Complexity of Restricted Variants of Skolem and Related Problems

S. Akshay[1], Nikhil Balaji*[2], and Nikhil Vyas[3]

1 Department of Computer Science and Engineering, IIT Bombay, India
akshayss@cse.iitb.ac.in
2 Aalen University, Aalen, Germany
nikhilrbalaji@gmail.com
3 Department of Computer Science and Engineering, IIT Bombay, India
nikhilvyas@cse.iitb.ac.in

Abstract

Given a linear recurrence sequence (LRS), the Skolem problem, asks whether it ever becomes zero. The decidability of this problem has been open for several decades. Currently decidability is known only for LRS of order upto 4. For arbitrary orders (i.e., number of terms the n^{th} depends on), the only known complexity result is NP-hardness by a result of Blondel and Portier from 2002.

In this paper, we give a different proof of this hardness result, which is arguably simpler and pinpoints the source of hardness. To demonstrate this, we identify a subclass of LRS for which the Skolem problem is in fact NP-complete. We show the generic nature of our lower-bound technique by adapting it to show stronger lower bounds of a related problem that encompasses many known decision problems on linear recurrent sequences.

1998 ACM Subject Classification F.1.1 Models of computation, F.2 Analysis of Algorithms and Problem Complexity, F.2.1. Numerical Algorithms and Problems

Keywords and phrases Linear recurrence sequences, Skolem problem, NP-completeness, Program termination

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.78

1 Introduction

While linear dynamical systems have been studied for a long time, several interesting and computationally relevant decision problems remain unsolved. The *Skolem problem* is a long-standing open problem in mathematics which asks whether zero ever occurs in the infinite sequence generated by a given linear recurrence sequence (LRS) with specific initial conditions. The *positivity problem* asks if the values of an LRS are always positive. Both these problems have received consider attention from mathematicians and computer scientists over the years. The positivity problem is related to program termination for initialized linear loop programs [23, 8, 16], while the Skolem and its variants have been considered in probabilistic verification [1, 2, 3] among other applications. However, despite decades of active research, the problems in their full generality have remained open.

While a result of Blondel and Portier [7] showed NP-hardness for the Skolem problem, the only known positive results are for very restricted class of recurrences, with restrictions

* Supported by DFG grant TH 472/4. Part of this work was done when the author was a Postdoctoral fellow at IIT Bombay.

42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017).
Editors: Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin; Article No. 78; pp. 78:1–78:14
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

on either the order of the recurrence (i.e., number of terms defining the sequence) or on the roots of the characteristic polynomial associated with the recurrence. On one hand, the Skolem problem is known to be decidable for order 4 [17, 25] and positivity for degree 6 [19]. On the other hand, by restricting LRS to only considering those with distinct roots (these are called simple LRS), Ouaknine and Worrell show decidability of positivity for order 9 LRS [18] and decidability of a related variant, *ultimate positivity* (is there a point after which the LRS is always positive) [20]. Further, in [18] they show that the decidability of the the positivity problem for order 6 LRS would entail solutions to longstanding open problems on Diophantine approximations. While it is well-known and probably a folklore result ([25]) that if the roots of characteristic polynomial are real (in fact, more generally, if the LRS has a single dominant root) then Skolem and positivity are decidable, the exact complexity of these problems have not been mapped out. Indeed, it is customary for papers in the area to study LRS that are *non-degenerate* (which is when there are no two characteristic roots such that their ratio is a root of unity), since it is known that the general case reduces to this case as far as decidability is concerned.

In this paper, we focus on linear recurrence sequences, whose characteristic polynomial has roots of some special form. Our contributions are the following: we give a new NP-hardness proof for the Skolem problem by a reduction from the classic Subset Sum problem. This gives an alternate proof of NP-hardness of Skolem (as well as coNP-hardness for positivity), which matches the best lower bound known for the Skolem problem, due to Blondel and Portier [7]. A closer inspection of our proof shows that the LRS that is output by our reduction is a special subclass of LRS whose characteristic polynomial has roots that are complex roots of unity (i.e., complex numbers α such that $\alpha^n = 1$ for some integer n). We investigate this natural class of LRS and match our lower bound by showing that the Skolem problem for this class can be solved in NP. Thus, we obtain a natural subclass of LRS of arbitrary order with an NP-complete Skolem problem, which to the best of our knowledge has not been observed before. Finally, we show that both the lower bound and upper bound techniques can be lifted to other problems.

We now explain the significance of all these three results and place them in the context of existing results. We start with the hardness result, where as mentioned earlier, Blondel and Portier [7] already proved NP-Hardness of Skolem. However, our proof is of independent interest for the following reasons:

- Our proof is a direct reduction from the classical subset sum problem and is arguably simpler/shorter than the proof in [7], which goes via automata theory, by showing a reduction from universality of unary NFA.
- The proof in [7] shows NP-hardness by considering LRS whose characteristic polynomials have 0/1-coefficients. While this is indeed a simple subclass of LRS, the characteristic polynomial of such LRS could still have complex roots with phase/angle that is an irrational multiple of π. Current techniques seem inadequate to solve the Skolem and positivity problem for LRS of this kind and hence do not give effective upper bounds. In contrast, for the subclass of LRS arising from our hardness proof, the Skolem problem admits an NP algorithm. [1]
- Our NP-hardness proof can be extended to show hardness for other problems as shown in Section 4.

Next, we turn to the NP upper bound. We first note that we are able to achieve this result for LRS of arbitrary orders. All upper bounds currently known for restricted variants of the

[1] In fact, a closer inspection of Blondel and Portier's proof, reveals that their hard instances actually fall into a stricter subclass, which can be shown to be NP-complete using our techniques.

Skolem (and related problems) problem, restrict the order to a fixed constant [18] or assume that the recurrence with arbitrary order is simple [20]. Our upper bound techniques rely on basic linear algebra and complexity theory and do not need the development or application of advanced techniques from algebraic number theory and Diophantine approximation as in the other results in [18, 20]. This indeed makes our proofs more elementary, but allows for easy generalization to other problems as we show next.

