Ultimate Positivity is Decidable for Simple Linear Recurrence Sequences*

Joël Ouaknine and James Worrell

Department of Computer Science, University of Oxford, UK

Abstract. We consider the decidability and complexity of the Ultimate Positivity Problem, which asks whether all but finitely many terms of a given rational linear recurrence sequence (LRS) are positive. Using lower bounds in Diophantine approximation concerning sums of S-units, we show that for simple LRS (those whose characteristic polynomial has no repeated roots) the Ultimate Positivity Problem is decidable in polynomial space. If we restrict to simple LRS of a fixed order then we obtain a polynomial-time decision procedure. As a complexity lower bound we show that Ultimate Positivity for simple LRS is at least as hard as the decision problem for the universal theory of the reals: a problem that is known to lie between **coNP** and **PSPACE**.

1 Introduction

A ***linear recurrence sequence (LRS)*** is an infinite sequence $\boldsymbol{u} = \langle u_0, u_1, \ldots \rangle$ of rational numbers satisfying a recurrence relation

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n \tag{1}$$

for all $n \geq 0$, where $a_1, a_2, \ldots, a_k$ are fixed rational numbers with $a_k \neq 0$. Such a sequence is determined by its initial values $u_0, \ldots, u_{k-1}$ and the recurrence relation. We say that the recurrence has ***characteristic polynomial***

$$f(x) = x^k - a_1 x^{k-1} - \ldots - a_{k-1} x - a_k \, .$$

The least k such that $\boldsymbol{u}$ satisfies a recurrence of the form (1) is called the ***order*** of $\boldsymbol{u}$. If the characteristic polynomial of this (unique) recurrence has no repeated roots then we say that $\boldsymbol{u}$ is ***simple***.

multiplicity = 1 for every root

Given an LRS $\boldsymbol{u}$ there are polynomials $p_1, \ldots, p_k \in \mathbb{C}[x]$ such that

$$u_n = p_1(n)\gamma_1^n + \ldots + p_k(n)\gamma_k^n \, ,$$

where $\gamma_1, \ldots, \gamma_k$ are the roots of the characteristic polynomial. Moreover $\boldsymbol{u}$ is simple if and only if it admits such a representation in which each polynomial p_i is a constant. Simple LRS are a natural and widely studied subclass of LRS whose analysis nevertheless remains extremely challenging [1, 10, 12, 24].

* The full version of this paper is available as [23].

Motivated by questions in language theory and formal power series, Rozenberg, Salomaa, and Soittola [27, 29] highlight the following four decision problems concerning LRS. Given an LRS $\langle u_n \rangle_{n=0}^{\infty}$ (represented by a linear recurrence and sequence of initial values):

1. Does $u_n = 0$ for some n?
2. Does $u_n = 0$ for infinitely many n?
3. Is $u_n \geq 0$ for all n?
4. Is $u_n \geq 0$ for all but finitely many n?

Linear recurrence sequences are ubiquitous in mathematics and computer science, and the above four problems (and assorted variants) arise in a variety of settings; see [25] for references. For example, an LRS modelling population size is biologically meaningful only if it never becomes negative.

Problem 1 is known as ***Skolem's Problem***, after the Skolem-Mahler-Lech Theorem [18, 19, 28], which characterises the set $\{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS $\boldsymbol{u}$ as an ultimately periodic set. The proof of the Skolem-Mahler-Lech Theorem is non-effective, and the decidability of Skolem's Problem is open. Blondel and Tsitsiklis [6] remark that "the present consensus among number theorists is that an algorithm [for Skolem's Problem] should exist". However, so far decidability is known only for LRS of order at most 4: a result due independently to Vereschagin [32] and Mignotte, Shorey, and Tijdeman [21]. At order 5 decidability is not known, even for simple LRS [22]. Decidability of Skolem's Problem is also listed as an open problem and discussed at length by Tao [30, Section 3.9]. The problem can furthermore be seen as a generalisation of the Orbit Problem, studied by Kannan and Lipton [16, Section 5].

In contrast to the situation with Skolem's Problem, Problem 2—hitting zero infinitely often—was shown to be decidable for arbitrary LRS by Berstel and Mignotte [4].

Problems 3 and 4 are respectively known as the ***Positivity*** and ***Ultimate Positivity*** Problems. The problems are stated as open in [2, 14, 17], among others, while in [27] the authors assert that the problems are "generally conjectured [to be] decidable". Decidability of Positivity entails decidability of Skolem's Problem via a straightforward algebraic transformation of LRS (which however does not preserve the order) [14].

Hitherto, all decidability results for Positivity and Ultimate Positivity have been for low-order sequences. The paper [25] gives a detailed account of these results, obtained over a period of time stretching back some 30 years, and proves decidability of both problems for sequences of order at most 5. It is moreover shown in [25] that obtaining decidability for either Positivity or Ultimate Positivity at order 6 would necessarily entail major breakthroughs in Diophantine approximation.

