On Termination of Integer Linear Loops

Joël Ouaknine  
Department of Computer Science  
Oxford University, UK  

João Sousa Pinto  
Department of Computer Science  
Oxford University, UK  

James Worrell  
Department of Computer Science  
Oxford University, UK  

Abstract

A fundamental problem in program verification concerns the termination of simple linear loops of the form:

\[ x \leftarrow u; \text{ while } Bx \geq b \text{ do } x \leftarrow Ax + a, \]

where \( A \) and \( B \) are integer matrices, and \( u, a, \) and \( b \) are integer vectors. We give a decision procedure for the problem of whether such a loop terminates for all initial integer vectors \( u \), provided that the matrix \( A \) is diagonalisable. The correctness of our algorithm relies on sophisticated tools from algebraic and analytic number theory, Diophantine geometry, and real algebraic geometry.

To the best of our knowledge, this is the first substantial advance on a 10-year-old open problem of Tiwari [35] and Braverman [8].

1 Introduction

Termination is a fundamental decision problem in program verification. In particular, termination of programs with linear assignments and linear conditionals has been extensively studied over the last decade. Most notably this has led to the development of powerful techniques to prove termination via synthesis of linear ranking functions [6, 7, 11, 14, 29], leading to the development of tools such as Microsoft's TERMINATOR [15].

A very simple form of linear programs are simple linear loops, that is, programs of the form

\[ P1: x \leftarrow u; \text{ while } Bx \geq b \text{ do } x \leftarrow Ax + a, \]

where \( x \) is an \( d \)-dimensional vector of variables, \( u \) and \( a \) are \( d \)-dimensional vectors of integers, and \( b \) is a \( c \)-dimensional vectors of integers, \( A \) is a \( d \times d \) integer matrix, and \( B \) is a \( c \times d \) integer matrix. Here the loop guard is a conjunction of \( c \) linear inequalities and the loop body consists in a simultaneous affine assignment to \( x \). If the vectors \( a \) and \( b \) are both zero then we say that the loop is homogeneous.

We say that \( P1 \) terminates on a set \( S \subseteq \mathbb{R}^d \) if it terminates for all initial vectors \( u \in S \). Tiwari [35] gave a procedure to decide whether a given simple linear loop terminates on \( \mathbb{R}^d \). Later Braverman [8] showed decidability of termination on \( \mathbb{Q}^d \). However the most natural problem, from the point of view of program verification, is termination on \( \mathbb{Z}^d \). While termination on \( \mathbb{Z}^d \) reduces to termination on \( \mathbb{Q}^d \) in the homogeneous case (by a straightforward scaling argument), termination on \( \mathbb{Z}^d \) in the general case is stated as an open problem in [8, 35, 5]. The main result of this paper is a procedure to decide termination on \( \mathbb{Z}^d \) for simple linear loops when the assignment matrix \( A \) is diagonalisable. This represents the first substantial progress on this open problem in over 10 years.

Termination of more complex linear programs can often be reduced to termination of simple linear loops (see, e.g., [35, Section 6] or [15]). On the other hand, termination becomes undecidable for mild generalisations of simple linear loops, for example, allowing the update function in the loop body to be piecewise linear [5].

To prove our main result we focus on eventual non-termination, where \( P1 \) is said to be eventually non-terminating on \( u \in \mathbb{Z}^d \) if after executing the loop body \( x \leftarrow Ax + a \) a finite number of times (disregarding the loop guard), we eventually reach a value on which \( P1 \) fails to terminate. Clearly \( P1 \) is non-terminating on \( \mathbb{Z}^d \) if and only if it is eventually non-terminating on some \( u \in \mathbb{Z}^d \).

Given an integer linear loop we show how to compute a convex semi-algebraic set \( W \subseteq \mathbb{R}^d \) such that the integer points \( u \in W \) are precisely the integer eventually non-terminating initial values. Since it is decidable
whether a convex semi-algebraic set contains an integer point \(21\), we can decide whether an integer linear loop is terminating.

Termination over the set of all integer points is easily seen to be coNP-hard. Indeed, if the update function in the loop body is the identity then the loop is non-terminating if and only if there is an integer point satisfying the guard. Thus non-termination subsumes integer programming, which is NP-hard. By contrast, even though not stated explicitly in \[35\] and \[8\], deciding termination on \(\mathbb{R}^d\) and \(\mathbb{Q}^d\) can be done in polynomial time.\[5\]

While our algorithm for deciding termination requires exponential space, it should be noted that the procedure actually solves the more general problem of whether a given convex semi-algebraic set contains an eventually non-terminating integer point. For reference, the closely related problem of deciding termination on the integer points in a given polytope is EXPSPACE-hard \[3\].

As well as making extensive use of algorithms in real algebraic geometry, the soundness of our decision procedure relies on powerful lower bounds in Diophantine approximation that generalise Roth’s Theorem. (The need for such bounds in the inhomogeneous setting was hinted at in the discussion in the conclusion of \[8\].) We also use classical results in number theory, such as the Skolem-Mahler-Lech Theorem \[22\] \[25\] \[33\] on linear recurrences. Crucially the well-known and notorious ineffectiveness of Roth’s Theorem (and its higher-dimensional and \(p\)-adic generalisations) and of the Skolem-Mahler-Lech Theorem are not a problem for deciding eventual non-termination, which is key to our approach.

1.1 Related Work

Consider the termination problem for a homogeneous linear loop program

\[
P2 : x \leftarrow u ; \text{ while } Bx \geq 0 \text{ do } x \leftarrow Ax
\]

don a single initial value \(u \in \mathbb{Z}^d\). Each row \(b^T\) of matrix \(B\) corresponds to a loop condition \(b^T x \geq 0\). For each such condition consider the integer sequence \((x_n : n \in \mathbb{N})\) defined by \(x_n = b^T A^n u\). Then \(P2\) fails to terminate on an initial value \(u\) if and only if each such sequence \((x_n)\) is positive, i.e., \(x_n \geq 0\) for all \(n\). It is not difficult to show that each sequence \((x_n)\) considered above is a linear recurrence sequence. Thus deciding whether a homogeneous linear loop program terminates on a given initial value is at least as hard as the Positivity Problem for linear recurrence sequences, that is, the problem of deciding whether a given linear recurrence sequence has exclusively non-negative terms.

The Positivity Problem has been studied at least as far back as the 1970s \[4\] \[18\] \[21\] \[30\] \[31\]. Thus far decidability is known only for sequences satisfying recurrences of order at most 5. It is moreover known that showing decidability at order 6 will necessarily entail breakthroughs in transcendental number theory, specifically significant new results in Diophantine approximation \[27\].

The key difference between studying termination over \(\mathbb{Z}^d\) rather than a single initial value is that the former problem can be approached through eventual termination. This allows us to bring powerful non-effective Diophantine-approximation techniques to bear, specifically the \(S\)-units Theorem of Evertse, van der Poorten, and Schlickewei \[17\] \[36\]. Such tools allow us to obtain decidability of termination for matrices of arbitrary dimension, assuming diagonalisability.

The paper \[12\] studies point-to-set reachability problems in linear systems. These are versions of termination problem for linear loops over a fixed initial value. That work uses substantially different technology than the current paper, including Baker’s Theorem on linear forms in logarithms \[2\], and correspondingly relies on restrictions on the dimension of data in problem instances.

