# Positivity Problems for Reversible Linear Recurrence Sequences


**George Kenison**
Technische Universität Wien

**Joris Nieuwveld**
Max Planck Institute for Software Systems

**Joël Ouaknine**
Max Planck Institute for Software Systems

**James Worrell**
University of Oxford



## Abstract

It is a longstanding open problem whether there is an algorithm to decide the Positivity Problem for linear recurrence sequences (LRS) over the integers, namely whether given such a sequence, all its terms are non-negative. Decidability is known for LRS of order 5 or less, i.e., for those sequences in which every new term depends linearly on the previous five (or fewer) terms. For *simple* LRS (i.e., those whose characteristic polynomial has no repeated roots), decidability of Positivity is known up to order 9.

In this paper, we focus on the important subclass of *reversible* LRS, i.e., those integer LRS $\langle u_n \rangle_{n=0}^{\infty}$ whose bi-infinite completion $\langle u_n \rangle_{n=-\infty}^{\infty}$ also takes exclusively integer values; a typical example is the classical Fibonacci (bi-)sequence $\langle \ldots, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, \ldots \rangle$. Our main results are that Positivity is decidable for reversible LRS of order 11 or less, and for simple reversible LRS of order 17 or less.



**2012 ACM Subject Classification** Mathematics of computing → Discrete mathematics; Computing methodologies → Algebraic algorithms

**Keywords and phrases** The Positivity Problem, Linear Recurrence Sequences, Verification


## 1 Introduction

### The Positivity Problem

The class of *threshold problems* considers whether a given loop program's variables remain above a fixed threshold before and after each iteration of the loop. In automated verification, this class of decision problems is relevant to program correctness, and particularly questions regarding termination, persistence, and reachability. The moniker *Positivity* is used when the chosen threshold is zero. In this paper, we shall consider the Positivity Problem (and its variants) for a particular class of integer-valued linear recurrence sequences.

An integer-valued *linear recurrence sequence (LRS)* $\langle u_n \rangle_n$ satisfies a relation of the form

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_1 u_{n+1} + a_0 u_n \tag{1}$$

where the coefficients $a_{d-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ and, without loss of generality, we can assume that $a_0 \neq 0$. The sequence $\langle u_n \rangle_n$ is then wholly determined by the recurrence relation and the initial values $u_0, u_1, \ldots, u_{d-1}$. The relation in (1) is said to have *length* $d$ and the *order* of an LRS $\langle u_n \rangle_n$ is equal to the length of the shortest relation that $\langle u_n \rangle_n$ satisfies. The polynomial $f(X) = X^d - a_{d-1}X^{d-1} - \cdots - a_1 X - a_0$ is the *characteristic polynomial* associated with relation (1).

Given an LRS $\langle u_n \rangle_n$, the *Positivity Problem* consists in determining whether $u_n \geq 0$ for each $n \in \mathbb{N}_0$. Positivity is a longstanding open problem and is intimately related to the well-known *Skolem Problem*, which asks to determine whether an LRS vanishes at some term [6, 8]. Indeed, if one could establish decidability of Positivity, then decidability of Skolem would necessarily follow (cf. [14]). One of the motivations to study Positivity lies in its connections to program verification [16]. Take, for example, the following linear loop $P$ with inputs $\underline{w}, \underline{b} \in \mathbb{Z}^d$ and $A \in \mathbb{Z}^{d\times d}$ where

$$P\colon \underline{v} \leftarrow \underline{w};\ \ \textbf{while}\ \underline{b}^\top \underline{v} \geq 0\ \textbf{do}\ \underline{v} \leftarrow A\underline{v}. \tag{2}$$

Let $\langle u_n \rangle_n$ be the LRS with terms given by $u_n = \underline{b}^\top A^n \underline{w}$. It is clear that loop $P$ terminates if and only if there exists an $n \in \mathbb{N}_0$ such that $u_n < 0$. Conversely, to each LRS $\langle u_n \rangle_n$ we can associate a linear loop of the form (2): one need only take $A$ to be the transpose of the companion matrix associated with $\langle u_n \rangle_n$ so that

$$A = \begin{pmatrix} a_{d-1} & 1 & \cdots & 0 & 0 \\ \vdots & 0 & \ddots & 0 & 0 \\ a_2 & 0 & \cdots & 1 & 0 \\ a_1 & 0 & \cdots & 0 & 1 \\ a_0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \underline{b}^\top = (u_{d-1}, \ldots, u_1, u_0), \text{ and } \underline{w} = (1, 0, \ldots, 0)^\top$$

in order to recover the terms $u_{n+d-1} = \underline{b}^\top A^n \underline{w}$.

Variants of the Positivity Problem have also garnered attention in the literature. For example, the *Ultimate Positivity Problem* weakens the guard clause: given an LRS $\langle u_n \rangle_n$, determine whether there exists an $N \in \mathbb{N}$ such that $u_n \geq 0$ if $n > N$. By contrast, the *Simple Positivity Problem* restricts the class of sequences under consideration to those that are simple. Here an LRS $\langle u_n \rangle_n$ is *simple* if each of the roots of the associated characteristic polynomial has algebraic multiplicity one. In this paper, we focus on the *Reversible Positivity Problem*, i.e., the restriction of the Positivity Problem to the class of LRS that are reversible (as defined below).

### Background and Motivation

Lipton *et al.* [11] coined the term *reversible* to describe the class of LRS that assume exclusively integer values, whether the sequences are expanded forwards or backwards. Equivalently, such LRS can be shown to satisfy relations of the form (1) with the condition $a_0 = \pm 1$ (or, alternatively, the associated characteristic polynomial satisfies $f(0) = \pm 1$). The subclass of while loops (as in (2)) naturally associated with reversible sequences have *unimodular* update matrices. The inverse $A^{-1}$ of a unimodular matrix $A$ is likewise unimodular. Thus the uniquely defined bi-infinite extension $\langle u_n \rangle_{n=-\infty}^{\infty}$ with each $u_n = \underline{b}^\top A^n \underline{w}$ (as above) is integer-valued.

The decidability of Reversible Skolem—where one restricts the Skolem Problem to reversible LRS—was established up to order 7 in a recent paper by Lipton *et al.* [11]. Kenison [9] gave an alternative proof of this decidability result, leveraging a powerful result for algebraic units due to Dubickas and Smyth [5]. In general, the Skolem Problem is only known to be decidable for arbitrary LRS up to order four [12, 23]. The Positivity Problem was shown decidable for arbitrary LRS of order five or less [17], and for simple LRS of order 9 or less [14]. The Ultimate Positivity Problem is also decidable for arbitrary LRS of order 5 of less, as well as for simple LRS of arbitrary order [17, 15].

### Contributions

In this paper, we shall consider Positivity problems for reversible LRS. We will exploit spectral properties of reversible LRS and employ techniques from both Galois theory and Diophantine approximation to establish decidability at higher orders than is currently known for general positivity. Our main contributions are as follows:

▶ **Theorem 1.** *For reversible LRS, the Positivity and Ultimate Positivity Problems are both decidable up to order* 11*.*

▶ **Theorem 2.** *For simple reversible LRS, the Positivity Problem is decidable up to order* 17*.*

### Structure

The remainder of this paper is structured as follows. In the next section we review necessary preliminary material. In Section 3, we prove results on the root structures of characteristic polynomials associated with reversible LRS. In Section 4, we prove Theorems 1 and 2. We also consider barriers impeding further progress to the state of the art (i.e., decidability results at higher orders) by exhibiting sequences that are not amenable to standard Diophantine approximation techniques due to certain spectral properties (see Section 5). The calculations involved in preparing these hard instances were performed in SageMath [4].

# 2 Preliminaries

## 2.1 Linear Recurrence Sequences

We expand upon the standard terminology for LRS given in the introduction. It is straightforward to see that an LRS $\langle u_n\rangle_n$ is wholly determined by a recurrence relation (as in (1)) and the initial values $u_0, u_1, \ldots, u_{d-1}$.

