Multiple Reachability in Linear Dynamical Systems

Toghrul Karimov
toghs@mpi-sws.org
Max Planck Institute for Software Systems
Saarbrücken, Germany

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

Joël Ouaknine
joel@mpi-sws.org
Max Planck Institute for Software Systems
Saarbrücken, Germany

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

ABSTRACT

We consider reachability decision problems for linear dynamical systems: Given a linear map on $\mathbb{R}^d$, together with source and target sets, determine whether there is a point in the source set whose orbit, obtained by repeatedly applying the linear map, enters the target set. When the source and target sets are semialgebraic, this problem can be reduced to a point-to-polytope reachability question. The latter is generally believed not to be substantially harder than the well-known Skolem and Positivity Problems. The situation is markedly different for *multiple* reachability, *i.e.* the question of whether the orbit visits the target set at least m times, for some given positive integer m. In this paper, we prove that when the source set is semialgebraic and the target set consists of a hyperplane, multiple reachability is undecidable; in fact we already obtain undecidability in ambient dimension $d = 10$ and with fixed $m = 9$. Moreover, as we observe that procedures for dimensions 3 up to 9 would imply strong results pertaining to effective solutions of Diophantine equations, we mainly focus on the affine plane ($\mathbb{R}^2$). We obtain two main positive results. We show that multiple reachability is decidable for halfplane targets, and that it is also decidable for general semialgebraic targets, provided the linear map is a rotation. The latter result involves a new method, based on intersections of algebraic subgroups with subvarieties, due to Bombieri and Zannier.

CCS CONCEPTS

• **Theory of computation → Models of computation**; **Logic and verification**; **Verification by model checking**; *Automated reasoning*.

KEYWORDS

Linear Dynamical Systems, Linear Recurrence Sequences, Reachability, Multiple Reachability

Conference acronym 'XX, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06
https://doi.org/XXXXXXX.XXXXXXX

ACM Reference Format:
Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. 2018. Multiple Reachability in Linear Dynamical Systems. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 13 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

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

$$O_M(\mathbf{p}) \stackrel{\text{def}}{=} \left\{\mathbf{p} \cdot M^n \ : \ n \in \mathbb{N}\right\}.$$

Besides being one of the most fundamental and simplest kinds of dynamical systems, there is wide interest in studying such systems coming from two directions. First, number theory, through the study of linear recurrence sequences and exponential polynomials; and second, more recently, computer science, and in particular the quest to analyse and verify simple families of programs, such as while loops with affine assignments and guards. Yet despite substantial and sustained research attention from the scientific community over several decades, which has given rise to a voluminous literature, many basic problems remain unsolved. The text [9] contains some of the central theorems of this field as well as a number of applications.

One of the central properties of the orbit we wish to understand is reachability: Does the orbit reach some target set? A general phrasing of this question is the following. Given source and target sets $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$, decide whether there is some point $\mathbf{p} \in \mathbf{S}$ whose orbit reaches $\mathbf{T}$, *i.e.* whether

$$O_M(\mathbf{p}) \cap \mathbf{T} \neq \emptyset.$$

Point-to-point reachability, *i.e.* the case in which both the source and target sets are singletons, $\mathbf{S} = \{\mathbf{p}\}$, $\mathbf{T} = \{\mathbf{t}\}$, is decidable in polynomial time [13]. But essentially every other question 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, but remain unsolved in general.

Singletons, hyperplanes, and halfspaces are fairly simple subsets of $\mathbb{R}^d$. One might therefore expect that for more complicated subsets, the reachability problem becomes truly intractable. This is not the case. For the rather general family of semialgebraic subsets of

$\mathbb{R}^d$ (*i.e.* subsets definable in terms of polynomial inequalities), the problem is no harder than point-to-polytope reachability:

THEOREM 1.1. *Semialgebraic-to-semialgebraic reachability can effectively be reduced to point-to-polytope reachability.*

In other words, simultaneously reaching halfspaces (*i.e.* a polytope) is the most difficult reachability type question. This suggests that it is unlikely that more complex reachability questions are undecidable if the Positivity and Skolem Problems are not.

