On the p-adic Skolem Problem

Piotr Bacik
University of Oxford, UK
Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

Joël Ouaknine
Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

David Purser
University of Liverpool, UK

James Worrell
University of Oxford, UK

Abstract

The Skolem Problem asks to determine whether a given linear recurrence sequence (LRS) has a zero term. Showing decidability of this problem is equivalent to giving an effective proof of the Skolem-Mahler-Lech Theorem, which asserts that a non-degenerate LRS has finitely many zeros. The latter result was proven over 90 years ago via an ineffective method showing that such an LRS has only finitely many p-adic zeros. In this paper we consider the problem of determining whether a given LRS has a p-adic zero, as well as the corresponding function problem of computing all p-adic zeros up to arbitrary precision. We present algorithms for both problems and report on their implementation within the Skolem tool. The output of the algorithms is unconditionally correct, and termination is guaranteed subject to the p-adic Schanuel Conjecture (a standard number-theoretic hypothesis concerning the p-adic exponential function). While these algorithms do not solve the Skolem Problem, they can be exploited to find natural-number and rational zeros under additional hypotheses. To illustrate this, we apply our results to show decidability of the *Simultaneous Skolem Problem* (determine whether two coprime linear recurrences have a common natural-number zero), again subject to the p-adic Schanuel Conjecture.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Skolem Problem, p-adic Schanuel Conjecture, Skolem Conjecture, Exponential Local-Global Principle

Supplementary Material Online tool: `https://skolem.mpi-sws.org/?padic`

1 Introduction

1.1 The Skolem Problem

A *linear recurrence sequence* (LRS) $\boldsymbol{u} = \langle u_n \rangle_{n=0}^{\infty}$ is a sequence of algebraic numbers satisfying a linear recurrence relation:

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n \tag{1.1}$$

where $a_0, \ldots, a_{d-1} \in \overline{\mathbb{Q}}$. We call d the order of the recurrence. If d is the minimum order of a recurrence satisfied by $\boldsymbol{u}$ then we call d the *order* of $\boldsymbol{u}$. A *rational LRS* is one all of whose entries are rational numbers.

The zero set of an LRS $\boldsymbol{u}$ is $\{n \in \mathbb{N} : u_n = 0\}$. The celebrated Skolem-Mahler-Lech theorem [16, 12, 10] states that the zero set is comprised of a union of a finite set and finitely many arithmetic progressions. The statement may be refined via the concept of *non-degeneracy*. Define the *characteristic polynomial* of the recurrence (1.1) to be

$$g(X) := X^d - a_{d-1}X^{d-1} - \cdots - a_0\,. \tag{1.2}$$

Let $\lambda_1, \ldots, \lambda_s \in \overline{\mathbb{Q}}$ be the distinct roots of g; these are called the *characteristic roots* of $\boldsymbol{u}$. We say $\boldsymbol{u}$ is *non-degenerate* if no ratio λ_i/λ_j of distinct characteristic roots is a root of unity. A given LRS can be effectively decomposed as the merge of finitely many non-degenerate LRS [9, Theorem 1.6]. The core of the Skolem-Mahler-Lech Theorem is that a non-degenerate LRS that is not identically zero has finitely many zero terms. Unfortunately, the proof of this result remains ineffective: there is no known algorithm to determine whether a non-degenerate LRS has a zero. This is the famous *Skolem Problem*:

▶ **Problem 1** (The Skolem Problem). *Given an LRS $\boldsymbol{u}$ specified by a non-degenerate linear recurrence and a set of initial values (with all data consisting of algebraic numbers), determine whether there exists $n \in \mathbb{N}$ such that $u_n = 0$.*

One can also formulate a corresponding function version of this problem in which the task is to compute the finite set of zeros of a given non-degenerate LRS. We denote the decision version by $\mathtt{SP}(\mathbb{N})$ and the function version by $\mathtt{FSP}(\mathbb{N})$. This notation makes explicit that we are looking for natural-number zeros of the LRS.

It is folklore that computability of $\mathtt{FSP}(\mathbb{N})$ reduces to decidability of $\mathtt{SP}(\mathbb{N})$. Assuming the latter, given an LRS $\boldsymbol{u}$, the finitely many zeros in each non-degenerate subsequence of $\boldsymbol{u}$ can be found by brute-force search and, since the infinite suffix of an LRS remains an LRS, one can use a decision procedure for $\mathtt{SP}(\mathbb{N})$ to certify that no zeros remain to be found. However, decidability of the Skolem Problem has remained open for close to a century, with only partial results known from restricting the order (see the exposition of [2] on results of [17, 18, 1]), restricting to reversible sequences of low order [11], or restricting to *simple* LRS and assuming certain number-theoretic conjectures [3].

In the remainder of this section we introduce various relaxations of the Skolem Problem that arise by extending LRS to larger domains and seeking zeros of such extensions.

1.2 The Bi-Skolem Problem

The first variant of the Skolem Problem involves bi-infinite (that is, two-way infinite) sequences. Indeed, given a recurrence (1.1) and initial values $u_0, \ldots, u_{d-1} \in \overline{\mathbb{Q}}$, there is a unique bi-infinite sequence $\boldsymbol{u} = \langle u_n \rangle_{n=-\infty}^{\infty}$ that satisfies the recurrence. We call $\boldsymbol{u}$ a *linear recurrent bi-sequence* (LRBS). For example, the Fibonacci sequence extends to an LBRS $\langle \ldots, 5, -3, 2 - 1, 1, 0, 1, 1, 2, 3, 5 \ldots \rangle$.

▶ **Problem 2** (Bi-Skolem Problem)**.** *Given an LRBS* $\boldsymbol{u}$*, specified by a non-degenerate linear recurrence and a set of initial values, determine whether there exists* $n \in \mathbb{Z}$ *such that* $u_n = 0$*.*

We use the notation $\mathtt{SP}(\mathbb{Z})$ to refer to the above decision problem and we write $\mathtt{FSP}(\mathbb{Z})$ for the corresponding function version, in which we output the finite set of zeros of a given non-degenerate bi-infinite sequence.

For function problems P_1, P_2, write $P_1 \leq P_2$ if there is a Turing reduction from P_1 to P_2. Here for purposes of comparison we view decision problems as function problems with outputs in $\{\mathtt{TRUE}, \mathtt{FALSE}\}$. Write $P_1 \equiv P_2$ if $P_1 \leq P_2$ and $P_2 \leq P_1$. Then it is easy to see that

$$\mathtt{SP}(\mathbb{Z}) \leq \mathtt{FSP}(\mathbb{Z}) \equiv \mathtt{FSP}(\mathbb{N}) \equiv \mathtt{SP}(\mathbb{N})\,.$$

Indeed, the reduction $\mathtt{FSP}(\mathbb{Z}) \leq \mathtt{FSP}(\mathbb{N})$ is realised by splitting a given bi-infinite LRS around the index zero into forward and backward sequences (both of which are LRS) and computing the respective zeros of each of the two one-way infinite sequences.

Unlike for Skolem's Problem, it is not known whether the function version of the Bi-Skolem Problem reduces to its decision version, i.e., it is not known whether $\mathtt{FSP}(\mathbb{Z}) \leq \mathtt{SP}(\mathbb{Z})$. The reduction holds if one assumes the weak p-adic Schanuel Conjecture [3].

1.3 The Rational Skolem Problem

Having expanded the index set of an LRS to $\mathbb{Z}$ in the Bi-Skolem Problem, we consider a further expansion of its domain to $\mathbb{Q}$, which leads us to consider *rational zeros* of an LRS. One way to realise this generalisation is via the exponential-polynomial formulation of LRS. It is classical that an LRS $\boldsymbol{u}$ of order d with characteristic roots $\lambda_1, \ldots, \lambda_s$ admits the following representation:

$$u_n = \sum_{i=1}^{s} P_i(n)\lambda_i^n\,, \tag{1.3}$$

where the P_i are polynomials with algebraic coefficients and degree one less than the multiplicity of λ_i as a root of g, the characteristic polynomial of $\boldsymbol{u}$. We say that $\frac{a}{b} \in \mathbb{Q}$ is a rational zero of $\boldsymbol{u}$ if $\sum_{i=1}^{s} P(\frac{a}{b})\lambda_i^{\frac{a}{b}} = 0$, where $\lambda^{\frac{a}{b}}$ denotes any b-th root of λ^a. For example, the sequence $u_n = 4^n + 2$ has a rational zero at $\frac{1}{2}$ that is witnessed by setting $4^{1/2} := -2$. The Rational Skolem Problem $\mathtt{SP}(\mathbb{Q})$ asks to determine whether a given LRS has a rational zero, while its function analog $\mathtt{FSP}(\mathbb{Q})$ asks to compute all rational zeros of a non-degenerate sequence. We note that the definition of rational zeros is consistent with that of integer zeros, that is, the integer rational zeros of $\boldsymbol{u}$ are precisely the zeros of the bi-infinite extension of $\boldsymbol{u}$.