Our third and final contribution is to show that our lower bound proof and the upper bound techniques can be extended. To illustrate this, we consider a related variant of the Skolem and positivity problem which we call the *polytope containment problem.* We will define this problem in the matrix form rather than in terms of LRS, while noting that we can use Cayley-Hamilton theorem and basic linear algebra to see their equivalence (see [25] for details). Recall that a *(convex) polytope* is an intersection of finitely many half-spaces and it is said to be *bounded* if the region enclosed in it is bounded. Given a bounded polytope V_1 and a (possibly unbounded) polytope V_2 over $\mathbb{Z}^d$ and a $d * d$ matrix M with integer entries, the *Integer Polytope Containment Problem* asks if for all $v \in V_1$ does there exist a positive integer n such that $vM^n \in V_2$.

There are two main motivations to look at this problem. First, it generalizes the Skolem problem, higher-order orbit problem [10] and polyhedron hitting problem [9] over integers. For the former, we set V_1 to be the initial vector and V_2 the space orthogonal to the target vector (defined as the intersection of halfspaces $\{x \mid x \cdot w \leq 0 \wedge x \cdot w \geq 0\}$). The higher-order orbit problem is obtained by fixing V_1 as the initial vector and no restrictions on V_2.

The second main motivation is that the negation of this problem is closely related to program termination of linear loops. Program termination is a classical undecidable problem, but the special case of the problem over linear loops has received considerable attention ([21] surveys these results as well as their link to linear recurrence sequences). There are two main variants of this problem. First, the initialized termination problem asks: starting from a initial vector v, is it the case that for all $n \in \mathbb{N}$, $vM^n > 0$? Next the uninitialized termination problem asks: does there exist an initial vector v such that for all $n \in \mathbb{N}$, we have $vM^n > 0$? In [23, 8], Tiwari and Braverman showed that the uninitialized problem is decidable in polynomial time for reals and integers respectively. The initialized problem, often called the positivity problem, however is still open in its fully generality though some results in restricted cases have been proved recently [18, 20, 19].

We observe that the negation of the above defined polytope containment problem is: given a bounded polytope V_1 and a polytope V_2, does there exist $v \in V_1$ such that for all $n \in \mathbb{N}$, $vM^n \notin V_2$. By fixing V_2 to be the halfspace $\{x \in \mathbb{Z}^d \mid c^T x \leq 0\}$, we obtain (i) the initialized termination problem over integers by fixing V_1 to be the singleton initial vector and (ii) the uninitialized termination problem over integers by fixing V_1 to be the entire space $\mathbb{Z}^d$. Thus, this problem generalizes both initialized and uninitialized linear program termination problems. For e.g., the following is an instance of this problem.

> Given M, V_1 (a bounded polytope), c, does the following loop terminate for all $x \in V_1$
> 1: **while** $c^T x > 0$ **do**
> 2: $\quad x \leftarrow Mx$

Showing decidability of this problem in general would imply the decidability of the many of these longstanding open problems, including Skolem and Positivity. Nevertheless, one may ask whether looking at this general problem allows us to prove better lower bounds or/and upper bounds in restricted cases. We remark here that if we generalize V_1 to allow unbounded polytopes, it turns out that we can encode Petri net reachability and hence this problem is EXPSPACE-hard [6]. However, this hardness result crucially depends on the unboundedness of V_1 and does not seem to work for a bounded initial space over integers.

As before, we restrict ourselves to the subclass whose characteristic roots are all complex roots of unity (or zero). We are able to then show that for this restricted class, the problem is Π_2^P-complete, building upon our lower-bound and upper-bound techniques.

2 Preliminaries

For a complex number $z = x + iy$, the absolute value and phase of the complex number are respectively denoted by $|z| = \sqrt{x^2 + y^2}$ and $arg(z) = \tan^{-1}(\frac{y}{x})$. We denote by e_i the k-dimensional standard basis vector that has 1 at the i-th position and 0 elsewhere.

2.1 Linear Recurrence Sequences

We recall some definitions and basic properties of linear recurrence sequences that will be useful in the rest of the paper. For a detailed treatment, we refer the reader to the excellent text of Everest et al. [12].

▶ **Definition 1** (Linear Recurrence Sequence). A sequence $\langle u \rangle = \langle u_n \rangle_{n=0}^{\infty}$ is called a *linear recurrence sequence* (LRS) of *order* k if k is the smallest positive integer such that the n^{th} term of the sequence can be expressed as $u_n = a_{k-1}u_{n-1} + \ldots + a_1 u_{n-k-1} + a_0 u_{n-k}$, for every $n \geq k$, where $a_j \in \mathbb{Z}$ for $j \in \{0, 1, \ldots, k-1\}$ and $a_0 \neq 0$. Such a sequence is uniquely determined by the *initial conditions* $u_0, u_1, \ldots, u_{k-1}$.

An LRS $\langle u \rangle = \{u_n\}_{n=0}^{\infty}$ is said to be *periodic* with period p if $u_n = u_{n+p}$ for every $n \geq 0$. For a linear recurrence sequence $\langle u \rangle$ of order k, we denote by $||u||$, the size of the bit representation of the coefficients of $\langle u \rangle$, namely $a_0, a_1, \ldots, a_{k-1}$ and the initial conditions $u_0, u_1, \ldots, u_{k-1}$.

To every such recurrence sequence $\langle u \rangle$ above, one can associate a univariate polynomial $\chi_u(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_1 x - a_0$ of degree at most k. $\chi_u(x)$ is called the *characteristic polynomial* of the recurrence $\langle u \rangle$. The roots of the characteristic polynomial are called the *characteristic roots* and they yield useful information about the asymptotic behavior of the recurrence. More formally, let $\{\lambda_1, \lambda_2, \ldots, \lambda_d\}$ be the roots of $\chi_u(x)$ with multiplicity $\rho_1, \rho_2, \ldots, \rho_d$ respectively. Then the n^{th} term of such an LRS $\langle u \rangle$, denoted u_n can be expressed as

$$u_n = \sum_{j=1}^{d} q_j(n)\lambda_j^n \tag{1}$$

where $q_j(x) \in \mathbb{C}[x]$ are univariate polynomials with complex coefficients of degree at most $\rho_j - 1$ such that $\sum_{j=1}^{d} \rho_j = k$. We say an LRS is *simple* when for every j, $\rho_j = 1$. Equivalently, for a simple LRS for every j, $q_j \in \mathbb{C}$ is a constant.