This article is about **multiple (or repeated) reachability**: the question is not merely whether the target can be reached, but whether it can be reached a prescribed number of times. More precisely, we want to decide whether there exists a point $\mathbf{p} \in \mathbf{S}$ such that

$$|O_M(\mathbf{p}) \cap \mathbf{T}| \geq m,$$

for a positive integer $m \in \mathbb{N}$ given as input. At first blush, it may seem that this is a small generalisation leading to slightly more complex decision problems. Perhaps surprisingly, this is not the case: multiple reachability is considerably more difficult than mere one-time reachability. In particular, in contrast to Theorem 1.1, for multiple reachability we cannot always reduce to the point-to-polytope case. In fact we will prove:

THEOREM 1.2. *Algebraic-to-hyperplane multiple reachability is undecidable.*

Natural problems that are undecidable are quite rare in this field. Intuitively, this 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 choice, *i.e.* when the dynamics is governed by at least two maps, undecidable problems abound. For example, emptiness of probabilistic automata 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 1.2. 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 feasible 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 it were.

Hilbert's tenth problem is undecidable for 9 variables, and consequently our reduction implies that algebraic-to-hyperplane multiple reachability is undecidable in dimension $d = 19$ for fixed $m = 9$, and the same for semialgebraic-to-hyperplane, but in dimension $d = 10$. Algorithms for dimensions $d = 9, \ldots, 3$ would imply effective solutions of Diophantine equations with $d - 1$ variables, which is considered very difficult even when $d = 3$ (and for $d > 4$ it 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. Consequently, we focus our search for positive results on the two-dimensional affine plane $\mathbb{R}^2$.

We establish the following two results:

THEOREM 1.3. *On the plane, semialgebraic-to-halfplane multiple reachability is decidable.*

THEOREM 1.4. *On the plane, semialgebraic-to-semialgebraic multiple reachability is decidable for rotations.*

The first theorem is proved using some standard tools, notably a theorem of Kronecker together with Tarski's quantifier-elimination procedure for the first-order logic of real-closed fields. The second result, Theorem 1.4, is the main contribution of the present paper. Contrary to most positive results in the theory of linear dynamical systems, its proof does not employ the central tool of this area, namely Baker's effective bounds on linear forms in logarithms. Instead, we make use of certain structure theorems due to Bombieri and Zannier which bound the height of algebraic points in the set of intersections between a variety and algebraic subgroups of low dimension. We expect that these tools, alongside with the underlying algorithms of the above theorems, will find applications in other problems regarding linear dynamical systems.

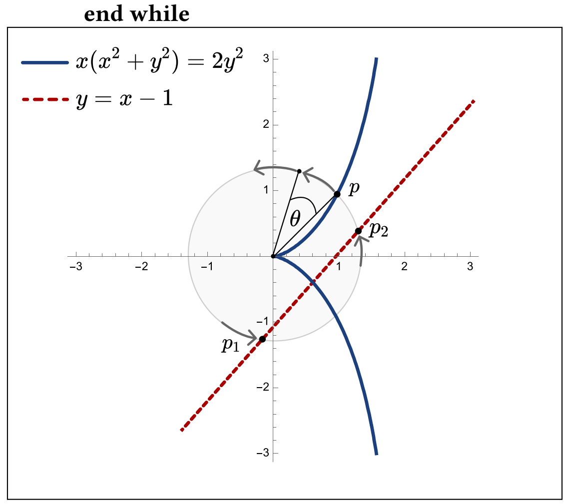
Unsatisfactorily, we leave the general problem of semialgebraic-to-semialgebraic multiple reachability on the plane open. It does not seem to lend itself to the techniques that are known to us. It is intriguing, however, that sophisticated methods seem to be required, even on the plane.

