Near-Optimal Complexity Bounds for Fragments of the Skolem Problem

S. Akshay
IIT Bombay, India
akshayss@cse.iitb.ac.in

Nikhil Balaji
University of Oxford, UK
nikhil.balaji@cs.ox.ac.uk

Aniket Murhekar
University of Illinois, Urbana Champaign, Urbana, IL, USA
aniket1602@gmail.com

Rohith Varma
Indian Institute of Technology Palakkad, India
rvarma.kvm@gmail.com

Nikhil Vyas
MIT, Cambridge, MA, USA
nikhilv@mit.edu

Abstract

Given a linear recurrence sequence (LRS), specified using the initial conditions and the recurrence relation, the Skolem problem asks if zero ever occurs in the infinite sequence generated by the LRS. Despite active research over last few decades, its decidability is known only for a few restricted subclasses, by either restricting the *order* of the LRS (upto 4) or by restricting the *structure* of the LRS (e.g., roots of its characteristic polynomial).

In this paper, we identify a subclass of LRS of arbitrary order for which the Skolem problem is *easy*, namely LRS all of whose characteristic roots are (possibly complex) roots of real algebraic numbers, i.e., roots satisfying $x^d = r$ for r real algebraic. We show that for this subclass, the Skolem problem can be solved in $\mathsf{NP}^{\mathsf{RP}}$. As a byproduct, we implicitly obtain *effective* bounds on the zero set of the LRS for this subclass. While prior works in this area often exploit deep results from algebraic and transcendental number theory to get such effective results, our techniques are primarily algorithmic and use linear algebra and Galois theory. We also complement our upper bounds with a NP lower bound for the Skolem problem via a new direct reduction from 3-CNF-SAT, matching the best known lower bounds.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness

Keywords and phrases Linear Recurrences, Skolem problem, NP-completeness, Weighted automata

Digital Object Identifier 10.4230/LIPIcs.STACS.2020.37

Funding This work was partly supported by DST/CEFIPRA/INRIA Associated team EQuaVE.
S. Akshay: Partly supported by DST-INSPIRE Faculty Award [IFA12-MA-17] and SERB Matrices grant MTR/2018/000744.
Nikhil Vyas: Supported by NSF CCF-1909429.

Acknowledgements This research was supported in part by the International Centre for Theoretical Sciences (ICTS) during a visit for participating in the program - Workshop on Algebraic Complexity Theory (Code: ICTS/wact2019/03).

37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020).
Editors: Christophe Paul and Markus Bläser; Article No. 37; pp. 37:1–37:18

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

1 Introduction

A (rational) linear recurrence sequence (LRS) is an infinite sequence of rationals $u_1 \ldots$ such that the n-th term can be written as a linear combination of the previous terms, $u_n = a_1 u_{n-1} + \ldots + a_k u_{n-k}$, where each coefficient a_i is a rational. The number k is called the *order* of the LRS. Once we fix the initial k values, the equation above uniquely determines the infinite sequence. LRS are a fundamental object of study in discrete mathematics, with a rich theory and widespread applications and have been widely investigated. However, some very basic computational questions remain unsolved for the last several decades despite considerable interest. The most well-known of these is the so-called Skolem problem (or Skolem-Pisot problem): given an LRS $\mathbf{u} = \{u_n\}_{n=0}^{\infty}$ with coefficients $\{a_i\}_{i=1}^{k}$ and initial conditions $\{u_i\}_{i=1}^{k}$, does there exist an n such that $u_n = 0$. This problem is known to be NP-hard [9] (see also [3]), but even decidability is open. A fundamental result in this area is the Skolem-Mahler-Lech theorem, which states that the *zero set* of an LRS is a *semi-linear set*[18], i.e, the zero set is the union of a finite set and a finite union of arithmetic progressions. Unfortunately, this nice characterization does not result in an algorithm due its use of *non-effective* techniques [28], and it does not help in deciding if the zero set is non-empty. To obtain decidability of the Skolem problem, researchers have considered restricted classes of LRS, along two broad avenues.

The first is by *restricting the order* of the LRS. Vereshchagin [30] gave an algorithm to decide Skolem problem up to order 4; the computational complexity of this algorithm was analyzed by Chonev, Ouaknine and Worrell (Appendix of [12]) to show that it is in the complexity)[1] class $\mathsf{NP}^{\mathsf{RP}}$, which is contained in the second level of Polynomial Hierarchy (PH). But, no lower bound is known and hence we do not know if these results are tight, even upto the RP-oracle. Indeed, the NP-hardness reductions in [9, 3] do not work when the order is restricted. The second approach to obtaining decidability has been to *restrict the spectral structure* of the LRS. Given an LRS $\mathbf{u}$ of order k, the roots of its characteristic polynomial $x^k - a_1 x^{k-1} \ldots - a_k = 0$, also called characteristic roots, can be used to give a closed form expression for the LRS (see Proposition 1). Restricting the spectral structure of the LRS refers to imposing conditions on these roots, i.e., considering classes of LRS where the characteristic roots have special properties. In [3], it was shown that for LRS whose characteristic roots are complex roots of unity, the Skolem problem is NP-complete. To the best of our knowledge, no efficient bounds (e.g., within the Polynomial Hierarchy) or optimality results are known for the Skolem problem for any other natural non-trivial subclasses (e.g., for simple LRS, where the roots are distinct), even if decidability is known or considered folklore [31, 4, 7, 17].

In this paper, we take a step in this direction, and provide optimal complexity bounds on the Skolem problem for a highly expressive subclass of LRS, obtaining by restricting its spectral structure. More precisely, we consider the class of LRS where all the roots of the characteristic polynomial are roots of real numbers, i.e., λ such[2] that $\lambda^n = r$ for some $n \in \mathbb{N}, r$ real algebraic. We denote this class by LRS(r$\mathbb{R}$) (and by LRS($\mathbb{R}$) the class of LRS with real characteristic roots). Notice that this class considerably extends the subclass in [3], which corresponds to roots of unity, i.e., λ such that $\lambda^n = 1$ for some $n \in \mathbb{N}$. Restricting the spectrum of a polynomial to be reals or roots of reals has been used to recover decidability

[1] RP is the class of problems that admits a randomized polynomial time algorithm with one-sided error
[2] Notice that every complex algebraic number is a root of a quadratic polynomial with real coefficients. However not all complex algebraic numbers are n-th roots of a real number.

across various areas, ranging from hybrid systems [17] to probabilistic verification [4, 1], and weighted automata [7]. Our results allow us to infer strong complexity results on these models, and solves an open problem stated in [7], as discussed later in the paper.

Our contributions: Our main result is that the Skolem problem for LRS(r$\mathbb{R}$) can be solved in $\mathsf{NP}^{\mathsf{RP}}$. Since this class contains LRS over roots of unity, it inherits the NP hardness for Skolem. Now standard [20] derandomization assumptions in computational complexity imply that $\mathsf{P} = \mathsf{RP}$, under which condition, we obtain that our result on Skolem problem for LRS(r$\mathbb{R}$) is tight. To the best of our knowledge, this is the first tight, upto derandomization, complexity bound on the Skolem problem for a class of LRS whose roots may contain arbitrary reals. We also remark that our results combined with the order 4 results (where also an $\mathsf{NP}^{\mathsf{RP}}$ upper bound is obtained in [12]), seem to suggest that when Skolem problem is decidable, it is easy, i.e., in $\mathsf{NP}^{\mathsf{RP}}$.

To understand the difficulty in showing our result, note that while it is a folklore result that the Skolem problem for LRS($\mathbb{R}$) is decidable, standard ideas don't seem to yield even a PSPACE upper bound. The usual way to analyze an LRS is via the *exponential polynomial solution* (Proposition 1), where the coefficients of the exponential polynomials can be shown to be algebraic numbers from a (exponentially) large field extension of $\mathbb{Q}$. A linear combination of these algebraic numbers could be double exponentially small (See for example the work of Tiwari on the sign problem [29] and Allender et al. [5]) and we currently don't have techniques to handle numerical computation in this regime efficiently. Thus, while one does get decidability, none of these approaches seem to immediately provide precise complexity bounds beyond NEXP to the best of our knowledge. Another example comes from a recent work of Fijalkow et al. [17], where to decide the reachability problem for Linear Time Invariant systems (which they also prove to be Skolem-hard) specified by a matrix A, a key step in the algorithm relies on the Jordan block decomposition $P^{-1}DP$ of A to analyse the product $P^{-1}D^nP$ for various values of n. Though the authors do not analyse the complexity of their algorithm, since the matrices P and P^{-1} have algebraic numbers of exponential degree, a similar complexity bottleneck seems unavoidable.

Thus, in order to prove our results, we introduce new techniques to circumvent numerical difficulties that are usually encountered in computations involving irrational numbers, which we believe could be of independent interest. Numerical difficulties arise regularly in problems in computational geometry (for example, the Square roots sum problem [29]), numerical analysis [10] and algorithmic game theory (computing Nash equilibria of 3-player games [15]), to mention a few examples. A key step in our proof is to revisit and strengthen the folklore result (Proposition 1) that LRS correspond precisely to the class of exponential polynomials. We give a refined version (see Lemma 6) of the closed form of the LRS. Using this and appealing to the classical root separation theorems [23], we obtain an $\mathsf{NP}^{\mathsf{RP}}$ algorithm for the Skolem problem over reals, i.e., LRS($\mathbb{R}$) (Theorem 7). We then reduce Skolem problem for LRS(r$\mathbb{R}$) to that of LRS($\mathbb{R}$) in two steps. First we reduce the Skolem problem for LRS(r$\mathbb{R}$) to the Skolem problem for *simple* LRS(r$\mathbb{R}$), i.e., where the roots are assumed to be all distinct. Then we show that we can reduce the Skolem problem for *simple* LRS(r$\mathbb{R}$) to exponentially many instances of the Skolem problem for *simple* LRS($\mathbb{R}$). In doing so, the most technical part is to prove that numerical issues do not surface again after the reduction (Lemma 12).

