On the Skolem Problem for Reversible Sequences

George Kenison ✉

Institute of Logic and Computation, TU Wien, Vienna, Austria

---- **Abstract** ----

Given an integer linear recurrence sequence $\langle X_n \rangle_{n=0}^{\infty}$, the Skolem Problem asks to determine whether there is an $n \in \mathbb{N}_0$ such that $X_n = 0$. Recent work by Lipton, Luca, Nieuwveld, Ouaknine, Purser, and Worrell proved that the Skolem Problem is decidable for a class of reversible sequences of order at most seven. Here we give an alternative proof of their result. Our novel approach employs a powerful result for Galois conjugates that lie on two concentric circles due to Dubickas and Smyth.

1 Introduction

The Skolem Problem

An integer-valued *linear recurrence sequence* $\langle X_n \rangle_{n=0}^{\infty}$ satisfies a relation of the form

$$X_{n+d} = a_{d-1}X_{n+d-1} + \cdots + a_1 X_{n+1} + a_0 X_n \tag{1}$$

for each $n \in \mathbb{N}_0$. Without loss of generality, we shall assume that each of the coefficients $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}$ and additionally that $a_0 \neq 0$. We call d the *length* of the recurrence relation and the *order* of $\langle X_n \rangle_n$ is the length of the shortest relation satisfied by $\langle X_n \rangle_n$. 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 such a sequence, the *Skolem Problem* [8, 11] asks to determine whether there exists an $n \in \mathbb{N}$ such $X_n = 0$. The Skolem Problem is well-motivated with connections to research topics such as program verification [27]. 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

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

Let $\langle X_n \rangle_n$ be the linear recurrence sequence with terms given by $X_n = \underline{b}^{\top} A^n \underline{w}$. It is clear that loop P terminates if and only if there exists an $n \in \mathbb{N}_0$ such that $X_n = 0$.

Motivation

A recent resurgence of interest in the Skolem Problem (and related problems) has lead to the publication of a number of papers that consider restricted variants. The resulting specialised decision procedures generally fall into two categories: those that consider an infinite subset of the natural numbers [14, 20] or those that restrict the class of linear recurrence sequences. Our motivation is the latter type of specialisation and, in particular, a recent paper by Lipton et al. [19] that establishes the following theorem.

47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022).
Editors: Stefan Szeider, Robert Ganian, and Alexandra Silva; Article No. 61; pp. 61:1–61:15

Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

▶ **Theorem 1.** *The Skolem Problem is decidable for the class of reversible integer linear recurrences of order at most seven.*

An integer linear recurrence sequence $\langle X_n \rangle_{n=0}^{\infty}$ is *reversible* if it satisfies a recurrence relation of the form (1) such that $a_0 = \pm 1$. As observed in Lipton et al. [19], given an integer linear recurrence sequence $\langle X_n \rangle_{n=0}^{\infty}$, the unique bi-infinite extension $\langle X_n \rangle_{n=-\infty}^{n=\infty}$ has integral terms if and only if $\langle X_n \rangle_{n=0}^{\infty}$ is reversible (this claim follows from a classical observation for Fatou rings [9]). We can also characterise the subclass of while loops (as in (2)) naturally associated with reversible sequences: the update matrix A with characteristic polynomial f is *unimodular*; that is, A has integer entries and $\det(A) = -f(0) = \pm 1$. If A is unimodular, then A^{-1} also has integer entries. Thus, again, $\langle X_n \rangle_{n=-\infty}^{n=\infty}$ with each $X_n = \underline{b}^\top A^n \underline{w}$ (as above) is integer-valued.

Unimodular matrices appear elsewhere in the dynamical systems literature. Some classes lead to prototypical invertible maps with hyperbolic and ergodic properties; specifically, classes of *linear toral automorphisms* $T_A \colon \mathbb{R}^d \to \mathbb{R}^d$ given by $T_A(\underline{x}) = A\underline{x}$ [13].

A famous example of a reversible sequence is the Fibonacci sequence, which is defined by the initial values $X_0 = 0$, $X_1 = 1$ and for each $n \in \mathbb{N}_0$, $X_{n+2} = X_{n+1} + X_n$. The Fibonacci sequence can be uniquely extended to a bi-infinite sequence of integer values $\langle \ldots, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, \ldots \rangle$.

In the sequel, we call the restricted variant of the Skolem Problem for reversible sequences the *Reversible Skolem Problem.*

Background

Let us assess the current state of play with regards to the decidability of the Skolem Problem. A classical result due to Skolem [31] (which was later generalised by Mahler [22, 23], and Lech [18]) states that $\{n \in \mathbb{N} : X_n = 0\}$ is the union of a finite set together with a finite number of (infinite) arithmetic progressions. The phenomenon that causes these vanishing arithmetic progressions is termed *degeneracy*. A sequence is *degenerate* when one of the ratios of two distinct characteristic roots of the sequence is a root of unity. These arithmetic progressions can be determined algorithmically and so, from the viewpoint of verification, to decide the Skolem Problem it suffices to consider *non-degenerate* recurrence sequences – those sequences that have only finitely many zeros. Indeed, this is where the difficulty lies: there is no known general method to compute this finite set. We refer the interested reader to Corollary 1.20 and Chapter 2 in [8] for further details. In summary, all known proofs of the Skolem–Mahler–Lech Theorem (as it is now known) are non-constructive and so the decidability of the Skolem Problem remains open.

Limited progress has been made on the decidability of the Skolem Problem when one considers linear recurrence sequences of low order. Groundbreaking work by Mignotte, Shorey, and Tijdeman [24], and, independently, Vereshchagin [35] establish the following.

▶ **Theorem 2.** *The Skolem Problem is decidable for the class of non-degenerate linear recurrences with at most three simple characteristic roots that are maximal in modulus.*

As a consequence, the Skolem Problem is decidable for linear recurrences of order at most four. The aforementioned papers employ techniques from p-adic analysis and algebraic number theory and, in addition, Baker's theorem for linear forms in logarithms of algebraic numbers. Unfortunately the route taken via Baker's Theorem does not appear to extend easily to recurrences of higher order.

A class of recurrence sequences of order five that the state of the art cannot handle impedes further progress on the decidability of the Skolem Problem [25]. The minimal polynomial for each member of this class has four distinct roots $\alpha, \overline{\alpha}, \beta, \overline{\beta} \in \mathbb{C}$ (two pairs

of complex-conjugate roots) such that $|\alpha| = |\beta|$, and a fifth real root γ of strictly smaller modulus. Hence the terms of such a sequence $\langle X_n \rangle_n$ are given by an exponential polynomial of the form $X_n = a(\alpha^n + \overline{\alpha}^n) + b(\beta + \overline{\beta}^n) + c\gamma^n$. Here $a, b, c \in \mathbb{R}$ are algebraic numbers and, as far as we are aware, there is no known general procedure to determine $\{n \in \mathbb{N} : X_n = 0\}$ when $|a| \neq |b|$.