Given an LRS $\langle u \rangle$ of order k with characteristic polynomial $\chi_u(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_1 x - a_0$, one can associate a $k \times k$ matrix M_u called the *companion matrix* of the recurrence as shown in the following figure.

$$M_u^T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{bmatrix}$$

Given a vector v of dimension $k \times 1$ containing the k initial conditions of the recurrence, one can easily observe that $u_1 = e_1 M_u^T v$ and $e_1 (M_u^T)^n v$ gives u_n. Further, the eigenvalues of this matrix are exactly the roots of the characteristic polynomial of the LRS. In what follows, we sometimes abuse notation and call them as eigenvalues of the LRS. It is often useful to rewrite each λ_j in polar coordinates as $r_j e^{i\theta_j}$. In this representation, the n^{th}-term of the sequence is given by

$$u_n = \sum_{j=1}^{d} q_j(n) r_j^n e^{in\theta_j} \tag{2}$$

The following folklore lemma says that the sum and product of two LRS is an LRS (see for example, Theorem 4.1[12]). It is also known that the resulting LRS is constructible in P.

▶ **Lemma 2.** *Let $\langle u_1 \rangle, \ldots, \langle u_\ell \rangle$ be LRS of order $k_1, \ldots k_\ell$ respectively and let $\chi_{u_1}(x), \ldots, \chi_{u_\ell}(x)$ be their respective characteristic polynomials. Then the following properties hold:*

1. $\langle u \rangle = \sum_{i=1}^{\ell} \langle u_i \rangle$ *is also an LRS of order at most* $\sum_{i=1}^{\ell} k_i$. *Moreover,* $\chi_u(x)$ *is a factor of* $\prod_{i=1}^{\ell} \chi_{u_i}(x)$.
2. $\langle u \rangle = \langle u_1 \rangle \langle u_2 \rangle$ *is also an LRS of order (and* $\chi_u(x)$ *is of degree) at most* $k_1 k_2$.

It is an easy observation via Lemma 2, that the complement of the Skolem problem reduces to the Positivity problem (since $u_n \neq 0$ if and only if $u_n^2 > 0$ for all n).

2.2 Algebraic Numbers

We will extensively use algebraic numbers and their properties throughout the paper. We refer the reader to the excellent text by Cohen [11] for a extensive treatment of the computational aspects of algebraic number theory. Here we collect below some useful definitions and facts that are used throughout the rest of the paper.

A complex number α is called *algebraic* if there is a unique univariate polynomial $p_\alpha(x)$ with integer coefficients of minimum degree that vanishes at α. p_α is said to be the *defining polynomial* or the *minimal polynomial* of the algebraic number α. The *degree* and *height* of α are then the degree and height of p_α (Height of a polynomial is the maximum value of its coefficients). The roots of p_α are called the *Galois conjugates* of α.

▶ **Definition 3** (Roots of unity)**.** A complex number r is an n-th root of unity if $r^n = 1$ and a *primitive* n-th root of unity if in addition, n is the smallest $k \in \{1, \ldots, n\}$ for which $r^k = 1$.

▶ **Definition 4** (Cyclotomic polynomial)**.** The n-th Cyclotomic polynomial, denoted $\Phi_n(x)$ is the unique monic irreducible (over $\mathbb{Q}$) polynomial with integer coefficients that is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$. Its roots are all the n-th primitive roots of unity. Formally, $\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ gcd(k,n)=1}} \left(x - e^{\frac{i2\pi k}{n}}\right)$.

An important relation involving Cyclotomic polynomials (See for example [5]) and primitive n-th roots of unity is that

$$x^n - 1 = \prod_{1\le k\le n}\left(x - e^{\frac{i2\pi k}{n}}\right) = \prod_{d|n}\prod_{\substack{1\le k\le n\\ gcd(k,n)=1}}\left(x - e^{\frac{i2\pi k}{n}}\right) = \prod_{d|n}\Phi_{n/d}(x) = \prod_{d|n}\Phi_d(x)$$

The degree of $\Phi_n(x)$ (which is also precisely the number of n-th roots of unity) is $\phi(n)$ where ϕ is Euler's totient function, $\phi(n) = |\{k \mid k \le n, \gcd(k,n) = 1\}$. An expression for $\phi(n)$ is given by $\phi(n) = n\prod_{p|n}(1 - \frac{1}{p})$. For $n \ge 2$, $\phi(n) \ge \sqrt{\frac{n}{2}}$.

2.3 Problem statements

We now formally define three problems of interest on LRS. We will define a fourth all-encompassing problem in Section 4.

▶ **Definition 5** (Skolem, Positivity, Ultimate Positivity)**.** Given a LRS $\langle u\rangle$,

- *Skolem Problem*: Decide if there exists an $n \in \mathbb{N}$ such that $u_n = 0$.
- *Positivity problem*: Decide if $u_n > 0$ for all $n \in \mathbb{N}$.
- *Ultimate Positivity problem*: Decide if there exists $n_0 \in \mathbb{N}$ s.t., $u_n > 0$ for all $n > n_0$.

As mentioned in the introduction, we consider restriction of these problems to linear recurrent sequences with special properties, namely, the roots of their characteristic polynomial (also called characteristic roots henceforth) are complex roots of unity. We denote by Skolem_ω Pos_ω UPos_ω the Skolem, Positivity and Ultimate Positivity questions respectively for linear recurrence sequences whose characteristic roots are roots of unity.

3 LRS with roots of unity – an NP-complete subclass

In this section, we consider the special subclass of linear recurrence sequences, whose characteristic roots are exactly roots of unity, and show that the Skolem problem restricted to this subclass is NP-complete.

First, we show that Skolem_ω is NP-hard, UPos_ω and Pos_ω are coNP-hard for this class. This immediately shows NP-hardness (respectively coNP-hardness) for the Skolem problem (respectively Positivity and Ultimate Positivity) for LRS of unbounded order.

▶ **Theorem 6.** Skolem_ω *is* NP*-hard and* Pos_ω *and* UPos_ω *are* coNP*-hard.*

Proof. We show a reduction from Subset Sum to Skolem_ω. Denote by $\mathsf{SUBSETSUM}(A,T)$ the following instance of the Subset Sum problem: We have a set $A = \{a_1, a_2, \ldots, a_m\}$ where $a_i \in \mathbb{N}$ and a target $T \in \mathbb{N}$. Now, $\mathsf{SUBSETSUM}(A,T) = 1$ if there exists a subset S of A whose sum is equal to T. The *Subset Sum problem*, i.e., given A, T deciding whether $\mathsf{SUBSETSUM}(A,T) = 1$, is a classic NP-complete problem [15]. We will now construct a linear recurrence sequence $\langle u_{A,T}\rangle$ over integers which has a zero i.e., there exists r such that $u_r = 0$, iff there is a set $S \subseteq T$ such that $\sum_{s\in S} a_s = T$.

