'}) \stackrel{\text{def}}{=} \sum_{i=1}^{m'} \vartheta \ b_{i,j} \ y_i.$$

Choose some element of $\zeta \in \mathbf{R}'$ and write it as:

$$\big(\exp(\alpha_1 2\pi\mathbf{i}), \ldots, \exp(\alpha_m 2\pi\mathbf{i})\big).$$

Let $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ be an integral vector such that $\sum u_i L_i(\mathbf{y})$ has integer coefficients, considered as a form in the indeterminates y_i. A small computation shows that since α is irrational, for such $\mathbf{u}$ we must have $\mathbf{u}\ B = \mathbf{0}$, where B is the matrix that has the vectors $b_1, \ldots, b_{m'}$ as columns. This means that such vectors $\mathbf{u}$ belong to the orthogonal complement of the linear subspace $V \subseteq \mathbb{R}^m$, spanned by $b_1, \ldots, b_{m'}$. By virtue of ζ belonging to $\mathbf{R}'$ and hence also $\mathbf{R}$, we have that $(\alpha_1, \ldots, \alpha_m)$ belongs to V, and consequently $\sum u_i \alpha_i = 0$. We have proved that Statement 2 in the above theorem holds for our real vector α. Applying the theorem gives us Statement 1, namely that there are integral vectors $\mathbf{a}$ that make $L_j(\mathbf{a})$ get arbitrarily close to α_j. As $\mathbf{a}$ ranges over $\mathbb{Z}^{m'}$, $(L_1(\mathbf{a}), \ldots, L_m(\mathbf{a}))$ range over $\vartheta\Lambda$, which in turn means that

$$(\lambda^{L_1(\mathbf{a})/\vartheta}, \ldots, \lambda^{L_m(\mathbf{a})/\vartheta}) \in \mathbf{R}, \tag{12}$$

and gets arbitrarily close to ζ. Finally, since $\mathbf{R}'$ is an open subset of $\mathbf{R}$, by choosing ϵ small enough, we get some $\mathbf{a}$ such that the tuple of (12) belongs to the subset $\mathbf{R}'$. The point ζ was chosen arbitrarily, so the infinitude of $(x_1, \ldots, x_m) \in \Lambda$ for which $(\lambda^{x_1}, \ldots, \lambda^{x_m})$ is in $\mathbf{R}'$ follows. This concludes the proof of Claim 24 and that of the lemma. ◀

▶ **Lemma 16.** *For all* $(a_1, \ldots, a_k) \in \mathbb{Z}^k$*, the point* $(\lambda^{a_1}, \ldots, \lambda^{a_k})$ *belongs to an algebraic subgroup of dimension 1.*

Proof. If all $a_i = 0$, then the lemma clearly holds, so suppose that there is some j such that $a_j \neq 0$. The tuple $(a_1, \ldots, a_k)$ belongs to the linear subspace that is defined by the linear equations:

$$a_i x_j - a_j x_i = 0, \qquad i \neq j, \text{ and } 1 \le i \le k.$$

These are $k - 1$ equations, defining a linear subspace V. It follows that $\Lambda := V \cap \mathbb{Z}^k$ is generated by a set of $k - 1$ vectors (and no smaller set). This in turn implies that the point in the statement of the lemma belongs to the algebraic subgroup H_Λ, which is a subgroup of dimension 1. ◀

▶ **Lemma 20.** *([2, Theorem 3.3.9]). Let $X \subseteq \mathbb{G}^n$ be a subvariety and H a linear torus of dimension $r \geq 1$. Then there exists a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$, which can be computed, such that*

$$\bigcup_{gH \subseteq X} gH = \varphi_A(X_1 \times \mathbb{G}^r),$$

where $X_1 \subseteq \mathbb{G}^{n-r}$ is a subvariety, whose defining polynomials can be computed.

Proof. Using Proposition 18 we can conclude that $H = H_\Lambda$ where Λ is a subgroup of $\mathbb{Z}^n$ of rank $n-r$, and from Proposition 17, we can compute a matrix A, such that $H = \varphi_A(\mathbf{1}_{n-r} \times \mathbb{G}^r)$. If we define $\widetilde{X}$ to be $\varphi_A^{-1}(X)$, we have

$$\bigcup_{gH \subseteq X} gH = \bigcup_{g \cdot (\mathbf{1}_{n-r} \times \mathbb{G}^r) \subseteq \widetilde{X}} g \cdot (\mathbf{1}_{n-r} \times \mathbb{G}^r).$$

Note that since A can be computed, so can the polynomials of $\widetilde{X}$. Let $f_1, \ldots, f_k$ be these defining polynomials of $\widetilde{X}$. Then $g \cdot (\mathbf{1}_{n-r} \times \mathbb{G}^r)$ being a subset of $\widetilde{X}$ means that

$$f_i(g_1, \ldots, g_{n-r}, y_{n-r+1}, \ldots, y_n) = 0, \qquad 1 \leq i \leq k,$$

are identically satisfied in $y_{n-r+1}, \ldots, y_n$. This is just a set of polynomial equations in indeterminates $g_1, \ldots, g_{n-r}$, i.e., a subvariety of $\mathbb{G}^{n-r}$, which we call X_1. So if $g \in X_1$, then $g \cdot (\mathbf{1}_{n-r} \times \mathbb{G}^r) \subseteq \widetilde{X}$, or equivalently $\varphi_A(g \cdot (\mathbf{1}_{n-r} \times \mathbb{G}^r)) \subseteq X$. The lemma follows. ◀