We may also contrast our techniques with those of earlier results on the Skolem problem. While the authors of [12] also obtain a $\mathsf{NP}^{\mathsf{RP}}$ upper bound for the Skolem problem (only up to order 4), they use Baker's theorem on linear forms in logarithms [6]. Though Baker's theorem seems unavoidable to show decidability for special cases where the characteristic

roots have irrational phases (even here, currently the method can help prove decidability of Skolem problem only for LRS up to order 4), it is potentially an obstacle to prove good complexity bounds since the "effective" version of Baker's theorem has constants that could be double exponentially small as a function of the order of the LRS. Since [12] deal only with constant order LRS, the constants from Baker's theorem do not pose a problem. Since LRS(r$\mathbb{R}$) does not have roots with irrational phases, we can avoid using Baker's theorem and instead rely on elementary linear algebra and Galois theory to obtain a strong lower bound on the zeros of the LRS.

As a final contribution, we also analyze the hardness proof for Skolem to see how it behaves with respect to various parameters. Towards this, we first provide a direct reduction from 3-CNF-SAT for showing the NP-hardness proof. Using this we observe that Skolem is strongly NP-hard with respect to the initial conditions while it is only weakly NP-hard with respect to the coefficients as they seem to blow up in the reduction. Note that this strengthens the lower bound from [3], which only shows weak NP-hardness in both initial conditions and coefficients. We must however point out that a careful analysis of [9] suggests that their indirect reduction, through universality of automata, is also weakly NP-hard wrt coefficients and strongly wrt initial conditions. However, all the three reductions are weakly NP-hard wrt the coefficients of the LRS since in all the reductions the numerical value of the coefficients may require polynomially (in the size of the LRS) many bits to represent.

Other related work. A recent work of Min Sha [25] shows effective bounds for *simple* LRS, when there are one or two dominant roots (and other roots are arbitrary), using Baker's theorem on linear forms of logarithms. The class of LRS considered here are orthogonal to the one in the current paper since they cannot handle the case of repeated complex dominant roots, even if the roots are complex roots of rationals (for which we obtain $\mathsf{NP}^{\mathsf{RP}}$) or roots of unity (for which we have containment in NP by [3]). On the other hand, we require all roots to be roots of reals, even if there is a single dominant root.

2 Preliminaries and notations

We first set up some notation that we use throughout the paper. We denote by $\mathsf{poly}(m)$, any quantity that is bounded from above by $m^{O(1)}$ and by $\exp(m)$ any quantity that is bounded from above by $2^{m^{O(1)}}$. By $\mathbb{Q}_{\exp(m)}$ we denote rational numbers where both the numerator and denominator are bounded by integers of magnitude at most $\exp(m)$. Note that such a number can be represented in binary by a string of length at most $\mathsf{poly}(m)$. Throughout the paper, we say that the magnitude of a rational number being $\exp(m)$-bounded and the rational number being representable by $\mathsf{poly}(m)$-bits interchangeably. For an algebraic number λ, we denote by $\mathbb{Q}_{\exp(m)}(\lambda)$ all the elements of the field extension which are obtained by rational linear combination of powers of λ, where the rationals used in the linear combination are $\exp(m)$-bounded. Also for a field $\mathbb{F}$, we use $\overline{\mathbb{F}}$ to denote its algebraic closure.

We introduce some standard definitions and properties of LRS. For a detailed treatment of LRS, see the book of Evereste et al. [16]. An LRS of order k is a sequence whose n^{th} term is given by $u_n = \sum_{i=1}^{k} a_i u_{n-i}$, where $u_1, \ldots, u_k$ and $a_1, \ldots, a_k$ are respectively called the *initial conditions* and *coefficients* of the LRS. We assume all initial conditions and coefficients to be rational and hence all terms are rational. Such LRS are sometimes called rational LRS, but we will call them just LRS for simplicity, and denote by $\mathbf{u}$ a rational LRS and by u_n the n^{th} term of $\mathbf{u}$.

Given an LRS, its *characteristic polynomial* is $\chi_{\mathbf{u}}(x) = x^k - \sum_{i=0}^{k-1} a_{k-i}x^i = \prod_{j=1}^{g} f_j(x)^{h_j}$, where the latter equality is obtained by factorizing into irreducible square-free factors f_j over $\mathbb{Q}$. We can also break as $\chi_{\mathbf{u}}(x) = \prod_{j=1}^{r}(x-\lambda_j)^{e_j}$, where λ_j is a root, called a characteristic root with multiplicity e_j and $e_j = h_{j'}$ if λ_j is a root of $f_{j'}$. A *perfect field* is one where every irreducible polynomial over the field has distinct roots. It is known that all characteristic zero fields are perfect. As a result, when $\mathbf{u}$ is a rational LRS, all characteristic roots coming from an irreducible factor occur with same multiplicty. An LRS is called *simple* if $e_j = 1$ for all j, i.e., the characteristic roots are distinct.

▶ **Definition 1** (Exponential polynomial). *An exponential polynomial over a field $\mathbb{F}$ is a special bivariate polynomial $P(x,y) \in \mathbb{F}(x,y)$ of the form $P(x,e^x)$. Such a polynomial is a finite polynomial combination of exponentials $E(x) = \sum_{i=1}^{k} p_i(x)e^{\delta_i x}$, where $\delta_i \in \mathbb{F}$ and $p_i(x) \in \mathbb{F}(x)$.*

▶ **Proposition 1** (Exponential polynomial solution [16]). *Given an LRS $\mathbf{u}$, a closed form solution of the n-th term of the LRS is given as a solution to an exponential polynomial, i.e., $u_n = \sum_{j=1}^{r} p_j(n)\lambda_j^n$, where for $j \in [r]$, $\lambda_j \in \mathbb{C}$, $p_j(n) = \sum_{\ell=0}^{e_j-1} c_{j\ell}n^\ell$ are polynomials of degree at most (e_j-1) and $c_{j\ell} \in \bar{\mathbb{Q}}(\lambda_1,\ldots,\lambda_n)$. Note that for a simple LRS we get $u_n = \sum_{j=1}^{r} c_{j0}\lambda_j^n$.*

Let $e = \max_j(e_j)$ be the highest multiplicity. With this, we can rewrite this equation as

$$u_n = \sum_{j=1}^{r}\left(\sum_{\ell=0}^{e_j-1} c_{j\ell}n^\ell\right)\lambda_j^n \tag{1}$$

We call the coefficients $c_{j\ell}$ the *defining coefficients* of the LRS u_n. We denote by m the bit-size needed to describe the LRS, namely the order, coefficients and initial conditions of the LRS, i.e., $m = ||u|| = k + \sum_{i=1}^{k}(\log a_i + \log u_i)$. We refer to m as the *size* of the LRS.

▶ **Proposition 2.** *Given LRS $\mathbf{u}$ of size m, $n \leq \mathsf{poly}(m)$, u_n is $\mathsf{poly}(m)$-bit representable.*

Algebraic numbers. We introduce some basic notions about algebraic numbers, found in any standard text (e.g., Cohen [13]).

▶ **Definition 2** (Algebraic number, Height, Degree). *A complex number α is called* algebraic *if there is a univariate polynomial $p_\alpha(x)$ with rational 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 the maximum value of the coefficients of p_α. The roots of p_α are called the* Galois conjugates *of α.*

▶ **Lemma 3** (Mignotte's Root Separation bound [23]). *If α_i and α_j are roots of an integer polynomial $p(x)$ of degree d and height H, then $|\alpha_i - \alpha_j| > \frac{\sqrt{6}}{d^{\frac{d+1}{2}}H^{d-1}}$*

▶ **Proposition 3.** *If α is an algebraic number of degree d and height H, then the degree and height of α^t are bounded by d and $exp(d)H^{dt}$ respectively for any $t \in \mathbb{N}$.*

We call an algebraic number α, t^{th} primitive root of unity if $\alpha^t = 1$ and for all $i \in \mathbb{N}$, $i, 0 \leq i < t$, $\alpha^i \neq 1$.

3 LRS to Exponential Polynomials : A finer analysis

In this section, we give a refined analysis of the exponential polynomials obtained from LRS, thus strengthening Proposition 1. To do this, we show two lemmas which are possibly of independent interest. The first is a structural lemma, which shows how one can decompose an LRS into a polynomial combination of *simple* LRS, with only a polynomial blow-up in the resulting size.