Let $\langle u_n\rangle_n$ be an LRS with characteristic polynomial $f$. It is well-known that an LRS admits a closed-form representation as an exponential polynomial; specifically, for each $n \in \mathbb{N}_0$, we have $u_n = A_1(n)\lambda_1^n + \cdots + A_\ell(n)\lambda_\ell^n$. Here the *characteristic roots* $\lambda_1, \ldots, \lambda_\ell$ are the distinct roots of $f$. Further, the polynomial coefficients $A_j \in \overline{\mathbb{Q}}[X]$ are completely determined by the initial values of $\langle u_n\rangle_n$. The polynomial coefficients for a simple LRS are all constants; that is, if $\langle u_n\rangle_n$ is simple, then $u_n = A_1\lambda_1^n + \cdots + A_\ell\lambda_\ell^n$.

An LRS is *degenerate* when there are two distinct characteristic roots whose quotient is a root of unity. Otherwise, the sequence is said to be *non-degenerate*.

Let $\lambda_1, \ldots, \lambda_\ell$ be the characteristic roots of an LRS $\langle u_n\rangle_n$. A characteristic root $\lambda$ of $\langle u_n\rangle_n$ is *dominant* if $|\lambda| \geq |\lambda_j|$ for each $j \in \{1, \ldots, \ell\}$. By convention, when we talk about the number of dominant roots *we do not count multiplicity*, e.g., a recurrence sequence that satisfies the relation $u_{n+2} = 2u_{n+1} - u_n$ with characteristic polynomial $(X-1)^2$ has only one dominant root.

In the sequel, we will state and prove technical results for polynomials in $\mathbb{Z}[X]$. Here we say that a polynomial in $\mathbb{Z}[X]$ is *non-degenerate* if no quotient of distinct roots is a root of unity and we say that it is *reversible* if it is monic and has constant term $\pm 1$. Note that our use of these terms for both recurrence sequences and their characteristic polynomials is consistent.

## 2.2 The Positivity Problem

In this subsection we briefly recall decidability results for the Positivity Problem for LRS. We first recall the standard assumptions that permit us to reduce the problem of deciding positivity to that of deciding positivity for LRS that are both non-degenerate and possess a positive dominant characteristic root.

First, it is well known (cf. [6, 8]) that we can effectively reduce the computational study of LRS to that of non-degenerate LRS. This observation follows because each degenerate LRS can be realised as an interleaving of finitely many non-degenerate LRS of the same order. Thus we need only consider non-degenerate LRS when studying positivity. We note also that this reduction preserves the quality of having simple characteristic roots.

Second, let us recall the following classical consequence of the Vivanti–Pringsheim Theorem from complex analysis [24, 18] (see also [22, Section 7.21]).

▶ **Lemma 3.** *Suppose that a non-zero LRS $\langle u_n\rangle_n$ has no positive dominant characteristic root. Then the sets $\{n \in \mathbb{N} : u_n > 0\}$ and $\{n \in \mathbb{N} : u_n < 0\}$ are both infinite.*

As a consequence of Lemma 3, we can reduce the problem of deciding positivity to LRS that possess a positive dominant characteristic root.

Together, the two preceding assumptions show that the sequences we consider have an odd number of dominant roots: the set of dominant roots comprises complex-conjugate pairs of roots and a single positive dominant root. Note that a second real dominant root would violate non-degeneracy.

Ouaknine and Worrell showed that the Simple Positivity Problem for LRS is decidable up to order nine [14]. The main technical contribution of that paper was the following result, which, in combination with the various observations above, covers all sequences up to order nine.

▶ **Theorem 4.** *Let $\langle u_n\rangle_n$ be a non-degenerate simple LRS with characteristic polynomial $f \in \mathbb{Z}[x]$ and a positive dominant root. If $f \in \mathbb{Z}[x]$ has either at most eight dominant roots or precisely nine roots, then we can determine whether $u_n \geq 0$ for each $n \in \mathbb{N}_0$.*

## 2.3 Number Theory

An algebraic integer is a *unit* if its multiplicative inverse is also an algebraic integer. It is a basic fact that an algebraic number is a unit if and only if its minimum polynomial in $\mathbb{Z}[X]$ is monic and and has constant term $\pm 1$. Thus the characteristic roots of a reversible LRS are all units.

## 2.4 Group Theory

A group $G$ is said to act *transitively* on a set $X$ if for each pair $x, y \in X$ there is a $g \in G$ such that $gx = y$. The *stabilizer* $G_x$ of an element $x$ in $X$ is defined as the set $\{g \in G : gx = x\}$. The Orbit-Stabilizer Theorem (see, for example, [19, Theorem 3.19]) implies that if $G$ acts transitively on $X$, the cardinality of $G_x$ is the same for each $x \in X$. Further, $\#\{g \in G : gx = y\}$ is the same for all $x, y \in G$ in this scenario.

## 2.5 Galois Theory

We assume familiarity with basic notions in Galois theory and the theory of number fields. For reference, we recommend standard textbooks such as [3, 21].

Recall the following theorem due to Kronecker [10].

▶ **Theorem 5.** *Let $f \in \mathbb{Z}[x]$ be a monic polynomial such that $f(0) \neq 0$. Suppose that all the roots of $f$ have absolute value at most $1$. Then all the roots of $f$ are roots of unity.*

We deduce the following. If $f \in \mathbb{Z}[x]$ is the characteristic polynomial of a reversible LRS $\langle u_n \rangle_n$ such that the roots of $f$ all lie in the unit disk $\{z \in \mathbb{C} : |z| \leq 1\}$, then the roots of $f$ are all roots of unity and so $\langle u_n \rangle_n$ is of order one or degenerate. In the former case, positivity of $\langle u_n \rangle_n$ is easily determined and in the latter case, determining whether $\langle u_n \rangle_n$ reduces to studying positivity for associated non-degenerate LRS. Thus in the sequel we shall always assume, without loss of generality, that the dominant roots of $f$ lie on a circle with radius strictly larger than 1.

The roots of an irreducible polynomial are necessarily Galois conjugates. We call the quotient of two distinct roots of an irreducible polynomial a *conjugate ratio*.

Key to the technical lemmas we prove in the sequel are results concerning identities between the roots of irreducible polynomials. We employ a powerful result due to Dubickas and Smyth [5], Theorem 6 below, concerning necessary conditions for an algebraic unit and all its Galois conjugates to lie on two concentric circles centred at the origin. (Theorem 6 is a specialisation of the general result [5, Theorem 2.1].)

▶ **Theorem 6.** *Suppose that $f \in \mathbb{Z}[X]$ is an irreducible, reversible polynomial of degree $d$ such that all the roots of $f$ lie on two circles centred at the origin. Let $r, R$ be the radii of the respective circles and, in addition, suppose that at most half of the roots of $f$ lie on the circle of radius $r$. Then $d$ is either even and on both circles lie an equal number of roots, or $d$ is a multiple of three and one-third lie on the circle of radius $R$. In the latter case, we additionally have that for every root $\beta$ on the circle of radius $r$ there exists $n > 0$ such that $\beta^n \in \mathbb{R}$.*

We shall frequently employ the following lemma, versions of which were proved by Smyth [20] and Ferguson [7].

▶ **Lemma 7.** *Suppose that $\lambda$ is an algebraic number with Galois conjugates $\beta$ and $\gamma$ satisfying $\lambda^2 = \beta\gamma$. Then the conjugate ratio $\lambda/\beta$ is a root of unity.*

## 3 Root Analysis of Reversible Polynomials

The main result of this section is Theorem 13, concerning the number of dominant roots of a reversible polynomial. Essentially the theorem says that, excepting a number of special cases, no more than half of the roots of such a polynomial can be dominant. This is the key technical tool behind our main decidability results for the Positivity Problem for reversible LRS.

Our starting point is the following two lemmas about dominant roots of reversible polynomials. These can be considered as weak forms of the main result of the section (and are used in the proof thereof).