Let us give an illustrating example.

1.1 An Example

Consider the following program:

(x, y) satisfying $x^3 + xy^2 = 2y^2$
$m \leftarrow 2$
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 to be carried in parallel (simultaneously). Does this program terminate? More precisely, is there some initialisation of the variables $x, y \in \mathbb{R}$ such that they satisfy the polynomial[1]

$$x^3 + xy^2 = 2y^2, \tag{1}$$

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 θ 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 that we present in this paper can be used to answer questions like these (and more). In this example, the answer is no; there are no points in the cissoid that can be rotated by θ to two different points on the line. Therefore if the variables x, y are initialised such that they satisfy the polynomial (1), the procedure above does not terminate.

1.2 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 [14].

Directly related to the present paper, the semialgebraic-to-semialgebraic (single) reachability problem was assiduously studied in [1]. There, this decision problem is shown decidable when the dimension is 3, using Baker's effective estimates. Furthermore, [1] 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 1.1 appears implicitly in [1, 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 nondegenerate 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 nondegenerate linear recurrence sequences of a certain order. Equivalently, what is the largest number of times a nondegenerate linear dynamical system from a singleton source hits a hyperplane target? There are many interesting and deep answers to this question, see [9, Chapter 2.2] and references therein.

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 [6]. The conjecture was proved by Derksen and Masser a few years ago in [8], 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 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 [19]. This means that given a formula:

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

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

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

for some formula Φ, are called **semialgebraic sets**. Due to the closure under projection of semialgebraic sets, it is not difficult to see that the semialgebraic sets are exactly the sets $S \subseteq \mathbb{R}^d$ that can be written as finite unions of sets of tuples $(x_1, \ldots, x_d) \in \mathbb{R}^d$ that satisfy simultaneously:

$$\begin{cases} P_0(x_1, \ldots, x_d) & = 0, \\ P_1(x_1, \ldots, x_d) & > 0, \\ \vdots \\ P_k(x_1, \ldots, x_d) & > 0, \end{cases} \tag{2}$$

where $P_i \in \mathbb{Z}[x_1, \ldots, x_d]$. To see this, note that 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 a linear equation, *i.e.* $(x_1, \ldots, x_d) \in \mathbb{R}^d$ for which

$$a_1x_1 + \cdots + a_dx_d + a_{d+1} = 0,$$

where a_i are integers. A **halfspace** is the set of solutions of a linear *inequality*, and a **polytope** is the intersection of finitely many halfspaces. By the adjective **homogeneous**, when applied to the

[1]This curve is the *cissoid of Diocles*, discovered around 180 BC. See [16, Chapter 15].

notions above, we mean that the topological closure contains the origin. On $\mathbb{R}^2$, a hyperplane is just a **line**, and a halfspace is called a **halfplane**.

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

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}, \tag{3}$$

for all $n > d$ where a_i are rational numbers. The minimal number d for which the sequence satisfies (3) is called the **order** of the sequence. Linear recurrence sequences and linear dynamical systems are basically the same object, as summarised in the two following propositions.

Proposition 2.1. *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 2.2. *Let $M \in \mathbb{Q}^{d\times d}$ be a matrix with rational entries, and $1 \le i, j \le d$. Then*

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

is a linear recurrence sequence of order at most d.

The proof of Proposition 2.1 is elementary, and Proposition 2.2 follows from the Cayley-Hamilton theorem, see [9, Chapter 1] for more details. Furthermore both operations are effective.

The **characteristic polynomial** of a linear recurrence (3) 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 our first result, Theorem 1.1, which we recall here.