The main result of this paper is that the Ultimate Positivity Problem for simple LRS of arbitrary order is decidable. The restriction to simple LRS allows us to circumvent the strong "mathematical hardness" result for sequences of order 6 alluded to above. However, our decision procedure is non-constructive: given an ultimately positive LRS $\langle u_n \rangle_{n=0}^{\infty}$, the procedure does not compute a threshold N such that $u_n \geq 0$ for all $n \geq N$. Indeed the ability to compute such a threshold N would immediately yield an algorithm for the Positivity Problem for simple LRS since the signs of $u_0, \ldots, u_{N-1}$ can be checked directly. In turn this would yield decidability of Skolem's Problem for simple LRS. But Skolem's Problem is open for simple LRS of order 5, while (as discussed below) Positivity for simple LRS is only known to be decidable up to order 9.

The non-constructive aspect of our results arises from our use of lower bounds in Diophantine approximation concerning sums of *S-units*. These bounds were proven in [11, 31] using Schlickewei's p-adic generalisation of Schmidt's Subspace Theorem (itself a far-reaching generalisation of the Thue-Siegel-Roth Theorem), and therein applied to study the asymptotic growth of LRS in absolute value. By contrast, in [24] we use Baker's Theorem on linear forms in logarithms to show decidability of Positivity for simple LRS of order at most 9. Unfortunately, while Baker's Theorem yields effective Diophantine-approximation lower bounds, it appears only to be applicable to low-order LRS. In particular, the analytic and geometric arguments that are used in [24] to bring Baker's Theorem to bear (and which give that work a substantially different flavour to the present paper) do not apply beyond order 9.

Relying on complexity bounds for the decision problem for first-order formulas over the field of real numbers, we show that our procedure for deciding Ultimate Positivity requires polynomial space in general and polynomial time for LRS of each fixed order. As a complexity lower bound, we give a polynomial-time reduction of the decision problem for the universal theory of the reals to both the Positivity and Ultimate Positivity Problems for simple LRS. The decision problem for the universal theory of the reals is easily seen to be **coNP**-hard and, from the work of Canny [8], is contained in **PSPACE**. Thus the complexity of the Ultimate Positivity problem for simple LRS lies between **coNP** and **PSPACE**. Hitherto the best lower bound known for either Positivity or Ultimate Positivity was **coNP**-hardness [3].

Full proofs of all results can be found in the long version of this paper [23].

2 Background

Number Theory. A complex number α is ***algebraic*** if it is a root of a univariate polynomial with integer coefficients. The ***defining polynomial*** of α, denoted p_α, is the unique integer polynomial of least degree, whose coefficients have no common factor, that has α as a root. The ***degree*** of α is the degree of p_α, and the ***height*** of α is the maximum absolute value of the coefficients of p_α. If p_α is monic then we say that α is an ***algebraic integer***.

For computational purposes an algebraic number α can be represented by a polynomial f that has α as a root, together with an approximation of α with rational real and imaginary parts of sufficient accuracy to distinguish α from the other roots of f [15]. We denote by $||\alpha||$ the length of this representation.[1] It

[1] In general we denote by $||X||$ the length of the binary representation of a given object X.

can be shown that $||\alpha||$ is polynomial in the degree and logarithm of the height of α. Given a univariate polynomial f, it is moreover known how to obtain representations of each of its roots in time polynomial in $||f||$.

A ***number field*** K is a finite-dimensional extension of $\mathbb{Q}$. The set of algebraic integers in K forms a ring, denoted $\mathcal{O}$. Given two ideals I, J in $\mathcal{O}$, the product IJ is the ideal generated by the elements ab, where $a \in I$ and $b \in J$. An ideal P of $\mathcal{O}$ is ***prime*** if $ab \in P$ implies $a \in P$ or $b \in P$. The fundamental theorem of ideal theory states that any non-zero ideal in $\mathcal{O}$ can be written as the product of prime ideals, and the representation is unique if the order of the prime ideals is ignored.

We will need the following classical result of Dirichlet [13].

Theorem 2.1 (Dirichlet). *Let P be the set of primes and $P_{a,b}$ the set of primes congruent to a mod b, where* $\gcd(a, b) = 1$*. Then*

$$\lim_{n\to\infty} \frac{|P_{a,b} \cap \{1, \ldots, n\}|}{|P \cap \{1, \ldots, n\}|} = \frac{1}{\varphi(b)} ,$$

where φ denotes Euler's totient function.

Linear Recurrence Sequences. Let $\boldsymbol{u} = \langle u_n \rangle_{n=0}^{\infty}$ be a sequence of rational numbers satisfying the recurrence relation $u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n$. We represent such an LRS as a $2k$-tuple $(a_1, \ldots, a_k, u_0, \ldots, u_{k-1})$ of rational numbers (encoded in binary). Given an arbitrary representation of $\boldsymbol{u}$, we can compute the coefficients of the unique minimal-order recurrence satisfied by $\boldsymbol{u}$ in polynomial time by straightforward linear algebra. Henceforth we will always assume that an LRS is presented in terms of its minimal-order recurrence. By the characteristic polynomial of an LRS we mean the characteristic polynomial of the minimal-order recurrence. The roots of this polynomial are called the ***characteristic roots***. The characteristic roots of maximum modulus are said to be ***dominant***.

