# Multiple Reachability in Linear Dynamical Systems

Toghrul Karimov
*MPI for Software Systems*
Saarbrücken, Germany
toghs@mpi-sws.org

Edon Kelmendi
*Queen Mary University of London*
London, United Kingdom
e.kelmendi@qmul.ac.uk

Joël Ouaknine
*MPI for Software Systems*
Saarbrücken, Germany
joel@mpi-sws.org

James Worrell
*University of Oxford*
Oxford, United Kingdom
jbw@cs.ox.ac.uk

***Abstract*—We consider reachability problems for linear dynamical systems. In dimension $d$ these problems are 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 $d \in \{3, \ldots, 9\}$ 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 theorem in arithmetic geometry, due to Bombieri and Zannier, concerning intersections of algebraic subgroups with subvarieties.**

***Index Terms*—Linear dynamical systems, linear recurrence sequences, Skolem Problem**

## I. Introduction

A **linear dynamical system** in ambient dimension $d$ is specified by a $d\times d$ matrix $M \in \mathbb{Q}^{d\times d}$ with rational entries. We are interested in understanding and deciding properties of the system's **orbit** for initial points $\mathbf{p} \in \mathbb{Q}^d$, which is defined as:

$$\mathcal{O}_M(\mathbf{p}) \stackrel{\text{def}}{=} \{\mathbf{p}\ M^n \ : \ n \in \mathbb{N}\}\,.$$

These are one of the simplest dynamical systems that we do not yet fully understand. They have been extensively studied for almost a hundred years. The motivations vary from finding solutions to Diophantine equations in number theory, to deciding linear loop termination in computer science, model checking simple programs *etc.* The text [Everest et al.(2003)] is the principal introduction to linear dynamical systems, featuring the main theorems as well as a number of applications. See also [Karimov et al.(2022)] for a recent survey.

The core property we are interested in is *reachability*: does the orbit reach some target set? More precisely, a general phrasing of the **Reachability Problem** is the following. We are given respective source and target semialgebraic sets (defined by boolean combinations of polynomial inequalities) $\mathbf{S}, \mathbf{T} \subset \mathbb{R}^d$, and a matrix $M \in \mathbb{Q}^{d\times d}$. The task is to decide whether there exists some point in the source set $\mathbf{p} \in \mathbf{S}$, whose orbit under $M$ intersects the target set. In other words, does there exist $\mathbf{p} \in \mathbf{S}$ such that

$$\mathcal{O}_M(\mathbf{p}) \cap \mathbf{T} \neq \emptyset?$$

A celebrated paper of Kannan and Lipton [Kannan and Lipton(1986)] 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 current state of the art (see [Almagor et al.(2019)]) 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 II.3 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 the **Multiple Reachability Problem**. This is a generalisation that does not merely ask whether the orbit intersects the target set, but rather whether it intersects it in at least $m$ points where $m \in \mathbb{N}$ is part of the input. More precisely, we are given semialgebraic sets $\mathbf{S}, \mathbf{T} \subset \mathbb{R}^d$, a matrix $M \in \mathbb{Q}^{d\times d}$, as well as a positive integer $m \in \mathbb{N}$. The task is to decide if there is a point in the source set $\mathbf{p} \in \mathbf{S}$ such that

$$|\mathcal{O}_M(\mathbf{p}) \cap \mathbf{T}| \geq m.$$

**Example I.0.1.** *Here is a simple example:*

$$\mathbf{S} = \left\{(x, y) \in \mathbb{R}^2 \ : \ y = x^2\right\},$$
$$\mathbf{T} = \left\{(x, y) \in \mathbb{R}^2 \ : \ x < y < -100\right\},$$
$$M = \begin{pmatrix} 2 & 0 \\ 0 & -10/9 \end{pmatrix}, \text{ and } m = 5.$$

Toghrul Karimov and Joël Ouaknine were supported by DFG grant 389792660 as part of TRR 248 (see https://perspicuous-computing.science). Joël Ouaknine was supported by the European Research Council under Grant Agreement 101167561 (ERC Synergy Grant DynAMiCs), and is also affiliated with Keble College, Oxford as `emmy.network` Fellow. James Worrell was supported by EPSRC Fellowship EP/N008197/1.

*The answer to the multiple reachability problem for this instance is* yes. *Since the linear map given by the matrix $M$ is particularly simple we can see the answer at once. Choose a point in* $\mathbf{S}$ *that is also in the second quadrant,* e.g. $\mathbf{p} := (-1, 1)$. *Observe that multiplication with $M^{2k+1}$, $k \in \mathbb{N}$, sends* $\mathbf{p}$ *to the fourth quadrant ($x < 0$ and $y < 0$), and the relation $x < y$ is invariant under this multiplication. Finally, from $\det M > 1$ it is clear that the orbit of* $\mathbf{p}$ *under $M$ enters the target set* $\mathbf{T}$ *at least $m = 5$ times. Indeed it enters the target infinitely often.*

What is the difference between the Reachability and Multiple Reachability problems? Our first observation is that, surprisingly, the Multiple Reachability Problem is computationally much more difficult than (single) Reachability.

### A. Contributions

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

This is in stark contrast to 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-polytope variant.

Intuitively, the lack of natural undecidable variants for reachability is because there is a single deterministic rule that governs the dynamics of the system. In other words, these are programs without conditionals. In dynamical systems which have some non-determinism, *i.e.* when the dynamics is governed by at least two maps, undecidable problems abound. For example, emptiness of probabilistic automata [Gimbert and Oualhadj(2010)] can be seen as a point-to-halfspace reachability problem, but where we have at least two linear maps $M_1$, $M_2$ at our disposal, to move the point to the target. The choice between the two dynamics is used to simulate a Turing machine. We have to proceed differently for the proof of Theorem I.1. We reduce from a variant of Hilbert's tenth problem. The instances are encoded in the source set $\mathbf{S} \subseteq \mathbb{R}^d$, so that points $\mathbf{p} \in \mathbf{S}$ contain some *real* solution to the given polynomial. Afterwards, the matrix $M$ is constructed in such a way that the orbit of $\mathbf{p}$ under $M$ reaches some hyperplane if and only if the coordinates of $\mathbf{p}$ are distinct natural numbers. This last step is made possible by the fact that every univariate polynomial of degree $d$ satisfies the same linear recurrence relation. In the reduction the matrix $M$ is not diagonalisable, and the proof would not work if we restricted $M$ to be diagonalisable.

Hilbert's tenth problem is undecidable for 9 variables, and consequently our reduction implies that multiple reachability with algebraic initial and hyperplane target sets is undecidable in dimension $d = 19$ for fixed $m = 9$. Similarly, for semialgebraic initial and hyperplane target sets undecidability follows in dimension $d = 10$. More generally, decidability of the Multiple Reachability Problem in dimension $d$ would give us algorithms to solve Diophantine equations in $d-1$ variables, which is open and considered very difficult already for $d = 3$. For $d \geq 4$, it is conceivable that whether a solution exists might even be undecidable. Indeed, effectively solving Thue equations (homogeneous equations in two variables) was only possible after Baker's work on linear forms in logarithms in 1966; See, for example, [Waldschmidt(2020)]. Therefore, we focus our search for positive results on the two-dimensional affine plane $\mathbb{R}^2$. Here we show:

**Theorem I.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 I.2(i) is proved using Kronecker's Theorem on Diophantine approximation and quantifier-elimination for the first-order theory of real-closed fields. Theorem I.2(ii), is the main contribution of the present paper.

Most decidability results about linear dynamical systems are proved using Baker's effective bounds on linear forms in logarithms. For the proof of Theorem I.2(ii), we make 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.

### B. Theorem I.2(ii) Proof and Algorithm Overview

We reduce to the following natural problem: Given a semialgebraic[1] set $\mathbf{T} \subset \mathbb{C}^k$, and an algebraic number $\lambda$ with $|\lambda| = 1$, decide whether the intersection of

$$\{(\lambda^{x_1}, \ldots, \lambda^{x_k}) \ : \ x_1 \ldots, x_k \text{ distinct positive integers}\} \quad (1)$$

with $\mathbf{T}$ is empty. To prove that this problem is decidable, we give a procedure for solving systems of polynomial (in)equalities in powers of an algebraic number $\lambda$ which is in the unit circle.

Every point in the set of powers of $\lambda$ in (1) belongs to an algebraic group of dimension 1. Algebraic groups are algebraic sets, *i.e.* solutions to a system of polynomial equations, that have a group structure. In our case the group operation is component-wise multiplication. Intuitively, the dimension is 1 because we have only one algebraic number $\lambda$ and it lies on the unit circle. On the other hand, the semialgebraic set $\mathbf{T}$ can be assumed to be the intersection of an algebraic set, or variety, $X$, and another open semialgebraic set that is specified as an intersection of strict polynomial inequalities.

