The Skolem Problem

Contents

1 Introduction

Let R be a unital commutative ring with no zero divisors. A linear recurrence sequence (LRS) over R is a sequence $\mathbf{u} = \{u_n\}_{n=0}^{\infty}$ of elements in R which satisfies a recurrence of the form

$$u_{n+k} = a_0 u_{n+k-1} + \cdots + a_{k-1} u_n, \tag{1}$$

where the constants $a_0, \ldots, a_{k-1} \in R$ are referred to as the recurrence coefficients of $\mathbf{u}$ and say that $\mathbf{u}$ is an R-LRS. We will refer to (1) as the recurrence relation of $\mathbf{u}$, here (1) has order k. We write $\mathbf{u}$ to refer to the whole sequence and u_n for a specific term, indexed by $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$. With $u_0, \ldots, u_{n-1}$ (referred to as initial terms of $\mathbf{u}$), (1) uniquely determines $\mathbf{u}$. The LRS $\mathbf{u}$ may satisfy many different recurrences but it satisfies a unique recurrence of minimal order - we will assume that the recurrence relation for every LRS $\mathbf{u}$ in this article is of minimal order, so in (1), we have $a_{k-1} \neq 0$ and we define the order of the LRS $\mathbf{u}$ to be k. We define $\mathrm{Ann}(\mathbf{u}) = \{n \in \mathbb{N} \mid u_n = 0\}$ to be the annihilator of $\mathbf{u}$. What is the shape of $\mathrm{Ann}(\mathbf{u})$?

Example 1.1. Consider the Fibonacci sequence given by $u_0 = u_1 = 1$ and $u_{n+2} = u_{n+1} + u_n$. Clearly $u_n > 0$ for all $n \geq 0$ so $\mathrm{Ann}(\mathbf{u}) = \emptyset$. If instead we considered a shifted Fibonacci sequence $u_0 = 0, u_1 = 1$, then we would, by the same argument, have $\mathrm{Ann}(\mathbf{u}) = \{0\}$, a finite set.

Example 1.2. Consider the following modification of the Fibonacci sequence given by $u_0 = 0, u_1 = 0, u_2 = 1, u_3 = 0$ and the recurrence $u_{n+4} = u_{n+2} + u_n$. At every even n, it is the sum of two zeroes, for odd n, we get the typical Fibonacci sequence. Therefore $\mathrm{Ann}(\mathbf{u}) = \{1\} \cup \{n \mid n \equiv 0 \bmod 2\}$, the union of a finite set and an arithmetic progression.

These examples cover every case, according to the Skolem-Mahler-Lech theorem [36, 24, 7] which characterises the set $\mathrm{Ann}(\mathbf{u})$:

Theorem 1.3 (Skolem-Mahler-Lech Theorem)**.** *Let $\boldsymbol{u}$ be a LRS over a field of characteristic zero. Then we have $r, j_1, \ldots, j_m \in \mathbb{N}$ (m may be zero) and a finite set $S \subset \mathbb{N}$ such that*

$$Ann(\boldsymbol{u}) = S \cup \bigcup_{i=1}^{m} \{j_i + rq \mid q \in \mathbb{N}\}.$$

The integers $r, j_1, \ldots, j_m$ and the finite set S depend only on $\boldsymbol{u}$.

Sets of the same form as $\mathrm{Ann}(\mathbf{u})$ will frequently appear so we make the following definition:

Definition 1.4. A set A is quasi-periodic if it is the union of a finite set and finitely many arithmetic progressions.

All known proofs of the Skolem-Mahler-Lech theorem are non constructive - they provide no algorithm to determine the zero set. This leads us to the Skolem Problem:

Problem 1.5 (Skolem Problem)**.** Let $\mathbf{u}$ be a LRS over a field of characteristic zero. Is there an algorithm to determine whether $\operatorname{Ann}(\mathbf{u}) \neq \emptyset$?

The Skolem Problem has been characterised by Tao [37] as 'the halting problem for linear automata'. Decidability of the Skolem Problem is important to several areas and problems in thereotical computer science, such as loop termination [30] and the algorithmic analysis of stochastic systems [9]. It also has appeared in other contexts, such as formal power series [31] and control theory [4].

In this essay, first we will prove the Skolem-Mahler-Lech theorem for LRS over a field of characteristic zero, following a proof in [16]. Then we will demonstrate the decidability of the Skolem Problem for $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS of order up to 4 - and define the MSTV class, a class of LRS for which the Skolem Problem is decidable as shown in [28, 18]. The second half of the essay will be concerned with two modern developments. The first, based on [20, 3], considers results conditional on the Skolem Conjecture, a resolution for an analogous Skolem Problem for linear recurrence bisequences, a sequence obtained by running a LRS forwards and backwards. Assuming this conjecture and the p-adic Schanuel conjecture, an important conjecture in transcendental number theory, we show that the Skolem Problem is decidable for all simple $\mathbb{Q}$-LRS. The second, based on [21, 23], constructs (which we only cite) a set within which the Skolem Problem is solvable, a universal Skolem set, and shows that this set has positive density of at least 0.29 unconditionally and density 1 conditional on the Bateman-Horn conjecture - a vast generalisation of many conjectures and problems on the distribution of primes.

2 Preliminaries

Here we outline properties of LRS which will be used throughout the essay, following chapter 1 of [12]. Throughout this essay, we write $\overline{\mathbb{Q}}$ to mean the algebraic closure of $\mathbb{Q}$, a subfield of $\mathbb{C}$. Every ring in this essay will be a unital commutative ring with no zero divisors and every field considered will be of characteristic zero, unless stated otherwise.

Basic properties of Linear Recurrence Sequences

Let $\mathbf{u}$ be a LRS over a ring R with recurrence coefficients $a_0, \dots, a_{k-1} \in R$. We define the characteristic polynomial g of $\mathbf{u}$ by

$$g(x) = X^k - a_0 X^{k-1} - \cdots - a_{k-1}. \tag{2}$$

If R is a field, say K, let L be the splitting field of g. We can apply the following results for LRS $\mathbf{u}$ in a field to $\mathbf{Z}$-LRS by viewing a $\mathbf{Z}$-LRS as a $\mathbf{Q}$-LRS. Then we can factorise the characteristic polynomial over L:

$$g(x) = \prod_{i=1}^{l} (X - \lambda_i)^{\nu_i}.$$

$\lambda_1, \ldots, \lambda_l \in L$ are the distinct roots of $g(x)$, of multiplicity $\nu_1, \ldots, \nu_l$ respectively - we shall refer to the λ_i as characteristic roots. The minimality of the LRS gives $a_{k-1} \neq 0$ so each $\lambda_i \neq 0$. If $\nu_i = 1$ for all i then we say that the LRS $\mathbf{u}$ is simple. If the ratio $\frac{\lambda_i}{\lambda_j}$ for $i \neq j$ of characteristic roots is never a root of unity then we say that $\mathbf{u}$ is non degenerate, otherwise it is degenerate.

The connection between the characteristic polynomial of recurrence relation of a LRS $\mathbf{u}$ can be seen by substituting $u_n = \lambda^n$ into (1) for $\lambda \in L$ and $n \in \mathbb{N}$ - we get $g(\lambda) = 0$. This leads us to the exponential-polynomial representation of $\mathbf{u}$:

$$u_n = \sum_{i=1}^{l} Q_i(n)\lambda_i^n \tag{3}$$

where $Q_i(X) \in L[X]$ are polynomials of degrees $\nu_i - 1$ for $i = 1, \ldots, l$.

Remark 2.1. When dealing with a $\mathbb{Q}$-LRS $\mathbf{u}$, it can be useful to rescale $\mathbf{u}$ into a $\mathbb{Z}$-LRS $\mathbf{v}$. This can be done with a geometric scaling $v_n = C^n u_n$ where C is the least common multiple of the denominators of $u_0, \ldots, u_{n-1}, a_0, \ldots, a_{n-1}$ for $n \in \mathbb{N}$. The recurrence relation (1) which $\mathbf{v}$ satisfies has recurrence coefficients $b_i = C^{i+1}a_i$ for $0 \leq i \leq k-1$ so its characteristic roots are multiplied by C, $\mu_i = C\lambda_i$ for $1 \leq i \leq l$. In particular, the ratios of characteristic roots are preserved. We can also use a geometric scaling to a $\overline{\mathbb{Q}}$-LRS to turn the recurrence coefficients into algebraic integers.

Remark 2.2. A decomposition of $\mathbf{u}$ into a collection of non degenerate LRS can be done as shown in claim 2.3. Recall λ_i are distinct so the ratio $\frac{\lambda_i}{\lambda_j}$ is never 1. Assume that the ratio $\frac{\lambda_i}{\lambda_j}$ is a root of unity for some $i \neq j$ - otherwise there would be nothing to prove.

Claim 2.3. *Let M be the least common multiple of the orders of the roots of unity in the set $\{\frac{\lambda_i}{\lambda_j} \mid i, j \leq l\}$. Then for each $0 \leq j < M$, the subsequence $\mathbf{u}_{M,j} = (u_{Mn+j})_{n \geq 0}$ is non degenerate or zero.*

Proof. The characteristic roots of $\mathbf{u}_{M,j}$ are distinct members $\beta_1, \ldots, \beta_s$ of the set $\{\lambda_1^M, \ldots, \lambda_l^M\}$. If the LRS $\mathbf{u}_{M,j}$ is zero then we have no β_j so suppose it is non zero. Then if $\mathbf{u}_{M,j}$ is degenerate, we have, for $i \neq j$ and some minimal integer t, $(\frac{\beta_i}{\beta_j})^t = (\frac{\lambda_i}{\lambda_j})^{Mt} = 1$. Since M was the least common multiple, we have $t = 1$ so $\beta_i = \beta_j$, contradicting the assumption that they are distinct. This gives us a decomposition of $\mathbf{u}$ into a union of LRS $\mathbf{u}_{M,r}$ which are either zero or non degenerate. $\mathbf{u}_{M,j}$ satisfies a recurrence relation of order at most k and M can be computed effectively - both claims are shown in [21], Section II B. □

Another useful representation of a LRS is the matrix representation, valid over rings R. Let $\mathbf{u}$ be a LRS over a ring R with characteristic polynomial g. Let A

be the companion matrix of g

$$A = \begin{pmatrix} a_0 & \cdots & a_{k-2} & a_{k-1} \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

With $\alpha = (0 \dots 01)$ and $\beta = (u_{k-1} \dots u_1 u_0)^T$ we have

$$u_n = \alpha A^n \beta \text{ for } n \in \mathbb{N} \tag{4}$$

Remark 2.4. We refer to A as the companion matrix of $\mathbf{u}$. Note that $\det(A) = \pm a_{k-1}$. Because of the assumption of minimality, we know $a_{k-1} \neq 0$ so A is invertible. If $R = K$ is a field, then given a row vector γ, a column vector δ and an invertible matrix B, we can perform row reduction to cast B in the same form as the companion matrix as the rows and columns are linearly independent. Therefore the sequence $v_n = \gamma B^n \delta$ is also a LRS.

Heights

In this section, we detail relevant material on heights that will be used throughout the essay, following Chapter 14 of [25]. We will only consider heights of algebraic numbers. We will define a height $H(\beta)$ which has the important property that for any $d \in \mathbb{N}$ and $\mathcal{H} \in \mathbb{R}$ there are only finitely many algebraic numbers β of degree d such that $H(\beta) \leq \mathcal{H}$, known as Northcott's theorem.

Suppose $\beta \in \overline{\mathbb{Q}}$ is of degree $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$. Then it has a non zero minimal polynomial $B \in \mathbb{Q}[X]$. By clearing denominators, we can write

$$B(x) = b_0 X^d + b_1 X^{d-1} + \cdots + b_d$$

where $\gcd(b_0, \dots, b_d) = 1$. Enforcing $b_0 \geq 1$, this fixes B uniquely. Over $\mathbb{C}$ we can factorise B as

$$B(X) = b_0 (X - \beta_1) \dots (X - \beta_d)$$

Then we define the height of β by

$$H(\beta)^d = b_0 \max(1, |\beta_1|) \dots \max(1, |\beta_d|) \geq 1$$

We have the following set of properties of the height H:

Proposition 2.5. Let $\beta_1, \dots, \beta_n$ be non zero algebraic numbers and suppose that $\alpha \in K$ is a non zero algebraic number where K is a number field such that $[K : \mathbb{Q}] = D$. Then we have

(a) Let $P \in \mathbb{Z}[X_1, \dots, X_n]$ be of degree at most $L_1, \dots, L_n$ in $X_1, \dots, X_n$ respectively. Then we have

$$H(P(\beta_1, \dots, \beta_n)) \leq \mathcal{L}(P) H(\beta_1)^{L_1} \dots H(\beta_n)^{L_n}$$

where $\mathcal{L}(P)$ is the sum of absolute values of the coefficients of P.

(b) $H(\alpha) = H\left(\frac{1}{\alpha}\right)$.

(c) $H(\alpha)^{-D} \leq |\alpha| \leq H(\alpha)^D$.

(d) $|N_{K/\mathbb{Q}}(\alpha)| \leq H(\alpha)^D$.

Proof. (a) This is Proposition 14.7 of [25]

(b) This claim is in the remarks following Proposition 14.4 of [25]; it is equation (14.24) on Page 174.

(c) The first inequality $H(\alpha)^{-D} \leq |\alpha|$ of is Proposition 14.13 of [25]. The second inequality follows through a combination of this with (b):

$$\left|\frac{1}{\alpha}\right| \geq H\left(\frac{1}{\alpha}\right)^{-D} = H(\alpha)^{-D} \implies |\alpha| \leq H(\alpha)^D$$

(d) We have, where α_i are Galois conjugates of α,

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{d} |\alpha_i| \leq \max(1, |\alpha_1|) \ldots \max(1, |\alpha_d|) \leq H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

Now $|N_{K/\mathbb{Q}}(\alpha)| = |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|^{[K:\mathbb{Q}(\alpha)]} \leq H(\alpha)^D$ by the tower law as $H(\alpha) \geq 1$.

□

Remark 2.6. Let $\alpha_1, \ldots, \alpha_r$ be algebraic numbers. Throughout this essay, we say a real number x is computable in terms of $\alpha_1, \ldots, \alpha_r$ if there is an algorithm which can compute an upper bound for x in terms of the heights and degrees of $\alpha_1, \ldots, \alpha_r$. From Proposition 2.5, quantities expressible in terms of a polynomial with algebraic coefficients in $\alpha_1, \ldots, \alpha_r$ are computable. This is because by (a), we have

$$H(\alpha\beta) \leq H(\alpha)H(\beta), H(\alpha^n) \leq H(\alpha)^n, H(\alpha + \beta) \leq 2H(\alpha)H(\beta)$$

where $n \in \mathbb{Z}$ in combination with (b).

If $\beta \in \mathcal{O}_K$ then $v_{\mathfrak{p}}(\beta) = m$ is computable in terms of β. This is because $(\beta) = \mathfrak{p}^m I$ for an ideal I such that $\mathfrak{p} \nmid I$ so $N_{K/\mathbb{Q}}((\beta)) \geq N_{K/\mathbb{Q}}(\mathfrak{p})^m$ so m is computable. Say $\mathfrak{p}$ lies above a rational prime p and $(\beta) = \mathfrak{p}^m I$ where $m \geq 1$. Then p is computable in terms of β as $p \mid N_{K/\mathbb{Q}}(\mathfrak{p})$ so $p \leq N_{K/\mathbb{Q}}((\beta))^{\frac{1}{m}} \leq N_{K/\mathbb{Q}}((\beta))$.

Let $\mathbf{u}$ be a LRS with characteristic roots λ_i, recurrence coefficients a_i and exponential-polynomial representation $u_n = \sum_{i=1}^{n} Q_i(n)\lambda_i^n$. As in [23] page 4, we can see that Cramer's rule allows us to find the coefficients of Q_i in terms of the recurrence coefficients a_i and the characteristic roots λ_j so they are computable in terms of the a_i and λ_j. Notably, if $\mathbf{u}$ is a $\overline{\mathbb{Q}}$-LRS, the coefficients of Q_i are also algebraic.

$\mathfrak{p}$-adic valuation

Let K be a number field, $\mathcal{O}_K$ be its its ring of integers and $\mathfrak{p}$ be a non zero prime ideal in $\mathcal{O}_K$. A $\mathfrak{p}$-adic valuation can be defined analogously to the p-adic valuation v_p on $\mathbb{Q}$. We define the function $v_\mathfrak{p} : \mathcal{O}_K - \{0\} \to \mathbb{N}$ as follows. If $x \in \mathcal{O}_K - \{0\}$ then $x\mathcal{O}_K = \mathfrak{p}^m I$ for some ideal I for which $\mathfrak{p} \nmid I$ and $m \geq 0$. We set $v_\mathfrak{p}(x) = m$.

