Clemens Fuchs

An upper bound for the G.C.D. of two linear recurring sequences

Mathematica Slovaca, Vol. 53 (2003), No. 1, 21--42

Persistent URL: http://dml.cz/dmlcz/130345

Mathematica Slovaca

Math. Slovaca, **53** (2003), No. 1, 21–42

AN UPPER BOUND FOR THE G.C.D. OF TWO LINEAR RECURRING SEQUENCES

Clemens Fuchs

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Let (G_n) and (H_n) be linear recurring sequences of integers defined by $G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n$ and $H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n$, where $t, s \geq 2$, c_i, d_j are non-zero complex numbers and where G_n does not divide H_n in the ring of power sums. Then, provided $n > C_1$, we have

$$\mathrm{G.C.D.}(G_n, H_n) < |G_n|^c,$$

for all n aside of a finite set of exceptions, whose cardinality can be bounded by C_2, where C_1, C_2 and $c < 1$ are effectively computable numbers depending on the c_i, d_j, α_i and β_j, $i = 1, \dots, t$, $j = 1, \dots, s$. This quantifies a very recent result [Bugeaud, Y.—Corvaja, P.—Zannier, U.: *An upper bound for the* G.C.D. *of* $a^n - 1$ *and* $b^n - 1$, Math. Z. (To appear.)]

1. Introduction

Let $A_1, A_2, \dots, A_k$ and $G_0, G_1, \dots, G_{k-1}$ be integers and let (G_n) be a kth order linear recurring sequence given by

$$G_n = A_1 G_{n-1} + \cdots + A_k G_{n-k} \qquad \text{for} \quad n = k, k+1, \dots. \tag{1}$$

Let $\alpha_1, \alpha_2, \dots, \alpha_t$ be the distinct roots of the corresponding characteristic polynomial

$$X^k - A_1 X^{k-1} - \cdots - A_k. \tag{2}$$

Then for $n \geq 0$

$$G_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{3}$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i; the coefficients of $P_i(n)$ are elements of the field: $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$.

2000 Mathematics Subject Classification: Primary 11D45, 11D61.
Keywords: Subspace Theorem, linear recurring sequences, Diophantine inequalities.

This work was supported by the Austrian Science Foundation FWF, Grant S8307-MAT.

We shall be interested in linear recurring sequences (G_n), where all roots of the characteristic polynomial of (G_n) are pairwisely different, which means that

$$G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n\,, \tag{4}$$

for some $c_i, \alpha_i \in \mathbb{C}$. If we restrict the roots to come from a multiplicative semigroup $A \subset \mathbb{C}$, then we let $\mathcal{E}_A$ denote the ring of complex functions on $\mathbb{N}$ of the form (4) where $\alpha_i \in A$. Below, A will be usually $\mathbb{Z}$; moreover in that case we define by $\mathcal{E}_{\mathbb{Z}}^+$ the subring formed by those functions having only positive roots, i.e. by the semigroup $\mathbb{N}$. Working in this domain causes no loss of generality: this assumption may be achieved by written $n = 2m + r$ and considering the cases $r = 0, 1$ separately.

The recurring sequence (G_n) is called *nondegenerate* if no quotient α_i/α_j for all $1 \le i < j \le t$ is equal to a root of unity.

The arithmetic properties of such recurring sequences have been widely investigated. We may mention the so-called Hadamard Quotient theorem (proved by van der Poorten, cf. [5]), which says that if $(G_n), (H_n) \in \mathcal{E}_{\mathbb{Z}}^+$, then $H_n/G_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$ can only hold if there is a recurring sequence $(I_n) \in \mathcal{E}_{\mathbb{Z}}^+$ such that $H_n = G_n \cdot I_n$ for all $n \in \mathbb{N}$. Roughly speaking this means that the quotient may have values in $\mathbb{Z}$ for all $n \in \mathbb{N}$ only when this is obvious in the sense that it comes from an identical relation.

Corvaja and Zannier showed by using deep tools from Diophantine Approximation a stronger result. They showed that if (G_n), (H_n) are as above and if $H_n/G_n \in \mathbb{Z}$ for infinitely many n, then there exists a recurring sequence (I_n) such that $H_n = G_n \cdot I_n$ for all $n \in \mathbb{N}$. This result can be found in [2].

The above diophantine problems arise of investigating the finiteness of the set of natural numbers n such that H_n/G_n is an integer. Let us mention that in a very recent paper, Corvaja and Zannier solved this question in complete generality (i.e. for arbitrary linear recurrences G_n and H_n; cf. [3]).

Recently, Bugeaud, Corvaja and Zannier [1] proved that the same techniques can be used to obtain more explicit results, bounding the cancellation in the fraction H_n/G_n, which is represented by the G. C. D. of G_n and H_n. In fact they showed that, if a, b are integers ≥ 2, and b is not a power of a, then, provided n is sufficiently large, we have

$$\text{G. C. D.}(a^n-1, b^n-1) \ll a^{\frac{n}{2}}\,. \tag{5}$$

The number $1/2$ in the exponent is best-possible, in view of the example $a = c^2$, $b = c^s$ for odd s.

In the case when a and b are multiplicatively independent, they proved a sharper bound: Let $\varepsilon > 0$. Then, provided n is sufficiently large, we have

$$\text{G. C. D.}(a^n-1, b^n-1) < \exp(\varepsilon n)\,. \tag{6}$$

They remarked that due to the ineffectiveness of Schmidt's Subspace Theorem, which is needed in the proof, the method does not allow to compute an integer $n_0 = n_0(a,b,\varepsilon)$ such that the above inequality holds for $n > n_0$. The aim of the present paper is to remark that one can get at least some information about such an index n_0.

2. Results

We will use a quantitative version of Schmidt's Subspace Theorem, which is, due to Evertse [4], to show that one can calculate an index n_0 such that the above inequalities are true for all $n > n_0$ aside from a finite set of exceptions whose cardinality can also be bounded effectively.

Moreover, we will formulate the result of equation (5) for arbitrary linear recurring sequences in $\mathcal{E}_{\mathbb{Z}}^{+}$ instead of (a^n-1) and (b^n-1) (see also [1; Remark 4]).