Complexity

In [3], Blondel and Portier proved that the Skolem Problem is NP-hard. As a brief aside, let us consider the complexity of the reversible variant of the Skolem Problem. One of the questions considered by S. Akshay et al. [1] is the complexity of the Skolem Problem for the restricted class of linear recurrence sequences whose characteristic roots are all roots of unity (the so-called *Cyclotomic Skolem Problem*). Those authors showed, by a reduction from the Subset-Sum Problem, that the Cyclotomic Skolem Problem is NP-hard. Because the characteristic polynomial associated with each element in this restricted class is given by a product of cyclotomic polynomials, it follows that each instance of the Cyclotomic Skolem Problem is an instance of the Reversible Skolem Problem. Thus the Reversible Skolem Problem is also NP-hard.

Contributions

The main contribution in this note is an alternative proof of Theorem 1. By comparison to the extensive case analysis employed in [19], we use results in number theory for Galois conjugates that obey polynomial identities. In particular, we make repeated use of a result due to Dubickas and Smyth [7] for algebraic integers that lie alongside all their Galois conjugates on two (but not one) concentric circles centred at the origin.

For context, Dubickas and Smyth's result is part of a large corpus of research on algebraic numbers whose conjugates lie on a conic or a union of conics. Let α be an algebraic number with Galois conjugates $\alpha = \alpha_1, \ldots, \alpha_d$. We call the set $S(\alpha) := \{\alpha_1, \ldots, \alpha_d\}$ the *conjugate set* of α. When $S(\alpha)$ is a subset of the unit circle, a result of Kronecker's (a weaker version of Theorem 5) proves that α is a root of unity. Number theorists have long-studied classes of algebraic integers where one or more of the conjugates leaves the circle; for example, a real algebraic integer α is a *Salem number* if $\alpha > 1$, $\alpha^{-1} \in S(\alpha)$, and the remaining conjugates all lie on the unit circle, i.e., $S(\alpha) = \{\alpha^{\pm 1}, e^{\pm i\theta_2}, \ldots, e^{\pm i\theta_d}\}$.

With regards to the Reversible Skolem Problem at order eight, we exhibit a family of recurrence sequences that, as far as we know, are not amenable to standard techniques and so decidability is very much open. The authors of [19] also demonstrated a concrete family of examples in this regard. It is interesting to note that the techniques used and families obtained are very different. Each member of our family is an octic palindromic polynomial (the same is not true for the family of examples in [19]). The coefficients of a *palindromic* polynomial form a palindromic string of integers. For example, two palindromes that are also family members are $x^8 + x^7 - x^6 + x^5 + 5x^4 + x^3 - x^2 + x + 1$ and $x^8 + x^7 - 3x^6 + x^5 + 9x^4 + x^3 - 3x^2 + x + 1$. Using any modern computer algebra system, it is easy to verify that the roots of each polynomial satisfy the following. First, the roots lie on two (but not one) concentric circles centred at the origin. Second, no ratio of any two of its roots is a root of unity. The calculations involved in preparing these (and later) examples were performed in PARI/GP [34]. In Subsection 4.2, we study the Galois groups of irreducible palindromic octics in the aforementioned family as a further investigation into the symmetries between their roots.

In Subsections 5.1 and 5.2, we prove new decidability results on restricted variants of the Positivity and Skolem Problems using Dubickas and Smyth's theorem and make suggestions for further work in these directions. For brevity, we refer to the Positivity Problem for the class of simple reversible integer linear recurrences as the *Simple Reversible Positivity Problem*. Here a linear recurrence is *simple* if the associated characteristic polynomial has no repeated roots. We have the following results:

▶ **Corollary 3.** *The Simple Reversible Positivity Problem is decidable for integer-valued linear recurrences of order at most ten.*

▶ **Corollary 4.** *The Skolem Problem is decidable for rational-valued linear recurrences that satisfy a relation of the form $X_{n+5} = a_4 X_{n+4} + a_3 X_{n+3} + a_2 X_{n+2} + a_1 X_{n+1} \pm X_n$ with $a_1, a_2, a_3, a_4 \in \mathbb{Q}$.*

Structure

The remainder of this paper is structured as follows. In the next section we review necessary preliminary material. In Section 3, we give a new and novel proof of Theorem 1. In Section 4, we construct a family of octic palindromes that shows the current state of the art cannot settle decidability of the Reversible Skolem Problem at order eight and then discuss the Galois groups associated with the irreducible members of this family. In the final section, Section 5, we discuss directions and motivate this discussion with the proofs of Corollaries 3 and 4.

2 Preliminaries

2.1 Recurrence Sequences

A sequence $\langle X_n \rangle_{n=0}^{\infty}$ of integers satisfying a recurrence relation of the form (1) with fixed integer constants $a_0, a_1, \ldots, a_{d-1}$ such that $a_0 \neq 0$ is a *linear recurrence sequence*. The sequence $\langle X_n \rangle_n$ is then wholly determined by the recurrence relation and the initial values $X_0, X_1, \ldots, X_{d-1}$. 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). From our earlier definition, it is clear that $\langle X_n \rangle_n$ is reversible if and only if $f(0) = \pm 1$. There is a recurrence relation of minimal length associated to $\langle X_n \rangle_n$ and we call the characteristic polynomial of this minimal length relation the *minimal polynomial* of $\langle X_n \rangle_n$. The *order* of a linear recurrence sequence is the degree of its minimal polynomial.

Let f be the minimal polynomial of a linear recurrence sequence $\langle X_n \rangle_n$ and K the splitting field of f. The polynomial f factorises as a product of powers of distinct linear factors like so $f(x) = \prod_{\ell=1}^{m} (x - \lambda_\ell)^{n_\ell}$. The constants $\lambda_1, \lambda_2, \ldots, \lambda_m \in K$ are the *characteristic roots* of $\langle X_n \rangle_n$ with multiplicities $n_1, n_2, \ldots, n_m$. One can realise the terms of a linear recurrence sequence as an *exponential polynomial* $X_n = \sum_{\ell=1}^{m} p_\ell(n) \lambda_\ell^n$ where the λ_ℓ are the aforementioned characteristic roots of $\langle X_n \rangle_n$ and the polynomial coefficients $p_\ell \in K[x]$ are determined by the initial values. We say a characteristic root of $\langle X_n \rangle_n$ is *dominant* if in the set of characteristic roots of $\langle X_n \rangle_n$ it is maximal in modulus. Thus, by Theorem 2, the Skolem Problem is decidable for the class of non-degenerate linear recurrence sequences with at most three dominant characteristic roots [24, 35].

