Accepted Manuscript

Effective results on the Skolem Problem for linear recurrence sequences

Min Sha

PII: S0022-314X(18)30247-6
DOI: https://doi.org/10.1016/j.jnt.2018.08.012
Reference: YJNTH 6111

To appear in: *Journal of Number Theory*

Received date: 20 July 2018
Revised date: 23 July 2018
Accepted date: 26 August 2018

Please cite this article in press as: M. Sha, Effective results on the Skolem Problem for linear recurrence sequences, *J. Number Theory* (2019), https://doi.org/10.1016/j.jnt.2018.08.012

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

EFFECTIVE RESULTS ON THE SKOLEM PROBLEM FOR LINEAR RECURRENCE SEQUENCES

MIN SHA

ABSTRACT. In this paper, given a simple linear recurrence sequence of algebraic numbers, which has either a dominant characteristic root or exactly two characteristic roots of maximal modulus, we give some explicit lower bounds for the index beyond which every term of the sequence is non-zero. It turns out that this case covers almost all such sequences whose coefficients are rational numbers.

ACCEPTED MANUSCRIPT

1. INTRODUCTION

1.1. **Background and motivation.** Linear recurrence sequences (LRS) appear almost everywhere in mathematics and computer science, and they have been studied for a very long time; see [10] for a deep and extensive introduction. In this paper, we focus on the *Skolem Problem*, which asks whether there is a zero term in a given LRS.

As usual, let $\bar{\mathbb{Q}}$ be the field of all algebraic numbers, which is an algebraic closure of the rational numbers $\mathbb{Q}$. Recall that an LRS of *order* $m \geq 1$ is a sequence $\{u_n\}_{n=0}^{\infty}$ with elements in $\bar{\mathbb{Q}}$ satisfying a recurrence relation

$$u_{n+m} = a_{m-1}u_{n+m-1} + \cdots + a_0 u_n \quad (n = 0, 1, 2, \ldots), \tag{1.1}$$

where $a_0, \ldots, a_{m-1} \in \bar{\mathbb{Q}}$, $a_{m-1} \neq 0$ and $u_j \neq 0$ for at least one j in the range $0 \leq j \leq m-1$. Here, we call $a_0, \ldots, a_{m-1}$ the *coefficients* of the sequence $\{u_n\}$, and the *initial terms* of $\{u_n\}$ are $u_0, \ldots, u_{m-1}$.

Several crucial properties of the sequence $\{u_n\}$ rely on its *characteristic polynomial*, which is defined as

$$f(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_0 = \prod_{i=1}^{k}(X - \alpha_i)^{d_i} \in \bar{\mathbb{Q}}[X]$$

with distinct $\alpha_1, \alpha_2, \ldots, \alpha_k$ (which are called the *characteristic roots* of the sequence $\{u_n\}$) and $d_i > 0$ for $1 \leq i \leq k$. Then, u_n can be

2010 *Mathematics Subject Classification.* 11B37, 11C08, 11G50, 11J86.

Key words and phrases. Linear recurrence sequence, the Skolem Problem, height, linear form in logarithms.

ACCEPTED MANUSCRIPT

expressed as

$$u_n = \sum_{i=1}^{k} f_i(n)\alpha_i^n, \tag{1.2}$$

where f_i is some polynomial of degree at most $d_i - 1$ ($i = 1, 2, \ldots, k$). We call the sequence $\{u_n\}$ *simple* if $k = m$ (that is $d_1 = \cdots = d_m = 1$) and *non-degenerate* if α_i/α_j is not a root of unity for any $i \neq j$ with $1 \le i, j \le k$. It is well-known that if $\{u_n\}$ is non-degenerate, then there are only finitely many integers n such that $u_n = 0$. In fact, it has been shown in [6] that almost all integer polynomials are non-degenerate.

The celebrated Skolem-Mahler-Lech Theorem asserts that the *zero set* $\{n : u_n = 0\}$ is the union of a finite set and finitely many arithmetic progressions (for instance, see [10, Theorem 2.1]). However, all of its existing proofs are in a non-constructive manner. Berstel and Mignotte [1] showed how to obtain all the arithmetic progressions effectively mentioned in the theorem. So, it remains to decide the finite part of the zero set, where one must decide whether the finite part is empty or not. The *Skolem Problem*, posed in 1930s, asks whether it is algorithmically decidable that there exists some n such that $u_n = 0$.

There are only few results towards the decidability of the Skolem Problem. For such sequences of order 1 and 2, this problem is relatively straightforward. Decidability for LRS over $\bar{\mathbb{Q}}$ of orders 3 and 4 is independently settled positively by Mignotte, Shorey and Tijdeman [18], as well as Vereshchagin [21]. More recently, the decidability of the Skolem Problem for integer LRS of order 5 was claimed in [11], and the decidability for rational LRS of any order was claimed in [13], but as pointed out in [19], both are incorrect. The Skolem Problem is also listed as an open problem and discussed by Tao [20, Section 1.9]; see also [19] for a survey. To taste the difficulty of the problem, we want to point out that Blondel and Portier [2, Corollary 2.1] showed that it is NP-hard to decide whether a given integer LRS has a zero.

Most recently, when the order of $\{u_n\}$ is 2, 3, or 4, Chonev, Ouaknine and Worrell [5, Theorem 2.1] gave an effective (not explicit) lower bound N, which roughly is a polynomial function of its coefficients and initial terms, such that $u_n \neq 0$ for any $n > N$; see also [4, Theorem 19] for a more clear version.

In this paper, we want to obtain an explicit version for such an upper bound N when the sequence $\{u_n\}$ is simple and it has either a dominant characteristic root or exactly two characteristic roots of maximal modulus (but we don't restrict its order). This can be viewed as an explicit version of partial results in [18, Corollary 1]. It turns

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

out that this case covers almost all LRS of algebraic numbers whose coefficients are rational numbers.

1.2. **Main results.** We now present the main results and discuss briefly their proofs and coverage.