There are a number of conjectures and results, variants of Mordell-Lang, that roughly say: if the intersection between an algebraic group of low dimension and a variety is *large* then there must be some simple algebraic reason for this. See the book [Zannier(2012)] by Zannier for an overview of this

[1]Here we mean that the image of $T$ under the map $f\colon \mathbb{C}^k \to \mathbb{R}^{2k}$ that extracts real and imaginary parts of coordinates is semialgebraic.

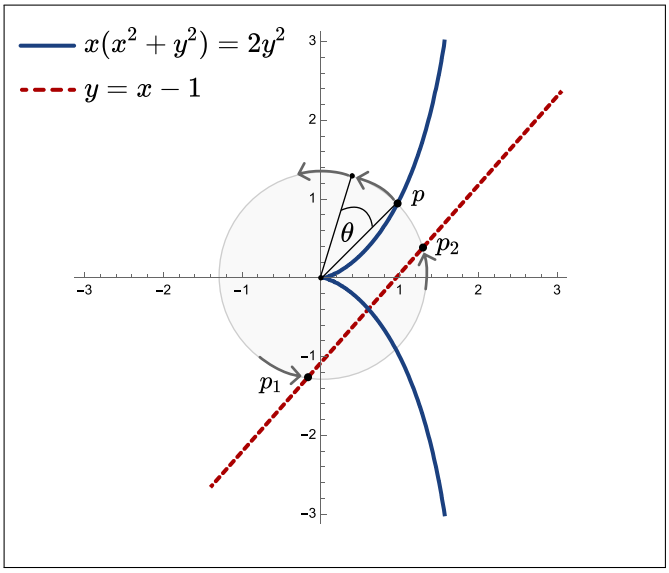
theme. The salient result for us is by Bombieri and Zannier, that can be found in the appendix of [Schinzel(2000)]. This theorem says that there is a partition of any variety $X$ into $X = X^\circ \cup X^\bullet$ such that the intersection of $X^\circ$ with the union of all groups of dimension 1 has bounded Weil height; moreover, inspecting the proof, one sees that the bound is effective by inspecting the proof. This upper bound directly translates to a bound on $x_i$ in the intersection (1). Further results by Bombieri, Schmidt, Zannier and others are used for computing the defining equations of the set $X^\bullet$, which contains all solutions that are degenerate in some sense.

The algorithm computes the description of the subset $X^\bullet$ as the set of common zeros of finitely many polynomials, as well as the bound on the exponents $x_i$ of $\lambda$. It then checks finitely many tuples $(x_1, \ldots, x_k)$ to see whether they form a solution. These tests use Tarski's algorithm for quantifier elimination in real closed fields as a subroutine.

### C. Example

Here is a slightly more complex example, which also highlights the connection to program analysis. Consider the following program:

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




The curly brace on the left of the two assignments signifies that they are simultaneous. Does this program terminate? More precisely, is there some initialisation of the variables $x, y \in \mathbb{R}$ such that they satisfy the polynomial relation[2]

$$x^3 + xy^2 = 2y^2, \tag{2}$$

and for which the program terminates? Let us reinterpret this question as follows. First we notice that the vector $(x, y)$ is being updated with the matrix

$$\begin{pmatrix} 4/5 & 3/5 \\ -3/5 & 4/5 \end{pmatrix},$$

which has the property that for all $n \in \mathbb{N}$ and $\theta = -\cos^{-1}(4/5)$:

$$\begin{pmatrix} 4/5 & 3/5 \\ -3/5 & 4/5 \end{pmatrix}^n = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix}.$$

We see that with every loop iteration, the updates rotate the point $(x, y)$ by the angle $\theta$ on the affine plane. So the question of the termination of the program above is the question of whether there is some point $\mathbf{p}$ in the cissoid defined above, that can be rotated into at least two points of the line $y = x-1$.

The algorithms we present in this paper can be used to answer questions like the above (and more). In this example, the answer turns out to be negative; there are no points in the cissoid that can be rotated by $\theta$ to two different points on the line. Therefore, if the variables $x, y$ are initialised such that they satisfy the polynomial (2), the procedure above does not terminate.

### D. Related Work

Effective procedures for reachability in linear dynamical systems have been investigated for a long time. There are various partial results. A brief survey of the state of the art can be found in [Karimov et al.(2022)].

Directly related to the present paper, the semialgebraic-to-semialgebraic (single) reachability problem was assiduously studied in [Almagor et al.(2019)]. There, this decision problem is shown decidable when the dimension is 3, using Baker's effective estimates. Furthermore, [Almagor et al.(2019)] shows by way of hardness that an algorithm for deciding this problem in dimension 4 would entail the ability to effectively estimate Lagrange constants of certain transcendental numbers. The proof of Theorem II.3 appears implicitly in [Almagor et al.(2019), Theorem 11].

More 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 non-degenerate linear recurrence sequence $\langle u_n \rangle_{n \in \mathbb{N}}$, there are only finitely many $n$ for which $u_n = k$. Thus one can ask what is the largest such number of $n$ one can have when $\langle u_n \rangle_{n \in \mathbb{N}}$ ranges over non-degenerate linear recurrence sequences of a certain order. Equivalently, what is the largest number of times a non-degenerate linear dynamical system from a singleton source hits a hyperplane target? There are many interesting and deep answers to this question, see [Everest et al.(2003), Chapter 2.2] and references therein.

[2]This curve is the *cissoid of Diocles*, discovered around 180 BC. See [Lockwood(1967), Chapter 15].

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 [Cerlienco et al.(1987)]. The conjecture was proved by Derksen and Masser a few years ago in [Derksen and Masser(2015)], 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.

## II. Definitions and Basic Properties

We define the natural numbers as the set $\mathbb{N} = \{1, 2, 3, \ldots\}$. Atomic formulas of the **first-order logic of reals** are propositions of the type:

$$P(x_1, \ldots, x_n) > 0,$$

where $x_1, \ldots, x_n$ are first-order variables ranging over $\mathbb{R}$, and $P \in \mathbb{Z}[x_1, \ldots, x_n]$ is a polynomial with integer coefficients. Atomic propositions can be combined with Boolean connectives, and we can also quantify over the set of real numbers. This logic admits effective quantifier elimination via Tarski's algorithm [Tarski(1951)]. This means that given a formula:

$$\exists x_0 \ \Phi(x_0, x_1, \ldots, x_n),$$

there is an equivalent quantifier-free formula $\Gamma(x_1, \ldots, x_n)$ that can be effectively computed. In particular, given a sentence (*i.e.* a formula with no free variables), Tarski's procedure can be used to decide whether the sentence is true for real numbers.

Subsets $\mathbf{S} \subseteq \mathbb{R}^d$ that can be expressed using formulas in the logic described above, that is

$$\mathbf{S} = \left\{ (x_1, \ldots, x_d) \in \mathbb{R}^d \ : \ \Phi(x_1, \ldots, x_d) \right\},$$

for some formula $\Phi$, are called **semialgebraic**. Due to quantifier elimination, semialgebraic sets are exactly the sets $\mathbf{S} \subseteq \mathbb{R}^d$ that can be written as finite unions of sets of tuples $(x_1, \ldots, x_d) \in \mathbb{R}^d$ that satisfy simultaneously

$$\begin{cases} P_0(x_1, \ldots, x_d) & = 0, \\ P_1(x_1, \ldots, x_d) & > 0, \\ \vdots & \\ P_k(x_1, \ldots, x_d) & > 0, \end{cases} \tag{3}$$

where $P_i \in \mathbb{Z}[x_1, \ldots, x_d]$. We only need one equality because the intersection of real zeros of polynomials $P$ and $Q$ is exactly the set of real zeros of the polynomial $P^2 + Q^2$. In this setting, an **algebraic set** is the set of zeros of a polynomial with integer coefficients. A **hyperplane** is the set of solutions of an affine equation, *i.e.* $(x_1, \ldots, x_d) \in \mathbb{R}^d$ for which

$$a_1 x_1 + \cdots + a_d x_d + a_{d+1} = 0,$$

where $a_i$ are integers. A **halfspace** is the set of solutions of an affine *inequality*, and a **polytope** is the intersection of finitely many halfspaces. On $\mathbb{R}^2$, a hyperplane is just a **line**, and a halfspace is called a **halfplane**. Finally, when discussing semialgebraicity for subsets of $\mathbb{C}^d$, we identify the latter with $\mathbb{R}^{2d}$ by taking real and imaginary parts.

A **linear recurrence sequence** is a sequence $\langle u_n \rangle_{n\in\mathbb{N}}$ of rational numbers that satisfies a linear recurrence relation

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}, \tag{4}$$

for all $n > d$, where $a_i$ are rational numbers. The smallest positive number $d$ for which the sequence satisfies (4) is called the **order** of the sequence. A **linear dynamical system** evolves according to the map $x \mapsto Mx$ for $M \in \mathbb{Q}^{d\times d}$. Linear recurrence sequences and linear dynamical systems are essentially the same object, as summarised in the two following propositions.