THEOREM 1. *Let (G_n) and (H_n) be linear recurring sequences of integers defined by $G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n$ and $H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n$, where $t,s \geq 2$, c_i, d_j are non-zero complex numbers and where $\alpha_1 > \cdots > \alpha_t > 0$, $\beta_1 > \cdots > \beta_s > 0$. Furthermore we assume that G_n does not divide H_n in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$. Then, provided $n > C_1$, we have*

$$\mathrm{G.\,C.\,D.}(G_n, H_n) < |G_n|^c$$

for all n aside of a finite set of exceptions, whose cardinality can be bounded by C_2, where C_1, C_2 and $c < 1$ are effectively computable numbers depending on the c_i, d_j, α_i and β_j, $i = 1,\dots,t$, $j = 1,\dots,s$.

Remark 1. Let us mention that by G. C. D. we denote here the uniquely determined positive greatest common divisor of two integers.

Remark 2. The condition that G_n does not divide H_n in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$ is clearly needed and can be verified explicitly (see [2] and Lemma 3 below). A sufficient, but rather strong condition is that the roots $\alpha_1,\dots,\alpha_t$, $\beta_1,\dots,\beta_s$ are multiplicatively independent.

Remark 3. In fact, c can be chosen arbitrarily within the range

$$\frac{\binom{t+h-1}{h}s}{\binom{t+h-1}{h}s+1} < c < 1\,,$$

where h is an arbitrary integer with

$$h > \max\left\{1,\ \frac{\log\beta_1}{\log\alpha_1 - \log\alpha_2} - 1\right\}$$

and t, s are as in Theorem 1.

In the case $\alpha_2 = 1$, i.e. $t = 2$, which means that we have

$$G_n = c_1\alpha_1^n + c_2,$$

a stronger result on the constant c can be shown.

COROLLARY 1. *Let (G_n) and (H_n) be linear recurring sequences of integers defined by $G_n = c_1\alpha^n + c_2$ and $H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n$, where $s \geq 2$, c_i, d_j are non-zero complex numbers and where $\alpha > 1$, $\beta_1 > \cdots > \beta_s > 0$ and let $\varepsilon > 0$. Furthermore we assume that G_n does not divide H_n in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$. Then, provided $n > C_1$, we have*

$$\mathrm{G.C.D.}(G_n, H_n) < |G_n|^{1-\frac{1}{s}+\varepsilon},$$

for all n aside of a finite set of exceptions, whose cardinality can be bounded by C_2, where C_1, C_2 are effectively computable numbers depending on the c_i, d_j, α, β_j, $i = 1, 2$, $j = 1, \ldots, s$ and ε.

Remark 4. Observe that this result includes the result of Bugeaud, Corvaja and Zannier [1] mentioned in the introduction, who showed that

$$\mathrm{G.C.D.}(a^n-1, b^n-1) < (a^n - 1)^{\frac{1}{2}+\varepsilon}, \tag{7}$$

provided that b is not a power of a, which is equivalent to the assumption that $a^n - 1$ does not divide $b^n - 1$ in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$ (which is just an elementary algebraic fact), and n is sufficiently large.

Remark 5. The number $1 - 1/s + \varepsilon$ in the exponent is best-possible in view of the following example. Let c be an integer, $c \geq 2$, and $s \geq 2$ be arbitrary. Set $G_n = c^{sn} - 1$ and $H_n = c^{(s-1)n} + \cdots + c^n + 1$. Then we have

$$\begin{aligned}\mathrm{G.C.D.}&\big(c^{sn}-1, c^{(s-1)n}+\cdots+c^n+1\big)\\ &= c^{(s-1)n} + \cdots + c^n + 1 \gg c^{(s-1)n} = (c^{sn})^{1-\frac{1}{s}}.\end{aligned}$$

In the most simplest case, when $G_n = a^n - 1$, $H_n = b^n - 1$ and a, b are multiplicatively independent integers, $a, b \geq 2$, Bugeaud, Corvaja and Zannier [1] obtained a considerably better bound.

If we consider (as in the theorem above) recurrences of the form

$$G_n = c_1\alpha^n + c_2, \qquad \text{and} \qquad H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n,$$

then it is no longer sufficient to assume that α and β_1 are multiplicatively independent, e.g. we have

$$\frac{6^n - 3^n + 2^n - 1}{2^n - 1} = 3^n - 1,$$

but the dominant roots are multiplicatively independent. Therefore we use a stronger condition to prove a similar result to that of Bugeaud, Corvaja and Zannier with recurrences (H_n) of arbitrary large order.

THEOREM 2. *Let* (G_n) *and* (H_n) *be linear recurring sequences of integers defined by* $G_n = c_1\alpha^n + c_2$ *and* $H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n$, *where* $s \ge 2$, c_i, d_j *are non-zero complex numbers and where* $\alpha > 1$, $\beta_1 > \cdots > \beta_s > 0$ *are integers with* α, $\beta_1\beta_2\cdots\beta_s$ *coprime. Furthermore, let* $\varepsilon > 0$. *Then, provided* $n > C_1$, *we have*

$$\mathrm{G.C.D.}(G_n, H_n) < |G_n|^{\varepsilon}$$

for all n *aside of a finite set of exceptions, whose cardinality can be bounded by* C_2, *where* C_1, C_2 *are effectively computable numbers depending on the* c_i, d_j, α, β_j, $i = 1,2$, $j = 1,\dots,s$ *and* ε.

Remark 6. Observe that for other classes of linear recurrences even better upper bounds can be obtained. For example, let $c \ge 2$ be an integer and let $s > r \ge 2$ with $\mathrm{G.C.D.}(r,s) = 1$. Then we have

$$\mathrm{G.C.D.}\big(c^{(r-1)n} + \cdots + c^n + 1, c^{(s-1)n} + \cdots + c^n + 1\big) < C_3$$

for all n, where C_3 is a constant independent of n. This follows from the fact that the polynomials $(X^r - 1)/(X-1)$ and $(X^s - 1)/(X-1)$ are relatively prime.

3. Auxiliary results

The proofs of our theorems depend on a quantitative version of the Subspace Theorem due to J.-H. Evertse [4].

Let K be an algebraic number field. Denote its ring of integers by O_K and its collection of places by M_K. For $v \in M_K$, $x \in K$, we define the absolute value $|x|_v$ by

(i) $|x|_v = |\sigma(x)|^{1/[K:\mathbb{Q}]}$ if v corresponds to the embedding $\sigma\colon K \hookrightarrow \mathbb{R}$;
(ii) $|x|_v = |\sigma(x)|^{2/[K:\mathbb{Q}]} = |\bar\sigma(x)|^{2/[K:\mathbb{Q}]}$ if v corresponds to the pair of conjugate complex embeddings $\sigma, \bar\sigma\colon K \hookrightarrow \mathbb{C}$;
(iii) $|x|_v = (N\wp)^{-\operatorname{ord}_\wp(x)/[K:\mathbb{Q}]}$ if v corresponds to the prime ideal $\wp$ of O_K.