A recent result [4, Proposition 4.5] shows that the denominator of any rational zero can be effectively bounded. This allows us to determine the relationship of the Rational Skolem Problem with the Bi-Skolem Problem and the usual Skolem Problem. We have

$$\mathtt{SP}(\mathbb{Q}) \overset{(1)}{\equiv} \mathtt{SP}(\mathbb{Z}) \overset{(2)}{\leq} \mathtt{SP}(\mathbb{N}) \equiv \mathtt{FSP}(\mathbb{N}) \equiv \mathtt{FSP}(\mathbb{Z}) \overset{(3)}{\equiv} \mathtt{FSP}(\mathbb{Q})\,,$$

where, as noted earlier, (2) is an equivalence assuming the weak p-adic Schanuel Conjecture. Indeed, suppose $\boldsymbol{u}$ is an LRS satisfying (1.3). We may compute a bound $b_{\max}$ on the largest denominator of any rational zero of $\boldsymbol{u}$. For the reduction (1) we note that deciding $\mathtt{SP}(\mathbb{Q})$ is equivalent to deciding $\mathtt{SP}(\mathbb{Z})$ on every LRS $\boldsymbol{v}$ defined by $v_n := \sum_{i=1}^{s} P_i(\frac{n}{b})(\lambda_i^{1/b})^n$, where $1 \leq b \leq b_{\max}$. The reduction (3) is similar.

1.4 The p-adic Skolem Problem

The main contributions of this paper concern the p-adic zeros of an LRS, that is, zeros lying in a p-adic completion $\mathbb{Z}_p$ of the integers with respect to a given prime p. Roughly speaking, the idea is to extend a given LRS $\boldsymbol{u} = \langle u_n \rangle_{n=0}^{\infty}$ to a map $f : \mathbb{Z}_p \to \mathbb{Z}_p$ such that $f(n) = u_n$ for all $n \in \mathbb{Z}$. We then determine whether f has any zeros in $\mathbb{Z}_p$ and, if yes, we approximate them to arbitrary precision. It turns out that f can have zeros other than the integer or rational zeros of the original LRS $\boldsymbol{u}$. Hence the ability to determine the existence of p-adic zeros does not directly solve Skolem's Problem. Nevertheless, as our results and experiments show, working p-adically offers a practical approach to finding integer zeros of an LRS that can moreover find all integer zeros subject to additional assumptions and hypotheses.

By way of example, consider the ring $\mathbb{Z}_3$ of 3-adic integers, which is the Cauchy completion of $\mathbb{Z}$ with respect to the absolute value $|\cdot|_3$. The latter is defined by writing $|a|_3 := 3^{-k}$, where k is the order of 3 as a divisor of $a \in \mathbb{Z}$ (the larger k, the smaller the absolute value). It turns out that the LRS $u_n = 4^n + 2$ extends uniquely to a continuous map $f : \mathbb{Z}_3 \to \mathbb{Z}_3$. It is not difficult to see that $f(\frac{1}{2}) = 0$. Indeed, write $n_k := \frac{1+3^k}{2}$ for all $k \in \mathbb{N}$. Since $2n_k = 1 + 3^{k+1}$ we see that $\lim_{k\to\infty} n_k = \frac{1}{2}$ in $\mathbb{Z}_3$. On the other hand, it can be shown by induction that $u_{n_k} \equiv 0 \bmod 3^{k+1}$ for all k and hence $\lim_{k\to\infty} u_{n_k} = 0$ in $\mathbb{Z}_3$. By continuity we conclude that $f(\frac{1}{2}) = 0$.

We define the $\mathfrak{p}$-adic Skolem Problem in a slightly more general setting than in the discussion above in order to accommodate LRS $\boldsymbol{u}$ taking values in the ring $\mathcal{O}$ of integers of a number field. We refer to Section 2 for full details. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we denote by $\mathcal{O}_\mathfrak{p}$ the Cauchy completion of $\mathcal{O}$ with respect to the $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p}$. Assuming that $\mathfrak{p}$ does not divide the constant term of the recurrence (1.1), there exists $N \geq 1$ and analytic functions $f_0, \ldots, f_{N-1} : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$ such that $u_{Nn+\ell} = f_\ell(n)$ for all $n \in \mathbb{N}$. Let us call a zero of one of the above functions f_ℓ a *$\mathfrak{p}$-adic zero of $\boldsymbol{u}$*. The proof of the Skolem-Mahler-Lech Theorem shows that $\boldsymbol{u}$ has finitely many $\mathfrak{p}$-adic zeros—but it does not allow one to determine whether a given $\boldsymbol{u}$ has any $\mathfrak{p}$-adic zeros and, if so, how to compute them (hence the proof does not tell us anything about computing the integer zeros either). This motivates:

▶ **Problem 3** (The $\mathfrak{p}$-adic Skolem Problem)**.** *Given a non-degenerate LRS $\boldsymbol{u}$ and prime ideal $\mathfrak{p}$ in the splitting field of its characteristic polynomial, determine whether $\boldsymbol{u}$ has a $\mathfrak{p}$-adic zero.*

The function version of this problem asks to compute a finite representation of all $\mathfrak{p}$-adic zeros of $\boldsymbol{u}$ (see Definition 7), allowing us both to count the number of $\mathfrak{p}$-adic zeros and to approximate them to arbitrary precision (with respect to the p-adic absolute value). As shorthand we denote the decision and function problems respectively by $\mathtt{SP}(\mathcal{O}_\mathfrak{p})$ and $\mathtt{FSP}(\mathcal{O}_\mathfrak{p})$.

It is open whether any of the above-mentioned variants of Skolem's Problem can be reduced to $\mathtt{SP}(\mathcal{O}_\mathfrak{p})$ or $\mathtt{FSP}(\mathcal{O}_\mathfrak{p})$. The essential problem is that we do not know how to determine in general whether a $\mathfrak{p}$-adic zero of a given LRS is rational or not. While our decision procedure can approximate such a zero to arbitrary precision, it cannot in general certify that it is irrational or even non-integer. See Section 3.4 for further discussion.

1.5 Main Results

Our main theoretical result is the following.

▶ **Theorem 4.** *Assuming the p-adic Schanuel Conjecture, $\mathtt{SP}(\mathcal{O}_\mathfrak{p})$ is decidable and $\mathtt{FSP}(\mathcal{O}_\mathfrak{p})$ is computable.*

When the characteristic polynomial of $\boldsymbol{u}$ splits in $\mathbb{Z}_p$ (which occurs for infinitely many primes p by the Chebotarev density theorem), we may take $\mathcal{O}_\mathfrak{p} = \mathbb{Z}_p$. In this case we have

implemented the algorithm for $\texttt{FSP}(\mathcal{O}_\mathfrak{p})$ in the Skolem tool.[1] Preliminary experiments in Section 4 show the practical applicability of our algorithm, including for the task of finding rational and integer zeros.

The main technical lemma (also subject to the p-adic Schanuel Conjecture) behind the proof of Thm. 4 shows that if two exponential polynomials are coprime in the ring of exponential polynomials, then every common p-adic zero must be rational. This lemma allows us to decide the *Simultaneous Skolem Problem*: determine whether two LRS have a common integer zero.

▶ **Theorem 5.** *Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.*

An in-principle decision procedure for the $\mathfrak{p}$-adic Skolem Problem can be obtained from a result in the PhD thesis of Mariaule [13], showing that the first-order theory of the structure $(\mathcal{O}_\mathfrak{p}, +, \cdot, 0, 1, E_p)$ is decidable assuming the p-adic Schanuel Conjecture (where $E_p(x) = e^{px}$). Schanuel's Conjecture is used in [13] via a desingularisation construction that is similar in spirit to Lem. 12, but which is not practical to implement. We note also that Thm. 5 does not follow from the result of [13] since $\mathbb{Z}$ is not first-order definable in $(\mathcal{O}_\mathfrak{p}, +, \cdot, 0, 1, E_p)$, as this would contradict decidability of the latter structure.