▶ **Lemma 4.** *[Splitting lemma] Given an (rational) LRS $\boldsymbol{u}$ of size m and order k, we can write $\boldsymbol{u} = \sum_{\ell=0}^{e-1} n^\ell \mathbf{u}^\ell$, with the following properties:*
1. *$\mathbf{u}^\ell$ is a **simple** LRS of order $k_\ell \geq 1$ such that $\sum_{\ell=0}^{e-1} k_\ell = k$.*
2. *The initial conditions and coefficients of $\mathbf{u}^\ell$ are also $\mathsf{poly}(m)$-bit rationals.*

Proof. From equation 1 we have

$$u_n = \sum_{j=1}^{r} \left(\sum_{\ell=0}^{e_j-1} c_{j\ell} n^\ell \right) \lambda_j^n = \sum_{\ell=0}^{e-1} n^\ell \left(\sum_{j:e_j>\ell} c_{j\ell} \lambda_j^n \right) = \sum_{\ell=0}^{e-1} n^\ell u_n^\ell$$

for $e = \max_j(e_j)$ and $u_n^\ell = \sum_{j:e_j>\ell} c_{j\ell}\lambda_j^n$. Note that $\sum_{j:e_j>\ell} c_{j\ell}\lambda_j^n$ is a simple rational LRS because it is an exponential sum. The only λ_j that occur in the expression for u_n^ℓ are the ones with $e_j > \ell$ or the roots of all $f_{j'}$ such that $h_{j'} > \ell$. Hence the characteristic polynomials of u_n^ℓ is $\chi_{\mathbf{u}^\ell}(x) = \prod_{j:h_j>\ell} f_j(x)$. Since $\chi_{\mathbf{u}}(x) = \prod_{j=1}^{g} f_j(x)^{h_j}$ is a rational univariate polynomial, we have that $\chi_{\mathbf{u}^\ell}$ is a product of all those irreducible factors of $\chi_{\mathbf{u}}(x)$ where $h_j > \ell$. Hence the coefficients of the polynomial $\chi_{\mathbf{u}^\ell}(x)$ are all $\mathsf{poly}(m)$-bit bounded since the coefficients of $\chi_{\mathbf{u}}(x)$ can all be written in $\leq m$ bits. Thus in fact the coefficients of each LRS $\mathbf{u}^\ell$ have size $\mathsf{poly}(m)$ bits.

Further the order of $\mathbf{u}^\ell$ is exactly $k_\ell = \ell(\sum_{j:h_j>\ell} deg(f_j))$. Since $deg(\chi_{\mathbf{u}}(x)) = \sum_{j=1}^{g} h_j deg(f_j)$ we have $\sum_{\ell=0}^{e-1} k_\ell = k$ by double counting. We now set up a system of k linear equations with the initial conditions of the LRSs $\mathbf{u}^\ell$ as variables. Each of the k linear equations expresses one initial condition of $\mathbf{u}$ as a linear combination of the initial conditions of $\mathbf{u}^\ell$. This requires us to in turn express the first k terms of $\mathbf{u}^\ell$ as a linear combination of the k_ℓ initial terms of $\mathbf{u}^\ell$ (variables in our system).

Suppose $u_n^\ell = \sum_{i=1}^{k_\ell} a_i u_{n-i}^\ell$ is the recurrence equation for $\mathbf{u}^\ell$, with $u_1^\ell, \ldots, u_{k_\ell}^\ell$ being the initial conditions, and $a_1, \ldots, a_{k_\ell}$ the coefficients of the recurrence. We first express u_n^ℓ for $k_\ell < n \leq k$ in terms of the initial values as $u_n^\ell = c_1 u_1^\ell + \cdots + c_k u_{k_\ell}^\ell$ by applying the recurrence repeatedly. The constants c_i are $\mathsf{poly}(m)$-bit bounded, since $c_i < (a_1 + a_2 + \cdots + a_{k_\ell})^n$. Thus $c_i < (k_\ell \cdot 2^{\mathsf{poly}(m)})^n \leq (m \cdot 2^m)^k = 2^{\mathsf{poly}(m)}$, since we have seen that each a_i is $\mathsf{poly}(m)$-bit bounded. Hence we have a linear system with k equations and k variables, the initial conditions of each $\mathbf{u}^\ell$. Further all constants in the linear systems are $\mathsf{poly}(m)$-bit bounded, and thus we get that all initial conditions of each $\mathbf{u}^\ell$ are also $\mathsf{poly}(m)$-bit bounded. ◀

Our second step is to show that for a *simple* LRS, the coefficients of the exponential polynomial solution are exponentially bounded (and poly in the bit representation).

▶ **Lemma 5.** *Let $\boldsymbol{u}$ be a simple LRS of order k and size m, whose exponential polynomial solution is given by $u_n = \sum_{i=1}^{k} c_i \lambda_i^n$ and initial conditions are $u_1, \ldots, u_k$. Then the coefficients c_i in the exponential polynomial solution are uniquely determined and have the property $c_i \in \mathbb{Q}_{\exp(m)}(\lambda_i)$. That is, c_i are bounded in magnitude by $\frac{1}{2^{\mathsf{poly}(m)}} \leq c_i \leq 2^{\mathsf{poly}(m)}$ for all $i \in [k]$.*

Proof. We proceed by interpolation. We set up a system of linear equations by substituting $n = 1, 2, \ldots, k$. We get, $Vc = U$, where V is the classical Vandermonde matrix given by $V_{ij} = \lambda_j^i$, for $1 \leq i, j \leq k$ and $c = [c_1 c_2 \ldots c_k]^T$ and $U = [u_1 u_2 \ldots u_k]^T$. Now we have $c = V^{-1}U$, and in fact c_i is given by the inner product $\sum_{j=1}^{k} V_{ij}^{-1} u_j$. Since $U \in \mathbb{Q}^{k\times 1}$, to prove the claim, it suffices to show that $V_{ij}^{-1} \in \mathbb{Q}(\lambda_i)$ for $j \in [k]$. To this end, we start with the following well-known (See for example [21], Exercise 40 in Section 1.2.3, wherein the expression is attributed to De Moivre [14]) formula for the inverse of the Vandermonde matrix given by $V = (b_{i,j})_{1\leq i,j\leq k}$ where

$$b_{ij} = \begin{cases} (-1)^{j-1} \left(\dfrac{\displaystyle\sum_{\substack{1 \leq \ell_1 < \ldots < \ell_{k-j} \leq k \\ \ell_1, \ldots, \ell_{k-j} \neq i}} \lambda_{\ell_1} \cdots \lambda_{\ell_{k-j}}}{\lambda_i \displaystyle\prod_{\substack{1 \leq \ell \leq k \\ \ell \neq i}} (\lambda_\ell - \lambda_i)} \right) & : 1 \leq j < k \\ \dfrac{1}{\lambda_i \displaystyle\prod_{\substack{1 \leq \ell \leq k \\ \ell \neq i}} (\lambda_i - \lambda_\ell)} & : j = k \end{cases}$$

First let's consider the denominator. As $\chi_u(x) = x^k - a_{k-1}x^{k-1} + \cdots + a_0 = \prod_{i\in[k]} (x - \lambda_i)$ its derivative $\chi'_u(x) = kx^{k-1} - (k-1)a_{k-1}x^{k-2} + \cdots + a_1 = \sum_{i\in[k]} \prod_{j\in[k], j\neq i} (x - \lambda_j)$. Now we observe that the denominator is just $\lambda_i \chi'_u(\lambda_i) \in \mathbb{Q}_{exp(m)}(\lambda_i)$ as a_i's are m bit rationals.

Now notice that all elements of the k-th column of the Vandermonde matrix is just 1 scaled by a $\mathsf{poly}(m)$-bit number. The $(k-1)$-th column is given by,

$$b_{i,k-1} = (-1)^{k-2} \sum_{1\leq \ell_1 \leq k; \ell_1 \neq i} \lambda_{\ell_1} = (-1)^{k-2}(a_{k-1} - \lambda_i)$$

where a_{k-1} is the coefficient of x^{k-1} in the characteristic polynomial of the recurrence via Vieta's identities [32].

Similarly we use the fact that the coefficient of x^{k-2} in the characteristic polynomial is the elementary symmetric polynomial of its roots (namely the $\{\lambda_i\}_{i=1}^k$) and rewrite the expression of the Vandermonde inverse above to get

$$\begin{aligned} b_{i,k-2} &= (-1)^{k-3}\Big(\sum_{1\leq \ell_1, \ell_2 \leq k; \ell_1, \ell_2 \neq i} \lambda_{\ell_1}\lambda_{\ell_2} \Big) = (-1)^{k-3}\Big(a_{k-2} - \lambda_i \sum_{1\leq \ell \leq k; \ell \neq i} \lambda_\ell\Big) \\ &= (-1)^{k-3}(a_{k-2} - (-1)^{k-1}\lambda_i(a_{k-1} - \lambda_i)) \end{aligned}$$

Proceeding inductively, let us assume that $b_{i,j+1} \in \mathbb{Q}(\lambda_i)$. Let $e_k^j(x_1, \ldots, x_k)$ denote the j-th elementary symmetric polynomial in the variables $\{x_1, \ldots, x_k\}$. Now we have,

$$\begin{aligned} b_{i,j} &= \left((-1)^{j-1} \sum_{\substack{1 \leq \ell_1 < \ldots < \ell_{k-j} \leq k \\ \ell_1, \ldots, \ell_{k-j} \neq i}} \lambda_{\ell_1} \cdots \lambda_{\ell_{k-j}} \right) \\ &= (-1)^{j-1}(e_k^j(\lambda_1, \ldots, \lambda_k) - \lambda_i b_{i,j+1}) \\ &= (-1)^{j-1}(a_{k-j} - \lambda_i b_{i,j+1}) \end{aligned}$$

which indeed shows that $b_{i,j} \in \mathbb{Q}(\lambda_i)$.