2.2 Number Theory

We shall assume some familiarity with Galois theory and the theory of number fields. The necessary background material can be found in a number of standard textbooks [5, 33].

Recall the following theorem due to Kronecker [16].

▶ **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 f is a product of cyclotomic polynomials. Therefore all the roots of f are roots of unity.*

Thus, if $f \in \mathbb{Z}[x]$ is the characteristic polynomial of a reversible linear recurrence sequence 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. It follows that the associated recurrence sequence is either order one (and is thus constant) or degenerate. In either case the Skolem Problem is decidable. 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.

In the sequel, our construction of an infinite family of octics uses the following corollary of Vieta's formulae.

▶ **Lemma 6.** *Suppose that $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial such that $f(x) = \prod_{i=1}^{d}(x - \lambda_i)$. Let $f_n(x) := \prod_{i=1}^{d}(x - \lambda_i^n)$. Then $f_n \in \mathbb{Z}[x]$ for each $n \in \mathbb{N}$.*

Proof. The coefficients of the polynomial f_n are determined by symmetric polynomials in d variables. By the fundamental theorem of symmetric polynomials, each symmetric polynomial is given by a $\mathbb{Z}$-linear combination of elementary symmetric polynomials. The result follows as a straightforward application of Vieta's formulae and the evaluation of elementary symmetric polynomials over conjugate algebraic integers. ◄

The roots of an irreducible polynomial are necessarily Galois conjugates. We use the term *conjugate ratios* for the ratios between two distinct roots of an irreducible polynomial. A non-zero algebraic number α is *reciprocal* if α is conjugate to α^{-1}. Let τ be a Salem number whose minimal polynomial has degree $2d$ or a reciprocal quadratic. In the former case, $S(\tau) = \{\tau^{\pm 1}, \tau_2^{\pm 1}, \ldots, \tau_d^{\pm 1}\}$ and in the latter, $S(\tau) = \{\tau^{\pm 1}\}$. An algebraic number ψ is a *Salem half-norm* if $\psi = \tau^{\varepsilon_1}\tau_2^{\varepsilon_2}\cdots\tau_d^{\varepsilon_d}$ for some such τ and $\varepsilon_j = \pm 1$ for each $j \in \{1, \ldots, d\}$. The properties of Salem half-norms are discussed further in [7].

In the ring of algebraic integers of a given number field K, $\gamma \in K$ is a *unit* (sometimes an *algebraic unit*) if it has a multiplicative inverse δ so that $\gamma\delta = \delta\gamma = 1$. Let $\alpha \in K$ be an algebraic integer. Then the constant coefficient of the minimal polynomial $f \in \mathbb{Z}[x]$ of α is equal to ± 1 if and only if α is a unit. This observation follows easily from norm considerations and the fact that the constant coefficient of f (up to sign) is given by the product of α and its Galois conjugates. Since the characteristic polynomial $f \in \mathbb{Z}[x]$ of a reversible sequence $\langle X_n \rangle_n$ has constant coefficient ± 1, we deduce that each of the characteristic roots of $\langle X_n \rangle_n$ is a unit. In the sequel we make frequent use of the following simple observation.

▶ **Lemma 7.** *If α is an algebraic unit that lies on the circle $|z| = R$ with $R > 1$, then a conjugate of α lies in the interior of the unit disk.*

Key to the proofs in the sequel is a powerful result due to Dubickas and Smyth [7] concerning polynomial identities between the roots of irreducible polynomials. Theorem 8 gives necessary conditions for a unit in the algebraic integers and all its Galois conjugates to lie on two (but not one) concentric circles centred at the origin [7]. In fact, Dubickas and Smyth prove a far more general result [7, Theorem 2.1], but we need only the specialised version for units below.

▶ **Theorem 8.** *Suppose that α is a unit in the algebraic integers of degree d lying, with all its Galois conjugates, on two circles $|z| = r$ and $|z| = R$, but not just one. Without loss of generality assume that at most half of the conjugates lie on $|z| = r$. Then, one of the following holds:*

1. *$d = 3m$, $R = r^{-1/2}$ such that there are $d/3$ conjugates of α on $|z| = r$, and the remaining $2d/3$ lie on $|z| = r^{-1/2}$. Assume, without loss of generality, $|\alpha| = r$. Then, in addition, there exists an $n \in \mathbb{N}$ such that α^n is a real, but non-totally real, cubic unit.*

2. *$d = 2m$, $R = r^{-1}$ where $R > 1$ without loss of generality, and $d/2$ Galois conjugates of α lie on each circle. Further, there exists an $n \in \mathbb{N}$ such that $\alpha^n =: \psi$ is a Salem half-norm defined by a Salem number or a reciprocal quadratic.*

Let us explain the term *totally real* in the last theorem. An algebraic number α is *totally real* if α and all its Galois conjugates are real. A number field K is *totally real* if $K = \mathbb{Q}[\alpha]$ such that α is totally real.

From this point to the end of the subsection, the terminology and results we recall are used only in Section 4 (and so are not required for the proof of Theorem 1).

A field is *Kroneckerian* if it is either a totally real algebraic number field or a totally imaginary quadratic extension of a totally real field. In the sequel, we make use of the following observation about complex conjugation lying in the centre of the Galois group of a Kroneckerian field (see [30, Chapter 6]).

▶ **Corollary 9.** *A number field K is Kroneckerian if and only if for every $\alpha \in K$ one has $\overline{\alpha} \in K$ and for every embedding σ of K into $\mathbb{C}$ one has $\overline{\alpha^\sigma} = \overline{\alpha}^\sigma$.*

A unit is *unimodular* if it lies on the unit circle in $\mathbb{C}$. In [21], MacCluer and Parry prove that a normal imaginary field contains unimodular units other than roots of unity exactly when its real subfield is not normal over $\mathbb{Q}$. Daileda [6] generalises this result and provides the following classification of the number fields that have unimodular units that are not roots of unity. Recall that a number field K is a *CM-field* if K is a totally complex quadratic extension of a totally real field.

▶ **Theorem 10.** *Let K be a number field closed under complex conjugation. Then K contains unimodular units that are not roots of unity if and only if K is imaginary and not a CM-field.*

2.3 Group Theory

In the sequel we employ the notation S_n for the symmetric group on n elements, A_n for the alternating group on n elements, D_n for the Dihedral group of order $2n$, C_n for the cyclic group on n elements, and K_4 for the Klein 4-group.