2 Preliminaries

We briefly recall relevant notions about p-adic numbers. We refer to [15] for more details. Let $\mathbb{K}$ be a number field and $\mathfrak{p}$ be a prime ideal in its ring of integers $\mathcal{O}$. Define the absolute value $|\cdot|_\mathfrak{p}$ in $\mathbb{K}$ by $|a|_\mathfrak{p} = N(\mathfrak{p})^{-v_\mathfrak{p}(a)}$, where $N(\mathfrak{p})$ is the order of the residue field $\mathcal{O}/\mathfrak{p}$ and $v_\mathfrak{p}(a)$ is the order of $\mathfrak{p}$ as a divisor of the fractional ideal $a\mathcal{O}$. We denote by $\mathbb{K}_\mathfrak{p}$ the completion of $\mathbb{K}$ with respect to $|\cdot|_\mathfrak{p}$ and define $\mathcal{O}_\mathfrak{p} := \{a \in \mathbb{K}_\mathfrak{p} : |a|_\mathfrak{p} \leq 1\}$. An element $a \in \mathcal{O}_\mathfrak{p}$ can be represented uniquely as an infinite series $a = \sum_{n=0}^{\infty} a_n \pi^n$ where the a_n lie in a fixed set of representatives of $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ and π is a *uniformiser*, that is, a generator of the unique maximal ideal of $\mathcal{O}_\mathfrak{p}$. In the special case that $\mathbb{K}$ is the field $\mathbb{Q}$ of rational numbers and $\mathfrak{p}$ is the ideal $p\mathbb{Z}$ for a prime p, the above completion yields the field $\mathbb{Q}_p$ of p-adic numbers and the ring $\mathbb{Z}_p$ of p-adic integers. We denote by $\mathbb{C}_p$ the Cauchy completion of the algebraic closure of $\mathbb{Q}_p$. For a prime $\mathfrak{p}$ lying over p we can regard $\mathbb{K}_\mathfrak{p}$ as a subfield of $\mathbb{C}_p$.

Consider an LRS $\boldsymbol{u}$ given by the formula (1.3) and let $\mathbb{K}$ be the field generated by the characteristic roots and the initial values of $\boldsymbol{u}$. Pick a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ that does not divide the constant term of the recurrence for $\boldsymbol{u}$ (so that $v_\mathfrak{p}(\lambda_i) = 0$ for all i). Choose $N \in \mathbb{Z}_{\geq 1}$ to be the smallest positive integer such that $v_\mathfrak{p}(\lambda_i^N - 1) > \frac{e}{p-1}$ for all i, where $e = e_\mathfrak{p}$ is the ramification index. For $\ell \in \{0, 1, \ldots, N-1\}$ we define the ℓ-th $\mathfrak{p}$-adic interpolant of $\boldsymbol{u}$ to be the analytic function

$$f_\ell(x) = \sum_{i=1}^{s} P_i(Nx + \ell)\lambda_i^\ell \exp(x \log \lambda_i^N) \tag{2.1}$$

with $x \in \mathcal{O}_\mathfrak{p}$. Then $f_\ell(n) = u_{Nn+\ell}$ for each $n \in \mathbb{Z}_{\geq 0}$ and so (2.1) defines an extension of $\boldsymbol{u}$ to $\mathcal{O}_\mathfrak{p}$. In fact, the right-hand side of (2.1) converges for any $x \in \mathcal{O}_{\mathbb{C}_p}$ and we call such an x an *extended* $\mathfrak{p}$*-adic zero* if $f_\ell(x) = 0$ for some $\ell \in \{0, \ldots, N-1\}$.

The following is a key lemma for finding zeros of power series on $\mathbb{K}_\mathfrak{p}$.

[1] Skolem may be experimented with online at `https://skolem.mpi-sws.org/?padic`. For the algorithm described in this paper, toggle the switch labelled "Use p-adic algorithm".

▶ **Theorem 6** (Hensel's Lemma for power series). *Let f be a power series with coefficients in $\mathcal{O}_\mathfrak{p}$ that converges on $\mathcal{O}_\mathfrak{p}$. If $a \in \mathcal{O}_\mathfrak{p}$ satisfies*

$$|f(a)|_\mathfrak{p} < |f'(a)|_\mathfrak{p}^2$$

then there is a unique $\alpha \in \mathcal{O}_\mathfrak{p}$ such that $f(\alpha) = 0$ and $|\alpha - a|_\mathfrak{p} < |f'(\alpha)|_\mathfrak{p}$.

The following definition explains how we treat approximate $\mathfrak{p}$-adic zeros of power series:

▶ **Definition 7.** *A specification of a $\mathfrak{p}$-adic zero $x \in \mathcal{O}_\mathfrak{p}$ of an analytic function $f : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$ is an element $y = a_0 + \cdots + a_r\pi^r$, where π is a uniformiser for $\mathcal{O}_\mathfrak{p}$, such that $|f(y)|_\mathfrak{p} < |f'(y)|_\mathfrak{p}^2$, and $|x - y| < |f'(y)|_\mathfrak{p}$.*

Hensel's Lemma ensures that x is defined uniquely.

In the rest of the section we list some results on which we rely.

▶ **Theorem 8** (Masser [14]). *Let $\mathbb{K}$ be a number field of degree D over $\mathbb{Q}$. For $s \geq 1$ let $\lambda_1, \ldots, \lambda_s$ be non-zero elements of $\mathbb{K}$ having height at most h over $\mathbb{Q}$. Then the group of multiplicative relations*

$$L = \{(k_1, \ldots, k_s) \in \mathbb{Z}^s : \lambda_1^{k_1} \ldots \lambda_s^{k_s} = 1\}$$

is generated (as an additive subgroup of $\mathbb{Z}^s$) by a collection of vectors all of whose entries have absolute value at most

$$(csh)^{s-1} D^{s-1} \frac{(\log(D+2))^{3s-3}}{(\log\log(D+2))^{3s-4}}.$$

The following is a generalisation of Strassman's Theorem, commonly known via the notion of the Newton Polygon; see [15], page 307.

▶ **Theorem 9.** *Let p be a prime, and let $f(X) = \sum a_n X^n \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ be a nonzero convergent power series. Given $r \geq 0$, suppose $\mu < \nu$ are the extreme indices n for which $v_p(a_n) + nr = \min_{j \geq 0} v_p(a_j) + jr$. Then f has exactly $\nu - \mu$ zeros (counting multiplicities) on the sphere $\{x \in \mathbb{C}_p : v_p(x) = r\}$.*

Finally we state the p-adic Schanuel Conjecture (see [5, 13]), and the Skolem Conjecture.

▶ **Conjecture 10** (p-adic Schanuel's Conjecture). *Let $n \geq 1$ and $t_1, \ldots, t_n \in \mathbb{C}_p$ (with valuation at least $\frac{1}{p-1}$) linearly independent over $\mathbb{Q}$. Then*

$$\operatorname{trdeg}_\mathbb{Q} \mathbb{Q}(t_1, \ldots, t_n, \exp(t_1), \ldots, \exp(t_n)) \geq n$$

where $\operatorname{trdeg}_\mathbb{Q} \mathbb{K}$ denotes the transcendence degree of $\mathbb{K}$ over $\mathbb{Q}$.

▶ **Conjecture 11** (The Skolem Conjecture). *Let $\boldsymbol{u}$ be a simple rational LRBS taking values in the ring $\mathbb{Z}[\frac{1}{b}]$ for some integer b. Then $\boldsymbol{u}$ has no integer zero iff, for some integer $m \geq 2$ with $gcd(b, m) = 1$, we have that $u_n \not\equiv 0 \bmod m$ for all $n \in \mathbb{Z}$.*

3 Decidability of the p-adic Skolem Problem

3.1 Informal Outline of the Algorithm

In this section we prove Thm. 4, assuming the p-adic Schanuel Conjecture. We start with an informal description of an algorithm that attempts to find the $\mathfrak{p}$-adic zeros of an LRS $\boldsymbol{u}$

using only brute-force search and Hensel's Lemma. We note the problem with this approach, which motivates the subsequent development involving p-adic Schanuel's Conjecture.