We construct the LRS as follows: For every $i \in \{1, \ldots, m\}$, let p_i be the i-th-prime. Then, for each i, we have a LRS $\langle u^i\rangle$, whose n-th term is defined as

$$u^i_n = \begin{cases} 0 & \text{if } 1 \le n < p_i \\ a_i & \text{if } n = p_i \\ u^i_{n-p_i} & \text{otherwise} \end{cases}$$

This is a periodic LRS of period p_i, where the first p_i terms are $(0, 0, \dots, a_i)$. Note that the order (and hence the degree of the characteristic polynomial) of this LRS is p_i.

We are now ready to define LRS $\langle u_{A,T}\rangle$: the n^{th} term of $\langle u_{A,T}\rangle$ is given by $\langle u_{A,T}\rangle_n = \sum_{i=1}^{m} u_n^i - T$. Since the sum of LRS is also an LRS (by Lemma 2), $u_{A,T}$ is also an LRS. Now, by the prime number theorem (see [13] for instance), it follows that the number of primes less than $n \in \mathbb{N}$ asymptotically grows as $\frac{n}{\log(n)}$, which implies that the n^{th} prime number is of magnitude $\mathcal{O}(n \log n)$. Thus, from this and Lemma 2, it follows that the order (and hence also the degree of the characteristic polynomial) of $u_{A,T}$ is at most $(\sum_{i=1}^{m} p_i) + 1 = \mathcal{O}(m^2 \log m)$ and $u_{A,T}$ can be constructed from a given instance of SUBSETSUM(A, T) in polynomial time. We have the following

▶ **Claim 7.** *$\langle u_{A,T}\rangle$ is zero if and only if there exists a subset $S \subseteq [m]$ such that $\sum_{s\in S} a_s = T$.*

Proof. Suppose there exists r such that $u_r = 0$. Then $\sum_{i=1}^{m} u_r^i = S$. As u_n^i can either be a_i or 0, this implies that there exists a subset $S \subseteq [m]$ such that $\sum_{s\in S} a_s = T$. This proves the forward direction of the claim. For the other direction, let us suppose there exists a subset $S \subseteq [m]$ such that $\sum_{s\in S} a_s = T$. Consider $N = \prod_{s\in S} p_s$. Then it is easy to see that u_N is precisely $\sum_{s\in S} a_s - T = 0$. ◀

This completes the NP-hardness of Skolem problem. The coNP-hardness of Positivity follows from noting that the square of a linear recurrence is also a linear recurrence. The complement of the Skolem problem reduces to the Positivity problem because $u_n \neq 0$ if and only if $u_n^2 > 0$ for all n. A closer observation of the proof of hardness yields the following important property of $u_{A,T}$: *the roots of $\chi_{u_{A,T}}$ are roots of unity.* This follows by observing that the characteristic polynomial of $\langle u^i\rangle$ is precisely $x^{p_i} - 1 = 0$. Hence all its roots are the p_i-th roots of unity. Now by Lemma 2, $\chi_{u_{A,T}}$ is a factor of the product $(x-1)\prod_{i=1}^{m}(x^{p_i} - 1)$ (here the term $x - 1$ is contributed by the integer $-T$ in the subset sum instance). The LRS $u_{A,T}$ is hence an instance[2] of Skolem_ω.

For the positivity problem, we have to square $u_{A,T}$ and since the characteristic roots of $(u_{A,T}^2)_n = \left(\beta_0 + \sum_{j=1}^{m} \beta_j e^{i\theta_j}\right)^2 = \sum_{j,\ell\in[m]} \beta_j\beta_\ell e^{i\theta_j} e^{i\theta_\ell}$, the characteristic roots of $u_{A,T}^2$ are also roots of unity. Hence the positivity problem for the LRS derived from the subset sum is actually an instance of Pos_ω. It is easy to see that for periodic LRS, the questions of positivity and ultimate positivity are equivalent. Since $u_{A,T}$ constructed in our proof is periodic, the coNP-hardness of Pos_ω also entails the same hardness for UPos_ω. ◀

To complement the hardness result from Theorem 6, we now prove that Skolem_ω(respectively Pos_ω and UPos_ω) is decidable in NP(respectively coNP). It is worthwhile to contrast this with the case of arbitrary recurrences for which decidability is open. We have the following

▶ **Theorem 8.** *Skolem_ω is in NP, Pos_ω and UPos_ω are in coNP.*

The rest of this section will prove the above theorem. We start with some basic properties. Consider the general form of the n^{th} term of an LRS as given in Equation 2. When the eigenvalues are roots of unity, this simplifies to

$$u_n = \sum_{j=1}^{d} q_j(n) e^{in\theta_j} \tag{3}$$

[2] In fact, it is easy to transform our recurrence $u_{A,T}$ in to another recurrence $u'_{A,T}$, while maintaining the property YES and NO instances of subset sum are mapped to YES and NO instance of Skolem_ω for $u'_{A,T}$, such that $u'_{A,T}$ is also a simple LRS.

where q_j are polynomials of degree at most $k-1$ and $\sum_{j=1}^{d}(\deg(q_j)+1) = k$ and $\theta_j = \frac{a_j 2\pi}{b_j}$ as roots of characteristic equation are roots of unity. In order to prove an NP upper bound, it suffices to show that there exists an $N \le 2^{\mathsf{poly}(||u||)}$ such that if u is zero at all, then $u_N = 0$ and this can verified in P. Recall that $||u||$ denotes the size of the bit representation of the coefficients of u_n, namely $a_0, a_1, \dots, a_{k-1}$ and the initial conditions $u_0, u_1, \dots, u_{k-1}$. We first note a few easy observations about the characteristic roots:

▶ **Proposition 9.** *If $e^{i\theta_j}$ is a characteristic root of multiplicity ρ_j of an LRS of order k, with $\theta_j = \frac{2\pi a_j}{b_j}$, $gcd(a_j, b_j) = 1$ then*

- *For any $1 \le a < b_j$ such that $gcd(a, b_j) = 1$, and $\theta = \frac{2\pi a}{b_j}$, $e^{i\theta}$ is also a root with multiplicity ρ_j.*
- $\rho_j b_j \le k^3$

This implies that the characteristic roots can be partitioned into multisets $\vartheta_j = \{e^{\frac{i2\pi a}{b_j}} \mid gcd(a, b_j) = 1\}$ and $|\vartheta_j| = \rho_j \phi(b_j)$, where ϕ is Euler's totient function.