The action of G on a set X is *transitive* if for every pair $x, y \in X$ there is a $g \in G$ such that $gx = y$; that is to say, there is a single group orbit. We note here (and again later) that S_4, A_4, D_4, C_4, and K_4 are the transitive subgroups of S_4.

3 Proof of Theorem 1

We briefly outline our route to proving Theorem 1. We claim that if $\langle X_n \rangle_n$ is a non-degenerate reversible integer recurrence sequence of order at most seven, then $\langle X_n \rangle_n$ has at most three dominant characteristic roots. The decidability of the Skolem Problem for such instances then follows from Theorem 2. The above claim follows as a corollary of the next theorem.

▶ **Theorem 11.** *No monic polynomial $f \in \mathbb{Z}[x]$ with constant coefficient ± 1 of degree at most seven satisfies the following two properties:*

(H1) *f has at least four distinct dominant roots; and*

(H2) *no quotient of two distinct roots of f is a root of unity.*

Thus all that remains is to prove Theorem 11. This result is an immediate consequence of the sequence of Propositions 12, 14, and 15 below. In each of the proofs of these propositions we play a similar game: we assume, for a contradiction, that there exists a polynomial $f \in \mathbb{Z}[x]$ (of degree five, six, or seven respectively) that satisfies hypotheses H1 and H2. We show that such a candidate is necessarily irreducible. We then employ Theorem 8 to derive a contradiction: such a candidate cannot satisfy both H1 and H2 and, at the same time, satisfy the restrictive root identities prescribed by Theorem 8.

For the avoidance of doubt, this route to Theorem 1 is similar to that carved out by [19]. The contribution of this paper is the novel application of Theorem 8. Indeed, our assumption, that each of the characteristic roots of a recurrence in our class of non-degenerate reversible sequences is a unit, leads to (rather startling) restrictive polynomial relations between Galois conjugates.

We begin our sequence of propositions.

▶ **Proposition 12.** *No monic polynomial $f \in \mathbb{Z}[x]$ of degree at most five with constant term ± 1 satisfies hypotheses H1 and H2.*

Proof. Assume, for a contradiction, that such an f of degree $d \leq 5$ exists. By Theorem 5, the dominant roots lie on the circle $|z| = R$ for some $R > 1$ for otherwise the roots of f are necessarily all roots of unity, which is not permitted under hypothesis H2. Each of the dominant roots of f is a unit in the algebraic integers and so, by Lemma 7, has a Galois conjugate in the interior of the unit disk. In order that f satisfies hypothesis H1, we conclude that f has four simple dominant roots and a single non-dominant root. Since f has degree $d = 5$ and $f(0) = \pm 1$, all the dominant roots of f are (Galois) conjugate to the single non-dominant root, f is irreducible.

Let α be a root of f. Then α is an algebraic integer of degree 5, a unit, and lies with all its Galois conjugates on two circles. We apply Theorem 8 to the quintic f and find that 5 is either even, or a multiple of 3, a contradiction. ◀

▶ **Remark 13.** The application of Theorem 8 in the proof of Proposition 12 is excessive (even if the derived contradiction is rather satisfying). By comparison, the approach in Lipton et al. [19] is direct. We reproduce the final part of those authors' proof below as it gives a gentle introduction to some of the techniques we apply in Proposition 14 and Proposition 15.

Proof of Proposition 12 (cf. [19]). Let $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ be the four dominant roots of f and ρ the non-dominant root of f. Since f is irreducible, the Galois group G of f acts transitively on the roots of f. Thus there exists a $\sigma \in G$ such that $\sigma(\alpha) = \rho$. The element σ must preserve the equality $\alpha\overline{\alpha} = \beta\overline{\beta}$ and so we have $\rho\sigma(\overline{\alpha}) = \sigma(\beta)\sigma(\overline{\beta})$. We derive a contradiction: $|\rho||\sigma(\overline{\alpha})| \neq |\sigma(\beta)||\sigma(\overline{\beta})|$ since the two roots $\sigma(\beta)$ and $\sigma(\overline{\beta})$ on the right-hand side are necessarily dominant. ◀

▶ **Proposition 14.** *No monic polynomial $f \in \mathbb{Z}[x]$ of degree six with constant term ± 1 satisfies hypotheses H1 and H2.*

Proof. Assume, for a contradiction, that such an f exists. As in the proof of Proposition 12, f has at least four simple dominant roots $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ that lie on a circle $\{z \in \mathbb{C} : |z| = R\}$ for some $R > 1$ as complex-conjugate pairs. We note that the group G of automorphisms of

the splitting field of f must preserve the equality $\alpha\overline{\alpha} = \beta\overline{\beta}$. Because α is a unit on $|z| = R$, by Lemma 7 there is both a root γ of f that lies in the unit disk and a permutation $\sigma \in G$ such that $\sigma(\alpha) = \gamma$. Now consider $\sigma(\alpha)\sigma(\overline{\alpha}) = \sigma(\beta)\sigma(\overline{\beta})$. It is straightforward to elicit a contradiction that breaks this equality if either $\sigma(\overline{\alpha})$ is non-dominant, or both $\sigma(\beta)$ and $\sigma(\overline{\beta})$ are dominant. Thus we can assume that f has two non-dominant roots and further that they are of equal modulus. Clearly these two roots $\gamma, \overline{\gamma}$ are a complex-conjugate pair by H2. Combining these observations of the roots of f, we quickly deduce that f is necessarily irreducible.

Because the roots of the irreducible polynomial $f \in \mathbb{Z}[x]$ lie on two concentric circles, we can apply Theorem 8. Thus there is a non-dominant root, γ say, and $m \in \mathbb{N}$ such that γ^m is a real cubic unit. It follows that $\gamma^m/\overline{\gamma}^m = 1$ and so one of the conjugate ratios of f is a root of unity, which contradicts hypothesis H2.   ◀

▶ **Proposition 15.** *No monic polynomial $f \in \mathbb{Z}[x]$ of degree seven with constant term ± 1 satisfies hypotheses H1 and H2.*

Proof. Assume, for a contradiction, that such an f exists. As in the proof of Proposition 12, f has at least four simple dominant roots $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ that lie on a circle $\{z \in \mathbb{C} : |z| = R\}$ for some $R > 1$ as complex-conjugate pairs. Mutatis mutandis, one can use the methods in the proof of Proposition 14 to make the following two deductions. First, f is irreducible. Second, f has precisely one real root δ and another complex-conjugate pair of roots $\gamma, \overline{\gamma}$. Additionally, we have that $\delta, \gamma, \overline{\gamma}$ are all non-dominant roots of f such that $|\gamma| \neq |\delta|$. We note that if one supposes, for a contradiction, that the septic polynomial f has $|\gamma| = |\delta|$ or $|\alpha| = |\delta|$, then, by Theorem 8, it follows that 7 is either even, or a multiple of 3.