Here $N\wp = \#(O_K/\wp)$ is the norm of $\wp$, and $\operatorname{ord}_\wp(x)$, the exponent of $\wp$ in the prime ideal composition of (x) with $\operatorname{ord}_\wp(0) := \infty$. In case (i) or (ii) we call v *real infinite* or *complex infinite*, respectively; in case (iii) we call v *finite*. These absolute values satisfy the *Product formula*

$$\prod_{v \in M_K} |x|_v = 1 \qquad \text{for} \quad x \in K^* . \tag{8}$$

The *height* of $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ with $\mathbf{x} \neq \mathbf{0}$ is defined as follows: for $v \in M_K$ put

$$|\mathbf{x}|_v = \begin{cases} \left(\sum_{i=1}^n |x_i|_v^{2[K:\mathbb{Q}]}\right)^{1/(2[K:\mathbb{Q}])} & \text{if } v \text{ is real infinite}, \\ \left(\sum_{i=1}^n |x_i|_v^{[K:\mathbb{Q}]}\right)^{1/[K:\mathbb{Q}]} & \text{if } v \text{ is complex infinite}, \\ \max(|x_1|_v, \dots, |x_n|_v) & \text{if } v \text{ is finite} \end{cases}$$

(note that for infinite places v, $|\cdot|_v$ is a power of the Euclidean norm). Now define

$$\mathcal{H}(\mathbf{x}) = \mathcal{H}(x_1, \dots, x_n) = \prod_v |\mathbf{x}|_v .$$

For a linear form $l(\mathbf{X}) = a_1 X_1 + \dots + a_n X_n$ with algebraic coefficients we define $\mathcal{H}(l) := \mathcal{H}(\mathbf{a})$, where $\mathbf{a} = (a_1, \dots, a_n)$ and if $\mathbf{a} \in K^n$, then we put $|l|_v = |\mathbf{a}|_v$ for $v \in M_K$. Further we define the number field $K(l) := K(a_1/a_j, \dots, a_n/a_j)$ for any j with $a_j \neq 0$; this is independent of the choice of j.

We are now ready to state Evertse's result [4]. The following notations are used:

- S is a finite set of places on K of cardinality s containing all infinite places;
- $\{l_{1v}, \dots, l_{nv}\}$, $v \in S$, are linearly independent sets of linear forms in n variables with algebraic coefficients such that

$$\mathcal{H}(l_{iv}) \leq H, \quad [K(l_{iv}) : K] \leq D \qquad \text{for} \quad v \in S, \ i = 1, \dots, n.$$

We choose for every place $v \in M_K$ a continuation of $|\cdot|_v$ to the algebraic closure of K and denote this also by $|\cdot|_v$.

THEOREM 3 (Quantitative Subspace Theorem, Evertse). *Let $0 < \delta < 1$ and consider the inequality for $\mathbf{x} \in K^n$:*

$$\prod_{v \in S} \prod_{i=1}^n \frac{|l_{iv}(\mathbf{x})|_v}{|\mathbf{x}|_v} < \left(\prod_{v \in S} |\det(l_{1v}, \dots, l_{nv})|_v\right) \cdot \mathcal{H}(\mathbf{x})^{-n-\delta}. \tag{9}$$

Then the following assertions hold:

(i) *There are proper linear subspaces $T_1, \dots, T_{t_1}$ of K^n with*

$$t_1 \leq \left(2^{60n^2} \cdot \delta^{-7n}\right)^s \log 4D \cdot \log\log 4D$$

such that every solution $\mathbf{x} \in K^n$ of (9) satisfying $\mathcal{H}(\mathbf{x}) \geq H$ belongs to $T_1 \cup \dots \cup T_{t_1}$.

(ii) *There are proper linear subspaces* $S_1, \dots, S_{t_2}$ *of* K^n *with*

$$t_2 \leq \left(150n^4 \cdot \delta^{-1}\right)^{ns+1}\left(2 + \log\log 2H\right)$$

such that every solution $\mathbf{x} \in K^n$ *of* (9) *satisfying* $\mathcal{H}(\mathbf{x}) < H$ *belongs to* $S_1 \cup \dots \cup S_{t_2}$.

Below we have collected some simple lemmas which are needed in our proofs.

Lemma 1. *Let* $N_{j,k}$ *denote the number of formal summands of* $(a_1 + \dots + a_k)^j$, *where* $a_1, \dots, a_k$ *denote formal commuting variables. Then*

$$N_{j,k} = \binom{k+j-1}{j}.$$

This is well known from combinatorics.

Next, we need an estimate for the number of 0's occurring in a linear recurring sequence (this number is called the *zero multiplicity of the recurrence*).

Lemma 2. *Let* (G_n) *be linear recurring sequence defined by* $G_n = c_1\alpha_1^n + c_2\alpha_2^n + \dots + c_t\alpha_t^n$ *where* $t \geq 2$, c_i *are non-zero complex and* $\alpha_1 > \dots > \alpha_t > 0$ *real numbers. Then the number of solutions of the equation*

$$G_n = 0$$

is at most t.

Proof. We prove our assertion by induction on t. The case $t = 1$ is trivial. Now consider the function of one real variable

$$g(x) = c_1 \exp\left(x \log(\alpha_1/\alpha_t)\right) + \dots + c_{t-1} \exp\left(x \log(\alpha_{t-1}/\alpha_t)\right) + c_t.$$

Clearly, the zeros of g at positive integral points are exactly the zeros of G_n. Now, $g(x)$ is a differentiable function of the real variable x. So, between any two zeros of g one can find a zero of the derivative g' of g. Since the derivative is a function of the same type with $t-1$ terms, the inductive hypothesis can be applied and the desired conclusion follows. □

Let us mention the remarkable result that there exists an upper bound (which does only depend on the order t, but in fact triply exponentially) for the zero multiplicity of arbitrary nondegenerate linear recurring sequences of complex numbers due to W. M. Schmidt [9].