▶ **Lemma 8.** *Let $f \in \mathbb{Z}[X]$ be an irreducible non-degenerate polynomial with a real dominant root $\lambda$. Then $f$ has exactly one dominant root.*

**Proof.** Let $\lambda$ be a real dominant root. Suppose $\beta$ is also a dominant root. Then $\lambda^2 = \beta\overline{\beta}$ and hence $\lambda/\beta$ is a root of unity by Lemma 7. Since $f$ is non-degenerate we have $\lambda = \beta$, that is, $f$ has exactly one dominant root. ◀

▶ **Lemma 9.** *Suppose that $f \in \mathbb{Z}[X]$ is irreducible, non-degenerate, and reversible, with $2m$ non-real dominant roots and no real dominant roots. Then $\deg(f) > 3m$ if $m \geq 2$. Further, $\deg(f) \leq 3m$ only if $(\deg(f), m) = (3, 1)$ or $f$ is constant.*

**Proof.** Since $f$ has at least $2m$ roots, it is clear that $\deg(f) \geq 2m$. The case where $m = 0$ pertains to constant polynomials, thus we need only consider the case when $m \geq 1$.

We will first show that $\deg(f) > 2m$. Assume, for a contradiction, that $\deg(f) = 2m$. Then the roots of $f$ all lie on the circumference of some circle centred at the origin. We make the following two observations. First, $f$ is reversible, and hence monic. Second, by Vieta's formulas, $|f(0)| = 1$ is equal to the absolute value of the product of the roots of $f$. From these observations, we conclude that the roots of $f$ all lie on the unit circle and, by Theorem 5, are therefore roots of unity. As $m \geq 1$, $f$ has at least two roots, and their conjugate ratio is thus a root of unity. We have reached a contradiction: $f$ is assumed to be non-degenerate. Thus $\deg(f) > 2m$.

Consider the subcase where $m = 1$. Assume that $2m < \deg(f) \leq 3m$, then clearly we have $\deg(f) = 3$. The assertion in the lemma trivially holds. Hereafter we assume that $m \geq 2$.

We now show that under the assumption that $m \geq 2$, we necessarily have $\deg(f) \geq 3m$. Let $\lambda_1, \overline{\lambda_1}, \ldots, \lambda_m, \overline{\lambda_m}$ be the $2m$ dominant roots of $f$. Thus $\lambda_1\overline{\lambda_1} = \lambda_i\overline{\lambda_i}$ for each $i \in \{1, \ldots, m\}$. Since $2m < \deg(f)$, $f$ has a non-dominant root $\gamma$. Further, since $f$ is irreducible, there is a Galois automorphism $\sigma$ such that $\sigma(\lambda_1) = \gamma$. We claim that for each $i \in \{2, \ldots, m\}$ at least one of $\sigma(\lambda_i)$ and $\sigma(\overline{\lambda_i})$ is a non-dominant root of $f$. Assume, for a contradiction, that the claim does not hold. Then there is an $i \in \{2, \ldots, m\}$ such that both $\sigma(\lambda_i)$ and $\sigma(\overline{\lambda_i})$ are dominant roots. The map $\sigma$ necessarily preserves polynomial symmetries between the roots of $f$ and so $\gamma\sigma(\overline{\lambda_1}) = \sigma(\lambda_i)\sigma(\overline{\lambda_i})$. However, since $\sigma(\lambda_1) = \gamma$ is strictly smaller in absolute value than both $\sigma(\lambda_i)$ and $\sigma(\overline{\lambda_i})$, we have $|\gamma\sigma(\overline{\lambda_1})| < |\sigma(\lambda_i)\sigma(\overline{\lambda_i})|$. This last inequality contradicts the aforementioned symmetry between dominant roots. We conclude that the list of non-dominant roots of $f$ includes $\gamma$ and at least one of $\sigma(\lambda_i)$ and $\sigma(\overline{\lambda_i})$ for each $i \in \{2, \ldots, m\}$. Thus $f$ has at least $m$ non-dominant roots and so $\deg(f) \geq m + 2m = 3m$.

Finally, we eliminate the case that $\deg(f) = 3m$ when $m \geq 2$. Assume, for a contradiction, that $\deg(f) = 3m$. We can apply the preceding argument to the reciprocal polynomial of $f$ to deduce that the $m$ non-dominant of $f$ are equal in modulus and so all lie on a circle $\{z \in \mathbb{C} : |z| = r\}$ for some $r > 0$. Observe that $f$ is an irreducible and reversible polynomial whose roots lie on exactly two concentric circles centred at the origin. Thus, by Theorem 6, each non-dominant root of $f$ takes the form $r\mathrm{e}^{\mathrm{i}\theta}$ where $\mathrm{e}^{\mathrm{i}\theta}$ is a root of unity. Since $m \geq 2$, there are at least two distinct roots of $f$, say $r\mathrm{e}^{\mathrm{i}\theta}$ and $r\mathrm{e}^{\mathrm{i}\theta'}$, of the prescribed form. It follows that the conjugate ratio $r\mathrm{e}^{\mathrm{i}\theta}/r\mathrm{e}^{\mathrm{i}\theta'}$ is a root of unity, which contradicts our assumption that $f$ is non-degenerate. Hence $\deg(f) > 3m$ if $m \geq 2$, from which the desired result follows. ◀

In order to improve the bound from from $\deg(f) > 3m$ to $\deg(f) \geq 4m$, we shall introduce new and novel techniques for counting symmetries in the roots of $f$. Let $\lambda_1, \ldots, \lambda_\ell$ be the roots of $f$. The interesting case occurs when all dominant roots are non-real, say $\lambda_1, \overline{\lambda_1}, \ldots, \lambda_m, \overline{\lambda_m}$. Let $\mu_1 := \lambda_1\overline{\lambda_1}$ and $g$ be the minimal polynomial of $\mu_1$ (hereafter we shall refer to $g$ as the *dominating polynomial of* $f$). Let $\mu_2, \ldots, \mu_n$ be the Galois conjugates of $\mu_1$ (and thus the other roots of $g$) and $\sigma_1, \ldots, \sigma_n$ the Galois automorphisms associated with $g$ such that $\sigma_j(\mu_1) = \mu_j$.

Set $K = \mathbb{Q}(\mu_1, \ldots, \mu_n)$ and $L = \mathbb{Q}(\lambda_1, \ldots, \lambda_\ell)$. Clearly, $K \subset L$, and so each $\sigma_j$ can be lifted to an automorphism $\widetilde{\sigma_j}$ in $\mathrm{Gal}_{\mathbb{Q}}(L)$ such that $\widetilde{\sigma_j}|_K = \sigma_j$. Applying these $\widetilde{\sigma_j}$ on

$\lambda_1\overline{\lambda_1} = \cdots = \lambda_m\overline{\lambda_m} = \mu_1$ gives rise to the following $n$ equations:

$$\begin{array}{ccc} \alpha_{1,1,1}\alpha_{1,1,2} = \ldots = \alpha_{m,1,1}\alpha_{m,1,2} & = \mu_1 \\ \vdots \quad \vdots & \vdots \\ \alpha_{1,n,1}\alpha_{1,n,2} = \ldots = \alpha_{m,n,1}\alpha_{m,n,2} & = \mu_n \end{array} \tag{3}$$

where $\alpha_{i,j,1} = \widetilde{\sigma_j}(\lambda_i)$ and $\alpha_{i,j,2} = \widetilde{\sigma_j}(\overline{\lambda_i})$. Thus, all $\alpha_{i,j,k}$ are roots of $f$. For a root $\lambda$ of $f$, we define the *equation number*

$$E = \#\{(i,j,k) : \alpha_{i,j,k} = \lambda \text{ for } 1 \le i \le m, 1 \le j \le n, k = 1, 2\}.$$

In Lemma 11, it will be shown that $E$ is independent of the choice of root $\lambda$. It is useful to see the two roots of $f$ in one position in one equation in (3) as a *pair*. In other words, $\alpha_{i,j,1}$ and $\alpha_{i,j,2}$ are *paired* for all $1 \le i \le m$ and $1 \le j \le n$. Further, for $j = 1, \ldots, n$, denote $\mathscr{A}_j = \{\alpha_{1,j,1}, \alpha_{1,j,2}, \ldots, \alpha_{m,j,1}, \alpha_{m,j,2}\}$. Note that $\#\mathscr{A}_j = 2m$, as $\widetilde{\sigma_j}$ is a bijection between the set of dominant roots of $f$ and $\mathscr{A}_j$.