**Proposition II.1.** *Let $\langle u_n \rangle_{n\in\mathbb{N}}$ be a linear recurrence sequence of order $d$. Then there exists $M \in \mathbb{Q}^{d\times d}$ such that*

$$u_n = (M^n)_{1,d} \text{ for all } n \in \mathbb{N}.$$

**Proposition II.2.** *Let $M \in \mathbb{Q}^{d\times d}$ and $1 \leq i, j \leq d$. Then*

$$\langle (M^n)_{i,j} \rangle_{n\in\mathbb{N}}$$

*is a linear recurrence sequence of order at most $d$.*

The proof of Theorem II.1 is elementary, and Theorem II.2 follows from the Cayley-Hamilton theorem; See [Everest et al.(2003), Chapter 1] for more details. Furthermore, both propositions are effective.

The **characteristic polynomial** of the linear recurrence (4) 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**, which is an expression of the form

$$u_n = \sum_{i=1}^{k} P_i(n) \ \Lambda_i^n,$$

where $P_i \in \overline{\mathbb{Q}}[n]$ are polynomials of degree at most $m_i - 1$. Furthermore, all generalized power sums satisfy linear recurrence relations with algebraic coefficients. A consequence of this fact is that linear recurrence sequences are closed under addition and product. More precisely, 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 are the sequences $\langle u_n + v_n \rangle_{n\in\mathbb{N}}$ and $\langle u_n \cdot v_n \rangle_{n\in\mathbb{N}}$.

These are all the necessary facts required to prove the following:

**Theorem II.3.** *The general Reachability Problem reduces to the point-to-polytope variant.*

The main idea appears implicitly in the proof of [Almagor et al.(2019), Theorem 11].

*Proof.* Suppose that we are given an instance of the semialgebraic to semialgebraic reachability problem. Let $d \in \mathbb{N}$ be the dimension of its ambient space, $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$ be the source and target sets respectively, and $M$ be the given matrix. Denote by $\Phi_{\mathbf{S}}$, $\Phi_{\mathbf{T}}$, the formulas defining the respective sets $\mathbf{S}, \mathbf{T}$. Write $\mathbf{x}$ for the tuple of variables $(x_1, \ldots, x_d)$ and $A$ for the $d \times d$ matrix of variables $(A_{1,1}, \ldots, A_{d,d})$, and define the formula

$$\Gamma(\mathbf{x}, A) \stackrel{\text{def}}{=} \Phi_{\mathbf{S}}(\mathbf{x}) \text{ and } \Phi_{\mathbf{T}}(\mathbf{x} \cdot A).$$

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. Since the first-order theory of reals admits effective quantifier elimination, we first use Tarski's algorithm to produce a quantifier-free formula $\Gamma'(A)$, which is equivalent to the projection $\exists \mathbf{x}\ \Gamma(\mathbf{x}, A)$. Now the reachability problem is equivalent to the question of whether there exists some $n$ such that $\Gamma'(M^n)$ holds. Since $\Gamma'$ is quantifier-free, it can be written as a disjunction of formulas $\varphi_1, \ldots, \varphi_m$, for some $m \in \mathbb{N}$, such that each $\phi_i$ is of the form (3). It suffices to construct, for each $\varphi_i$, 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 is reached from some point in $\mathbf{S}$. We can then take the union of these polytopes as the single polytopic target. Let $\varphi$ be one of the disjuncts, written in the form

$$\bigwedge \begin{cases} P_0(A_{1,1}, \ldots, A_{d,d}) & = 0, \\ P_1(A_{1,1}, \ldots, A_{d,d}) & > 0, \\ \vdots & \\ P_k(A_{1,1}, \ldots, A_{d,d}) & > 0. \end{cases}$$

Define for $i \in \{0, \ldots, k\}$ the sequences

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

It follows from Theorem II.2 and the closure of linear recurrence sequences under component-wise addition and multiplication, that all the sequences $\langle u_{i,n} \rangle_{n \in \mathbb{N}}$ are themselves linear recurrence sequences. Write $d_i$ for the order of $\langle u_{i,n} \rangle_{n \in \mathbb{N}}$. Applying Theorem II.1 we construct matrices $N_i$ of size $d_i \times d_i$ for $0 \leq i \leq k$, with the property that the upper-right corner of $N_i^n$ is equal to $u_{i,n}$.

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 $N_0, \ldots, N_k$, and whose size is $D \times D$. Then the equivalent instance of the point-to-polytope problem has as initial point $\mathbf{p}_0 := (1, \ldots, 1) \in \mathbb{R}^D$, the matrix is $N$ and the polytope is the intersection of the following halfspaces. The closed halfspaces are 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 $\Delta(d_1), \ldots, \Delta(d_k)$. □

Why does a similar proof not work for multiple reachability? The critical difference occurs after we obtain the projection $\Gamma'$. 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.

## III. Hilbert's Tenth Problem and Linear Dynamical Systems

In this section we prove the undecidability of the multiple reachability problem, with algebraic starting sets and hyperplane targets, by reducing from a variant of Hilbert's tenth problem.[3] The variant that we reduce from is the following:

**Problem III.1.** *Given a polynomial $P(x_1, \ldots, x_k)$ with integer coefficients, decide whether there are distinct positive integers $n_1, n_2, \ldots, n_k$ such that*

$$P(n_1, \ldots, n_k) = 0.$$

**Proposition III.2.** *Theorem III.1 is undecidable.*

*Proof.* Let $Q(x_1, \ldots, x_n)$ be an arbitrary polynomial with integer coefficients. For any partition $\mathcal{P}$ of $\{1, \ldots, n\}$, define $Q_{\mathcal{P}}$ to be the polynomial obtained by taking $Q$ and for every $A \in \mathcal{P}$ replacing all variables $x_i$, for $i \in A$, by a single fresh variable. Clearly $Q$ has a zero in positive integers $x_1, \ldots, x_n$ if and only if one of the polynomials $Q_{\mathcal{P}}$ has a zero in *distinct* positive integers. Since Hilbert's tenth problem is undecidable (*i.e.* there is no procedure that can decide whether a given polynomial has a zero in positive integers, see [Davis et al.(1976), Chapter 5]), it follows that Theorem III.1 is also undecidable. □

Hilbert's tenth problem is known to be undecidable even when the number of variables is fixed, equal to 9. As a consequence of the proof above we have the following corollary.

**Proposition III.3** ( [Jones(1982)]). *Theorem III.1 is undecidable for fixed $k = 9$.*

We will now show that Theorem III.1 can be reduced to the multiple reachability problem. This comprises two steps. First we prove that all univariate polynomials of degree $d$ satisfy the same linear recurrence relation, which is then turned into a matrix form. In the second step we construct a certain algebraic set from the polynomial of Theorem III.1.

[3] A sketch of this proof has already appeared in [Karimov et al.(2022)].

**Lemma III.4.** *Let $P$ be a univariate polynomial of degree $d$. The unique sequence $\langle v_n \rangle_{n\in\mathbb{N}}$ that satisfies the recurrence*

$$\sum_{i=0}^{d+1}(-1)^i\binom{d+1}{i}v_{n-i}=0, \qquad n>d+1. \tag{5}$$

*and whose first $d+1$ entries are $P(1),P(2),\ldots,P(d+1)$ is the sequence*

$$\langle P(n)\rangle_{n\in\mathbb{N}}.$$

*Proof.* Let $P$ be a univariate polynomial of degree $d$. We prove that the sequence $\langle P(n)\rangle_{n\in\mathbb{N}}$ satisfies the recurrence relation (5). This suffices because any sequence satisfying a recurrence relation of order $d+1$ is determined by its first $d+1$ terms.