Proof. The elements in multiset ϑ_j are exactly $e^{i\theta_j}$ and their Galois conjugates hence they must all occur, with same multiplicity. The cardinality of such numbers is exactly $\phi(b_j) \ge \sqrt{\frac{b_j}{2}}$ (where ϕ is Euler's totient function). Since the number of roots is k and each element in ϑ_j occurs ρ_j times, we obtain that each $\rho_j \phi(b_j) \le k$. As $\phi(b_j) \ge \sqrt{\frac{b_j}{2}}$ we get $\rho_j b_j \le k^3$. ◀

The solution set of Skolem$_\omega$ instances are very structured given the fact that the characteristic roots are roots of unity. Consider for each $m \in \mathbb{N}$, a polynomial $P_m = \sum_{j=1}^{d} q_j(x) e^{im\theta_j}$ and let P denote the set of polynomials $\{P_m \mid m \in \mathbb{N}\}$. We have the following

▶ **Lemma 10.** *The set P is finite i.e., $P = \{P_m \mid m \in [0, k^{3k}]\}$ where $k^{3k} < 2^{\mathsf{poly}(||u||)}$.*

Proof. When characteristic roots are roots of unity, each θ_j is of the form $\frac{2\pi a_j}{b_j}$ for some (positive) integers $a_j \le b_j$. Now $b_j \le k^3$ by Proposition 9. Each $e^{im\theta_j} = e^{i(m+b_j)\theta_j}$ for all m, i.e., they repeat after b_j steps. Hence $P_m = P_{m+t}$ for $t = \mathrm{lcm}\{b_1, \dots b_d\}$. Therefore $|P| \le t = \mathrm{lcm}\{b_1, \dots, b_d\} \le b_1 \cdots b_d \le k^{3k} \le 2^{k^4}$. Since $k < \mathsf{poly}(||u||)$, the result follows. ◀

Note that even though q_j could be polynomials with complex coefficients, the coefficients of polynomials in P are rational. This is because, all the polynomials P_m evaluate to integer values at infinitely many integers via Equation 3, since the recurrence always evaluates to integer values). By interpolation, these coefficients have to be rational.

Hence deciding Skolem$_\omega$ essentially boils down to finding the union of zero sets of all the polynomials in P. This naturally leads us to the problem of bounding the coefficients of polynomials in P since this immediately yields a bound on the roots. A natural way to proceed here would be to use interpolation to bound the coefficients (see e.g., [14]). The problem with this approach is that this yields an expression for the coefficients q_{kj} of the polynomials q_j in terms of linear combinations of λ_j, which are algebraic numbers. Standard techniques (see for example, the work of Tiwari on the sign problem [24]) however, do not yield a lower bound which is exponential in d, the degree of the roots. Thus, while this suffices to obtain an NP upper bound for LRS of fixed order (where d becomes constant), for the case of unbounded order LRS, it does not yield an NP upper bound. In the next two lemmas, we show how to sidestep this issue, by crucially exploiting the fact that our characteristic roots are roots of unity.

First, note that χ_u can be written as

$$\chi_u(x) = \prod_{j=1}^{d}(x - e^{2\pi i \frac{a_j}{b_j}})^{\rho_j} = \prod_{j=1}^{D} \prod_{\substack{1 \le a \le b_j \\ gcd(a,b_j)=1}} (x - e^{2\pi i \frac{a}{b_j}})^{\rho_j} \tag{4}$$

where D is the number of distinct values of b_j. We know from Lemma 2 that the sum of LRS is again a LRS. We obtain here a partial converse of part 1 of Lemma 2.

▶ **Lemma 11.** *Let $\langle u \rangle$ be a LRS with characteristic polynomial $\chi_u(x) = p_1(x)p_2(x)$ where p_1 and p_2 do not share a common root. Then we can find LRS $\langle u^1 \rangle$ and $\langle u^2 \rangle$ with characteristic polynomials p_1 and p_2 such that $\langle u \rangle = \langle u^1 \rangle + \langle u^2 \rangle$.*

Proof. We know that $u_n = \sum_{j=1}^{d} q_j(n)\lambda_j^n$. Let $R(p)$ denote the set of roots of polynomial $\chi_u(x)$. Since p_1 and p_2 do not share a common root i.e. $R(p_1) \cap R(p_2)$ is empty and $R(p_1) \cup R(p_2) = R(p)$, we can rewrite the exponential polynomial solution from Equation 1 as $u_n = \sum_{\lambda_j \in \ R(p_1)} q_j(n)\lambda_j^n + \sum_{\lambda_j \in \ R(p_2)} q_j(n)\lambda_j^n$.

Let us consider the set of LRS defined by the characteristic polynomial p_1 (by fixing all possible initial conditions). This is a vector space and one can see that the set $\{n^i\lambda_j^n : \lambda_j \in \ R(p_1), 0 \le i \le \text{multiplicity of } \lambda_j \text{ in } p_1\}$ describes a basis for this vector space. As $\sum_{\lambda_j \in \ R(p_1)} q_j(n)\lambda_j^n$ is just a linear combination of such terms, it is also a possible LRS with characteristic polynomial p_1, let us call this u_n^1. Similarly $\sum_{\lambda_j \in \ R(p_2)} q_j(n)\lambda_j^n$ defines an LRS u_n^2. Hence u_n can be written as $u_n^1 + u_n^2$. ◀

As none of the inner products in Equation 4 share a root by Lemma 11 we can break the linear recurrence as a sum of linear recurrences. Let $\langle u \rangle = \langle u^1 \rangle + \ldots + \langle u^D \rangle$ where the characteristic polynomial of $\langle u^j \rangle$ is exactly $\prod_{\substack{1 \le a \le b_j \\ gcd(a,b_j)=1}} (x - e^{2\pi i \frac{a}{b_j}})^{\rho_j}$. This is exactly the b_j^{th} cyclotomic polynomial raised to ρ_j. Note that this is a integral polynomial with coefficients bounded by $\mathsf{poly}(||u||)$-many bits. Now, we have the following:

▶ **Lemma 12.** *The first k^3 values of all u^j are $\mathsf{poly}(||u||)$-bit bounded rationals and can be calculated in* P.