It is well-known (see, e.g., [2, Thm. 2]) that if an LRS $\boldsymbol{u}$ has no real positive dominant characteristic root then there are infinitely many n such that $u_n < 0$ and infinitely many n such that $u_n > 0$. Clearly such an LRS cannot be ultimately positive.

Since the characteristic polynomial of $\boldsymbol{u}$ has real coefficients, its set of roots can be written in the form $\{\rho_1, \ldots, \rho_\ell, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_m, \overline{\gamma_m}\}$, where each $\rho_i \in \mathbb{R}$. If $\boldsymbol{u}$ is simple then there are non-zero real algebraic constants $b_1, \ldots, b_\ell$ and complex algebraic constants $c_1, \ldots, c_m$ such that, for all $n \geq 0$,

$$u_n = \sum_{i=1}^{\ell} b_i \rho_i^n + \sum_{j=1}^{m} \left(c_j \gamma_j^n + \overline{c_j \gamma_j}^n \right) . \tag{2}$$

Conversely, a sequence $\boldsymbol{u}$ that admits the representation (2) is a simple LRS over $\mathbb{R}$, with characteristic roots among $\rho_1, \ldots, \rho_\ell, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_m, \overline{\gamma_m}$. Arbitrary LRS admit a more general "exponential-polynomial" representation in which the coefficients b_i and c_j are replaced by polynomials in n.

An LRS is said to be ***non-degenerate*** if it does not have two distinct characteristic roots whose quotient is a root of unity. A non-degenerate LRS is either identically zero or only has finitely many zeros. The study of arbitrary LRS can effectively be reduced to that of non-degenerate LRS using the following result from [10].

Proposition 2.2. *Let $\langle u_n \rangle_{n=0}^{\infty}$ be an LRS of order k over $\mathbb{Q}$. There is a constant $M = 2^{O(k\sqrt{\log k})}$ such that each subsequence $\langle u_{Mn+l} \rangle_{n=0}^{\infty}$ is non-degenerate for $0 \leq l < M$.*

The constant M in Proposition 2.2 is the least common multiple of the orders of all roots of unity appearing as quotients of characteristic roots of $\boldsymbol{u}$. This number can be computed in time polynomial in $||\boldsymbol{u}||$ since determining whether an algebraic number α is a root of unity (and computing the order of the root) can be done in polynomial time in $||\alpha||$ [15]. From the representation (2) we see that if the original LRS is simple with characteristic roots $\lambda_1, \ldots, \lambda_k$, then each subsequence $\langle u_{Mn+l} \rangle_{n=0}^{\infty}$ is also simple, with characteristic roots among $\lambda_1^M, \ldots, \lambda_k^M$.

The following is a celebrated result on LRS [18, 19, 28].

Theorem 2.3 (Skolem-Mahler-Lech). *The set $\{n : u_n = 0\}$ of zeros of an LRS $\boldsymbol{u}$ comprises a finite set together with a finite number of arithmetic progressions. If $\boldsymbol{u}$ is non-degenerate and not identically zero, then its set of zeros is finite.*

Suppose that $\boldsymbol{u}$ and $\boldsymbol{v}$ are LRS of orders k and l respectively, then the pointwise sum $\langle u_n + v_n \rangle_{n=0}^{\infty}$ is an LRS of order at most $k + l$, and the pointwise product $\langle u_n v_n \rangle_{n=0}^{\infty}$ is an LRS of order at most kl. Given representations of $\boldsymbol{u}$ and $\boldsymbol{v}$ we can compute representations of the sum and product in polynomial time by straightforward linear algebra.

First-Order Theory of the Reals. Let $\boldsymbol{x} = x_1, \ldots, x_m$ be a list of m real-valued variables, and let $\sigma(\boldsymbol{x})$ be a Boolean combination of atomic predicates of the form $g(\boldsymbol{x}) \sim 0$, where each $g(\boldsymbol{x})$ is a polynomial with integer coefficients in the variables $\boldsymbol{x}$, and $\sim$ is either $>$ or $=$. We consider the problem of deciding the truth over the field $\mathbb{R}$ of sentences φ in the form

$$Q_1 x_1 \ldots Q_m x_m \, \sigma(\boldsymbol{x}) \,, \tag{3}$$

where each Q_i is one of the quantifiers $\exists$ or $\forall$. We write $||\varphi||$ for the length of the syntactic representation of φ.

The collection of true sentences of the form (3) is called the **first-order theory of the reals**. Tarski famously showed that this theory admits quantifier elimination and is therefore decidable. In this paper we rely on decision procedures for two fragments of this theory. We use the result of Canny [8] that if each Q_i is a universal quantifier, then the truth of φ can be decided in space polynomial in $||\varphi||$. We also use the result of Renegar [26] that for each fixed

$M \in \mathbb{N}$, if the number of variables in φ is at most M, then the truth of φ can be determined in time polynomial in $||\varphi||$.

Given a representation of an algebraic number α, as described in Section 2, both the real and imaginary parts of α are straightforwardly definable by quantifier-free formulas $\varphi(x)$ of size polynomial in $||\alpha||$.