Theorem 1.1. *Semialgebraic-to-semialgebraic reachability can effectively be reduced to point-to-polytope reachability.*

The main idea appears implicitly in the proof of [1, 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, $\mathbf{S}, \mathbf{T} \subseteq \mathbb{R}^d$ the source and target sets respectively, and M 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:

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

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 is some n such that $\Gamma'(M^n)$ holds. Since Γ' is quantifier-free, it can be written as a disjunction of formulas $\varphi_1, \ldots, \varphi_m$, for some $m \in \mathbb{N}$, such that each ϕ_i is of the form (2). 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:

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

Define, for all $i \in \{0, \ldots, k\}$ 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 Proposition 2.2 and the closure of linear recurrence sequences under component-wise addition and multiplication, that the sequences $\langle u_{i,n}\rangle_{n\in\mathbb{N}}$ are themselves linear recurrence sequences, of orders d_i, say. Applying Proposition 2.1 we construct matrices N_i of size $d_i \times d_i$, $0 \le i \le k$, that have 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, $1 \le i \le k$ 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 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 $\Delta(d_1), \ldots, \Delta(d_k)$. $\square$

Why does a similar proof not work for multiple reachability? The critical difference is 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.

3 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.[2] The variant that we reduce from is the following:

[2] A sketch of this proof has already appeared in [14].

Problem 3.1. *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 3.2. *Problem 3.1 is undecidable.*

Proof. Let $Q(x_1, \ldots, x_n)$ be an arbitrary polynomial with integer coefficients. For any subset $A \subseteq \{1, \ldots, n\}$, define Q_A to be the polynomial that one obtains by taking Q and 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 $x_1, \ldots, x_n$ if and only if one of the 2^n polynomials Q_A 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 [7, Chapter 5]), it follows that Problem 3.1 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 3.3 ([12]). *Problem 3.1 is undecidable for fixed $k = 9$.*

We will now show that Problem 3.1 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 Problem 3.1.

Lemma 3.4. *Let P be a univariate polynomial of degree d. The unique sequence that satisfies the recurrence*

$$\sum_{i=0}^{d+1} (-1)^i \binom{d+1}{i} v_{n-i} = 0, \qquad n > d+1. \tag{4}$$

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. The characteristic polynomial of the recurrence (4) 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., [9, Section 1.1.6]) that the set of solutions of (4) 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 (4) 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. □

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 (4) 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

$$\big(P(1), P(2), \ldots, P(d+1)\big)\, M_d^n\, \mathbf{h}_d^\top = P(n), \qquad \text{for all } n \in \mathbb{N}. \tag{5}$$

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 the algebraic set $S \subseteq \mathbb{R}^{2n+1}$ as:

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

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 3.5. *The following two statements are equivalent:*

- *The polynomial F has a solution in distinct positive integers.*
- *There is some $\mathbf{p} := (x_1, \ldots, x_{n+1}, y_1, \ldots, y_n) \in S$ 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 (5) imply that for all $r \in \mathbb{N}$ we have

$$\mathbf{p}\, M^r\, \mathbf{h}^\top = (r-y_1)(r-y_2)\cdots(r-y_n). \tag{6}$$

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 (6) 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. □

Proposition 3.2 and Lemma 3.5 imply that algebraic-to-hyperplane multiple reachability is undecidable, *i.e.* Theorem 1.2. Indeed the set S defined above is algebraic,[3] 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, in general we get 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 Proposition 3.3, we have the following theorem.

Theorem 3.6. *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 [2, 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 Positivity for diagonalisable linear recurrence sequences.

4 ALGORITHMS ON THE AFFINE PLANE

This section is devoted to proving Theorem 1.3 and Theorem 1.4. We give algorithms for deciding multiple reachability for various targets on the affine plane. The dimension $d = 2$ is fixed. The system is given in the form of a 2×2 matrix with rational entries. The eigenvalues of such a matrix can be one of the following: (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 $\rho \in \overline{\mathbb{Q}} \cap \mathbb{R}$. When the eigenvalues are a pair of complex conjugates and furthermore $|\lambda| = 1$ we say that the matrix is a **rotation**.