To see that $\frac{1}{2^{\mathcal{O}(m)}} \leq c_i \leq 2^{\mathcal{O}(m)}$, just notice that c_i is obtained as a rational linear combination of powers of λ_i. Since λ_i are the roots of the characteristic polynomial of the LRS we started out with, their magnitude is upper bounded by $2^{\mathcal{O}(m)}$ (which is also the

height of the characteristic polynomial) and lower bounded by $1/2^{\mathcal{O}(m)}$ (to see this just notice that if α is a root of $\chi_u(x)$, then $1/\alpha$ is a root of $x^k\chi_u(1/x)$, where k is the degree of $\chi_u(x)$). This concludes the proof. ◀

Armed with these lemmas, we are now able to refine Proposition 1 considerably. Most standard references on the subject [31, 16] observe that the coefficients $c_{j\ell}$ reside in a finite extension of the rationals, namely $\bar{\mathbb{Q}}(\lambda_1, \ldots, \lambda_n)$. We have the following

▶ **Lemma 6.** *Given a LRS* $\boldsymbol{u} = \langle u_n \rangle$*, the exponential polynomial solution is:* $u_n = \sum_{j=1}^{r} p_j(n)\lambda_j^n$ *where* $p_j(n) = \sum_{\ell=0}^{e_j-1} c_{j\ell}n^\ell$*. Then, the defining coefficients* $c_{j\ell} \in \mathbb{Q}_{\exp(m)}(\lambda_j)$*, where* m *is the size of the given LRS instance.*

Proof. We want to show here that all the coefficients appearing in the polynomials $p_j(n)$ in the exponential polynomial solution belong to $\mathbb{Q}(\lambda_j)$ and are expressible in $\mathsf{poly}(m)$-bits. To show this we rely on Lemmas 4 and 5. When the LRS is simple, we have from Lemma 5 that each coefficient c_i in the exponential polynomial solution $u_n = \sum_{j=1}^{r} c_j\lambda_j^n$ belongs to $\mathbb{Q}_{\exp(m)}(\lambda_j)$. From Lemma 4, we can write $\mathbf{u} = \sum_{i=0}^{e-1} n^i\mathbf{u^i}$, where each $\mathbf{u^i}$ is a simple LRS of order d_i whose initial conditions and recurrence coefficients belong to $\mathbb{Q}_{\exp(m)}$. Let $u_n^i = \sum_{\ell'=1}^{d_i} c_{i\ell'}\lambda_{i\ell'}^n$. From Lemma 5, we have that each $c_{i\ell'} \in \mathbb{Q}_{\exp(m)}(\lambda_{i\ell'})$, since size of $\mathbf{u^i}$ is also $\mathsf{poly}(m)$. Together with Equation 1, we have: $u_n = \sum_{j=1}^{r}\left(\sum_{\ell=0}^{e_j-1} c_{j\ell}n^\ell\right)\lambda_j^n = \sum_{i=0}^{e-1} n^i\left(\sum_{\ell'=1}^{d_i} c_{i\ell'}\lambda_{i\ell'}^n\right)$

Note from the expression on the left that $c_{j\ell}$ is exactly the coefficient of $n^\ell\lambda_j^n$. By comparing the two expressions, we see that the coefficient of $n^\ell\lambda_j^n$ in the expression on the right is exactly $c_{i\ell'}$ where $i = \ell$ and $\lambda_{i\ell'} = \lambda_j$. Thus we have that each $c_{j\ell} \in \mathbb{Q}_{\exp(m)}(\lambda_j)$, since we noted that each $c_{i\ell'} \in \mathbb{Q}_{\exp(m)}(\lambda_{i\ell'})$. ◀

The lemma above is implicit in the work of Cai [11] on computing Jordan forms of matrices. However, we give a direct proof using elementary techniques. The main purpose of Lemma 6 is to provide a good upper and lower bound on the magnitude of the coefficients of $p_j(n)$ in the exponential polynomial solution to *any* LRS. While, this is of no consequence with respect to decidability, as we elaborate in the forthcoming sections, it affects the computational complexity of the problem considerably.

4 Real characteristic roots

In this section we analyze the exact complexity of the Skolem problem for LRS($\mathbb{R}$) and obtain an upper bound of $\mathsf{NP}^{\mathsf{RP}}$.

▶ **Theorem 7.** *Given an LRS* u *with real characteristic roots, Skolem problem is decidable in* $\mathsf{NP}^{\mathsf{RP}}$

Proof. Let $\mathbf{u}$ be a LRS of order k with distinct (not considering repeated) roots $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$. Let m denote the number of bits required to specify the LRS $\mathbf{u}$. We first assume that all roots are positive. We then show a decision procedure for zero testing in this case by showing that there is an exponential bound after which all terms of the LRS are non-zero, and thus it is enough to only consider terms before this bound. In fact, we show this for a class of real exponential polynomials:

▶ **Lemma 8.** *Consider a real exponential polynomial* $\mathbf{u}$ *given by* $u_n = \sum_{j=1}^{r} p_j(n)\lambda_j^n$ *s.t.,*

1. $\lambda_j \in \mathbb{R}^+$ *are the (distinct) absolute values of the roots of a polynomial* $\chi_u(x)$ *whose coefficients are expressible in* m *bits,*
2. *the coefficients of all the polynomials* $p_j(n)$ *are expressible in* $\mathsf{poly}(m)$ *bits,*

3. *r and the degrees of each $p_j(n) \leq m$.*
where m is a size parameter. Then there exists $N = 2^{m^{\mathcal{O}(1)}}$ such that either (i) for all $n > N$, $u_n > 0$, or (ii) for all $n > N$, $u_n < 0$.

Proof. Note first that the number of bits required to specify the real exponential polynomial as the coefficients of $p_j(n)$, λ_j's and r is $\mathsf{poly}(m)$. Let us assume $\lambda_1 > \lambda_2 > \cdots > \lambda_r > 0$. Now we can write:

$$\frac{u_n}{\lambda_1^n} = p_1(n)\left(\frac{\lambda_1}{\lambda_1}\right)^n + \sum_{j=2}^{r} p_j(n)\left(\frac{\lambda_j}{\lambda_1}\right)^n = p_1(n)1^n + \sum_{j=2}^{r} p_j(n)\rho_j^n$$

where $\rho_j = \lambda_j/\lambda_1$ and $\rho_j \in (0,1)$ for $2 \leq j \leq r$. Let $r(n) = \sum_{j=2}^{r} p_j(n)\rho_j^n$. We first place bounds on $r(n)$:

▷ Claim 9. There exist $\epsilon \in (0,1)$ and N, where $1/\epsilon = 2^{m^{\mathcal{O}(1)}}$ and $N = 2^{m^{\mathcal{O}(1)}}$ such that for every $n > N$, $|r(n)| < (1-\epsilon)^n$.

Proof. Note that $|r(n)| \leq \sum_{j=2}^{r} |p_j(n)|{\rho_j}^n$. We are considering a class of real exponential polynomials where the degree of any polynomial p_j is at most m, and that for every $j \in [r]$, the defining coefficients of $p_j(n)$ are upper and lower bounded by numbers expressible in $\mathsf{poly}(m)$-bits. Hence the height of $p_j(n)$ is $2^{\mathcal{O}(m)}$, and putting the height and degree bounds together, we can upper and lower[3] bound $|p_j(n)|$ by $2^{\mathcal{O}(m)}n^m$.

Now we are left with obtaining bounds on ρ_j to have a bound on $r(n)$. Consider a polynomial χ'_u which has roots $1, \rho_2, \ldots, \rho_r$. The roots of χ'_u are the roots of the polynomial χ_u scaled by a constant factor $1/\lambda_1$. Since χ_u has size $\mathcal{O}(m)$, so does χ'_u. Thus bounds on its degree $d = \mathcal{O}(m)$ and height $H = 2^{\mathcal{O}(m)}$ follow. We now use Mignotte's root separation bound (Lemma 3). When applied to χ'_u this gives: $|1-\rho_j| > \frac{\sqrt{6}}{d^{(d+1)/2}H^{d-1}} = \frac{1}{2^{m^{\mathcal{O}(1)}}}$. Since $\rho_j \in (0,1)$, we have ${\rho_j}^n < (1-2^{-m^{\mathcal{O}(1)}})^n$. Now observe that,

$$|r(n)| = \sum_{j=2}^{r} |p_j(n)||\rho_j|^n \leq \sum_{j=2}^{r} 2^{\mathcal{O}(m)}n^{\mathcal{O}(m)}(1-2^{-m^{\mathcal{O}(1)}})^n$$

We also have that the polynomials $p_j(n)$ for $j \in [n]$ have coefficients upper and lower bounded by values that are expressible in $\mathsf{poly}(m)$-bits. Since an exponential function eventually (after a certain N) dominates a polynomial function, we can find an ϵ such that $|r(n)| < (1-\epsilon)^n$ for all $n > N$. Since the degree of the polynomial is $\mathsf{poly}(m)$, the height of the polynomial is $\mathsf{poly}(m)$-bit bounded, and the base of the (decaying) exponential function is $(1-2^{-m^{\mathcal{O}(1)}})$, $1/\epsilon$ and N are exponentially bounded in m. ◁

We now proceed to prove Lemma 8. The n-th term of the sequence is given by: $\frac{u_n}{\lambda_1^n} = p_1(n) + r(n)$. From Claim 9, there exist $\epsilon \in (0,1)$ and N_1, where $1/\epsilon = 2^{m^{\mathcal{O}(1)}}$ and $N_1 = 2^{m^{\mathcal{O}(1)}}$ such that for every $n > N_1$, $|r(n)| < (1-\epsilon)^n$. We also know from Lemma 6 that the coefficients of $p_1(n)$ are $\mathsf{poly}(m)$-bit bounded. Thus, similar to the proof of Claim 9, we can find an exponentially bounded $N_2 = 2^{m^{\mathcal{O}(1)}}$ such that for all $n > N_2$, $|p_1(n)| > (1-\epsilon)^n$. Note here that Lemma 6 was crucial in obtaining the exponential bound on N_2, since without

[3] Notice that just an upper bound is not sufficient, as since the coefficient are algebraic numbers, it might be the case that the coefficients are too small, which might hurt the complexity of our algorithm. However this turns out not to be the case, thanks to Lemma 6

it only a double exponentially smaller lower bound on the coefficients of $p_1(n)$ is known, which does not translate to an exponential bound on N_2.