3 Multiplicative Relations

Throughout this section let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_s)$ be a tuple of algebraic numbers, each of height at most H and degree at most d. Assume that each λ_i is represented in the manner described in Section 2.

We define the group of multiplicative relations holding among the λ_i to be the subgroup $L(\boldsymbol{\lambda})$ of $\mathbb{Z}^s$ defined by

$$L(\boldsymbol{\lambda}) = \{(v_1, \ldots, v_s) \in \mathbb{Z}^s : \lambda_1^{v_1} \ldots \lambda_s^{v_s} = 1\}.$$

Bounds on the complexity of computing a basis of $L(\boldsymbol{\lambda})$, considered as a free abelian group, can be obtained from the following result of Masser [20] which gives an upper bound on the magnitude of the entries of the vectors in such a basis.

Theorem 3.1 (Masser). *The free abelian group $L(\boldsymbol{\lambda})$ has a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l \in \mathbb{Z}^s$ for which*

$$\max_{1 \le i \le l,\, 1 \le j \le s} |\boldsymbol{v}_{i,j}| = (d \log H)^{O(s^2)}.$$

Corollary 3.2. *A basis of $L(\boldsymbol{\lambda})$ can be computed in space polynomial in $||\boldsymbol{\lambda}||$. If s and d are fixed, such a basis can be computed in time polynomial in $||\boldsymbol{\lambda}||$.*

Proof. Masser's bound entails that there is a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ whose total bit length is polynomial in s, $\log d$ and $\log \log H$, all of which are polynomial in $||\boldsymbol{\lambda}||$. Moreover the membership problem "$\lambda_1^{v_1} \ldots \lambda_s^{v_s} = 1$?" for a potential basis vector $\boldsymbol{v} \in \mathbb{Z}^s$ is decidable in space polynomial in $||\boldsymbol{\lambda}||$ by reduction to the decision problem for existential sentences over the reals.

A set of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ in $L(\boldsymbol{\lambda})$ is a basis if every vector $\boldsymbol{v} \in L(\boldsymbol{\lambda})$ whose entries satisfy the bound in Theorem 3.1 lies in the integer span of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$. For each such vector $\boldsymbol{v}$ this can be checked by solving a system of linear equations over the integers. Thus we can compute a basis of $L(\boldsymbol{\lambda})$ in space polynomial in $||\boldsymbol{\lambda}||$ by brute-force search.

If s and d are fixed then the same brute-force search can be done in time polynomial in $||\boldsymbol{\lambda}||$, noting that the number of possible bases is polynomial in $||\boldsymbol{\lambda}||$ and the membership problem "$\lambda_1^{v_1} \ldots \lambda_s^{v_s} = 1$?" is decidable in time polynomial in $||\boldsymbol{\lambda}||$ by reduction to the decision problem for existential sentences over the reals with a fixed number of variables. $\square$

The following is an easy consequence of Corollary 3.2.

Corollary 3.3. *Given $M \in \mathbb{N}$, a basis of $L(\lambda_1^M, \ldots, \lambda_s^M)$ can be computed in space polynomial in $||M||$ and $||\boldsymbol{\lambda}||$.*

Next we relate the group $L(\boldsymbol{\lambda})$ to the ***orbit*** $\{(\lambda_1^n, \ldots, \lambda_s^n) \mid n \in \mathbb{N}\}$ of $\boldsymbol{\lambda}$. Recall from [9] the following classical theorem of Kronecker on inhomogeneous Diophantine approximation.

Theorem 3.4 (Kronecker). *Let $\theta_1, \ldots, \theta_s$ and $\psi_1, \ldots, \psi_s$ be real numbers. Suppose moreover that for all integers $u_1, \ldots, u_s$, if $u_1\theta_1 + \ldots + u_s\theta_s \in \mathbb{Z}$ then also $u_1\psi_1 + \ldots + u_s\psi_s \in \mathbb{Z}$, i.e., all integer relations among the θ_i also hold among the ψ_i (modulo $\mathbb{Z}$). Then for each $\varepsilon > 0$, there exist integers $p_1, \ldots, p_s$ and a non-negative integer n such that $|n\theta_i - p_i - \psi_i| \le \varepsilon$.*

Write $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ and consider the s-dimensional torus $\mathbb{T}^s$ as a group under coordinatewise multiplication. The following can be seen as a multiplicative formulation of Kronecker's Theorem.

Proposition 3.5. *Let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_s) \in \mathbb{T}^s$ and consider the group $L(\boldsymbol{\lambda})$ of multiplicative relations among the λ_i. Define a subgroup $T(\boldsymbol{\lambda})$ of the torus $\mathbb{T}^s$ by*

$$T(\boldsymbol{\lambda}) = \{(\mu_1, \ldots, \mu_s) \in \mathbb{T}^s \mid \mu_1^{v_1} \ldots \mu_s^{v_s} = 1 \text{ for all } \boldsymbol{v} \in L(\boldsymbol{\lambda})\}\,.$$

Then the orbit $S = \{(\lambda_1^n, \ldots, \lambda_s^n) \mid n \in \mathbb{N}\}$ is a dense subset of $T(\boldsymbol{\lambda})$.