We claim that $\mathscr{A}_j$ is independent of the choice of lift $\widetilde{\sigma_j}$ of $\sigma_j$. If $\lambda$ and $\lambda'$ are roots of $f$ such that $\lambda\lambda' = \mu_j$, then $\widetilde{\sigma_j}^{-1}(\lambda)\widetilde{\sigma_j}^{-1}(\lambda') = \mu_1$. Because $\widetilde{\sigma_j}^{-1}(\lambda)$ and $\widetilde{\sigma_j}^{-1}(\lambda')$ are roots of $f$ whose product is equal to $\mu_1 = \lambda_1\overline{\lambda_1}$, we easily deduce that both $\widetilde{\sigma_j}^{-1}(\lambda)$ and $\widetilde{\sigma_j}^{-1}(\lambda')$ are dominant roots of $f$. Further, since $\widetilde{\sigma_j}$ is a bijection, $\lambda = \widetilde{\sigma_j}\left(\widetilde{\sigma_j}^{-1}(\lambda)\right) \in \mathscr{A}_j$ (and similarly $\lambda' \in \mathscr{A}_j$). We make two deductions. First, if $\mu_j$ is the product of two distinct roots of $f$ then those roots are two elements of $\mathscr{A}_j$. Second, we infer our claim that $\mathscr{A}_j$ is independent of the choice of $\widetilde{\sigma_j}$.

In the case of one dominant root, the same construction applies: $g$ is defined as the minimum polynomial of $\lambda_1^2$, where $\lambda_1$ is the sole dominant root of $f$. By non-degeneracy, the squares of all roots of $f$ are distinct, and so $\deg(f) = \deg(g)$, $\mu_j = \lambda_j^2$ for $j = 1, \ldots, \deg(f)$ and $E = 2$ for all roots of $f$ (it appears once as a square). Only, $\mathscr{A}_j = \{\lambda_j\}$ consists of exactly one root of $f$.

▶ **Lemma 10.** *Suppose that $f \in \mathbb{Z}[x]$ is reversible, non-degenerate, and irreducible with $2m$ non-real dominant roots and has degree less than $4m$. Write $g$ for the dominating polynomial of $f$. Then $g$ is also non-degenerate.*

**Proof.** Assume, for a contradiction, that the conjugate ratio $\mu_j/\mu_{j'}$ of $g$ is a root of unity. Both root sets $\mathscr{A}_j$ and $\mathscr{A}_{j'}$ have cardinality $2m$. Since $\deg(f) < 4m = \#\mathscr{A}_j + \#\mathscr{A}_{j'}$, we deduce that $\mathscr{A}_j \cap \mathscr{A}_{j'}$ is non-empty. Let $\lambda \in \mathscr{A}_j \cap \mathscr{A}_{j'}$ and $\kappa, \kappa'$ be roots of $f$ such that $\lambda\kappa = \mu_j$ and $\lambda\kappa' = \mu_{j'}$. Since $\mu_j \neq \mu_{j'}$, we have $\kappa \neq \kappa'$. It follows that $f$ is degenerate because $\kappa/\kappa' = \mu_j/\mu_{j'}$ is a root of unity. From this contradiction, we deduce that $g$ is non-degenerate. ◀

▶ **Lemma 11.** *Suppose that $f \in \mathbb{Z}[X]$ is reversible, non-degenerate, and irreducible with $2m$ non-real dominant roots. Write $g$ for the dominant polynomial of $f$. Then all roots of $f$ have the same equation number $E$ and*

$$2m\deg(g) = E\deg(f). \tag{4}$$

**Proof.** We use the notation of $\lambda_i, \mu_j, \sigma_j, \widetilde{\sigma_j}$, $\alpha_{i,j,k}$, $K$, $L$, etc. as above.

Set $H = \mathrm{Gal}_{\mathbb{Q}}(K)$ and $G = \mathrm{Gal}_{\mathbb{Q}}(L)$. By the Orbit-Stabilizer Theorem , the number of $\sigma \in H$ such that $\sigma(\mu_1) = \mu_j$ is independent of the choice of $j \in \{1, \ldots, n\}$. Now each $\sigma \in H$ has the same number of lifts to $G$, and so the number of elements of $G$ that map $\mu_1$

to each $\mu_j$ is independent of $j \in \{1, \dots, n\}$. Thus the number of elements of $G$ such that the image of $\mathscr{A}_1$ is $\mathscr{A}_j$ is also independent of the choice of $j$. Here we note that we cannot have $\mathscr{A}_{j_1} = \mathscr{A}_{j_2}$ for$j_1 \neq j_2$. Indeed, this phenomenon is witnessed only if $\mu_{j_1}/\mu_{j_2}$ is a root of unity. This phenomenon cannot come to pass because $g$ is non-degenerate (Lemma 10).

Once again by the Orbit-Stabilizer Theorem, for every choice of two roots $\lambda, \lambda'$ of $f$, the number of $\sigma \in G$ such that $\sigma(\lambda) = \sigma(\lambda')$ is equal. Thus for each root $\lambda$ of $f$, the number of $\sigma \in G$ such that one of $\widetilde{\sigma}(\lambda_1), \widetilde{\sigma}(\overline{\lambda_1}), \dots, \widetilde{\sigma}(\lambda_m), \widetilde{\sigma}(\overline{\lambda_m})$ equals $\lambda$ is independent of the choice of $\lambda$. Together, this shows that the equation number $E$ is independent of the choice of the root $\lambda$.

The equation $2m \deg(g) = E \deg(f)$ follows from counting the number of $\alpha_{i,j,k}$. On the one hand, there are $\deg(g)$ equations with $2m$ entries. On the other hand, there are $\deg(f)$ roots each appearing $E$ times. ◀

This next result increases the bound on the degree of $f$ to $\deg(f) \geq 4m$.

▶ **Theorem 12.** *Let $f \in \mathbb{Z}[X]$ be an irreducible, non-degenerate, and reversible polynomial with $2m$ dominant non-real roots and no real dominant roots, then $(\deg(f), m) = (3, 1)$ or $\deg(f) \geq 4m$.*

**Proof.** Assume, for a contradiction, that $f$ is a counterexample to the theorem of minimal degree.

From Lemma 9, we deduce that $\deg(f) > 3m$ if we are not in the exceptional case $(\deg(f), m) = (3, 1)$. As we assume that $f$ is a counterexample to Theorem 12, $\deg(f) < 4m$ as well. We shall employ the preceding notation for the dominating polynomial $g$, the sets of roots $\mathscr{A}_j$ of $f$, and the equation number $E$.

Consider that there are $2m$ distinct roots of $f$ in each equation in (3). Since $\deg(f) < 4m$ and $f$ has $2m$ dominant roots, there is at least one dominant root of $f$ in each such equation. Let $\gamma$ be a root of $f$ with minimal absolute value, then $|\gamma\lambda_1|$ is the minimal absolute value attained by any root of $g$. We now show that at least half of the roots of $g$ lie on the circle $\{z \in \mathbb{C} : |z| = |\gamma\lambda_1|\}$. Observe that $\gamma$ is witnessed in $E$ (and so more than half) of the pairings in (3) and, further, is necessarily paired with a dominant root (for otherwise, a pairing between $\gamma$ and a non-dominant root breaks the equality in (3)). From (4) and our assumption that $\deg(f) < 4m$, we deduce that $2E > \deg(g)$, and so $\gamma$ appears in more than half of the equations in (3). Each such equation is in correspondence with a root of $g$ of minimal absolute value.

Consider the polynomial $h(X) := g(0)X^n g(X^{-1})$. The polynomial $X^n g(X^{-1})$ is the reciprocal polynomial of $g$ and so immediately, the roots of $h$ are precisely $\mu_1^{-1}, \dots, \mu_n^{-1}$ and $n = \deg(g) = \deg(h)$. From the preceding discussion, more than half of the roots of $h$ are dominant. Moreover, we can easily deduce that $h$ is reversible, irreducible, and non-degenerate as $g$ has these properties. Thus $h$ is another counterexample to the statement in Theorem 12. All that remains is to derive a contradiction from our assumption that $f$ has minimal degree. We derive this contradiction by proving that $\deg(h) < \deg(f)$ and $h$ does not belong to either one of the exceptional cases.