Proof. The linear recurrence for u^j has degree $\phi(b_j)\rho_j$. We think of the first $\phi(b_j)\rho_j$ initial values as variables. Fixing them fixes u^j. We can express first k^3 values of u^j as integral combinations of first $\phi(b_j)\rho_j$ values. In this integral combination the weights are $\mathsf{poly}(||u||)$-bit bounded as weight $<$ (sum of coefficients of $u^j)^{k^3}$. Next we argue that these k^3 initial values of the u^j are $\mathsf{poly}(||u||)$-bit bounded rationals. We remember that sum of all u^k is u and we have k initial values of u. We know that $\sum_{j=1}^{D} \phi(b_j)\rho_j = k$ as both LHS and RHS represent number of roots of χ_u. The initial values for these D sequences can be found by setting up a system of k linear equations in k variables and solving them where each the n^{th} equation says that $\sum_{j=1}^{D} u_n^k = u_n$. Note that for u^j only first $\phi(b_j)\rho_j$ values are variables not all k, but all of them can be represented as integral combination of first $\phi(b_j)\rho_j$ values with $\mathsf{poly}(||u||)$-bit bounded weights. Note that since the initial values of $\langle u \rangle$ are given as integers as a part of the input hence they are representable in $\mathsf{poly}(||u||)$-bit. Hence for the linear equations all coefficients are $\mathsf{poly}(||u||)$-bit bounded. Hence the initial values of the D linear recurrences are also obtainable as rationals of bit length at most polynomial in $||u||$. As any of the first k^3 values is expressible as integral combinations of first $\phi(b_j)\rho_j$ values with $\mathsf{poly}(||u||)$-bit bounded weights, hence all of first k^3 values are $\mathsf{poly}(||u||)$-bit bounded. ◀

Now as we had defined P for original linear recurrence u we can define P^j for u^j. Note that $|P^j| \leq b_j < k^3$ and hence polynomially bounded in k unlike $|P|$ for which we could only give an exponential bound. Similar to P coefficients of P^j are also rationals. The degree of any polynomial is P^j is at most the multiplicity which is ρ_j.

▶ **Lemma 13.** *Coefficients of any polynomial in P^j are* $\mathsf{poly}(||u||)$*-bit bounded rationals and can be calculated in* P.

Proof. By the definition of P^j, $u^k_n = P^j_q(n)$ when n is of the form $n = bp + q$ and $0 \leq q < b$. Now we can interpolate to get coefficients of this polynomial. We need ρ_j values to interpolate where one value occurs every b_j terms. By Proposition 9 $b_j \rho_j < k^3$ and by Lemma 12 we know that first k^3 values are $\mathsf{poly}(||u||)$-bit bounded rationals. The other coefficients in the interpolation are of the form n^i where $n < k^3$ and $i < k$ hence they are also bounded by k^{3k} ($\mathsf{poly}(||u||)$-bit). So the interpolated coefficients will also be $\mathsf{poly}(||u||)$-bit bounded rationals. ◀

We are now ready to prove Theorem 8:

Proof. (of Theorem 8) First, notice that any n such that $u_n = 0$, n is a root of one of the polynomials in P. For any of these polynomials the coefficient is the sum of corresponding coefficients in P^j's, which are $\mathsf{poly}(||u||)$-bit bounded rationals by Lemma 13. Hence their sum i.e. coefficient of any polynomial in P is also $\mathsf{poly}(||u||)$-bit bounded and can be calculated P. Note that as mentioned above, this property also does not hold for arbitrary algebraic numbers. Now as the coefficients of all the polynomials in P can be represented by rational numbers in $\mathsf{poly}(||u||)$ bits hence their roots are bounded in magnitude by $2^{\mathsf{poly}(||u||)}$ (unless one of the polynomials is identically 0). As we are only interested in integer roots, this implies that any integer root n of a non-zero polynomial in P can be written in $\mathsf{poly}(||u||)$ bits. For a zero polynomial $P_m \in P$, at $n = m$ $u_n = P_m(m) = 0$ hence $n = m$ is a zero and can be written in $\mathsf{poly}(||u||)$ bits by Lemma 10. In both cases n is therefore a short ($\mathsf{poly}(||u||)$-bit bounded) certificate for the Skolem problem, guessed by an NP machine.

Now observe that for such a n, $u_n = P_m(n)$. As both the coefficients of P_m and n are $\mathsf{poly}(||u||)$-bit bounded hence u_n is also $\mathsf{poly}(||u||)$-bit bounded. Hence the guessed n can be verified in P by observing that $u_n = e_1(M_u^T)^n v$, where M_u^T is the corresponding companion matrix. $e_1(M_u^T)^n v$ can be calculated in P via repeated squaring : Since the companion matrix M also satisfies the characteristic polynomial of the recurrence by Cayley-Hamilton theorem, its entries satisfy the recurrence u_n. Hence the preceding argument that u_n is $\mathsf{poly}(||u||)$-bit bounded, also works for each of these entries of the $(M_u^T)^n$. This proves that $\mathsf{Skolem}_\omega$is in NP. To see that $\mathsf{Pos}_\omega$is in coNP note that we need the following 2 conditions to ensure positivity:

- Since the zeros of all the polynomials in the set P (which is also exponentially bounded in size) lie in the range $[0, 2^{\mathsf{poly}(||u||)}]$, it suffices to check that for all the polynomials evaluated at all the points in this range evaluate to a positive value
- All polynomials in set P are ultimately positive.

For condition 1 we need to ensure $u_n \neq 0$ for all $n \in [1, 2^{\mathsf{poly}(||u||)}]$. As u_n can be calculated in P for such an n, this can be implemented in coNP. We can ensure condition 2 for a P_m by making sure that the first non-zero coefficient in positive. By Lemma 10 we just need to ensure this for $m \in [1, 2^{\mathsf{poly}(||u||)}]$ but as coefficients for any m can be calculated in P we can implement this check also in coNP. Hence Pos_ω is in coNP. UPos_ω requires us to just check condition 2, hence it is also in coNP. ◀

Combining the above theorem with Theorem 6, we obtain our completeness results as stated, i.e., if all characteristic roots of an LRS are roots of unity, then Skolem (resp. Positivity, Ultimate Positivity) for such recurrences is NP-complete (resp. coNP-complete).