Proof. For $j = 1, \ldots, s$, let $\theta_j \in \mathbb{R}$ be such that $\lambda_j = e^{2\pi i\theta_j}$. Notice that multiplicative relations $\lambda_1^{v_1} \ldots \lambda_s^{v_s} = 1$ are in one-to-one correspondence with additive relations $\theta_1 v_1 + \ldots + \theta_s v_s \in \mathbb{Z}$. Let $(\mu_1, \ldots, \mu_s)$ be an arbitrary element of $T(\boldsymbol{\lambda})$, with $\mu_j = e^{2\pi i\psi_j}$ for some $\psi_j \in \mathbb{R}$. Then the hypotheses of Theorem 3.4 apply to $\theta_1, \ldots, \theta_s$ and $\psi_1, \ldots, \psi_s$. Thus given $\varepsilon > 0$, there exist $n \ge 0$ and $p_1, \ldots, p_s \in \mathbb{Z}$ such that $|n\theta_j - p_j - \psi_j| \le \varepsilon$ for $j = 1, \ldots, s$. Whence for $j = 1, \ldots, s$,

$$|\lambda_j^n - \mu_j| = |e^{2\pi i(n\theta_j - p_j)} - e^{2\pi i\psi_j}| \le |2\pi(n\theta_j - p_j - \psi_j)| \le 2\pi\varepsilon\,.$$

It follows that $(\mu_1, \ldots, \mu_s)$ lies in the closure of S. $\square$

4 Algorithm for Ultimate Positivity

Let K be a number field of degree d over $\mathbb{Q}$. Recall that there are d distinct field monomorphisms $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ (see, e.g., [13]). Given a finite set S of prime ideals in the ring of integers $\mathcal{O}$ of K, we say that $\alpha \in \mathcal{O}$ is an S-***unit*** if the principal ideal (α) is a product of prime ideals in S. The following lower bound on the magnitude of sums of S-units, whose key ingredient is Schlickewei's p-adic generalisation of Schmidt's Subspace Theorem, was established in [11, 31] to analyse the growth of LRS.

Theorem 4.1 (Evertse, van der Poorten, Schlickewei). *Let m be a positive integer and S a finite set of prime ideals in $\mathcal{O}$. Then for every $\varepsilon > 0$ there exists a constant C, depending only on m, K, S, and ε with the following property:*

for any 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

$$|x_1 + \ldots + x_m| \geq CXY^{-\varepsilon}, \tag{4}$$

where $X = \max\{|x_i| : 1 \leq i \leq m\}$, $Y = \max\{|\sigma_j(x_i)| : 1 \leq i \leq m,\, 1 \leq j \leq d\}$.

We first consider how to decide Ultimate Positivity in the case of a non-degenerate simple LRS $\boldsymbol{u}$. As explained in Section 2, we can assume without loss of generality that $\boldsymbol{u}$ has a positive real dominant root. Furthermore, by considering the LRS $\langle k^{n+1} u_n \rangle_{n=0}^{\infty}$ for a suitable integer $k \geq 1$, we may assume that the characteristic roots and coefficients in the closed-form solution (2) are all algebraic integers.

Suppose that $\boldsymbol{u}$ has dominant characteristic roots $\rho, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_s, \overline{\gamma_s}$, where ρ is real and positive. Then we can write $\boldsymbol{u}$ in the form

$$u_n = b\rho^n + c_1\gamma_1^n + \overline{c_1\gamma_1}^n + \ldots + c_s\gamma_s^n + \overline{c_s\gamma_s}^n + r(n), \tag{5}$$

where $r(n) = o(\rho^{n(1-\varepsilon)})$ for some $\varepsilon > 0$. Now let $\lambda_i = \gamma_i/\rho$ for $i = 1, \ldots, s$. Then we can write

$$u_n = \rho^n f(\lambda_1^n, \ldots, \lambda_s^n) + r(n), \tag{6}$$

where $f : \mathbb{T}^s \to \mathbb{R}$ is defined by $f(z_1, \ldots, z_s) = b + c_1 z_1 + \overline{c_1 z_1} + \ldots + c_s z_s + \overline{c_s z_s}$.

Proposition 4.2. *The LRS $\langle u_n \rangle_{n=0}^{\infty}$ is ultimately positive if and only if $f(\boldsymbol{z}) \geq 0$ for all $\boldsymbol{z} \in T(\boldsymbol{\lambda})$.*

Proof. Consider the expression (5). Let K be the number field generated over $\mathbb{Q}$ by the characteristic roots of $\boldsymbol{u}$ and let S be the set of prime ideal divisors of the dominant characteristic roots $\rho, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_s, \overline{\gamma_s}$ and the associated coefficients $b, c_1, \overline{c_1}, \ldots, c_s, \overline{c_s}$. (These coefficients lie in K by straightforward linear algebra.) Then the term

$$b\rho^n + c_1\gamma_1^n + \overline{c_1\gamma_1}^n + \ldots + c_s\gamma_s^n + \overline{c_s\gamma_s}^n \tag{7}$$

is a sum of S-units.