Because f is irreducible, the Galois group of f acts transitively on the roots of f. Thus there is a permutation σ in the Galois group of f such that $\sigma(\alpha) = \delta$. We know that σ must preserve the equality $\alpha\overline{\alpha} = \beta\overline{\beta}$ and so we have $|\delta\sigma(\overline{\alpha})| = |\sigma(\beta)\sigma(\overline{\beta})|$. The left-hand side is equal to one of $|\delta||\gamma|$ or $|\delta|R$ depending on $\sigma(\overline{\alpha})$. There are three cases to consider for the right-hand side. The roots $\sigma(\beta)$ and $\sigma(\overline{\beta})$ are either both dominant, both non-dominant, or one of each. It is clear that the modulus in each of these (respective) cases R^2, $|\gamma|^2$, and $|\gamma|R$ breaks the aforementioned equality between the left- and right-hand sides, a contradiction.   ◀

Hence we have proved Theorem 11, as required.

4   Palindromic Octics

A monic polynomial $f \in \mathbb{Z}[x]$ is *palindromic* if its coefficients string together to form a palindrome. That is to say, for $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + 1$ we have that $a_k = a_{d-k}$ for each $k \in \{0, 1, \ldots, d\}$. In other sources, the term *self-reciprocal* is sometimes used since if α is a root of f then α^{-1} is also a root of f. If $\alpha \in \mathbb{C}$ is a root of f, then so are $\overline{\alpha}, 1/\alpha$, and $1/\overline{\alpha}$. Further, when α is neither real nor lies on the unit circle then these four roots are distinct. The class of palindromic polynomials appear in areas across mathematics and computer science in fields such as: coding theory, algebraic curves over finite fields, knot theory, and linear feedback shift registers, to name but a few (see the survey [12]).

▶ Remark 16. Let us further motivate the study of the *Palindromic Skolem Problem* (the Skolem Problem restricted to the study of sequences with palindromic characteristic polynomials). From the viewpoint of dynamical systems, we observe that the equations of motion (1) governing a recurrence sequence with palindromic characteristic polynomial (hereafter

a *palindromic recurrence sequence*) possess a *time-reversing symmetry*; that is to say, the recurrence relation is invariant under the time reversal map $n \mapsto -n$. More concretely, let $\langle X_n \rangle_{n=0}^{\infty}$ and $\langle Y_{-n} \rangle_{n=0}^{\infty}$ be recurrence sequences satisfying the palindromic relations

$$X_{n+d} = a_{d-1}X_{n+d-1} + \cdots + a_{d-1}X_{n+1} + X_n \qquad \text{and}$$
$$Y_{-n-d} = a_{d-1}Y_{-n-d+1} + \cdots + a_{d-1}Y_{-n-1} + Y_{-n},$$

respectively. Then $Y_{-n} = X_n$ for each $n \in \mathbb{N}_0$ if $Y_{-m} = X_m$ for each $m \in \{0, 1, \dots, d-1\}$.

For further information on the topic of time-reversing symmetries, we refer the interested reader to the exposition in Lamb's article [17] and the recent survey by Baake [2] (and the references therein).

4.1 Hard instances of the Reversible Skolem Problem at order eight

In Proposition 17, we construct an infinite family of palindromic octics that satisfy both H1 and H2. This result blocks any obvious attempt to settle decidability of the Reversible Skolem Problem at order eight with current state-of-the-art techniques. Another family of octics that satisfy both H1 and H2 is discussed in Lipton et al. [19]. The additional restriction (palindromic coefficients) we require demonstrates a refinement in the discussion of hard instances of the Reversible Skolem Problem at order eight.

▶ **Proposition 17.** *There are infinitely many palindromic octics in $\mathbb{Z}[x]$ that satisfy both H1 and H2.*

Proof. Let $f \in \mathbb{Z}[x]$ be such a palindromic octic with four simple dominant roots (that is, two complex-conjugate pairs) that lie on a circle of radius $r > 1$. Write $f(x) = \prod_{i=1}^{8}(x - \lambda_i)$ and for each $n \in \mathbb{N}$, define $f_n(x) := \prod_{i=1}^{8}(x - \lambda_i^n)$. By the symmetries in the roots λ_i^n, it is straightforward to verify the following three observations. First, each octic f_n in the sequence $\langle f_n \rangle_{n=1}^{\infty}$ is palindromic. Second, each octic f_n satisfies both H1 and H2. Third, by Lemma 6, $f_n \in \mathbb{Z}[x]$ for each $n \in \mathbb{N}$.

We finish the proof by showing that there are infinitely many distinct polynomials in the sequence $\langle f_n \rangle_{n=1}^{\infty}$. Let $re^{\pm i\theta}, re^{\pm i\psi}$ be the four dominant roots of f. Let $f_n(x) = x^8 + a_{7,n}x^7 + \cdots + 1$. Then, by Vieta's formulae, $a_{7,n}$ is given by the sum of the nth powers of the roots of f; that is,

$$a_{7,n} = (r^n + r^{-n})(e^{ni\theta} + e^{-ni\theta} + e^{ni\psi} + e^{-ni\psi}).$$

Assume, for a contradiction, that the non-degenerate integer linear recurrence sequence $\langle a_{7,n} \rangle_n$ takes only finitely many values. By the Pigeonhole Principle, there is an $a \in \mathbb{Z}$ and an infinite subsequence $\langle n_k \rangle_k$ of natural numbers such that $a_{7,n_k} = a$ for each $k \in \mathbb{N}$. We make two observations. First, the integer linear recurrence sequence $\langle a_{7,n} - a \rangle_n$ has characteristic polynomial $f(x)(x-1)$ (see [8, Theorem 1.1]) and so is non-degenerate. Second, the sequence $\langle a_{7,n} - a \rangle_n$ vanishes infinitely often. We have a contradiction: a non-degenerate linear recurrence sequence has only finitely many zero terms. It follows that there are infinitely many distinct palindromic octics in the sequence $\langle f_n \rangle_n$, as desired. ◀

▶ Remark 18. A *symplectic matrix* M is a $2\ell \times 2\ell$ matrix that preserves the *symplectic form* J in 2ℓ dimensions; that is to say, $M^\top J M = J$ where

$$J = \begin{pmatrix} 0 & I_\ell \\ -I_\ell & 0 \end{pmatrix}.$$

It is well-known that the characteristic polynomial of a symplectic matrix is a palindromic polynomial. In fact, the following constructive result proves the converse. Rivin [28, Theorem A.1] attributes the result to Kirby [15][1].