4 Integer Polytope Containment Problem

In this section, we consider a new problem on dynamical systems. We start by fixing some notation. A *(convex) polytope* is an intersection of finitely many half-spaces. A polytope is said to be *bounded* if the region enclosed in it is bounded.

▶ **Definition 14** (Integer Polytope Containment Problem)**.** Given a bounded polytope $V_1 \subset \mathbb{Z}^d$ and a (possibly unbounded) polytope $V_2 \subseteq \mathbb{Z}^d$ and a $d * d$ matrix M with integer entries, the Polytope Containment Problem asks if for all $v \in V_1$ (for $v \in \mathbb{Z}^d$), does there exist a positive integer n such that $vM^n \in V_2$.

As before, we restrict ourselves to a subclass of this problem, where the eigenvalues are all complex roots of unity.

▶ **Definition 15** ($\mathsf{Contain}_\omega$)**.** $\mathsf{Contain}_\omega$ is the subclass of Polyhedron Containment Problem when the corresponding matrix M has roots of unity and 0 as eigenvalues.

▶ **Theorem 16.** $\mathsf{Contain}_\omega$ *is* Π_2^P*-hard.*

For definitions of coNP, $\Pi_2^P$and other standard complexity classes, we refer the reader to the excellent text due to Arora and Barak [4]. Interestingly, our proof can be seen as an application or generalization of our earlier technique to obtain the reduction of the Skolem problem from the Subset Sum problem. Indeed, since we use our NP-hard instance of the Skolem for this reduction, it is not clear how we can do a similar lift from the earlier NP-hardness proof of Blondel-Portier [7], or indeed any other existing approach.

The rest of this section forms the proof of the above theorem. We start by considering the following generalized form of the subset sum (GSS) problem, which is known to be Π_2^P-complete [22]. Given two vectors $b = (b_1, \dots b_\ell)$ and $a = (a_1, \dots a_m)$ and $\alpha \in \mathbb{Z}$, for all $x \in \{0,1\}^\ell$, does there exist $y \in \{0,1\}^m$ such that $x \cdot b + y \cdot a = \alpha$?[3] We will also use the set notation $B = \{b_1, \dots b_\ell\}$ and $A = \{a_1, \dots, a_m\}$ when convenient.

Our goal is to reduce this above problem to $\mathsf{Contain}_\omega$. In order to do so, we will use the Subset-sum to Skolem_ω reduction from Section 3. Consider the LRS u_A whose n^{th} term is $\sum_{i=1}^m u_n^i$, where u_n^i is the LRS constructed in Section 3. We can observe the following properties about this LRS:

- **(F1)** Each entry of u_A gives a sum of a subset of elements from A, i.e., $y \cdot a$ for some $y \in \{0,1\}^m$.
- **(F2)** Every subset of sum of elements of A occurs as some entry of u_A.
- **(F3)** The LRS u_A is periodic, i.e., the elements repeat after a certain period (product of the first m-primes to be precise). Thus the bound that they repeat after or the period is exponentially bounded.
- **(F4)** The LRS u_A can be written in matrix form as a matrix M_A such that for all $n \geq 0$, $\langle u_A \rangle_{n+1} = vM^n w$ where v is the first m entries of the LRS and $w = (1, 0, \dots 0, 0)$. Further, the roots of the characteristic polynomial of u_A (which were noted earlier to be roots of unity) are the eigenvalues of M_A. The proof of these facts follows by simple linear algebra and can be found for instance in [25]. Further, we may also observe that

[3] In fact, to be precise, [22] defines the complement of this problem.

the entries in the matrix are exponentially bounded in the input-size of the subset-sum instance and can be computed in poly-time. It follows that the sequence of numbers vM^nw for all $n \geq 0$ satisfy the three properties (F1–F3) listed above.

Given an instance of GSS problem, we will build an instance of $\mathsf{Contain}_\omega$as follows. Define a square matrix G of dimension $\ell+m+2$, as shown below. Note that the eigenvalues of G are all roots of unity and 0. This follows from the fact that G is a block upper triangular matrix hence $det(G - \lambda I) = det(I_{(\ell+1)\times(\ell+1)} - \lambda I_{(\ell+1)\times(\ell+1)})det(M_{m\times m} - \lambda I_{m\times m})det(-\lambda)$, which implies that the eigenvalues are 1, eigenvalues of M and 0. We fix V_1 to be the set of all vectors $\{(x_1, \dots x_\ell, 1, v, 0) \mid x_i \in \{0,1\}, \text{ for all } 1 \leq i \leq \ell\}$. Note that this is a polytope, i.e., an intersection of half spaces. Next, we fix V_2 to be the polytope $\{y \in \mathbb{Z}^{\ell+m+2} \mid y \cdot e_{\ell+m+2} = 0\}$, where $e_{\ell+m+2}$ is the $\ell + m + 2$-dimension vector $(0, \dots 0, 1)$.

$$G = \left[\begin{array}{c|c|c} I_{(\ell+1)\times(\ell+1)} & 0 & \begin{matrix} b_1 \\ b_2 \\ \vdots \\ b_\ell \\ -\alpha \end{matrix} \\ \hline 0 & M_{m\times m} & w \\ \hline 0 & 0 & 0 \end{array}\right]$$

Let $z = (x, 1, v, 0) \in V_1$ for some $x \in \{0,1\}^\ell$. By induction, we obtain that for all $n \geq 1$, $z \cdot G^n = (x, 1, v \cdot M_A^n, x \cdot b - \alpha + v \cdot M_A^{n-1} \cdot w)$. Now GSS has a solution iff for all $x \in \{0,1\}^\ell$, there exists $y \in \{0,1\}^m$ such that $x \cdot b + y \cdot a = \alpha$. From facts above, it follows that for each such $y \in \{0,1\}^m$, there exists $n \geq 0$ such that $y \cdot a = vM^nw$. In other words, GSS has a solution iff for all $x \in \{0,1\}^\ell$, there exists $n \geq 0$ such that $x \cdot b + vM^nw = \alpha$. That is, GSS has a solution iff for all $z \in V_1$, there exists $n \geq 0$ such that $z \cdot G^{n+1} \cdot e_{\ell+m+2} = 0$ iff for all $z \in V_1$, there exists $n' \geq 1$ such that $z \cdot G^{n'} \in V_2$. This gives the solution for our instance of the $\mathsf{Contain}_\omega$problem and completes the proof of correctness of the reduction.