Last but not least, we need some information about the structure of the ring of recurrences $\mathcal{E}_{\mathbb{Z}}^{+}$ considered here. In fact, if two recurrences (G_n) and (H_n) are given, they lie in a much smaller ring, namely in $\mathcal{E}_A$ where A is the multiplicative group generated by the roots of G_n and H_n. It is well known (see [5]) and in fact easy to prove that this ring is isomorphic to the ring

$$\mathbb{C}[T_1, \dots, T_t, T_1^{-1}, \dots, T_t^{-1}]$$

if A has rank $t \geq 1$. We simply choose a basis $\gamma_1, \dots, \gamma_t$ of A and associate the variable T_i the function $n \mapsto \gamma_i^n$. Now it is easy to show:

Lemma 3. *Let $(G_n), (H_n) \in \mathcal{E}_{\mathbb{Z}}^{+}$. If $\alpha_1 \cdots \alpha_t$ and $\beta_1 \cdots \beta_s$ are coprime, then (G_n) and (H_n) are coprime in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$.*

Proof. Let $G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n$ and $H_n = d_1\beta_1^n + d_2\beta_2^n + \cdots + d_s\beta_s^n$, where $t, s \geq 2$, c_i, d_j are non-zero complex numbers and where $\alpha_1 > \cdots > \alpha_t > 0$, $\beta_1 > \cdots > \beta_s > 0$ are integers. We denote by A the multiplicative group generated by $\alpha_1, \ldots, \alpha_t$, $\beta_1, \ldots, \beta_s$ and we choose a basis $\gamma_1, \ldots, \gamma_r$ for A.

By the correspondence mentioned above we may write

$$G_n = g(\gamma_1^n, \ldots, \gamma_r^n) \qquad \text{and} \qquad H_n = h(\gamma_1^n, \ldots, \gamma_r^n)$$

with $g, h \in \mathbb{C}[T_1, \ldots, T_r]$ since the roots are integers. By the assumption that $\alpha_1 \cdots \alpha_t$ and $\beta_1 \cdots \beta_s$ are coprime it follows that g and h consist of different variables. But from this it is clear that the polynomials g and h are coprime and consequently the conclusion follows. □

4. Proof of Theorem 1

In the sequel $C_1, C_2, \ldots$ will denote positive numbers depending only on c_i, d_j, α_i and β_j, $i = 1, \ldots, t$, $j = 1, \ldots, s$.

According to Lemma 2 the number of n such that $G_n = 0$ is at most t. In this case we have

$$\mathrm{G.C.D.}(G_n, H_n) = H_n,$$

and therefore these n must be excluded. Consequently, we can restrict ourselves to numbers n for which $G_n \neq 0$. We write

$$z(n) = \frac{H_n}{G_n} = \frac{\mathfrak{c}_n}{\mathfrak{d}_n},$$

where $\mathfrak{c}_n$, $\mathfrak{d}_n$ are nonzero integers. Observe that we only consider those n for which $G_n \neq 0$. Thus we have

$$\mathrm{G.C.D.}(G_n, H_n) \cdot \mathfrak{d}_n = G_n. \tag{10}$$

We now assume that

$$|\mathfrak{d}_n| \leq |G_n|^{1-c} \tag{11}$$

for all n in a set Σ of natural numbers and for some c, which will be specified later. We will show that, provided $n > C_1$ is large enough, (11) can only hold for a finite number of n and we give an upper bound C_2 for $|\Sigma|$. Then we can conclude that, provided $n > C_1$, we have

$$|\mathfrak{d}_n| > |G_n|^{1-c}$$

for all $n \notin \Sigma$ and using (10) we conclude

$$\mathrm{G.C.D.}(G_n, H_n) = |G_n| \cdot |\mathfrak{d}_n|^{-1} < |G_n|^c$$

for all $n \notin \Sigma$ with $|\Sigma| < C_2$. Thus the assertion of our theorem will follow from this.

Fix an integer $h > 0$ and observe the following expansion

$$\begin{aligned}
\frac{1}{G_n} &= \frac{1}{c_1\alpha_1^n} \cdot \sum_{j=0}^{\infty}(-1)^j \left(\sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^j \\
&= \frac{1}{c_1\alpha_1^n} \cdot \sum_{j=0}^{h}(-1)^j \left(\sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^j \\
&\qquad + \frac{1}{c_1\alpha_1^n} \cdot \sum_{j=h+1}^{\infty}(-1)^j \left(\sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^j \\
&= \frac{1}{c_1\alpha_1^n} \cdot \sum_{j=0}^{h}(-1)^j \left(\sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^j \\
&\qquad + \frac{1}{c_1\alpha_1^n} \cdot \frac{(-1)^{h+1}\left(\sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^{h+1}}{1 + \sum_{i=2}^{t} \frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n}.
\end{aligned}$$

Let us remark that for

$$n > C_4 := \frac{\log(2\bar{c})}{\log\alpha_1 - \log\alpha_2}$$

we have

$$\begin{aligned}
|G_n| &= |c_1\alpha_1^n + \cdots + c_t\alpha_t^n| \\
&= |c_1||\alpha_1|^n \left| 1 + \sum_{j=2}^{t} \frac{c_j}{c_1}\left(\frac{\alpha_j}{\alpha_1}\right)^n \right| \\
&\geq |c_1||\alpha_1|^n \left| 1 - \underbrace{\sum_{j=2}^{t} \left|\frac{c_j}{c_1}\right| \left|\frac{\alpha_j}{\alpha_1}\right|^n}_{\leq \bar{c}(\alpha_2/\alpha_1)^n \leq 1/2 \text{ for } n > C_4} \right| \geq \frac{|c_1|}{2}\alpha_1^n,
\end{aligned}$$

where

$$\bar{c} := \max\left\{1, \left|\tfrac{c_2}{c_1}\right|, \ldots, \left|\tfrac{c_t}{c_1}\right|\right\}.$$

Next we are going to approximate $z(n) = H_n/G_n$ by a finite sum extracted from the above expansion. We define

$$\tilde{z}(n) := H_n \cdot \frac{1}{c_1\alpha_1^n}\sum_{j=0}^{h}(-1)^j\left(\sum_{i=2}^{t}\frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^j,$$

where $h \geq 1$ is an integer to be chosen later. We may write

$$\tilde{z}(n) = \sum_{j=1}^{N} e_j\left(\frac{f_j}{b}\right)^n, \qquad n \in \Sigma,$$

where the $e_j \in \mathbb{Q}^*$ and the f_j, b are integers, $b > 0$, and the f_j/b are nonzero distinct rational numbers. Clearly $\tilde{z}(n)$ is nondegenerate. In fact, we take

$$b = \alpha_1^{h+1}.$$

Moreover, by Lemma 1 we have

$$N \leq \binom{h+t-1}{h}s =: C_5. \tag{12}$$

Now we estimate the approximation error we make when we approximate $z(n)$ through $\tilde{z}(n)$. We have