Let $f_\ell : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$ be an interpolant of a given LRS $\boldsymbol{u}$. We would like to compute specifications of all the zeros of f_ℓ in $\mathcal{O}_\mathfrak{p}$. The idea is to search for zeros lying in the residue classes of $\mathcal{O}_\mathfrak{p}$ modulo π^r for $r = 1, 2, 3, \ldots$, where π is a uniformiser of $\mathcal{O}_\mathfrak{p}$. Consider a representative $z \in \mathcal{O}_\mathfrak{p}$ of a residue class of $\mathcal{O}$ modulo π^r. If $f_\ell(z) \not\equiv 0 \bmod \pi^r$ then the residue class of z does not contain a zero of f_ℓ, and we can proceed to search other residue classes. If $f_\ell(z) \equiv 0 \bmod \pi^r$ and $v_\mathfrak{p}(f_\ell(z)) > 2v_\mathfrak{p}(f'_\ell(z))$ then the residue class contains a unique zero of f_ℓ by Hensel's Lemma. If neither of the above cases hold then the residue class may contain any number of zeros of f_ℓ. Note that we can use Thm. 9 to determine the exact the number of extended $\mathfrak{p}$-adic zeros (lying in the extension $\mathbb{C}_p$ of $\mathcal{O}_\mathfrak{p}$) of f_ℓ in the residue class of z.[2] If this number is zero then we can again proceed to consider other residue classes. If the number is positive then we can refine our search by looking at residue classes modulo π^{r+1} contained in the current class. If all the zeros of f_ℓ in $\mathcal{O}_\mathfrak{p}$ are simple then this search will eventually terminate. However, if there is a zero of multiplicity two or more then the search will run forever (as the inequality $v_\mathfrak{p}(f_\ell(z)) > 2v_\mathfrak{p}(f'_\ell(z))$ will never hold). The key challenge is thus to identify multiple zeros of f_ℓ in $\mathcal{O}_\mathfrak{p}$ and determine their multiplicity.

It so happens that for irreducible factors of f_ℓ, assuming p-adic Schanuel's Conjecture, the only possible zeros of multiplicity two or more are rational. This is the content of the main technical results in this section and it allows us to amend the above algorithm so that it always terminates. Specifically, in parallel with the above-described process, we search by enumeration for rational zeros of f_ℓ. We thus find all $\mathfrak{p}$-adic zeros either by specifying them with Hensel's Lemma or by enumerating and checking directly. We use Thm. 9 to certify that all zeros have thereby been found.

3.2 Simultaneous Zeros of Coprime Exponential Polynomials

We now state our main technical lemma.

▶ **Lemma 12.** *Let $\mathbb{K}$ be a number field, $P, Q \in \mathbb{K}[x_0, x_1, \ldots, x_{2s}]$ be coprime multivariate polynomials, that are also coprime to any irreducible polynomial of the form $\sum_{i=1}^{s}(a_i + b_i x_0)x_i$, $a_i, b_i \in \mathbb{Z}$, a_i and b_i not all 0. Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal lying above prime $p \in \mathbb{Z}$. Let $\lambda_1, \ldots, \lambda_s \in \mathbb{K}$ be such that $v_\mathfrak{p}(\lambda_i - 1) > \frac{e}{p-1}$ where $e = e_{\mathfrak{p}/p}$ is the ramification index, and such that the $\mathfrak{p}$-adic logarithms $\log\lambda_1, \ldots, \log\lambda_s$ are linearly independent over $\mathbb{Q}$. Let $f_P(x) = P(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s))$, with f_Q defined analogously.*

Assuming the p-adic Schanuel Conjecture, if $f_P(x) = f_Q(x) = 0$, then $x \in \mathbb{Q}$.

Proof. Suppose $x \in \mathcal{O}_\mathfrak{p}$ satisfies $f_P(x) = f_Q(x)$. Suppose that $x \notin \mathbb{Q}$. First, assume that the set $S = \{\log\lambda_1, \ldots, \log\lambda_s, x\log\lambda_1, \ldots, x\log\lambda_s\}$ is linearly independent over $\mathbb{Q}$. By the p-adic Schanuel Conjecture,

$$\begin{aligned} &\operatorname{trdeg}_\mathbb{Q}\mathbb{Q}(S \cup \{\exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s), \lambda_1, \ldots, \lambda_s\}) \\ &= \operatorname{trdeg}_\mathbb{Q}\mathbb{Q}(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s)) \geq 2s\,. \end{aligned} \tag{3.1}$$

[2] Let $f_\ell(x) = \sum_{n=0}^{\infty} a_n(x-z)^n$ be a power-series expansion of f_ℓ around z and calculate the respective smallest and largest indices $\mu < \nu$ for which $v_\mathfrak{p}(a_n) + nr = \min_{j\geq 0} v_\mathfrak{p}(a_j) + jr$ by computing each derivative $f_\ell^{(j)}(z) \bmod \pi^k$ for increasing powers k. By Thm. 9 there are $\nu - \mu$ extended $\mathfrak{p}$-adic zeros in the same residue class as z modulo π^r.

Now $f_P(x) = f_Q(x) = 0$ implies that $T = \{x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s)\}$ is comprised of at most $2s-1$ algebraically independent elements. Indeed, pick some element σ of $\{x_i : 0 \le i \le 2s\}$ with positive degree in P. Then $f_P(x) = 0$ implies that the component of T corresponding to σ is algebraic over the remaining components of T. Now $f_Q(x) = 0$ implies that the remaining components of S are algebraically dependent. Indeed, if σ does not appear in Q then this is obviously true, otherwise since P and Q are coprime, the multivariate resultant $\mathrm{Res}_\sigma(P, Q)$ is a non-zero polynomial in the remaining components of $\{x_i : 0 \le i \le 2s\} \setminus \{\sigma\}$ with a zero at $(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s))$ (see, e.g., [7, pp. 163–164]). Thus

$$\mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s)) \le 2s-1 \tag{3.2}$$

which contradicts (3.1).

We deduce that the set S must be linearly dependent over $\mathbb{Q}$. Consequently, we have

$$\sum_{i=1}^{s}(a_i + b_i x)\log\lambda_i = 0$$

for some a_i, $b_i \in \mathbb{Z}$, with the b_i not all zero. Without loss of generality, assume that $b_1 \neq 0$. Suppose now that $S \setminus \{x\log\lambda_1\}$ is a $\mathbb{Q}$-linearly independent set. Then the p-adic Schanuel Conjecture gives

$$\begin{aligned}&\mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(S \cup \{\exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s), \lambda_1, \ldots, \lambda_s\})\\ &= \mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s)) \ge 2s-1\,.\end{aligned} \tag{3.3}$$

Note that the multivariate polynomial $R(x_0, \ldots x_s) = \sum_{i=1}^{s}(a_i + b_i x_0)x_i$ is irreducible. Indeed, if R were reducible then $R = R_1R_2$ with $R_1 = R_1(x_0)$ and $R_2 = R_2(x_1, \ldots, x_s)$ linear polynomials with rational coefficients. Since $x \notin \mathbb{Q}$, $R_1(x) \neq 0$ so $R_2(\log\lambda_1, \ldots, \log\lambda_s) = 0$, which contradicts $\mathbb{Q}$-linear independence of $\log\lambda_1, \ldots, \log\lambda_s$.

Now we have $f_P(x) = f_Q(x) = \sum_{i=1}^{s}(a_i + b_i x)\log\lambda_i = 0$, and the multivariate polynomials P, Q and $R(x_0, \ldots x_s) = \sum_{i=1}^{s}(a_i + b_i x_0)x_i$ are all coprime. Hence, by repeating the earlier argument with resultants several times on P, Q, R, the set T is comprised of at most $2s-2$ algebraically independent elements. Therefore,

$$\mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(x, \log\lambda_1, \ldots, \log\lambda_s, \exp(x\log\lambda_1), \ldots, \exp(x\log\lambda_s)) \le 2s-2 \tag{3.4}$$

which contradicts (3.3). We conclude that the elements $\log\lambda_1, \ldots, \log\lambda_s, x\log\lambda_2, \ldots, x\log\lambda_s$ are linearly dependent over $\mathbb{Q}$. So

$$\sum_{i=1}^{s}(a_i + b_i x)\log\lambda_i = \sum_{i=1}^{s}(c_i + d_i x)\log\lambda_i = 0$$

for $a_i, b_i, c_i, d_i \in \mathbb{Z}$, and $b_1 \neq 0$, $d_1 = 0$. Therefore,

$$x = -\frac{\sum_{i=1}^{s} a_i\log\lambda_i}{\sum_{j=1}^{s} b_j\log\lambda_j} = -\frac{\sum_{i=1}^{s} c_i\log\lambda_i}{\sum_{j=1}^{s} d_j\log\lambda_j}$$

and hence

$$\left(\sum_{i=1}^{s} a_i\log\lambda_i\right)\left(\sum_{j=1}^{s} d_j\log\lambda_j\right) - \left(\sum_{i=1}^{s} c_i\log\lambda_i\right)\left(\sum_{j=1}^{s} b_j\log\lambda_j\right) = 0\,. \tag{3.5}$$

This is a non-trivial algebraic relationship between $\log \lambda_1, \ldots, \log \lambda_s$. Indeed, suppose the coefficients of any monomial in $\log \lambda_1, \ldots, \log \lambda_s$ in the equation (3.5) are all zero. This gives the system of equations

$$\{a_i d_j + a_j d_i = c_i b_j + c_j b_i : 1 \leq i, j \leq s\}.$$

By taking the equation corresponding to $i = j = 1$, $d_1 = 0$ and $b_1 \neq 0$ imply that $c_1 = 0$. Therefore, we have

$$a_1 d_j = c_j b_1, \forall 1 \leq j \leq s$$

so $c_j = \frac{a_1}{b_1} d_j$ for all $1 \leq j \leq s$. Therefore $x = \frac{a_1}{b_1}$, contradicting our assumption that $x \notin \mathbb{Q}$.