We then have both $v_\mathfrak{p}(x+y) \geq \min\{v_\mathfrak{p}(x), v_\mathfrak{p}(y)\}$ and $v_\mathfrak{p}(xy) = v_\mathfrak{p}(x)+v_\mathfrak{p}(y)$ for non zero $x, y \in \mathcal{O}_K$. We can extend $v_\mathfrak{p}$ to $K^\times$ - if $z = \frac{x}{y}$ for non zero $x, y \in \mathcal{O}_K$ then define $v_\mathfrak{p}(z) = v_\mathfrak{p}(x) - v_\mathfrak{p}(y)$. This is well defined and $v_\mathfrak{p}$ extends to a valuation on K as shown in [10].

The p-adic exponential and the p-adic logarithm

Let p be an odd rational prime. Recall the p-adic absolute value $| \ |_p$ defined on $\mathbb{Q}$ and let $x \in \mathbb{Q}_p$. Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. Then $| \ |_p$ extends uniquely to $\mathbb{C}_p$ [15]. We define the p-adic exponential by the following series:

$$\exp_p(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!} \tag{5}$$

This series converges on $S = \{x \in \mathbb{C}_p \mid |x|_p < p^{-\frac{1}{p-1}}\}$. Similarly, the p-adic logarithm can be defined by the series

$$\log_p(x) = \sum_{k=0}^{\infty} \frac{(-1)^{k+1}(x-1)^k}{k} \tag{6}$$

This series converges on $T = \{x \in \mathbb{C}_p \mid |x-1|_p < 1\}$. Note that $T \cap \mathbb{Q}_p = 1+p\mathbb{Z}_p$. We have $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ for $x, y \in S$, $\log_p(zw) = \log_p(z)+\log_p(w)$ for $z, w \in T$. By setting $\log_p(p) = 0$ we can extend $\log_p$ to $\mathbb{C}_p^\times$ using this last property.

Useful theorems

Here we record some useful theorems that will be used throughout the essay. Let K be a number field with ring of integers $\mathcal{O}_K$. A useful result by Kronecker [19] is the following:

Theorem 2.7. *Every non zero $\alpha \in \mathcal{O}_K$ that lies with its conjugates in the closed unit disc $|z| \leq 1$ is a root of unity.*

This is Theorem 1.5.9 of [5]. A useful corollary is the following:

Theorem 2.8. *If $\alpha \in K^\times$ is not a root of unity and all of its Galois conjugates have modulus 1 then there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $v_\mathfrak{p}(\alpha_1) \neq 0$.*

Proof. By Theorem 2.7 we know that $\alpha \notin \mathcal{O}_K$. Therefore if n is such that $n\alpha \in \mathcal{O}_K$ then $n > 1$. Suppose to the contrary that $v_\mathfrak{p}(\alpha) = 0$ for all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$. Then we have that

$$v_\mathfrak{p}(n\alpha) = v_\mathfrak{p}(n) + v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(n).$$

This is true for all prime ideals so $(n\alpha) = (n)$ so $\alpha \in \mathcal{O}_K^\times$, a contradiction. □

3 The Skolem-Mahler-Lech Theorem

The Skolem-Mahler-Lech Theorem was first proven by Skolem in 1933 [36] for $\mathbb{Q}$-LRS, extended by Mahler in 1935 [24] to $\overline{\mathbb{Q}}$-LRS and extended again by Lech in 1953 [7] to LRS over a field of characteristic zero. We will follow a simpler proof by Hansel [16]. First, the theorem will be proven $\mathbb{Q}$-LRS. Then it will be extended to LRS over finite transcendental field extensions of $\mathbb{Q}$ and finally to LRS over fields of characteristic zero. The following exposition simplifies Hansel's proof by working with LRS instead of rational series and by using the matrix representation of a LRS (4).

The rational case

We aim to prove the following proposition:

Proposition 3.1. Let $(d_i)_{i\in\mathbb{N}}$ be a sequence of integers. For $n \in \mathbb{N}$, let $b_n = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$ for an odd prime p. Then $\operatorname{Ann}(\mathbf{b})$ is finite or all of $\mathbb{N}$.

Through the matrix representation of $\mathbf{u}$, this will be used to prove the Skolem-Mahler-Lech theorem for $\mathbb{Q}$-LRS by examining the companion matrix A of $\mathbf{u}$ modulo p for some prime p which doesn't divide $\det(A)$. Then we will have $A^r = I + pA'$ for some integer r and matrix A'. Then we calculate u_{j+rn} via the matrix representation for specific integers j and any $n \in \mathbb{N}$ and use Proposition 3.1.

Let p be a prime and let $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[X]$. Recall the p-adic valuation v_p defined on $\mathbb{Q}$. Define, for $i \in \mathbb{N}$, $v_p^i(P) = \inf(v_p(a_j)$ for $j \geq i)$ - if $i > n$, take $v_p^i(P) = \infty$. To prove Proposition 3.1, we begin by collecting results on $v_p^i(P)$.

We have

$$\begin{aligned} v_p(P(m)) &= v_p(a_0 + a_1 m + \cdots + a_n m^n) \\ &\geq \inf_{1\leq i\leq n}(v_p(a_i m^i)) \\ &\geq v_p(a_j m^j) \text{ for some } j \\ &= v_p(a_j) + v_p(m^j) \geq v_p(a_j) \geq v_p^0(P) \end{aligned}$$

With this, we prove the following lemma:

Lemma 3.2. *Let $P(x) \in \mathbb{Q}[X]$ and $m \in \mathbb{Z}$. Then if $R(x) = (x-m)P(x)$ we have $v_p^i(P) \geq v_p^{i+1}(R)$ for all $i \in \mathbb{N}$.*

Proof. Write $P(x) = a_0 + a_1x + \cdots + a_nx^n$ and $R(x) = b_0 + b_1x + \cdots + b_{n+1}x^{n+1}$. We have $b_{n+1} = a_n$ and $b_{i+1} = a_i - ma_{i+1}$ for $i = 0, 1, \ldots, n-1$. Solving for a_i, we get $a_i = b_{i+1} + mb_{i+2} + m^2b_{i+3} + \cdots + m^{n-i}b_{n+1}$ for $0 \leq i \leq n$. In the same way as the proof of $v_p(P(m)) \geq v_p^0(P)$, we see that $v_p(a_i) \geq v_p^{i+1}(R)$ so $v_p^i(P) \geq v_p^{i+1}(R)$. □

Now we can prove Proposition 3.1.

Proof of Proposition 3.1. Suppose that $\text{Ann}(\mathbf{b})$ is infinite. We will show that it is all of $\mathbb{N}$ by showing that for any pair $(q, u) \in \mathbb{N}^2$ that $v_p(b_q) \geq u$ so $b_q = 0$ for all $q \in \mathbb{N}$.

Let $R_n(x) = \sum_{i=0}^{n} \frac{x(x-1)\ldots(x-i+1)}{i!} d_ip^i$. We have that if $m \leq n$ then $R_n(m) = R_m(m) = b_m$. Next we show, for any $i \in \mathbb{N}$, that $v_p^i(R_n) \geq i - \frac{i}{p-1}$ (note p is an odd prime). If $R_n(x) = \sum_{i=0}^{n} c_i^{(n)}x^i$, then $c_i^{(n)}$ is a $\mathbb{Z}$-linear combination of $\frac{d_jp^j}{j!}$ where $j \geq i$. We have

$$v_p\left(\frac{d_jp^j}{j!}\right) \geq j - v_p(j!) \geq j - \frac{j}{p-1} \geq i - \frac{i}{p-1}$$

where $v_p(j!) \geq \frac{j}{p-1}$ by Legendre's formula. So for $i \in \mathbb{N}$, $v_p(c_i^{(n)}) \geq i - \frac{i}{p-1}$. Therefore $v_p^i(R_n) \geq i - \frac{i}{p-1}$.

Now fix $(q, u) \in \mathbb{N}^2$ and $i \in \mathbb{N}$ such that $i - \frac{i}{p-1} \geq u$. Let $m_1, \ldots, m_i$ be distinct members of $\text{Ann}(\mathbf{b})$ in increasing order and $N = \max(q, m_i)$. Then we know that $R_N(m_j) = 0$ for each $1 \leq j \leq i$ so we can write $R_N(x) = (x - m_1)\ldots(x - m_i)P(x)$ for some $P \in \mathbb{Q}[X]$. Therefore by Lemma 3.2, we have

$$v_p(b_q) = v_p(R_N(q)) \geq v_p(P(q)) \geq v_p^0(P) \geq v_p^i(R_N) \geq i - \frac{i}{p-1} \geq u$$

This completes the proof. □

Now we prove the Skolem-Mahler-Lech theorem for $\mathbb{Q}$.

Theorem 3.3 (Skolem-Mahler-Lech for $\mathbb{Q}$)**.** *Let $\boldsymbol{u}$ be a $\mathbb{Q}$-LRS of order k with companion matrix A. If p is an odd prime such that $p \nmid \det A$ then there is an integer $r \mid |GL_k(\mathbb{F}_p)|$ and $j_1, \ldots, j_m \in \{0, \ldots, r-1\}$ (m may be zero) and a finite set S such that*

$$Ann(\boldsymbol{u}) = S \cup \bigcup_{i=1}^{m} \{j_i + rq \mid q \in \mathbb{N}\}$$

Proof. Recall the matrix representation $u_n = \alpha A^n \beta$ for $n \geq 0$ by (4). Since we are looking for zeroes, we can rescale $\mathbf{u}$ to be a $\mathbb{Z}$-LRS without loss of generality. Then the companion matrix A has integer elements. Therefore $\det A = \pm a_{k-1} \in \mathbb{Z}$ and is non zero as the recurrence relation for $\mathbf{u}$ is minimal. Choose a prime p such that $p \nmid a_{k-1}$. Then the reduction $\overline{A}$ of A modulo p has determinant $\pm a_{k-1} \bmod p \not\equiv 0 \bmod p$ so $\overline{A}$ is invertible. Therefore by Lagrange's theorem, $\overline{A}^r = I$ and so $A^r = I + pA'$ for some matrix kxk matrix A' with integer entries and $r \mid |\mathrm{GL}_k(\mathbb{F}_p)|$. Taking $d_i = \alpha A^j A'^n \beta$, we have, for some $j \in \{0, \ldots, r-1\}$,

$$u_{j+rn} = \alpha A^{rn+j} \beta = \alpha A^j (I + pA')^n \beta = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$$

Ann($\mathbf{u}$) is the finite union of the sets $\{j + rn \mid u_{j+rn} = 0\}$ which are finite or $(j+rn)_{n \in \mathbb{N}}$ by Proposition 3.1. This proves the theorem. □

Remark 3.4. Note that we have an effective bound on r; we know that $r < (p^k - 1)(p^k - p) \ldots (p^k - p^{k-1})$. In the proof we rescaled the $\mathbb{Q}$-LRS $\mathbf{u}$ into a $\mathbb{Z}$-LRS. As in Remark 2.1, the ratios of the characteristic roots λ_i are preserved. Therefore $\lambda_i \in \mathcal{O}_K$ where $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_s)$ and $\mathcal{O}_K$ is the ring of integers. As $A^r \equiv I \bmod p$, we have $\lambda^r \equiv 1 \bmod p$ i.e $\lambda^r \in 1 + p\mathcal{O}_K$. For $i \neq j$, if $\frac{\lambda_i}{\lambda_j} = \omega$ is a root of unity of order n then $\lambda_i^r, \lambda_j^r \equiv 1 \bmod p$ so $\omega^r \equiv 1 \bmod p$. But this means that $n \mid r$ as $1, \omega, \ldots, \omega^{n-1}$ are distinct modulo p. This is because the polynomial $T^n - 1$ is separable modulo p if $p \nmid n$ - such p exists as there are infinitely many primes p which do not divide a_{k-1} and there are only finitely many ω. So we know that every root of unity among the ratios $\frac{\lambda_i}{\lambda_j}$ has an order dividing r. Combining the bound proven in Theorem 3.3 and the effective calculation of L as in Remark 2.2, we have a simple procedure to calculate r. We also know that $\mathbf{u}_{L,r} = (u_{Ln+r})_{n \geq 0}$ is a non degenerate sequence. It can be shown that the annihilator of a non degenerate sequence is finite or all of $\mathbb{N}$ as in Theorem 2.1 of [12].

Finite Transcendental Extensions of $\mathbb{Q}$

This section will be focused on extending Theorem 3.3 to $\mathbb{Q}(X_1, \ldots, X_m)$ - the field of rational functions in m variables with rational coefficients. Let $\mathbf{u}$ be a LRS of order k over $\mathbb{Q}(X_1, \ldots, X_m)$ with recurrence coefficients $a_i \in \mathbb{Q}(X_1, \ldots, X_m)$ and companion matrix $A \in \mathrm{GL}_k(\mathbb{Q}(X_1, \ldots, X_m))$. For $(h_1, \ldots, h_m) \in \mathbb{Q}^m$, write $\mathbf{u}(h_1, \ldots, h_m)$ for the $\mathbb{Q}$-LRS which satisfies a recurrence with recurrence coefficients $a_i(h_1, \ldots, h_m)$. Our proof will similarly work by rescaling the LRS to a $\mathbb{Z}[X_1, \ldots, X_m]$ LRS and finding a prime which doesn't divide the determinant of $A(h_1, \ldots, h_m)$ for all m tuples $(h_1, \ldots, h_m) \in \mathbb{Z}^m$. Since the determinant is now a polynomial, we seek a lemma to ensure this.

Lemma 3.5. *Let $P \in \mathbb{Z}[X_1, \ldots, X_m]$. Then there is an odd prime p and infinite sets $H_1, \ldots, H_m$ such that for $(h_1, \ldots, h_m) \in H_1 \times \cdots \times H_m$, $p \nmid P(h_1, \ldots, h_m)$.*

The following lemma will help us prove Lemma 3.5:

Lemma 3.6. *Let $P(X_1, \ldots, X_m)$ be a polynomial in m variables with coefficients in any field K. Suppose there are sets $S_1, \ldots, S_m$ in K such that*

1. *For each $i = 1, \ldots, m$, $|S_i| > \deg_{X_i}(P)$.*
2. *For all $(s_1, \ldots, s_m) \in S_1 \times \cdots \times S_m$, $P(s_1, \ldots, s_m) = 0$.*

Then P is the zero polynomial.

Proof. This is clear by induction. □

Now we prove Lemma 3.5.

Proof of Lemma 3.5. Let p be an odd prime which doesn't divide any coefficient of P and suppose that $p > \max(\deg_{X_i}(P))$ for each i. Then $\overline{P} \in (\mathbb{Z}/p\mathbb{Z})[X_1, \ldots, X_m]$, the reduction of P modulo p, is a non zero polynomial. For $i = 1, \ldots, m$, let $S_i = \{0, 1, \ldots, \deg_{X_i}(P)\}$. By Lemma 3.6 with $K = \mathbb{Z}/p\mathbb{Z}$, we have $(s_1, \ldots, s_m) \in \mathbb{Z}^m$ such that $\overline{P}(s_1, \ldots, s_m) \neq 0$ so we have $p \nmid P(s_1 + n_1 p, \ldots, s_m + n_m p)$ for all $(n_1, \ldots, n_m)$. With $H_i = \{s_i + np \mid n \in \mathbb{Z}\}$, we get the desired result. □

We now prove the Skolem-Mahler-Lech theorem for finite transcendental extensions by reducing to the rational case:

Theorem 3.7. *Let $\boldsymbol{u}$ be a LRS of order k with recurrence coefficients $a_i \in \mathbb{Q}(X_1, \ldots, X_m)$. There is a prime p for which if $r = |GL_k(\mathbb{F}_p)|!$, there are integers $j_1, \ldots, j_m \in \{0, \ldots, r-1\}$ (m may be zero) and a finite set S such that*

$$Ann(\boldsymbol{u}) = S \cup \bigcup_{i=1}^{m} \{j_i + rq \mid q \in \mathbb{N}\}.$$

Proof. We can scale the LRS $\mathbf{u}$ by a non zero polynomial $R \in \mathbb{Z}[X_1, \ldots, X_m]$ so that the recurrence coefficients $a_i \in \mathbb{Z}[X_1, \ldots, X_m]$ as in Remark 2.1. Then we have $\det A \in \mathbb{Z}[X_1, \ldots, X_m]$. By Lemma 3.5, we can find an odd prime p and infinite subsets $H_1, \ldots, H_m$ of $\mathbb{Z}$ such that if $(h_1, \ldots, h_m) \in H_1 \times \cdots \times H_m$ then $p \nmid \det A(h_1, \ldots, h_m)$. $A(h_1, \ldots, h_m)$ is the companion matrix associated to $\mathbf{u}(h_1, \ldots, h_m)$ so we know that $\mathrm{Ann}(\mathbf{u}(h_1, \ldots, h_m))$ is quasi-periodic by Theorem 3.3 with period $t < |\mathrm{GL}_k(\mathbb{F}_p)|$. Therefore $r = |\mathrm{GL}_k(\mathbb{F}_p)|!$ is a common period for each $\mathrm{Ann}(\mathbf{u}(h_1, \ldots, h_m))$. Finally, we claim that

$$\mathrm{Ann}(\mathbf{u}) = \bigcap_{(h_1, \ldots, h_m) \in H_1 \times \cdots \times H_m} \mathrm{Ann}(\mathbf{u}(h_1, \ldots, h_m))$$

- this would show that $\mathrm{Ann}(\mathbf{u})$ is quasi-periodic with period r. To show both inclusions, we know that if $n \in \mathrm{Ann}(\mathbf{u})$, u_n is zero for every input $(h_1, \ldots, h_m)$. For the other direction, by Lemma 3.6, if $u_n(h_1, \ldots, h_m) = 0$ for all $(h_1, \ldots, h_m) \in H_1 \times \cdots \times H_m$ then $u_n = 0$. This completes the proof. □

Like in the case of $\mathbb{Q}$, the period r is bounded. We know $r \mid |\mathrm{GL}_k(\mathbb{F}_p)|!$ at best.