Observe that $h$ cannot belong to one of the exceptional cases since (4) has no integer solutions when $n = 1, 2, 3$ and $3m < \deg(f) < 4m$. Thus it remains to show that $n \geq \deg(f)$ is absurd. Let us assume, for a contradiction, that $\lambda_1$ appears in a product pair with a dominant root other than $\overline{\lambda_1}$ in the $j$th equation of (3). Then $\mu_1$ and $\mu_j$ have equal absolute value. If $\mu_j$ is real, $\mu_1/\mu_j = \pm 1$ contradicting our non-degeneracy assumption (Lemma 10). Similarly, we derive a contradiction to our non-degeneracy assumption if $\mu_j$ is non-real by Lemma 7. Thus, we can pair $\lambda_1$ with the $\deg(f) - 2m < 2m$ non-dominant roots of $f$ and $\overline{\lambda_1}$.

This gives the upper bound $E \leq \deg(f) - 2m + 1 \leq 2m$ on $E$. We substitute our assumption that $n = \deg(g) \geq \deg(f)$ into (4) to obtain a lower bound $2m \leq E$. Thus, $E = 2m$.

We use the equality $E = 2m$ to deduce that $\deg(f) = 4m - 1$ and make the following observations. Each of the $2m$ dominant roots of $f$ pair with their respective complex conjugate and all of the $2m - 1$ non-dominant roots of $f$. Thus we can pair each non-dominant root of $f$ with $2m$ dominant roots. Further, every pair of non-dominant roots of $f$ appears in at least one equation in (3). Thus the roots of $g$ and $h$ lie on two concentric circles centred at the origin. The roots of $g$ are distributed so that $g$ has exactly one dominant root and $2m + (2m - 1) - 1 = 4m - 2$ non-dominant roots. By construction, $h$ has exactly one non-dominant root and $4m - 2$ dominant roots. This distribution of roots is not possible by Theorem 6, hence a contradiction.

In summary, $f$ cannot be a counterexample to Theorem 12 of smallest possible degree. We thus deduce that all polynomials that satisfy the hypothesis in the theorem obey the bound $\deg(f) \geq 4m$, as required. ◀

The only superfluous assumption in this theorem is that $f$ has to be irreducible. It can be circumvented by a careful case analysis.

▶ **Theorem 13.** *Let $f$ be a non-degenerate reversible polynomial. Suppose that more than half of the roots of $f$ are dominant. Then either $f$ is linear or $f$ is cubic with two dominant roots.*

**Proof.** Let $f$ be a counterexample of minimal degree, and factor $f$ into irreducible polynomials $f_1, \dots, f_k$. For $1 \leq i \leq k$, let $m_i'$ be the number of dominant roots of $f_i$. Call an irreducible factor *sharp* if $2m_i' = \deg(f_i)$ and *special* if $2m_i' > \deg(f_i)$. From Lemma 8 and Theorem 12, it follows that if an irreducible factor is special, then $(\deg(f_i), m_i') = (1, 1)$ or $(3, 2)$. If $k = 1$, then $f$ is irreducible and the result follows automatically. Thus we can freely assume that $k \geq 2$. Since $f$ is a counterexample of minimal degree, a straightforward proof by contradiction permits us to assume $k = 2$. Thus our argument reduces to the following cases: we need only show that the product of either two special polynomials or a special and a sharp polynomial breaks the hypothesis. By renumbering, we can assume $f_1$ is special and $f_2$ is either sharp or special. We observe that under our assumptions the dominant roots of $f_1$ and $f_2$ are necessarily equal in absolute value and, as we do not count multiplicity, $f_1 \neq f_2$.

We begin our case analysis. First, consider the case where $(\deg(f_1), m_1') = (1, 1)$. Then $f_1(X) = X \pm 1$ as $f_1$ is reversible. Since the root $\mp 1$ of $f_1$ is a dominant root of $f$, we deduce that all roots of $f$ lie on the unit circle as the roots of $f$ are algebraic units. When we combine Lemma 8, Theorem 12, and our assumption that at least half of the roots of $f$ are dominant, we deduce that $(\deg(f_2), m_2') = (1, 1)$ and so $f_2(X) = X \mp 1$. Thus $-1$ and 1 are both roots of $f$, which contradicts our assumption that $f$ is non-degenerate.

Second, let us suppose that $(\deg(f_1), m_1') = (3, 2)$. Following the argument in the preceding case, either $(\deg(f_2), m_2') = (3, 2)$ or $\deg(f_2) = 2m_2'$. In the former, the non-dominant roots $\gamma_1$ and $\gamma_2$ of $f_1$ and $f_2$ (respectively) are both real and equal in modulus. This is straightforward to see since each $f_j$ is of the form $f_j = (x - \gamma_j)(x - R\mathrm{e}^{\mathrm{i}\theta_j})(x - R\mathrm{e}^{-\mathrm{i}\theta_j})$ for some $R > 1$ and $\gamma_j := \pm R^{-2}$. We cannot have two such irreducible factors since then the ratio $\gamma_1/\gamma_2 = \pm 1$, which breaks either the non-degeneracy assumption on $f$ or the assumption that $f_1 \neq f_2$.

We continue with the latter subcase $(\deg(f_1), m_1') = (3, 2)$ and $\deg(f_2) = 2m_2'$. Since the dominant roots of $f_1$ and $f_2$ are dominant roots of $f$, the dominating polynomials of $f_1$ and $f_2$ are one and the same, say $g$. Let $E_1$ and $E_2$ be the respective equation numbers of $f_1$ and $f_2$. From (4), $2\deg(g) = E_1 \deg(f_1) = 3E_1$. We thus deduce that $E_1$ is even.

Since $1 \leq E_1 \leq \deg(f_1) = 3$ (each pairing is distinct), we have that $E_1 = 2$ and, it follows immediately, $\deg(g) = 3$. We substitute this result and our assumption that $\deg(f_2) = 2m_2'$ into (4) in order to obtain $m_2' \deg(g) = 3m_2' = 2E_2m_2'$. We have reached a contradiction: $E_2 = 3/2$ is not an integer. We have exhausted the possibilities for constructing a minimal counterexample $f$ and find that no such counterexample exists. We have thus proved Theorem 13. ◀

## 4 Decidability at Low Orders

In this section we complete the proofs of our two main theorems concerning the Positivity Problem for reversible LRS. We start with Theorem 2, which states that positivity of reversible sequences that are moreover simple is decidable up to order 17.

**Proof of Theorem 2.** As previously noted, can reduce the Simple Reversible Positivity Problem to deciding positivity for the subclass of simple reversible LRS that are additionally both non-degenerate and in possession of a positive dominant root.

In light of the preceding paragraph, consider the subclass of non-degenerate, simple, and reversible LRS with a positive dominant root. Let $f$ be the characteristic polynomial associated with a sequence in this class. Without loss of generality, we can additionally assume that fewer than half of the roots of $f$ are dominant. If $f \in \mathbb{Z}[X]$ has at least nine dominant roots, then, by Theorem 13, we have the bound $\deg(f) \geq 18$. Taking the contrapositive, if $f$ is again the characteristic polynomial of a sequence in this subclass with $\deg(f) \leq 17$, then $f$ has at most eight dominant roots.

Now we invoke Theorem 4 to deduce that, in the aforementioned subclass, positivity is decidable for LRS up to order 17. As noted at the beginning of this proof, this deduction is sufficient to obtain the desired result: simple reversible positivity is decidable up to order 17. ◀

We now turn our attention to reversible sequences in general, i.e., no longer assuming that the characteristic roots are simple. Here, as stated in Theorem 1, we have decidability up to order 11.

**Proof of Theorem 1.** Assume, for a contradiction, that $\langle u_n \rangle_n$ is a reversible LRS and counterexample to the statement; that is to say, $\langle u_n \rangle_n$ is a reversible LRS with order at most 11 for which we cannot determine positivity or ultimate positivity.