$$\begin{aligned}
|z(n) - \tilde{z}(n)| &= \left| H_n \cdot \frac{1}{c_1\alpha_1^n} \cdot \frac{(-1)^{h+1}\left(\sum\limits_{i=0}^{t}\frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^{h+1}}{1+\sum\limits_{i=2}^{t}\frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n}\right| \\
&= \left| H_n \cdot \frac{(-1)^{h+1}\left(\sum\limits_{i=0}^{t}\frac{c_i}{c_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^{h+1}}{G_n}\right| \\
&\leq |H_n| \cdot \frac{2}{|c_1|}\alpha_1^{-n}\left(\bar{c}\frac{\alpha_2}{\alpha_1}\right)^{n(h+1)} \\
&\leq \frac{2\tilde{d}\bar{c}^{h+1}}{|c_1|}\beta_1^n\alpha_1^{-n}\left(\frac{\alpha_2}{\alpha_1}\right)^{n(h+1)},
\end{aligned} \tag{13}$$

where

$$\tilde{d} := \max\{1, |d_1|, \ldots, |d_s|\}.$$

We choose the integer h so that

$$\left(\frac{\alpha_2}{\alpha_1}\right)^{h+1}\beta_1 < 1. \tag{14}$$

To get this, we must have

$$h > \max\left\{1,\ \frac{\log\beta_1}{\log\alpha_1 - \log\alpha_2} - 1\right\}.$$

Observe that from now on h is fixed and therefore also $N, e_j,\ f_j, b$ are fixed. Now let S be the set of absolute values of $\mathbb{Q}$ consisting of ∞ and all primes dividing some of the f_j or b and therefore $\alpha_1\cdots\alpha_t\beta_1\cdots\beta_s$. Thus,

$$|S| \le \omega(\alpha_1\cdots\alpha_t\beta_1\cdots\beta_s) := 1 + \sum_{p|\alpha_1\cdots\alpha_t\beta_1\cdots\beta_s} 1\,.$$

We shall apply Theorem 3, so let us define for every $v \in S$, $N+1$ independent linear forms in $\boldsymbol{X} := (X_0, \ldots, X_N)$ as follows: put

$$L_{0,\infty}(\boldsymbol{X}) = X_0 - e_1X_1 - \cdots - e_NX_N$$

and for $v \in S$, $0 \le i \le N$, $(i,v) \ne (0,\infty)$ put

$$L_{i,v}(\boldsymbol{X}) = X_i\,.$$

Observe that for each $v \in S$, the linear forms $L_{0,v}, \ldots, L_{N,v}$ are indeed linearly independent. We have

$$\mathcal{H}(L_{i,v}) \le C_7 := \max\{1, C_6H\}\,,$$

where

$$H := \prod_{v\in M_{\mathbb{Q}}} \max_{\substack{j=1,\ldots,s\\ 0\le i_2,\ldots,i_t\le h\\ 0\le i_2+\cdots+i_t\le h}} \left\{\left|d_j\cdot\frac{c_2^{i_2}\cdots c_t^{i_t}}{c_1^{i_2+\cdots+i_t+1}}\right|_v\right\}$$

for $v \in S$, $i = 0, \ldots, h$ and where $C_6 = \sqrt{C_5+1}$. Furthermore $\mathbb{Q}(L_{i,v}) = \mathbb{Q}$ which means that the coefficients just lie in $\mathbb{Q}$ and therefore

$$[\mathbb{Q}(L_{i,v}) : \mathbb{Q}] = 1 \qquad \text{for all} \quad v \in S\,,\quad i = 0,\ldots,N\,.$$

Moreover, we have

$$\det(L_{0,v}, \ldots, L_{N,v}) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0\\ * & 1 & 0 & \ldots & 0\\ * & 0 & 1 & \ldots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ * & 0 & 0 & \ldots & 1\end{vmatrix} = 1\,,$$

which yields

$$\left|\det(L_{0,v}, \ldots, L_{N,v})\right|_v = 1 \qquad \text{for all} \quad v \in S\,.$$

For $n \in \Sigma$ define the vectors $\mathbf{x}_n = \mathfrak{d}_n\big(b^n z(n), f_1^n, \dots, f_N^n\big) \in \mathbb{Z}^{N+1}$ and consider the double product

$$\prod_{v\in S}\prod_{i=0}^{N} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}.$$

By putting

$$\begin{aligned} L_{0,\infty}(\mathbf{x}_n) &= \mathfrak{d}_n b^n \left(z(n) - e_1\left(\frac{f_1}{b}\right)^n - \cdots - e_N\left(\frac{f_N}{b}\right)^n \right) \\ &= \mathfrak{d}_n b^n \big(z(n) - \tilde{z}(n)\big), \end{aligned}$$

we can rewrite the double product as

$$|L_{0,\infty}(\mathbf{x}_n)|_\infty \cdot \Bigg(\prod_{v\in S\setminus\{\infty\}} |\mathfrak{c}_n b^n|_v\Bigg)\Bigg(\prod_{v\in S}\prod_{j=1}^{N} |\mathfrak{d}_n f_j^n|_v\Bigg)\Bigg(\prod_{v\in S}|\mathbf{x}_n|_v\Bigg)^{-(N+1)}.$$

Observe that, due to our choice of S, the f_j^n are S-units for $j \geq 1$. In particular, this implies

$$\Bigg(\prod_{v\in S}\prod_{j=1}^{N} |f_j^n|_v\Bigg) = 1$$

and therefore

$$\Bigg(\prod_{v\in S}\prod_{j=1}^{N} |\mathfrak{d}_n f_j^n|_v\Bigg) \leq |\mathfrak{d}_n|^N, \tag{15}$$

and

$$\Bigg(\prod_{v\in S\setminus\{\infty\}} |\mathfrak{c}_n b^n|_v\Bigg) \leq \prod_{v\in S\setminus\{\infty\}} |b^n|_v = b^{-n} = \alpha_1^{-n(h+1)}, \tag{16}$$

where we have used the product formula (8). Therefore we get, using (13), (15) and (16),

$$\prod_{v\in S}\prod_{i=0}^{N} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v} \leq |\mathfrak{d}_n|^{N+1} \frac{2\tilde{d}\tilde{c}^{h+1}}{|c_1|} \beta_1^n \alpha_1^{-n} \left(\frac{\alpha_2}{\alpha_1}\right)^{n(h+1)} \Bigg(\prod_{v\in S}|\mathbf{x}_n|_v\Bigg)^{-(N+1)}.$$

Recall that we are assuming $n \in \Sigma$, i.e.