Putting these two together, we observe that if $p_1(n)$ has a positive leading coefficient, we have that for all $n \geq \mathsf{max}\{N_1, N_2\}$, $u_n > p_1(n) - |r(n)| > (1-\epsilon)^n - (1-\epsilon)^n > 0$. If $p_1(n)$ has a negative leading coefficient, then consider $-u_n = q(n) - r(n)$, where $q(n) = -p(n)$ has a positive leading coefficient, and again, we can have that for all $n \geq \mathsf{max}\{N_1, N_2\}$, $-u_n > 0$. This means that all terms of the sequence beyond $N = \mathsf{max}\{N_1, N_2\}$ are either all strictly positive or all strictly negative. ◀

We now show how to decide Skolem problem for LRSs with positive real roots using Lemma 8. Recall that m is the size of the LRS. Now observe that

1. u_n is an exponential polynomial solution (see Equation 1).
2. λ_j's are positive reals, and roots of $\chi_u(x)$, the characteristic polynomial of the LRS. Since the coefficients of $\chi_u(x)$ are part of the input, they are expressible in m bits.
3. r and the degrees of the polynomials are all $\leq k$, which in turn is $\leq m$.

Thus we can apply Lemma 8. Thus we see that deciding if there is an n such that $u_n = 0$ amounts to checking the only terms u_n where $n < N$, where N is the exponentially bounded constant in Lemma 8. Since N can be represented in polynomial number of bits in the size of the input LRS, we can guess $0 \leq n < N$ in NP and check if $u_n = 0$ by iterated squaring of the companion matrix of the LRS, which can be represented as a small circuit. We can now invoke the randomized algorithm for circuit zero testing (commonly called EqSLP, see for example [5]). This places Skolem problem for LRSs with positive real characteristic roots in $\mathsf{NP}^{\mathsf{EqSLP}}$ which is in $\mathsf{NP}^{\mathsf{RP}}$, since $\mathsf{EqSLP} \subseteq \mathsf{coRP}$. To reduce the general case of real roots (LRS with both positive and negative real roots) to the case of positive real roots discussed above, notice that since reals form an ordered field, any LRS with real characteristic roots can have at most two dominant roots: say λ_1 and $-\lambda_1$. We have: $u_n = p_1(n)\lambda_1^n + p_2(n)(-\lambda_1)^n + \sum_{j=3}^{r} p_j(n)\lambda_j^n$. Consider the sequences $\mathbf{v}$ and $\mathbf{w}$ defined by $v_n = u_{2n}$ and $w_n = u_{2n+1}$

$$v_n = u_{2n} = (p'_1(n) + p'_2(n))(\lambda_1^2)^n + \sum_{j=3}^{r} p'_j(n)(\lambda_j^2)^n$$

$$w_n = u_{2n+1} = (p''_1(n) + p''_2(n))(\lambda_1^2)^n + \sum_{j=3}^{r} p''_j(n)(\lambda_j^2)^n$$

where $p'_1(n) = p_1(2n)$, $p''_1(n) = \lambda_1 p_1(2n)$, and so on. Since the expressions for v_n and w_n are in the exponential polynomial form, the sequences $\mathbf{v}$ and $\mathbf{w}$ are linear recurrences. Observing the exponential polynomial solution further reveals their characteristic roots are squares of the characteristic roots of $\mathbf{u}$, and thus are positive reals. Notice that deciding Skolem problem for $\mathbf{u}$ is equivalent to deciding Skolem problem for both $\mathbf{v}$ and $\mathbf{w}$. Since the LRSs $\mathbf{v}$ and $\mathbf{w}$ can be computed in polynomial time from $\mathbf{u}$, and using the fact that Skolem problem can be decided in $\mathsf{NP}^{\mathsf{RP}}$ for LRSs with positive real roots, we have that Skolem problem for LRSs with real algebraic characteristic roots is also in $\mathsf{NP}^{\mathsf{RP}}$. ◀

5 Roots of reals

In this section, we use the results proved in the previous sections, to finally show the following main result of this paper.

▶ **Theorem 10.** *Skolem problem for* $\mathrm{LRS}(\mathrm{r}\mathbb{R})$ *can be decided in* $\mathsf{NP}^{\mathsf{RP}}$

At a high level, the main idea is to show that the Skolem problem for an LRS $\mathbf{u} \in \text{LRS}(\text{r}\mathbb{R})$ can be reduced to testing for zeros of a set of *real* exponential polynomials, for which we can then appeal to Lemma 8. We divide the proof into two parts: first we show the result for *simple* LRS and then, we use splitting lemma (Lemma 4) to solve the general case. We start with a technical lemma about the phases of roots in a $\text{LRS}(\text{r}\mathbb{R})$ instance:

▶ **Lemma 11.** *For an irreducible polynomial which factors as* $p(x) = \prod_{j=1}^{d}(x - \alpha_j\omega_j)$*, where* $\alpha_j \in \overline{\mathbb{Q}} \cap \mathbb{R}$ *and* $\omega_j = e^{\frac{2\pi\iota s_j}{t_j}}$ *is a* t_j*-th primitive root of unity, we have for all* $j, t_j = O(d^2 \log d)$ *and* $lcm\{t_j\}_{j=1}^{d} = 2^{O(d \log d)}$*.*

Proof. Let ω be some ω_j, which is the $t_j = t^{th}$ primitive root of unity. Since $\alpha\omega$ is a root of an irreducible polynomial of degree d, we have $deg_{\mathbb{Q}}(\alpha\omega) = d$. Notice that $\alpha\omega^{-1}$ is a conjugate of $\alpha\omega$ and hence also satisfies $deg_{\mathbb{Q}}(\alpha\omega^{-1}) = d$. Hence we have $[\mathbb{Q}(\alpha\omega, \alpha\omega^{-1}) : \mathbb{Q}] \leq d^2$, by the multiplicative property of field extensions. This gives $(\alpha\omega)/(\alpha\omega^{-1}) = \omega^2 \in \mathbb{Q}(\alpha\omega, \alpha\omega^{-1})$. Hence $deg_{\mathbb{Q}}(\omega) \leq 2d^2$. But $\phi(t) = deg_{\mathbb{Q}}(\omega)$. Now, a well-known lower bound for the Euler totient function is $\phi(t) \geq \Omega\left(\frac{t}{\log t}\right)$ (see for example Theorem 328 in [19]) and together with $\phi(t) \leq 2d^2$, this yields $t = O(d^2 \log d)$ and the LCM bound follows. ◀

The lemma above can be considered as a weak generalization of the well-known fact that any polynomial with degree-d^2 cannot have as one of its roots a d'-th primitive root of unity, whenever $d' > d$.

5.1 The case of Simple LRS($\text{r}\mathbb{R}$)

We first set up some notation. Let $\mathbf{v} = \{v_n\}_{n\geq 0} \in \text{LRS}(\text{r}\mathbb{R})$ be a simple LRS of order k having size m. Let the characteristic roots of the LRS $\mathbf{v}$ be $\alpha_j\omega_j$, for $j \in [k]$, where $\alpha_j \in \mathbb{R}^+$, and $\omega_j = e^{\iota 2\pi s_j/t_j}$ (where $s_j \in \mathbb{Z}$ and $t_j \in \mathbb{Z}^+$ and $\mathsf{lcm}(|s_j|, t_j) = 1$) is the t_j^{th} primitive root of unity. For a multiset S, define $\mathsf{supp}(S)$ to be the set obtained from S. Let A be the set of absolute values of the characteristic roots, $A = \mathsf{supp}(\{\alpha_j\}_{j=1}^{k}) = \{\beta_j\}_{j=1}^{k'}$. Define the set $T = \mathsf{supp}(\{t_j\}_{j=1}^{k})$. Let $K = \mathsf{lcm}(\{t \mid t \in T\})$. We call a number from the set $\{0, \ldots, K-1\}$ as the *global phase* of the LRS and numbers from T as the *local phases*.