But since $\log \lambda_1, \ldots, \log \lambda_s$ are $\mathbb{Q}$-linearly independent, the p-adic Schanuel Conjecture implies they are algebraically independent. This contradicts (3.5). We conclude finally that our initial assumption that $x \notin \mathbb{Q}$ must have been false, and so $x \in \mathbb{Q}$. ◀

Some remarks are in order.

▶ Remark 13. The result also holds if we work instead with Schanuel's Conjecture on elements of $\mathbb{C}$, and logarithms and exponentials over $\mathbb{C}$.

▶ Remark 14. By taking Q to be an integer polynomial in x_0 in the lemma statement, one sees that irrational algebraic numbers cannot be zeros of exponential polynomials that are not polynomials in the usual sense.

▶ Remark 15. In the language of the theorem, call f_P an exponential polynomial with algebraic coefficients if x_i does not appear in P with positive degree for $1 \leq i \leq s$. Then the theorem shows that any irrational zero z of an exponential polynomial with algebraic coefficients has a unique irreducible exponential polynomial with algebraic coefficients that it is a root of (if z is algebraic this is just its normal minimal polynomial). Therefore, just as in the case of algebraic numbers, we may associate to any *exponential-algebraic number* (i.e., a root of an exponential polynomial with algebraic coefficients) a unique *minimal* exponential polynomial with algebraic coefficients that it is a root of.

The application of this result to LRS is the following corollary.

▶ **Corollary 16.** *Let $\mathbb{K}$, $\lambda_1, \ldots, \lambda_s$ be as in Lem. 12. Let $P \in \mathbb{K}[x_0, x_1, \ldots, x_{2s}]$ be non-zero and irreducible and such that $x_1, \ldots x_s$ do not appear with positive degree in P. Let $f_P(x) = P(x, \log \lambda_1, \ldots, \log \lambda_s, \exp(x \log \lambda_1), \ldots, \exp(x \log \lambda_s))$. Assuming the p-adic Schanuel Conjecture, if $x \in \mathcal{O}_\mathfrak{p}$ is a zero of f_P with multiplicity ≥ 2 then $x \in \mathbb{Q}$.*

Proof. Let $Q \in \mathbb{K}[x_0, \ldots, x_{2s}]$ be the polynomial such that

$$f'_P(x) = Q(x, \log \lambda_1, \ldots, \log \lambda_s, \exp(x \log \lambda_1), \ldots, \exp(x \log \lambda_s)).$$

Suppose f_P, f'_P have an irrational common zero. We are done if we show P, Q are coprime to each other and to any irreducible polynomial $R = \sum_{i=1}^{s} (a_i + b_i x_0) x_i$ for any $a_i, b_i \in \mathbb{Z}$ not all zero, as then we can immediately conclude this cannot hold by Lem. 12.

Since P is irreducible, P, Q only fail to be coprime if $P \mid Q$. Note that

$$Q = \partial_0 P + \sum_{i=1}^{s} x_i x_{s+i} \partial_{s+i} P$$

Since P has no x_i component for each $1 \leq i \leq s$, we have $P|_{x_i=0,\, i \in I} = P$ is a non-zero polynomial dividing $Q|_{x_i=0,\, i \in I}$ for any subset $I \subseteq \{1, \ldots, s\}$. In particular this implies

that $P \mid \partial_0 P$, hence $\partial_0 P = 0$ since it has strictly lower total degree than P. Now using $I = \{1, \ldots, s\} \setminus i$ for each i, we also have $P \mid x_i x_{s+i} \partial_{s+i} P$. Since we assume f_P has a zero, we must have $P \mid \partial_{s+i} P$, implying $\partial_{s+i} P = 0$ since it has strictly smaller total degree than P. We conclude that P must be constant as all of its partial derivatives vanish. This is impossible as we assume f_P has a zero, so P and Q are coprime.

Now, since P has no x_i component for $1 \leq i \leq s$, P, R are obviously coprime.

Finally, R, Q are only not coprime if $R \mid Q$. Suppose that $Q = RT$ for some $T \in \mathbb{K}[x_0, \ldots, x_{2s}]$. Then setting all $x_i = 0$ for $1 \leq i \leq s$ makes both sides of the equation vanish, so in particular $\partial_0 P = 0$. But then P has no x_0 component, so clearly R cannot divide Q, so this is a contradiction. Thus, P, Q, R are all coprime for any choice of R as described, so Lem. 12 applies. This completes the proof. ◀

We may now ask, do there exist rational zeros of exponential polynomials f with irreducible underlying multivariate polynomials, with multiplicity greater than 1? Unfortunately, the answer is yes.

▶ **Example 17.** Let $Q(x, y) = x^2(x-1)+y^2$. Then $(x-1)$ is a prime ideal in $\overline{\mathbb{Q}}[x]$ which divides $x^2(x-1)$ exactly once and does not divide the coefficient of y^2, so by Eisenstein's criterion $Q(x, y)$ is irreducible in $\overline{\mathbb{Q}}[x][y] = \overline{\mathbb{Q}}[x, y]$. Now let $f(x) = Q(\exp(x \log 2) - 1, \exp(x \log 3) - 1)$. It is easy to see that 0 is a multiplicity 2 root of f.

It would be interesting to determine the lowest possible order of an LRS with irreducible associated multivariate polynomial and a zero with multiplicity greater than 1, however we do not investigate this further here.

3.3 The Algorithm and the Proof of Termination and Correctness

With Corollary 16 in hand, we may amend the algorithm outlined earlier for finding the $\mathfrak{p}$-adic zeros of an LRS. First we define a recursive subroutine given by Algorithm 1, which finds the $\mathfrak{p}$-adic zeros of a suitable $\mathfrak{p}$-adic analytic function f.

Using the subroutine in Algorithm 1, we present an algorithm to find all the $\mathfrak{p}$-adic zeros of an LRS as Algorithm 2. Computing the multiplicatively independent subset in Line 1 can be done by Masser's Theorem (Thm. 8). In Line 2 we use multiplicative relations to express the M-th power of each root that is not in the multiplicatively independent set as a monomial (with positive and negative integer powers) in those roots in the set. This allows us to express the subsequence $\langle u_{Mn+t} \rangle_{n=0}^{\infty}$ as a polynomial in n and the n-th powers of the multiplicatively independent roots.

Theorem 4 follows from the next result.

▶ **Proposition 18.** *Assuming the p-adic Schanuel Conjecture, Algorithm 2 always terminates. Upon termination it outputs all* $\mathfrak{p}$*-adic zeros of the given LRS* $\boldsymbol{u}$*.*

Proof. Since each factor P defined on line 5 is irreducible, by Corollary 16, the p-adic Schanuel Conjecture implies that every zero in $\mathcal{O}_{\mathfrak{p}}$ of f either has multiplicity 1 or is rational. Therefore, in the `zeroSearch` subroutine (Algorithm 1), all $\mathfrak{p}$-adic zeros of f with multiplicity greater than 1 will eventually be found by the search for rational zeros on line 14, and all $\mathfrak{p}$-adic zeros of f with multiplicity equal to 1 will eventually be found by the Hensel condition on line 8. Note that the multiplicity of every rational zero q can be determined by finding the first j such that $f^{(j)}(q) \neq 0$. This can be done as $f^{(j)}(q)$ is a polynomial in $\log \lambda_1^{MN}, \ldots, \log \lambda_s^{MN}$. By the p-adic Schanuel Conjecture, these logarithms are algebraically independent, hence $f^{(j)}(q) = 0$ iff the coefficients of $\log \lambda_i^{MN}$ are 0 for all i.

Algorithm 1 The `zeroSearch` subroutine

Input: A non-zero $\mathfrak{p}$-adic analytic function $f : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$, integer r representing the depth of the residue class considered, and residue class representative z_r of class $z_r \bmod \mathfrak{p}^r$. We let π be a computed uniformiser for $\mathfrak{p}$, and A a set of representatives of the residue field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ (both may be easily computed given $\mathbb{K}$ and $\mathfrak{p}$).