While we use spectral and number-theoretic techniques in this paper, another well-studied approach for proving termination of linear loops involves designing linear ranking functions, that is, linear functions from the state space to a well-founded domain such that each iteration strictly decreases the image by this function. However, this approach is incomplete: it is not hard to construct an example of a universally terminating loop which admits no linear ranking function. Complete and sound methods for synthesising linear ranking functions can be found in \[29\] and \[6\]. Whether such a function exists can be decided in polynomial time when the state space is \(\mathbb{Q}^2\) and is coNP-complete when the state space is \(\mathbb{Z}^2\).

\[1\] This observation relies on the facts that one can compute Jordan canonical forms of integer matrices and solve instances of linear programming problems with algebraic numbers in polynomial time \[2\] \[4\].
2 Overview of Main Results

Recall that we are interested in deciding termination of simple linear loops, that is, loops of the form $P_1$, on $\mathbb{Z}^d$ (see Section 1). We will obtain decidability under the assumption that the update matrix $A$ is diagonalisable or has dimension at most 4.

Let $f : \mathbb{R}^d \rightarrow \mathbb{R}^d$ be the affine function $f(x) = Ax + a$ computed by the body of the while loop in $P_1$ and $\mathcal{P} = \{ x \in \mathbb{R}^d : Bx \geq b \}$ the polytope corresponding to the loop guard. We define the set of non-terminating points to be

$$NT = \{ u \in \mathbb{R}^d : \forall n \in \mathbb{N} f^n(u) \in \mathcal{P} \}.$$  

We moreover define the set of eventually non-terminating points to be

$$ENT = \{ u \in \mathbb{R}^d : \exists n \in \mathbb{N} f^n(u) \in NT \}.$$  

It is easily seen from the above definitions that both $NT$ and $ENT$ are convex sets.

By definition, $P_1$ is non-terminating on $\mathbb{Z}^d$ if and only if $NT$ contains an integer point. It is moreover clear that $NT$ contains an integer point if and only if $ENT$ contains an integer point.

Define $W \subseteq \mathbb{R}^d$ to be a non-termination witness set (or simply a witness set) if it satisfies the following two properties (where $\mathcal{A}$ denotes the set of algebraic numbers):

(i) $W$ is convex and semi-algebraic;

(ii) $W \cap \mathcal{A}^d = ENT \cap \mathcal{A}^d$.

The integer points in a witness set $W$ are precisely the integer points of $ENT$, and so $P_1$ is non-terminating on $\mathbb{Z}^d$ precisely when $W$ contains an integer point. Our approach to solving the termination problem consists in computing a witness set $W$ for a given program and then using the following theorem of Khachiyan and Porkolab [21] to decide whether $W$ contains an integer point.

**Theorem 1** (Khachiyan and Porkolab). Let $W \subseteq \mathbb{R}^d$ be a convex semi-algebraic set defined by polynomials of degree at most $D$ and that can be represented in space $S$. In that case, if $W \cap \mathbb{Z}^d \neq \emptyset$, then $W$ must contain an integral point that can be represented in space $SD^{O(d^2)}$.

Our approach does not try to characterise the set $ENT$ directly, but rather uses the witness set $W$ as a proxy. However, as an aside, we note here some properties of $ENT$. It holds that the topological closure $\overline{ENT}$ is semi-algebraic. Indeed from property (ii) of a witness set it can be shown that $W = \overline{ENT}$. (In order to show this one relies on the fact that algebraic points are dense both in $\mathrm{span}(ENT)$ and $W$. The former follows from work in [8], while the latter is an instance of the general fact that algebraic points are dense in any semi-algebraic set—see the Appendix for details). But the closure of a semi-algebraic set is again semi-algebraic, and thus $ENT$ is semi-algebraic. We leave open the question of whether $ENT$ itself is semi-algebraic.

We next describe some simplifications that will ease our upcoming analysis.

Program $P_1$ terminates on a given initial value $u \in \mathbb{Z}^d$ if and only if the homogeneous program $P_3$ below terminates for the same value of $u$:

$$P_3 : x \leftarrow \begin{pmatrix} u \\ 1 \end{pmatrix} \ ; \ \text{while} \ (B \ -b) x \geq 0 \ \text{do} \ x \leftarrow \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} x.$$  

Note that if $A$ is diagonalisable then the only eigenvalue of $\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix}$ that may be defective is 1. Now if $W$ is a witness set for program $P_3$ then \[ \{ u \in \mathbb{R}^d : \ \begin{pmatrix} u \\ 1 \end{pmatrix} \in W \} \] is a witness set of $P_1$. We conclude that, in order to settle the inhomogeneous case with a diagonalisable matrix, it suffices to compute a witness set in the case of a homogeneous linear loop $P_2$ in which the only defective eigenvalues of matrix $A$ are positive and real (namely, the eigenvalue 1), due to the obvious relation between the set of eventually non-terminating points of $P_1$ and that of $P_3$. Likewise, to handle the inhomogeneous case for matrices of dimension at most $d$, it suffices to be able to compute witness sets in the homogeneous case for matrices of dimension at most $d+1$.
We can further simplify the homogeneous case by restricting to loop guards that comprise a single linear inequality. To see this, first note that program $P_2$ above is eventually non-terminating on $u$ if and only if for each row $b^T$ of $B$ program $P_4$ below is eventually non-terminating on $u$:

$$P_4 : x \leftarrow u ; \text{while } b^T x \geq 0 \text{ do } x \leftarrow Ax.$$ 

Noting that the finite intersection of convex semi-algebraic sets is again convex and semi-algebraic, we can compute a witness set for $P_2$ as the intersection of witness sets for each version of $P_4$.

The final simplification concerns the notion of non-degeneracy. We say that matrix $A$ is degenerate if it has distinct eigenvalues $\lambda_1 \neq \lambda_2$ whose quotient $\lambda_1/\lambda_2$ is a root of unity.

Given an arbitrary matrix $A$, let $L$ be the least common multiple of all orders of quotients of distinct eigenvalues of $A$ which are roots of unity. It is known that $L = 2^{O(d \sqrt{\log d})}$ [10]. The eigenvalues of the matrix $A^L$ have the form $\lambda^L$ for $\lambda$ an eigenvalue of $A$, by the spectral mapping theorem. It follows that $A^L$ is non-degenerate, since if $\lambda_1, \lambda_2$ are eigenvalues of $A$ such that $\lambda_1^L/\lambda_2^L$ is a root of unity then $\lambda_1/\lambda_2$ is a root of unity and hence $\lambda_1^L/\lambda_2^L = 1$.

Now program $P_4$ is eventually non-terminating on $u \in \mathbb{Z}^d$ if and only if program $P_5$ below is eventually non-terminating on the set $\{u, Au, \ldots, A^{L-1}u\}$:

$$P_5 : x \leftarrow v ; \text{while } b^T x \geq 0 \text{ do } x \leftarrow A^Lx.$$ 

Thus if $W$ is a witness set for $P_5$ then $\bigcap_{k=0}^{L-1} \{u \in \mathbb{Z}^d : A^k u \in W\}$ is a witness set for $P_4$.