Define the discrete difference operator $\Delta : \mathbb{Z}[x]\to\mathbb{Z}[x]$ by

$$(\Delta f)(x) \stackrel{\text{def}}{=} f(x)-f(x+1).$$

Note that $\Delta$ is linear and that $\Delta f$ has degree at most $\deg(f)-1$. It follows that $\Delta^{d+1}P=0$, since $P$ has degree $d$. We establish the identity

$$(\Delta^k P)(x)=\sum_{i=0}^{k}(-1)^i\binom{k}{i}P(x+1), \tag{6}$$

by induction on $k$. The base case is evident, for the induction step we proceed as follows. Using the linearity of $\Delta$ we have:

$$(\Delta^{k+1}P)(x)=\sum_{i=0}^{k}(-1)^i\binom{k}{i}\left(P(x+i)-P(x+i+1)\right)$$

Taking out the first and last term, splitting the sum and shifting the index by one, it is possible to write the right hand side of the equation above as:

$$\begin{aligned}&P(x)+(-1)^{k+1}P(x+k+1)\\&+\sum_{i=1}^{k}(-1)^i\left(\binom{k}{i}+\binom{k}{i+1}\right)P(x+i).\end{aligned}$$

Using a binomial identity now we can finish the proof by writing the above as

$$\begin{aligned}&P(x)+(-1)^{k+1}P(x+k+1)+\sum_{i=1}^{k}(-1)^i\binom{k+1}{i}P(x+i)\\&=\sum_{i=0}^{k+1}(-1)^i\binom{k+1}{i}P(x+i).\end{aligned}$$

Thus we have the identity (6), which when instantiated for $k=d+1$ proves that the sequence $\langle P(n)\rangle_{n\in\mathbb{N}}$ satisfies the recurrence relation (5). □

Let us turn the statement of the above lemma into matrix form. To this end let $d\in\mathbb{N}$ be a natural number. Denote the $d+1$ coefficients of the recurrence (5) 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 $d$, and all $n\in\mathbb{N}$, we have

$$\big(P(1),P(2),\ldots,P(d+1)\big)\ M_d^n\ \mathbf{h}_d^\top = P(n). \tag{7}$$

To reduce the variant of Hilbert's tenth problem to the algebraic-to-hyperplane multiple reachability, we proceed as follows. Let $F\in\mathbb{Z}[y_1,\ldots,y_n]$ be an arbitrary polynomial with integer coefficients. We define an algebraic set $S\subseteq\mathbb{R}^{2n+1}$ as:

$$\begin{aligned}&(x_1,\ldots,x_{n+1},y_1,\ldots,y_n)\in S \Leftrightarrow\\&\bigwedge\begin{cases}F(y_1,\ldots,y_n)=0,\\ x_1=(1-y_1)(1-y_2)\cdots(1-y_n),\\ x_2=(2-y_1)(2-y_2)\cdots(2-y_n),\\ \vdots\\ x_{n+1}=(n+1-y_1)(n+1-y_2)\cdots(n+1-y_n).\end{cases}\end{aligned}$$

The idea is that to check whether a root $(y_1,\ldots,y_n)$ of $F$ is in $\mathbb{N}^n$, we need only check that the sequence $(m-y_1)\cdots(m-y_n)$, $m\in\mathbb{N}$, has $n$ zeros. More precisely, denote by $M$ the $(2n+1)\times(2n+1)$ matrix whose first $(n+1)\times(n+1)$ block is equal to $M_n$ and the other entries are 0, and set $\mathbf{h}:=\mathbf{h}_{2n}$.

**Lemma III.5.** *The following two statements are equivalent:*

- *The polynomial $F$ has a root consisting of distinct positive integers.*
- *There is some $\mathbf{p}:=(x_1,\ldots,x_{n+1},y_1,\ldots,y_n)\in S$ and distinct positive integers $r_1,\ldots,r_n$ such that*

$$\mathbf{p}\ M^{r_i}\ \mathbf{h}^\top = 0, \qquad 1\le i\le n.$$

*Proof.* ($\Rightarrow$) Let $y_1,\ldots,y_n$ be distinct positive integers that are 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 (7) imply that for all $r\in\mathbb{N}$ we have

$$\mathbf{p}\ M^r\ \mathbf{h}^\top = (r-y_1)(r-y_2)\cdots(r-y_n). \tag{8}$$

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 $r_1,\ldots,r_n$ be such that the second statement holds. Then (8) implies that the tuple $(y_1,\ldots,y_n)$ is a permutation of the tuple of distinct positive

integers $(r_1, \ldots, r_n)$. It then follows from the definition of $S$ that the same permutation is also a root of $F$. □

Theorem III.2 and Theorem III.5 imply that algebraic-to-hyperplane multiple reachability is undecidable, *i.e.* Theorem I.1. Indeed the set $S$ defined above is algebraic,[4] and $\mathbf{h}$ is the normal vector of some hyperplane (recall that a point $\mathbf{x}$ is on the hyperplane with a normal vector $\mathbf{h}$ if and only if $\mathbf{x} \cdot \mathbf{h}^\top = 0$).

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 $S$ 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. In light of Theorem III.3, we have the following theorem.

**Theorem III.6.** *Algebraic-to-hyperplane multiple reachability is undecidable in dimension* 19*, and semialgebraic-to-hyperplane multiple reachability is undecidable in dimension* 10*.*

Effectively solving Diophantine equations is notoriously difficult. Even Thue equations, *i.e.* equations of the type $P(\mathbf{x}) = m$ where $P$ is a homogeneous polynomial, could only be solved effectively in the second half of the twentieth century, after the work of Alan Baker [Baker(1990), Theorem 4.1]. As a consequence, in the next section, we focus our efforts in understanding the multiple reachability problem on the affine plane, *i.e.* when the dimension is fixed at $d = 2$. As we shall see, even on the plane, multiple reachability can be quite challenging.

In the undecidability proof of this section, the matrix $M$ is not diagonalisable. It is interesting to explore the multiple reachability problem for diagonalisable matrices, as the latter is a property that holds for generic matrices. This is at least as hard as the Positivity Problem for diagonalisable linear recurrence sequences.

## IV. Algorithms on the Affine Plane

This section is devoted to the proof of Theorem I.2. The dimension $d = 2$ is fixed. The system is given in the form of a $2 \times 2$ matrix with rational entries. The eigenvalues of such a matrix have one of the following forms: (a) a pair of complex conjugates $\lambda, \overline{\lambda} \in \overline{\mathbb{Q}}$, (b) two real roots $\rho_1, \rho_2 \in \overline{\mathbb{Q}} \cap \mathbb{R}$, or (c) a repeated real root $\rho \in \overline{\mathbb{Q}} \cap \mathbb{R}$. When the eigenvalues are a pair of complex conjugates and $|\lambda| = 1$ we say that the matrix is a **rotation**.

Theorem I.2 consists of two statements. The first statement, Theorem I.2(i), restricts targets to halfspaces (whereas the matrix is arbitrary), and its proof is postponed to Section A. The second statement, Theorem I.2(ii), restricts the matrix to rotations (whereas the target is arbitrary), and what follows is its proof.

### A. Rotations

We will first give the simple reduction to solving systems of polynomial inequalities in powers of some $\lambda$, as discussed in the introduction, followed by a proof overview.

*1) Reduction:* Let $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^2$ be the source and target semialgebraic sets, given by the formulas $\Phi_{\mathbf{S}}, \Phi_{\mathbf{T}}$ of first-order logic of reals. Further let $M$ be a matrix whose eigenvalues are the pair $\lambda, \overline{\lambda}$ on the unit circle, that is $|\lambda| = 1$, and let $m \in \mathbb{N}$. We have to give a procedure for deciding 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 all $i \in \{1, 2, \ldots, m\}$.

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 $2 \times 2$ matrices of fresh variables, and consider the following formula:

$$\Gamma(\mathbf{v}, V_1, \ldots, V_m) \stackrel{\text{def}}{=} \Phi_{\mathbf{S}}(\mathbf{v}) \wedge \bigwedge_{i=1}^{m} \Phi_T(\mathbf{v}\ V_i).$$

The multiple reachability decision problem asks whether there is some $\mathbf{p} \in \mathbb{R}^2$ and distinct positive integers $x_1, \ldots, x_m$ such that

$$\Gamma(\mathbf{p}, M^{x_1}, \ldots, M^{x_m}) \tag{9}$$

holds. Eliminating the existential quantifiers for $\mathbf{v}$ from $\Gamma$, we effectively obtain another formula $\Gamma'(V_1, \ldots, V_m)$ such that (9) 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 $\Gamma'$ form a semialgebraic set; which can be written as a finite union of sets of the form (3), 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:

$$\Psi(V_1, \ldots, V_m) \stackrel{\text{def}}{=} \bigwedge \begin{cases} P_0(V_1, \ldots, V_m) & = 0, \\ P_1(V_1, \ldots, V_m) & > 0, \\ \vdots & \\ P_\ell(V_1, \ldots, V_m) & > 0. \end{cases}$$

We want to prove that we can decide whether there are distinct positive integers $x_1, \ldots, x_m$ such that

$$\Psi(M^{x_1}, \ldots, M^{x_m}) \tag{10}$$

holds. We will simply 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 $n \in \mathbb{N}$

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

[4] As mentioned in the previous section, the real vectors $\mathbf{x}$ for which $P(\mathbf{x}) = 0$ and $Q(\mathbf{x}) = 0$ coincide with the real vectors $\mathbf{x}$ for which $P(\mathbf{x})^2 + Q(\mathbf{x})^2 = 0$.

So when polynomials $P_0, \ldots, P_\ell$ are instantiated with $M^x$ they can be seen as polynomials in $\lambda^x$ and $\overline{\lambda}^x = \lambda^{-x}$; in other words there are 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 $0 \leq i \leq \ell$ and all tuples of integers $(x_1, \ldots, x_m) \in \mathbb{Z}^m$. Let us assume at once that as part of the strict inequalities we have ones of the type

$$\lambda^{x_j} + \lambda^{-x_j} > \lambda^{x_k} + \lambda^{-x_k}, \tag{11}$$

for $j \neq k$ to ensure that the $x_i$ are all distinct. This is without loss of generality because any solution would certainly belong to one of these augmented semialgebraic sets. We will show how to decide if there is a solution.