For any polynomial $f(X) \in \bar{\mathbb{Q}}[X]$ of degree m, let δ_f be the smallest positive integer such that all the coefficients of the polynomial $\delta_f f(X)$ are algebraic integers. Denote $\delta_f f(X)$ by $f^*(X)$ and write

$$f^*(X) = \sum_{i=0}^{m} a_i^* X^i. \tag{1.3}$$

Theorem 1.1. *Let $\{u_n\}$ be a simple LRS of algebraic numbers defined by (1.1) of order $m \geq 2$, and let $f(X)$ be its characteristic polynomial. Suppose that $f(X)$ has a dominant root. Let d be the degree of the Galois closure of the field $\mathbb{Q}(a_0, a_1, \ldots, a_{m-1})$ over $\mathbb{Q}$, and let D be the degree of the number field generated by $u_0, \ldots, u_{m-1}$ over $\mathbb{Q}$. Let $f^*(X) = \sum_{i=0}^{m} a_i^* X^i$ be defined as in (1.3), and let*

$$I(f^*) = 2^{dm}(m+1)^{d/2} \prod_{i=0}^{m} \exp(d\mathrm{h}(a_i^*))$$

and

$$J(f^*) = 2^{dm(dm-1)/4}(dm+1)^{-d^3m^3/4+3dm/4-7} I(f^*)^{-d^3m^3/2+d^2m^2+dm/2-11}.$$

Denote

$$B(u) = m! \cdot dD\Big(\sum_{i=0}^{m-1} \mathrm{h}(u_i) + 3dm^2 \sum_{i=0}^{m} \mathrm{h}(a_i^*) + 3dm^2 \log(m+1)\Big).$$

Then, if $n > N_1(u)$, we have $u_n \neq 0$, where

$$N_1(u) = (2B(u) + \log m)(1 + H(f))J(f^*)^{-1}.$$

If furthermore f is a real polynomial, then in the lower bound $N_1(u)$, $J(f^*)$ can be replaced by

$$2^{-dm(dm-1)(dm-2)/2}(dm+1)^{-dm(dm-1)-1/2} I(f^*)^{-2dm(dm-1)-1}.$$

For the lower bound $N_1(u)$ in Theorem 1.1, if we fix f (that is, fixing the coefficients $a_0, a_1, \ldots, a_{m-1}$), then we have

$$N_1(u) \ll_f D\Big(\sum_{i=0}^{m-1} \mathrm{h}(u_i) + 1\Big).$$

Here, we use the Vinogradov symbol $\ll$. Recall that the assertion $U \ll V$ is equivalent to the inequality $|U| \leq cV$ with some absolute

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

constant $c > 0$. To emphasise the dependence of the implied constant c on some parameter ρ, we write $U \ll_\rho V$.

Theorem 1.2. *Let $\{u_n\}, f, f^*, d, D, I(f^*), J(f^*), B(u)$ be defined as in Theorem 1.1. Suppose that f has exactly two roots of maximal modulus, and moreover their quotient is not a root of unity. Denote*

$$C(u) = 2^{39}(m! \cdot dD)^2\pi(2B(u) + \pi)(2\log I(f^*) + \pi)\log(m! \cdot edD).$$

Then, if $n > N_2(u)$, we have $u_n \neq 0$, where

$$N_2(u) = 4C(u)I(f^*)J(f^*)^{-1}\log\left(2C(u)I(f^*)J(f^*)^{-1}\right).$$

For the lower bound $N_2(u)$ in Theorem 1.1, fixing f, we have

$$N_2(u) \ll_f D^3(\log(D+1))^2\Big(\sum_{i=0}^{m-1} \mathrm{h}(u_i) + 1\Big)\log\Big(\sum_{i=0}^{m-1} \mathrm{h}(u_i) + 2\Big).$$

We will prove Theorems 1.1 and 1.2 in Sections 3 and 4 respectively after making some preparations in Section 2. The approach of the proofs is straightforward. For any simple LRS $\{u_n\}$ of order m, as in (1.2) we can write $u_n = \sum_{j=1}^m b_j\alpha_j^n$, then we try to find a lower bound for the index beyond which the absolute value of the part of the summation related to the roots of maximal modulus is greater than the absolute value of the rest of the summation. For this, we need to obtain lower bounds on separating the absolute values $|\alpha_1|, \ldots, |\alpha_m|$, and estimate the sizes of the coefficients $b_1, \ldots, b_m$. Especially, when there are two characteristic roots of maximal modulus, we need to employ Matveev's bound on linear forms in logarithms.

Finally, we say something about the coverage of the main results.

By [7, Theorem 1.1], almost all monic integer polynomials in $\mathbb{Z}[X]$ have a dominant root. In other words, Theorem 1.1 covers almost all the linear recurrence sequences of algebraic numbers whose coefficents are rational integers.

Besides, by [6, Theorem 4] and [8, Theorem 1.1], almost all integer polynomials in $\mathbb{Z}[X]$ (not necessarily monic) are non-degenerate and have either a dominant root or exactly two roots of maximal modulus. Note that each monic polynomials in $\mathbb{Q}[X]$ can become an integer polynomial by multipling some positive integer. So, we can say that Theorem 1.1 and Theorem 1.2 cover almost all the linear recurrence sequences of algebraic numbers whose coefficents are rational numbers.

2. Preliminaries

2.1. **Height and Mahler measure.** Given a polynomial

$$f(X) = a_mX^m + a_{m-1}X^{m-1} + \cdots + a_0 = a_m(X - \alpha_1)\cdots(X - \alpha_m) \in \mathbb{C}[X]$$

ACCEPTED MANUSCRIPT

of degree $m \geq 1$, we assume that the roots $\alpha_1, \ldots, \alpha_m$ (listed with multiplicities) are labelled so that $|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_m|$. In case $|\alpha_1| = \cdots = |\alpha_r| > |\alpha_{r+1}|$, we say that f *has exactly* r *roots of maximal modulus*. If $r = 1$, we say that f has a *dominant root* (that is, α_1). Clearly, the dominant root is a real number if f is a real polynomial.

For the polynomial f, its *length* is defined by

$$L(f) = |a_0| + \cdots + |a_m|,$$

its *height* by

$$H(f) = \max_{0 \leq i \leq m} |a_i|,$$

and its *Mahler measure* by

$$M(f) = |a_m| \prod_{i=1}^{m} \max\{1, |\alpha_i|\}.$$

These quantities are related by the following inequality

$$H(f)2^{-m} \leq M(f) \leq H(f)\sqrt{m+1}, \tag{2.1}$$

for instance, see [22, (3.12)]. If furthermore $f \in \mathbb{Z}[X]$ is square-free, then for any two distinct roots α, β of f, Mahler's inequality [14] asserts that

$$|\alpha - \beta| > \sqrt{3}m^{-m/2-1}M(f)^{-m+1}. \tag{2.2}$$

Given another polynomial $g \in \mathbb{C}[X]$, by definition we have

$$M(fg) = M(f)M(g).$$

Accordingly, for a non-zero algebraic number α, its *Mahler measure* $M(\alpha)$ is defined as the Mahler measure of its minimal polynomial f over the integers $\mathbb{Z}$, that is, $M(\alpha) = M(f)$.