We will assume that $\lambda/\overline{\lambda}$ is not a root of unity, because this case is essentially the same as the case when 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.

[3] 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 $P(\mathbf{x})^2 + Q(\mathbf{x})^2 = 0$.

Proposition 4.1. *Let* $\mathbf{p} \in \mathbb{R}^2$ *be any point, not the origin,* 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 nondegenerate matrix. If 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.

$$\mathbf{p}\, M^n\, \mathbf{h}^\top = \mathbf{p}\, M^m\, \mathbf{h}^\top = 0, \tag{7}$$

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 (7) 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 (7) 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 (7) 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.[4]

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 [1] 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

[4] 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 [4].

example, the proposition above is about a target that passes through the origin, so the stretching effect of the linear map is not relevant.

4.1 Halfplane Targets

A semialgebraic set S is said to be **bounded** if there exists a real $\rho > 0$ such that S is contained in the open disk $x^2 + y^2 < \rho$. We call the infimum among such ρ the **radius** of the set S. The infimum among $\rho \geq 0$ such that the set S intersects the open disk of radius ρ 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 1.3, by giving an algorithm that decides multiple reachability for halfplanes. To this end, let S be the initial semialgebraic set, $\mathbf{T}$ the target halfplane, M a 2×2 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, φ). 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

$$(sr|\lambda|^n, n\vartheta + \vartheta_0 + \varphi). \tag{8}$$

The numbers s, r and $|\lambda|$ are real algebraic whose formulas we can compute, while ϑ and ϑ_0 are logarithms of algebraic numbers. We will make use of the following fact from Diophantine approximation. It is a corollary of [5, 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 4.2. *If ϑ is an irrational multiple of 2π, we have*

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

Proof of Theorem 1.3 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 $\mathbf{T}$. This simply means that 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 (8) is an irrational multiple of 2π. So by applying Lemma 4.2 to this number, we see that the intersection of the set

$$\{n\vartheta + \vartheta_0 + \phi \mod 2\pi \ : \ n \in \mathbb{N}\} \tag{9}$$

and the interval (ϕ_1, ϕ_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 $|\lambda| < 1$.[5] When the halfplane $\mathbf{T}$ has distance to the origin equal to 0, or when the source 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 S be bounded with radius ρ. Choose some $N \in \mathbb{N}$ such that $\rho|\lambda|^N < \delta$, then for any source point $\mathbf{p} \in \mathrm{S}$, 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

$$\mathrm{S}_n \stackrel{\text{def}}{=} \{\mathbf{p} \in \mathrm{S} \ : \ \mathbf{p}M^n \in \mathbf{T}\},$$

and decide whether there are m among them that have nonempty intersection. ◻

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

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 the diagonal matrix and B is invertible matrix with real algebraic entries. We can replace S by $\mathrm{S} \cdot B$, 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 4.3. *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, from some point on, the orbit either is in H and remains there forever, or it is outside H, and never enters 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. ◻

From this proof 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 4.3 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 has the form

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

Then the expression corresponding to (11) is

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

which likewise changes sign at most twice.

Proof of Theorem 1.3 for M with real eigenvalues. Lemma 4.3 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

$$\mathbf{p}M^{n_i} \in \mathbf{T} \quad \text{and} \quad 0 < n_{i+1} - n_i \leq 4 \quad \text{for all } n_i.$$

This contiguous multiple reachability question can easily be reduced to a union single reachability queries. Indeed, an orbit contains a pattern (of visits and not visits to H) of length $4m$ if and only if it reaches a certain polytopic the subset $\mathbf{P}$ of $\mathbb{R}^2$; A formula defining P can be constructed by considering the sets $\{x \in \mathbb{R}^2 \colon M^k x \in H\}$ and$\{x \in \mathbb{R}^2 \colon M^k x \notin H\}$ 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]. ◻

4.2 Rotations

Now we prove Theorem 1.4, which says that semialgebraic-to-semialgebraic multiple reachability is decidable on the plane for rotations.