*2) Proof Overview:* We begin in the next subsection by considering the case that there are only polynomial inequalities to satisfy. This case is simpler. Intuitively, on the complex plane the angles of $\lambda^n$, for integer $n$, are dense in $[0, 2\pi]$, and the target set is made out of strict polynomial inequalities and therefore is open in the usual topology. This in turn means that if the target set is non-empty, we can rotate into it. The proof uses a theorem of Kronecker on simultaneous Diophantine approximation.

In subsection IV-A4, we develop the theory of algebraic subgroups and linear tori to the extent that is needed in the sequel. As we described briefly in the introduction, the reason for considering algebraic subgroups is because all $(\lambda^{x_1}, \ldots, \lambda^{x_m})$ for $x_i \in \mathbb{Z}$ belong to an algebraic subgroup of dimension 1. We want to apply the result of Bombieri and Zannier which says that the intersection of algebraic subgroups of dimension 1 and a variety has bounded (Weil) height. For us the variety (which we denote by $X$) is just the zero set of the polynomial $Q_0$.

It is possible for a variety to contain a whole algebraic subgroup. When this happens, the height of points in the intersection cannot be bounded. These cases need to be treated by separate means. This is the reason for the partition $X = X^\circ \cup X^\bullet$, as those *degenerate* points are contained in $X^\bullet$. The end goal of subsection IV-A4 is to show that we can compute the polynomial equations that define $X^\bullet$, and to state a structure theorem, giving more information about this subset.

In subsection IV-A5 we introduce heights and the Zannier-Bombieri theorem. In the end we tie these three subsections together by describing how the theorems can be used to decide the existence of solutions. The algorithm is conceptually simple. To check whether there is a solution in $X^\circ$ we use the height bound to derive an upper bound on the absolute value of the exponents $|x_i|$, and then simply try every one of the finitely many possibilities. If no solution is found, it remains to check whether there is one in $X^\bullet$. To this end, the algorithm constructs the defining polynomials of $X^\bullet$, and by exploiting the structure theorem, the check for solutions in $X^\bullet$ is reduced to the problem of whether there is a solution in a set defined by strict polynomial inequalities.

*3) System of Inequalities:* We prove a slightly more general result, where we allow $(x_1, \ldots, x_m)$ to range over members of a (additive) subgroup of $\mathbb{Z}^m$.

**Lemma IV.1.** *Let $\Lambda \subseteq \mathbb{Z}^m$ be a subgroup, where the group operation is component-wise addition. Let $\lambda \in \overline{\mathbb{Q}}$ be as above, and suppose that we are given polynomials $S_1, \ldots, S_k$ in $2m$ variables and algebraic coefficients, such that $S_i(z_1, \overline{z_1}, \ldots, z_m, \overline{z_m})$ is real-valued for all complex $z_j$ and all $i$. Then there is a procedure to decide whether there exists $(x_1, \ldots, x_m)$ in $\Lambda$, with positive coordinates, simultaneously satisfying*

$$S_i(\lambda^{x_1}, \ldots, \lambda^{-x_m}) > 0, \text{ for all } i \in \{1, \ldots, k\}. \tag{12}$$

*Proof.* Suppose that the subgroup $\Lambda$ 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:

$$\Lambda = \{\mathbf{x} \in \mathbb{Z}^m \ : \ \mathbf{x}\, A = \mathbf{0}\}.$$

First check that this subgroup contains elements with positive coordinates, if it does not, clearly we answer no.

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:

$$\mathbf{R} \stackrel{\text{def}}{=} \{\mathbf{z} \in \mathbb{T}^m \ : \ \mathbf{z}^{\mathbf{a}_i} = 1 \text{ for all } 1 \leq i \leq m'\},$$
$$\mathbf{R}' \stackrel{\text{def}}{=} \{\mathbf{z} \in \mathbf{R} \ : \ S_i(z_1, z_1^{-1}, \ldots, z_m, z_m^{-1}) > 0, \text{ for all } 1 \leq i \leq k\}.$$

Intuitively, the set $\mathbf{R}$ is all the numbers with coordinates in the unit circle and exponents that belong to the subgroup $\Lambda$. In particular, $(\lambda^{x_1}, \ldots, \lambda^{x_m})$ is in $\mathbf{R}$ if and only if $\mathbf{x} \in \Lambda$. Meanwhile, $\mathbf{R}'$ is the subset of such numbers that also satisfy the polynomial inequalities (12). Clearly, if $\mathbf{R}'$ is empty, there are no solutions to (12); but if it is not empty we argue below that there will always be at least one solution. Since $\mathbf{R}'$ is a semialgebraic set, we can use Tarski's algorithm to decide whether it is empty or not.

To show that $\mathbf{R}' \neq \emptyset$ implies existence of a solution we use the following theorem due to Kronecker on simultaneous Diophantine approximations.

**Theorem IV.2** (Theorem IV in Page 53 of [Cassels(1959)])**.** *Let*

$$L_j(\mathbf{y}) = L_j(y_1, \ldots, y_{m'}), \quad 1 \leq j \leq m,$$

*be $m$ homogeneous linear forms in any number $m'$ 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*

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

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 $\Lambda$. Write $\lambda = \exp(\vartheta 2\pi\mathbf{i})$, where the angle $\vartheta$ is not a rational number, because if it were, then $\lambda$ would be a root of 1, in which case the lemma is trivial. For $1 \le j \le m$ define:

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

Suppose that $\mathbf{R}'$ is nonempty, and choose some element $\zeta \in \mathbf{R}'$ 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 short computation shows that since $\vartheta$ 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 $\zeta$ 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 $\alpha$. 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 $\alpha_j$. 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

$$(\lambda^{L_1(\mathbf{a})/\vartheta}, \ldots, \lambda^{L_m(\mathbf{a})/\vartheta}) \in \mathbf{R}, \tag{13}$$

and gets arbitrarily close to $\zeta$. Finally, since $\mathbf{R}'$ is an open subset of $\mathbf{R}$, by choosing $\epsilon$ small enough, we get some $\mathbf{a}$ such that the tuple of (13) belongs to the subset $\mathbf{R}'$.

It remains to check that we can find one such $\mathbf{a}$ such that the exponents in (13) are positive. We know that the subgroup $\Lambda$ has elements with positive coordinates, and this is in fact sufficient, due to an equidistribution theorem of Weyl that can be found in the section starting at Page 64 of [Cassels(1959)]. □

*4) Algebraic Subgroups and Tori:* We begin with a few definitions. The general theory is developed more extensively in [Schmidt(1996)], [Schinzel(2000)], and especially in [Bombieri and Gubler(2007), 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 each $f_i$ has 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 non-zero algebraic numbers. In other words it is the subset of $\overline{\mathbb{Q}}^n$ satisfying $z_1 \cdots z_n \neq 0$. It has a group structure under component-wise multiplication:

$$(y_1, \ldots, y_n) \cdot (z_1, \ldots, z_n) = (y_1 z_1, \ldots, y_n z_n).$$

The variety that we are interested in, which we will denote by $X \subseteq \mathbb{G}^n$, is the zero set of our polynomial $Q_0$, conjoined with polynomial equations

$$z_j z_{j+1} - 1 = 0,$$

where $1 \le j \le n$ is an odd number, to ensure that the conjugacy relations hold. We assume that $X$ 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, [Bombieri and Gubler(2007), Corollary 3.2.15]. Further, if $\Lambda$ is a subgroup of $\mathbb{Z}^n$ of rank $n - r$ then $H_\Lambda$ is an algebraic subgroup of dimension $r$. By dimension here we mean the dimension of the variety, see for example [Hartshorne(1977), Definition on Page 5]. One way of defining the dimension of a variety $X$ is as the maximum length of a chain $X_0 \subset X_1 \subset \cdots \subset X_k$ of irreducible subvarieties of $X$.

We prove that powers of $\lambda$ belong to algebraic subgroups of dimension 1, as remarked in the introduction.

**Lemma IV.3.** *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 that define 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), in other words, it has rank $k-1$. This in turn implies that the point in the statement of the lemma belongs to the algebraic subgroup $H_\Lambda$, which is a subgroup of dimension 1. See [Bombieri and Gubler(2007), Proposition 3.2.7]. □

We will 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

$$\mathcal{H}_1 \cap X,$$

as according to the lemma above, this intersection will contain all

$$(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m})$$

for which

$$Q_0(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}) = 0,$$

where $x_i$ are integers.

In order to analyse the intersection above, the variety $X$ will be partitioned into two subsets which we now define. 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 $Y \subseteq \mathbb{G}^n$ we denote by $Y^\bullet$ the union of all nontrivial torus cosets that are contained entirely in $Y$, in other words:

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

Also define

$$Y^\circ \stackrel{\text{def}}{=} Y \setminus Y^\bullet.$$

We give another definition of $Y^\bullet$ which is effective and apply it to $X$.