Applying Theorem 4.1 to the sum of S-units in (7), we have $X = C_1\rho^n$ for some constant $C_1 > 0$ and $Y = C_2\rho^n$ for some constant $C_2 > 0$ (since an embedding of K into $\mathbb{C}$ maps characteristic roots to characteristic roots). The theorem tells us that for each $\varepsilon > 0$ there is a constant $C > 0$ such that

$$|b\rho^n + c_1\gamma_1^n + \overline{c_1\gamma_1}^n + \ldots + c_s\gamma_s^n + \overline{c_s\gamma_s}^n| \geq C\rho^{n(1-\varepsilon)}$$

for all but finitely many values of n. (Since $\boldsymbol{u}$ is non-degenerate, it follows from the Skolem-Mahler-Lech Theorem that each non-empty sub-sum of the left-hand side vanishes for finitely many n.)

Now choose $\varepsilon > 0$ such that $r(n) = o(\rho^{n(1-\varepsilon)})$ in (5). Then for all sufficiently large n, $u_n \geq 0$ if and only if $b\rho^n + c_1\gamma_1^n + \overline{c_1\gamma_1}^n + \ldots + c_s\gamma_s^n + \overline{c_s\gamma_s}^n > 0$. Equivalently, looking at (6), for all sufficiently large n we have $u_n \geq 0$ if and only if $f(\lambda_1^n, \ldots, \lambda_s^n) \geq 0$. But the orbit $\{(\lambda_1^n, \ldots, \lambda_s^n) : n \in \mathbb{N}\}$ is a dense subset of $T(\boldsymbol{\lambda})$ by Proposition 3.5. Thus u_n is ultimately positive if and only if $f(\boldsymbol{z}) \geq 0$ for all $\boldsymbol{z} \in T(\boldsymbol{\lambda})$. ∎

We can now state and prove our main result.

Theorem 4.3. *The Ultimate Positivity Problem for simple LRS is decidable in polynomial space in general, and in polynomial time for LRS of fixed order.*

Proof. A decision procedure is given in the table below. Correctness follows from the fact that $\boldsymbol{u}$ is ultimately positive if and only if each of the non-degenerate subsequences $\boldsymbol{v}$ considered in Step 2 is ultimately positive. But ultimate positivity of these subsequences is determined in Step 2.4 using Proposition 4.2. It remains to account for the complexity of each step.

As noted in Section 2, Step 1 requires time polynomial in $||\boldsymbol{u}||$.

For LRS of fixed order, there is an absolute bound on M in Step 2, while for LRS of arbitrary order, M is exponentially bounded in $||\boldsymbol{u}||$ by Proposition 2.2. We show that for each subsequence $\boldsymbol{v}$, Steps 2.1–2.4 require polynomial time for fixed-order LRS and polynomial space in general.

Using iterated squaring, the coefficients b_i and c_j in the expression (8) for $\boldsymbol{v}$ are definable in terms of the characteristic roots of $\boldsymbol{u}$ and the corresponding coefficients in the closed-form expression for $\boldsymbol{u}$ by a polynomial-size first-order formula that uses only universal quantifiers. This accomplishes Step 2.1.

Combining Corollaries 3.2 and 3.3, Step 2.3 can be done in polynomial space for arbitrary LRS and polynomial time for LRS of fixed order.

Step 2.4 uses a decision procedure for universal sentences over the reals, having already noted that the coefficients b_i and c_j are first-order definable. By the results described in Section 2 this can be done in polynomial space for arbitrary LRS and polynomial time for LRS of fixed order. □

Decision procedure for ultimate positivity of a simple LRS $\boldsymbol{u}$

---

1. Compute the characteristic roots $\{\rho_1, \ldots, \rho_\ell, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_m, \overline{\gamma_m}\}$ of $\boldsymbol{u}$. Writing $\alpha \sim \beta$ if α/β is a root of unity, let $M = \mathrm{lcm}\{\mathrm{ord}(\alpha/\beta) : \alpha \sim \beta$ are characteristic roots$\}$. Moreover let $\{\rho_i : i \in I\} \cup \{\gamma_j, \overline{\gamma_j} : j \in J\}$ contain a unique representative from each equivalence class.
2. For $l = 0, \ldots, M-1$, check ultimate positivity of the non-degenerate subsequence $v_n = u_{Mn+l}$ as follows:

   2.1. Compute the coefficients b_i and c_j in the closed-form solution

$$v_n = \sum_{i \in I} b_i \rho_i^{Mn} + \sum_{j \in J} \left(c_j \gamma_j^{Mn} + \overline{c_j \gamma_j}^{Mn} \right) . \tag{8}$$

   2.2. If $\boldsymbol{v} \not\equiv 0$ and there is no dominant real characteristic root in (8) then $\boldsymbol{v}$ is not ultimately positive.