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; M a matrix whose eigenvalues are the pair $\lambda, \overline{\lambda}$ on the unit circle, that is $|\lambda| = 1$, and let $m \in \mathbb{N}$. We show in this section that we can decide 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 begin our proof by treating an easier problem first, namely the question of entering the target set infinitely often.

Proposition 4.4. *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 1.3 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. ◻

If the first alternative in the proposition holds for some point in the source set, then clearly the answer to the multiple reachability problem is *yes*. We assume for the rest of this section that from every point in the source set, the target can be reached only finitely many times. More precisely:

Remark 4.5. *Assume that the input is such that for every point $\mathbf{p} \in \mathbf{S}$ in the source set, there are only finitely many positive or negative integers x such that $\mathbf{p}\, M^x \in \mathbf{T}$. In other words, the second alternative of Proposition 4.4 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 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

$$\Gamma(\mathbf{p}, M^{x_1}, \ldots, M^{x_m}) \tag{12}$$

holds. Eliminating the existential quantifiers for $\mathbf{v}$ from Γ, we effectively get another formula $\Gamma'(V_1, \ldots, V_m)$ such that (12) 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 (2), 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

$$\Psi(M^{x_1}, \ldots, M^{x_m}) \tag{13}$$

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 $n \in \mathbb{N}$

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

So when polynomials $P_0, \ldots, P_\ell$ are instantiated with M^x they can be seen as polynomials in λ^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 $(x_1, \ldots, x_m) \in \mathbb{Z}^m$.

When P_0 is identically zero, we will prove that there cannot be any solutions. This is due to the assumption that we have made in Remark 4.5. In fact, we prove a more general statement which will be useful later on.

Lemma 4.6. *Let $\Lambda \subseteq \mathbb{Z}^m$ be a subgroup, where the group operation is component-wise addition. If 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 (or equivalently 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 for Diophantine approximation to prove that if there is some element of the subgroup $(x_1, \ldots, x_m) \in \Lambda$ for which

$$Q_i(\lambda^{x_1}, \ldots, \lambda^{-x_m}) > 0,$$

then there are infinitely many of them—which contradicts the assumption that we have made in Remark 4.5.

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:

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

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:

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

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 this claim:

Claim 4.7. *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 (12) holds which contradicts the assumption made in Remark 4.5, 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 a theorem from Diophantine approximations due to Kronecker, which is convenient to state here.

Theorem 4.8 (Theorem IV in Page 53 of [5]). *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 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 $1 \leq j \leq m$ 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:

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

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

$$(\lambda^{L_1(\mathbf{a})/\vartheta}, \ldots, \lambda^{L_m(\mathbf{a})/\vartheta}) \in \mathbf{R}, \tag{14}$$

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 (14) 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 4.7 and that of the lemma. ◻

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

Lemma 4.9. *There exists an effective bound $B \in \mathbb{N}$ depending only on Q_0, such that if there is some solution in $\mathbb{N}^m$, then there is one (call it $\mathbf{x}$) in $\mathbb{Z}^m$, with*

$$\|\mathbf{x}\| \stackrel{\text{def}}{=} \sum |x_i| \leq B.$$

Since both λ and the coefficients of the polynomials are algebraic numbers, we can use Tarski's algorithm to check whether each of $\mathbf{x}$, $\|\mathbf{x}\| \leq B$, is a solution. Therefore as a consequence of Lemma 4.9 and Proposition 4.4, multiple reachability for rotations is decidable, *i.e.* Theorem 1.4 holds.