In summary, we may henceforth assume that all simple linear loops are homogeneous, with a single guard, and with a non-degenerate transition matrix $A$. In unbounded dimension, we also assume that the only defective eigenvalue of $A$ is 1. Otherwise, we assume that $A$ has dimension at most 5.

Under the above restrictions we compute a witness set $W$ for a simple linear loop $P_4$ as follows. First we partition the eigenvalues of the update matrix $A$ by grouping eigenvalues of equal modulus. Correspondingly we write $\mathbb{R}^d$ as a direct sum $\mathbb{R}^d = V_1 \oplus \ldots \oplus V_m$, where each subspace $V_i$ is the sum of (generalised) eigenspaces of $A$ associated to eigenvalues of the same modulus. Assume that $V_1$ corresponds to the eigenvalues of maximum modulus, $V_2$ the next greatest modulus, etc. Then there are two main steps in the construction of $W$:

1. By analysing multiplicative relationships among eigenvalues of the same modulus, we show that for each subspace $V_i$ the set $\text{ENT} \cap V_i$ of eventually non-terminating initial values in $V_i$ is semi-algebraic.

2. Given $v \in \mathbb{R}^d$, we can write $v = v_1 + \ldots + v_m$, with $v_i \in V_i$. Using Theorem [10] on $S$-units, we show that if all entries of $v$ are algebraic numbers then the eventual non-termination of $P_4$ on $v$ is a function of its eventual non-termination on each $v_i$ separately. More precisely we look for the first $v_i$ such that the sequence $\{b^T A^n v_i : n \in \mathbb{N}\}$ is not identically 0. Then $P_4$ is eventually non-terminating on $v$ if and only if it is eventually non-terminating on $v_i$.

The computability of a witness set $W$ easily follows from items 1 and 2 above. Our techniques require either that the update matrix in the original linear loop $P_1$ be either diagonalisable or have dimension at most 4. Eliminating these restrictions seems to require solving the Ultimate Positivity Problem for linear recurrence sequences of order greater than 5, which in turn requires solving some open problems in the theory of Diophantine approximation [27].

### 3 Groups of Multiplicative Relations

This section introduces some concepts concerning groups of multiplicative relations among eigenvalues. Here we will assume some basic notions from algebraic number theory and the first-order theory of reals. Details of the relevant notions can be found in the Appendix.

Letting $T = \{z \in \mathbb{C} : |z| = 1\}$, we define the $s$-th dimensional torus as $T^s$, which is a group under componentwise multiplication.

Given $\lambda = (\lambda_1, \ldots, \lambda_s) \in T^s$ and $v = (v_1, \ldots, v_s) \in \mathbb{Z}^s$, we define $\lambda^v = \lambda_1^{v_1} \cdots \lambda_s^{v_s}$. Moreover, if $\lambda$ is a tuple of algebraic numbers, we define the group of multiplicative relations of $\lambda$, which is an additive subgroup of $\mathbb{Z}^s$, as

$$L(\lambda) = \{v \in \mathbb{Z}^s : \lambda^v = 1\}$$
Since \( \mathbb{Z}^s \) is a free abelian group, so must be all its subgroups. In particular, this implies that \( L(\lambda) \) has a well-defined finite dimension and a basis. The following powerful theorem, by Masser [26], allows us to compute such a basis in polynomial space.

**Theorem 2** (Masser). The free abelian group \( L(\lambda) \) has a basis \( \mathbf{v}_1, \cdots, \mathbf{v}_l \in \mathbb{Z}^s \) for which

\[
\max_{1 \leq i \leq l, 1 \leq j \leq s} |v_{i,j}| \leq (D \log H)^{O(s^2)}
\]

where \( H \) and \( D \) bound respectively the heights and degrees of all the \( \lambda_i \).

Moreover, we consider the following multiplicative subgroup of \( \mathbb{T}^s \):

\[
T(\lambda) = \{ \mathbf{\mu} \in \mathbb{T}^s : \forall \mathbf{v} \in L(\lambda), \mathbf{\mu}^\mathbf{v} = 1 \}
\]

Having a basis for \( L(\lambda) \) allows us to effectively test membership of \( T(\lambda) \), and most importantly lets us represent it as a semi-algebraic set.

We will use the following lemma, due to Kronecker, in order to show that the orbit \( \{ \lambda^n : n \in \mathbb{N} \} \) is a dense subset of \( T(\lambda) \).

**Lemma 1** (Kronecker). Let \( \theta, \psi \in \mathbb{R}^s \). Adding to that, suppose that for all \( \mathbf{v} \in \mathbb{Z}^s \), if \( \mathbf{v}^T \theta \in \mathbb{Z} \) then also \( \mathbf{v}^T \psi \in \mathbb{Z} \), i.e., all integer relations among the coordinates of \( \theta \) also hold among those of \( \psi \) (modulo \( \mathbb{Z} \)). Then, for each \( \varepsilon > 0 \), there exist \( \mathbf{p} \in \mathbb{Z}^s \) and a non-negative integer \( n \) such that

\[
\|n \theta - \mathbf{p} - \mathbf{\psi}\|_\infty \leq \varepsilon
\]

Therefore, as claimed:

**Theorem 3.** Let \( \lambda \in \mathbb{T}^s \). Then the orbit \( \{ \lambda^n : n \in \mathbb{N} \} \) is a dense subset of \( T(\lambda) \).

*Proof.* Let \( \theta \in \mathbb{R}^s \) be such that \( \lambda = e^{2\pi i \theta} \) (coordinatewise). Notice that \( \lambda^n = 1 \Leftrightarrow \mathbf{v}^T \theta \in \mathbb{Z} \). If \( \mathbf{\mu} \in T(\lambda) \), we can likewise define \( \psi \in \mathbb{R}^s \) to be such that \( \mathbf{\mu} = e^{2\pi i \psi} \). Then the premisses of Kronecker’s lemma apply to \( \theta \) and \( \psi \). Thus, given \( \varepsilon > 0 \), there exist a non-negative integer \( n \) and \( \mathbf{p} \in \mathbb{Z}^s \) such that \( \|n \theta - \mathbf{p} - \mathbf{\psi}\|_\infty \leq \varepsilon \). Whence

\[
\|\lambda^n - \mathbf{\mu}\|_\infty = \|e^{2\pi i (n \theta - \mathbf{p})} - e^{2\pi i \psi}\|_\infty \leq 2\pi \|n \theta - \mathbf{p} - \mathbf{\psi}\|_\infty \leq 2\pi \varepsilon
\]

\[\Box\]

### 4 Algorithm for Universal Termination

Recall that our goal is to compute a witness set for linear loops of the form

\[
P4 : x \leftarrow \mathbf{u} ; \text{while } b^T x \geq 0 \text{ do } x \leftarrow A x.
\]

where \( A \) is a \( d \times d \) integer matrix and \( b \) and \( u \) are \( d \)-dimensional integer vectors.

Let \( \sigma(A) \) denote the spectrum of \( A \) and for each \( \lambda \in \sigma(A) \), let \( \nu(\lambda) \) be the index of \( \lambda \), that is, its multiplicity as a root of the minimal polynomial of \( A \), or equivalently the size of its largest corresponding Jordan block.