The general case

Now we proceed to the general case of a field K of characteristic zero. We reduce to the previous case of a finite transcendental extension of $\mathbb{Q}$ by the use of the following lemma.

Lemma 3.8. *Let L be a field with the following property P: If $\mathbf{u}$ is a L-LRS, then Ann($\mathbf{u}$) is a quasi-periodic subset of $\mathbb{N}$. Any finite algebraic extension K of L also has property P.*

Proof. Let K be an algebraic extension of degree d. It is a d dimensional vector space over L so let $\alpha_1, \ldots, \alpha_d$ be d linearly independent linear forms from K to L - these can be viewed as row vectors. Let $\mathbf{u}$ be a L-LRS. $\mathbf{u}$ can be expressed in matrix form $u_n = \alpha A^n \beta$ as in (4). Define $(u_{\alpha_i})_n = \alpha_i(\alpha A^n \beta) = (\alpha_i \circ \alpha) A^n B = \gamma A^n \beta$ where $\alpha_i \circ \alpha$ is interpreted as a composition of linear forms from K to L while γ is viewed as a row vector. By Remark 2.4, we know $(\mathbf{u}_{\alpha_i})$ is a L-LRS. Therefore by property P, $\text{Ann}(\mathbf{u}_{\alpha_i})$ is a quasi-periodic sequence. As the α_i are linearly independent, if $s \in K$, $s = 0$ if and only if $\alpha_i(s) = 0$. Therefore

$$\text{Ann}(\mathbf{u}) = \bigcap_{i=1}^{d} \text{Ann}(\mathbf{u}_{\alpha_i}).$$

So K has property P as $\text{Ann}(\mathbf{u})$ is quasi-periodic. □

We can now prove the Skolem-Mahler-Lech theorem for characteristic zero fields.

Theorem 3.9 (Skolem-Mahler-Lech for characteristic zero)**.** *Let K be a field of characteristic zero and $\mathbf{u}$ be a K-LRS. Then Ann($\mathbf{u}$) is a quasi-periodic set.*

Proof. Let $\mathbf{u}$ be a K-LRS with recurrence coefficients $a_0, \ldots, a_{k-1}$. Let $W = \{a_0, \ldots, a_{k-1}, u_0, \ldots, u_{k-1}\}$. Then $\mathbf{u}$ is a sequence in $\mathbb{Q}(W)$ so without loss of generality, assume that $K = \mathbb{Q}(W)$. Let W' be a maximal subset of W that is algebraically independent over $\mathbb{Q}$. Then $L = \mathbb{Q}(W')$ is isomorphic to $\mathbb{Q}(X_1, \ldots, X_m)$, the field of rational functions in m variables over $\mathbb{Q}$, where $m = |W|$ (some elements may be repeated in W). By definition of W', every element $w \in W \backslash W'$ is algebraic over L so K is a finite algebraic extension of L. Therefore, by Theorem 3.7 and Lemma 3.8, we are done. □

Since this proof is based on that of Theorem 3.7, the period r of the arithmetic progressions can be effectively determined. Therefore the Skolem Problem amounts to deciding whether the finite set is empty or not as there is an effective procedure to decide whether $\text{Ann}(\mathbf{u})$ is finite as shown in [2].

A reasonable question is to ask to what extent does the Skolem-Mahler-Lech theorem hold in positive characteristic. An analogous statement doesn't hold - consider the LRS over $\mathbb{F}_p(X)$ with recurrence relation

$$u_n = (2x+2)u_{n-1} - (x^2+3x+1)u_{n-2} + (x^2+x)u_{n-3}$$

with $u_0 = -1, u_1 = 0$ and $u_2 = 2x^2$. This sequence has solution $u_n = (x+1)^n - x^n - 1$. By Fermat's little theorem, we know that $u_{p^k} = 0$ for all $k \in \mathbb{N}$ which is not a quasi-periodic set. The extension of the Skolem-Mahler-Lech theorem can be found in [11] - this example is essentially the only way the analog of the Skolem-Mahler-Lech theorem in positive characteristic fails.

4 Special Cases

Partial answers to the Skolem Problem can be attained by fixing some extra conditions. One such condition is the order - the lower the order, the simpler the resulting recurrence so the problem becomes more tractable. More specifically, imposing conditions on the characteristic roots of an LRS makes it easier to control via its exponential-polynomial representation. For a $\overline{\mathbb{Q}}$-LRS $\mathbf{u}$, the first difficult case is order 3 LRS, particularly when $\mathbf{u}$ has 3 dominant roots - 3 roots equally large in modulus. This was settled by Mignotte [28] in 1975 when $\mathbf{u}$ is simple. Later, the 3 dominant roots case was fully solved and the order 4 case for $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS was also settled independently by Mignotte, Shorey and Tijdeman [29] and Vereshchagin [18] in 1984 and 1985 respectively. These results are state of the art - they haven't been improved outside of very exceptional special cases to this day. The following will outline a combination of the methods in [29] and [18].

In this section we work with a $\overline{\mathbb{Q}}$-LRS $\mathbf{u}$ of order k with distinct characteristic roots $\lambda_1, \dots, \lambda_l$. Since we are looking for zeroes and there is an effective algorithm to decompose $\mathbf{u}$ into a sequence of non degenerate LRS (Remark 2.2), it suffices to work with non degenerate LRS. For a characteristic root λ_i, it is dominant if $|\lambda_i| \geq |\lambda_j|$ for any other characteristic root $|\lambda_j|$. We say λ_i is dominant with respect to $v_\mathfrak{p}$ if $v_\mathfrak{p}(\lambda_i) \leq v_\mathfrak{p}(\lambda_j)$ for the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ where $F = \mathbb{Q}(\lambda_1, \dots, \lambda_l)$ where $v_\mathfrak{p}$ is defined above. We assume that $\mathbf{u}$ has r dominant roots where $r \leq l$ and label the characteristic roots in order of modulus i.e $|\lambda_1| = \dots = |\lambda_r| > |\lambda_{r+1}| \geq \dots |\lambda_l|$.

Throughout this section, c_i denote computable constants. Each of these are computable by Proposition 2.5 and its following remark and so justification for why a number is computable will only be provided if it isn't immediate from Proposition 2.5 and its following remark. We will prove the following theorems:

Theorem 4.1 (Decidability for 3 dominant roots). *Let $\boldsymbol{u} = \{u_m\}_{m=0}^\infty$ be a non degenerate $\overline{\mathbb{Q}}$-LRS such that $r \leq 3$. Then there exists positive computable numbers c_1 and c_2, depending only on $\boldsymbol{u}$, such that*

$$|u_m| \geq |\lambda_1|^m \exp(-c_1 (\log m)^2) \tag{7}$$

for $m \geq c_2$.

With the effective bound c_2, this gives a resolution of the Skolem Problem for LRS with up to 3 dominant roots - in particular, for order 3 LRS. An analogous result won't be found for $r = 4$ but instead for $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS with $l = 4$ charactersitic roots.

Theorem 4.2 (Decidability 4 characteristic roots)**.** *Let $\boldsymbol{u}$ be a non zero, non degenerate $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS with $l = 4$ characteristic roots. Then every m such that $u_m = 0$ is bounded by some computable constant, only depending on $\boldsymbol{u}$.*

A notable corollary is the decidability of the Skolem Problem for order 4 LRS. To prove these theorems, we will use Baker's theorem as in [1]. Let $\alpha_1, \dots, \alpha_t$ be non zero algebraic numbers and $K = \mathbb{Q}(\alpha_1, \dots, \alpha_t)$ with $[K : \mathbb{Q}] = d$. Let the heights of $\alpha_1, \dots, \alpha_{t-1}$ and α_t be at most A' and $A \geq 2$ respectively. Then we have the following theorem:

Theorem 4.3. *There exists a computable number $c_3 > 0$ depending only on t, d, A' such that for any δ with $0 < \delta < \frac{1}{2}$, the inequalities*

$$0 < |b_1 \log \alpha_1 + \cdots + b_t \log \alpha_t| < \left(\frac{\delta}{B'} \right)^{c_3 \log A} e^{-\delta B}$$

have no solution in rational integers $b_1, \dots, b_{t-1}$ and $b_t \neq 0$ with absolute values at most B and B' respectively.

We also use the following consequence of Theorem 4.3, Lemma 1 of [34]:

Theorem 4.4. *Let λ and μ be non zero algebraic numbers such that $|\lambda| \geq |\mu|$ and $\frac{\lambda}{\mu}$ isn't a root of unity. Suppose that a_1 and a_2 are non zero algebraic numbers of degrees at most D and heights at most $H \geq 3$. Let $n \geq 2$ be a rational integer. Then there exist positive computable numbers c_4, c_5 depending only on D, λ, μ such that*

$$|a_1 \lambda^n + a_2 \mu^n| \geq |\lambda|^n H^{-c_4 \log n} \tag{8}$$

when $n \geq c_5 \log H$.

This theorem, along with a version to handle the $r = 3$ case, Theorem 4.8, are key to proving Theorem 4.1. We also use a p-adic analog, due to van der Poorten [39].

Theorem 4.5. *Let $\mathfrak{p}$ be a prime ideal of K lying above a rational prime p. Suppose that $b_1, \dots, b_{t-1}$ and $b_t = -1$ are rational integers of absolute value at most B. There is a computable number $c_6 > 0$ depending only on t, d and A' such that for any $0 < \delta < 1$, if $\delta B < v_{\mathfrak{p}}(\alpha_1^{b_1} \dots \alpha_t^{b_t} - 1) < \infty$ then $B \leq c_6 \delta^{-1} p^d \log(\delta^{-1} p^d) \log A$.*

Remark 4.6. Since the dependence on A is explicit, we can vary α_t as long as it is of bounded degree and belongs to some fixed number field K. A notable case is if $\alpha_t = \frac{S(n)}{T(n)}$ for some $n \in \mathbb{N}$ and polynomials S, T with algebraic coefficients. We know that α_t is in the field F generated by the coefficients of S and T so we can take $K = F(\alpha_1, \dots, \alpha_{t-1})$ and apply the theorem - notably α_t has bounded degree. If the coefficients of S and T are computable then we know that the height of α_t is at most $A = n^v$ where v is some computable constant in terms of these coefficients and the degree of S and T, by Proposition 2.5. An analogous statement for a_1 and a_2 as in Theorem 4.4 is true too.

Now we prove the theorem on the sum of three terms, following the method in [18]. First, we need to know that the sum is non zero, a detail Vereshchagin didn't cover so we use the following theorem from [29].

Theorem 4.7. *Let a_1, a_2, a_3 be non-zero algebraic numbers of degrees at most D and heights at most H. Let $\gamma_1, \gamma_2, \gamma_3$ be non zero algebraic numbers such that at least one ratio $\frac{\gamma_i}{\gamma_j}$ for $i \neq j$ is not equal to a root of unity. Then if*

$$a_1\gamma_1^n + a_2\gamma_2^n + a_3\gamma_3^n = 0 \tag{9}$$

then $n \leq c_7 \log H$ for a computable number c_7 depending only on $\gamma_1, \gamma_2, \gamma_3$ and D.

Once we have proven this theorem, we can prove the following:

Theorem 4.8. *Suppose $a_1, a_2, a_3, \gamma_1, \gamma_2, \gamma_3$ are as in Theorem 4.7 and also that the γ_i are distinct and $|\gamma_1| = |\gamma_2| = |\gamma_3|$. Then there are computable positive constants c_8, c_9, depending only on $\gamma_1, \gamma_2, \gamma_3, H, D$ such that for $n \geq c_8$, we have*

$$|a_1\gamma_1^n + a_2\gamma_2^n + a_3\gamma_3^n| \geq |\gamma_1|^n n^{-c_9 \log H} \tag{10}$$

We begin with the proof of Theorem 4.7. We follow the presentation in [29] where I have filled in important details in their argument.

Proof of Theorem 4.7. Without loss of generality, assume that $\frac{\gamma_1}{\gamma_2}$ is not a root of unity. Let $L = \mathbb{Q}(a_1, a_2, a_3, \gamma_1, \gamma_2, \gamma_3)$ and note that $[L : \mathbb{Q}] \leq c_{10}$ by the tower law. In this proof, every computable constant depends only on $\gamma_1, \gamma_2, \gamma_3$ and D. Whenever we apply Theorem 4.3 or 4.5, recall that the heights of $\alpha_1, \dots, \alpha_{t-1}$ and α_t are at most A' and $A \geq 2$ respectively and that they all belong to a number field K of degree d.

We will use (9) to reduce to equations with two terms. Then upon supposing $\frac{\gamma_1}{\gamma_2}$ is a unit, we can find a prime ideal to let us use Theorem 4.5 and when it isn't a unit, we use Theorem 4.3. These will give us the desired bound on n. Suppose that $\frac{\gamma_1}{\gamma_2}$ is not a unit. Then there is a prime ideal $\mathfrak{p} \lhd \mathcal{O}_L$ such that $v_{\mathfrak{p}}(\frac{\gamma_1}{\gamma_2}) \neq 0$. By permuting indices, we may suppose it is positive. By (9), we have

$$a_1\left(\frac{\gamma_1}{\gamma_2}\right)^n = -a_2 + a_3\left(\frac{\gamma_3}{\gamma_2}\right)^n \tag{11}$$

and $a_2\gamma_2^n + a_3\gamma_3^n \neq 0$. By considering the order of $\mathfrak{p}$ dividing both sides of (11), we have

$$\begin{aligned} n \leq v_{\mathfrak{p}}\left(\left(\frac{\gamma_1}{\gamma_2}\right)^n\right) &= v_{\mathfrak{p}}(a_2a_1^{-1}) + v_{\mathfrak{p}}\left(-\left(\frac{\gamma_3}{\gamma_2}\right)^n\frac{a_3}{a_2} - 1\right) \\ &\leq c_{11}\log H + v_{\mathfrak{p}}\left(-\left(\frac{\gamma_3}{\gamma_2}\right)^n\frac{a_3}{a_2} - 1\right) \end{aligned}$$

Now if $v_{\mathfrak{p}}(-(\frac{\gamma_3}{\gamma_2})^n\frac{a_3}{a_2} - 1) \geq \frac{n}{2}$ then we have $n \leq c_{12}\log H$. If not, then we can apply Theorem 4.5. Set $t = 2, \alpha_1 = \frac{\gamma_3}{\gamma_2}, \alpha_2 = -\frac{a_2}{a_3}, \delta = \frac{1}{2}$, $B = n$. We have $d \leq c_{13}, p \leq c_{14}, A' = c_{15}, A = H^{c_{16}}$. Then we have that $n \leq c_{17}\log H$ as required.