From our earlier discussion on the Positivity Problem and Ultimate Positivity Problem in Subsection 2.2, it follows that we can reduce both problems for reversible LRS to deciding (ultimate) positivity for the subclass of reversible LRS that are additionally both non-degenerate and in possession of a positive dominant root.

For the class of reversible LRS with one dominant root, decidability of (ultimate) positivity is considered folklore. Thus we freely assume that $\langle u_n \rangle_n$ has at least three dominant roots (the positive root and a pair of complex conjugate roots). By Theorem 2 for positivity and the earlier mentioned results in [15] for ultimate positivity, we can also assume that $\langle u_n \rangle_n$ has a non-simple characteristic root. Now consider the exponential polynomial representation of $\langle u_n \rangle_n$: deciding (ultimate) positivity for LRS whose dominant characteristic roots are all simple reduces to deciding (ultimate) positivity for simple LRS. So, in addition, we shall assume that $\langle u_n \rangle_n$ has a non-simple dominant characteristic root. We will use the following claims, whose proofs are given immediately below.

▷ Claim 14. Suppose that the real positive dominant root $\rho$ of sequence $\langle u_n\rangle_n$ (as above) is the only non-simple dominant root of $\langle u_n\rangle_n$. Then we can determine whether $\langle u_n\rangle_n$ is (ultimately) positive.

▷ Claim 15. Suppose that sequence $\langle u_n\rangle_n$ (as above) possesses non-real dominant roots that are not simple and, further, that the real dominant root $\rho$ is simple. Then $\langle u_n\rangle_n$ is neither ultimately positive nor positive.

In light of the preceding claims, we freely assume that the counterexample $\langle u_n\rangle_n$ has at least three non-simple dominant characteristic roots and this collection must include the real dominant root $\rho$ as well as a complex conjugate pair $\lambda$ and $\overline{\lambda}$.

Let $f$ be the monic integer-valued polynomial of the smallest degree with $\rho$ and $\lambda$ as roots. Then, $f$ is non-degenerate and reversible. By Theorem 13, it follows that at most half of the roots of $f$ are dominant if $f$ is neither linear or cubic with two dominant roots. As such, $f$ has degree at least 6, and as each of these roots is non-simple being a Galois conjugate of either $\rho$ or $\lambda$, $\langle u_n\rangle_n$ has order at least 12.

We thus deduce the desired result: positivity and ultimate positivity are decidable for sequences up to order 11. ◀

**Proof of Claim 14.** Suppose that the real positive dominant root $\rho$ of $\langle u_n\rangle_n$ is the only non-simple dominant root of the sequence. If such a phenomenon were to take place then $u_n = A_\rho(n)\rho^n + O(\rho^n)$ where $A_\rho$ is a non-constant polynomial. It is straightforward to deduce whether $\langle u_n\rangle_n$ is (ultimately) positive if and only if $A_\rho(n)$ is (ultimately) positive in this instance. ◀

**Proof of Claim 15.** We will show that claim follows from the following lemma from [1].

▶ **Lemma 16.** *Let $\gamma_1, \ldots, \gamma_k \in \{z \in \mathbb{C} : |z| = 1, z \neq 1\}$ be distinct complex numbers, $\alpha_1, \ldots, \alpha_k$ be in $\mathbb{C} \setminus \{0\}$, and $w_n = \sum_{\ell=1}^{k} \alpha_\ell \gamma_\ell^n$. Then there is a $c < 0$ such that $\mathrm{Re}(w_n) < c$ for infinitely many $n$.*

To prove the claim, let $d$ be the maximum of the degrees of the roots of $\langle u_n\rangle_n$. Note $d \geq 1$ since, by assumption, $\langle u_n\rangle_n$ has a non-real dominant root that is not simple. We consider the normalised sequence $\langle v_n\rangle_n$ with terms given by $v_n = u_n/(\rho^n n^d)$ where $\rho$ is the dominant root of $\langle u_n\rangle_n$. Note it is sufficient to establish that $\langle v_n\rangle_n$ is neither positive not ultimately positive to obtain the desired result.

From analysis of the exponential polynomial of $\langle u_n\rangle_n$, we find

$$v_n = \sum_{\ell=1}^{2k} \frac{A_\ell(n)}{n^d} \frac{\lambda_\ell^n}{\rho^n} + O(n^{-d})$$

where $\lambda_1, \ldots, \lambda_{2k}$ are the non-real dominant roots of $\langle u_n\rangle_n$. From the coefficient sequences $\langle A_\ell(n)/n^d\rangle_n$ in the above sum, we infer that there exist algebraic constants $\alpha_\ell$ such that

$$v_n < r(n) + \sum_{\ell=1}^{2k} \alpha_\ell \frac{\lambda_\ell^n}{\rho^n} =: r(n) + w_n$$

where $r(n) \in O(n^{-1})$ and the real-valued LRS $\langle w_n\rangle_n$ is a simple LRS whose characteristic roots are all non-real and lie on the unit circle. Therefore, $w_n$ fits the hypothesis of Lemma 16, and so for some $c < 0$, and infinitely many $n$, $v_n < r(n) + w_n < r(n) + c$ holds. As $r(n) \in O(n^{-1})$, we have that for infinitely many $n$, $v_n < 0$. Hence $\langle u_n\rangle_n$ is neither positive nor ultimately positive. ◀

# 5 Hard Instances

In this section we discuss obstacles to extending our results for deciding positivity of reversible LRS of higher orders. Specifically, we construct a simple reversible LRS of order 18 and sketch the construction of reversible LRS of order 12 that, to the best of our knowledge, lie outside the known classes for which the Positivity Problem can be decided. In particular, these examples lie beyond the scope of Theorem 4.

We start with simple reversible LRS of order 18. In order to illustrate the technical arguments and guide our construction of a hard instance, it is useful to recall the techniques employed by Ouaknine and Worrell in their proof of Theorem 4 [14]. For the sake of brevity, we shall give only a brief outline here; we direct the interested reader to the full argument given in [14].

## 5.1 Sketch proof of Theorem 4

Let $\langle u_n \rangle_n$ be a simple LRS satisfying the assumptions of Theorem 4. We first normalise $\langle u_n \rangle_n$ and so assume that the dominant roots $\lambda_1, \dots, \lambda_k$ of $\langle u_n \rangle_n$ lie on the unit circle in the complex plane. Then, for each $n \in \mathbb{N}$,

$$u_n = \alpha_1 \lambda_1^n + \cdots + \alpha_k \lambda_k^n + \beta_1 \mu_1^n + \cdots + \beta_{k'} \mu_{k'}^n$$

where $\mu_1, \dots, \mu_{k'}$ are the non-dominant roots of $\langle u_n \rangle_n$ and $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_{k'}$ are algebraic numbers.

We then compute a basis for the multiplicative relations between the dominant roots and consider a maximal subset $\lambda_1, \dots, \lambda_\ell$ whose elements are multiplicatively independent. By Kronecker's Theorem on simultaneous Diophantine approximation (cf. [2, page 53]), $\{(\lambda_1^n, \dots, \lambda_\ell^n) : n \in \mathbb{N}\}$ is a dense subset of the torus $T := \{z \in \mathbb{C} : |z| = 1\}^\ell$, which is compact.

The authors then construct a continuous function $\tau \colon T \to \mathbb{R}$ satisfying $\tau(\lambda_1^n, \dots, \lambda_\ell^n) = \alpha_1 \lambda_1^n + \cdots + \alpha_k \lambda_k^n$ with the following properties. If $\min_T \tau = 0$, the sequence is ultimately positive. That is to say, there is a number $N$ such that $u_n \geq 0$ for all $n \geq N$. If $\min_T \tau < 0$, the sequence is not ultimately positive (and thus also not positive). Finally, if $\min_T \tau > 0$, then the sequence grows quickly, and deciding positivity is relatively straightforward. Hence the critical case occurs when $\min_T \tau = 0$. Moreover, one can determine which of the three cases occur (that is, compute $\min_T \tau$).