For a number field K, we denote by M_K the set of all valuations v of K extending the standard infinite and p-adic valuations of the rational numbers $\mathbb{Q}$: $|2|_v = 2$ if $v \in M_K$ is Archimedean, and $|p|_v = p^{-1}$ if v extends the p-adic valuation of $\mathbb{Q}$. In particular, if the valuation v of K corresponds to a prime ideal $\mathfrak{p}$ of K lying above a prime number p, we also denote the valuation $|\ |_v$ by $|\ |_{\mathfrak{p}}$, then for any $\alpha \in K$ we have

$$|\alpha|_{\mathfrak{p}} = p^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)/e_{\mathfrak{p}}},$$

where $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ is the exponent of $\mathfrak{p}$ appearing in the prime decomposition of the fractional ideal $\alpha\mathcal{O}_K$, $\mathcal{O}_K$ is the ring of integers of K, and $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over p. For any $v \in M_K$, let K_v be the completion of K with respect to the valuation v, and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of v. When the valuation v corresponds to a prime

ACCEPTED MANUSCRIPT

ideal $\mathfrak{p}$ lying above a prime number p, we also denote K_v by $K_{\mathfrak{p}}$ and $\mathbb{Q}_v$ by $\mathbb{Q}_p$, respectively.

For the above number field K, the *(Weil) absolute logarithmic height* of any non-zero $\alpha \in K$ is defined by

$$\mathrm{h}(\alpha) = d^{-1} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\}. \tag{2.3}$$

Actually, we have

$$\mathrm{h}(\alpha) = d^{-1} \log M(\alpha); \tag{2.4}$$

see [22, Lemma 3.10].

Given non-zero $\alpha \in K$, in view of (2.3) and $\mathrm{h}(\alpha) = \mathrm{h}(\alpha^{-1})$, for any valuation $v \in M_K$ we have

$$|\log |\alpha|_v| \le d\mathrm{h}(\alpha)/d_v \le d\mathrm{h}(\alpha). \tag{2.5}$$

In the sequel, we use the following formulas without special reference (see, e.g., [22]). For any $n \in \mathbb{Z}$ and $\beta_1, \cdots, \beta_k, \gamma \in \bar{\mathbb{Q}}$, we have

$$\begin{aligned}
&\mathrm{h}(\beta_1 + \cdots + \beta_k) \le \mathrm{h}(\beta_1) + \cdots + \mathrm{h}(\beta_k) + \log k,\\
&\mathrm{h}(\beta_1 \cdots \beta_k) \le \mathrm{h}(\beta_1) + \cdots + \mathrm{h}(\beta_k),\\
&\mathrm{h}(\gamma^n) = |n|\mathrm{h}(\gamma),\\
&\mathrm{h}(|\gamma|) \le \mathrm{h}(\gamma),\\
&\mathrm{h}(\zeta) = 0 \quad \text{for any root of unity } \zeta \in \bar{\mathbb{Q}}.
\end{aligned}$$

We also need the following result, which is exactly [22, Lemma 3.7].

Lemma 2.1. *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ be a non-zero polynomial in n variables. Then, for any algebraic numbers $\gamma_1, \ldots, \gamma_n$, we have*

$$\mathrm{h}(f(\gamma_1, \ldots, \gamma_n)) \le \log L(f) + \sum_{i=1}^{n} \mathrm{h}(\gamma_i) \deg_{X_i} f,$$

where $\deg_{X_i} f$ is the partial degree of f with respect to X_i.

2.2. **Absolute root separation.** Mahler has given a celebrated result in [14] on separating distinct roots of a polynomial in $\mathbb{Z}[X]$. For our purpose, we need a result on separating the absolute values of the roots of a polynomial with coefficients as algebraic integers.

The following lemma is a classical result due to Cauchy; see [17, Proposition 2.5.9].

Lemma 2.2. *Let $f(X) \in \mathbb{C}[X]$ be a polynomial of degree $m \ge 1$ defined by*

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0,$$

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

where $a_0 \neq 0$ and $(a_1, \dots, a_m) \neq (0, \dots, 0)$. Then, for any root z of f, we have

$$|z| < 1 + \frac{1}{|a_m|} \max\{|a_0|, \dots, |a_{m-1}|\}.$$

We reproduce [7, Lemma 2.4 and Lemma 2.5] as follows.

Lemma 2.3. *Let $f(X) \in \mathbb{Z}[X]$ be a quadratic polynomial. Suppose that f has two real roots α and β with $|\alpha| \neq |\beta|$. Then, we have*

$$||\alpha| - |\beta|| \geq H(f)^{-1}.$$

Lemma 2.4. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $m \geq 2$, and let α and β be two roots of f satisfying $|\alpha| \neq |\beta|$. Then,*

$$||\alpha| - |\beta|| > 2^{m(m-1)/4}(m+1)^{-m^3/4+3m/4-3}H(f)^{-m^3/2+m^2+m/2-2} \tag{2.6}$$

if both α and β are non-real. If, furthermore, α is real and β is non-real, then

$$||\alpha| - |\beta|| \geq 2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2}H(f)^{-2m(m-1)-1}. \tag{2.7}$$

Finally, if both α and β are real, then

$$||\alpha| - |\beta|| > (2m+1)^{-3m}H(f)^{2-4m}. \tag{2.8}$$

We remark that there is an improvement upon (2.8) in [3] for real roots under some further conditions. Note that for large enough m, (2.8) is better than (2.7), and (2.7) is better than (2.6). However, for small integer m, this might be not true. For simplicity, we put them together into two uniform forms.

Lemma 2.5. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $m \geq 2$, and let α and β be two roots of f satisfying $|\alpha| \neq |\beta|$. Then,*

$$||\alpha| - |\beta|| > 2^{m(m-1)/4}(m+1)^{-m^3/4+3m/4-7}H(f)^{-m^3/2+m^2+m/2-11}; \tag{2.9}$$

if furthermore α is real, then

$$||\alpha| - |\beta|| \geq 2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2}H(f)^{-2m(m-1)-1}. \tag{2.10}$$

Proof. By Lemma 2.3, we can assume that $m \geq 3$. We first prove (2.10). Notice that the inequality (2.10) is the same as (2.7). For any $m \geq 4$, we have

$$2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2} < 2^{-3m}(m+1)^{-3m} < (2m+1)^{-3m}$$

and $-2m(m-1)-1 < 2-4m$, and so (2.8) is included in (2.10) when $m \geq 4$. We now consider $m = 3$ individually. Assume that f has two

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

real roots α and β such that $|\alpha| \neq |\beta|$. Then, its third root, say γ, is also real. If $\gamma \neq \pm\alpha$ and $\gamma \neq \pm\beta$, then by [3, Theorem 1] we have

$$||\alpha| - |\beta|| \geq 2^{-5.5} H(f)^{-2},$$

which is certainly included in (2.10) by setting $m = 3$. Now, if $\gamma = \pm\alpha$ or $\gamma = \pm\beta$, then the polynomial $f(X)f(-X)$ has a multiple root (α or β). Let $g(X)$ be the squarefree part of $f(X)f(-X)$. Then, we have $\deg g \leq 5$. Note that $\pm\alpha$ and $\pm\beta$ are real roots of g. So, the value $||\alpha| - |\beta||$ is in fact equal to the absolute value of the difference of two distinct roots of g. Thus, applying (2.1) and (2.2) to g, we obtain

$$||\alpha|-|\beta|| > \sqrt{3}\cdot 5^{-3.5} M(g)^{-4} \geq \sqrt{3}\cdot 5^{-3.5} M(f)^{-8} \geq \sqrt{3}\cdot 5^{-3.5}\cdot 2^{-8} H(f)^{-8},$$

which is also included in (2.10) by setting $m = 3$. This completes the proof of (2.10).