For the proof of Lemma 4.9, we will make use of certain interesting results regarding the intersection of varieties with algebraic subgroups of dimension 1, due to Zannier, Bombieri, and Schmidt. In order to state these results, we need a few definitions. The general theory is developed more extensively in [18], [17], and especially in [3, 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[6] $\mathbb{G}_m^n$ 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 has a group structure, where the group operation is given by 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 $X_0 \subseteq \mathbb{G}_m^n$, is the zero set of our polynomial Q_0, conjoined with polynomial equations

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

where $1 \leq j \leq n$ 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 $\mathbb{G}_m^n$ that is also a subgroup. As an example, given an additive subgroup $\Gamma \subseteq \mathbb{Z}^n$, we can see that it determines an algebraic subgroup

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

In fact every algebraic subgroup is of this type, [3, 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 [10, Definition on Page 5].

Lemma 4.10. *For all $(a_1, \ldots, a_k) \in \mathbb{Z}^k$, the point*

$$\left(\lambda^{a_1}, \ldots, \lambda^{a_k}\right)$$

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:

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

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. □

We will denote by $\mathcal{H}_1(n)$ the union of all algebraic subgroups of $\mathbb{G}_m^n$ 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 according to the lemma above, this 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_0 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 $g \in \mathbb{G}_m^n$.

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

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

Also define

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

We will analyse the points in $X_0^\bullet \cap \mathcal{H}_1$ and those in $X_0^\circ \cap \mathcal{H}_1$ in the next two subsections, calling them respectively the tall points and the short points.

4.2.1 *Tall Points.* 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 $\varphi_A \;:\; \mathbb{G}_m^n \to \mathbb{G}_m^n$ 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 ± 1, φ_A is an isomorphism[7] 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 important basic results related to the structure of algebraic subgroups. Recall that we have used the notation $\|\mathbf{a}\|$ for the ℓ^1 norm; when A is a matrix, we denote by $\|A\|$ the maximum of ℓ^1 norms of its columns.

Proposition 4.11 ([3, 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*

[6] The subscript m in the notation $\mathbb{G}_m^n$ stands for "multiplicative" and is unrelated to the input $m \in \mathbb{N}$ in our decision problem which stands for the number of times we aim enter the target set.

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

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*

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

where

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

From the bounds of $\mathbb{G}_m^A$, we can effectively compute this matrix, given $n-r$ independent vectors of Λ.

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

Proposition 4.12 ([3, Proposition 3.2.14]). *Let* $X \subseteq \mathbb{G}_m^n$ *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* $\mathbb{G}_m^n$ *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 simply isomorphic to $\mathbb{G}_m^r$, 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 $\mathbb{G}_m^{n-r}$ 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 $g^{-1}X$. Proposition 4.12 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 4.13. *We can effectively construct a (possibly empty) 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

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

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

Lemma 4.14 ([3, Theorem 3.3.9]). *Let* $X \subseteq \mathbb{G}_m^n$ *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*

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

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

Proof. Using Proposition 4.12 we can conclude that $H = H_\Lambda$ where Λ is a subgroup of $\mathbb{Z}^n$ of rank $n-r$, and from Proposition 4.11, we can compute a matrix A, such that $H = \varphi_A(\mathbf{1}_{n-r} \times \mathbb{G}_m^r)$. If we define $\widetilde{X}$ to be $\varphi_A^{-1}(X)$, we have

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

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

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

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

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 4.9, we first discuss the points in X°.

4.2.2 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 [3]. 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

$$\log^+ t = \max(0, \log t).$$

Then the **height**[8] of a point $\mathbf{z} = (z_1,\dots,z_n) \in K^n$ 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 $(\lambda^{x_1},\dots,\lambda^{x_n})$, where $x_i \in \mathbb{Z}$. The height of such points has the following properties:

Lemma 4.15. *Let* $\mathbf{x} \in \mathbb{Z}^n$*, and denote by* $M = \max_j |x_j|$. *Then*

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

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

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

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 [3, Lemma 1.5.18]), we get the upper bound. For the lower bound:

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

◻

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

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 4.16 ([17, Theorem 1, Page 524]). *Let $X \subseteq \mathbb{G}_m^n$ be a subvariety. Then there exists an effective bound $b \in \mathbb{N}$ depending only on X such that for all algebraic points $\mathbf{z} \in \mathbb{G}_m^n$,*

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

The theorem cited in [17] does not explicitly state that the bound is effective, but upon a closer inspection of the proof one can see that almost 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 it is possible to describe the algorithm that computes the bound of Lemma 4.9.