▶ **Lemma 21.** *Let $\mathbf{x} \in \mathbb{Z}^n$, and denote by $M = \max_j |x_j|$. Then*

$$Mh(\lambda) \leq h\big((\lambda^{x_1}, \ldots, \lambda^{x_n})\big) \leq 2Mh(\lambda).$$

Proof. By the definition of height and absolute value we have:

$$h\big((\lambda^{x_1}, \ldots, \lambda^{x_n})\big) = \sum_{v \in M_K} \max_j \log^+ |\lambda^{x_j}|_v = \sum_{v \in M_K} \max_j \log^+ |\lambda|_v^{x_j}.$$

Since for every absolute value $|\cdot|_v$, $|\lambda|_v |\lambda^{-1}|_v = 1$, it follows that

$$\sum_{v \in M_K} \max_j \log^+ |\lambda|_v^{x_j} \leq M(h(\lambda) + h(\lambda^{-1})),$$

and since $h(\alpha) = h(\alpha^{-1})$ for every algebraic number α (see [2, Lemma 1.5.18]), we get the upper bound. For the lower bound:

$$h\big((\lambda^{x_1}, \ldots, \lambda^{x_n})\big) \geq h(\lambda^M) = Mh(\lambda).$$

◀

B Missing cases for Theorem 2

- Diagonalisable M with a single negative eigenvalue.
Suppose that the matrix M is

$$M = \begin{pmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{pmatrix}$$

where $\rho_1 < 0$ and $\rho_2 > 0$. (We do not make any assumptions on $|\rho_1|$ and $|\rho_2|$.) Consider a starting point $(x, y) \in \mathbb{R}^2$ and a halfplane H defined by $c_1x + c_2y > c_3$. The orbit of (x, y) visits H at time n if

$$\begin{cases} c_1x|\rho_1|^n + c_2y\rho_2^n > c_3, & \text{n even}, \quad (13a) \\ -c_1x|\rho_1|^n + c_2y\rho_2^n > c_3, & \text{n odd}. \quad (13b) \end{cases}$$

Depending on the signs of x and y, one of the inequalities implies the other. Without loss of generality suppose (13a) implies (13b). By Lemma 11, the set of n satisfying (13a) forms an interval subset of $\mathbb{N}$. It follows that the gaps between two consecutive visits from (x, y) to H is at most 2.

- Diagonalisable M with two negative eigenvalues.

Next, suppose that $\rho_1 < 0$ and $\rho_2 < 0$. Clearly, for all $c_1, c_2, c_3 \in \mathbb{R}$ with $c_3 \leq 0$ and c_1, c_2 not both zero, the inequality $c_1\rho_1^n + c_2\rho_2^n > c_3$ has infinitely many solutions. We thus focus on the case that $c_3 > 0$. Here we prove that the gap between two consecutive visits of the orbit of $(x, y) \in \mathbb{R}^2$ to H is at most 3. To this end, let $(x, y) \in \mathbb{R}^2$, and define the function $F : \mathbb{R} \to \mathbb{R}$,

$$F(t) \stackrel{\text{def}}{=} c_1x|\rho_1|^t + c_2y|\rho_2|^t.$$

Then we have that for $n \in \mathbb{N}$,

$$c_1x\rho_1^n + c_2y\rho_2^n = \begin{cases} F(n) \text{ if } n \text{ is even}, \\ -F(n) \text{ if } n \text{ is odd}. \end{cases} \quad (14)$$

Assuming that c_1, c_2 and x, y are nonzero (otherwise we would have an even simpler case), and $\rho_1 \neq \rho_2$, we see that the function $F(t)$ is bounded for positive reals t if and only if $|\rho_1| \leq 1$ and $|\rho_2| \leq 1$. If $F(t)$ is unbounded, then from (14) we see that for any $(x, y) \in \mathbb{R}^2$ nonzero, the system enters the halfplane H infinitely many times.

If on the other hand $F(t)$ is bounded in $\mathbb{R}_+$ then the following two inequalities cannot hold simultaneously:

$$c_1x\rho_1 + c_2y\rho_2 < c_3$$
$$c_1x\rho_1^3 + c_2y\rho_2^3 > c_3.$$

Indeed, the two expressions on the left hand side have the same sign, however the second one is smaller in magnitude due to $|\rho_1| \leq 1$ and $|\rho_2| \leq 1$. The claim that the gaps between two consecutive visits from (x, y) to H is at most 2 follows.

- Non-diagonalisable M with a repeated eigenvalue.

A version of Lemma 11 also holds in case M has a repeated eigenvalue ρ. In this case, every orbit under M can switch from H to $\mathbb{R}^2 \setminus H$, or conversely, at most once. Indeed, by a change of basis, we can assume that M has the form

$$M = \begin{pmatrix} \rho & 1 \\ 0 & \rho \end{pmatrix}$$

Then the expression corresponding to (11) is

$$(nxc_2\rho^{-1} + c_2y + c_1x)\rho^n + c_3.$$

If $\rho > 0$, then it is clear that this expression can change sign at most once as n ranges over $\mathbb{N}$. If, on the other hand, $\rho < 0$, we can do a similar analysis as above. If $|\rho| > 1$ then the halfplane is entered infinitely often. If $|\rho| \leq 1$, we can prove, as we did above, that the gaps between two consecutive visits in H is at most 2.

- M with a zero eigenvalue.

This case is one-dimensional, and it can be shown directly that the orbit can switch from H to $\mathbb{R}^2 \setminus H$ (or vice versa) at most once.