The main idea behind our algorithm is that once a global phase ℓ is fixed, the terms of the LRS v_n where $n \equiv \ell \mod K$ can be captured by a real exponential polynomial $q_\ell(n)$. More formally we have the following,

▶ **Lemma 12.** *Given a simple LRS* $\boldsymbol{v} \in \text{LRS}(\text{r}\mathbb{R})$*, for every* $\ell \in \{0, 1, \ldots, K-1\}$*, there exists a* real *exponential polynomial* $q_\ell(n) = \sum_{j=1}^{k'} c_{\ell j}\beta_j^n$ *such that* $v_n = q_\ell(n)$ *whenever* $n \equiv \ell \mod K$*. Further* $c_{\ell j} \in \mathbb{Q}_{\exp(m)}(\beta_j)$ *and can be computed in* $\mathsf{poly}(m)$ *time.*

The crucial point to establish is that the coefficients of this real exponential polynomial are also bounded by polynomially many bits. Once we have this, checking the existence of a Skolem zero reduces to zero testing of a real exponential polynomial, as was done in Lemma 8. Armed with Lemma 12, we can now prove

▶ **Theorem 13.** *The Skolem problem for simple LRS from the class* $\text{LRS}(\text{r}\mathbb{R})$ *is decidable in* $\mathsf{NP}^{\mathsf{RP}}$*.*

Proof. The following algorithm takes as input the LRS $\mathbf{v}$ and outputs "yes" if and only if $v_n = 0$ for some n:

1. Guess the global phase, i.e., a value ℓ from $\{0, 1, \ldots, K-1\}$.

2. Compute a real exponential polynomial $q_\ell(n) = \sum_{j=1}^{k'} c_{\ell j}\beta_j^n$ such that $v_n = q_\ell(n)$ for $n \equiv \ell \mod K$. We will show in Lemma 12 below that each $c_{\ell j} \in \mathbb{Q}_{exp(m)}(\beta_j)$ and can be computed in $\mathsf{poly}(m)$ time.
3. Use the algorithm of Lemma 8 to guess a zero n' of the real exponential polynomial $q_\ell(n)$. If $q_\ell(n') = 0$ and $n' \equiv \ell \mod K$, then output "yes", else output "no".

Correctness. Suppose there is a Skolem zero n' such that $v_{n'} = 0$, and that $n' \equiv \ell \mod K$. Then the algorithm correctly guesses ℓ and the zero n' of $q_\ell(n)$. On the other hand if the algorithm finds an n' in step 3 such that $n' \equiv \ell \mod K$, and $q_\ell(n') = 0$, then by Lemma 12 it holds that $v_{n'} = q_\ell(n') = 0$. Thus n' is a Skolem zero.

Complexity. Guessing ℓ, n' and computing $q_\ell(n)$ can be done in polynomial time. This is due to Lemma 12 and because $\ell \leq 2^{\mathsf{poly}(k)}$ due to Lemma 11. Due to the bounds established in Lemma 8, checking if $n' \equiv \ell \mod K$ and if $q_\ell(n') = 0$ can be done in RP. Thus, this algorithm runs in $\mathsf{NP}^{\mathsf{RP}}$. ◀

It remains to prove Lemma 12.

Proof of Lemma 12. We fix some $\ell \in \{0, 1, \ldots, K-1\}$. From the exponential polynomial solution (Definition 1), we have $v_n = \sum_{j=1}^{k} c_j(\alpha_j\omega_j)^n$. For $n \equiv \ell \mod K$, we have that $n \equiv \ell \mod t$, for every $t \in T$. Thus,

$$v_n = \sum_{j=1}^{k} c_j\omega_j^n\alpha_j^n = \sum_{j=1}^{k} c_j\omega_j^{\ell \bmod t_j}\alpha_j^n$$

Grouping terms by same α_j's, we have that

$$v_n = \sum_{j=1}^{k'} \Big(\sum_{j':\alpha_{j'}=\beta_j} c_{j'}\omega_{j'}^{\ell \bmod t_{j'}} \Big)\beta_j^n \tag{2}$$

Now we show that the coefficient of β_j^n in the above expression is in $\mathbb{Q}_{exp(m)}(\beta_j)$ for each j. To do this, we first divide up the characteristic roots of the LRS into sets defined as follows, for each $\alpha \in A$ and $t \in T$:

$$S_t^\alpha = \{j \mid \alpha_j = \alpha, \omega_j \text{ is a } t_j^{th} \text{ primitive root of unity s.t. } t_j = t\}$$
$$S_{\preceq t}^\alpha = \{j \mid \alpha_j = \alpha, \omega_j \text{ is a } t_j^{th} \text{ primitive root of unity s.t. } t_j \preceq t\}$$

where $\preceq$ is the partial order given by $a \preceq b \iff a \mid b$. The utility of these sets is that we have $j \in S_{\preceq t}^\alpha$, if and only if $(\alpha_j\omega_j)^t = \alpha^t$. We now show:

▷ Claim 14. For every $\alpha \in A$ and $t \in T$, the constants $c_{\alpha t} = \sum_{j \in S_t^\alpha} c_j\omega_j^\ell$ and $d_{\alpha t} = \sum_{j \in S_{\preceq t}^\alpha} c_j\omega_j^\ell$ are in $\mathbb{Q}_{exp(m)}(\alpha)$, and can be computed in $\mathsf{poly}(m)$ time.

Proof. We first show that $d_{\alpha t} \in \mathbb{Q}_{\exp(m)}(\alpha)$ can be computed in $\mathsf{poly}(m)$-time. Let $\mathsf{supp}(\{(\alpha_j\omega_j)^t \mid j \in [k]\}) = \{\tau_j \mid j \in [h]\}$. We proceed by grouping terms in the exponential polynomial solution for v_n for the first h values of n where $n \equiv \ell \mod t$. Specifically, for each $0 \leq g < h$, we write $\sum_{j=1}^{k} c_j(\alpha_j\omega_j)^{gt+\ell} = v_{gt+\ell}$. We rewrite this equation as follows:

$$\sum_{j=1}^{k} c_j(\alpha_j\omega_j)^{\ell-t}[(\alpha_j\omega_j)^t)^{g+1}] = v_{gt+\ell}$$

Grouping terms according with same $(\alpha_j\omega_j)^t$, we get:

$$\sum_{j=1}^{h}\left(\sum_{j':(\alpha_{j'}\omega_{j'})^t=\tau_j} c_{j'}(\alpha_{j'}\omega_{j'})^{\ell-t}\right)\tau_j^{g+1} = v_{gt+\ell}$$

Denoting by c'_j the expression in the bracket, we see that we have h equations in h variables, namely the c'_j. We get the following linear system, $Tc' = V$, where $T_{ij} = \tau_j^i$ for $1 \le i, j \le h$ and $c' = [c'_1 c'_2 \dots c'_h]^T$ and $V = [v_\ell v_{t+\ell} \dots v_{(h-1)t+\ell}]^T$. Notice that T is a Vandermonde matrix. Also, since we know t is polynomially bounded in k, by Proposition 2 the values $v_\ell, \dots, v_{(h-1)t+\ell}$ are in $\mathbb{Q}_{\exp(m)}$. We can now invoke the following lemma with $\lambda_j = \tau_j$ and $\gamma_j = \alpha_j\omega_j$ to conclude that each constant $c'_j \in \mathbb{Q}_{exp(m)}(\tau_j)$.

▶ **Lemma 15.** *Let u be a sequence of order k, whose exponential polynomial solution is given by $u_n = \sum_{i=1}^{k} c_i\lambda_i^n$ and initial conditions are given by $u_1, \dots, u_k$. Let $\chi(x) = x^{k'} - a_{k'-1}x^{k'-1} + \dots + a_0$ be a polynomial with $a_i \in \mathbb{Q}_{exp(m)}$, roots $(\gamma_j)_{j=1}^{k'}$, $k \le k' \le poly(k)$. Define the set $\{\lambda_i\}_{i=1}^{k}$ from the multiset $\{\gamma_j^t\}_{j=1}^{k'}, t \le \mathsf{poly}(k)$. Then the coefficients c_i in the exponential polynomial solution have the property that $c_i \in \mathbb{Q}_{exp(m)}(\lambda_i)$.*

Proof. For all λ_i there exists a j such that $\lambda_i = \gamma_j^t$. As $t \le \mathsf{poly}(m)$ by Proposition 3 all λ_i's have a monic polynomial over $\mathbb{Q}$ with coefficients from $\mathbb{Q}_{\exp(m)}$.

Let $conj(\gamma)$ be the set of all galois conjugates of γ over $\mathbb{Q}$. Let $\{\delta_i\}_{i=1}^{k''} = \cup_{i=1}^{k'} conj(\lambda_i)$. Each λ_i has degree $\mathsf{poly}(k)$ as it is a $\mathsf{poly}(k)$ power of some γ_j which itself has degree $\mathsf{poly}(k)$. Hence $k'' \le k' \max_i(deg(\lambda_i)) \le \mathsf{poly}(k)$. The product of all the monic polynomials of λ_i's has exactly the list of roots $\{\delta_i\}_{i=1}^{k''}$ with no repeated roots. Also this product has coefficients from $\mathbb{Q}_{\exp(m)}$ as we are multiplying at most $\mathsf{poly}(k) \le \mathsf{poly}(m)$ polynomials of $\mathsf{poly}(k) \le \mathsf{poly}(m)$ degree each having coefficients from $\mathbb{Q}_{\exp(m)}$.