In the critical case where $\min_T \tau = 0$, one can sometimes exploit the set of points $Z = \{(z_1, \dots, z_\ell) \in T : \tau(z_1, \dots, z_\ell) = 0\}$ where the minimum is attained. If $(z_1, \dots, z_\ell) \in Z$, then Baker's Theorem on linear forms shows $\lambda_1^n$ cannot get too "close" to $z_1$ for $n$ greater than a computable bound. As such, if $Z$ is finite, then one can decide whether $\langle u_n \rangle_n$ is positive.

Theorem 4 is now proven as follows. If $\langle u_n \rangle_n$ has at most eight dominant characteristic roots and falls into the critical case, then $Z$ is finite. Likewise, if $\langle u_n \rangle_n$ has exactly nine characteristic roots all of which are dominant, then $\langle u_n \rangle_n$ is positive in the critical case as $u_n \geq \min_T \tau = 0$.

The approach described breaks down when there are nine dominant roots since then $Z$ is possibly infinite. Briefly, in this setting the state of the art cannot show that $(\lambda_1^n, \dots, \lambda_\ell^n)$ does not approach this infinite set too "closely". This gives rise to examples of hard LRS for which we cannot currently determine positivity.

## 5.2 Construction

Our hard sequence is constructed from a function $\tau$ that assumes its minimum infinitely often on the torus $T = \{(z_1, z_2) \in \mathbb{C} : |z_1| = |z_2| = 1\}$. To this end, we define $\tau : T \to \mathbb{R}$ by

$$\tau(z_1, z_2) = (az_1 + \overline{a}z_1^{-1} + bz_2 + \overline{b}z_2^{-1})^2$$

for some non-zero $a, b \in \mathbb{C}$ with $|a| \neq |b|$. Then $\min_T \tau$ is equal to 0 and $\tau$ attains its minimum on an infinite subset of $T$. This property prevents the application of Theorem 4.

▶ **Example 17.** We shall construct a simple reversible LRS sequence of order 18. An analysis of the spectral properties of this sequence shows that it lies beyond the current state-of-the-art techniques for deciding positivity. This hard instance is derived from the irreducible polynomial

$$f(X) = X^8 - 3X^7 + 4X^6 - 4X^5 + 11X^4 - 21X^3 + 19X^2 - 7X + 1,$$

which has eight non-real roots $\lambda_1, \ldots, \overline{\lambda_4}$ such that $\lambda_1$ and $\lambda_2$ are dominant, $\lambda_3$ and $\lambda_4$ are both non-dominant, and $1.143 \approx |\lambda_3| > 1 > |\lambda_4|$.

Let $\phi = (1 + \sqrt{5})/2$ denote the golden ratio. Then, with a certain labeling of complex conjugates,

$$\lambda_1\overline{\lambda_1} = \lambda_2\overline{\lambda_2} = \phi^2 \quad \text{and} \quad \lambda_3\lambda_4 = \overline{\lambda_3}\,\overline{\lambda_4} = \phi^{-2},$$

which, due to the number of relations, severely limits the possible Galois automorphisms. In particular, the Galois group has the form of a *wreath product* $D_4 \wr C_2$. Thus a dihedral group $D_4$ acts on $\lambda_1, \overline{\lambda_1}, \lambda_2$, and $\overline{\lambda_2}$ and is generated by the elements (written in cycle notation) $(\lambda_1\ \lambda_2\ \overline{\lambda_1}\ \overline{\lambda_2})$ and $(\lambda_1\ \overline{\lambda_1})$. Another group $D_4$ acts on $\lambda_3, \overline{\lambda_3}, \lambda_4, \overline{\lambda_4}$ and is generated by $(\lambda_3\ \overline{\lambda_3}\ \lambda_4\ \overline{\lambda_4})$ and $(\lambda_3\ \lambda_4)$. Lastly, there is a $C_2$ group acting on these two sets of four roots generated by the permutation $(\lambda_1\ \lambda_3)(\overline{\lambda_1}\ \lambda_4)(\lambda_2\ \overline{\lambda_3})(\overline{\lambda_2}\ \overline{\lambda_4})$.

The explicit sequence is now defined as follows:

$$u_n = \frac{1}{\sqrt{5}}\Big((1+\lambda_1)\lambda_1^n + (1+\overline{\lambda_1})\overline{\lambda_1}^n + (1+\lambda_2)\lambda_2^n + (1+\overline{\lambda_2})\overline{\lambda_2}^n\Big)^2 - \frac{1}{\sqrt{5}}\Big((1+\lambda_3)\lambda_3^n + (1+\overline{\lambda_3})\overline{\lambda_3}^n + (1+\lambda_4)\lambda_4^n + (1+\overline{\lambda_4})\overline{\lambda_4}^n\Big)^2.$$

By the action of the Galois group, it can be seen that each term $u_n$ is rational and further that $\langle u_n \rangle_n$ is simple, reversible, and has exactly order 18. The initial values $u_0, \ldots, u_{17}$ of $\langle u_n \rangle_n$ are

$$-11, -8, 0, 240, 704, -20, 192, 5508, 46305, 2625, 13425, 73117, 2469800, 536000, 554151, 77287, 108792361, 66461616.$$

The simple LRS $\langle u_n \rangle_n$ satisfies the relation

$$\begin{aligned} u_{n+18} &= u_{n+17} - 10u_{n+16} + 6u_{n+15} + 43u_{n+14} - 93u_{n+13} + 672u_{n+12} - 596u_{n+11} \\ &\quad + 120u_{n+10} + 3972u_{n+9} - 15345u_{n+8} + 29654u_{n+7} - 36108u_{n+6} + 23847u_{n+5} \\ &\quad - 9572u_{n+4} + 2361u_{n+3} - 325u_{n+2} + 26u_{n+1} - u_n. \end{aligned}$$

Observe that $u_0, u_1$, and $u_5$ are negative, but up to $n = 10^5$ these are the only negative terms. Thus, the question is to prove that $u_n \geq 0$ for all $n \geq 6$. We reiterate that, as far as the authors are aware, there are no known techniques in the state of the art that can tackle this question.

It remains to show that the torus $T$ associated with $\langle u_n \rangle_n$ has the "squaring form" described earlier and that $\langle u_n \rangle_n$ is non-degenerate. To start, $u_n$ is positive if and only if $\frac{u_n}{\phi^{2n}}$ and $|1+\lambda_1|$ and $|1+\lambda_2|$, and $\lambda_1/\phi$ and $\lambda_2/\phi$ both lie on the unit circle. Thus, for $a = 1+\lambda_1, b = \lambda_2$ and some $r < 1$, we have that

$$\begin{aligned}\frac{u_n}{\phi^{2n}} &= \frac{1}{\phi^{2n}}\Big((1+\lambda_1)\lambda_1^n + (1+\overline{\lambda_1})\overline{\lambda_1}^n + (1+\lambda_2)\lambda_2^n + (1+\overline{\lambda_2})\overline{\lambda_2}^n\Big)^2 + O(r^n)\\ &= \left(a\left(\frac{\lambda_1}{\phi}\right)^n + \overline{a}\left(\frac{\lambda_1}{\phi}\right)^{-n} + b\left(\frac{\lambda_2}{\phi}\right)^n + \overline{b}\left(\frac{\lambda_2}{\phi}\right)^{-n}\right)^2 + O(r^n)\end{aligned}$$

is close to the squaring method form discussed at the start of this subsection. In fact, we have that $u_n/\phi^{2n} = \tau((\lambda_1/\phi)^n, (\lambda_2/\phi)^n) + O(r^n)$. Here, the term $O(r^n)$ decreases exponentially fast and determines how closely the square should approach zero to contradict positivity. To use this squaring form, we need to show that the points to which we restrict $\tau$ are dense on the torus $T$. That, we need to show that $\lambda_1/\phi$ and $\lambda_2/\phi$ are multiplicatively independent. This lack of multiplicative relations also immediately implies that $\langle u_n \rangle_n$ is non-degenerate. We complete the spectral analysis of sequence $\langle u_n \rangle_n$ with the following proposition.