Recall that for a vector of integers $\mathbf{a} \in \mathbb{Z}^n$ 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 write by $\varphi_A \ : \ \mathbb{G}^n \to \mathbb{G}^n$ the map

$$\varphi_A(\mathbf{z}) \stackrel{\text{def}}{=} \left(\mathbf{z}^{A_1}, \ldots, \mathbf{z}^{A_n}\right).$$

One can show that $\varphi_{AB} = \varphi_B \circ \varphi_A$, and as a consequence for matrices $A$ with determinant $\pm 1$, $\varphi_A$ is an isomorphism[5] with inverse $\varphi_{A^{-1}}$. Such an isomorphism is called a **monoidal transformation**. The group of $n \times n$ integer matrices with determinant $\pm 1$ is the special linear group, denoted $\mathrm{SL}(n, \mathbb{Z})$.

We state here some important basic results related to the structure of algebraic subgroups. Recall that we have used the notation $\|\mathbf{a}\|$ for the $\ell^1$ norm; when $A$ is a matrix, we denote by $\|A\|$ the maximum of $\ell^1$ norms of its columns.

**Proposition IV.4** ( [Bombieri and Gubler(2007), Proposition 3.2.10 and Corollary 3.2.9]). *Let $H_\Lambda$ be a linear torus, where $\Lambda$ is a subgroup of $\mathbb{Z}^n$ of rank $n-r$ and suppose that $\Lambda$ has $n-r$ independent vectors of norm at most $N$. Then there is a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$ with $\|A\| \leq n^3 N^{n-r}$ and $\left\|A^{-1}\right\| \leq n^{2n-1} N^{(n-1)^2}$, such that*

$$\varphi_A(\mathbf{1}_{n-r} \times \mathbb{G}^r) = H_\Lambda,$$

*where*

$$\mathbf{1}_{n-r} \stackrel{\text{def}}{=} \{\underbrace{(1, \ldots, 1)}_{\text{unit of } \mathbb{G}^{n-r}}\}.$$

From the bounds on $A$, we can effectively compute such a matrix given $n-r$ independent vectors of $\Lambda$. Next, let $X \subseteq \mathbb{G}^n$ be our subvariety. We say that an algebraic subgroup $H$ of $\mathbb{G}^n$ is **maximal** in $X$ if $H \subseteq X$ and $H$ is not contained in a larger subgroup of $X$.

**Proposition IV.5** ( [Bombieri and Gubler(2007), Proposition 3.2.14]). *Let $X \subseteq \mathbb{G}^n$ be a subvariety, defined by polynomial equations $f_i(\mathbf{x}) := \sum c_{i,\mathbf{a}} \mathbf{x}^{\mathbf{a}} = 0$, $1 \leq i \leq k$, 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 $\Lambda$ is generated by vectors of type $\mathbf{a}'_i - \mathbf{a}_i$, with $\mathbf{a}'_i, \mathbf{a}_i \in E_i$, for $i = 1, \ldots, k$.*

The first proposition above says that linear tori of dimension $r$ are simply 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 simply by the exponents of monomials that appear in the definition of $X$.

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 $g^{-1}X$. Theorem IV.5 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 factorising in the number field $\mathbb{Q}(\lambda)$, we have:

**Lemma IV.6.** *We can effectively construct a (possibly empty) set $\mathcal{T}_X$ of positive-dimensional linear 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, another way of defining the subset $X^\bullet$ is

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

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

Although we can effectively construct the subgroups $H$, we do not yet have an effective method of constructing the union of all maximal cosets $gH$ that are contained in $X$. This is done in the following lemma.

**Lemma IV.7** ( [Bombieri and Gubler(2007), 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 Theorem IV.5 we can conclude that $H = H_\Lambda$ where $\Lambda$ is a subgroup of $\mathbb{Z}^n$ of rank $n - r$, and from Theorem IV.4, 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 defining 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. □

To summarise, in this section we proved that (i) we can compute the finite set of subgroups $H$, such that $gH$ is some maximal coset contained in $X$. We called this finite set of subgroups $\mathcal{T}_X$. We also showed (ii) that for any $H \in \mathcal{T}_X$ the union of all maximal cosets $gH$ that are contained in $X$ are isomorphic to $X_1 \times \mathbb{G}^r$ for some $r \geq 1$. Furthermore, the defining equations of $X_1$ can also be computed and the isomorphism map too.

These facts give sufficient information to decide if there are any solutions in $X^\bullet$. Next, we discuss heights and the Bombieri-Zannier theorem.

*5) Heights:* 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 [Bombieri and Gubler(2007)]. 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. Define

$$\log^+ t \stackrel{\text{def}}{=} \max(0, \log t).$$

Then the **height**[6] 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 IV.8.** *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:

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

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 $\alpha$ (see [Bombieri and Gubler(2007), Lemma 1.5.18]), we get the upper bound. For the lower bound:

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

□

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 IV.9** ( [Schinzel(2000), 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 algebraic points $\mathbf{z} \in \mathbb{G}^n$,*

$$z \in X^\circ \cap \mathcal{H}_1 \qquad \Rightarrow \qquad h(\mathbf{z}) \leq b.$$

The theorem cited in [Schinzel(2000)] does not explicitly state that the bound is effective, but upon a closer inspection of the proof one can see that all the bounds are explicit, with the exception of the points $(c_1^*, \ldots, c_h^*) \in \mathbb{Z}^h$ which are chosen to be outside a finite number of linear subspaces of $\mathbb{Q}^h$. It is plain that we can effectively construct such a point.

Now we have all the tools to describe the algorithm and justify its correctness.

[6] The long name is the absolute logarithmic (Weil) height.

*6) Algorithm:* The procedure first searches for solutions in $X^\circ$. Let $b \in \mathbb{N}$ be an upper bound on the height of algebraic points in the intersection of $\mathcal{H}_1$ (which is the union of all subgroups of dimension 1) and $X^\circ$. Such an upper bound can be computed with Theorem IV.9. From Theorem IV.3 we know that for all integers $x_1, \ldots, x_m \in \mathbb{Z}$, the algebraic points

$$\left(\lambda^{x_1}, \lambda^{-x_1}, \ldots, \lambda^{x_m}, \lambda^{-x_m}\right) \tag{14}$$

all belong to $\mathcal{H}_1$. So if any of the points in (14) is in $X^\circ$ it is also in the intersection $X^\circ \cap \mathcal{H}_1$. The upper bound $b$ on the height of points in this intersection translates to an upper bound on the exponents $\|\mathbf{x}\|$ due to Theorem IV.8. It remains to check whether any of the finitely many points (14), with $\|\mathbf{x}\| \leq b$, satisfy the polynomial equality $Q_0 = 0$ and inequalities $Q_i > 0$, $1 \leq i \leq \ell$. These checks are performed by using Tarski's algorithm, making sure that the exponents are distinct and positive. If a solution is found, we return yes, otherwise we continue the search in $X^\bullet$.

Now, by applying Theorem IV.6 we compute the defining polynomials of tori that are in the set $\mathcal{T}_X$. Recall that this set contains all positive dimensional tori, which have a maximal coset entirely contained in $X$. If $\mathcal{T}_X$ is empty, so is the set $X^\bullet$, and we are done: the algorithm returns no, because no solutions were found in $X^\circ$ and $X^\bullet = \emptyset$.

So suppose that $\mathcal{T}_X$ is nonempty. The procedure searches for solutions in all the elements of $\mathcal{T}_X$ in turn, in the following way. Let $H \in \mathcal{T}_X$ be an element, of dimension $r$. By definition, this means that $H$ is a torus for which there is a maximal coset $gH$ entirely contained in $X$, and $r \geq 1$.

If $H$ has dimension $r = n$, then this essentially means that $X^\bullet = \mathbb{G}^n$ and hence $X = X^\bullet$, which in turn implies that the polynomial $Q_0$ is identically 0. So it is only the strict polynomial inequalities $Q_i > 0$ that need to hold for there to be a solution. We can check whether the inequalities can be satisfied by applying Theorem IV.1, with $\Lambda = \mathbb{Z}^m$, and polynomials $Q_1, \ldots, Q_\ell$. Recall that the requirement for the exponents to be distinct is assumed to be encoded in the polynomial inequalities, as remarked in the beginning of this section. So much for deciding the case when $H$ has dimension $r = n$.