$$|\mathfrak{d}_n| \leq |G_n|^{1-c} \leq \tilde{c}\alpha_1^{n(1-c)},$$

where

$$\tilde{c} := \max\{1, |c_1|\bar{c}\}.$$

Hence, we get

$$\prod_{v\in S}\prod_{i=0}^{N}\frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}\le C_8\left(\beta_1\alpha_1^{(N+1)(1-c)-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{h+1}\right)^n\left(\prod_{v\in S}|\mathbf{x}_n|_v\right)^{-(N+1)},$$

where

$$C_8:=\frac{2\tilde{c}^{(C_5+1)}\tilde{d}\tilde{c}^{h+1}}{|c_1|}.$$

Last we need an upper bound for $\mathcal{H}(\mathbf{x}_n)$. We have

$$\mathcal{H}(\mathbf{x}_n)\le|\mathbf{x}_n|_\infty=|\mathfrak{d}_n|\max\{|b^n z(n)|,|f_1^n|,\dots,|f_N^n|\},\tag{17}$$

where we have used the choice of S. By using the fact that

$$1\le|b^n\mathfrak{c}_n|\le|b^nH_n|\le\tilde{d}\alpha_1^{n(h+1)}\beta_1^n$$

and $|f_j^n|\le\alpha_1^{hn}$ for $j=1,\dots,N$ we get

$$\mathcal{H}(\mathbf{x}_n)\le\tilde{c}\tilde{d}\left(\alpha_1^{h+1}\beta_1\right)^n.\tag{18}$$

Let us point out that the constant does not depend on n.

We now choose $0<\delta<1$ so that

$$\left(\alpha_2\alpha_1^{-1}\right)^{h+1}\beta_1\left(\alpha_1^{h+1}\beta_1\right)^\delta<1.\tag{19}$$

This will be fulfilled for

$$0<\delta<\frac{(h+1)[\log\alpha_1-\log\alpha_2]-\log\beta_1}{(h+1)\log\alpha_1+\log\beta_1},$$

which is possible in view of (14).

In view of the bound for the double product we derived and (18), the verification of (9) of the Quantitative Subspace Theorem 3 will follow from

$$C_8\left(\beta_1\alpha_1^{(N+1)(1-c)-1}\left(\alpha_2\alpha_1^{-1}\right)^{h+1}\right)^n<\left(\tilde{c}\tilde{d}\left(\alpha_1^{h+1}\beta_1\right)^n\right)^{-\delta},$$

which is the same as

$$\left(\alpha_1^{(N+1)(1-c)-1}\left(\alpha_2\alpha_1^{-1}\right)^{h+1}\beta_1\left(\alpha_1^{h+1}\beta_1\right)^\delta\right)^n<\left(C_8\left(\tilde{c}\tilde{d}\right)^\delta\right)^{-1}.$$

However, this latter inequality follows from (19) for

$$n>C_9:=\frac{\log\left(C_8\left(\tilde{c}\tilde{d}\right)^\delta\right)}{\log\left(\alpha_1^{(C_5+1)(c-1)+1+(h+1)(1-\delta)}\alpha_2^{-(h+1)}\beta_1^{-(1+\delta)}\right)},$$

whenever we have

$$\frac{C_5}{C_5+1} < c < 1\,,$$

which implies that

$$(N+1)(1-c)-1 \le (C_5+1)(1-c)-1 < 0\,.$$

Therefore, by the Quantitative Subspace Theorem 3, there exist finitely many non-zero linear forms $\Lambda_1(\boldsymbol{X}),\dots,\Lambda_g(\boldsymbol{X})$ with coefficients in $\mathbb{Q}$ and with

$$g \le C_{10} := \left(2^{60C_5^2}\delta^{-7C_5}\right)^{\omega(\alpha_1\cdots\beta_s)}(2+\log\log 2C_7)\,,$$

such that each vector $\boldsymbol{x}_n$ is a zero of some Λ_j.

Suppose first Λ_j does not depend on X_0. Then, if $\Lambda_j(\boldsymbol{x}_n)=0$, we have a nontrivial relation

$$\sum_{i=1}^{N} u_i\left(\frac{f_i}{b}\right)^n = 0\,, \qquad u_i\in\mathbb{Q}, \quad i=1,\dots,N\,.$$

By Lemma 2 this can hold for at most a finite number of n. More precisely, we can conclude that the number of those solutions can be bounded by

$$N \le C_5\,,$$

which follows from Lemma 2.

Suppose that Λ_j depends on X_0 and that $\Lambda_j(\boldsymbol{x}_n)=0$. Then we have

$$z(n) = \sum_{i=1}^{N} v_i\left(\frac{f_i}{b}\right)^n, \qquad v_i\in\mathbb{Q}, \quad i=1,\dots,N\,. \tag{20}$$

Let us assume that this equality holds for infinitely many n. In that case we would get a relation of the form

$$b^n H_n = G_n R_n\,,$$

where R_n is a power sum with positive roots, valid for infinitely many n. This in turn implies the validity of the same relation for all n, which is excluded by the hypothesis. An upper bound follows now from the fact that the left hand side of

$$H_n - G_n\cdot\sum_{i=1}^{N} v_i\left(\frac{f_i}{b}\right)^n = 0 \tag{21}$$

is a nontrivial recurring sequence with positive roots and therefore equation (21) can hold for at most $C_5\cdot t+s$ many n by Lemma 2.

The number of exceptions $|\Sigma|$ can be bounded by

$$C_2 := t + \left(2^{60C_5^2}\delta^{-7C_5}\right)^{\omega(\alpha_1\cdots\beta_s)}(2+\log\log 2C_7)\big(C_5(t+1)+s\big)$$

and $C_1 := \max\{C_4, C_9\}$. This completes the proof.

5. Proof of Corollary 1

The proof is essentially the same as the proof of Theorem 1. We use the same notations as in the proof before and mention only the part that must be modified.

In this case we approximate $z(n)$ by:

$$\tilde{z}(n) := H_n \cdot \frac{1}{c_1 \alpha_1^n} \sum_{j=0}^{h} (-1)^j \left(\frac{c_2}{c_1} \left(\frac{1}{\alpha_1} \right)^n \right)^j ,$$

which we may write as

$$\tilde{z}(n) = \sum_{j=1}^{N} e_j \left(\frac{f_j}{b} \right)^n , \qquad n \in \Sigma ,$$

where the $e_j \in \mathbb{Q}^*$ and the f_j, b are integers, $b > 0$, and the f_j/b are nonzero distinct rational numbers. Consequently, we have the estimate

$$N \leq (h+1)s . \tag{22}$$

The approximation error is

$$|z(n) - \tilde{z}(n)| \leq \frac{2\tilde{d}\tilde{c}^{h+1}}{|c_1|} \beta_1^n \alpha_1^{-n} \left(\alpha_1^{-n} \right)^{h+1} ,$$

where the constants are defined as before.