From this we immediately obtain, that the Integer Polytope Containment Problem is Π_2^P hard. Finally, we will show that:

▶ **Theorem 17.** $\mathsf{Contain}_\omega$ *is* Π_2^P*-complete.*

Proof. We have already shown hardness for $\mathsf{Contain}_\omega$ in Theorem 16 so now we only need to show inclusion in Π_2^P. Description size of any integer value $x \in V_1$ i.e. $||x||$ is $\mathsf{poly}(||V_1||)$ where V_1 is a bounded polytope and is specified as intersection of hyperplanes. This because the corner points are solutions of linear equations which is bounded by $\mathsf{poly}(||V_1||)$-bits. Hence all integral points inside are also bounded by $\mathsf{poly}(||V_1||)$-bits. As checking if a particular $x \in V_1$ can be done P we can go over all $x \in V_1$ in coNP. After fixing x, this the problem reduces to Skolem_ω which, by Theorem 8, is in NP. Hence $\mathsf{Contain}_\omega$ is in $\mathsf{coNP}^{\mathsf{NP}} = \Pi_2^P$. ◀

While our hardness results lift to the non-integer case, our containment proofs do not extend immediately to the non-integer case. However, we conjecture that using techniques from [8], we can obtain similar decidability results, for this subclass for rational/real cases.

5 Conclusion

In this paper, we investigate linear recurrence sequences whose characteristic roots which are complex roots of unity. We show that the Skolem problem (resp. positivity, ultimate positivity) restricted to this subclass of LRS is NP-complete (resp. coNP-complete). The lower bound is via a novel reduction from subset sum, which we are also able to extend to show Π_2^P-hardness for a more general yet interesting problem on LRS. Note that this lower bound (as well as the one in [7]), requires LRS to be of arbitrary or unbounded orders. One interesting open question is whether one could show any non-trivial lower bound (e.g., NP-hardness) for LRS of a fixed order.

Our approach for upper-bounds can be extended further to tackle LRS whose characteristic roots are complex roots of any real number, i.e., complex numbers whose phases are rational multiples of π. However, we get more relaxed upper-bounds, without matching lower-bounds. While disappointing, this is not surprising since any improvement in the lower-bound would be a highly remarkable result as commented in the conclusion of [21].

Acknowledgements. We would like to thank the anonymous reviewers for their insightful comments and helpful remarks.

References

1 Manindra Agrawal, S. Akshay, Blaise Genest, and P. S. Thiagarajan. Approximate verification of the symbolic dynamics of markov chains. *J. ACM*, 62(1):2:1–2:34, 2015.

2 S. Akshay, Timos Antonopoulos, Joël Ouaknine, and James Worrell. Reachability problems for markov chains. *Inf. Process. Lett.*, 115(2):155–158, 2015.

3 S. Akshay, Blaise Genest, Bruno Karelovic, and Nikhil Vyas. On regularity of unary probabilistic automata. In *33rd Symposium on Theoretical Aspects of Computer Science, STACS 2016, February 17-20, 2016, Orléans, France*, pages 8:1–8:14, 2016.

4 Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. URL: `http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264`.

5 M. Artin. *Algebra*. Pearson Prentice Hall, 2011. URL: `https://books.google.de/books?id=QsOfPwAACAAJ`.

6 Amir M. Ben-Amram, Samir Genaim, and Abu Naser Masud. On the termination of integer loops. *ACM Trans. Program. Lang. Syst.*, 34(4):16:1–16:24, December 2012.

7 V. D. Blondel and N. Portier. The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. In *Linear Algebra and its Applications*, pages 351–352. Elsevier, 2002.

8 Mark Braverman. Termination of integer linear programs. In *Computer Aided Verification, 18th International Conference, CAV 2006, Seattle, WA, USA, August 17-20, 2006, Proceedings*, pages 372–385, 2006.

9 Ventsislav Chonev, Joël Ouaknine, and James Worrell. The polyhedron-hitting problem. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 940–956, 2015. `doi:10.1137/1.9781611973730.64`.

10 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the complexity of the orbit problem. *J. ACM*, 63(3):23:1–23:18, 2016. `doi:10.1145/2857050`.

11 Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

12 Graham Everest, Alfred J. van der Poorten, Igor E. Shparlinski, and Thomas Ward. *Recurrence Sequences*, volume 104 of *Mathematical surveys and monographs*. American Mathematical Society, 2003. URL: `http://www.ams.org/bookstore?fn=20&arg1=survseries&item=SURV-104`.

13 Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers (5. ed.)*. Clarendon Press, 1995.

14 Dan Kalman. The generalized vandermonde matrix. *Mathematics Magazine*, 57(1):15–21, 1984.

15 Richard M Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103. Springer, 1972.

16 Joël Ouaknine, João Sousa Pinto, and James Worrell. On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 957–969, 2015. `doi:10.1137/1.9781611973730.65`.

17 Joël Ouaknine and James Worrell. Decision problems for linear recurrence sequences. In *Reachability Problems - 6th International Workshop, RP 2012, Bordeaux, France, September 17-19, 2012. Proceedings*, pages 21–28, 2012. `doi:10.1007/978-3-642-33512-9_3`.

18 Joël Ouaknine and James Worrell. On the positivity problem for simple linear recurrence sequences,. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 318–329, 2014. `doi:10.1007/978-3-662-43951-7_27`.

19 Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 366–379, 2014. `doi:10.1137/1.9781611973402.27`.

20 Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 330–341, 2014. `doi:10.1007/978-3-662-43951-7_28`.

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

22 Marcus Schaefer and Christopher Umans. Completeness in the polynomial-time hierarchy: A compendium. *SIGACT news*, 33(3):32–49, 2002.

23 Ashish Tiwari. Termination of linear programs. In *Computer Aided Verification, 16th International Conference, CAV 2004, Boston, MA, USA, July 13-17, 2004, Proceedings*, pages 70–82, 2004.

24 Prasoon Tiwari. A problem that is easier to solve on the unit-cost algebraic RAM. *J. Complexity*, 8(4):393–397, 1992. `doi:10.1016/0885-064X(92)90003-T`.

25 M.Hirvensalo V.Halava, T.Harju and J.Karhumäki. Skolem's problem on the border between decidability and undecidability. In *TUCS Technical Report Number 683*, 2005.