We assume now that $H$ has dimension $r$, where $0 < r < n$. Using Theorem IV.7, we next compute a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$, and a subvariety $X_1 \subseteq \mathbb{G}^{n-r}$, such that

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

Now $X_1 \subseteq \mathbb{G}^{n-r}$ does not contain any positive dimensional coset, *i.e.* $X_1 = X_1^\circ$. To see this, assume towards a contradiction that there is some $g_1$ and a torus $H_1$ of dimension $r_1 > 0$ such that $g_1 H_1 \subseteq X_1$. Then we have

$$\bigcup_{gH \subseteq X} gH \supseteq \varphi_A(g_1 H_1 \times \mathbb{G}^r).$$

Theorem IV.4 implies that there exists a monoidal transformation $\varphi_1$ such that

$$\bigcup_{gH \subseteq X} gH \supseteq \varphi_A\big(\varphi_1(\mathbf{1}_{n-r-r_1} \times \mathbb{G}^{r_1}) \times \mathbb{G}^r\big). \tag{15}$$

From the proof of Theorem IV.7 it plainly follows that there is a bijection between points in $X_1$ and cosets $gH$ that are contained in $X$. This fact together with the inclusion (15) yield the existence of a coset $gH$ of dimension $r$ that is contained in a coset of dimension $r + r_1$, both of which are inside $X$. Since $r_1 > 0$, the coset $gH$ is contained in a strictly larger coset; contradicting the definition of $\mathcal{T}_X$ which says that all $gH$ should be maximal.

Now we can write the union of all cosets $gH$ contained in $X$ as

$$\varphi_A(X_1^\circ \times \mathbb{G}^r).$$

The union of all subgroups of dimension one, $\mathcal{H}_1$, is invariant under monoidal transformations. Therefore,

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

and since $\varphi_A$ is an isomorphism we have

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

Through composition with the polynomial defining the monoidal transformation $\varphi_A$, we can construct polynomials $\widetilde{Q_0}, \ldots, \widetilde{Q_\ell}$ such that if

$$\mathbf{z} \in \varphi_A\big(\mathcal{H}_1 \cap (X_1^\circ \times \mathbb{G}^r)\big)$$

satisfies the polynomial (in)equalities $Q_0 = 0$, $Q_i > 0$ for $1 \leq i \leq \ell$, then

$$\varphi_{A^{-1}}(\mathbf{z}) \in \mathcal{H}_1 \cap (X_1^\circ \times \mathbb{G}^r),$$

satisfies the polynomial (in)equalities $\widetilde{Q_0} = 0$, $\widetilde{Q_i} > 0$, for $1 \leq i \leq \ell$. Using the procedure of Theorem IV.9 we compute a bound $b_1 \in \mathbb{N}$ for the intersection

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

where $\mathcal{H}_1(n-r)$ is the union of all algebraic subgroups of $\mathbb{G}^{n-r}$. As above, we search for $(\lambda^{x_1}, \ldots, \lambda^{x_{n-r}})$ with $\|x\| \leq b_1$ that belong to $X_1^\circ$. If none are found, the procedure halts and returns no. Since $\varphi_A$ sends powers of $\lambda$ to powers of $\lambda$, the no answer is justified, as indeed there are no solutions.

If a finite number of $(\lambda^{x_1}, \ldots, \lambda^{x_{n-r}})$ belonging to $X_1^\circ$ are found, we try each in turn to see if they can be made to satisfy the inequalities as well. Let $(\lambda^{x_1}, \ldots, \lambda^{x_{n-r}})$ be one such point. Fixing the first $n-r$ coordinates to these powers of $\lambda$ in the polynomial (in)equalities makes $\widetilde{Q_0}$ identically zero, and gives us new inequalities $R_i > 0$, $1 \leq i \leq \ell$. By construction, the polynomials $R_i$ will satisfy the hypothesis of Theorem IV.1, so we can apply this lemma for $\Lambda = \mathbb{Z}^r$ to determine if $R_1, \ldots, R_\ell$ are satisfied by some powers of $\lambda$. If such powers of $\lambda$ are found, the procedure halts and

returns yes[7]. If there is not, we continue with another candidate $(\lambda^{y_1}, \ldots, \lambda^{y_{n-r}})$ that has $\|x\| \leq b_1$, and which belongs to $X_1^\circ$. This concludes the proof of Theorem I.2(ii).

We 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 that in Theorem IV.9, but for subgroups of dimension 2. There are finiteness results, often as special cases of the Mordell-Lang conjecture, see *e.g.* [Laurent(1984)], but to our knowledge, no effective bounds are known.

## References


[Almagor et al.(2019)] Shaull Almagor, Joël Ouaknine, and James Worrell. 2019. The Semialgebraic Orbit Problem. In *36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019, March 13-16, 2019, Berlin, Germany (LIPIcs, Vol. 126)*, Rolf Niedermeier and Christophe Paul (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 6:1–6:15. https://doi.org/10.4230/LIPIcs.STACS.2019.6

[Baker(1990)] Alan Baker. 1990. *Transcendental number theory*. Cambridge university press.

[Bombieri and Gubler(2007)] Enrico Bombieri and Walter Gubler. 2007. *Heights in Diophantine geometry*. Cambridge university press.

[Brindza et al.(2001)] B. Brindza, Á. Pintér, and W. M. Schmidt. 2001. Multiplicities of binary recurrences. *Canad. Math. Bull.* 44, 1 (2001), 19–21.

[Cassels(1959)] J. W. S. Cassels. 1959. *An Introduction To Diophantine Approximation*.

[Cerlienco et al.(1987)] L. Cerlienco, M. Mignotte, and F. Piras. 1987. Linear recurrent sequences: algebraic and arithmetical properties. *Enseign. Math.(2)* 33, 1-2 (1987), 67–108.

[Davis et al.(1976)] Martin Davis, Yuri Matijasevic, and Julia Robinson. 1976. *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution*. 323–378 pages. https://doi.org/10.1090/pspum/028.2/0432534

[Derksen and Masser(2015)] H. Derksen and D. Masser. 2015. Linear equations over multiplicative groups, recurrences, and mixing II. *Indagationes Mathematicae* 26, 1 (Jan 2015), 113–136. https://doi.org/10.1016/j.indag.2014.08.002

[Everest et al.(2003)] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. 2003. *Recurrence Sequences*. https://doi.org/10.1090/surv/104

[Gimbert and Oualhadj(2010)] Hugo Gimbert and Youssouf Oualhadj. 2010. Probabilistic Automata on Finite Words: Decidable and Undecidable Problems. In *Automata, Languages and Programming*, Samson Abramsky, Cyril Gavoille, Claude Kirchner, Friedhelm Meyer auf der Heide, and Paul G. Spirakis (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 527–538.

[Hartshorne(1977)] Robin Hartshorne. 1977. *Algebraic Geometry*. https://doi.org/10.1007/978-1-4757-3849-0

[Jones(1982)] James P. Jones. 1982. Universal Diophantine Equation. *The Journal of Symbolic Logic* 47, 3 (1982), 549–571. http://www.jstor.org/stable/2273588

[Kannan and Lipton(1986)] R. Kannan and R. J. Lipton. 1986. Polynomial-Time Algorithm for the Orbit Problem. *J. ACM* 33, 4 (1986), 808–821. https://doi.org/10.1145/6490.6496

[Karimov et al.(2022)] Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. 2022. *What's Decidable About Discrete Linear Dynamical Systems?* Springer Nature Switzerland, Cham, 21–38. https://doi.org/10.1007/978-3-031-22337-2_2

[Laurent(1984)] Michel Laurent. 1984. Equations diophantiennes exponentielles. *Inventiones mathematicae* 78 (1984), 299–327.


[7] A detail that needs to be justified is that $x_i$ need to be positive after the application of $\varphi_{A^{-1}}$. But we can find such $x_i$ due to the equidistribution theorem that was used in the proof of Theorem IV.1.


[Lockwood(1967)] Edward Harrington Lockwood. 1967. *A book of curves*. Cambridge University Press.

[Schinzel(2000)] Andrzej Schinzel. 2000. *Polynomials with special regard to reducibility. With an Appendix by Umberto Zannier.* Vol. 77. Cambridge University Press. 517–x pages.

[Schmidt(1996)] W. M. Schmidt. 1996. Heights of points on subvarieties of $\mathbb{G}_m^n$. *Number Theory (Paris, 1993– 1994), London Math. Soc. Lecture Note Ser. 235* (1996), 157–187.

[Tarski(1951)] Alfred Tarski. 1951. A decision method for elementary algebra and geometry. (1951).

[Waldschmidt(2020)] Michel Waldschmidt. 2020. Thue Diophantine Equations: A Survey. *Class Groups of Number Fields and Related Topics* (2020), 25–41.

[Zannier(2012)] Umberto Zannier. 2012. *Some Problems of Unlikely Intersections in Arithmetic and Geometry (AM-181)*. Princeton University Press.


## Appendix

We will assume that $\lambda/\overline{\lambda}$ is not a root of unity, because this case is essentially the same as the case where the eigenvalues are real. Matrices in which no ratio of distinct eigenvalues is a roots of unity are called **non-degenerate**.