   2.3. Let $\rho_1, \gamma_1, \overline{\gamma_1}, \ldots, \gamma_s, \overline{\gamma_s}$ be dominant among the characteristic roots appearing in (8). Define $\lambda_1 = \gamma_1/\rho_1, \ldots, \lambda_s = \gamma_s/\rho_1$ and compute a basis of $L(\lambda_1^M, \ldots, \lambda_s^M)$.

   2.4. Define $f : \mathbb{T}^s \to \mathbb{R}$ by $f(z_1, \ldots, z_s) = b_1 + c_1 z_1 + \overline{c_1 z_1} + \ldots + c_s z_s + \overline{c_s z_s}$. Then $\boldsymbol{v}$ is ultimately positive if and only if $f(\boldsymbol{z}) \geq 0$ for all $\boldsymbol{z} \in T(\boldsymbol{\lambda}^M)$.

We note that a related proof strategy (passing from a finitely generated group to its closure and appealing to the theory of the reals) was used in [5] in the context of threshold problems for quantum automata.

5 Complexity Lower Bound

In this section we give a reduction of the decision problem for universal sentences over the field of real numbers to the Positivity and Ultimate Positivity Problems. The former problem is easily seen to be **coNP**-hard and, through the work of Canny [8], is known to be in **PSPACE**. Typically this **PSPACE** upper bound is stated for the complement problem: the decision problem for existential sentences over the field of reals.

It is known that the problem 4-FEAS of whether a degree-4 polynomial has a real root is polynomial-time equivalent to the decision problem for the existential theory of the reals [7]. Here we consider a related problem, 4-POS, which asks whether a degree-4 polynomial $f(x_1, \ldots, x_n)$ with rational coefficients satisfies $f(\boldsymbol{x}) \geq 0$ for all $\boldsymbol{x} \in [0,1]^n$. Using the above-mentioned result on 4-FEAS in tandem with bounds on magnitude of definable numbers in the existential theory of the reals we can prove:

Theorem 5.1. *There is a polynomial-time reduction of the decision problem for the universal theory of the reals to the problem 4-POS.*

We now reduce 4-POS to the Positivity and Ultimate Positivity Problems. The first step of the reduction is to compute a collection of s multiplicatively independent algebraic numbers of absolute value 1.

By a classical result of Lagrange, a prime number is congruent to 1 modulo 4 if and only if it can be written as the sum of two squares [13]. By Theorem 2.1, the class of such primes has asymptotic density $1/2$ in the set of all primes, and therefore, by the Prime Number Theorem, asymptotic density $1/(2\log n)$ in the set of natural numbers. It follows that one can compute the first s such primes $p_1, \ldots, p_s$ and their decomposition as sums of squares in time polynomial in s. Writing $p_j = a_j^2 + b_j^2$, where $a_j, b_j \in \mathbb{Z}$, define $\lambda_j = \frac{a_j + ib_j}{a_j - ib_j}$ for $j = 1, \ldots, s$. Then each λ_j is an algebraic number of degree 2 and absolute value 1.

Proposition 5.2. *$\lambda_1, \ldots, \lambda_s$ are multiplicatively independent.*

Proof. Recall that the ring of Guassian integers $\mathbb{Z}(i)$ is a unique factorisation domain and that $a + ib \in \mathbb{Z}(i)$ is prime iff $a^2 + b^2$ is a rational prime [13]. Now $\lambda_1^{n_1} \ldots \lambda_s^{n_s} = 1$ if and only if

$$(a_1 + ib_1)^{n_1} \ldots (a_s + ib_s)^{n_s} = (a_1 - ib_1)^{n_1} \ldots (a_s - ib_s)^{n_s}$$

But each factor $a_j + ib_j$ and $a_j - ib_j$ is prime by construction. Thus by unique factorisation we must have $n_1 = 0, \ldots, n_s = 0$. $\square$

Theorem 5.3. *There are polynomial-time reductions from 4-POS to the Positivity and Ultimate Positivity Problems for LRS.*

Proof. Suppose we are given an instance of 4-POS, consisting of a polynomial $f(x_1, \ldots, x_s)$. Let $\lambda_1, \ldots, \lambda_s$ be multiplicatively independent algebraic numbers, constructed as in Proposition 5.2. For $j = 1, \ldots, s$, the sequence $\langle y_{j,n} : n \in \mathbb{N} \rangle$ defined by $y_{j,n} = \frac{1}{2}(\lambda_j^n + \overline{\lambda_j}^n)$ satisfies a second-order linear recurrence $y_{j,n+2} = (2a_j/p_j)y_{j,n+1} - y_{j,n}$ with rational coefficients.

Recall, moreover, that given two simple LRS of respective orders l and m, their sum is a simple LRS of order at most $l + m$, their product is a simple LRS of order at most lm, and representations of both can be computed in polynomial time in the size of the input LRS. Thus the sequence $\boldsymbol{u} = \langle u_n : n \in \mathbb{N} \rangle$ given by $u_n = f(y_{1,n}^2, \ldots, y_{s,n}^2)$ is a simple LRS over the rationals. Since f has degree at most 4, the order of $\boldsymbol{u}$ is at most 4^4 times the number of monomials in f and the recurrence satisfied by $\boldsymbol{u}$ can be computed in time polynomial in $||f||$. (Observe that if the degree of f were not fixed, then the above reasoning would yield an upper bound on the order of $\boldsymbol{u}$ that is exponential in the degree of f.)