Therefore we may assume that $\frac{\gamma_1}{\gamma_2}$ is a unit. By Theorem 2.7, as $\frac{\gamma_1}{\gamma_2}$ isn't a root of unity, there is an embedding σ of L such that $|\sigma(\gamma_1)| > |\sigma(\gamma_2)|$. By applying σ to (9), we can assume that $|\gamma_1| > |\gamma_2|$ without loss of generality. By (9), we have $a_1\gamma_1^n + a_3\gamma_3^n \neq 0$. Therefore

$$0 \neq |a_1\gamma_1^n + a_3\gamma_3^n| = |a_1\gamma_1^n|\left|-\left(\frac{\gamma_3}{\gamma_1}\right)^n\frac{a_3}{a_1} - 1\right|$$

We now apply Theorem 4.3 to

$$|b_1\log\alpha_1 + \cdots + b_t\log\alpha_t| = \left|n\log\left(\frac{\gamma_3}{\gamma_1}\right) + V\log(-1) + \log\left(\frac{a_3}{a_1}\right)\right|$$

where all logarithms have their principal values and $|V| \leq 2n+3$ is a rational integer to ensure this. Set $t = 3$, $b_1 = n, b_2 = V, b_3 = 1$ and $\alpha_1 = \frac{\gamma_3}{\gamma_1}, \alpha_2 = -1, \alpha_3 = \frac{a_3}{a_1}$ and $\delta = \min(\frac{1}{4}\log|\frac{\gamma_1}{\gamma_2}|, \frac{1}{4})$. Then we can apply Theorem 4.3 with $d \leq c_{13}$, $\log A' = c_{18}$, $\log A = c_{19}\log H$,$B' = 1$,$B = 2n+3$ so we get

$$\begin{aligned} \left|n\log\left(\frac{\gamma_3}{\gamma_1}\right) + V\log(-1) + \log\left(\frac{a_3}{a_1}\right)\right| &\geq \left(\frac{\delta}{B'}\right)^{c_{20}\log A} e^{-\delta B} \\ &= \delta^{c_{21}\log H}e^{-(2n+3)\delta} \\ &= H^{-c_{22}}e^{-(2n+3)\delta} \text{ as } \delta \leq \frac{1}{4} \\ &\geq H^{-c_{23}}\left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} \text{ as } \delta \leq \frac{1}{4}\log\left|\frac{\gamma_1}{\gamma_2}\right| \end{aligned}$$

The upper bound of $\frac{1}{4}$ on δ is to ensure $\delta < \frac{1}{2}$ so we can apply Theorem 4.3. Then we claim that for all positive integers n, there is a computable constant c_{24} such that

$$\left|-\left(\frac{\gamma_3}{\gamma_1}\right)^n\frac{a_3}{a_1} - 1\right| \geq H^{-c_{24}}\left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} \tag{12}$$

Suppose that this inequality isn't true, that for any computable constant c_{25}, there is some n for which

$$\left|-\left(\frac{\gamma_3}{\gamma_1}\right)^n \frac{a_3}{a_1} - 1\right| < H^{-c_{25}} \left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} \tag{13}$$

Then since log is Lipschitz around 1 and $\log 1 = 0$, for some real constant Z we have that

$$\left|\log\left(-\left(\frac{\gamma_3}{\gamma_1}\right)^n \frac{a_3}{a_1}\right)\right| < Z\left|-\left(\frac{\gamma_3}{\gamma_1}\right)^n \frac{a_3}{a_1} - 1\right| < ZH^{-c_{25}} \left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} = H^{-c_{26}} \left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}}$$

Now

$$\begin{aligned}\log\left(-\left(\frac{\gamma_3}{\gamma_1}\right)^n \frac{a_3}{a_1}\right) &= \log(-1) + n\log\left(\frac{\gamma_3}{\gamma_1}\right) + \log\left(\frac{a_3}{a_1}\right) + 2mi\pi \\ &= (2m+1)\log(-1) + n\log\left(\frac{\gamma_3}{\gamma_1}\right) + \log\left(\frac{a_3}{a_1}\right)\end{aligned}$$

where $|m| \leq n+1$ is an integer chosen so that each logarithm is principal valued. This contradicts the bound we have already established on this quantity, giving us (12).

Since $|a_1| \geq H^{-D}$, we conclude that

$$|a_1\gamma_1^n + a_3\gamma_3^n| \geq |\gamma_1^n| \left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} H^{-c_{27}}$$

Also, as $|a_2| \leq H^D$, we have

$$|a_2\gamma_2^n| \leq H^D|\gamma_2|^n$$

So by (9), $|a_1\gamma_1^n + a_3\gamma_3^n| = |a_2\gamma_2^n|$ so

$$|\gamma_1|^n \left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{n}{2}} H^{-c_{27}} \geq H^D|\gamma_2|^n \implies \left|\frac{\gamma_1}{\gamma_2}\right|^{\frac{n}{2}} \leq H^{c_{28}}$$

Since $|\gamma_1| > |\gamma_2|$, we get $n \leq c_{29}\log H$, completing the proof of the theorem. □

Now we prove Theorem 4.8, using methods in [18] with details filled in.

Proof of Theorem 4.8. Let $\varepsilon = a_3 + a_1(\frac{\gamma_1^n}{\gamma_3^n}) + a_2(\frac{\gamma_2^n}{\gamma_3^n})$. By Theorem 4.7, we know that $\varepsilon \neq 0$ if $n \geq c_{30}$, depending on $\gamma_1, \gamma_2, \gamma_3$ and D. Then $(x_1, x_2) = (\frac{\gamma_1^n}{\gamma_3^n}, \frac{\gamma_2^n}{\gamma_3^n})$ is a solution to the equation

$$a_1x_1 + a_2x_2 + (a_3 - \varepsilon) = 0 \tag{14}$$

Note that $|x_1| = |x_2| = 1$. We will solve the system for $\varepsilon = 0$ and use these solutions to approximate the solutions for $\varepsilon \neq 0$. Combining this with Theorem 4.4, we get a lower bound on ε. We aim to prove a lower bound on $|\varepsilon|$ so we are free to assume upper bounds on $|\varepsilon|$.

Let $a_3' = a_3 - \varepsilon$ and define real variables v_1, v_2, w_1, w_2 such that $v_j + iw_j = \frac{a_j x_j}{a_3'}$. Then

$$v_1 + v_2 + i(w_1 + w_2) + 1 = \frac{a_1x_1 + a_2x_2 + a_3 - \varepsilon}{a_3 - \varepsilon} = 0$$

Since these variables are real, we obtain $v_1 + v_2 + 1 = 0$ and $w_1 = -w_2$. Moreover, $v_j^2 + w_j^2 = |\frac{a_j x_j}{a_3'}|^2 = |\frac{a_j}{a_3'}|^2$. This yields a system of quadratic equations which can be solved, yielding the solutions

$$\begin{aligned} x_1(\varepsilon) &= \frac{a_3'(|a_2|^2 - |a_1|^2 - |a_3'|^2 \pm i\sqrt{D(\varepsilon)})}{2a_1|a_3'|^2} \\ x_2(\varepsilon) &= \frac{a_3'(|a_1|^2 - |a_2|^2 - |a_3'|^2 \mp i\sqrt{D(\varepsilon)})}{2a_2|a_3'|^2} \\ D(\varepsilon) &= ((|a_1| + |a_2|)^2 - |a_3'|^2)(|a_3'|^2 - (|a_1| - |a_2|)^2) \end{aligned}$$

Without loss of generality, assume that $|a_1| \leq |a_2| \leq |a_3|$. Solutions to this system exist if only if $D(\varepsilon) > 0$. For $\varepsilon = 0$, we have solutions if and only if $|a_3| < |a_1| + |a_2|$ and $|a_3| > |a_2| - |a_1|$, geometrically this corresponds to the vectors in (14) forming the sides of a triangle. From these expressions, we see that $x_1(0)$ and $x_2(0)$ can be expressed entirely in terms of a_1, a_2, a_3 and their moduli, so they are algebraic and their heights and degrees are computable in terms of H and D, the heights and degrees of a_1, a_2, a_3.

Now we estimate $|x_1(\varepsilon) - x_1(0)|$ with both being chosen with the same sign of the square root. Consider two cases, $D(0) \geq 0$ and $D(0) < 0$. Suppose $|\varepsilon| < \frac{|a_3|}{4}$, this assumption simplifies calculations.

Case 1: $D(0) \geq 0$. Split $|x_1(\varepsilon) - x_1(0)|$ into two summands by the triangle inequality:

$$\left|\frac{a_3'(|a_2|^2 - |a_1|^2 - |a_3'|^2)}{2a_1|a_3'|^2} - \frac{a_3(|a_2|^2 - |a_1|^2 - |a_3|^2)}{2a_1|a_3|^2}\right| \leq \frac{A_1|\varepsilon|}{|a_1|}$$

$$\left|\frac{a_3'\sqrt{D(\varepsilon)}}{2a_1|a_3'|^2} - \frac{a_3\sqrt{D(0)}}{2a_1|a_3|^2}\right| \leq \frac{A_2|\varepsilon|}{|a_1|} + \left|\frac{\sqrt{D(\varepsilon)} - \sqrt{D(0)}}{a_1a_3}\right| \leq \begin{cases} A_3\sqrt{|\varepsilon|} & D(\varepsilon) = 0 \\ A_4|\varepsilon| & D(\varepsilon) > 0 \end{cases}$$

where $A_1, \ldots, A_4$ are constant functions of $|a_3|$ and $\sqrt{D(0)}$, calculated with our upper bound on $|\varepsilon|$.

Case 2: $D(0) < 0$. If $D(0) < 0$ then we have $|a_3| > |a_2| + |a_1|$ and since $D(\varepsilon)$ is continuous, we can find an computable δ_1, in terms of $D(0)$ and a_3, such that if $|\varepsilon| < \delta_1$ then $D(\varepsilon) < 0$ so that (14) has no solutions. In this case,

$$|a_1\gamma_1^n + a_2\gamma_2^n + a_3\gamma_3^n| = |\gamma_3|^n|\varepsilon| \geq |\gamma_3|^n(|a_3| - |a_2| - |a_1|) > 0$$

as $|x_1| = |x_2| = 1$ which is in the required form. So we can assume $D(0) \geq 0$.

Our overall bound therefore is

$$|x_1(\varepsilon) - x_1(0)| \leq \left(\frac{A_1 + A_2}{|a_1|} + A_4\right)|\varepsilon| + \frac{A_3}{|a_1|}\sqrt{|\varepsilon|} = O(\sqrt{|\varepsilon|})$$

by taking $|\varepsilon| < 1$. Set $A = \frac{A_1+A_2}{|a_1|} + \max(\frac{|A_3|}{|a_1|}, A_4)$ and $\delta = \min(1, \delta_1, \frac{|a_3|}{4})$. Then we have that for $|\varepsilon| < \delta$, if $x_1(\varepsilon), x_2(\varepsilon)$ are solutions of (14), then $x_1(0), x_2(0)$ are defined and that

$$|x_1(\varepsilon) - x_1(0)| \leq A\sqrt{|\varepsilon|} \tag{15}$$

Now we aim to use Theorem 4.4 to get a lower bound on ε. Recalling the beginning, a particular solution of (14) was $x_1(\varepsilon) = (\frac{\gamma_1}{\gamma_3})^n$. Then

$$|x_1(\varepsilon) - x_1(0)| = \left|\left(\frac{\gamma_1}{\gamma_3}\right)^n - x_1(0)\right| = |\gamma_3|^{-n}|\gamma_1^n - x_1(0)\gamma_3^n|$$

Since $x_1(0)$ is algebraic and of height at most $H^{c_{31}}$, we can apply Theorem 4.4 with the constants as $1, -x_1(0)$ and $\lambda = \gamma_1$, $\mu = \gamma_3$ to get, for sufficiently large $n \geq c_{32}$, that

$$|x_1(\varepsilon) - x_1(0)| \geq \left|\frac{\gamma_1}{\gamma_3}\right|^n H^{-c_{33}\log n} = n^{-c_{33}\log H}$$

If $x_1(0) = 0$ then this conclusion is clear. If $\frac{\gamma_1}{\gamma_3}$ is a root of unity then we can find the same conclusions for $\frac{\gamma_2}{\gamma_3}$ as it won't be a root of unity, giving c_{33} dependence on γ_2 too. Combining (15) and the above gives $|\varepsilon| > \min\{\delta, A^{-2}n^{-2c_{33}\log H}\}$ which proves the theorem. Note that c_{32}, c_{33} depend on the height and degree of $x_1(0)$ (which depends on the heights and degrees of a_1, a_2, a_3) and $\gamma_1, \gamma_2, \gamma_3$ as claimed. □

Remark 4.9. If one of the ratios is a root of unity then the dependence on c_9 in (10) can be removed by restricting the range of n. This is because if $\frac{\gamma_1}{\gamma_3}$ is a root of unity, its order d is computable as in [21] Section II A. Then if n is a multiple of d, we have

$$|a_1\gamma_1^n + a_2\gamma_2^n + a_3\gamma_3^n| = \left|a_1 + a_2 + a_3\left(\frac{\gamma_2}{\gamma_1}\right)^n\right||\gamma_1|^n$$

As $\frac{\gamma_2}{\gamma_1}$ isn't a root of unity, we can use Theorem 4.4. The conditions of the theorem are satisfied unless $a_1 = -a_2$ in which case the result is clear.

We now have the tools to prove Theorems 4.1 and 4.2. We assume that $\mathbf{u}$ has exponential-polynomial representation $u_n = \sum_{i=1}^{l} Q_i(n)\lambda_i^n$ and has recurrence coefficients a_i. For Theorem 4.1, we follow the presentation in [29] with a more careful consideration of repeat dominant roots.

Proof of Theorem 4.1. Consider a non degenerate $\overline{\mathbb{Q}}$-LRS $\mathbf{u}$ with $r \leq 3$ i.e at most 3 dominant roots. Let $\Lambda = Q_1(n)\lambda_1^n + \cdots + Q_r(n)\lambda_r^n$. Recall that the λ_i are distinct and say they are of multiplicity ν_i in the characteristic polynomial g of $\mathbf{u}$. Then we know that, by the triangle inequality,

$$\begin{aligned} |u_n| &= |\Lambda + (Q_{r+1}(n)\lambda_{r+1}^n + \cdots + Q_l(n)\lambda_l^n| \\ &\geq |\Lambda| - n^{c_{35}^2}|\lambda_{r+1}|^n \end{aligned}$$

for $n \geq c_{34}$ as λ_{r+1} is the largest non dominant root. Here, c_{35} is a constant computable in terms of the heights and degrees of a_i and λ_i as it is dependent on the degrees of Q_j and the heights of its coefficients for $j = r+1, \ldots, l$. Therefore $|\Lambda|$ is the leading order term so it suffices to show that

$$|\Lambda| \geq |\lambda_1|^n \exp(-c_{36}(\log n)^2) \text{ for } n \geq c_{37} \tag{16}$$

We aim to use Theorems 4.4 and 4.8 which we can use as $\mathbf{u}$ is a non denegerate LRS. We can find a better bound if we have a dominant root of greatest multiplicity (among the dominant roots), suppose this is the case. Without loss of generality, say λ_1 is this dominant root of greatest multiplicity and that $\nu_i \geq \nu_j$ for $1 < j \leq r$. Then

$$\begin{aligned} |\Lambda| &= |(b_{\nu_1-1}n^{\nu_1-1} + \ldots)\lambda_1^n + \cdots + (\cdots + d_{\nu_r-1}n^{\nu_r-1})\lambda_r^n| \\ &\geq n^{\nu_1-1}|\lambda_1|^n \left(|b_{\nu_1-1}| - \cdots - \frac{|d_{\nu_r-1}|}{n^{\nu_1-\nu_r}}\right) \end{aligned}$$

We know that for any $x \in \overline{\mathbb{Q}}$, $|x|$ is bounded by an expression in its height and degree so we can choose $n \geq c_{38}$, giving us a stronger bound than (16). This covers the $r = 1$ case too.

For $r = 2$, we can apply Theorem 4.4 with $a_1 = Q_1(n), a_2 = Q_2(n), \lambda = \lambda_1, \mu = \lambda_2$ and by Remark 4.6, $\log H = c_{39} \log n$ giving

$$|Q_1\lambda_1^n + Q_2\lambda_2^n| \geq |\lambda_1|^n H^{-c_{40}\log n} = |\lambda_1|^n \exp(-c_{41}(\log n)^2) \tag{17}$$

for $n \geq c_{42} \log n$ so $n \geq c_{43}$ as expected. For $r = 3$, we apply Theorem 4.7 (so that we know the sum is non zero) and Theorem 4.8 with $a_i = Q_i(n), \gamma_i = \lambda_i$ for $1 \leq i \leq 3$ and $\log H = c_{44} \log n$ again to get

$$|Q_1\lambda_1^n + Q_2\lambda_2^n + Q_3\lambda_3^n| \geq |\lambda_1|^n n^{-c_{45}\log n} = |\lambda_1|^n \exp(-c_{46}(\log n)^2)$$

for $n \geq c_{47}$ in the same way as above, completing the proof. □

In the case that the λ_i are simple roots, we recover exactly the same result as shown in [28]. Next, we prove Theorem 4.2, following the presentation in [29]. The proof of this theorem in [29] is for 4 characteristic roots, Theorem 2 in [29], which is stronger than Vereshchagin's Theorem 4 which considers only order 4 $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS [18].