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 [Almagor et al.(2019)], 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 A.1.** *Let $\mathbf{p} \in \mathbb{R}^2 \setminus \{(0,0)\}$, $h$ a line going through the origin given by the normal vector $\mathbf{h} \in \mathbb{R}^2$, and $M \in \mathbb{R}^{2\times 2}$ a non-degenerate matrix. Suppose there are distinct positive integers $n, m \in \mathbb{N}$ such that both $M^n$ and $M^m$ send $\mathbf{p}$ to the line $h$,* i.e.

$$\mathbf{p}\ M^n\ \mathbf{h}^\top = \mathbf{p}\ M^m\ \mathbf{h}^\top = 0. \tag{16}$$

*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 (16) 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 (16) cannot hold unless $M$ is the zero matrix, or the other eigenvalue is 1, in which case the conclusion holds. If $M$ is invertible then

$$r\ \mathbf{p} = \mathbf{p}\ M^{m-n}$$

and hence $r$ is an eigenvalue of $M^{m-n}$. By non-degeneracy, 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 (16) 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 $k \in \mathbb{N}$. □

The hypothesis that the target line passes through the origin is important. Indeed, perhaps surprisingly, when the target is a line that does *not* pass through the origin, multiple reachability becomes more difficult. What is the difficulty? First, the above proposition fails in that case. Such a target can be reached multiple times.[8]

Second, almost all known effective methods are based on Baker's work on linear forms in logarithms. Such methods yield an effective time bound, after which it is guaranteed that the orbit will not go in the target. This bound however depends on the height of the initial points. It is not clear how to apply these methods when the initial point is replaced by a set. One possibility is to take the projection of the initial set (as in [Almagor et al.(2019)] and the last subsection of this paper), but then the multiple reachability problem is reduced to a problem about intersections of algebraic subgroups with varieties inside tori. There are finiteness results about such intersections, but few of them effective.

To provide some more intuition, consider a linear map on $\mathbb{R}^2$. 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.

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

We prove Theorem I.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 $2\times 2$ matrix with rational entries and $m \in \mathbb{N}$ a positive integer, the minimum number of times we wish to enter the target. We consider, separately, the case when $M$ has complex conjugate eigenvalues $\lambda, \overline{\lambda}$, and the case when it has real eigenvalues. We begin with the former.

Let $\mathbf{p} \in \mathbb{R}^2$ be a point with polar coordinates $(r, \varphi)$. It is possible to 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

$$(sr|\lambda|^n, n\vartheta + \vartheta_0 + \varphi). \tag{17}$$

To see this, simply write $\mathbf{p}M^n$ as $|\lambda|^n\mathbf{p}U^n$, where $U$ is a rotation matrix and then follow the second example in the Introduction. The numbers $s, r$ and $|\lambda|$ are real algebraic whose defining formulas (in first-order logic of reals) can be computed, while $\vartheta$ and $\vartheta_0$ are logarithms of algebraic numbers. We will make use of the following fact from Diophantine approximation. It is a corollary of [Cassels(1959), 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 A.2.** *If $\vartheta$ is an irrational multiple of $2\pi$, we have*

$$\{\{n\vartheta\}_{2\pi} : n \in \mathbb{N}\} \textit{ is dense in } [0, 2\pi].$$

*Proof of Theorem I.2 for non-real eigenvalues.* If $|\lambda| > 1$, the algorithm answers *yes*. The justification is as follows. When $\mathbf{T}$ is a halfplane, there exist positive real numbers $\alpha_0, \phi_1, \phi_2$, with $\phi_1 < \phi_2$, such that for all $\alpha > \alpha_0$ and $\phi_1 < \phi < \phi_2$, the point with polar coordinates $(\alpha, \phi)$ is in $\mathbf{T}$. This simply means that the halfplane contains a cone minus a bounded set.

The matrix $M$ is assumed to be non-degenerate, which implies that the rotation angle $\vartheta$ in (17) is an irrational multiple of $2\pi$. So by applying Theorem A.2 to this number, we see that the intersection of the set

$$\{n\vartheta + \vartheta_0 + \phi \mod 2\pi \ : \ n \in \mathbb{N}\} \tag{18}$$

and the interval $(\phi_1, \phi_2)$ contains infinitely many points. From $|\lambda| > 1$, it follows that the sequence of points $\mathbf{p}M^n$ will enter the cone mentioned above, which is a subset of $\mathbf{T}$, infinitely many times.

Suppose now that $|\lambda| < 1$.[9] When the halfplane $\mathbf{T}$ has distance to the origin equal to 0, or when the source $\mathbf{S}$ is unbounded, the algorithm answers *yes*, with a justification symmetric to the one above. Assume that $\mathbf{T}$ has distance to the origin equal to $\delta > 0$ and let $\mathbf{S}$ be bounded with radius $\rho$. 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 all $n \in \{0, 1, \ldots, N\}$ 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 intersection. □

We turn our attention now to the case where the eigenvalues of the matrix $M$ are real. We do a case analysis depending on

[8] 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 [Brindza et al.(2001)].

[9] The rotation case $|\lambda| = 1$ is handled in the next subsection in a more general setting.

whether the eigenvalues are distinct or not, and whether they are positive or not.

*1) Diagonalisable $M$ with distinct positive eigenvalues.:* In Jordan normal form, the matrix $M$ is $BDB^{-1}$ where $D$ is the 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 simply 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 A.3.** *Let $M$ be as above, $H$ a halfplane, $\mathbf{p} \in \mathbb{R}^2$ a point, and $\mathbf{p}_0, \mathbf{p}_1, \ldots$ 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

$$x \mapsto a_1 b_1^x + a_2 b_2^x + a_3, \tag{19}$$

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 $\alpha_1, \alpha_2$, 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

$$c_1 x \rho_1^n + c_2 y \rho_2^n + c_3. \tag{20}$$

From the observation about the zeros of (19) above, this expression as a function of $n$ may change sign at most twice, which establishes the lemma. □

From this proof we observe that when the halfplane is given by a homogeneous inequality, the orbit cannot leave the halfplane and come back. For other cases, we proceed to prove that the gaps between consecutive visits to the halfplane $H$ cannot be longer than 3.

*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 $c_1 x + c_2 y > c_3$. The orbit of $(x, y)$ visits $H$ at time $n$ if

$$\begin{cases} c_1 x |\rho_1|^n + c_2 y \rho_2^n > c_3, & \text{n even}, \quad (21a) \\ -c_1 x |\rho_1|^n + c_2 y \rho_2^n > c_3, & \text{n odd}. \quad (21b) \end{cases}$$

Depending on the signs of $x$ and $y$, one of the inequalities implies the other. Without loss of generality suppose (21a) implies (21b). By Theorem A.3, the set of $n$ satisfying (21a) forms an interval in $\mathbb{N}$. It follows that the gaps between two consecutive visits from $(x, y)$ to $H$ is at most 2.

*3) 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 $F : \mathbb{R} \to \mathbb{R}$,

$$F(t) \stackrel{\text{def}}{=} c_1 x |\rho_1|^t + c_2 y |\rho_2|^t.$$

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

$$c_1 x \rho_1^n + c_2 y \rho_2^n = \begin{cases} F(n) \text{ if } n \text{ is even}, \\ -F(n) \text{ if } n \text{ is odd}. \end{cases} \tag{22}$$

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 (22) we see that for any $(x, y) \in \mathbb{R}^2$ nonzero, the system will enter 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:

$$c_1 x \rho_1 + c_2 y \rho_2 < c_3$$
$$c_1 x \rho_1^3 + c_2 y \rho_2^3 > c_3.$$

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.

*4) Non-diagonalisable $M$ with a repeated eigenvalue.:* A version of Lemma A.3 also holds in case $M$ has a repeated eigenvalue $\rho$. 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 (20) is

$$(nxc_2\rho^{-1} + c_2 y + c_1 x)\rho^n + c_3.$$

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.

*5) $M$ 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.

Having handled all the cases, we are now ready to give a proof of Theorem I.2 for real eigenvalues.

*Proof of Theorem I.2(i) for $M$ with real eigenvalues.* Theorem A.3 and the case analysis above, implies 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 3. 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

$$\mathbf{p}M^{n_i} \in \mathbf{T} \quad \text{and} \quad 0 < n_{i+1} - n_i \leq 3 \quad \text{for all } n_i.$$

This contiguous multiple reachability question can easily be reduced to a union of single reachability queries. Indeed, an orbit contains a pattern (of visits and not visits to $H$) of length $3m$ if and only if it reaches a certain polytope subset $\mathbf{P}$ of $\mathbb{R}^2$; A formula defining $P$ can be constructed by considering the sets $\left\{x \in \mathbb{R}^2 \ : \ M^k x \in H\right\}$ and $\left\{x \in \mathbb{R}^2 \ : \ M^k x \notin H\right\}$ for $0 \leq k \leq 3m$. Thus multiple reachability is reduced to at most $2^{3m}$ instances of single reachability from $\mathbf{S}$ to $\mathbf{P}$, which can be solved by invoking the algorithm from [Almagor et al.(2019)]. □