▶ **Theorem 19.** *For each monic palindromic polynomial $f \in \mathbb{Z}[x]$ of degree 2ℓ, there is a symplectic matrix $M \in \mathbb{Z}^{2\ell \times 2\ell}$ such that $\det(xI_{2\ell} - M) = f(x)$.*

Note the group of $2\ell \times 2\ell$ symplectic matrices with entries in $\mathbb{Z}$ is closed under multiplication. This observation leads to an alternative proof of Proposition 17 as follows. Let $f \in \mathbb{Z}[x]$ be an octic palindrome satisfying H1 and H2. Now let $M \in \mathbb{Z}^{8 \times 8}$ be a symplectic matrix with characteristic polynomial f. Consider the sequence $\langle f_n \rangle_n$ where $f_n(x) := \det(xI_{2\ell} - M^n) \in \mathbb{Z}[x]$. As before, we need to verify that each polynomial in this sequence satisfies the root assumptions H1 and H2. We then proceed in a similar fashion to the proof of Proposition 17, in order to generate an infinite sequence of octic palindromes with the desired properties.

4.2   Galois theory of octic palindromes

It is interesting to consider the root symmetries of the characteristic polynomials of reversible linear recurrence sequences. In this subsection we focus our attention on the Galois groups of octic palindromes; in particular, those underlying hard instances of the Reversible Skolem Problem. We present a new result (Theorem 20). The problem of root symmetries follows naturally from our approach to Theorem 1 where we explored polynomial identities between roots of certain irreducible polynomials. Such results are also motivated by hard open problems such as (polynomial) invariant generation and loop synthesis in the field of program verification.

The task of computing the Galois groups of irreducible polynomials in $\mathbb{Z}[x]$ is well-known. Families of polynomials associated with reversible sequences include the cyclotomic and Salem polynomials. The authors of [4] discuss ramifications to the Galois group of moving two of the Galois conjugates off of the unit circle. For the interested reader, two accounts of the Galois theory of palindromic polynomials are [36, 29]. 'Generically', the Galois group of a palindromic polynomial of degree $2d$ is $S_d \wr C_2$ (the *signed permutation group* or the *hyperoctahedral group*). In the case $d = 4$, the order of $S_4 \wr C_2$ is 384.

Here we shall consider the Galois groups associated with irreducible octic palindromes of the form constructed in Proposition 17. Recall that each polynomial in that family has roots of the form $r^{\pm 1}e^{\pm i\theta}, r^{\pm 1}e^{\pm i\psi}$. When a polynomial with this root distribution is irreducible, some of the powers of these roots are given by Salem half-norms (Theorem 8).

▶ **Theorem 20.** *Suppose that $f \in \mathbb{Z}[x]$ is an irreducible and simple palindromic octic with four dominant roots such that none of its conjugate ratios are roots of unity (so that H1 and H2 are satisfied). Then, the associated Galois group is isomorphic to either $S_4 \times C_2$ or $A_4 \times C_2$.*

Proof. Let $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ be the four dominant roots of f. As before, we can assume without loss of generality that these roots lie on a circle $|z| = R$ with $R > 1$. The Galois group of the splitting field of f is necessarily a subgroup of the group of automorphisms G of the set $\{\alpha^{\pm 1}, \overline{\alpha}^{\pm 1}, \beta^{\pm 1}, \overline{\beta}^{\pm 1}\} \subset \mathbb{C}$. Further, the Galois group necessarily contains permutations

---

[1] The author was unable to access Kirby's article in order to verify this attribution.

that fix the relations $xx^{-1} = 1$ for x in the set and $\alpha\overline{\alpha}^{-1} - \beta\overline{\beta}^{-1} = 0$. We note that G also contains the *inversion map* $x \mapsto x^{-1}$. The action of G on the roots induces an action of (a subgroup of) S_4 on the set of C_2 orbits $\{x, x^{-1}\}$, which we lift to an action of (a subgroup of) S_4 on the roots.

It is easily verified that the transposition (12) induces one of the maps

$$(\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\overline{\alpha}, \alpha, \beta, \overline{\beta}), \quad \text{or} \quad (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\overline{\alpha}^{-1}, \alpha^{-1}, \beta^{-1}, \overline{\beta}^{-1}).$$

Both of these maps commute with inversion and we note the latter is obtained from the former by applying the inversion map. Thus, without loss of generality, we take (12) as the former map.

In fact, every transposition can be lifted and commutes with inversion. Hence $G = S_4 \times C_2$. The transformations are as follows:

$(12) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\overline{\alpha}, \alpha, \beta, \overline{\beta})$

$(13) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\beta^{-1}, \overline{\alpha}, \alpha^{-1}, \overline{\beta})$

$(14) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\overline{\beta}^{-1}, \overline{\alpha}, \beta, \alpha^{-1})$

$(23) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\alpha, \beta^{-1}, \overline{\alpha}^{-1}, \overline{\beta})$

$(24) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\alpha, \overline{\beta}^{-1}, \beta, \overline{\alpha}^{-1})$

$(34) \colon (\alpha, \overline{\alpha}, \beta, \overline{\beta}) \mapsto (\alpha, \overline{\alpha}, \overline{\beta}, \beta).$

By way of explanation, these transformations are deduced as follows. First, when choosing a lift of a transposition from the set of C_2-orbits to the set of roots, one can invert an even number of the orbit pairs $\{x, x^{-1}\}$. Second, the choice of inverting none or all four orbit pairs differs only by the inversion map. Similarly, the two options when inverting two of the orbit pairs differ only by inversion. A transposition σ necessarily preserves $\alpha\overline{\alpha} - \beta\overline{\beta} = 0$. Some careful accounting shows that permutations such as $\sigma(\overline{\alpha}) = \beta$ (or $\sigma(\overline{\alpha}) = \overline{\beta}$) lead to $\alpha\beta - \overline{\alpha}\overline{\beta} = 0$ (or $\alpha\overline{\beta} - \overline{\alpha}\beta = 0$) and so $\alpha\beta \in \mathbb{R}$ (or $\alpha\overline{\beta} \in \mathbb{R}$). Such conclusions contradict our assumptions on the conjugate ratios of f. Similar arguments lead to the conclusion that there is a unique (that is to say, unique up to inversion) automorphism of the roots that preserves the aforementioned relations. Hence the Galois group is a subgroup of $S_4 \times C_2$.