Proof of Theorem 4.2. Let $\mathbf{u}$ be a non degenerate $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS with characteristic polynomial g which has roots $\lambda_1, \ldots, \lambda_4$.

Let $L = \mathbb{Q}(u_0, \ldots, u_{k-1}, a_0, \ldots, a_{k-1})$. By Theorem 4.1, we can assume $r = 4$, that there are 4 dominant roots. As in the Remark 2.1, we can rescale $\mathbf{u}$ so that the recurrence coefficients $a_i \in \mathcal{O}_L$ using geometric scaling. Then the characteristic roots are roots of a monic polynomial $g \in \mathcal{O}_L[X]$ so $\lambda_i \in \mathcal{O}_L$. Next, we know that since $\mathbf{u}$ is non degenerate, each characteristic root λ_i is not real - otherwise, there would be at least two real roots whose ratio is ± 1. 1 is not possible as the λ_i are distinct and -1 isn't as $\mathbf{u}$ is non degenerate. So without loss of generality, assume that

$$\lambda_1 = \overline{\lambda_3} \text{ and } \lambda_2 = \overline{\lambda_4} \tag{18}$$

Let $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_4)$, h be the class number of K and $G = \mathrm{Gal}(K/\mathbb{Q})$. We assume that $u_m = 0$ so our aim is to find an upper bound on m. Therefore, we may freely assume any lower bound on m. We will show there are at most two dominant roots with respect to some $\mathfrak{p}$-adic valuation and derive our bound from Theorem 4.5.

Suppose that $t = \frac{\lambda_1}{\lambda_3}$ is a unit. By Theorem 2.7, as t is not a root of unity, there is some $\sigma \in G$ such that $|\sigma(\lambda_1)| > |\sigma(\lambda_3)|$. Then $\sigma(\mathbf{u})$ is a LRS with $r \leq 3$ so $\sigma(u_m) = 0$ for $m \geq c_{48}$ sufficiently large by Theorem 4.1. So we may assume that $m \geq c_{48}$.

Now suppose that t is not a unit. Then

$$\gcd((\lambda_1^h), \ldots, (\lambda_4^h)) = (\Pi)$$

for some $\Pi \in \mathcal{O}_K$. Setting $\Lambda_i = \lambda_i^h \Pi^{-1}$ for $1 \leq i \leq 4$, then $\Lambda_i \in \mathcal{O}_K$ and

$$\gcd((\Lambda_1^h), \ldots, (\Lambda_4^h)) = (1)$$

Since $|\lambda_3| = |\lambda_4|$, by (18) we have $\Lambda_1\Lambda_3 = \Lambda_2\Lambda_4$. We know that $\Lambda_1, \Lambda_3 \in \mathcal{O}_K$ so $\Lambda_1\Lambda_3$ isn't a unit. By considering the factorisation of $(\Lambda_1\Lambda_3)$, there is a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$ such that $\mathfrak{p} \mid (\Lambda_1\Lambda_3)$ so $\mathfrak{p} \mid (\Lambda_2\Lambda_4)$. Without loss of generality, we can assume that

$$\mathfrak{p} \mid (\Lambda_3) \text{ and } \mathfrak{p} \mid (\Lambda_4) \tag{19}$$

So Λ_1, Λ_2 are our two $\mathfrak{p}$-adically dominant characteristic roots. Now we aim to apply Theorem 4.5. Take $m = nh + q$ with $0 \leq q < h$ and define $z_i(X) =$

$Q_i(X)\lambda_i^q$ for $1 \le i \le 4$. Then $n+1 > mh^{-1}$. Therefore we have $n \ge \frac{m}{2h} \ge \frac{c_{48}}{2h}$.

Since $u_m = 0$, by multiplying both sides of the exponential polynomial representation by Π^{-n} we get $z_1(m)\Lambda_1^n + z_2(m)\Lambda_2^n = -z_3(m)\Lambda_3^n - z_4(m)\Lambda_4^n$. Counting powers of $\mathfrak{p}$ on both sides, we get

$$n \le v_{\mathfrak{p}}(\Delta)$$

where $\Delta = z_1(m)\Lambda_1^n + z_2(m)\Lambda_2^n$. This is because on the LHS we have $v_{\mathfrak{p}}(\Delta)$ and on the RHS we have at least n by (19). We want to show $\Delta \neq 0$ by Theorem 4.4 which we can apply as we know $\frac{\Lambda_1}{\Lambda_2}$ isn't a root of unity. The theorem gives us $\Delta \neq 0$ for sufficiently large n. More specifically, we need n to be larger than the bound required in Theorem 4.4 which only depends on Λ_1, Λ_2 and the degrees and heights of $Q_1(m), Q_2(m)$ - the degree is constant and the height is at most $c_{49} \log n$. As $n \ge \frac{m}{2h}$, by taking c_{48} large enough, this can be done - we need $n \ge c_{50} \log n$ which is true for $n \ge c_{51}$.

We have $\mathfrak{p}|(\Lambda_3)$ and $\mathfrak{p}|(\Lambda_4)$ and the gcd of the (Λ_i) is (1) so without loss of generality, assume $\mathfrak{p} \nmid \Lambda_1$. Then

$$\begin{aligned} v_{\mathfrak{p}}(\Delta) &= v_{\mathfrak{p}}(z_1(m)\Lambda_1^n + z_2(m)\Lambda_2^n) \\ &= v_{\mathfrak{p}}\left(z_2(m)\left(\frac{\Lambda_2}{\Lambda_1}\right)^n + z_1(m)\right) \text{ (as } v_{\mathfrak{p}}(\Lambda_1) = 0) \\ &= c_{52} \log m + v_{\mathfrak{p}}\left(-\left(\frac{\Lambda_2}{\Lambda_1}\right)^n \frac{z_2(m)}{z_1(m)} - 1\right) \end{aligned}$$

where $v_{\mathfrak{p}}(z_1(m)) = c_{52} \log m$ (from the powers of m) and the second term has been cast in the form to apply Theorem 4.5. Set $t = 3, \alpha_1 = \Lambda_2, \alpha_2 = \Lambda_1^{-1}, \alpha_3 = -\frac{z_1(m)}{z_2(m)}, d = c_{53}, \delta = \frac{1}{4h}, b_1 = b_2 = n, b_3 = -1$. $\mathfrak{p}$ lies above a rational prime p and so by Remark 2.6, $p = c_{54}$. A is the height of $\frac{z_2(m)}{z_1(m)}$ so $\log A = c_{55} \log m$. Let $B = n \ge \frac{m}{2h}$. Then by Theorem 4.5, if

$$\delta B = \frac{n}{4h} \le v_{\mathfrak{p}}\left(-\left(\frac{\Lambda_2}{\Lambda_1}\right)^n \frac{z_2(m)}{z_1(m)} - 1\right)$$

then $n \le c_{56} \log m$. Therefore $m \le c_{57} \log m$ as $n \ge \frac{m}{2h}$ so $m \le c_{58}$ and we'd be done. Otherwise, we have

$$n \le v_{\mathfrak{p}}(\Delta) \le c_{52} \log m + v_{\mathfrak{p}}\left(-\left(\frac{\Lambda_2}{\Lambda_1}\right) \frac{z_2(m)}{z_1(m)} - 1\right) \le c_{52} \log m + \frac{n}{4h}$$

Therefore we get $m \le c_{59}$, completing the proof. □

Our proof of Theorem 4.2 applies more generally than to just 4 characteristic roots - it applies to any $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS with at most two dominant roots with respect to some $\mathfrak{p}$ adic valuation. This motivates the definition of the MSTV class.

Definition 4.10 (MSTV class)**.** The Mignotte-Shorey-Tijdeman-Vereshchagin (MSTV) class consists of all $\mathbb{Z}$-LRS that either have at most three dominant roots in modulus or at most two dominant roots with respect to some $\mathfrak{p}$-adic valuation.

Remark 4.11. This covers many cases of order 5 LRS. It is shown in [20] and the appendix of [3] that an order 5 $\mathbb{Z}$-LRS $\mathbf{u}$ (also applies to $\mathbb{Q}$-LRS by rescaling) which don't belong to the MSTV class must have an exponential-polynomial representation $u_n = \alpha_1\lambda_1^n + \overline{\alpha_1}\overline{\lambda_1}^n + \alpha_2\lambda_2^n + \overline{\alpha_2}\overline{\lambda_2}^n + \alpha_3\lambda_3^n$ where α_i, λ_i are algebraic, $|\lambda_1| = |\lambda_2| > |\lambda_3|$, $\lambda_1, \lambda_2, \lambda_3$ aren't all units, $\lambda_3 \in \mathbb{R}$ and that $|\alpha_1| \neq |\alpha_2|$ if $\mathbf{u}$ is non degenerate.

5 The Bi-Skolem Problem

The unconditional results of the previous section were established in the 1980s. By introducing the notion of linear recurrence bi-sequences (LRBS), the MSTV class can be extended to include reversible $\mathbb{Z}$-LRS of order up to 7, that is, $\mathbb{Z}$-LRS for which $a_{k-1} = \pm 1$. The Bi-Skolem Problem, the analog of the Skolem Problem for LRBS is introduced along with the Skolem Conjecture, a proposed criterion for the resolution of the Bi-Skolem problem for simple LRBS. A Turing reduction of the Skolem Problem for LRS of order up to 5 to the Bi-Skolem Problem for LRBS of order up to 5 is demonstrated. With the p-adic Schanuel Conjecture, this Turing reduction will be extended to all orders of LRS and LRBS. We will detail these results, found in [20] and [3].

Main results

In this section, we will detail the main results to be proven. The first main result is an unconditional result for a specific type of $\mathbb{Z}$-LRS.

Theorem 5.1. *The Skolem problem for reversible $\mathbb{Z}$-LRS of order 7 or less is decidable.*

Next, the most important result, is a resolution of the Skolem Problem subject to two conjectures:

Theorem 5.2. *The Skolem Problem reduces to the Bi-Skolem Problem subject to the weak p-adic Schanuel Conjecture. In particular, the Skolem Problem for simple $\mathbb{Q}$-LRS is decidable subject to the weak p-adic Schanuel Conjecture and the Skolem Conjecture.*

The reduction to simple $\mathbb{Q}$-LRS is required by the Skolem Conjecture, as seen in its statement. The requirement of the p-adic Schanuel Conjecture can be removed for LRS of order up to 5:

Theorem 5.3. *There is a Turing reduction from the Skolem Problem for $\mathbb{Q}$-LRS of order at most 5 to the Bi-Skolem Problem for $\mathbb{Q}$-LRBS of order at most 5. In particular, the Skolem Problem for $\mathbb{Q}$-LRS of order at most 5 is decidable assuming the Skolem Conjecture.*

The proof of the last two theorems will give an algorithm that computes the set of zeroes of a non degenerate simple $\mathbb{Q}$-LRBS. It produces a certificate when all zeroes have been found. The conjectures assumed in (5.2) are to ensure the termination of this algorithm.

Definitions and Preliminaries

In this section, we will work with $\mathbb{Q}$-LRS and $\mathbb{Z}$-LRS - if not specified, we mean a $\mathbb{Q}$-LRS. When looking for zeroes, we can always rescale a $\mathbb{Q}$-LRS to a $\mathbb{Z}$-LRS. By taking a $\mathbb{Q}$-LRS $\mathbf{u}$ and running the recurrence backwards, the recurrence relation (1) defines a linear recurrence bisequence (LRBS) $\{u_k\}_{k=-\infty}^{\infty} = \overset{\leftrightarrow}{\mathbf{u}}$. We will refer to LRBS by $\mathbf{u}$ if the corresponding LRS is not being considered and by $\overset{\leftrightarrow}{\mathbf{u}}$ otherwise.

With this, we can now state the Skolem Conjecture:

Conjecture 5.4 (Skolem Conjecture)**.** Let $\overset{\leftrightarrow}{\mathbf{u}}$ be a simple $\mathbb{Q}$-LRBS satisfying (1) with $a_0, \ldots, a_{k-1}$ and $u_0, \ldots, u_{k-1}$ in $\mathbb{Z}$. Then $\overset{\leftrightarrow}{\mathbf{u}}$ has no zero if and only if for some integer $m \geq 2$ such that $\gcd(m, a_{k-1}) = 1$, we have that for all $n \in \mathbb{Z}$, $u_n \not\equiv 0 \bmod m$.

The Skolem Conjecture gives us means to detect zeroes - if a simple LRBS has no zero, this is witnessed modulo some integer m. This conjecture applies only to LRBS - we can take the Fibonacci sequence $\{0, 1, 1, 2, \ldots\}$ and take a shifted Fibonacci sequence $\{1, 1, 2, \ldots\}$ - the criteria cannot detect the zero because it starts at $m \geq 2$. Simplicity also cannot be removed; consider the LRBS given by the recurrence $u_{n+2} = 4u_{n+1} - 4u_n$ with $u_0 = 1, u_1 = 6$. Then $u_n = (2n+1)2^n$ so $u_n \neq 0$ for all $n \in \mathbb{Z}$ but for any integer $m \geq 2$, $u_n \equiv 0 \bmod m$ for infinitely many integers n, as in [20]. Some progress has been made on the Skolem Conjecture, for $\mathbb{Q}$-LRBS, it has been shown to hold for order 2 [6] and some cases of order 3 [33, 32]. Despite the similarity between the Skolem Conjecture and Skolem Problem, the truth of the Skolem Conjecture doesn't imply decidability of the Skolem Problem (nor the converse).

This conjecture immediately gives us a procedure to decide this following analog of the Skolem Problem for simple $\mathbb{Q}$-LRBS:

Problem 5.5 ($\mathbb{Q}$ Bi-Skolem problem)**.** Given a $\mathbb{Q}$-LRBS $\overset{\leftrightarrow}{\mathbf{u}}$, does it contain a zero?

The next conjecture we make use of is the weak p-adic Schanuel Conjecture, Conjecture 3.10 of [8]:

Conjecture 5.6 (Weak p-adic Schanuel Conjecture)**.** Let $\alpha_1, \ldots, \alpha_s$ be non-zero algebraic numbers contained in a finite extension field E of $\mathbb{Q}_p$. Let $\log_p : E^\times \to E$ be the p-adic logarithm normalised so that $\log_p(p) = 0$. If $\log_p \alpha_1, \ldots, \log_p \alpha_s$ are linearly independent over $\mathbb{Q}$, then $\log_p \alpha_1, \ldots, \log_p \alpha_s$ are algebraically independent over $\mathbb{Q}$.

A useful theorem is the following special case of Conjecture 5.6 - a p-adic analog of Baker's theorem.

Theorem 5.7. *Let $\alpha_1, \ldots, \alpha_s \in 1 + p\mathbb{Z}_p$ be algebraic over $\mathbb{Q}$ and such that $\log_p \alpha_1, \ldots, \log_p \alpha_s$ are linearly independent over $\mathbb{Q}$. Then $\beta_0 + \beta_1 \log_p \alpha_1 + \cdots + \beta \log_p \alpha_s \neq 0$ for all $\beta_0, \ldots, \beta_s \in \mathbb{Q}_p$ that are algebraic over $\mathbb{Q}$ and not all zero.*

It will also be useful to have a theorem on multiplicative dependence in a number field K. The following result from [26] establishes this:

Theorem 5.8. *Let K be a number field of degree D over $\mathbb{Q}$. For $s \leq 1$, let $\lambda_1, \ldots, \lambda_s$ be non zero elements of 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 whose entries have absolute value bounded by B where B is computable in terms of H and D.

Proving the unconditional result

This section is focused on establishing Theorem 5.1. For a $\mathbb{Z}$-LRS, the LRBS procedure may turn give a LRBS $\overset{\leftrightarrow}{\mathbf{u}}$ which takes rational values. If $\overset{\leftrightarrow}{\mathbf{u}}$ is a sequence of integers then we say that $\mathbf{u}$ is reversible. A result of [13] shows that a $\mathbb{Z}$-LRS is reversible if and only if $a_{k-1} = \pm 1$.