Henceforth, we will focus on proving the following result:

**Theorem 4.** Given a vector \( \mathbf{b} \in \mathbb{Z}^d \) a non-degenerate matrix \( A \in \mathbb{Z}^{d \times d} \), we can construct a witness set \( W \) for \( P2 \) in exponential space, as long as there is no pair \( (\alpha, \beta) \) of eigenvalues of \( A \) such that \( \alpha \in \mathbb{R}^+, \beta \in \mathbb{C} \setminus \mathbb{R}, |\alpha| = |\beta| \), and both \( \alpha \) and \( \beta \) have indices greater than one.

In particular, this is always the case if \( A \) is diagonalisable, if all defective eigenvalues are positive real, or if \( d \leq 5 \), since \( \lambda \in \sigma(A) \Rightarrow \chi \in \sigma(A) \) and \( \nu(\lambda) = \nu(\chi) \).

We remind the reader that the reduction step which made our problem instance homogeneous increased the dimension of the ambient space by 1, thus we can only solve non-diagonalisable inhomogeneous instances up to dimension 4 in general.
We can write matrix $A$ in the form $A = PJP^{-1}$ for some invertible matrix $P$ and block diagonal Jordan matrix $J$. The entries of $P$ are all algebraic numbers lying in the extension field of $\mathbb{Q}$ generated by the eigenvalues of $A$, and the entries of $J$ are all in the ring of integers of that number field.

One can easily compute closed-form expressions for powers of matrices in Jordan Canonical Form \cite{35,8}, and in particular there are vectors of polynomials $p_\lambda \in \mathbb{A}[x]^d$ with degrees $\nu(\lambda) - 1$ such that, for all $n \geq 0$,

\[ b^T A^n x = b^T P J^n P^{-1} x = \left( \sum_{\lambda \in \sigma(A)} p_\lambda(n) \lambda^n \right) x \text{ and } p_\lambda(n) = \sum_{j=0}^{\nu(\lambda) - 1} c(\lambda, j) n^j \]

Pick $t \in \mathbb{N}$ such that, for all $\lambda \in \sigma(A)$ and $j \in \{0, \ldots, \nu(\lambda) - 1\}$, $t c(\lambda, j)$ is a vector of algebraic integers, and since $b^T A^n x > 0 \iff t(b^T A^n x) > 0$, we can assume without loss of generality that all these coefficients are vectors whose coordinates are algebraic integers.

The first step in our analysis is to partition the eigenvalues of $A$ by grouping eigenvalues of equal modulus into classes $S_1, \ldots, S_m$. Correspondingly we write $\mathbb{R}^d$ as a direct sum of subspaces $\mathbb{R}^d = V_1 \oplus \cdots \oplus V_m$, where each subspace $V_j$ is the sum of the (generalised) eigenspaces of $A$ associated to eigenvalues of the same modulus and $\rho_1, \ldots, \rho_m$ correspond to the moduli of the eigenvalues in $S_1, \ldots, S_m$ respectively. We assume without loss of generality that $i < j \iff \rho_i > \rho_j$.

By assumption on $A$, no quotient of two distinct eigenvalues can be a root of unity, and in particular it must hold that $\rho \in \sigma(A) \Rightarrow -\rho \notin \sigma(A)$, and so no $S_i$ can simultaneously intersect $\mathbb{R}^+$ and $\mathbb{R}^-$, that is, $S_j$ has at most one real eigenvalue.

We tackle the cases where these classes $S_j$ may fall into several different categories:

- All complex eigenvalues have index one, a positive real eigenvalue has index at least one
- A conjugate-pair of complex eigenvalues has index at least one, all other eigenvalues have index one

We say that a class $S_j$ is \textbf{dominant for $x$} if no eigenvalue of norm greater than $\rho_j$ appears in the closed form expression for $b^T A^n x$, but some eigenvalue of norm $\rho_j$ does. It is well known that if $b^T A^n x$ is not identically zero and some class $S_j$ with no positive real eigenvalues is dominant for $x$, then $b^T A^n x < 0$ must hold for infinitely many $n \in \mathbb{N}$ \cite{35}, and so must $b^T A^n x > 0$.

We define

\[ \text{ZERO} = \{ x \in \mathbb{R}^d : \forall n \geq d, b^T A^n x = 0 \} \]

We will start by showing the following proposition:

\textbf{Proposition 1.} \textit{If $S_j$ fits in either category and for each $j \in \{1, \ldots, m\}$, ENT $\cap V_j$ and NULL $\cap V_j$ are convex semi-algebraic sets.}

Let ENT$_j = \text{ENT} \cap V_j$ and ZERO$_j = \text{ZERO} \cap V_j$, for each $j$. We now fix $S_j$ and $x = (x_1, \ldots, x_d) \in V_j$, and proceed to characterising ZERO$_j(x)$ and ENT$_j(x)$ with formulas in the first-order theory of reals, according to which case $S_j$ fits in.

\textbf{Case I: All complex eigenvalues have index one, a positive real eigenvalue has index at least one}

Assume that the eigenvalues in $S_j$ comprise a real eigenvalue $\rho_j$ and conjugate-pairs of complex eigenvalues $\lambda_1, 1, \ldots, \lambda_s, 1$.

For each $i \in \{1, \ldots, s\}$, let $\mu_i = \lambda_i / \rho_j$ and $\mu = (\mu_1, \ldots, \mu_s) \in \mathbb{T}^s$. We now define

\[ f : \mathbb{T}^s \rightarrow \mathbb{R}^d, \quad (z_1, \ldots, z_s) \mapsto c(\rho_j, 0) + \sum_{i=1}^s c(\lambda_i, 0) z_i + \overline{c(\lambda_i, 0) z_i} \]

If, for some $i \in \{1, \ldots, \nu(\rho_j) - 1\}$, it holds that $c(\rho_j, i) x \neq 0$, then the dominating term of $b^T A^n x$ will be $\Theta(n^M \rho_j^n)$, where $M = \max\{i : c(\rho_j, s) x \neq 0\}$, and so $b^T A^n x$ will tend to $\infty$ (and therefore be ultimately positive) as $n \rightarrow \infty$ when $c(\rho_j, M) x > 0$ and to $-\infty$ when $c(\rho_j, s) x < 0$. 

\[ \]
Otherwise, it will be the case that $b^T A^n x = \rho_j^n f(\mu^n) x$. But due to Theorem \[ \mu^n : n \in \mathbb{N} \] is dense in $T(\mu)$, and so we can take

$$
ENT_j(x) = \left\{ \begin{array}{l}
\bigvee_{i=1}^{\nu(\phi_i)-1} \left( c(\phi_i, i)x > 0 \land \bigwedge_{k=i+1}^{\nu(\phi_i)-1} c(\phi, k)x = 0 \right) \\
\end{array} \right\} \forall
$$

$$
\{ \bigwedge_{i=1}^{\nu(\phi_i)-1} c(\phi_i, i)x = 0 \} \land (\forall z \in T(\mu), f(z)x \geq 0)
$$

On the other hand, we define

$$
ZERO_j(x) = \left( \bigwedge_{i=1}^{\nu(\phi_i)-1} c(\phi_i, i)x = 0 \right) \land \left( \bigwedge_{\lambda \in S_j} c(\lambda, 0)^T x = 0 \right)
$$

The fact that $ZERO_j(x) \iff \forall n \geq d, b^T A^n x = 0$ follows immediately from the uniqueness part of [19, Proposition 2.11].