We make the following useful observations. Firstly, the Galois group is a transitive subgroup of $S_4 \times C_2$ because f is irreducible. Secondly, since the action of C_2 on the roots is *free* (given $g, h \in C_2$ and a root x with $gx = hx$ then necessarily $g = h$), the transitive subgroups of $S_4 \times C_2$ are precisely the direct product of C_2 and a transitive subgroup of S_4. Finally, we note that $(12)(34)$, representing complex conjugation, is certainly an element of the Galois group.

The transitive subgroups of S_4 are isomorphic to S_4, A_4, D_4, C_4, and K_4. Because C_4 and K_4 are Abelian groups, $(12)(34)$ either lies in the centre of each group or the subgroup does not contain $(12)(34)$. In the former case we deduce that the splitting field is a Kroneckerian field (by Corollary 9) and so the splitting field is either CM or totally real. The field cannot be totally real by our assumption that f has non-real roots. The field is also not a CM-field for otherwise the conjugate ratios are necessarily roots of unity by Theorem 10.

We now focus on eliminating the possibility that the Galois group of f is $D_4 \times C_2$. There are three conjugate subgroups of S_4 that are isomorphic to D_4:

$D_{4,0} = \{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\} = \langle (1324), (12) \rangle,$

$D_{4,1} = \{e, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\} = \langle (1234), (13) \rangle, \text{ and}$

$D_{4,2} = \{e, (14), (23), (14)(23), (12)(34), (13)(24), (1243), (1342)\} = \langle (1243), (14) \rangle.$

Note $(12)(34)$ lies in the centre of $D_{4,0}$ and so we can once again employ Theorem 10 to deduce that $D_{4,0} \times C_2$ cannot be the Galois group of the splitting field of f. Assume, for a contradiction, that $D_{4,1} \times C_2$ is the Galois group of the splitting field of f. It is easily verified that $\alpha/\beta + \overline{\alpha/\beta}$ is invariant under the action of $D_{4,1} \times C_2$. Hence $\alpha/\beta + \overline{\alpha/\beta} \in \mathbb{Q}$. Since $\alpha/\beta \notin \mathbb{Q}$, we deduce that

$$(x - \alpha/\beta)(x - \overline{\alpha/\beta}) = x^2 - (\alpha/\beta + \overline{\alpha/\beta})x + 1 \in \mathbb{Q}[x].$$

Thus α/β satisfies a quadratic monic polynomial; moreover, since α/β is an algebraic integer it follows that $\alpha/\beta + \overline{\alpha/\beta} \in \mathbb{Z}$. Since $|\alpha/\beta| = 1$, we find $\alpha/\beta + \overline{\alpha/\beta} \in \{\pm 2, \pm 1, 0\}$. Each of the roots of the five possible polynomials are roots of unity, which contradicts our assumption on the conjugate ratios. Mutatis mutandis, one eliminates the possibility that the Galois group is $D_{4,2} \times C_2$ by similar consideration of $\alpha/\overline{\beta} + \overline{\alpha}/\beta$.

Thus the Galois group of the splitting field of f is either $S_4 \times C_2$ or $A_4 \times C_2$, as required. ◀

▶ **Remark 21.** It is not possible to strengthen the above result: the Galois group of the palindrome $x^8 + x^7 - x^6 + x^5 + 5x^4 + x^3 - x^2 + x + 1$ is $S_4 \times C_2$, whilst the Galois group of the palindrome $x^8 + x^7 - 3x^6 + x^5 + 9x^4 + x^3 - 3x^2 + x + 1$ is $A_4 \times C_2$. Both polynomials satisfy the assumptions in Theorem 20. For the avoidance of doubt, the converse of the statement in Theorem 20 is not true: the Galois group of the palindrome $x^8 + x^6 + 6x^5 + 9x^4 + 6x^3 + x^2 + 1$, which possesses a single complex-conjugate pair of dominant roots, is $S_4 \times C_2$.

5   Directions for Future Research

Our main contribution to the state of the art is a new proof of Theorem 1: the Skolem Problem is decidable for the class of reversible integer linear recurrence sequences of order at most seven. The benefit of our approach (by comparison to the case analysis in [19]) is the potential for applications to related decision problems. In this section we suggest directions for future research; in particular, variations on the Positivity and Skolem Problems for linear recurrence sequences.

5.1   The Simple Reversible Positivity Problem

The *Positivity Problem* asks to decide whether the terms in an integer linear recurrence sequence are all non-negative. Ouaknine and Worrell [26] demonstrated that the Positivity Problem is decidable for *simple* linear recurrence sequences (those whose characteristic polynomials have no repeated roots) of order at most nine. The proofs therein very much depend on an approach via Baker's Theorem for linear forms in logarithms. Those authors identify the class of non-degenerate linear recurrence sequences of order ten that are not amenable to said approach: the characteristic polynomials in this class have one dominant real root, four complex-conjugate pairs of dominant roots, and one non-dominant root.

Consider the family of monic polynomials in $\mathbb{Z}[x]$ of degree ten, with constant coefficient ± 1, and the above distribution of roots. Suppose that $f \in \mathbb{Z}[x]$ is a polynomial in this class. We immediately find that f is irreducible since each dominant root of f is necessarily conjugate to the single non-dominant root. The roots of f lie on two concentric circles centred at the origin and so we can invoke Theorem 8 to derive a contradiction. Thus the obstruction to decidability falls away under our extra assumptions and so we extend the result in [26] in this restricted setting. In summary, the *Simple Reversible Positivity Problem* is decidable for recurrences of order at most ten and so we have proved Corollary 3.

▶ Remark 22. Let us give an alternative proof for Corollary 3; this alternative proof does not invoke Theorem 8.

Observe that any candidate polynomial in our discussion is irreducible. We can invoke standard results for irreducible polynomials with many dominant roots. For example, versions of the following lemma are found in [32, 10].

▶ **Lemma 23.** *Suppose that α is an algebraic number with Galois conjugates β and γ satisfying $\alpha^2 = \beta\gamma$. Then the conjugate ratio α/β is a root of unity.*

Now suppose that a polynomial $f \in \mathbb{Z}[x]$ of degree ten has the aforementioned distribution of roots and is the characteristic polynomial of a non-degenerate linear recurrence sequence. Since f is necessarily irreducible and has a dominant positive root, we can invoke Lemma 23. We deduce that f is the characteristic polynomial of a degenerate recurrence sequence, a contradiction. Thus the obstacle to deciding positivity of simple linear recurrence sequences at order ten falls away under our additional assumption of reversibility: there are no sequences in the aforementioned class. As an aside, Lemma 23 is used by Dubickas and Smyth [7] as a stepping-stone towards Theorem 8.