As the set $\{\delta_i\}_{i=1}^{k''}$ is a superset of $\{\lambda_i\}_{i=1}^{k}$, by Lemma 5 we have a unique solution $u_n = \sum_{j=1}^{k''} w_j\delta_j^n$ with $w_j \in \mathbb{Q}_{exp(m)}(\delta_j)$. But as we also have $u_n = \sum_{i=1}^{k} c_i\lambda_i^n$ it must be the case that $w_j = 0$ if $\delta_j \notin \{\lambda_i\}_{i=1}^{k}$ and $w_j = c_i$ when $\delta_j = \lambda_i$ some i. So we have $u_n = \sum_{i=1}^{k} c_i\lambda_i^n$ with $c_i = w_j \in \mathbb{Q}_{exp(m)}(\delta_i) = \mathbb{Q}_{exp(m)}(\lambda_i)$. ◀

We observed that $j \in S^{\alpha}_{\preceq t} \iff (\alpha_j\omega_j)^t = \alpha^t$. Let $\alpha^t = \tau_j$ for some $1 \le j \le h$. Thus all j' for which $(\alpha_{j'}\omega_{j'})^t = \tau_j$ are in fact in $S^{\alpha}_{\preceq t}$. Hence the constant

$$d_{\alpha t} = \sum_{j\in S^{\alpha}_{\preceq t}} c_j\omega_j^\ell = \sum_{j\in S^{\alpha}_{\preceq t}} \frac{c_j(\alpha_j\omega_j)^{\ell-t}(\alpha_j\omega_j)^t}{(\alpha_j)^\ell} = \sum_{j\in S^{\alpha}_{\preceq t}} \frac{c_j(\alpha_j\omega_j)^{\ell-t}\alpha^t}{\alpha^\ell} = c'_j\alpha^{t-\ell}$$

Since $c'_j \in \mathbb{Q}_{exp(m)}(\tau_j) = \mathbb{Q}_{exp(m)}(\alpha^t)$, and $t \le \mathsf{poly}(k)$, by Proposition 3 we have in fact $c'_j \in \mathbb{Q}_{exp(m)}(\alpha)$. Hence $d_{\alpha t} = c'_j(\alpha)^{t-\ell} \in \mathbb{Q}_{exp(m)}(\alpha)$. It is clear that since the expression for c'_j involves $\mathsf{poly}(m)$ operations on $\mathsf{poly}(m)$-sized algebraic numbers, $d_{\alpha t}$ can be computed in $\mathsf{poly}(m)$-time.

We now show that $c_{\alpha t} \in \mathbb{Q}_{\exp(m)}(\alpha)$ and can be computed in $\mathsf{poly}(m)$ time. For the minimal nodes of the partial order $\preceq$, i.e. for prime t, it is the case that $c_{\alpha t} = d_{\alpha t}$. Thus for such t, we directly have that $c_{\alpha t}$ is in $\mathbb{Q}_{exp(m)}(\alpha)$, and can be computed in $\mathsf{poly}(m)$ time.

For any other t we can compute $c_{\alpha t}$ recursively by using the equation:

$$c_{\alpha t} = \sum_{j\in S^{\alpha}_{t}} c_j\omega_j^\ell = \sum_{j\in S^{\alpha}_{\preceq t}} c_j\omega_j^\ell - \sum_{t'\prec t}\sum_{j'\in S^{\alpha}_{t'}} c_{j'}\omega_{j'}^\ell = d_{\alpha t} - \sum_{t'\prec t} c_{\alpha t'}$$

Since for all $t \in T$, $t \leq \mathsf{poly}(k)$, we have that the longest chain in this partial order is of length $O(\log k) = O(\log m)$. Using an inductive argument together with the proof that $d_{\alpha t} \in \mathbb{Q}_{\exp(m)}(\alpha)$, we see that all the relevant quantities appearing in the above equation are in $\mathbb{Q}_{exp(m)}(\alpha)$. This implies that $c_{\alpha t} \in \mathbb{Q}_{\exp(m)}(\alpha)$ and can be computed in $\mathsf{poly}(m)$ time. ◁

We now revisit Equation 2:

$$v_n = \sum_{j=1}^{k'} \Big(\sum_{j' : \alpha_{j'} = \beta_j} c_{j'} \omega_{j'}^{\ell \bmod t_{j'}} \Big) \beta_j^n = \sum_{j=1}^{k'} c_{\ell j} \beta_j^n$$

Here we define $c_{\ell j}$ as the coefficient of β_j^n in Equation 2. Roots with real part equal to β_j with different local phases contribute to $c_{\ell j}$. Separating roots according to different local phases, we have

$$c_{\ell j} = \sum_{j' : \alpha_{j'} = \beta_j} c_{j'} \omega_{j'}^{\ell \bmod t_{j'}} = \sum_{t \in T} \sum_{j' \in S_t^{\beta_j}} c_{j'} \omega_{j'}^{\ell \mod t} = \sum_{t \in T} c_{\beta_j t}$$

Now it follows directly from Claim 14 that for every j, $c_{\ell j} \in \mathbb{Q}_{exp(m)}(\beta_j)$ and can be computed in $\mathsf{poly}(m)$ time since $t \leq \mathsf{poly}(k)$. This establishes Lemma 12. ◀

5.2 The general case

We now consider the general case of LRS in LRS(r$\mathbb{R}$) and show:

▶ **Theorem 16.** *Skolem problem for the class* LRS(r$\mathbb{R}$) *is decidable in* $\mathsf{NP}^{\mathsf{RP}}$.

Proof. In the general case, the exponential polynomial solution (Definition 1) for a LRS $\mathbf{u} \in$ LRS(r$\mathbb{R}$) takes the following form: $u_n = \sum_{j=1}^{r} p_j(n)(\alpha_i \omega_j)^n$ where $p_j(n) = \sum_{i=0}^{e_j - 1} p_{ji} n^i$. From Lemma 5 and 6, we know that every defining coefficient $p_{ji} \in \mathbb{Q}_{\exp(m)}(\alpha_j \omega_j)$. We can now use Lemma 4 to decompose LRS $\mathbf{u}$ as: $u_n = \sum_{i=0}^{e-1} n^i \mathbf{u^i}$ where each $\mathbf{u}^i$ is a simple LRS in LRS(r$\mathbb{R}$). As in proof of Theorem 13, once we fix $\ell \in \{0, 1, \ldots, K-1\}$, whenever $n \equiv \ell \bmod K$, we have from Lemma 12 that we can write $u_n^i = \sum_{j=1}^{k'} c_{\ell ij} \beta_j^n$ for every LRS $\mathbf{u^i}$, where each $c_{\ell ij} \in \mathbb{Q}_{exp(m)}(\beta_j)$. Thus, whenever $n \equiv \ell \bmod K$, we have: $u_n = \sum_{i=0}^{e-1} n^i \left(\sum_{j=1}^{k'} c_{\ell ij} \beta_j^n \right)$. ◀

Observe that the right hand side of the equation above is a real exponential polynomial $q_\ell(n)$ and $c_{\ell ij}$ is the coefficient of $n^i \beta_j^n$, where $c_{\ell ij} \in \mathbb{Q}_{exp(m)}(\beta_j)$. This allows us to invoke Lemma 8 to accomplish zero testing of the exponential polynomial $q_\ell(n)$ in $\mathsf{NP}^{\mathsf{RP}}$. We note that if there is an n such that $q_\ell(n) = 0$ and $n \equiv \ell \mod K$ then $u_n = 0$. On the other hand if there is an n such that $u_n = 0$, then $q_\ell(n) = 0$ where $\ell \in \{0, 1, \ldots, K-1\}$ is such that $n \equiv \ell \mod K$. Thus the above is an algorithm to decide Skolem for LRS(r$\mathbb{R}$) in $\mathsf{NP}^{\mathsf{RP}}$.

6 Revisiting NP-hardness

Blondel and Portier [9] proved that Skolem problem is NP-hard by a reduction from the *non-universality problem* for unary NFAs [27]. More recently, in [3], an alternate proof was obtained by a reduction from the subset sum problem. In this section, we provide yet another proof of NP-hardness, by directly reducing from 3-SAT. Given a 3-SAT formula ϕ over s

variables $x_1, \ldots, x_s$, we will construct an LRS y such that ϕ is satisfiable if and only if the LRS y has a Skolem zero, i.e., $\exists n \in \mathbb{N}\ y_n = 0$. Let $p_1, \ldots, p_s$ be the first s primes. By the Prime number theorem, the number of primes less than s is roughly $s/\log s$, and thus $p_s \sim s \log s$.

For each prime p_i, define an LRS u^i with order p_i given by:

$$u^i_n = \begin{cases} 0, \text{ for } 1 \leq n < p_i \\ 1, \text{ for } n = p_i \\ u^i_{n-p_i}, \text{ for } n > p_i \end{cases}$$

With 1 and 0 representing the boolean values true and false, we define a surjection f from $\mathbb{N}$ to the set of assignments to variables of ϕ as $f : \mathbb{N} \to \{0,1\}^s$, given by $f(n) = (a_1, \ldots, a_s)$ where $a_i = 1 \iff p_j | n$. The inverse map of an assignment, $f^{-1}(a_1, \ldots, a_s)$ is the set $\{n : p_j | n \iff a_j = 1\}$. For sequences u, v and w, we will denote $u = v$ to mean $\forall n \in \mathbb{N}\ u_n = v_n$, and $w = u + v$ to mean $\forall n \in \mathbb{N}\ w_n = u_n + v_n$. Let $\phi = C_1 \wedge \cdots \wedge C_m$. For a clause $C_i = v_{i_1} \vee v_{i_2} \vee v_{i_3}$ define the LRS y^{i_l} for $l = 1, 2, 3$ as follows:

$$y^{i_l} = \begin{cases} 1 - u^k, \text{ if } v_{i_l} = x_k \text{ for some } k \in \{1, \ldots, s\}, \\ u^k, \text{ if } v_{i_l} = \neg x_k \text{ for some } k \in \{1, \ldots, s\} \end{cases}$$

Define the sequences $y^i = y^{i_1} y^{i_2} y^{i_3}$ for $1 \leq i \leq m$, and $y = y^1 + \cdots + y^m$. Since the sum and product of LRS is a LRS (see Theorem 4.1 in [16]), y is also an LRS. Then we have:

▷ Claim 17. $y^i_n = 0$ if and only if $f(n)$ satisfies C_i.

Now one can argue that

▶ **Proposition 18.** *ϕ is satisfiable if and only if $\exists n$ s.t. $y_n = 0$.*

The order of y is at most $m(p_s)^3$, and thus is polynomial in the number of variables and the clauses and y can be constructed from an instance of 3-SAT in polynomial time. Thus, we have shown that the Skolem problem for integral LRS is at least as hard as 3-SAT, and hence NP-hard.