Claim 5.9. If $\mathbf{u}$ is a reversible $\mathbb{Z}$-LRS then its decomposition into subsequences preserves reversibility. That is, the LRS $\mathbf{u}_{L,m} = (u_{Ln+m})_{n \in \mathbb{N}}$, is reversible for any positive integers L, m.

Proof. Let $\mathbf{u}$ be a $\mathbb{Z}$-LRS with characteristic polynomial g and recurrence coefficients a_i for $0 \leq i \leq k-1$. We know that reversibility is equivalent to $a_{k-1} = \pm 1$ by [13]. We first show that this condition is equivalent to each characteristic root λ_i being a unit in $\mathcal{O}_K$.

Let K be the splitting field of g. Since $\mathbf{u}$ is a $\mathbb{Z}$-LRS, we know that $\lambda_j \in \mathcal{O}_K$ where λ_j for $1 \leq j \leq l$ are the characteristic roots of $\mathbf{u}$. We know that a_{k-1} is, up to some sign, the product of the characteristic roots so each characteristic root is a unit in $\mathcal{O}_K$.

Conversely, if all the characteristic roots are units in $\mathcal{O}_K$ then their product is too. The product of all characteristic roots is rational so it must be ± 1.

Now when we pass to subsequences u_{Ln+m}, the characteristic roots are L^{th} powers of those for u_n so are also units so these LRS are also reversible. In particular, this holds for the decomposition into non degenerate LRS as in Remark 2.2. □

Now we prove Theorem 5.1.

Proof of Theorem 5.1. We will show that a non degenerate reversible $\mathbb{Z}$-LRS of order 7 has at most three dominant roots in modulus so it belongs to the MSTV class. To do this, we'll show that no monic polynomial $g \in \mathbb{Z}[X]$ with degree at most 7 and constant term ± 1 satisfies the following two properties:

(P1) g has at least four distinct roots of maximum modulus.

(P2) No quotient of two distinct roots of g is a root of unity.

We will then apply this to the characteristic polynomial of $\mathbf{u}$ which is a monic polynomial in $\mathbb{Z}[X]$ to prove the theorem. Suppose to the contrary that g has these properties. Let K be the splitting field of g and let $G = \mathrm{Gal}(K/\mathbb{Q})$. We know by (P2) that g cannot have two distinct real dominant roots, otherwise their ratio is -1. By (P1), g has at least four distinct dominant roots. By Theorem 2.7, the dominant roots have modulus strictly greater than 1 otherwise they would all be roots of unity, contradicting (P2). Since the roots of g are units in $\mathcal{O}_K$, they have norm ± 1 so any dominant root must have a conjugate of modulus strictly less than 1 - a non dominant conjugate. There are at least three complex dominant roots and so there are at least least two complex conjugate pairs of dominant roots which we will denote by $\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2}$. These four are all dominant roots. Since every dominant root has a non dominant conjugate, $\deg(g) \geq 5$ - denote by σ the automorphism of K such that $\sigma(\lambda_1) = t$ for some non dominant root t. We have

$$\lambda_1 \overline{\lambda_1} = \lambda_2 \overline{\lambda_2} \tag{20}$$

and so

$$\tau(\lambda_1)\tau(\overline{\lambda_1}) = \tau(\lambda_2)\tau(\overline{\lambda_2}) \tag{21}$$

for all $\tau \in G$. These facts will be used throughout the proof - a common theme will be using (20) and (21) derive contradictions by either considering the modulus of both sides or by contradicting (P2). We know $5 \leq \deg(g) \leq 7$ and so will work through each case. In each case, λ_1 will be a dominant root and t a non dominant root and $\sigma \in G$ is the element such that $\sigma(\lambda_1) = t$ as this exists in every case.

Degree 5: First, we take $\deg(g) = 5$. By (21) with σ, we have $t\sigma(\overline{\lambda_1}) = \sigma(\lambda_2)\sigma(\overline{\lambda_2})$ - a contradiction as σ maps every other root to a dominant root as there is only one non dominant root.

Degree 6: Next, take $\deg(g) = 6$. We can't have $\sigma(\overline{\lambda_1})$ non dominant otherwise, as there are at least four dominant roots, we must have $\sigma(\lambda_2)$ and $\sigma(\overline{\lambda_2})$ dominant, contradicting (21). So $\sigma(\overline{\lambda_1})$ is dominant and at most one of $\{\sigma(\lambda_2), \sigma(\overline{\lambda_2})\}$ is dominant - they cannot both be dominant or it would contradict (21). Therefore the final characteristic root must have the same modulus as t for (21) to hold. By (P2), as there is a second non dominant root v with the same modulus as t, we know that t is not real so $v = \bar{t}$. Working through cases with σ, σ^{-1} and complex conjugation, we see G is transitive so g is irreducible. Therefore the order of G is divisible by 6 so by Cauchy's theorem, it must contain an element τ of order 3 which is either a 3 cycle or the product of two 3 cycles.

By the above, a 3 cycle must either map dominant roots to another, possibly the same, dominant root or map at least two dominant roots to a non dominant root. Therefore we cannot have both $t, \bar{t}$ in the same 3 cycle (if so, t or $\bar{t}$ must map to the other) so if $\tau(t) \neq t$, it must contain another 3 cycle mapping $\bar{t}$ to some dominant root. Therefore the possible cases are $\tau = (D_1 D_2 t)(D_3 D_4 \bar{t})$ or a 3 cycle of the form $\tau = (\lambda_1 \lambda_2 \overline{\lambda_1})$ - where λ_1, λ_2 may have been relabelled. We claim that τ must be a product of 3 cycles $\tau = (D_1 D_2 t)(D_3 D_4 \bar{t})$ where $D_1, \ldots, D_4$ are the dominant roots.

Suppose, in hope of a contradiction, that $\tau = (\lambda_1 \lambda_2 \overline{\lambda_1})$. For (21) to hold for τ, we must have $\tau(\overline{\lambda_2})$ dominant i.e it must be equal to $\overline{\lambda_2}$. Then (21) gives $\lambda_2 \lambda_1 = \overline{\lambda_1 \lambda_2}$ - multiplying by $\overline{\lambda_1} \lambda_2$ and dividing by (20), we get $\lambda_2^2 = \overline{\lambda_1}^2$ which contradicts (P2). This proves the claim.

Next we consider different cases of the form of τ to derive a contradiction.

Case 1: Suppose that some 3 cycle in τ contains a complex conjugate pair. Without loss of generality, we can write $\tau = (\lambda_1 \overline{\lambda_1} t)(\lambda_2 \overline{\lambda_2} \bar{t})$. Applying τ twice to (20), we get both $\overline{\lambda_1} t = \overline{\lambda_2 t}$ and $t\lambda_1 = \bar{t}\lambda_2$. Multiplying these two equations together and dividing by (20) we get $t^2 = \bar{t}^2$, contradicting (P2).

Case 2: Suppose neither 3 cycle in τ contains a complex conjugate pair. By relabelling dominant roots, we can write $\tau = (\lambda_1 \lambda_2 t)(\overline{\lambda_2 \lambda_1} \bar{t})$ as both λ_2 and $\overline{\lambda_2}$ cannot map to non dominant roots. From (21), we have

$$\lambda_2 \bar{t} = t \overline{\lambda_1} \tag{22}$$

We consider two subcases.

Subcase 1: Suppose that $\lambda_1 \lambda_2 t$ is a root of unity. Multiply (22) by $\lambda_1 t^2$ to get $\lambda_1 \lambda_2 t^2 \bar{t} = \lambda_1 \overline{\lambda_1} t^3$. Dividing each side by its complex conjugate, we find that

$$\frac{\lambda_1 \lambda_2 t}{\overline{\lambda_1 \lambda_2 t}} = \left(\frac{t}{\bar{t}} \right)^3,$$

contradicting (P2).

Subcase 2: Next, suppose $\lambda_1 \lambda_2 t$ is not a root of unity. By Theorem 2.7, it has some conjugate $\varphi(\lambda_1 \lambda_2 t) = \varphi(\lambda_1)\varphi(\lambda_2)\varphi(t)$ with modulus greater than 1, for some $\varphi \in G$. But a product of three roots of g having modulus greater 1 means all three must be dominant as the product of two dominant roots and a non dominant root must have modulus 1. This is because the remaining three roots are complex conjugates of these three and the product of all 6 roots must be ± 1 as g has constant term ± 1. So we have some $\varphi \in G$ such that $\varphi(\lambda_1)$,$\varphi(\lambda_2)$ and $\varphi(t)$ are dominant. At most one of $\varphi(\overline{\lambda_1})$ or $\varphi(\overline{\lambda_2})$ can be dominant (as we have four dominant roots). For φ to preserve (20), we would need both to be non dominant. But then (22) is not preserved by φ. This contradiction completes the proof for $\deg(g) = 6$.

Degree 7: Finally, let $\deg(g) = 7$. In the same way as the degree 6 case, we have two complex conjugate pairs of dominant roots $\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2}$ and a pair of non dominant roots $t, \bar{t}$ and that these are contained in an orbit of G. But by the degree 6 case, we know that they cannot be the roots of a degree 6 polynomial so g doesn't have a degree 6 factor, meaning it's irreducible. The remaining root s is real. s cannot be dominant because it would satisfy the equation $\lambda_1\overline{\lambda_1} = \lambda_2\overline{\lambda_2} = s^2$ - applying σ such that $\sigma(\lambda_1) = t$, we must have that σ's image contains three non dominant roots which is not possible.

By the irreducibility of g, we know that the order of G is divisible by 7 so there must be an element τ of order 7 - a 7 cycle. To preserve (20), τ must map exactly two dominant roots to non dominant roots. Label the dominant roots by D_1, D_2, D_3, D_4 and the non dominant roots by N_1, N_2, N_3.

The three cases are $\tau = (D_1D_2N_1N_2D_3D_4N_3), (D_1D_2D_3N_1D_4N_2N_3)$ and $(D_1D_2D_3N_1N_2D_4N_3)$.

Case 1: In the first case, τ^2 maps three dominant roots to non dominant roots, so it doesn't preserve (20).

In both cases 2 and 3, any pair of dominant roots is mapped to some pair of non dominant roots by some power of τ. This means τ doesn't preserve (21) as we can map $\lambda_1, \overline{\lambda_1}$ to non dominant roots and only one of λ_2 or $\overline{\lambda_2}$ can be mapped to a non dominant root. This completes the proof for degree 7 g and so, the proof of the theorem. □

This proof relies on very specific numbers of dominant roots so it cannot be extended generally. Indeed, as in Section 4.2 of [20], a family of degree 8 polynomials with constant term ± 1 satisfying (P1) and (P2) is exhibited.

Skolem meets Schanuel

In this section, we demonstrate Theorem 5.2. The proof of this theorem gives an algorithm for the computation of the set of zeroes of a simple LRS - the Schanuel Conjecture and Skolem Conjecture are required for the termination of this algorithm.

p-adic Power series representation of a LRBS

Let $\mathbf{u}$ be a $\mathbb{Q}$-LRS with recurrence coefficients $a_0, \dots, a_{k-1}$. We can extend the matrix representation $u_n = \alpha A^n \beta$ (for α, β as in (4)) to an LRBS by taking inverse powers of A so that $u_n = \alpha A^n \beta$ for all $n \in \mathbb{Z}$. We can use this representation to express u_n as $f(n)$ where f is a p-adic power series i.e $f(X) = \sum_{j=0}^{\infty} b_j X^j$ with coefficients in $\mathbb{Z}_p$. To define f, we work with a prime p such that

1. p doesn't divide the a_{k-1}.
2. p doesn't divide the discriminant $\Delta\left(\dfrac{g}{\gcd(g, g')}\right)$
3. The characteristic polynomial g splits over $\mathbb{Z}_p$.

There are infinitely many primes satisfying this condition as in Section 2.2 of [3]. We know by Remark 3.4 that, upon scaling $\mathbf{u}$ into a $\mathbb{Z}$-LRS, there is an integer L for which $\lambda_i^L \equiv 1 \bmod p$ for a characteristic root λ_i. Therefore the p adic logarithm $\log_p \lambda_i^L$ is defined. Write $u_n = \sum_{i=1}^{l} Q_i(n)\lambda_i^n$, the exponential-polynomial representation. Then we have

$$u_{Ln} = \sum_{i=1}^{l} Q_i(Ln)\lambda_i^{Ln} = \sum_{i=1}^{l} Q_i(Ln)\exp_p(n\log_p(\lambda_i^L))$$

This motivates the definition

$$f(x) = \sum_{i=1}^{l} Q_i(Lx)\exp_p(x\log_p {\lambda_i}^L) \tag{23}$$

for all $x \in \mathbb{Z}_p$.

Then we have $u_{Ln} = f(n)$ and we can compute Taylor series coefficients b_j of f, giving us

$$b_j = \frac{1}{j!}\sum_{i=1}^{l}\sum_{k=0}^{j}\binom{j}{k} L^k Q_i^{(k)}(0)(\log_p \lambda_i^L)^{j-k} \tag{24}$$

An alternative formula for b_j can be found which makes computation of $v_p(b_j)$ much simpler. As $A^L \equiv I \bmod p$, set $A^L = I + pB$ for an integer matrix B. Then as $A^{Ln} = (I + pB)^n$, by binomial expansion we have:

$$\begin{aligned} u_{Ln} = \alpha(I+pB)^n\beta = \sum_{k=0}^{n}\binom{n}{k}p^k\alpha B^k\beta &= \sum_{k=0}^{\infty}\frac{n(n-1)\dots(n-k+1)}{k!}p^k\alpha B^k\beta \\ &= \sum_{k=0}^{\infty}\sum_{j=0}^{\infty} c_{k,j}n^j\frac{p^k}{k!} = \sum_{j=0}^{\infty}\sum_{k=j}^{\infty} c_{k,j}n^j\frac{p^k}{k!} \end{aligned}$$

for some $c_{k,j} \in \mathbb{Z}$ where $c_{k,j} = 0$ for $j > k$. The swapping of the series in the last step and the convergence of these series in $\mathbb{Z}_p$ are justified by Proposition 4.1.4 in [14]. If the summand $c_{k,j} n^j \frac{p^k}{k!} \to 0$ as $j \to \infty$ and converge to 0 uniformly in j as $k \to \infty$. This follows from $v_p(k!) < \frac{k}{p-1}$ (from Legendre's formula) so $v_p(c_{k,j} n^j \frac{p^k}{k!}) \geq \frac{(p-2)k}{p-1}$ for all $k \geq j$.

Consider the power series $h(X) = \sum_{j=0}^{\infty} d_j X^j$ where

$$d_j = \sum_{k=j}^{\infty} c_{k,j} \frac{p^k}{k!} \in \mathbb{Z}_p. \tag{25}$$

We now aim to use Proposition 4.4.3 of [14] - we can equate coefficients if we know that the two power series agree on $\mathbb{Z}$. By the previous discussion, we have $v_p(d_j) \geq \frac{(p-2)j}{p-1}$ so h converges on $\mathbb{Z}_p$ and has $h(n) = u_{Ln} = f(n)$ so h and f agree on $\mathbb{Z}$ so we have $b_j = d_j$ for all $j \in \mathbb{N}$. Using (25), we can calculate $v_p(b_j)$ for any j such that $b_j \neq 0$.

An algorithm for the zeroes of an LRBS

In this section we show that conditional on the weak p-adic Schanuel Conjecture that the set of all zeroes of a non degenerate LRBS is computable using an oracle for the Bi-Skolem Problem. This gives a Turing reduction of the Skolem Problem to the Bi-Skolem Problem. We then show that this reduction is unconditional for order 5 LRS.

Proposition 5.10. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be given by a convergent p-adic power series $f(X) = \sum_{k=0}^{\infty} b_k X^k$ with coefficients in $\mathbb{Z}_p$. Choose a positive integer t such that $b_0 = \cdots = b_{t-1} = 0$ and $b_t \neq 0$. With $\nu = v_p(b_t)$, we have $f(p^{\nu+1}x) \neq 0$ for all non zero $x \in \mathbb{Z}_p$.

Proof. Let $x \in \mathbb{Z}_p$ be non zero. For $m > t$, we have

$$v_p(b_t(p^{\nu+1}x)^t) = \nu + t(\nu+1) + v_p(x^t) < m(\nu+1) + v_p(x^m) \leq v_p(b_m(p^{\nu+1}x)^m)$$

So for any $m \geq t$, we have that

$$v_p\left(\sum_{k=0}^{m} b_k (p^{\nu+1}x)^k\right) = v_p(b_l(p^{\nu+1}x)^t)$$

Taking $m \to \infty$, we have $v_p(f(p^{\nu+1}x)) = v_p(b_l(p^{\nu+1}x)^t) < \infty$ so $f(p^{\nu+1}x) \neq 0$ as required. □

For an LRBS $\mathbf{u}$, the following proposition gives us an algorithm to find a positive integer M such that $u_{Mn} \neq 0$ for all $n \in \mathbb{Z}\backslash\{0\}$.