Now, if we set

$$c = 1 - \frac{1}{s} + \varepsilon ,$$

we have

$$\alpha_1^{s(1-c)-1} < 1$$

and we therefore can choose h such that

$$\left(\alpha_1^{s(1-c)-1} \right)^{h+1} \beta_1 < 1 . \tag{23}$$

We choose linear forms as above and get

$$\begin{aligned} \prod_{v \in S} \prod_{i=0}^{N} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v} &\leq C_8 \left(\beta_1 \alpha_1^{(N+1)(1-c)-1-(h+1)} \right)^n \left(\prod_{v \in S} |\mathbf{x}_n|_v \right)^{-(N+1)} \\ &= C_8 \left(\beta_1 \alpha_1^{(h+1)(s(1-c)-1)-c} \right)^n \left(\prod_{v \in S} |\mathbf{x}_n|_v \right)^{-(N+1)} . \end{aligned}$$

As above we have

$$\mathcal{H}(\mathbf{x}_n) \le |\mathbf{x}_n|_\infty = |\mathfrak{d}_n| \max\{|b^n z(n)|, |f_1^n|, \dots, |f_N^n|\} \le \tilde{c}\tilde{d}\left(\alpha_1^{h+1}\beta_1\right)^n ,$$

and we choose $0 < \delta < 1$ so that

$$\left(\alpha_1^{s(1-c)-1}\right)^{h+1} \beta_1 \left(\alpha_1^{h+1}\beta_1\right)^\delta < 1 .$$

This is possible in view of (23). With this, condition (9) of the Quantitative Subspace Theorem 3 is valid if $n > C_9$.

The rest of the arguments are as above, the assertion follows and so the proof is finished.

6. Proof of Theorem 2

In the sequel $C_1, C_2, \dots$ will denote positive numbers depending only on c_i, d_j, α and β_j, $i = 1, \dots, t$, $j = 1, \dots, s$ and ε.

First observe that the only zero of G_n can be

$$n = \frac{\log(-c_2/c_1)}{\log \alpha} .$$

We fix a positive integer k. Let us denote by $\mathcal{J} = \{\boldsymbol{j} = (j_1, \dots, j_s) \in \mathbb{N}^s : j_1 + \dots + j_s = k\}$. If we write $\boldsymbol{j}_i$ we mean the ith vector in $\mathcal{J}$ with respect to the lexicographical ordering. The cardinality of $\mathcal{J}$ is given by

$$M := |\mathcal{J}| = \binom{s+k-1}{k} .$$

For every $\boldsymbol{j} \in \mathcal{J}$, we define

$$H_{\boldsymbol{j},n} = \underline{\beta}^{n\boldsymbol{j}}\left(d_1\beta_1^n + d_2\beta_2^n + \dots + d_s\beta_s^n\right) ,$$

where we have abbreviated $\underline{\beta}^{(j_1,\dots,j_s)} = \beta_1^{j_1} \cdots \beta_s^{j_s}$. Moreover, we write

$$z_{\boldsymbol{j}}(n) = \frac{H_{\boldsymbol{j},n}}{G_n} = \frac{\mathfrak{c}_{\boldsymbol{j},n}}{\mathfrak{d}_n} ,$$

where $\mathfrak{c}_{\boldsymbol{j},n}$, $\mathfrak{d}_n$ are integers. Since G_n divides $H_{\boldsymbol{j},n}$ for all $\boldsymbol{j}$ and all positive integers n we may choose $\mathfrak{d}_n$ to be the denominator of H_n/G_n.

We now assume that $\varepsilon > 0$ is given and that

$$|\mathfrak{d}_n| \le |G_n|^{(1-\varepsilon)} \tag{24}$$

for all n in a set Σ of natural numbers. We will again show that, provided $n > C_1$ is large enough, (24) can only hold for at most C_2 many numbers n. Then we conclude

$$\mathrm{G.C.D.}(G_n, H_n) = |G_n| \cdot |\mathfrak{d}_n|^{-1} < |G_n|^{\varepsilon},$$

provided that $n > C_1$ for all $n \notin \Sigma$ with $|\Sigma| \leq C_2$. This will conclude our proof.

For a fixed integer $h > 1$ we consider the expansion

$$\begin{aligned}\frac{1}{G_n} &= \frac{1}{c_1\alpha^n}\sum_{i=0}^{\infty}(-1)^i\left(\frac{c_2}{c_1}\right)^i\alpha^{-ni}\\ &= \sum_{i=1}^{h}(-1)^{i-1}\frac{c_2^{i-1}}{c_1^i}\alpha^{-ni} + \frac{(-1)^h\left(\frac{c_2}{c_1}\right)^h\alpha^{-nh}}{G_n}.\end{aligned}$$

For

$$n > \frac{\log(2|c_2/c_1|)}{\log\alpha} =: C_4$$

we have

$$|G_n| = |c_1\alpha^n + c_2| \geq \frac{|c_1|}{2}\alpha^n.$$

For a given index $\boldsymbol{j} \in \mathcal{J}$ we thus obtain, on multiplying by $H_{\boldsymbol{j},n}$,

$$\begin{aligned}\left|z_{\boldsymbol{j}}(n) - H_{\boldsymbol{j},n}\cdot\sum_{i=1}^{h}(-1)^{i-1}\frac{c_2^{i-1}}{c_1^i}\alpha^{-ni}\right| &\leq |H_{\boldsymbol{j},n}|\cdot\frac{2|c_2|^h}{|c_1|^{h+1}}\alpha^{-n(h+1)}\\ &\leq \frac{2\tilde{d}\,|c_2|^h}{|c_1|^{h+1}}\beta_1^{(k+1)n}\alpha^{-n(h+1)}.\end{aligned} \tag{25}$$

Let us write C_{10} for the constant appearing in the last expression. We want to apply now the Subspace Theorem, viewing the left side of (25) as a "small" linear form. We shall consider several such linear forms, corresponding to values of $\boldsymbol{j} \in \mathcal{J}$ with k large enough. The idea of choosing this linear forms is similar to that used in [3].