▶ **Proposition 18.** *We have that $\lambda_1/|\lambda_1|$ and $\lambda_2/|\lambda_2|$ are multiplicatively independent.*

**Proof.** Note that $|\lambda_1| = |\lambda_2| = \phi$ as $\lambda_1\overline{\lambda_1} = \lambda_2\overline{\lambda_2} = \phi^2$. By the earlier described Galois action, we see that there are Galois automorphisms $\sigma$ and $\tau$ such that $\sigma(\lambda_1) = \tau(\lambda_1) = \lambda_3$, $\sigma(\lambda_2) = \lambda_4$ and $\tau(\lambda_2) = \overline{\lambda_3}$. Further, by this choice, $\sigma(\phi) = \tau(\phi) = -\phi^{-1}$.

Assume, for a contradiction, that $\lambda_1/|\lambda_1|$ and $\lambda_2/|\lambda_2|$ are multiplicatively dependent; that is to say, there are $a, b \in \mathbb{Z}$, not both 0, such that $(\lambda_1/|\lambda_1|)^a (\lambda_2/|\lambda_2|)^b = 1$. Applying $\sigma$ to this identity gives that

$$1 = \left(\frac{\lambda_3}{-\phi^{-1}}\right)^a \left(\frac{\lambda_4}{-\phi^{-1}}\right)^b = \zeta\left(\frac{|\lambda_3\lambda_4|}{\phi^{-2}}\right)^a \left(\frac{\lambda_4}{-\phi^{-1}}\right)^{b-a} = \zeta\left(\frac{\lambda_4}{-\phi^{-1}}\right)^{b-a}$$

for some $\zeta$ on the unit circle. As $|\lambda_4/-\phi^{-1}| \neq 1$, we conclude that $a = b$.

Applying $\tau$ to $(\lambda_1/|\lambda_1|)^a (\lambda_2/|\lambda_2|)^b = 1$ gives that

$$1 = \left(\frac{\lambda_3}{-\phi^{-1}}\right)^a \left(\frac{\overline{\lambda_3}}{-\phi^{-1}}\right)^b = \zeta'\left(\frac{|\lambda_3|}{|\overline{\lambda_3}|}\right)^a \left(\frac{\overline{\lambda_3}}{-\phi^{-1}}\right)^{b+a} = \zeta'\left(\frac{\overline{\lambda_3}}{-\phi^{-1}}\right)^{b+a}$$

for some $\zeta'$ on the unit circle. Since $|\overline{\lambda_3}/-\phi^{-1}| \neq 1$, this implies that $a = -b$. Together with $a = b$, we deduce that $a = b = 0$. Thus $\lambda_1/|\lambda_1|$ and $\lambda_2/|\lambda_2|$ are multiplicatively independent. ◀

## 5.3 A non-simple hard example of order 12

In this subsection, we briefly discuss reversible LRS of order 12 for which we cannot decide positivity nor ultimate positivity. As such examples are much easier to construct and are closely related to the extensively discussed examples in [13], we will refrain from a lengthy discussion. Recall from the proof of Theorem 1 that for a non-simple hard example of (ultimate) positivity one requires three simple dominant roots of which one is real and positive. One choice, which is closely related to the construction in example 4.5 of in [11], is to take

$$\rho = \sqrt{2}+1 \quad \text{and} \quad \lambda = \frac{1+\sqrt{1-4\rho^2}}{2}.$$

Then we have that $\rho$ and $\lambda$ are units of equal modulus, $\rho$ has one Galois conjugate $\tilde{\rho}$ which has smaller modulus, and $\lambda$ has three Galois conjugates: its complex conjugate and two real numbers $\lambda_3$ and $\lambda_4$ of smaller modulus. Lastly, let $q \in \mathbb{Q}_{>0}$. Then we construct the non-simple, reversible rational-valued LRS $\langle u_n \rangle_n$ as follows:

$$u_n^q = (n+\rho)\rho^n + (n+\tilde{\rho})\tilde{\rho}^n + q(n+\lambda)\lambda^n + q(n+\overline{\lambda})\overline{\lambda}^n + q(n+\lambda_3)\lambda_3^n + q(n+\lambda_4)\lambda_4^n.$$

For small $q$, $\langle u_n^q \rangle_n$ is positive and ultimate positive sufficiently large $q$, $\langle u_n^q \rangle_n$ will not be positive nor ultimate positive. However, we do not know how to compute on which side of the two divides an arbitrary $q$ falls. As such, for LRS like $\langle u_n^q \rangle_n$, we cannot decide positivity or ultimate positivity. Similarly, using the construction in Section 4.2 of [11], many more examples can be constructed. For a real quadratic algebraic unit $\rho > 1$, one can find a non-real algebraic unit $\lambda$ of equal modulus such that $\lambda$ has a minimum polynomial of degree 4. Then one can define an LRS like $\langle u_n^q \rangle_n$ for which the current methods are unable to settle positivity and ultimate positivity.

## References


1. Mark Braverman. Termination of integer linear programs. In *International conference on computer aided verification*, pages 372–385. Springer, 2006.
2. J. W. S. Cassels. *An introduction to Diophantine approximation.* Cambridge Tracts in Mathematics and Mathematical Physics, No. 45. Cambridge University Press, New York, 1957.
3. Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin, 1993.
4. The SageMath Developers. *sagemath/sage: 9.7*, 2022. `https://www.sagemath.org`.
5. A. Dubickas and C. J. Smyth. On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles. *Proc. Edinb. Math. Soc. (2)*, 44(1):1–17, 2001. doi:10.1017/S001309159900098X.
6. Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs.* Amer. Math. Soc., Providence, RI, 2003.
7. Ronald Ferguson. Irreducible polynomials with many roots of equal modulus. *Acta Arith.*, 78(3):221–225, 1997. doi:10.4064/aa-78-3-221-225.
8. Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki. Skolem's problem–on the border between decidability and undecidability. Technical report, Turku Centre for Computer Science, 2005.
9. George Kenison. On the Skolem Problem for Reversible Sequences. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 61:1–61:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2022.61.
10. L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1857(53):173–175, jan 1857. doi:10.1515/crll.1857.53.173.
11. Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the Skolem Problem and the Skolem Conjecture. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '22, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3531130.3533328.
12. Maurice Mignotte, Tarlok Shorey, and Robert Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die Reine und Angewandte Mathematik*, pages 63–76, 1984.

13 Joël Ouaknine and James Worrell. Decision problems for linear recurrence sequences. In *Reachability problems*, volume 7550 of *Lecture Notes in Computer Science*, pages 21–28. Springer, Heidelberg, 2012.

14 Joël Ouaknine and James Worrell. On the Positivity Problem for Simple Linear Recurrence sequences,. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, pages 318–329, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

15 Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, volume 8573 of *Lecture Notes in Computer Science*, pages 330–341. Springer, 2014. doi:10.1007/978-3-662-43951-7_28.

16 Joël Ouaknine and James Worrell. On linear recurrence sequences and loop termination. *ACM SIGLOG News*, 2(2):4–13, April 2015.

17 Joël Ouaknine and James Worrell. *Positivity Problems for Low-Order Linear Recurrence Sequences*, pages 366–379. 2014. URL: https://epubs.siam.org/doi/abs/10.1137/1.9781611973402.27, doi:10.1137/1.9781611973402.27.

18 Alfred Pringsheim. Ueber Functionen, welche in gewissen Punkten endliche Differentialquotienten jeder endlichen Ordnung, aber keine Taylor'sche Reihenentwickelung besitzen. *Mathematische Annalen*, 44(1):41–56, 1894.

19 J.J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 2012.

20 C. Smyth. Conjugate algebraic numbers on conics. *Acta Arithmetica*, 40(4):333–346, 1982.

21 I. Stewart and D. Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.

22 Edward Charles Titchmarsh. *The theory of functions*. Oxford University Press, 2nd edition, 1939.

23 Nikolai Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38(2):609–615, Aug 1985.

24 Giulio Vivanti. Sulle serie di potenze. *Annali di Matematica Pura ed Applicata (1867-1897)*, 21(1):193–194, 1893.