We propose that such approaches as outlined above could lead to further decidability results for variants of the Positivity Problem. The key observations on the characteristic polynomials were: irreducibility and a dominant positive root. Here we can make the latter assumption without loss of generality. Indeed, let us recall the following classical consequence of Pringsheim's Theorem in complex analysis that is pertinent to deciding positivity.

▶ **Lemma 24.** *Suppose that a non-zero real-valued linear recurrence sequence $\langle X_n \rangle_n$ has no positive dominant characteristic root. Then the cardinalities of the sets $\{n \in \mathbb{N} : X_n > 0\}$ and $\{n \in \mathbb{N} : X_n < 0\}$ are both infinite.*

5.2 The Skolem Problem and unit-norm roots

In this paper we invoke results such as Theorem 8 in order to reduce the reversible Skolem Problem at orders five, six, and seven, to decidable instances of the Skolem Problem (Theorem 2). It is interesting to speculate that techniques involving identities between roots (the Galois theory underlying Theorem 8) have further applications in establishing decidability results for linear recurrence sequences. Indeed, the general version of Theorem 8 (see [7, Theorem 2.1]) considers not only algebraic integers that are units, but also algebraic numbers that are *unit-norms*. An algebraic number α is a *unit-norm* if the minimal polynomial of α is of the form $a_d x^d - a_{d-1} x^{d-1} - \cdots - a_1 x - a_0 \in \mathbb{Z}[x]$ such that $|a_d| = |a_0|$. So the unit-norm algebraic integers are the units.

We can strengthen the statement in Proposition 12 by invoking [7, Theorem 2.1]: we deduce there is no polynomial $a_5 x^5 - a_4 x^4 - a_3 x^3 - a_2 x^2 - a_1 x \pm a_5 \in \mathbb{Z}[x]$ that satisfies hypotheses H1 and H2. Thus not only do we settle decidability of the reversible Skolem Problem at order five, but also decidability of the Skolem Problem at order five for the class of rational-valued linear recurrence sequences that satisfy a relation of the form

$$X_{n+5} = a_4 X_{n+4} + a_3 X_{n+3} + a_2 X_{n+2} + a_1 X_{n+1} \pm X_n$$

with $a_1, a_2, a_3, a_4 \in \mathbb{Q}$. Thus we have established Corollary 4.

────── **References** ──────

1 S. Akshay, Nikhil Balaji, and Nikhil Vyas. Complexity of Restricted Variants of Skolem and Related Problems. In Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin, editors, *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)*, volume 83 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 78:1–78:14, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. `doi:10.4230/LIPIcs.MFCS.2017.78`.

2 M. Baake. A brief guide to reversing and extended symmetries of dynamical systems. In *Ergodic theory and dynamical systems in their interactions with arithmetics and combinatorics*, volume 2213 of *Lecture Notes in Math.*, pages 117–135. Springer, Cham, 2018.

3 Vincent D. Blondel and Natacha Portier. The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. *Linear Algebra and its Applications*, 351-352:91–98, 2002. Fourth Special Issue on Linear Systems and Control. `doi:10.1016/S0024-3795(01)00466-9`.

4 Christos Christopoulos and James McKee. Galois theory of Salem polynomials. *Mathematical Proceedings of the Cambridge Philosophical Society*, 148(1):47–54, 2010. `doi:10.1017/S0305004109990284`.

5 Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

6 Ryan C. Daileda. Algebraic integers on the unit circle. *Journal of Number Theory*, 118(2):189–191, June 2006. `doi:10.1016/j.jnt.2005.09.002`.

7 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`.

8 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.

9 P. Fatou. Sur les séries entières à coefficients entiers. *Comptes Rendus Acad. Sci. Paris*, 138(130):342–344, 1904.

10 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`.

11 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.

12 David Joyner. Zeros of some self-reciprocal polynomials. In *Excursions in harmonic analysis. Volume 1*, Appl. Numer. Harmon. Anal., pages 329–348. Birkhäuser/Springer, New York, 2013. `doi:10.1007/978-0-8176-8376-4_17`.

13 Anatole Katok and Boris Hasselblatt. *Introduction to the Modern Theory of Dynamical Systems*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1995. `doi:10.1017/CBO9780511809187`.

14 G. Kenison, R. Lipton, J. Ouaknine, and J. Worrell. On the Skolem Problem and prime powers. In *International Symposium on Symbolic and Algebraic Computation, ISSAC '20*. ACM, 2020. `doi:10.1145/3373207.3404036`.

15 David Kirby. Integer matrices of finite order. *Rend. Mat.*, 2(6):403–408, 1969.

16 L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1857(53):173–175, January 1857. `doi:10.1515/crll.1857.53.173`.

17 J S W Lamb. Reversing symmetries in dynamical systems. *Journal of Physics A: Mathematical and General*, 25(4):925–937, February 1992. `doi:10.1088/0305-4470/25/4/028`.

18 Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2:417–421, 1953.

19 Richard J. Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the Skolem Problem and the Skolem Conjecture. To appear in the Symposium on Logic in Computer Science (LICS), 2022.

20 Florian Luca, Joël Ouaknine, and James Worrell. Universal Skolem Sets. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*, pages 1–6. IEEE, 2021. `doi:10.1109/LICS52264.2021.9470513`.

21 C. R. MacCluer and Charles J. Parry. Units of modulus 1. *Journal of Number Theory*, 7(4):371–375, November 1975. `doi:10.1016/0022-314x(75)90040-2`.

22 K. Mahler. Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amst.*, 38:50–69, 1935.

23 K. Mahler and J. Cassels. On the Taylor coefficients of rational functions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 52(1):39–48, 1956.

24 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.

25 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.

26 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.

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

28 Igor Rivin. Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. *Duke Mathematical Journal*, 142(2):353–379, 2008.

29 Igor Rivin. Large Galois groups with applications to Zariski density, 2015. `arXiv:1312.3009`.

30 A. Schinzel. *Polynomials with Special Regard to Reducibility*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2000. `doi:10.1017/CBO9780511542916`.

31 Thoralf Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *8de Skand. Mat. Kongress, Stockholm (1934)*, pages 163–188, 1934.

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

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

34 The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.3*, 2021. available from `http://pari.math.u-bordeaux.fr/`.

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

36 Paulo Viana and Paula Murgel Veloso. Galois theory of reciprocal polynomials. *The American Mathematical Monthly*, 109(5):466–471, 2002. `doi:10.1080/00029890.2002.11919875`.