Output: A complete list of elements of $\mathcal{O}_\mathfrak{p}$ that are either rational zeros of f or give a specification of a $\mathfrak{p}$-adic zero of f.

```
define zeroSearch (f, r, z_r, zerosFound):
foreach a ∈ A do
    z_{r+1} ← z_r + aπ^r;
    multCount ← sum of the multiplicities of zeros x in zerosFound with
      x ≡ z_{r+1} mod π^{r+1};
    n ← the number (counting multiplicity) of extended p-adic zeros
      ≡ z_{r+1} mod π^{r+1} (computed using Thm. 9);
    if n = multCount then next a;
    else if n = multCount + 1 then
        if v_p(f'(z_{r+1})) < 2v_p(f(z_{r+1})) then append z_{r+1} to zerosFound;
        else append zeroSearch (f, r + 1, z_{r+1}, zerosFound) to zerosFound;
        next a
    else
        in parallel until (1) or (2) terminate do
            (1) foreach q ∈ ℚ with q ≡ z_{r+1} mod π^{r+1} do
                if f(q) = 0 then
                    Append q to zerosFound;
                    Append zeroSearch (f, r + 1, z_{r+1}, zerosFound) to zerosFound;
            (2) Append zeroSearch (f, r + 1, z_{r+1}, zerosFound) to zerosFound;
        multCount ← sum of the multiplicities of zeros x in zerosFound with
          x ≡ z_{r+1} mod π^{r+1};
        next a
return zerosFound
```

Algorithm 2 An algorithm to compute the $\mathfrak{p}$-adic zeros of an LRS $\boldsymbol{u}$

Input: An LRS $\boldsymbol{u}$, number field $\mathbb{K}$ containing $\boldsymbol{u}$ and its characteristic roots, and prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ lying above prime p with $v_{\mathfrak{p}}(\lambda) = 0$ for all characteristic roots λ.

Output: A list of elements of $\mathcal{O}_{\mathfrak{p}}$ giving specifications of all the $\mathfrak{p}$-adic zeros of $\boldsymbol{u}$.

Compute a multiplicatively independent subset $\{\lambda_1, \ldots, \lambda_s\}$ of the characteristic roots;

Compute least integer $M > 0$ such that for each $0 \leq t \leq M-1$ we may write $u_{Mn+t} = P_t(n, \lambda_1^n, \ldots, \lambda_s^n)$ for multivariate polynomial P_t with algebraic coefficients;

Compute least integer $N > 0$ such that $v_{\mathfrak{p}}(\lambda_i^{MN} - 1) > \frac{e}{p-1}$ for all $1 \leq i \leq s$, where $e = e_{\mathfrak{p}/p}$ is the ramification index;

foreach $0 \leq t \leq M-1$, $0 \leq \ell \leq N-1$ **do**

  foreach P irreducible factor of of P_t **do**

    $f(x) \leftarrow P(Nx + \ell, \exp(x \log \lambda_1^{MN}), \ldots, \exp(x \log \lambda_s^{MN}))$;

    output: `zeroSearch` $(f, 0, 0, \emptyset)$

Now, if f has any extended $\mathfrak{p}$-adic zero $x \in \mathbb{C}_p \setminus \mathcal{O}_{\mathfrak{p}}$, there is some R such that for every $z \in \mathcal{O}_{\mathfrak{p}}$, $v_{\mathfrak{p}}(x - z) < R$. Therefore, for large enough r, the number n computed in `zeroSearch` $(f, r, z_r,$ zerosFound$)$ does not count any extended $\mathfrak{p}$-adic zeros. This ensures that `zeroSearch` $(f, r, z_r,$ zerosFound$)$ always terminates for large enough r (since eventually multCount will equal n), which implies that `zeroSearch` $(f, 0, 0, \emptyset)$ terminates due to the recursive structure of the subroutine.

Since all $\mathfrak{p}$-adic zeros of f are eventually found, and termination can only occur once all $\mathfrak{p}$-adic zeros are found, the output is correct. ◀

▶ Remark 19. We stress that the p-adic Schanuel Conjecture is required only for termination, not for correctness. When the algorithm terminates, its output is unconditionally correct.

We end by noting a consequence for the Simultaneous Skolem Problem. Given two LRS $\boldsymbol{u}$, $\boldsymbol{v}$, suppose their exponential-polynomial expansions may be written in terms of multiplicatively independent characteristic roots $\{\lambda_1, \ldots, \lambda_s\}$ (possibly after going to subsequences to deal with roots of unity brought on from the multiplicative relations). Suppose the multivariate polynomials defined by the respective exponential-polynomial expansions are coprime.[3] In this case we say that $\boldsymbol{u}$ and $\boldsymbol{v}$ are *coprime*. We define the Simultaneous Skolem Problem to be the problem of deciding whether two LRS $\boldsymbol{u}$ and $\boldsymbol{v}$ share an integer zero.

▶ **Theorem 5.** *Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.*

Proof. Pick p such that the characteristic polynomials of both $\boldsymbol{u}, \boldsymbol{v}$ split in $\mathbb{Z}_p$, and consider the LRS $\boldsymbol{w}$ defined by $w_n = v_n^2 + pu_n^2$. For some $N \geq 1$, and all $0 \leq \ell \leq N-1$, their interpolants with respect to p are related by $f_{w,\ell} = f_{v,\ell}^2 + pf_{u,\ell}^2$. For all $x \in \mathbb{Z}_p$, $f_{w,\ell}(x) = 0$ iff $f_{v,\ell}(x) = f_{u,\ell}(x) = 0$. Indeed, if $f_{v,\ell}(x), f_{u,\ell}(x)$ are non-zero then $v_p(f_{v,\ell}(x)^2)$ is even, and $v_p(pf_{u,\ell}(x)^2)$ is odd, so $f_{w,\ell} \neq 0$.

By Thm. 4, we may find all p-adic zeros of $\boldsymbol{w}$. By coprimality of $\boldsymbol{u}, \boldsymbol{v}$, all the p-adic zeros found must be rational according to Lem. 12. Therefore they may be found by a brute-force guess-and-check search, which in particular identifies all common integer zeros. ◀

[3] Note that two LRS that are coprime in the sense of [8] are coprime in our sense.

▶ Remark 20. The condition that $\boldsymbol{u}$ and $\boldsymbol{v}$ are coprime is fairly generic. A sufficient condition for $\boldsymbol{u}$ and $\boldsymbol{v}$ to be coprime is that $\boldsymbol{v}$ has a characteristic root that is multiplicatively independent from the characteristic roots of $\boldsymbol{u}$ (or vice-versa).

3.4 The Skolem Conjecture and the Skolem Problem

As noted earlier, it is open whether there is a Turing reduction between $\texttt{FSP}(\mathbb{N})$ and $\texttt{FSP}(\mathcal{O}_\mathfrak{p})$. For a given sequence $\boldsymbol{u}$, if we happen to choose a prime ideal $\mathfrak{p}$ such that all $\mathfrak{p}$-adic zeros of $\boldsymbol{u}$ are rational, then they can all be identified, and the output of Algorithm 2 gives a certificate that we have found all the integer zeros. This solves $\texttt{FSP}(\mathbb{N})$ for $\boldsymbol{u}$. One may ask whether such a prime ideal always exists. It turns out that a generalisation of this idea is equivalent to the Skolem Conjecture, also known as the Exponential Local-Global Principle (see Conjecture 11).

▶ **Theorem 21.** *The Skolem Conjecture is equivalent to the following statement: if $\boldsymbol{u}$ is a simple rational LRBS taking values in the ring $\mathbb{Z}[\frac{1}{b}]$ for some integer b, then $\boldsymbol{u}$ has no integer zero iff there exists $N \in \mathbb{Z}_{\geq 1}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ lying above primes $p_1, \ldots, p_t$ coprime to b such that for all $0 \leq \ell \leq N-1$, there exists i such that $u_{Nn+\ell}$ has no $\mathfrak{p}_i$-adic zeros in $\mathbb{Z}_{p_i}$.*

Proof. Suppose $\boldsymbol{u}$ is a simple rational LRBS of order d taking values in the ring $\mathbb{Z}[\frac{1}{b}]$ for some integer b and that $\boldsymbol{u}$ has no integer zeros (the reverse implication is trivial for both statements).