Now, we want to prove (2.9). By (2.10), we only need to prove that both (2.6) and (2.7) are included in (2.9). Note that (2.6) is automatically contained in (2.9). It remains to show that (2.7) is included in (2.9). First, for $m = 3, 4$ or 5, by direct computation we have

$$-m^3/2 + m^2 + m/2 - 11 \leq -2m(m-1) - 1,$$

and for $m \geq 6$, we obtain

$$-m^3/2 + m^2 + m/2 - 11 \leq -2m^2 + m/2 - 11 < -2m(m-1) - 1,$$

and thus, for any $m \geq 3$ we have

$$H(f)^{-m^3/2+m^2+m/2-11} \leq H(f)^{-2m(m-1)-1}. \tag{2.11}$$

On the other hand, for $m = 3, 4, 5$ or 6, by direct computation we have

$$2^{m(m-1)/4}(m+1)^{-m^3/4+3m/4-7} < 2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2},$$

and for any $m \geq 7$, it is easy to see that

$$2^{m(m-1)/4}(m+1)^{-m^3/4+3m/4-7} \leq 2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2}. \tag{2.12}$$

Indeed, to obtain (2.12) it is equivalent to show

$$2^{m(m-1)(m-2)/2+m(m-1)/4} \leq (m+1)^{m^3/4-3m/4-m(m-1)+13/2},$$

which follows from (note that $m \geq 7$)

$$\begin{aligned} 2^{m(m-1)(m-2)/2+m(m-1)/4} &\leq (m+1)^{m(m-1)(m-2)/6+m(m-1)/12} \\ &< (m+1)^{m^3/4-3m/4-m(m-1)+13/2}. \end{aligned}$$

So, for any $m \geq 3$, we obtain

$$2^{m(m-1)/4}(m+1)^{-m^3/4+3m/4-7} \leq 2^{-m(m-1)(m-2)/2}(m+1)^{-m(m-1)-1/2}. \tag{2.13}$$

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

Hence, combining (2.11) with (2.13), we deduce that (2.7) is included in (2.9). This completes the proof of (2.9). □

Moreover, we can extend the above lemma to polynomials whose coefficients are algebraic integers. For this, we need a simple preparation.

Lemma 2.6. *Let $f(X) = a_m X^m + \cdots + a_1 X + a_0$ be a polynomial of degree $m \geq 2$, where all the coefficients are algebraic integers. Let K be a Galois extension over $\mathbb{Q}$ containing the field $\mathbb{Q}(a_0, a_1, \ldots, a_m)$. Let $d = [K : \mathbb{Q}]$, and let G be the Galois group of K over $\mathbb{Q}$. Then, we have*

$$M(\prod_{\sigma \in G} \sigma(f)) \leq (m+1)^{d/2} \prod_{i=0}^{m} \exp(d\mathrm{h}(a_i)),$$

and

$$H(\prod_{\sigma \in G} \sigma(f)) \leq 2^{dm} (m+1)^{d/2} \prod_{i=0}^{m} \exp(d\mathrm{h}(a_i)).$$

Proof. For each $0 \leq i \leq m$, let d_i be the degree of a_i over $\mathbb{Q}$. Using (2.1), we have

$$\begin{aligned} M(\prod_{\sigma \in G} \sigma(f)) = \prod_{\sigma \in G} M(\sigma(f)) &\leq \prod_{\sigma \in G} \sqrt{m+1} H(\sigma(f)) \\ &= (m+1)^{d/2} \prod_{\sigma \in G} \max_{0 \leq i \leq m} |\sigma(a_i)| \\ &\leq (m+1)^{d/2} \prod_{i=0}^{m} M(a_i)^{d/d_i} \\ &= (m+1)^{d/2} \prod_{i=0}^{m} \exp(d\mathrm{h}(a_i)), \end{aligned}$$

where we also use the assumption that the coefficients $a_0, a_1, \ldots, a_m$ are algebraic integers. This completes the proof of the first inequality. The second inequality follows from the first one and (2.1). □

Now, we are ready to extend Lemma 2.5.

Lemma 2.7. *Let $f(X) = a_m X^m + \cdots + a_1 X + a_0$ be a polynomial of degree $m \geq 2$, where all the coefficients are algebraic integers. Let d be the degree of the Galois closure of the field $\mathbb{Q}(a_0, a_1, \ldots, a_m)$ over $\mathbb{Q}$. Denote*

$$I(f) = 2^{dm} (m+1)^{d/2} \prod_{i=0}^{m} \exp(d\mathrm{h}(a_i)).$$

ACCEPTED MANUSCRIPT

If α and β are two roots of f satisfying $|\alpha| \ne |\beta|$, then
(2.14)
$$||\alpha| - |\beta|| > 2^{dm(dm-1)/4}(dm+1)^{-d^3m^3/4+3dm/4-7}I(f)^{-d^3m^3/2+d^2m^2+dm/2-11};$$

if furthermore α is real, then
(2.15)
$$||\alpha| - |\beta|| \ge 2^{-dm(dm-1)(dm-2)/2}(dm+1)^{-dm(dm-1)-1/2}I(f)^{-2dm(dm-1)-1}.$$

Proof. Let K be the Galois closure of the number field $\mathbb{Q}(a_0, a_1, \dots, a_m)$ over $\mathbb{Q}$, and let G be the Galois group of K over $\mathbb{Q}$. By assumption, the polynomial $g = \prod_{\sigma \in G} \sigma(f)$ is a polynomial in $\mathbb{Z}[X]$. Clearly, $\deg g = dm$, because $|G| = d$. By Lemma 2.6, we have $H(g) \le I(f)$. Then, since α and β are also two roots of g, applying Lemma 2.5 to g we obtain the desired results. □

We remark that in Lemma 2.7, if the degree of each coefficient a_i over $\mathbb{Q}$ is d_i, $i = 0, 1, \dots, m$, then we have $d \le \prod_{i=0}^{m} d_i!$.

2.3. **Bounding coefficients.** For further deductions, we need to estimate the coefficients in (1.2) when the sequence $\{u_n\}$ is a simple LRS of algebraic numbers.