From Propositions 3.5 and 5.2 it follows that the orbit $\{(\lambda_1^n, \ldots, \lambda_s^n) : n \in \mathbb{N}\}$ is dense in the torus $\mathbb{T}^s$. Thus the set $\{(y_{1,n}^2, \ldots, y_{s,n}^2) : n \in \mathbb{N}\}$ is dense in $[0,1]^s$ and f assumes a strictly negative value on $[0,1]^s$ if and only if $u_n < 0$ for some (equivalently infinitely many) n. This completes the reduction. ◻

6 Conclusion

We have shown that the Ultimate Positivity Problem for simple LRS is decidable in polynomial space and as hard as the decision problem for universal sentences over the field of real numbers. A more careful accounting of the complexity of our decision procedure places it in **coNP** with an oracle for the universal theory of the reals. Thus a **PSPACE**-hardness result for Ultimate Positivity would have non-trivial consequences for the complexity of decision problems for first-order logic over the reals. On the other hand, the obstacle to improving the polynomial-space upper bound is the complexity of computing a basis of the group of multiplicative relations among the characteristic roots of the recurrence.

References

1. F. Amoroso and E. Viada. Small points on subvarieties of a torus. *Duke Mathematical Journal*, 150(3), 2009.
2. J. P. Bell and S. Gerhold. On the positivity set of a linear recurrence. *Israel Jour. Math.*, 57, 2007.
3. P. Bell, J.-C. Delvenne, R. Jungers, and V. Blondel. The continuous Skolem-Pisot problem. *Theor. Comput. Sci.*, 411(40-42):3625–3634, 2010.
4. J. Berstel and M. Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bull. Soc. Math. France*, 104, 1976.
5. V. Blondel, E. Jeandel, P. Koiran, and N. Portier. Decidable and undecidable problems about quantum automata. *SIAM J. Comput.*, 34(6):1464–1473, 2005.
6. V. Blondel and J. Tsitsiklis. A survey of computational complexity results in systems and control. *Automatica*, 36(9):1249–1274, 2000.

7. L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation.* Springer-Verlag, 1997.
8. J. Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of STOC'88*, pages 460–467. ACM, 1988.
9. J. Cassels. *An introduction to Diophantine approximation.* Camb. Univ. Pr., 1965.
10. G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence Sequences.* American Mathematical Society, 2003.
11. J.-H. Evertse. On sums of S-units and linear recurrences. *Compositio Mathematica*, 53(2):225–244, 1984.
12. J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt. Linear equations in variables which lie in a multiplicative group. *Ann. Math.*, 155(3), 2002.
13. A. Fröhlich and M. Taylor. *Algebraic Number Theory.* Camb. Univ. Press, 1993.
14. V. Halava, T. Harju, and M. Hirvensalo. Positivity of second order linear recurrent sequences. *Discrete Applied Mathematics*, 154(3), 2006.
15. 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.
16. R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *JACM*, 33(4), 1986.
17. V. Laohakosol and P. Tangsupphathawat. Positivity of third order linear recurrence sequences. *Discrete Applied Mathematics*, 157(15), 2009.
18. C. Lech. A note on recurring series. *Ark. Mat.*, 2, 1953.
19. K. Mahler. Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38, 1935.
20. D. W. Masser. Linear relations on algebraic groups. In *New Advances in Transcendence Theory.* Camb. Univ. Press, 1988.
21. M. Mignotte, T. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *J. für die reine und angewandte Math.*, 349, 1984.
22. J. Ouaknine and J. Worrell. Decision problems for linear recurrence sequences. In *Proceedings of RP'12*, volume 7550 of *LNCS*. Springer, 2012.
23. J. Ouaknine and J. Worrell. Ultimate Positivity is decidable for simple linear recurrence sequences. *CoRR*, abs/1309.1914, 2013.
24. J. Ouaknine and J. Worrell. On the Positivity Problem for simple linear recurrence sequences. In *Proceedings of ICALP'14*, 2014. *CoRR, abs*/1309.1550.
25. J. Ouaknine and J. Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of SODA'14*. ACM-SIAM, 2014.
26. J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. *J. Symb. Comp.*, 1992.
27. G. Rozenberg and A. Salomaa. *Cornerstones of Undecidability.* Prentice Hall, 1994.
28. T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In *Comptes rendus du congrès des mathématiciens scandinaves*, 1934.
29. M. Soittola. On D0L synthesis problem. In A. Lindenmayer and G. Rozenberg, editors, *Automata, Languages, Development.* North-Holland, 1976.
30. T. Tao. *Structure and randomness: pages from year one of a mathematical blog.* American Mathematical Society, 2008.
31. A. van der Poorten and H. Schlickewei. The growth conditions for recurrence sequences. *Macquarie Math. Reports*, (82-0041), 1982.
32. N. K. Vereshchagin. The problem of appearance of a zero in a linear recurrence sequence (in Russian). *Mat. Zametki*, 38(2), 1985.