Theorem 5.11. *Let $\mathbf{u} = \{u_n\}_{n=-\infty}^{\infty}$ be a non zero $\mathbb{Q}$-LRBS. Assuming the weak p-adic Schanuel Conjecture, we can compute a positive integer M such that $u_{Mn} \neq 0$ for all $n \in \mathbb{Z}\backslash\{0\}$.*

Proof. As in the previous section, let p be a prime and L be a positive integer such that $u_{Ln} = f(n)$ for $n \in \mathbb{Z}$ where $f(X) = \sum_{j=0}^{\infty} b_j X^j$ is a p-adic power series with coefficients in $\mathbb{Z}_p$. Recall the expression (23) for f where Q_i are from the exponential-polynomial representation and λ_i for $1 \leq i \leq l$ are characteristic roots.

Pick a maximal multiplicatively independent subset of characteristic roots, label them without loss of generality by $\{\lambda_1, \ldots, \lambda_t\}$ for some $t \leq l$. Let K be the subfield of $\mathbb{Q}_p$ generated by $\lambda_1, \ldots, \lambda_l$. With Theorem 5.8, we can compute integers m_i and $n_{i,j}$, where $m_i \neq 0$, such that for all $i \in \{1, \ldots, l\}$ and $j \in \{1, \ldots, t\}$, we have $\lambda_i^{m_i} = \lambda_1^{n_{i,1}} \ldots \lambda_t^{n_{i,t}}$. Then we have

$$\log_p {\lambda_i}^L = \frac{n_{i,1}}{m_i} \log_p {\lambda_i}^L + \cdots + \frac{n_{i,t}}{m_i} \log_p {\lambda_t}^L$$

This means for each $i \in \{1, \ldots, l\}$, we have $\log_p {\lambda_i}^L = \mathcal{L}_i(\log_p {\lambda_1}^L, \ldots, \log {\lambda_t}^L)$ where $\mathcal{L}_i$ is a computable linear form in t variables with rational coefficients.

For $j \in \mathbb{N}$, define $F_j \in K[X_1, \ldots, X_t]$ by

$$F_j(X_1, \ldots, X_t) = \frac{1}{j!} \sum_{i=1}^{l} \sum_{d=0}^{j} \binom{j}{d} L^d Q_i^{(d)}(0) l_i(X_1, \ldots, X_t)^{j-d}$$

By (24), we have

$$b_j = F_j(\log_p {\lambda_1}^L, \ldots, \log_p {\lambda_t}^L) \tag{26}$$

If F_j isn't identically zero, the coefficients of F_j are algebraic over $\mathbb{Q}$ and the set $\{\log_p \lambda_1, \ldots, \log_p \lambda_t\}$ is linearly independent over $\mathbb{Q}$, so we can apply the weak p-adic Schanuel conjecture to conclude that $b_j \neq 0$.

This gives us a procedure to calculate M:

1. Compute the polynomials $F_0, F_1, \ldots$

2. Let j_0 be the least index j such that F_j isn't identically zero. This exists as if all b_j are zero, $\mathbf{u}$ is the zero sequence so we know $j_0 \leq k-1$. Compute $\nu = v_p(b_{j_0})$. We know that this will terminate conditional on the p-adic Schanuel conjecture as it implies $b_{j_0} \neq 0$.

3. By proposition 7, for $M = Lp^{\nu+1}$ we have that $u_{Mn} \neq 0$ for all non zero integers n.

This completes the proof. □

The weak p-adic Schanuel conjecture is only required to guarantee the termination of the calculation of $v_p(b_{j_0})$. Next we prove Theorem 5.2.

Proof of Theorem 5.2. We use a recursive procedure. As we are looking for zeroes, by Remark 2.2 we can assume without loss of generality that our LRS $\{u_n\}_{n=0}^{\infty}$ is non degenerate and we can extend it to an LRBS $\mathbf{u} = \{u_n\}_{n=-\infty}^{\infty}$. Using the oracle for the Bi-Skolem problem, we either find $n_0 \in \mathbb{Z}$ such that $u_{n_0} = 0$ - if there is no such n_0, the procedure terminates and we are done. Reindexing so that $n_0 = 0$, we can then apply proposition 7 to find M such that $u_{Mn} \neq 0$ for non zero integers n. Then we can split the sequence u_n into u_{Mn+j} for $j \in \{0, \ldots, M-1\}$ and repeat the procedure on these sequences. This must terminate eventually because the Skolem-Mahler-Lech Theorem for non degenerate sequences states there are only finitely many zeroes, as in Theorem 2.1 of [12]. □

This is our algorithm, requiring both the p-adic Schanuel conjecture and the Skolem Conjecture to terminate. Restricting to LRS of up to order 5, we can remove the p-adic Schanuel dependence, Theorem 5.3.

Proof of Theorem 5.3. We only need to focus on $\mathbb{Q}$-LRS $\mathbf{u}$ not belonging to the MSTV class. By Remark 4.11, we know that $u_n = \sum_{i=1}^{5} \alpha_i \lambda_i^n$ where $\alpha_1 \neq -\alpha_3$ (as they aren't of equal modulus), $\lambda_5 \in \mathbb{R}$ and

$$\lambda_1 \lambda_2 = \lambda_3 \lambda_4 \tag{27}$$

- the four dominant roots. Let K be the number field generated by the λ_i, let $d = [K : \mathbb{Q}]$ and $\mathcal{O}_K$ be the ring of integers of K. We can rescale $\mathbf{u}$ so that no rational prime divides all of the characteristic roots and that $\lambda_i \in \mathcal{O}_K$. As we saw in the proof of Theorem 5.1 for the order 5 case, the set $\{\lambda_1, \ldots, \lambda_4\}$ is invariant under any automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Therefore any Galois conjugate of $\frac{\lambda_1}{\lambda_2}$ has modulus 1 so we know that by Theorem 2.8 that there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(\lambda_1) \neq v_{\mathfrak{p}}(\lambda_2)$. Without loss of generality, suppose that $\mathfrak{p}$ divides λ_1. If we can show that $v_{\mathfrak{p}}(\lambda_i) = 0$ for some $i \in \{2, 3, 4, 5\}$ then since $\mathbf{u}$ doesn't belong to the MSTV class, there are at least three dominant roots with respect to $v_{\mathfrak{p}}$. By (27) we then get that $v_{\mathfrak{p}}(\lambda_1) = v_{\mathfrak{p}}(\lambda_3) > 0$ and $v_{\mathfrak{p}}(\lambda_2) = v_{\mathfrak{p}}(\lambda_4) = v_{\mathfrak{p}}(\lambda_5) = 0$.

Suppose for contradiction that $\mathfrak{p}$ divides every characteristic root. Let $\mathfrak{p}$ lie above the rational prime p and let its ramification index be e. $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the prime ideals lying above p so every prime ideal above p divides every characteristic root to order at least d. We know $d \geq e$ as $e \mid d$. Therefore, there is a rational prime dividing every characteristic root, a contradiction. In summary, we have a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ that divides λ_1 and λ_3 but not $\lambda_2, \lambda_3, \lambda_5$.

Now to the proof of the theorem. We need to avoid the use of the weak p-adic Schanuel conjecture - proving that the procedure terminates unconditionally is sufficient. For this, it is enough to show that for such $\mathbb{Q}$-LRBS $\mathbf{u}$, we can compute M such that $u_{Mn} \neq 0$ for all non zero integers n. Our aim will be to find a multiplicative relation among the λ_i which involves λ_3 but not λ_1 - this will contradict the fact that there is an ideal $\mathfrak{p} \lhd \mathcal{O}_K$ which divides λ_1 and λ_3 but not $\lambda_2, \lambda_3, \lambda_5$.

Choose a prime p such that there is an embedding $K \hookrightarrow \mathbb{Q}_p$. Let $f(X) = \sum_{j=0}^{\infty} b_j X^j$ be a p-adic power series such that there is a positive integer L for which $u_{Ln} = f(n)$. From (24), in this case we have $b_1 = \sum_{i=1}^{5} \alpha_i \log_p {\lambda_i}^L$. We will prove that $b_1 \neq 0$. Suppose for contradiction that $b_1 = 0$. By (27), we have

$$\log_p {\lambda_1}^L + \log_p {\lambda_2}^L - \log_p {\lambda_3}^L - \log_p {\lambda_4}^L = 0$$

where L is an integer such that $\lambda_i^L \equiv 1 \bmod p$. Cancelling $\log_p {\lambda_1}^L$, we have

$$(\alpha_2 - \alpha_1) \log_p {\lambda_2}^L + (\alpha_3 + \alpha_1) \log_p {\lambda_3}^L + (\alpha_4 + \alpha_1) \log_p {\lambda_4}^L + \alpha_5 \log_p {\lambda_5}^L = 0 \tag{28}$$

Since $\alpha_1 \neq -\alpha_3$, the $\log_p \lambda_3^L$ term is non zero. By applying Theorem 5.7, we obtain an equation $\sum_{i=2}^{5} \beta_i \log {\lambda_i}^L \neq 0$ such that β_i are integers and $\beta_3 \neq 0$ - this gives us the contradictory multiplicative relation. □

Some examples of the algorithm established in the proof of Theorem 5.2 are given in Section 5 of [3].

6 Universal Skolem sets

A new approach to the Skolem problem was initiated in 2021 in [21]. Instead of placing restrictions on the LRS such as its order, we can place restrictions on the domain where we search for zeroes. This leads to the definition of a universal Skolem set, a set where the Skolem problem is decidable. In this essay, we will define the example of a universal Skolem set as in [23, 22] but will not prove this property. Instead, we will focus on showing it has positive density at least 0.29 unconditionally and density 1 conditional on the Bateman Horn conjecture, a very general conjecture regarding the distribution of primes.

Definition 6.1 (Universal Skolem Set)**.** An infinite set $S \subseteq \mathbb{N}$ is a universal Skolem Set if given any $\mathbb{Z}$-LRS $\mathbf{u}$, there is an effective procedure that outputs whether or not there is $n \in S$ such that $u_n = 0$.

We begin by defining S, the example of a universal Skolem set. For a real number $x > 1$ and positive integer m, we inductively define the repeated logarithm function $\log_m x$ by $\log_1 x = \log x$ and if $m \geq 2$, $\log_m x = \max(1, \log_{m-1}(\log x))$.

Fix a large positive integer X. We define the two disjoint intervals $A(X)$ and $B(X)$ by

$$A(X) = \left[\log_2 X, \sqrt{\log X}\right] \text{ and } B(X) = \left[\frac{\log X}{\sqrt{\log_3 X}}, \frac{2\log X}{\sqrt{\log_3 X}}\right] \tag{29}$$

Define the representation of an integer $n \in [X, 2X]$ by a triple (q, P, a) where $q \in A(X)$, $a \in B(X)$, P and q are prime and $n = Pq + a$. Say that two representations $n = Pq + a$ and $n = P'q' + a'$ are correlated if

$$q \neq q', a \neq a' \text{ and } |(a + \eta q) - (a' + \eta q')| < \sqrt{\log X}$$

for some $\eta \in \{\pm 1\}$. Denote the number of representations of n by $r(n)$. Then we define the set

$$S(X) = \{n \in [X, 2X] : r(n) > \log_4(X) \text{ and no two representations are correlated}\}$$

and define

$$S = \bigcup_{k \geq 10} S(2^k) \tag{30}$$

We cite the following theorem which demonstrates that S is a universal Skolem set - it shows that any zero belonging to S is bounded by some computable upper bound:

Theorem 6.2. *Let $\boldsymbol{u} = \{u_n\}_{n=0}^{\infty}$ be a non degenerate $\mathbb{Z}$-LRS of order $k \geq 2$ with recurrence coefficients $a_0, \ldots, a_{k-1}$ with initial terms $u_0, \ldots, u_{k-1}$ not all zero. If $n \in Ann(\boldsymbol{u}) \cap S$ then*

$$n < \max(\exp_3(A^2), \exp_5(10^{10}k^6)), \textit{ where } A = \max(10, |u_i|, |a_i| : 0 \leq i \leq k-1)$$

The proof of this theorem is in Section 3 of [23]. We will focus on the density of S, namely proving the following theorem:

Theorem 6.3 (Density of S)**.** *The density of S is unconditionally at least 0.29 and it is 1 subject to the Bateman-Horn conjecture.*

We begin with a discussion of the Bateman Horn Conjecture.

The Bateman Horn Conjecture

The Bateman Horn Conjecture [35] is a conjecture in number theory concerning the frequency of prime numbers among a system of polynomials.

Conjecture 6.4 (Bateman-Horn Conjecture)**.** Let $f_1, \ldots, f_k$ be polynomials in one variable with integer coefficients, positive leading coefficient and degrees $h_1, \ldots, h_k$. Assume that each of these polynomials are irreducible over $\mathbb{Q}$ and no two of them differ by a constant factor. Let $Q(f_1, \ldots, f_k; N) = \#\{1 \leq n \leq N : f_1(n), \ldots, f_k(n) \text{ are all primes}\}$ where n is an integer. Then

$$Q(f_1, \ldots, f_k; N) \sim \frac{C(f_1, \ldots, f_k)}{h_1 h_2 \cdots h_k} \int_2^N (\log u)^{-k}\, du,$$

where $C(f_1, \ldots, f_k) = \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega(p)}{p}\right)$.

where the product is taken over all primes p and $\omega(p)$ is the number of solutions to the congruence $f_1(x)f_2(x)\dots f_k(x) \equiv 0 \bmod p$ for $0 \leq x < p-1$. If $\omega(p) = p$ then the product is 0 - this happens if p divides the product $f_1(m)\dots f_n(m)$ for each $0 \leq m < p-1$. In this case, there can only be finitely many m for which all the f_i are simultaenously prime because if p divides their product, $f_i(m) = p$ for some i which can only happen finitely many times - at most h_i times. So in this case Q is finite - this case isn't of interest. A proof of the convergence of $C(f_1, \dots, f_k)$ and a heuristic argument for this conjecture can be found in [35].

We will use the result for linear functions $f_1(t) = a_1t + b_1, f_2(t) = a_2t + b_2$ where $a_1, a_2 > 0$ and a_1, a_2, b_1, b_2 are integers. Then we have an upper bound on $Q(f_1, f_2; N)$:

$$Q(f_1, f_2; N) \leq SC(f_1, f_2)\int_2^N (\log u)^{-k} \mathrm{d}u \tag{31}$$

where S is some positive real number. [35] gives $S = 8$ while the current best result found via the large sieve is $S = 3.418$, shown by Wu [38]. This upper bound will give us unconditional positive density results. From this, with $\Delta = |a_1a_2(a_1b_2 - b_1a_2)| \neq 0$, we deduce

$$Q(f_1, f_2; N) \ll \frac{\Delta}{\varphi(\Delta)}\frac{N}{(\log N)^2} \tag{32}$$

where $f \ll g$ is the Vinogradov notation, meaning $f = O(g(X))$.

Finding the density of S

Now we focus on proving Theorem 6.3. Fix a large positive integer X.

In the definition of S we removed $n \in \mathbb{N}$ which had two correlated representations. Therefore we will follow these steps to prove Theorem 6.3:

1. Prove that the set of n in $[X, 2X]$ which have two correlated representations has density zero.

2. Show that $\{n \in [X, 2X] : r(n) > \log_4 X\}$ has density one subject to the Bateman Horn conjecture, and density at least 0.29 unconditionally.

We follow the proof as in [23]. Originally, I followed the exposition in the August 2023 version of this paper, alongside the unconditional positive density result in [22]. In [35], I found that bounds of the form (31) existed which streamlined the positive density proof and gave a lower bound, but this was also found in the February 2024 edition of [23]. In this section, in sums and products, the indices p, q, P, P' run over positive primes. First, we need the following result:

Proposition 6.5. $\sum_{q \in A(X)} \frac{1}{q} \sim \log_3 X$

Proof. Mertens' first theorem [27] states $\sum_{p\leq X}\frac{1}{p} = \log_2 X + M + O(\frac{1}{\log X})$. Therefore

$$\sum_{q\in A(X)}\frac{1}{q} = \sum_{q\leq\sqrt{\log X}}\frac{1}{q} - \sum_{q\leq\log_2 X}\frac{1}{q} = \log_2\sqrt{\log X} - \log_4 X + o(1) \sim \log_3 X$$

as required. □

The following proposition is step 1 of our proof:

Proposition 6.6. The set of $n \in [X, 2X]$ which has two correlated representations has cardinality $O(\frac{X}{(\log X)^{1/3}})$. In particular, it has density 0.