Lemma 2.8. *Let $\{u_n\}$ be a simple LRS of algebraic numbers of order $m \ge 2$ defined by (1.1). Let $f(X)$ be its characteristic polynomial, and define the polynomial $f^*(X)$ as in (1.3). Write u_n as*

$$u_n = \sum_{j=1}^{m} b_j \alpha_j^n,$$

where $\alpha_1, \dots, \alpha_m$ are distinct roots of f and all b_j are non-zero. Then, for any $1 \le j \le m$ we have

$$\mathrm{h}(b_j) < \sum_{i=0}^{m-1} \mathrm{h}(u_i) + 2m \sum_{k \ne j} \mathrm{h}(\alpha_k) + m^2 \mathrm{h}(\alpha_j) + m(2m-3)\log 2 + \log m.$$

Let d be the degree of the Galois closure of the field $\mathbb{Q}(a_0, a_1, \dots, a_{m-1})$ over $\mathbb{Q}$. Then, we have

$$\mathrm{h}(b_j) < \sum_{i=0}^{m-1} \mathrm{h}(u_i) + 3dm^2 \sum_{i=0}^{m} \mathrm{h}(a_i^*) + 3dm^2 \log(m+1).$$

Proof. Here, we follow the arguments in the proof of [9, Theorem 3.1].

ACCEPTED MANUSCRIPT

Notice that

$$(u_0, u_1, \ldots, u_{m-1}) = (b_1, b_2, \ldots, b_m) \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{m-1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha_m & \ldots & \alpha_m^{m-1} \end{pmatrix}, \tag{2.16}$$

and $\alpha_1, \ldots, \alpha_m$ are distinct. To solve the above system of m linear equations in m unknowns $b_1, \ldots, b_m$, we denote the appearing Vandermonde matrix by $V = \big(\alpha_i^{j-1}\big)_{1\le i,j\le m}$. By [12, Formula (6)], the inverse of V is given by $V^{-1} = \big(w_{ij}\big)_{1\le i,j\le m}$, where

$$w_{ij} = \frac{(-1)^{i+j}\sigma_{m-i}(\alpha_1, \ldots, \widehat{\alpha}_j, \ldots, \alpha_m)}{\prod\limits_{l=1}^{j-1}(\alpha_j - \alpha_l) \prod\limits_{k=j+1}^{m}(\alpha_k - \alpha_j)}$$

and $\sigma_k(\alpha_1, \ldots, \widehat{\alpha}_j, \ldots, \alpha_m)$ stands for the k-th elementary symmetric function in the $m-1$ variables $\alpha_1, \ldots, \alpha_m$ without α_j; for instance, in the case $j = m$, we have $\sigma_1(\alpha_1, \ldots, \alpha_{m-1}) = \alpha_1 + \cdots + \alpha_{m-1}$ and $\sigma_{m-1}(\alpha_1, \ldots, \alpha_{m-1}) = \alpha_1 \cdots \alpha_{m-1}$.

So, for any j with $1 \le j \le m$ we have

$$b_j = \sum_{i=1}^{m} u_{i-1} w_{ij}.$$

Since $\sigma_{m-i}(\alpha_1, \ldots, \widehat{\alpha}_j, \ldots, \alpha_m)$ is a polynomial with coefficients 1 in $m-1$ variables $\alpha_1, \ldots, \alpha_m$ (without α_j) of degree $m-i$, length $\binom{m-1}{m-i}$, and degree 1 in each variable α_k, $k \ne j$, by Lemma 2.1 we find that

$$\mathrm{h}(\sigma_{m-i}(\alpha_1, \ldots, \widehat{\alpha}_j, \ldots, \alpha_m)) \le \log\binom{m-1}{m-i} + \sum_{k\ne j}\mathrm{h}(\alpha_k).$$

On the other hand, we observe that

$$\begin{aligned} \mathrm{h}\Big(\prod_{k\ne j}(\alpha_k - \alpha_j)\Big) &\le \sum_{k\ne j}\mathrm{h}(\alpha_k - \alpha_j) \\ &\le \sum_{k\ne j}\big(\mathrm{h}(\alpha_k) + \mathrm{h}(\alpha_j) + \log 2\big) \\ &= \sum_{k\ne j}\mathrm{h}(\alpha_k) + (m-1)\mathrm{h}(\alpha_j) + (m-1)\log 2. \end{aligned}$$

Thus, we obtain

$$\mathrm{h}(w_{ij}) \le 2\sum_{k\ne j}\mathrm{h}(\alpha_k) + (m-1)\mathrm{h}(\alpha_j) + (m-1)\log 2 + \log\binom{m-1}{m-i}.$$

ACCEPTED MANUSCRIPT

Hence, for $1 \le j \le m$ we conclude that

$$\begin{aligned} \mathrm{h}(b_j) &\le \sum_{i=1}^{m} (\mathrm{h}(u_{i-1}) + \mathrm{h}(w_{ij})) + \log m \\ &\le \sum_{i=0}^{m-1} \mathrm{h}(u_i) + 2m \sum_{k \ne j} \mathrm{h}(\alpha_k) + m(m-1)\mathrm{h}(\alpha_j) \\ &\qquad + m(2m-3)\log 2 + \log m, \end{aligned} \tag{2.17}$$

where we also use the fact that the binomial coefficient $\binom{m-1}{m-i} \le 2^{m-2}$ for any $1 \le i \le m$. This gives the first desired upper bound.

Now, we need to estimate $\mathrm{h}(\alpha_i)$ for each $1 \le i \le m$. By definition and using (2.4) and Lemma 2.6, we obtain

$$\begin{aligned} \mathrm{h}(\alpha_i) \le \log M(\alpha_i) &\le \log M\Big(\prod_{\sigma \in G} \sigma(f^*)\Big) \\ &\le d \sum_{i=0}^{m} \mathrm{h}(a_i^*) + \frac{d}{2}\log(m+1). \end{aligned} \tag{2.18}$$

Finally, combining (2.17) with (2.18) we have

$$\mathrm{h}(b_j) < \sum_{i=0}^{m-1} \mathrm{h}(u_i) + 3dm^2 \sum_{i=0}^{m} \mathrm{h}(a_i^*) + 3dm^2 \log(m+1).$$

This completes the proof. □

2.4. **Linear form in the logarithms of algebraic numbers.** One key technical tool in this paper is Baker's inequality on linear form in the logarithms of algebraic numbers. Here we restate one of its explicit forms due to Matveev [15, Corollary 2.3].

First, recall that for a non-zero complex number z, the principal value of the natural logarithm of z is

$$\log z = \log|z| + \sqrt{-1} \cdot \mathrm{Arg}\, z,$$

where $\mathrm{Arg}\, z$ is the principal value of the argument of z ($-\pi < \mathrm{Arg}\, z \le \pi$). Note that the definition here coincides with the natural logarithm of positive real numbers. We also want to indicate that the identity $\log(z_1 z_2) = \log z_1 + \log z_2$ can fail in our setting.