Note that, by Masser’s theorem, we can express the condition $z \in T(\mu)$ in the first-order theory of reals, and that, due to the Tarski-Seidenberg theorem [34, we can perform quantifier elimination in order to come up with equivalent quantifier-free formulas.

**Case II: A conjugate-pair of complex eigenvalues has index at least one, all other eigenvalues have index one**

Suppose $\phi \in S_j \setminus \mathbb{R}$ has index greater at least one and all other eigenvalues in $S_j$ have index one. If, for some $i \in \{1, \ldots, \nu(\phi)-1\}$, it holds that $c(\phi, i)x \neq 0$, then the dominating term of $b^T A^n x$ will be $\Theta(n^M (\phi^n + \phi^n)) = \Theta(n^M (\cos(\psi + n\theta)))$ for some $\psi, \theta$, where $\theta$ is the argument of $\phi$ and $M = \max \{ i : c(\phi, i)x \neq 0 \}$. Therefore, the sign of $b^T A^n x$ will keep oscillating. Thus, we take

$$
ENT_j(x) = \left( \bigwedge_{i=1}^{\nu(\phi_i)-1} c(\phi, i)^T x = 0 \right) \land (\forall z \in T(\mu), f(z)x \geq 0)
$$

where $\mu$ and $f$ are defined as in case I, and

$$
ZERO_j(x) = \left( \bigwedge_{i=1}^{\nu(\phi_i)-1} c(\phi, i)^T x = 0 \right) \land \left( \bigwedge_{\lambda \in S} c(\lambda, 0)^T x = 0 \right)
$$

Note that these cases cover not only the setting where $A$ is diagonalisable or where $1$ is the only defective eigenvalue, but also all possible settings when $d \leq 5$, and so this ends the proof of Proposition 1. The analysis above characterises $ENT \cap V_j$ for each $j$, but our ultimate goal is to construct a witness set $W$. In order to do so, we now look at $x \in \mathbb{A}^d$ (the algebraicity is required for reasons that will become clear later on, namely when using the S-units theorem) instead of $x \in V_j$. In fact, by a similar scaling argument to the one we did earlier in this section, we can assume without loss of generality that $x$ is a vector of algebraic integers.

Since $\mathbb{R}^d = V_1 \oplus \cdots \oplus V_m$, we can write $x = x_1 + \cdots + x_m$, where each $x_i$ is in $V_i$. Thus, we here on use $x_i$ to denote the projection of $x$ into $V_i$.

It is the case that $S_j$ is dominant for $x$ exactly when the following holds:

$$
DOM_j(x) = \left( \bigwedge_{i<j} ZERO_i(x_i) \right) \land \neg ZERO_j(x_j)
$$

We shall now focus on proving the following result:
Proposition 2. If $S_j$ is dominant for $x$, then $x \in \text{ENT}$ if and only if $x_j \in \text{ENT}$.

If $S_j$ is dominant for $x$, then for $n \geq d$ it holds that
\[ b^T A^n x = b^T A^n x_1 + \cdots + b^T A^n x_m = b^T A^n x_j + \cdots + b^T A^n x_m = b^T A^n (x_j + \cdots + x_m) \]

Take $\varepsilon \in (0, 1)$ to be such that $i > j \Rightarrow \rho_i < \rho_j^{1-\varepsilon}$. Thus
\[ b^T A^n x \geq 0 \iff b^T A^n x_j + o(\rho_j^{(1-\varepsilon)}) \geq 0 \]

In category I, if the fastest-growing term of $b^T A^n x$ is $\Theta(n^M \rho_j^n)$ for some $M \geq 1$, then $b^T A^n x_j = \omega(\rho_j^{n(1-\varepsilon)})$, and so for sufficiently large $n$, $b^T A^n x \geq 0 \implies b^T A^n x_j \geq 0$.

In category II, if the fastest-growing term of $b^T A^n x$ is $\Theta(n^M \phi^n)$ for some $M \geq 1$ and $\phi \in S_j \setminus \mathbb{R}$, then
\[ \lim_{n \to \infty} \rho_j^{-n(1-\varepsilon)} b^T A^n x_j = \infty \quad \text{and} \quad \liminf_{n \to \infty} \rho_j^{-n(1-\varepsilon)} b^T A^n x_j = -\infty \]

and so neither $b^T A^n x \geq 0$ nor $b^T A^n x_j \geq 0$ can eventually hold.

Otherwise, we will be in a setting where all terms in $b^T A^n x_j$ are $\Theta(\lambda^n)$, with $\lambda \in S_j$. In this case, $b^T A^n x_j = \rho_j^i f_j(\mu_j^i) x_j$. We will use the S-units theorem, which will be stated below, in order to lower bound $b^T A^n x_j$ as $\Omega(\rho_j^{n(1-\varepsilon)})$. Before, however, we need to introduce another result.

The following well-known theorem characterises the set of zeros of linear recurrence sequences. In particular, it gives us a sufficient condition for guaranteeing that the set of zeros of a non-identically zero linear recurrence sequence is finite.

Theorem 5 (Skolem-Mahler-Lech). The set \( \{ n \in \mathbb{N} : b^T A^n x \} \) is always a union of a finite set and finitely many arithmetic progressions. Moreover, if $A$ is non-degenerate, this set is actually finite.

Therefore, it follows from the Skolem-Mahler-Lech Theorem that any sub-sum of $\rho_j^n f_j(\mu_j^n) x$ can only be zero either for finitely many $n$ or for all $n$, since no ratio of the $\mu_i, \mu_j$ is a root of unity. If some sub-sum is identically zero, we can clearly just ignore it.

Let $S$ be a finite set of prime ideals of the ring of integers $\mathcal{O}$ of a number field $K$. We say that $\alpha \in \mathcal{O}$ is an S-unit if all the ideals appearing in the prime factorisation of $(\alpha)$, that is, the ideal generated by $\alpha$, are in $S$. The next theorem, by Evertse, van der Poorten, and Schlickewei, gives us a very strong lower bound on the magnitude of sums of S-units. Its key ingredient is Schlickewei’s $p$-adic generalisation [32] of Schmidt’s Subspace theorem, and it was established in [17, 36] to analyse the growth of linear recurrence sequences.

Theorem 6 (S-units). Let $K$ be a number field, $m$ be a positive integer, and $S$ be a finite set of prime ideals of $\mathcal{O}$. Then for every $\varepsilon > 0$ there exists a constant $C$, depending only on $m$, $K$, $S$, and $\varepsilon$, with the following property. For every set of S-units $x_1, \ldots, x_m \in \mathcal{O}$ such that $\sum_{i \in I} x_i \neq 0$ for all non-empty $I \subseteq \{1, \ldots, m\}$, it holds that
\[ |x_1 + \cdots + x_m| \geq CY^{-\varepsilon} \]

where $Y = \max\{|x_i| : 1 \leq i \leq m\}$ and $Z = \max\{\sigma_j(x_i) : 1 \leq i \leq m, 1 \leq j \leq d\}$ and $\sigma_j$ represent the different $\mathbb{Q}$-invariant monomorphisms from $K$ to $\mathbb{C}$.