Weak vs Strong NP-hardness. A simple consequence of the above reduction is that we can now show that the Skolem problem remains NP-hard even when the initial values are given in unary, i.e., it is *strongly* NP*-hard wrt the initial values*. This follows since the initial values of the LRS y used in the construction above, are at most m in value, and thus can be represented in $\log m$ bits, as opposed to poly(m) bits.

7 Applications and Discussion

We have shown that for a natural and large subclass of recurrences namely LRS(r$\mathbb{R}$), the Skolem problem can be solved in $\mathsf{NP}^{\mathsf{RP}}$. This immediately implies effective bounds for two well-known questions on LRS, namely, *Positivity and Ultimate Positivity for* LRS(r$\mathbb{R}$). Given an LRS $\mathbf{u}$, the *positivity problem* asks to decide if $u_n > 0$ for all $n \in \mathbb{N}$. Similarly, the *ultimate positivity problem* asks if there exists $n_0 \in \mathbb{N}$ s.t., $u_n > 0$ for all $n > n_0$. Using the machinery that we developed in this paper, we obtain:

▶ **Corollary 19** (to Theorem 10). *Positivity and Ultimate positivity for* LRS(r$\mathbb{R}$) *can be decided in*[4] $\mathsf{coNP}^{\mathsf{PosSLP}}$.

Proof. We can reduce an LRS(r$\mathbb{R}$) instance to a exponentially bounded set of real exponential polynomials, and in such polynomials the sign of the dominant root dominates the sign after an n that is exponentially bounded in m. Hence if the LRS is negative or zero before an exponential point, we can guess such an n in NP and verify the sign using PosSLP. This solves both Positivity and Ultimate Positivity in the fourth level of the Counting Hierarchy. ◀

Ultimate Positivity and Positivity are known to be hard for $\forall\mathbb{R}$ (the *universal theory of reals*) for the class of simple LRS [24] and hence considered unlikely to be in the Counting Hierarchy [5]. An inspection of the proof in [24] reveals that the LRS constructed to show hardness have characteristic roots with phases that are irrational multiple of π and hence do not fall in the class LRS(r$\mathbb{R}$). Finally, as mentioned in the introduction we show three applications of our results to obtain complexity bounds for problems from three completely different areas.

- **Weighted automata:** In a recent result, Barloy et al. [7] define a subclass of LRS called *poly-rational sequences*, denoted by rational expressions closed under sum and product. They show that polynomially ambiguous weighted automata, copyless cost-register automata, rational formal series, and LRS whose eigenvalues are roots of rational numbers (called **PolyRat**, these are exactly those LRS where the characteristic roots are of the form λ, where $\lambda^n = r$ for some $r \in \mathbb{Q}$) are equivalent. They leave open the precise complexity of the Skolem problem for **PolyRat** sequences. We solve this problem, since Theorem 10 immediately implies that Skolem for PolyRat is in $\mathsf{NP}^{\mathsf{RP}}$.
- **Probabilistic finite automata (PFA):** A second application is in the language theoretic properties of unary probabilistic finite automata. Given the link between the Skolem problem and the Markov chain reachability problem [2], the work in [4] considers regularity of unary PFA, whose dynamics are described using Markov chains. Proposition 2 give the decidability of reachability and positivity problems in the special case where roots are distinct (i.e., the "simple" case) roots of real numbers. Again, from Theorem 7 we obtain that these problems are in $\mathsf{NP}^{\mathsf{RP}}$ and $\mathsf{NP}^{\mathsf{PosSLP}}$ respectively. One interesting line of future work would be to see if the techniques introduced in this paper would also help in showing complexity bounds for regularity problems, which is the focus of [4].
- **Hybrid systems:** Most reachability problems on hybrid systems are known to be undecidable. Two well-behaved decidable fragments here are o-minimal hybrid systems [22] (Theorem 6.2), [26] (Theorem 4.6) and linear-time invariant (LTI) systems [17] (Theorem 3.10). In both these cases, decidability is obtained by assuming that the eigenvalues of the matrix associated with the linear system are reals or roots of reals (for example, called *simple* LTI systems in [17]). Given that [17] proves that reachability for LTI systems is hard for both the Skolem and Positivity problems for LRS, this raises the question of the precise computational complexity of reachability in LTI systems. Whether the techniques introduced in this paper will yield more precise complexity bounds to the computability results in these papers is part of ongoing research.

Implicit in our $\mathsf{NP}^{\mathsf{RP}}$ algorithm for Skolem problem for LRS(r$\mathbb{R}$) is an effective bound, i.e a number $N \in \mathbb{N}$ which is $\exp(m)$ such that for all $n > N$, $u_n \neq 0$. Since if such an n can be effectively bounded by $\exp(m)$ for all LRS would imply the decidability (in fact

[4] Given an arithmetic circuit representing a number, the PosSLP problem introduced by Allender et al. [5] is to decide if the number is positive. It is known to be P-hard and lies in the *Counting Hierarchy*.

in $\mathsf{NP}^{\mathsf{RP}}$) for the Skolem problem, one interesting way to improve the hardness result in Section 6 would be to construct an explicit LRS for which the first zero provably occurs[5] after $n > \exp(\exp(m))$. We leave this as a challenging open question for future work. In an orthogonal recent work, Bell et al. [8] introduce a class multidimensional version of LRS (n-LRS). In their language, Skolem problem is the question of finding zeroes in a 1-LRS. The zeroness problem for n-LRS of depth 2 is NP-hard, but in general the problem of n-LRS of depth k is undecidable. It would be interesting to see if spectral restrictions such as ours could yield decidability for special cases of n-LRS.

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, Nikhil Balaji, and Nikhil Vyas. Complexity of restricted variants of Skolem and related problems. In *42nd International Symposium on Mathematical Foundations of Computer Science, MFCS 2017, August 21-25, 2017 - Aalborg, Denmark*, pages 78:1–78:14, 2017.

4 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.

5 Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM J. Comput.*, 38(5):1987–2006, 2009. doi:10.1137/070697926.

6 Alan Baker. *Transcendental number theory*. Cambridge university press, 1990.

7 Corentin Barloy, Nathanaël Fijalkow, Nathan Lhote, and Filip Mazowiecki. A robust class of linear recurrence sequences. In *28th EACSL Annual Conference on Computer Science Logic, CSL 2020, January 13-16, 2020, Barcelona, Spain*, pages 9:1–9:16, 2020.

8 Paul C Bell, Igor Potapov, and Pavel Semukhin. On the mortality problem: From multiplicative matrix equations to linear recurrence sequences and beyond. In *44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

9 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.

10 J-Y Cai, Richard J Lipton, Robert Sedgewick, and AC-C Yao. Towards uncheatable benchmarks. In *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 2–11. IEEE, 1993.

11 Jin-yi Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. *International Journal of Foundations of Computer Science*, 5(03n04):293–302, 1994.

12 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.

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

14 Abraham De Moivre. The doctrine of chances. In *Annotated Readings in the History of Statistics*, pages 32–36. Springer, 2001.

15 Kousha Etessami and Mihalis Yannakakis. On the complexity of Nash equilibria and other fixed points. *SIAM Journal on Computing*, 39(6):2531–2597, 2010.

[5] This question was also raised by Kousha Etessami in a comment on a blogpost in [28]

16 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.

17 Nathanaël Fijalkow, Joël Ouaknine, Amaury Pouly, João Sousa-Pinto, and James Worrell. On the decidability of reachability in linear time-invariant systems. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, pages 77–86. ACM, 2019.

18 Georges Hansel. A simple proof of the Skolem-Mahler-Lech theorem. In *International Colloquium on Automata, Languages, and Programming*, pages 244–249. Springer, 1985.

19 Godfrey Harold Hardy, Edward Maitland Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

20 Russell Impagliazzo and Avi Wigderson. P= bpp unless e has subexponential circuits: derandomizing the xor lemma. In *Proceedings of the 29th STOC*, pages 220–229, 1997.

21 Donald E Knuth. The art of computer programming. volume 1: Fundamental algorithms. *Pearson education*, 1997.

22 Gerardo Lafferriere, George J Pappas, and Shankar Sastry. O-minimal hybrid systems. *Mathematics of control, signals and systems*, 13(1):1–21, 2000.

23 Maurice Mignotte. Some useful bounds. In *Computer algebra*, pages 259–263. Springer, 1983.

24 Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *International Colloquium on Automata, Languages, and Programming*, pages 330–341. Springer, 2014.

25 Min Sha. Effective results on the Skolem problem for linear recurrence sequences. *Journal of Number Theory*, 197:228–249, 2019.

26 Omid Shakernia, George J Pappas, and Shankar Sastry. Decidable controller synthesis for classes of linear systems. In *International Workshop on Hybrid Systems: Computation and Control*, pages 407–420. Springer, 2000.

27 Larry J Stockmeyer and Albert R Meyer. Word problems requiring exponential time (preliminary report). In *Proceedings of the fifth annual ACM symposium on Theory of computing*, pages 1–9. ACM, 1973.

28 Terence Tao. *Structure and randomness: pages from year one of a mathematical blog*. American Mathematical Society Providence, RI, 2008.

29 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.

30 Nikolai Konstantinovich Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical Notes*, 38(2):609–615, 1985.

31 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.

32 F Viete. Opera mathematica. 1579. *Reprinted Leiden, Netherlands*, 1646, 1970.