Let

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_k \log \alpha_k,$$

where $k \ge 2$, $b_1, \ldots, b_k \in \mathbb{Z}$, and $\alpha_1, \ldots, \alpha_k$ are non-zero elements of a number field K. Let $D = [K : \mathbb{Q}]$ and $B = \max\{|b_1|, \ldots, |b_k|\}$. For

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

any $1 \le j \le k$, choose a real number A_j such that

$$A_j \ge \max\{D\mathrm{h}(\alpha_j), |\log \alpha_j|, 0.16\}.$$

Suppose that $\Lambda \ne 0$. Then, we have

$$\log |\Lambda| > -2^{6k+20} D^2 A_1 \cdots A_k \log(eD) \log(eB), \tag{2.19}$$

where e is the base of the natural logarithm.

We remark that we in fact only need a lower bound on linear forms in three logarithms. However, all the existing lower bounds on linear forms in three logarithms are under some extra conditions, which do not always hold in our case (see, for instance, the best known estimate [16, Theorem 2]).

3. Proof of Theorem 1.1

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of f such that $|\alpha_1| > |\alpha_j|$ for any $2 \le j \le m$. Note that they are all distinct and also the roots of f^*.

Then, by (2.14) and the definition of $J(f^*)$, for any $2 \le j \le m$ we have

$$|\alpha_1| - |\alpha_j| > J(f^*). \tag{3.1}$$

As mentioned before, for any integer $n \ge 0$, u_n can be expressed as

$$u_n = \sum_{j=1}^{m} b_j \alpha_j^n,$$

where $b_1, \ldots, b_m$ are all non-zero complex numbers. Now, we want to find a lower bound beyond which the index n satisfies

$$|b_1 \alpha_1^n| > \sum_{j=2}^{m} |b_j \alpha_j^n|. \tag{3.2}$$

Then, $u_n \ne 0$ when the index n is greater than this lower bound. This will complete the proof. Note that it is equivalent to require that

$$|b_1| > \sum_{j=2}^{m} |b_j| \left(|\alpha_j|/|\alpha_1|\right)^n,$$

which, by (3.1), is implied in the inequality

$$|b_1| > \left(1 - J(f^*)/|\alpha_1|\right)^n \sum_{j=2}^{m} |b_j|. \tag{3.3}$$

On the other hand, for any $1 \le j \le m$, by (2.5) we know that

$$|\log |b_j|| \le [\mathbb{Q}(b_j) : \mathbb{Q}]\mathrm{h}(b_j).$$

ACCEPTED MANUSCRIPT

Since $b_j \in \mathbb{Q}(u_0, \ldots, u_{m-1}, \alpha_1, \ldots, \alpha_m)$ by (2.16), we have $[\mathbb{Q}(b_j) : \mathbb{Q}] \le m! \cdot dD$. So

$$|\log |b_j|| \le m! \cdot dD\mathrm{h}(b_j).$$

Using Lemma 2.8 and by the definition of $B(u)$, we get

$$|\log |b_j|| \le B(u),$$

that is

$$\exp(-B(u)) \le |b_j| \le \exp(B(u)) \tag{3.4}$$

for any $1 \le j \le m$.

Thus, by (3.4), the inequality (3.3) is implied in the following inequality

$$\exp(-B(u)) > m \exp(B(u)) \left(1 - J(f^*)/|\alpha_1|\right)^n,$$

which is equivalent to

$$n > \frac{2B(u) + \log m}{-\log(1 - J(f^*)/|\alpha_1|)}.$$

By Lemma 2.2, we have $|\alpha_1| < 1 + H(f)$. So, it suffices to ensure that

$$n > \frac{2B(u) + \log m}{-\log(1 - J(f^*)/(1 + H(f)))}.$$

Using the Taylor expansion $-\log(1-x) = x + x^2/2 + x^3/3 + \cdots$ for $|x| < 1$, it suffices to require that

$$n > \frac{2B(u) + \log m}{J(f^*)/(1 + H(f))}.$$

Thus, we get the desired lower bound $N_1(u)$ implying the inequality (3.2). This completes the proof of the first part.

Finally, if f is a real polynomial, then its dominant root α_1 is a real root, and so in the inequality (3.1) we use (2.15) instead of (2.14). This in fact gives the second result and completes the proof.

4. Proof of Theorem 1.2

Under the assumptions, we must have $m \ge 3$. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of f such that $|\alpha_1| = |\alpha_2| > |\alpha_j|$ for any $3 \le j \le m$. Note that they are also the roots of f^*. By (2.14) and the definition of $J(f^*)$, for any $3 \le j \le m$ we have

$$|\alpha_1| - |\alpha_j| > J(f^*).$$

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

Note that for any integer $n \geq 0$, u_n can be expressed as

$$u_n = \sum_{j=1}^{m} b_j \alpha_j^n,$$

where $b_1, \ldots, b_m$ are all non-zero complex numbers.

In the sequel, we want to find a lower bound beyond which the index n satisfies

$$|b_1\alpha_1^n + b_2\alpha_2^n| > \sum_{j=2}^{m} |b_j \alpha_j^n|. \tag{4.1}$$

So, whenever the index n is greater than this lower bound, we have $u_n \neq 0$. This will complete the proof.

The key step is to get a lower bound for the left-hand side of (4.1) by using Baker's inequality on linear form (2.19). Then, let the right-hand side of (4.1) be less than the lower bound, this can give the desired lower bound for the index n.

For any $n \geq 0$, we have

$$|b_1\alpha_1^n + b_2\alpha_2^n| = |b_1\alpha_1^n| \cdot \left|(-1) \cdot \frac{b_2}{b_1} \cdot (\frac{\alpha_2}{\alpha_1})^n - 1\right| \tag{4.2}$$

Here, for $n \geq 0$ we put

$$\Delta_n = (-1) \cdot \frac{b_2}{b_1} \cdot (\frac{\alpha_2}{\alpha_1})^n - 1,$$

and

$$\Lambda_n = \log(\Delta_n + 1). \tag{4.3}$$

Then, by definition, there exists an odd integer a such that

$$|a| \leq n + 1$$

and

$$\Lambda_n = a \log(-1) + \log(b_2/b_1) + n \log(\alpha_2/\alpha_1),$$

which gives a linear form in the logarithms of algebraic numbers.

In the following, we assume that

$$|\Delta_n| \leq 1/2. \tag{4.4}$$

If this is not true, then later on one can see that this implies much better results; see (4.13).