4.2.3 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 4.10 these points also belong to $\mathcal{H}_1 \cap X_0$. From Theorem 4.16 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 4.13 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 4.14 we can compute a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$ such that

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

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 4.6, so for all $\mathbf{x} \in \mathbb{Z}^m$, and $g \in \mathbb{G}_m^n$ 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 4.14, we compute a matrix $A \in \mathrm{SL}(n, \mathbb{Z})$, and the subvariety $X_1 \subseteq \mathbb{G}_m^{n-r}$, such that

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

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

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

Let b_1' be the bound we get from Theorem 4.16 when applied to the intersection

$$X_1^\circ \cap \mathcal{H}_1(n-r). \tag{15}$$

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 4.15, implies that if $\widetilde{y} > b_1'/h(\lambda)$, $(\lambda^{y_1}, \ldots, \lambda^{y_{n-r}})$ does not belong to the intersection in (15). 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 $\varphi_A(X_1^\circ \times \mathbb{G}_m^r)$, 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., [11]). 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 $\varphi_A(X_1^\circ \times \mathbb{G}_m^r)$, 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 4.14 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 4.13 is finite.

This concludes the proof of Lemma 4.9, and that of Theorem 1.4.

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 that in Theorem 4.16, but for subgroups of dimension 2. There are finiteness results, often as special cases of the Mordell-Lang conjecture, see *e.g.* [15], but to our knowledge, no effective bounds are known.

ACKNOWLEDGMENTS

Toghrul Karimov and Joël Ouaknine were supported by DFG grant 389792660 as part of TRR 248 (see https://perspicuous-computing.science). Joël Ouaknine is also affiliated with Keble College, Oxford as `emmy.network` Fellow. James Worrell was supported by EPSRC Fellowship EP/X033813/1.

REFERENCES

[1] 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

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

[3] Enrico Bombieri and Walter Gubler. 2007. *Heights in Diophantine geometry.* Number 4. Cambridge university press.

[4] w B Brindza, A Pintér, and WM Schmidt. 2001. Multiplicities of binary recurrences. *Canad. Math. Bull.* 44, 1 (2001), 19–21.

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

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

[7] 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

[8] 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

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

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

[11] Rui-Juan Jing and Marc Moreno Maza. 2017. Computing the integer points of a polyhedron, I: algorithm. In *International Workshop on Computer Algebra in Scientific Computing*. Springer, 225–241.

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

[13] 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

[14] 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

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

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

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

[18] 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.

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

A MISSING CASES FOR THEOREM 1.3

- 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

$$\begin{cases} c_1 x|\rho_1|^n + c_2 y\rho_2^n > c_3, & \text{n even}, \quad (16a) \\ -c_1 x|\rho_1|^n + c_2 y\rho_2^n > c_3, & \text{n odd}. \quad (16b) \end{cases}$$

Depending on the signs of x and y, one of the inequalities implies the other. Without loss of generality suppose (16a) implies (16b). By Lemma 4.3, the set of n satisfying (16a) 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 $F : \mathbb{R} \to \mathbb{R}$,

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

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

$$c_1 x\rho_1^n + c_2 y\rho_2^n = \begin{cases} F(n) \text{ if } n \text{ is even}, \\ -F(n) \text{ if } n \text{ is odd}. \end{cases} \quad (17)$$

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 (17) 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.

- Non-diagonalisable M with a repeated eigenvalue.

A version of Lemma 4.3 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

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

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.

- 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.