Proof. Let $n = qP + a = q'P' + a'$ be as in the definition of the representation of an integer - $q, q' \in A(X)$ and $a, a' \in B(X)$. Suppose that $q \neq q'$ and $a \neq a'$. Since $|(a + \eta q) - (a' - \eta q)| < \sqrt{\log X}$ (where $\eta = \pm 1$) and $q, q' \leq \sqrt{\log X}$, we have $|a - a'| < 2\sqrt{\log X}$. We will count the number of pairs of primes P, P' such that

$$qP + a = q'P' + a' \in [X, 2X] \tag{33}$$

Counting solutions to the system, as it's linear and $\gcd(q, q') = 1$, we can write the solutions (P, P') to this equation as $P = P_0 + q't, P' = P_0' + qt$ for some integer $t \geq 0$ and some minimal solution P_0, P_0'. This puts it in the form to use (32) as $\Delta = |qq'(qP_0 - q'P_0')| = |qq'(a - a')| \neq 0$. Since $qP + a \leq 2X$, we have $P \leq \frac{2X}{q}$ so that $t \leq \frac{2X}{qq'}$. Therefore by (32), we have that the number of t such that both $P_0 + q't$ and $P_0' + qt$ are prime is

$$\ll \frac{X}{qq'(\log X)^2}\left(\frac{|qq'(a-a')|}{\varphi(|qq'(a-a')|)}\right) \ll \frac{X\log_3 X}{qq'(\log X)^2} \tag{34}$$

where in the second line we use the inequality $\frac{m}{\varphi(m)} \ll \log_2 m$, (Theorem 328 of [17]) as $|qq'(a - a')| \leq 2(\log X)^{\frac{3}{2}}$ as $q, q' \leq \sqrt{\log X}$ and $|a - a'| \leq 2\sqrt{\log X}$. Next, we sum over the number of solutions of (33) over the different choices of $q \neq q' \in A(X)$ and $a \neq a' \in B(X)$ such that $|(a + \eta q) - (a' - \eta q)| < \sqrt{\log X}$. Recall that there are at most $2\sqrt{\log X}$ choices of a'. $a \in B(X)$ so there are at most $\frac{\log X}{\sqrt{\log_3 X}}$ ways of choosing a. This gives us a count of

$$\frac{X\log_3 X}{(\log X)^2}\left(\sum_{q\leq\sqrt{\log X}}\frac{1}{q}\right)^2\left(\frac{\log X}{\sqrt{\log_3 X}}\right)\sqrt{\log X} \ll \frac{X(\log_3 X)^{2.5}}{\sqrt{\log X}}$$

where constants are omitted because we're using Vinogradov notation. The first two terms come from summing over (34), with the sum being squared as q, q' are independent. The third and fourth terms are from the number of choices of a and a'. This gives the number of n coming from a tuple (q, q', a, a', P, P') as $O\left(\frac{X}{(\log X)^{\frac{1}{3}}}\right)$. This completes the proof. □

Next we prove step 2 in the plan. We use the same notation as before. We aim to count the number of representations $r(n)$ for $n \in [X, 2X]$ - if we can show that $r(n) = (C + o(1))\sqrt{\log_3 X}$ for $(1 + o(1))X$ integers n in $[X, 2X]$ then we have that $|S(X)| = (1 + o(1))X$ and so that S has density 1. We do this by considering zeroth to second moments of $r(n)$, let

$$M_i(X) = \sum_{\substack{n\in[X,2X] \\ r(n)>\log_4 X}} r(n)^i$$

for $i = 0, 1, 2$. Our aim is to show that $M_0(X) = (1 + o(1))X$. By the Cauchy Schwarz inequality, we know that $M_0(X)M_2(X) \geq M_1(X)^2$.

For the first moment,

$$\begin{aligned}\sum_{\substack{n\in[X,2X] \\ r(n)>\log_4 X}} r(n) = \sum_{\substack{q\in A(X) \\ a\in B(X)}} \sum_{\frac{X-a}{q}\leq p\leq\frac{2X-a}{q}} 1 &= (1 + o(1)) \sum_{\substack{q\in A(X) \\ a\in B(X)}} \frac{X}{q \log X} \\ &= (1 + o(1))X\sqrt{\log_3 X}\end{aligned}$$

by the prime number theorem and Theorem 6.5. If we can show that

$$\sum_{\substack{n\in[X,2X] \\ r(n)>\log_4 X}} r(n)^2 = (1 + o(1))X \log_3 X \tag{35}$$

then we would have $M_0(X) = (1 + o(1))X$ as $M_0(X)M_2(X) \geq M_1(X)^2$.

To prove this, we can use estimates on the number of pairs of primes P, P' such that (33) holds. For this we can apply the Bateman Horn conjecture as long as $a \neq a' \in B(X)$, $q \neq q' \in A(X)$, $\gcd(a - a', qq') = 1$ and $2 \mid (a - a')$. However from the previous discussion, if this isn't true we know that we fall into a degenerate case - indeed, if they don't hold then (33) has no solutions. We can also apply (31). This gives us that the number of solutions to (33) is

$$T = (C' + o(1))\frac{X}{qq'(\log X)^2} g(|a - a'|) \tag{36}$$

conditional on the Bateman Horn conjecture, where

$$C' = 2\prod_{p>2} \frac{p(p-2)}{(p-1)^2} \approx 1.32 \text{ and } g(m) = \prod_{\substack{p|m \\ p>2}} \frac{p-1}{p-2}.$$

C' is known as the twin prime constant and g is a multiplicative function. Unconditionally we have that the number of solutions is upper bounded by

3.418T by (31). Now we can calculate the second moment;

$$\begin{aligned}\sum_{n\in[X,2X]} r(n)^2 &= \sum_{\substack{a,a'\in B(X)\\ q,q'\in A(X)}} \sum_{P,P'} \mathbf{1}_{\{qP+a=q'P'+a'\in[X,2X]\}} \text{ (counting independent pairs)}\\ &= \sum_{\substack{a\neq a'\in B(X)\\ q\neq q'\in A(X)\\ 2|a-a'\\ \gcd(a-a',qq')=1}} (C'+o(1))\frac{X}{qq'(\log X)^2} g(|a-a'|) + O(X\sqrt{\log_3 X})\\ &= (C'+o(1))\frac{X(\log_3 X)^2}{(\log X)^2} \sum_{\substack{a\neq a'\in B(X)\\ 2|(a-a')}} g(|a-a'|) + O(X\sqrt{\log_3 X})\end{aligned}$$

by applying Proposition 6.5 twice. Here, the $O(X\sqrt{\log_3 X})$ term comes from the $q=q', a=a'$ case. To simplify the sum with g, we make use of the following theorem, from [38] Section 1.3, Theorem 11.

Theorem 6.7. *Let f be a multiplicative function with values in $[0,1]$. Write*

$$M_f = \prod_{p\ prime} (1-p^{-1}) \sum_{v=0}^{\infty} f(p^v)p^{-v},$$

where the infinite product is taken to be zero if it diverges. Then for Y tending to infinity, we have

$$\sum_{n\leq Y} f(n) = Y(M_f + o(1)).$$

Since g is a multiplicative function, we have for Y tending to infinity,

$$\sum_{\substack{n\leq Y\\ 2|n}} g(n) = \sum_{n\leq \frac{Y}{2}} g(n) = \frac{Y+o(Y)}{2}\prod_{p>2}\left(1+\frac{g(p)-1}{p}\right) = \frac{Y+o(Y)}{2}\prod_{p\geq 2}\left(1+\frac{1}{p(p-2)}\right)$$

where the first equality comes from $g(2n)=g(n)$ for all n, the second follows by Theorem 6.7 and the final equality comes from $g(p)=\frac{p-1}{p-2}$. The final product on the right hand side converges to a finite value. Finally, since $B(X)$ has length $\frac{\log X}{\sqrt{\log_3(X)}}$, we deduce

$$\begin{aligned}\sum_{\substack{a\neq a'\in B(X)\\ 2|(a-a')}} g(|a-a'|) &= \frac{1+o(1)}{2}\left(\frac{\log X}{\sqrt{\log_3 X}}\right)^2 \prod_{p>2}\left(1+\frac{1}{p(p-2)}\right)\\ &= \frac{1+o(1)}{C'}\left(\frac{\log X}{\sqrt{\log_3 X}}\right)^2.\end{aligned}$$

So overall we get

$$\sum_{n \in [X,2X]} r(n)^2 = (1 + o(1)) X \log_3 X \tag{37}$$

as required. If instead we had used the unconditional version of Bateman Horn, in the calculation of $M_2(X)$ we would get $M_2(X) \leq 3.418(1 + o(1))X \log_3(X)$ so through the Cauchy Schwarz argument, we will get a lower bound $M_0(X) \geq (0.29 + o(1))X$. This gives us our density results on S.

7 Conclusion

The key steps of this essay are the following:

1. We have proven the Skolem-Mahler-Lech theorem for LRS over a field of characteristic zero, following a proof by [16]. This proof was modified from its original form concerning power series of rational functions to LRS, simplifying the proofs. It was shown that the determination of the period of the arithmetic progression is effective for LRS over a field of characteristic zero. As it is possible to decide whether Ann($\mathbf{u}$) is finite, we found that the Skolem Problem is equivalent to deciding whether the finite set in Ann($\mathbf{u}$) is empty or not.

2. By combining the approaches in [18, 29], the Skolem Problem was shown to be decidable for LRS belonging to the MSTV class - notably, this includes all $\overline{\mathbb{Q}} \cap \mathbb{R}$-LRS of order up to 4. Through the notion of reversibility, a definition inspired by LRBS, we showed that reversible $\mathbb{Z}$-LRS of order up to 7 belong to the MSTV class. These methods could not be extended to order 8 though.

3. With dependence on the p-adic Schanuel conjecture, an important conjecture in transcendental number theory, it was shown that there is a Turing reduction from the Skolem Problem for $\mathbb{Q}$-LRS to the Bi-Skolem problem. By also assuming the Skolem Conjecture, it was shown that the Skolem Problem is decidable for simple LRS. The proof of this theorem produced an algorithm - the conjectural dependence is only required for the termination of the algorithm. Furthermore, the dependence on the p-adic Schanuel Conjecture can be removed in the case of simple LRS of order up to 5 so that only the Skolem Conjecture is required.

4. Instead of placing restrictions on the LRS to solve the decidability problem, instead restrictions can be placed on the set. This leads to the notion of a universal Skolem set, a set where the Skolem Problem is decidable for $\mathbb{Z}$-LRS. We cited the existence of a universal Skolem set and proved it is of positive density at least 0.29 and of density 1 assuming the Bateman-Horn conjecture, a vast generalisation of many famous theorems and conjectures in analytic number theory such as the prime number theorem and the twin prime conjecture.

Bibliography

References

[1] A. Baker. A sharpening of the bounds for linear forms in logarithms ii. *Acta Arithmetica*, 24(1):33–36, 1973. URL `http://eudml.org/doc/205210`.

[2] J. Berstel and M. Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France, Volume 104*, pages 175–184, 1976.

[3] Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. Skolem meets schanuel, 2022.

[4] V. Blondel and J. Tsitsiklis. A survey of computational complexity results in systems and control. *Automatica, 36(9)*, pages 1249–1274, 2000.

[5] Enrico Bombieri and Walter Gubler. *Heights in Diophantine Geometry*. New Mathematical Monographs. Cambridge University Press, 2006.

[6] Florian Luca Boris Bartolome, Yuri Bilu. On the exponential local-global principle. *Acta Arithmetica*, 159(2):101–111, 2013. URL `http://eudml.org/doc/286065`.

[7] Lech C. A note on recurring series. *Ark. Mat., 2*, 1953.

[8] Frank Calegari and Barry Mazur. Nearly ordinary galois deformations over arbitrary number fields, 2008.

[9] K. Chatterjee and L. Doyen. Stochastic processes with expected stopping time. *In 36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS*, pages 1–13, 2021.

[10] K. Conrad. Ostrowski for number fields.

[11] Harm Derksen. A skolem-mahler-lech theorem in positive characteristic and finite automata, 2005.

[12] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence Sequences*. American Mathematical Society, 2003.

[13] P. Fatou. Sur les séries entières à coefficients entiers. *Comptes Rendus Acad. Sci. Paris 138, 130*, pages 342–344, 1904.

[14] F. Gouvea. *p-adic Numbers: An Introduction, Second Edition*. Universitext. Springer, 1997.

[15] M. Hamburg. Construction of $\mathbb{C}_p$ and extension of p-adic valuations to $\mathbb{C}$. 2004.

[16] G. Hansel. Une démonstration simple du théorème de skolem-mahler-lech. *Theoretical Computer Science*, 43:91–98, 1986. ISSN 0304-3975. doi: https://doi.org/10.1016/0304-3975(86)90168-4. URL `https://www.sciencedirect.com/science/article/pii/0304397586901684`.

[17] G.H. Hardy and Wright E. M. *An introduction to the theory of numbers*. Clarendon Press, 1954.

[18] Vereshchagin N. K. The problem of appearance of a zero in a linear recurrence sequence. *Mathematical notes of the Academy of Sciences of the USSR Volume 38*, pages 609–615, 1985.

[19] L. Kronecker. Zwei satse ¨ uber ¨ gleichungen mit ganzzahligen coefficien-

ten. , *J. Reine Angew. Math. 53*, pages 173–175, 1857.

[20] Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the skolem problem and the skolem conjecture. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '22, New York, NY, USA, 2022. Association for Computing Machinery. ISBN 9781450393515. doi: 10.1145/3531130.3533328. URL `https://doi.org/10.1145/3531130.3533328`.

[21] F. Luca, J. Ouaknine, and J. Worrel. Universal skolem sets. *36th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 1–6, 2021.

[22] F. Luca, J. Ouaknine, and J. Worrel. A universal skolem set of positive lower density. *47th International Symposium on Mathematical Foundations of Computer Science, MFCS, volume 241 of LIPIcs*, pages 73:1–73:12, 2022.

[23] Florian Luca, James Maynard, Armand Noubissie, Joël Ouaknine, and James Worrell. Skolem meets bateman-horn, 2024.

[24] K. Mahler. *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen.* Noord-Hollandsche Uitgevers Mij, 1935. URL `https://books.google.co.uk/books?id=BUxy0AEACAAJ`.

[25] David Masser. *Auxiliary Polynomials in Number Theory.* Cambridge Tracts in Mathematics. Cambridge University Press, 2016.

[26] David William Masser. New advances in transcendence theory: Linear relations on algebraic groups. 1988. URL `https://api.semanticscholar.org/CorpusID:115368865`.

[27] F. Mertens. Ein beitrag zur analytischen zahlentheorie. *J. reine angew. Math. 78*, 1874.

[28] M. Mignotte. A note on linear recursive sequences. *J. Australian Math. Soc. 20 (Series A)*, pages 242–244, 1975.

[29] M. Mignotte, T. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *J. f¨ur die reine und angewandte Math., 349*, 1984.

[30] J. Ouaknine and J. Worrell. On linear recurrence sequences and loop termination. *ACM SIGLOG News, 2(2)*, pages 4–13, 2015.

[31] G. Rozenburg and A. Salomaa. *Cornerstones of Undecidability.* Prentice Hall, 1994.

[32] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith. 32, 3*, pages 245–274, 1977.

[33] A. Schinzel. On the congruence $u_n \equiv c \bmod p$ where un is a recurring sequence of the second order. *Acta Acad. Paedagog. Agriensis Sect. Math. 30*, pages 147–165, 2003.

[34] T. Shorey. Linear forms in members of a binary recursive sequence. *Acta Arithmetica*, 43(4):317–331, 1984. URL `http://eudml.org/doc/205912`.

[35] Bateman P. T and Horn R. A. A heuristic asymptotic formula concerning the distribution of prime numbers. *Mathematics of Computation*, 16(79): 363–367, 1962. ISSN 00255718, 10886842. URL `http://www.jstor.org/stable/2004056`.

[36] Skolem T. Ein verfahren zur behandlung gewisser exponentialer gleichungen. *Comptes rendus du congr‘es des math ́ematiciens scandinaves*, 1933.

[37] T. Tao. Structure and randomness: pages from year one of a mathematical blog, 2008.

[38] G. Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory: Third Edition*. American Mathematical Society, 2015.

[39] A. J. van der Poorten. Linear forms in logarithms in the p-adic case. *Transcendence Theory: Advances and Applications*, pages 29–57, 1977.