ACCEPTED MANUSCRIPT

Notice that for any complex number z with $0 < |z| \le r < 1$, using the Taylor expansion, we have

$$\begin{aligned} |\log(1+z)| &= |z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots | \\ &\le (1 + \frac{r}{2} + \frac{r^2}{3} + \cdots)|z| = \frac{|\log(1-r)|}{r}|z|. \end{aligned}$$

Using this estimate together with (4.3) and (4.4), we obtain

$$\frac{1}{2}|\Lambda_n| = \frac{1}{2}|\log(\Delta_n + 1)| < |\Delta_n|. \tag{4.5}$$

We first handle the exceptional case when $\Lambda_n = 0$. Suppose that $\Lambda_n = 0$. Then $\Delta_n = 0$, that is $b_1\alpha_1^n + b_2\alpha_2^n = 0$. Let

$$K = \mathbb{Q}(u_0, \ldots, u_{m-1}, \alpha_1, \ldots, \alpha_m).$$

Then, $[K:\mathbb{Q}] \le m! \cdot dD$. If α_1/α_2 is not a unit of K, then there exists a prime ideal $\mathfrak{p}$ in the ring of integers of K such that $\mathrm{ord}_{\mathfrak{p}}(\alpha_1/\alpha_2)$ is non-zero. Then, we get

$$n \le n|\mathrm{ord}_{\mathfrak{p}}(\alpha_1/\alpha_2)| = |\mathrm{ord}_{\mathfrak{p}}(b_2/b_1)| \le |\mathrm{ord}_{\mathfrak{p}}(b_1)| + |\mathrm{ord}_{\mathfrak{p}}(b_2)|. \tag{4.6}$$

On the other hand, by definition, for any $1 \le j \le m$, we know that

$$|b_j|_{\mathfrak{p}} = p^{-\mathrm{ord}_{\mathfrak{p}}(b_j)/e_{\mathfrak{p}}},$$

where p is the underlying prime number of $\mathfrak{p}$, and $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over p. Noticing $b_j \in K$ and using (2.5), we obtain

$$|\log|b_j|_{\mathfrak{p}}| \le \frac{[K:\mathbb{Q}]}{d_{\mathfrak{p}}}\mathrm{h}(b_j),$$

where $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$. Notice that $e_{\mathfrak{p}} \le d_{\mathfrak{p}}$. So, for any $1 \le j \le m$ we have

$$|\mathrm{ord}_{\mathfrak{p}}(b_j)| \le \frac{e_{\mathfrak{p}}[K:\mathbb{Q}]}{d_{\mathfrak{p}}\log p}\mathrm{h}(b_j) \le \frac{[K:\mathbb{Q}]}{\log p}\mathrm{h}(b_j) \le 2B(u), \tag{4.7}$$

where $B(u)$ has been defined in Theorem 1.1. Combining (4.6) with (4.7), we get

$$n \le 4B(u). \tag{4.8}$$

Now, we suppose that $\Lambda_n = 0$ and α_1/α_2 is a unit of K. Since α_1/α_2 is not a root of unity, there exists an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that $|\sigma(\alpha_1)/\sigma(\alpha_2)| > 1$. By (2.14) and the definition of $J(f^*)$, we have

$$|\sigma(\alpha_1)| - |\sigma(\alpha_2)| > J(f^*).$$

On the other hand, let G be the Galois group of the Galois closure of the field $\mathbb{Q}(a_0, a_1, \ldots, a_{m-1})$. Then, each $\sigma(\alpha_j), j = 1, 2, \ldots, m$, is a

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

root of the polynomial $\prod_{\tau\in G}\tau(f^*)\in\mathbb{Z}[X]$, and so, by Lemma 2.6 and the definition of $I(f^*)$, we obtain

$$|\sigma(\alpha_j)|\le M\Big(\prod_{\tau\in G}\tau(f^*)\Big)\le I(f^*). \tag{4.9}$$

Notice that

$$|\sigma(b_2)/\sigma(b_1)|\le \exp(2B(u)),$$

which can be deduced similarly as (3.4). In view of

$$\sigma(b_1)\sigma(\alpha_1)^n+\sigma(b_2)\sigma(\alpha_2)^n=0,$$

we deduce that

$$|\sigma(\alpha_1)/\sigma(\alpha_2)|^n=|\sigma(b_2)/\sigma(b_1)|\le \exp(2B(u)). \tag{4.10}$$

On the other hand, since

$$|\sigma(\alpha_1)/\sigma(\alpha_2)|^n>\big(1+J(f^*)/|\sigma(\alpha_2)|\big)^n\ge(1+J(f^*)/I(f^*))^n,$$

where the last inequality follows from (4.9), we consider the inequality

$$(1+J(f^*)/I(f^*))^n>\exp(2B(u)),$$

which gives

$$n>\frac{2B(u)}{\log(1+J(f^*)/I(f^*))}.$$

Since $\log(1+x)>x-x^2/2>x/2$ for $0<x<1$, it suffices to require that

$$n>4B(u)I(f^*)J(f^*)^{-1}. \tag{4.11}$$

Notice that the lower bound in (4.11) is much larger than the upper bound in (4.8). Thus, if integer n satisfies (4.11), then the inequality in (4.10) is not true, and we must have $\Lambda_n\ne 0$.

Now, we assume that n satisfies (4.11). So, $\Lambda_n\ne 0$. Applying Baker's inequality (2.19) to Λ_n, we find that

$$|\Lambda_n|>\exp\big(-2^{38}D_1^2A_1A_2A_3\log(eD_1)\log(en+e)\big), \tag{4.12}$$

where D_1 is the degree of the number field generated by b_2/b_1 and α_2/α_1 over $\mathbb{Q}$, and

$$\begin{aligned}
&A_1=\pi,\\
&A_2\ge\max\{D_1\mathrm{h}(b_2/b_1),|\log(b_2/b_1)|,0.16\},\\
&A_3\ge\max\{D_1\mathrm{h}(\alpha_2/\alpha_1),|\log(\alpha_2/\alpha_1)|,0.16\}.
\end{aligned}$$

Since both b_2/b_1 and α_2/α_1 are contained in K, we have

$$D_1\le[K:\mathbb{Q}]\le m!\cdot dD.$$

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

By Lemma 2.8 and the definition of $B(u)$, we get

$$D_1 \mathrm{h}(b_2/b_1) \le D_1(\mathrm{h}(b_1) + \mathrm{h}(b_2)) \le 2B(u).$$

In addition, by (2.5) we note that

$$|\log(b_2/b_1)| \le |\log|b_2/b_1|| + \pi \le D_1 \mathrm{h}(b_2/b_1) + \pi \le 2B(u) + \pi.$$

Thus, we choose

$$A_2 = 2B(u) + \pi.$$

Now, we want to choose A_3. Since α_1, α_2 are roots of the polynomial $\prod_{\tau \in G} \tau(f^*) \in \mathbb{Z}[X]$, by (2.4) and Lemma 2.6 we have

$$\mathrm{h}(\alpha_2/\alpha_1) \le \mathrm{h}(\alpha_2) + \mathrm{h}(\alpha_1) \le 2 \log M\Big(\prod_{\tau \in G} \tau(f^*)\Big) \le 2 \log I(f^*).$$