Thus, we can apply the S-units theorem to get a lower bound on $\rho_j f(\mu_j^n) x$ that holds for all but finitely many $n$ (corresponding to the $n$ for which some non-identically zero sub-sum is zero): let $K = \mathbb{Q}(\rho_j, \mu_1, \ldots, \mu_s, x_1, \ldots, x_d)$, let $\varepsilon$ be as defined above, and let $S$ be the set of prime ideals that divide the algebraic integers $\rho_j, \lambda_1, \lambda_1, \ldots, \lambda_s, x_1, \ldots, x_d$ and the coordinates of $c(\lambda, i), c(\lambda, i)$ appearing in $f$. Then $\rho_j^n f(\mu_j^n) x$ is a sum of S-units.

Hence, in the notation of the statement of the theorem, we have $Y = \Theta(\rho^n)$ and $Z = \Theta(\rho^n)$, since the monomorphisms $\sigma_i$ must map eigenvalues of $A$ into eigenvalues of $A$. Therefore, it holds that
\[ \rho_j^n f(\mu_j^n) x = \Omega(\rho_j^{n(1-\varepsilon)}) \]

and so $b^T A^n x \geq 0 \iff b^T A^n x_j \geq 0$, which finishes the proof of our claim.
It may happen that no $S_j$ is dominant for $x$, in which case $b^T A^n x$ is eventually zero, and in particular $x \in \text{ENT}$.

We can then define

$$W = \left\{ x \in \mathbb{R}^d : \left\lceil m \left( \sum_{j=1}^m \left( \text{DOM}_j(x) \land \text{ENT}_j(P_{V_j}(x)) \right) \right) \right\rceil \lor \left\lceil m \left( \bigwedge_{j=1}^m \text{ZERO}_j(x) \right) \right\rceil \right\}$$

Since, as mentioned above, the \text{ENT} is convex, the following result should not come as a surprise:

**Proposition 3.** The witness set $W$ is convex.

In fact, suppose $y, z \in W$, and let $x = \lambda y + (1 - \lambda)z$, where $0 < \lambda < 1$. Moreover, suppose that $S_i$ is dominant for $y$ and that $S_j$ is dominant for $z$. In that case, for all $k < \min\{i, j\}$, it holds that $x_k \in \text{ZERO}_k$, since $y_k \in \text{ZERO}_k$, $z_k \in \text{ZERO}_k$, and $\text{ZERO}_k$ is closed under addition. Adding to that, if $k = \min\{i, j\}$, then $x_k \in \text{ENT}_k$, since $\{y_k, z_k\} \cap \text{ENT}_k \neq \emptyset$ and $\text{ENT}_k$ is closed under addition by both $\text{ENT}_k$ and $\text{ZERO}_k$. Finally, note that $\text{ENT}_k \cap \text{DOM}_j$ is closed under addition.

## 5 Complexity Analysis

The purpose of this section is to justify our claim that our procedure requires only exponential space.

The aforementioned procedure by Khachiyan and Porkolab to decide whether a convex semi-algebraic set has an integer point runs in space $SD^{O(d^4)}$, where $S$ denotes the size of the representation of the formula defining this set, $D$ denotes the maximum degree of the polynomials occurring in that formula, and $d$ denotes the dimension of the ambient space. Since $d$ remains fixed throughout the procedure (apart from an increase by 1 in one of the preliminary reductions), it remains to show that $S$ and $D$ are at most exponential on the size of the input.

Suppose $D_0, H_0$ denote the maximum degree and height of all the eigenvalues of $A$, respectively. Their representation is clearly polynomial on the size of the input, since $D_0 \leq d$ and $\log H_0 \leq \log(d \max_{i,j} |A_{ij}|) \leq d \log(d \max_{i,j} |A_{ij}|)$.

In the non-degenerate case, before performing quantifier elimination, the maximum degree is bounded by $(D_0 \log H_0)^{O(d^3)}$, and the number of polynomials in the formula is bounded by $O(d)$, by Masser’s theorem.

After applying quantifier elimination, the degree is bounded by $(D_0 \log H_0)^{O(d^3)}$ and the space is bounded by $d^{O(d^7)}(D_0 \log H_0)^{O(d^4)}$.

Finally, as we have seen, our reduction to the non-degenerate case makes our formula grow by a factor of $L = 2^{d \log d}$, so $D \leq (D_0 \log H_0)^{O(d^3)}$ and $S \leq d^{O(d^7)}(D_0 \log H_0)^{O(d^4)}$.

Therefore, our procedure takes $\text{SPACE}((d \log(d \max_{i,j} |A_{ij}|))^{O(d^7)})$, since

$$SD^{O(d^4)} \leq d^{O(d^7)}(D_0 \log H_0)^{O(d^7)} \leq (d \log(d \max_{i,j} |A_{ij}|))^{O(d^7)}$$

Therefore, for bounded dimension, the complexity drops from $\text{EXPSPACE}$ to $\text{PSPACE}$.

## 6 Concluding Remarks

We have shown decidability of termination of simple linear loops over the integers under the assumption that the update matrix is diagonalisable, partially answering an open problem of [35, 3]. As we have explained before, the termination problem for fixed initial values for the same class of linear loops seems to be much more difficult. In this respect it is interesting to note that there are other settings in which universal termination is an easier problem than pointwise termination. For example, universal termination of Petri nets (also known as structural boundedness) is $\text{PTIME}$-decidable, but the pointwise termination problem is $\text{EXPSPACE}$-hard.

A natural subject for further work is extending our techniques to non-diagonalisable matrices, or showing that, as is the case for pointwise termination [27], there are unavoidable number-theoretic obstacles to proving decidable. We would also like to further study the computational complexity of the termination problem.
While there is a large gap between the coNP lower complexity bound mentioned in the Introduction and the exponential space upper bound of our procedure, this may be connected with the fact that our procedure computes a representation of the set of all integer eventually non-terminating points. Finally we would like to examine more carefully the question of whether the respective sets of terminating and non-terminating points are semi-algebraic. Note that an effective semi-algebraic characterisation of the set of terminating points would allow us to solve the termination problem over fixed initial values.

Acknowledgements

The authors would like to thank Elias Koutsoupias and Ventsislav Chonev for their patience and useful feedback.