Suppose the Skolem Conjecture holds, then there's an integer m with $\gcd(m, b) = 1$ and $u_n \not\equiv 0 \bmod m$ for all $n \in \mathbb{Z}$. Write

$$m = \prod_{i=1}^{t} p_i^{k_i}.$$

Since $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ has finitely many elements, the vector $(u_n, u_{n+1}, \ldots, u_{n+d-1})$ takes only finitely many values mod $p_i^{k_i}$ and thus eventually repeats. Since $\boldsymbol{u}$ has order d, this means that $u_n \bmod p^{k_i}$ is periodic, with some period N_i. Let $N = \prod_i N_i$. Then each subsequence $u_{Nn+\ell}$ for $0 \leq \ell \leq N-1$ is constant mod m. In particular, for each $0 \leq \ell \leq N-1$ there's i such that $u_{Nn+\ell} \not\equiv 0 \bmod p_i^{k_i}$. Therefore there are no $\mathfrak{p}_i$-adic zeros of $u_{Nn+\ell}$ in $\mathbb{Z}_{p_i}$.

Now suppose there exist N, $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, $p_1, \ldots, p_t$ as in the theorem statement. Then for each $0 \leq \ell \leq N-1$, the subsequence $u_{Nn+\ell}$ has no $\mathfrak{p}_i$-adic zeros in $\mathbb{Z}_{p_i}$ for some i, which means that $v_{p_i}(u_{Nn+\ell}) < k_\ell$ for some integer k_ℓ. Let $k = \max_\ell k_\ell$. Then the Skolem Conjecture holds for $\boldsymbol{u}$ with $m = \prod_i p_i^k$. ◀

4 Implementation and Experimental Analysis

The algorithm described in Algorithm 2 has been implemented into the Skolem tool[4] first introduced in [3], for primes p such that the characteristic polynomial g of a given LRS splits in $\mathbb{Z}_p$. Concretely, the tool first searches for the smallest prime greater than some prescribed lower bound (by default 3) such that g splits in $\mathbb{Z}_p$, before computing the p-adic zeros of $\boldsymbol{u}$. We have also implemented a shortened "Hensel-only" algorithm that assumes all zeros have multiplicity 1 and uses only Hensel's Lemma to identify zeros. This avoids having to

[4] `https://skolem.mpi-sws.org?padic`

d	Success (Count)	Total (Count)	%	🕐	Count of instances with n zeros for n: 0	1	2	3	4	5	6+	Avg prime	#Zeros of type $\mathbb{Z}$	$\mathbb{Q} \setminus \mathbb{Z}$	?
2	8886	8886	100%	0.6	4322	3730	625	112	59	20	18	9.2	839	108	4817
3	8921	8921	100%	2.2	3896	2825	1526	378	154	21	121	34.5	862	3	7962
4	9080	9160	99%	11.3	3527	3017	1687	537	183	28	101	144.7	983	2	9281
5	4892	9172	53%	25.7	1830	1710	903	316	95	13	25	263.8	568	0	4803
6	934	9162	10%	30.0	346	327	188	50	15	2	6	252.5	144	0	1081
7	96	9201	1%	33.3	29	34	22	8	3	0	0	240.9	17	0	97

Table 1 Summary of "Hensel-only" algorithm, for each order from $2-7$. The 🕐 indicates the average running time in seconds for successful cases (failed cases timeout at 60s). Averages are gray where skewed by having many timeouts (counts may also be affected, but should be considered relative to the successful cases).

d	Avg	StdDev	Max	Min	Timeouts
2	9	5	37	3	0/4435
3	35	29	227	5	0/4460
4	151	146	1831	5	0/4578
5	817	905	11677	7	0/4582
6	5962	6395	45413	7	1/4581
7	18164	13268	49957	31	1842/4602

(a) Growth of primes that would be used by the algorithm (mean, standard deviation, max and min of the required prime reported for each LRS order d), with timeout of 60s or if the prime would exceed 50000. The max at order 7 (gray) can be attributed to the timeout, rather than the true value.

d	Success	Total	%	🕐
2	8886	8886	100%	0.9
3	8920	8921	100%	3.0
4	8613	9160	94%	19.1
5	2	9172	0%	5.9
6	0	9162	0%	
7	0	9201	0%	

(b) Summary of the full algorithm with 60s timeout.

Table 2 Values gray where skewed by the timeout.

compute a multiplicatively independent subset of the characteristic roots, having to consider irreducible factors, and having to carry out a parallel search for rational zeros. LRS with p-adic zeros of multiplicity greater than 1 are relatively rare, so this shortened algorithm terminates for most (but not all) LRS in general. The tool is written in Python, using the SageMath computer-algebra system.

When a zero is found, the tool attempts to determine if it is an integer or rational zero. If this procedure is inconclusive the unidentified zero is likely to be transcendental over $\mathbb{Q}$, but we cannot be sure, thus it is reported as unknown. In the web interface, the user can request the p-adic expansion up to any given precision.

We report the analysis in Figure 1 and Tables 1, 2a, and 2b. Our experiments considered the same randomly generated set of LRS as used in [3], up to order 7 and ran with up to 24 instances in parallel on 32 core (including Hyper-Threading) Intel Xeon E5-2667 v2 machines with 256GB RAM. Instances which are degenerate or identically zero are excluded as unsupported. Recall that the goal of [3] was to find only *integer* zeros.

Table 1 considers the shortened "Hensel-only" algorithm. With a sixty-second timeout the tool completes almost all instances up to order 4, but reduces to around half of instances at order 5. In Table 2a and Figure 1d we considered the prime required on a 50% sample of the dataset, without computing the zeros (in order to speed up the computation). The tool appears to succeed within sixty seconds for LRS which require a prime up to between 400 and 500 (see Figure 1d). We observe the growth is approximately $d!$, and provides evidence of why the tool can easily handle order 4 and most of order 5, but order 6 would be an order

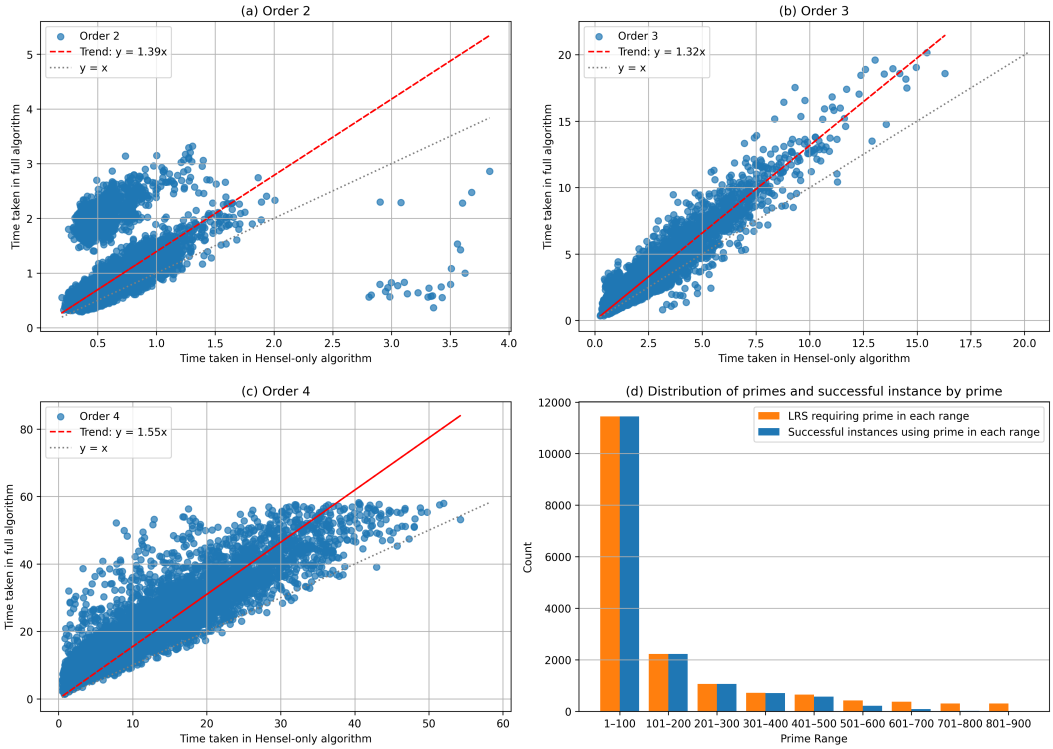

Figure 1 (a)-(c): Timing comparison between the Hensel-only and full algorithm (in seconds) in cases where both succeed within 60s. (d): Distribution of instances requiring a prime in a given range, and the instances for which the Hensel-only algorithm terminates in 60s (displayed up to 900); the system is highly effective up to primes of around 400-500 in this time limit.

of magnitude slower. The high standard deviation show that there is quite some spread.