On the other hand, we have

$$|\log(\alpha_2/\alpha_1)| \le |\log|\alpha_2/\alpha_1|| + \pi < 2 \log M\Big(\prod_{\tau \in G} \tau(f^*)\Big) + \pi \le 2 \log I(f^*) + \pi.$$

So, we can choose

$$A_3 = 2 \log I(f^*) + \pi.$$

Then, under (4.11) and recalling the definition of $C(u)$, the inequality (4.12) becomes

$$|\Lambda_n| > \exp(-C(u) \log n),$$

which, together with (4.2) and (4.5), implies that

$$|b_1\alpha_1^n + b_2\alpha_2^n| > \frac{1}{2}|b_1\alpha_1^n| \exp(-C(u) \log n). \tag{4.13}$$

Now, we are ready to find a lower bound for n such that

$$|b_1\alpha_1^n + b_2\alpha_2^n| > \sum_{j=3}^{m} |b_j\alpha_j^n|.$$

This is implied in the following inequality by using (4.13)

$$\frac{1}{2}|b_1\alpha_1^n| \exp(-C(u) \log n) \ge \sum_{j=3}^{m} |b_j\alpha_j^n|.$$

That is, we need that

$$|b_1| \exp(-C(u) \log n) \ge 2 \sum_{j=3}^{m} |b_j| \left(|\alpha_j|/|\alpha_1|\right)^n,$$

which follows from the inequality

$$|b_1| \exp(-C(u) \log n) \ge 2 \sum_{j=3}^{m} |b_j| \left(1 - J(f^*)/|\alpha_1|\right)^n. \tag{4.14}$$

ACCEPTED MANUSCRIPT

By (3.4), the inequality (4.14) is implied in the following inequality

$$\exp(-B(u) - C(u)\log n) \geq 2m \exp(B(u)) \left(1 - J(f^*)/|\alpha_1|\right)^n,$$

which is equivalent to

$$-n\log(1 - J(f^*)/|\alpha_1|) - C(u)\log n \geq 2B(u) + \log(2m).$$

Since $-\log(1-x) = x + x^2/2 + x^3/3 + \cdots$ for $0 < x < 1$ and noticing $|\alpha_1| \leq M\Big(\prod_{\tau \in G} \tau(f^*)\Big) \leq I(f^*)$, it suffices to require that

$$nJ(f^*)/I(f^*) - C(u)\log n \geq 2B(u) + \log(2m). \tag{4.15}$$

Notice that an integer n satisfying the following inequalities also satisfies (4.15),

$$\begin{cases} C(u)\log n \leq nJ(f^*)/(2I(f^*)), \\ \\ nJ(f^*)/(2I(f^*)) \geq 2B(u) + \log(2m). \end{cases} \tag{4.16}$$

Since the function $x/\log x$ is strictly increasing when $x \geq 3$, for $A \geq 3$, if $x \geq 2A\log A$, then $x/\log x \geq A$. Thus, if

$$n \geq 4C(u)I(f^*)J(f^*)^{-1}\log\left(2C(u)I(f^*)J(f^*)^{-1}\right), \tag{4.17}$$

then the first inequality in (4.16) holds, and in fact the second one also holds. Note that the lower bound in (4.17) is much bigger than that in (4.11).

So, if an integer n satisfies the inequality (4.17), then we have

$$|b_1\alpha_1^n + b_2\alpha_2^n| > \sum_{j=3}^{m} |b_j\alpha_j^n|.$$

Thus, $u_n \neq 0$. This completes the proof of the theorem.

Acknowledgements

The author wants to thank Manas Patra and Igor Shparlinski for introducing him into the Skolem Problem and also for useful discussions and helpful comments. The research was supported by the Australian Research Council Grant DP130100237 and also by the Macquarie University Research Fellowship.

References

[1] J. Berstel and M. Mignotte, *Deux propriétés décidables des suites récurrentes linéaires*, Bull. Soc. Math. France, **104** (1976), 175–184.

[2] V.D. Blondel and N. Portier, *The presence of a zero in an integer linear recurrent sequence is NP-hard to decide*, Linear Algebra Appl., **351-352** (2002), 91–98.

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

[3] Y. Bugeaud, A. Dujella, T. Pejković and B. Salvy, *Absolute real root separation*, Amer. Math. Monthly, **124** (2017), 930–936.

[4] V. Chonev, *Reachability problems for linear dynamical systems*, PhD thesis, University of Oxford, 2015.

[5] V. Chonev, J. Ouaknine and J. Worrell, *On the complexity of the orbit problem*, J. ACM, **63**(3):23:1–23:18, 2016.

[6] A. Dubickas and M. Sha, *Counting degenerate polynomials of fixed degree and bounded height*, Monatsh. Math., **177** (2015), 517–537.

[7] A. Dubickas and M. Sha, *Counting and testing dominant polynomials*, Exper. Math., **24** (2015), 312–325.

[8] A. Dubickas and M. Sha, *Positive density of integer polynomials with some prescribed properties*, J. Number Theory, **159** (2016), 27–44.

[9] A. Dubickas, M. Sha and I. Shparlinski, *Explicit form of Cassels' p-adic embedding theorem for number fields*, Can. J. Math., **67** (2015), 1046–1064.

[10] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Amer. Math. Soc., Providence, RI, 2003.

[11] V. Halava, T. Harju, M. Hirvensalo and J. Karhumäki, *Skolem's problem – on the border between decidability and undecidability*, Technical Report 683, Turku Centre for Computer Science, 2005.

[12] A. Klinger, *The Vandermonde matrix*, Amer. Math. Monthly, **74** (1967), 571–574.

[13] B. Litow, *A decision method for the rational sequence problem*, In: Electronic Colloquium on Computational Complexity (ECCC), volume 4, 1997.

[14] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J,. **11** (1964), 257–262.

[15] E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II*, Izv. Math., **64**(6) (2000), 1217–1269.

[16] M. Mignotte, *A kit on linear forms in three logarithms*, available at http://irma.math.unistra.fr/~bugeaud/travaux/kit.pdf.

[17] M. Mignotte and D. Ştefănescu, *Polynomials: an algorithmic approach*, Springer, Singapore, 1999.

[18] M. Mignotte, T.N. Shorey and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math., **349** (1984), 63–76.

[19] J. Ouaknine and J. Worrell, *Decision problems for linear recurrence sequences*, In: Proc. 6th Intern. Workshop on Reachability Problems (RP), LNCS **7550**, pp. 21–28, Springer, 2012.

[20] T. Tao, *Structure and randomness: pages from year one of a mathematical blog*, Amer. Math. Soc., Providence, RI, 2008.

[21] N.K. Vereshchagin, *Occurrence of zero in a linear recursive sequence*, Math. Notes, **38** (1985), 609–615.

[22] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables,* Grundlehren der Mathematischen Wissenschaften **326**, Springer, Berlin, 2000.

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: shamin2010@gmail.com

ACCEPTED MANUSCRIPT