References

[1] I. Adler and P.A. Beling. Polynomial algorithms for linear programming over the algebraic numbers. Algorithmica, 12(6):436–457, 1994.
[2] A. Baker and G. Wüstholz. Logarithmic forms and group varieties. Jour. Reine Angew. Math., 442, 1993.
[3] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. J. ACM, 43(6):1002–1045, 1996.
[4] J. P. Bell and S. Gerhold. On the positivity set of a linear recurrence. Israel Jour. Math., 57, 2007.
[5] A. M. Ben-Amram, S. Genaim, and A. N. Masud. On the termination of integer loops. ACM Trans. Program. Lang. Syst., 34(4), 2012.
[6] A.M. Ben-Amram and Samir Genaim. On the linear ranking problem for integer linear-constraint loops. In POPL, pages 51–62, 2013.
[7] Aaron R. Bradley, Zohar Manna, and Henny B. Sipma. Termination analysis of integer linear loops. In CONCUR, volume 3653 of Lecture Notes in Computer Science, pages 488–502. Springer, 2005.
[8] M. Braverman. Termination of integer linear programs. In Proc. Intern. Conf. on Computer Aided Verification (CAV), volume 4144 of LNCS. Springer, 2006.
[9] J.-Y. Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. Int. J. Found. Comput. Sci., 5(3/4):293–302, 1994.
[10] J. Canny. Some algebraic and geometric computations in PSPACE. In Proceedings of STOC’88, pages 460–467. ACM, 1988.
[11] Hong Yi Chen, Shaked Flur, and Supratik Mukhopadhyay. Termination proofs for linear simple loops. In SAS, volume 7460 of Lecture Notes in Computer Science, pages 422–438. Springer, 2012.
[12] V. Chonev, J. Ouaknine, and J. Worrell. The polyhedron-hitting problem. Submitted, 2014.
[13] H. Cohen. A Course in Computational Algebraic Number Theory. Springer-Verlag, 1993.
[14] Michael Colón and Henny Sipma. Synthesis of linear ranking functions. In TACAS, volume 2031 of Lecture Notes in Computer Science, pages 67–81. Springer, 2001.
[15] B. Cook, A. Podelski, and A. Rybalchenko. Termination proofs for systems code. In PLDI, pages 415–426. ACM, 2006.
[16] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. Recurrence Sequences. American Mathematical Society, 2003.
[17] J.-H. Evertse. On sums of $S$-units and linear recurrences. *Compositio Mathematica*, 53(2):225–244, 1984.

[18] V. Halava, T. Harju, and M. Hirvensalo. Positivity of second order linear recurrent sequences. *Discrete Applied Mathematics*, 154(3), 2006.

[19] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem’s problem – on the border between decidability and undecidability. Technical Report 683, Turku Centre for Computer Science, 2005.

[20] D. Tall I. Stewart. *Algebraic Number Theory and Fermat’s Last Theorem*. A K Peters, 2002.

[21] L. Khachiyan and L. Porkolab. Computing integral points in convex semi-algebraic sets. In *FOCS*, pages 162–171, 1997.

[22] C. Lech. A note on recurring series. *Ark. Mat.*, 2, 1953.

[23] A.K. Lenstra, H.W. Lenstra Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[24] L. Liu. Positivity of three-term recurrence sequences. *Elec. J. Comb.*, 17(1), 2010.

[25] K. Mahler. Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38, 1935.

[26] D. W. Masser. Linear relations on algebraic groups. In *New Advances in Transcendence Theory*. Camb. Univ. Press, 1988.

[27] J. Ouaknine and J. Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of SODA ’14*. ACM-SIAM, 2014.

[28] V. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12), 1996.

[29] A. Podelski and A. Rybalchenko. Transition invariants. In *LICS*, pages 32–41, 2004.

[30] G. Rozenberg and A. Salomaa. *Cornerstones of Undecidability*. Prentice Hall, 1994.

[31] A. Salomaa. Growth functions of Lindenmayer systems: Some new approaches. In A. Lindenmayer and G. Rozenberg, editors, *Automata, Languages, Development*. North-Holland, 1976.

[32] H.P. Schlickewei. The $p$-adic Thue-Siegel-Roth-Schmidt Theorem. *Arch. Math.*, 29:267–270, 1977.

[33] T. Skolem. Ein Verfahren zur Behandlung gewisser exponentieller Gleichungen. In *Comptes rendus du congrès des mathématiciens scandinaves*, 1934.

[34] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.

[35] A. Tiwari. Termination of linear programs. In *Proc. Intern. Conf. on Comp. Aided Verif. (CAV)*, volume 3114 of *LNCS*. Springer, 2004.

[36] A.J. van der Poorten and H.P. Schlickewei. The growth conditions for recurrence sequences. *Macquarie Math. Reports*, (82-0041), 1982.
7 Appendix

7.1 Algebraic Numbers

A complex number \( \alpha \) is said to be algebraic if it is the root of some polynomial with integer coefficients. Among those polynomials, there exists a unique one of minimal degree whose coefficients have no common factor, and it is said to be the defining polynomial of \( \alpha \), denoted by \( p_{\alpha} \), and it is always an irreducible polynomial. Moreover, if \( p_{\alpha} \) is monic, \( \alpha \) is said to be an algebraic integer. The degree of an algebraic number is defined as the degree of \( p_{\alpha} \), and its height as the maximum absolute value of the coefficients of \( p_{\alpha} \) (also said to be the height of that polynomial). The roots of \( p_{\alpha} \) are said to be the Galois conjugates of \( \alpha \). We denote the set of algebraic numbers by \( \mathbb{A} \), and the set of algebraic integers by \( \mathcal{O}_{\mathbb{A}} \). For all \( \alpha \in \mathbb{A} \), there exists some \( n \in \mathbb{N} \) such that \( n\alpha \in \mathcal{O}_{\mathbb{A}} \). It is well known that \( \mathbb{A} \) is a field and that \( \mathcal{O}_{\mathbb{A}} \) is a ring.

A number field of dimension \( d \) is a field extension \( K \) of \( \mathbb{Q} \) whose degree as a vector-space over \( \mathbb{Q} \) is \( d \). In particular, \( K \subseteq \mathbb{A} \) must hold. Recall that, in that case, there are exactly \( d \) monomorphisms \( \sigma_i : K \to \mathbb{C} \) whose restriction over \( \mathbb{Q} \) is the identity (and therefore these must map elements of \( K \) to their Galois conjugates).

The ring of integers \( \mathcal{O} \) of a number field \( K \) is the set of elements of \( K \) that are algebraic integers, that is, \( \mathcal{O} = K \cap \mathcal{O}_{\mathbb{A}} \). An ideal of \( \mathcal{O} \) is an additive subgroup of \( \mathcal{O} \) that is closed under multiplication by any element of \( \mathcal{O} \). An ideal \( \mathfrak{P} \) is said to be prime if \( ab \in \mathfrak{P} \) implies \( a \in \mathfrak{P} \) or \( b \in \mathfrak{P} \). The following theorem is central in Algebraic Number Theory:

**Theorem 7.** In any ring of integers, ideals can be uniquely factored as products of prime ideals up to permutation.

The following lemma allows us to represent any algebraic number by keeping its defining polynomial, an estimate for the root we want to store, and an upper bound on the error. We call this its standard representation.

**Lemma 2** (Mignotte). Let \( f \in \mathbb{Z}[x] \). Then

\[
f(\alpha_1) = 0 = f(\alpha_2) \Rightarrow |\alpha_1 - \alpha_2| > \frac{\sqrt{6}}{d(d+1)/2H^{d-1}}
\]

where \( d \) and \( H \) are respectively the degree and height of \( f \).

It is well known that arithmetic operations and equality testing on these numbers can be done in polynomial time on the size of the canonical representations of the relevant numbers, since one can:

- compute polynomially many bits of the roots of any polynomial \( p \in \mathbb{Q}[x] \) in polynomial time, due to the work of Pan in [28];
- find the minimal polynomial of an algebraic number by factoring the polynomial in its description in polynomial time using the LLL algorithm [23];
- use the sub-resultant algorithm (see Algorithm 3.3.7 in [13]) and the two forementioned procedures to compute canonical representations of sums, differences, multiplications, and divisions of canonically represented algebraic numbers.