The performance of Algorithm 2 is depicted in Table 2b. With a 60s timeout the tool is effective up to order 4, but a longer timeout would be required at order 5. Counts of zeros, zero types and average prime are not shown, but are comparable with Table 1 where computed. Not a single example of an LRS with a multiplicity of order greater than 1 was found in this randomly generated set of LRS, showing that these instances are relatively rare. Where both succeed for orders 2-4, the full alogrithm is between 1.3 to 1.5 times slower than the Hensel-only approach (see Figure 1a-c).

5 Concluding Remarks

5.1 A Remark on Rational Zeros

Note that rational non-integer zeros can be found as $\mathfrak{p}$-adic zeros for certain $\mathfrak{p}$, but not always. This is because, informally, interpolating an LRS $\boldsymbol{u}$ using some prime ideal $\mathfrak{p}$ fixes a definition of each $\lambda_i^{\frac{1}{b}}$ for each $b \in \mathbb{Z}_{\geq 1}$, whereas the notion of rational zero allows $\lambda_i^{\frac{1}{b}}$ to be any b-th root of λ_i. This phenomenon can be seen in the example below.

▶ **Example 22.** Consider the Tribonacci sequence, defined by $u_{n+3} = u_{n+2} + n_{n+1} + u_n$ and $u_0 = 0$, $u_1 = u_2 = 1$. In [4] it is shown that the set of rational zeros of the Tribonacci sequence is exactly $\{0, -1, -4, -17, 1/3, -5/3\}$.

The characteristic polynomial of the Tribonacci sequence splits in $\mathbb{Z}_p$ for $p = 47, 103, 199$ (among others). Let the ℓ-th interpolant with respect to p be denoted $f_{p,\ell}$, that is, the analytic function $f_{p,\ell} : \mathbb{Z}_p \to \mathbb{Z}_p$ such that $f_{p,\ell}(n) = u_{Nn+\ell}$ for $\ell \in \{0, \ldots, N-1\}$. Here we used $N = 46, 51, 198$ for $p = 47, 103, 199$ respectively. We used the tool to compute all the p-adic zeros of $\boldsymbol{u}$ for each p. Define $\mathcal{Z}_p$ to be the set of tuples (z, ℓ), where z is the p-adic zero of $\boldsymbol{u}$ such that $f_{p,\ell}(z) = 0$.

$$\begin{aligned}
\mathcal{Z}_{47} &= \{(0,0), (-2/3, 29), (-1, 29), (-2/3, 31), (-1, 42), (-1, 45)\} \\
\mathcal{Z}_{103} &= \{(0,0), (-1/3, 13), (-1/3, 16), (-1/3, 17), (-2/3, 17), (-2/3, 30), \\
&\qquad (-2/3, 33), (-2/3, 34), (-1, 34), (-1, 47), (-1, 50)\}, \\
\mathcal{Z}_{199} &= \{(0,0), (185 + 195 \cdot 199 + 135 \cdot 199^2 + \ldots, 26), (-1/3, 49), (-1/3, 62), \\
&\qquad (-1/3, 65), (-1/3, 66), (52 + 63 \cdot 199 + 3 \cdot 199^2 + \ldots, 92), (-2/3, 115), \\
&\qquad (-2/3, 128), (-2/3, 131), (-2/3, 132), (118 + 129 \cdot 199 + 69 \cdot 199^2 + \ldots, 158), \\
&\qquad (-1, 181), (-1, 194), (-1, 197)\}.
\end{aligned}$$

For each tuple (z, ℓ) corresponding to a rational zero of $\boldsymbol{u}$, recover the rational zero as $Nz + \ell$.

- For $p = 47$ and $N = 46$, all the rational zeros of $\boldsymbol{u}$ are correctly identified and there are no transcendental 47-adic zeros.
- For $p = 103$ and $N = 51$, each integer zero gives rise to three 103-adic zeros. For example, $n = -4$ gives rise to $(-1/3, 13), (-2/3, 30), (-1, 47)$. However, the rational zeros of $\boldsymbol{u}$ do not appear as 103-adic zeros of $\boldsymbol{u}$. There are also no transcendental 103-adic zeros of $\boldsymbol{u}$.
- For $p = 199$ and $N = 198$, again each integer zero gives rise to three 199-adic zeros. Similarly to $p = 103$, the rational zeros of $\boldsymbol{u}$ do not appear as 199-adic zeros, but there are several transcendental 199-adic zeros of $\boldsymbol{u}$.

5.2 Further Research

We have described and implemented an algorithm to determine a finite representation of all p-adic zeros of an LRS for suitable p, with termination subject to the p-adic Schanuel Conjecture. However, the ideas in this paper have further implications. Instead of interpolating an LRS in $\mathcal{O}_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$, we can instead choose a branch of the complex logarithm and interpolate an LRS $\boldsymbol{u}$ to get a function $f : \mathbb{C} \to \mathbb{C}$. Further, if $\boldsymbol{u}$ is a rational LRS, we can restrict to a function $f_\mathbb{R} : \mathbb{R} \to \mathbb{R}$. As pointed out in Remark 13, a version of Lem. 12 holds when interpolating in $\mathbb{R}$ or $\mathbb{C}$ as well, hence a version of Corollary 16 holds for such g too (subject to Schanuel's Conjecture). One can use this in conjunction with ideas of [6] to find an algorithm to determine whether $f_\mathbb{R}$ has a zero on bounded intervals, and in some cases in $\mathbb{R}$. We plan to explore this more in future work.

Furthermore, we note that any p-adic zero of an LRS $\boldsymbol{u}$ that has been found by Hensel's Lemma in our algorithm can be approximated to high precision very efficiently. In cases where an upper bound is known on the largest size of an integer zero of $\boldsymbol{u}$ (such as for order-4 LRS), this provides a potentially much faster way to elicit all the zeros of $\boldsymbol{u}$. We also plan to expand on this in a future paper.

References

1 Piotr Bacik. Completing the picture for the Skolem Problem on order-4 linear recurrence sequences, January 2025. arXiv:2409.01221 version: 2. `arXiv:2409.01221`.

2 Yuri Bilu. Skolem problem for linear recurrence sequences with 4 dominant roots (after mignotte, shorey, tijdeman, vereshchagin and bacik), 2025. `arXiv:2501.16290`.

3 Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. Skolem Meets Schanuel. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2022.20.

4 Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, and James Worrell. Twisted rational zeros of linear recurrence sequences, 2024. arXiv:2401.06537.

5 Frank Calegari and Barry Mazur. Nearly ordinary Galois deformations over arbitrary number fields. *Journal of the Institute of Mathematics of Jussieu*, 8(1):99–177, 2009. doi:10.1017/S1474748008000327.

6 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the Skolem Problem for Continuous Linear Dynamical Systems. In *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 100:1–100:13, Dagstuhl, Germany, 2016. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ICALP.2016.100.

7 David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, Cham, 2015. doi:10.1007/978-3-319-16721-3.

8 G. R. Everest and A. J. van der Poorten. Factorisation in the ring of exponential polynomials. *Proceedings of the American Mathematical Society*, 125(5):1293–1298, July 2002. doi:10.1090/S0002-9939-97-03919-1.

9 Graham Everest, Alf Van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*. Number v. 104 in Mathematical surveys and monographs. American Mathematical Society, Providence, RI, 2003.

10 Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2(5):417–421, 8 1953. doi:10.1007/BF02590997.

11 Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the Skolem Problem and the Skolem Conjecture. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 1–9, Haifa Israel, 2022. ACM. doi:10.1145/3531130.3533328.

12 K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38:50–60, 1935.

13 Nathanuel Mariaule. *On the decidability of the p-adic exponential ring*. PhD thesis, University of Manchester, 2013. URL: https://research.manchester.ac.uk/en/studentTheses/on-the-decidability-of-the-p-adic-exponential-ring.

14 D. W. Masser. *Linear relations on algebraic groups*, page 248–262. Cambridge University Press, 1988.

15 Alain Robert. *A course in p-adic analysis*. Number 198 in Graduate texts in mathematics. Springer, New York, NY, 2000. doi:10.1007/978-1-4757-3254-2.

16 Th. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. 8. Skand. Mat.-Kongr., 163-188 (1935)., 1935.

17 R. Tijdeman, M. Mignotte, and T.N. Shorey. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1984(349):63–76, May 1984. doi:10.1515/crll.1984.349.63.

18 N. K. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical Notes of the Academy of Sciences of the USSR*, 38(2):609–615, 1985. doi:10.1007/BF01156238.