Moreover, we will need to decide whether a given canonically represented algebraic number \( \alpha \) is a root of unity, that is, whether \( \alpha^r = 1 \) for some \( r \). If that is the case, then its defining polynomial will be the \( r \)-th cyclotomic polynomial, which has degree \( \phi(r) \), if \( r \) is taken to be minimal, that is, if \( \alpha \) is a primitive \( r \)-th root of unity. The following (crude) lower bound on \( \phi(r) \) allows us to decide this in polynomial time.

**Lemma 3.** Let \( \phi \) be Euler’s totient function. Then \( \phi(r) \geq \sqrt{(r/2)} \). Therefore, if \( \alpha \) has degree \( n \) and is a \( r \)-th root of unity, then \( r \leq 2n^2 \).

In fact, since \( p_{\alpha} \) is by definition an irreducible polynomial, it suffices to test whether \( p_{\alpha}(e^{2\pi i/k}) = 0 \) for \( k \in \{1, \ldots, 2n^2\} \). Alternatively, one could just check whether the greatest common divisor of \( p_{\alpha} \) and \( x^k - 1 \) is equal to \( p_{\alpha} \) for each \( k \). If equality holds for some \( k \), then \( \alpha \) is a \( k \)-th root of unity.
7.2 First-Order Theory of Reals

Let \( x = (x_1, \ldots, x_m) \) be a list of \( m \) real-valued variables, and let \( \sigma(x) \) be a Boolean combination of atomic predicates of the form \( g(x) \sim 0 \), where each \( g(x) \) is a polynomial with integer coefficients in the variables \( x \), and \( \sim \) is either \( > \) or \( = \). Tarski has famously shown that we can decide the truth over the field \( \mathbb{R} \) of sentences of the form \( \phi = Q_1 x_1 \cdots Q_m x_m \sigma(x) \), where \( Q_i \) is either \( \exists \) or \( \forall \). He did so by showing that this theory admits quantifier elimination (Tarski-Seidenberg theorem [34]).

Definition. A set \( X \subseteq \mathbb{R}^d \) is said to be semi-algebraic if it is a finite Boolean combination of sets of the form \( f(x) > 0 \) or \( g(x) = 0 \), where \( f \) and \( g \) are polynomials with integer coefficients.

Therefore, all sets that are definable in the first-order theory of reals without quantification are by definition semi-algebraic, and it follows from Tarski’s theorem that this is still the case if we allow quantification. We also remark that our standard representation of algebraic numbers allows us to write them explicitly in first-order theory of reals, that is, given \( \alpha \in \mathbb{A} \), there exists a sentence \( \sigma(x) \) such that \( \sigma(x) \) is true if and only if \( x = \alpha \). Thus, we allow their use when defining semi-algebraic sets, for simplicity.

It follows from the undecidability of Hilbert’s Tenth Problem that, in general, we cannot decide whether a given semi-algebraic set has an integer point.

We shall make use of the following result by Basu, Pollack, and Roy [3], which tells us how expensive it is, in terms of space usage, to perform quantifier elimination on a formula in the first-order theory of reals:

Theorem 8. Given a set \( Q = \{q_1, \ldots, q_s\} \) of \( s \) polynomials each of degree at most \( D \), in \( h + d \) variables, and a first-order formula \( \Phi(x) = Q y_1 \cdots Q y_h F(q_1(x, y), \ldots, q_s(x, y)) \), where \( Q \in \{\exists, \forall\} \), \( F \) is a quantifier-free Boolean combination with atomic elements of the form \( q_i(x, y) \sim 0 \), then there exists a quantifier-free formula \( \Psi(x) = \bigwedge_{i=1}^J \bigvee_{j=1}^{I_i} q_{i,j}(x) \sim 0 \), where \( I \leq (sD)^{O(hd)} \), \( J \leq (sD)^{O(d)} \), the degrees of the polynomials \( q_{i,j} \) are bounded by \( D^d \), and the bit-sizes of the heights of the polynomials in the quantifier-free formula are only polynomially larger than those of \( q_1, \ldots, q_s \).

We also make use of the following lemmas:

Lemma 4. If \( X \subseteq \mathbb{R}^d \) is semi-algebraic and non-empty, \( X \cap \mathbb{A}^d \neq \emptyset \).

Proof. We prove this result by strong induction on \( d \). Since \( X \) is semi-algebraic, there exists a quantifier-free sentence in the first-order theory of reals \( \sigma \) such that \( X = \{x \in \mathbb{R}^d \mid \sigma(x)\} \). Suppose that \( d > 1 \). Letting \( X_1 = \{x_1 \in \mathbb{R} \mid \exists x_2, \ldots, x_{d-1} \in \mathbb{R}^{d-1}, \sigma(x_1, \ldots, x_d)\} \) and since \( X_1 \neq \emptyset \) is semi-algebraic, by the induction hypothesis, there must be \( x_1^* \in \mathbb{A} \cap X_1 \). Moreover, we can define \( X_2 = \{(x_2, \ldots, x_d) \in \mathbb{R}^{d-1} \mid \sigma(x_1^*, x_2, \ldots, x_d)\} \), which is non-empty and semi-algebraic, and again by induction hypothesis there exists some \( (x_2^*, \ldots, x_d^*) \in \mathbb{A}^{d-1} \cap X_2 \).

It remains to prove this statement for \( d = 1 \). When \( d = 1 \), \( X \) must be a finite union of intervals and points, since semi-algebraic sets form an o-minimal structure on \( \mathbb{R} \) [34]. Clearly \( \mathbb{A} \) is dense in any interval, and each of these isolated points \( x \) corresponds to some constraint \( g(x) = 0 \), which implies that \( x \) must be algebraic, since \( g \) has integer coefficients.

Lemma 5. If \( X \subseteq \mathbb{R}^d \) is semi-algebraic, then \( X \cap \mathbb{A}^d \) is dense in \( X \).

Proof. Pick \( x \in X \) and \( \varepsilon > 0 \) arbitrarily. Let \( y \in \mathbb{Q}^d \) be such that \( ||x - y|| < \varepsilon/2 \). Since \( B(y, \varepsilon/2) \) is semi-algebraic, so must be \( X \cap B(y, \varepsilon/2) \), and so this set must contain an algebraic point, since it is nonempty (\( x \) is in it), and that point must therefore be at distance at most \( \varepsilon \) of \( x \), by the triangular inequality. By letting \( \varepsilon \to 0 \), we get a sequence of algebraic points which converges to \( x \).

Lemma 6. If \( X \subseteq \mathbb{R}^d \) is semi-algebraic, so is \( \overline{X} \).

Proof. Let \( \sigma \) be a sentence in the first-order theory of reals such that \( X = \{x \in \mathbb{R}^d \mid \sigma(x)\} \). Whence

\[
\overline{X} = \{x \in \mathbb{R}^d \mid \forall \varepsilon > 0, \exists y \in \mathbb{R}^d, \sigma(y) \land y \in B(x, \varepsilon)\}
\]