We define

$$\begin{aligned}\phi_{\boldsymbol{j}}(n) &:= z_{\boldsymbol{j}}(n) - H_{\boldsymbol{j},n}\cdot\sum_{i=1}^{h}(-1)^{i-1}\frac{c_2^{i-1}}{c_1^i}\alpha^{-ni}\\ &= z_{\boldsymbol{j}}(n) - \beta_1^{j_1n}\cdots\beta_s^{j_sn}\sum_{i=1}^{h}\sum_{l=1}^{s}(-1)^{i-1}d_l\frac{c_2^{i-1}}{c_1^i}\beta_l^n\alpha^{-ni}\end{aligned}$$

for every index $\boldsymbol{j} = (j_1, \ldots, j_s)$ with $j_1 + \cdots + j_s = k$.

Now, let S consist of ∞ and all primes dividing α or one of the β_i, $i = 1,\dots,s$. Second, we put

$$N = \binom{s+k-1}{k} + h\binom{s+k}{k+1}.$$

Observe that the first summand is equal to the cardinality of $\mathcal{J}$ and the second summand is an upper bound for the number of nonzero terms in the double sum above. For convenience we shall denote vectors in $\mathbb{Z}^N$ by writing

$$\mathbf{x} = (x_1,\dots,x_N) = (z_1,\dots,z_M,y_1,\dots,y_{N-M}).$$

We define for every $s \in S$, N independent linear forms in $\mathbf{X} = (X_1,\dots,X_N)$ as follows. For $j = 1,\dots,M$ let $\mathbf{j}_j \in \mathcal{J}$ be the jth vector with respect to the lexicographical ordering and put

$$L_{j,\infty}(\mathbf{X}) = Z_j - \sum_{i=1}^{h}\sum_{l=1}^{s}(-1)^{i-1}d_l\frac{c_2^{i-1}}{c_1^i}Y_{i,l,\mathbf{j}_j},$$

while, for $(i,v) \notin \{(1,\infty),\dots,(M,\infty)\}$ we put

$$L_{i,v}(\mathbf{X}) = X_i.$$

Observe that for each $s \in S$, the linear forms $L_{1,v},\dots,L_{N,v}$ are indeed linearly independent. We have

$$\mathcal{H}(L_{i,v}) \le C_{11} := \sqrt{N+1}\prod_{v\in M_{\mathbb{Q}}}\max_j\left\{\left|d_j\frac{c_2^h}{c_1^h}\right|_v, 1\right\}$$

for $v \in S$, $i = 1,\dots,N$. Furthermore $\mathbb{Q}(L_{i,v}) = \mathbb{Q}$ and therefore

$$[\mathbb{Q}(L_{i,v}):\mathbb{Q}] = 1 \qquad \text{for all} \quad v \in S,\ \ i = 1,\dots,N.$$

Moreover, we have

$$\det(L_{1,v},\dots,L_{N,v}) = 1,$$

which yields

$$|\det(L_{1,v},\dots,L_{N,v})|_v = 1 \qquad \text{for all} \quad v \in S.$$

For $n \in \Sigma$ define the vectors $\mathbf{x}_n$ by

$$\mathfrak{d}_n\alpha^{hn}\left(z_{\mathbf{j}_1}(n),\dots,z_{\mathbf{j}_M}(n),\dots,\beta_1^{j_1n}\beta_2^{j_2n}\cdots\beta_s^{j_sn}\beta_l^n\alpha^{-in},\dots\right),$$

where the indices vary lexicographically over all tuples $\mathbf{j} \in \mathcal{J}$, $l = 1,\dots,s$ and $i = 1,\dots,h$. Note that $\mathbf{x}_n \in \mathbb{Z}^N$ and that we have

$$L_{i,\infty}(\mathbf{x}_n) = \phi_{\mathbf{j}_i}(n), \qquad i = 1,\dots,M,$$

and consider the double product

$$\prod_{v\in S}\prod_{i=1}^{N}\frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}. \tag{26}$$

First observe that we have for $i > M$

$$\prod_{v\in S}|L_{i,v}(\mathbf{x}_n)|_v = \prod_{v\in S}\left|\mathfrak{d}_n\beta_1^{j_1 n}\cdots\beta_s^{j_s n}\beta_l^n\alpha^{(h-i)n}\right|_v \le |\mathfrak{d}_n|,$$

where $j_1,\dots,j_s$, l and i are suitable integers. Observe that we have used our choice of S again and the product formula to obtain $\prod_{v\in S}|\beta_1^{j_1 n}\cdots\beta_s^{j_s n}\beta_l^n\alpha^{(h-i)n}|_v = 1$.

Further, for $i \le M$ we have $x_i = \mathfrak{d}_n\alpha^{hn}z_{\mathbf{j}_i}(n) = \mathfrak{c}_{\mathbf{j}_i,n}\alpha^{hn}$, whence

$$\prod_{v\in S\setminus\{\infty\}}|L_{i,v}(\mathbf{x}_n)|_v \le \alpha^{-hn}.$$

Also, in view of (25), we have, again for $i \le M$,

$$|L_{i,\infty}(\mathbf{x}_n)| \le C_{12}|\mathfrak{d}_n|\beta_1^{(k+1)n}\alpha^{-n}.$$

Plugging these estimates into (26), we finally obtain

$$\begin{aligned}\prod_{v\in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x}_n)|_v &\le |\mathfrak{d}_n|^{N-M}\prod_{v\in S}\prod_{i=1}^{M}|L_{i,v}(\mathbf{x}_n)|_v\\ &\le C_{12}|\mathfrak{d}_n|^M\beta_1^{(k+1)Mn}\alpha^{-Mn}|\mathfrak{d}_n|^{N-M}\alpha^{-hMn}\\ &= C_{12}|\mathfrak{d}_n|^N\alpha^{-(h+1)Mn}\beta_1^{(k+1)Mn}.\end{aligned}$$

Recall that we are assuming $n \in \Sigma$, i.e.

$$|\mathfrak{d}_n| \le |G_n|^{1-\varepsilon} \le \tilde{c}\alpha^{(1-\varepsilon)n}.$$

Hence we have

$$\prod_{v\in S}\prod_{i=1}^{N}\frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v} \le C_{12}\tilde{c}^N\alpha^{(1-\varepsilon)Nn}\alpha^{-(h+1)Mn}\beta_1^{(k+1)Mn}\left(\prod_{v\in S}|\mathbf{x}_n|_v\right)^{-N}. \tag{27}$$

Let us point out here that the constant does not depend on n. We now choose the integer k such that

$$k > \frac{s-1-\varepsilon s}{\varepsilon}.$$

This implies that

$$\alpha^{(1-\varepsilon)N-(h+1)M} \le \alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mh} < 1.$$

We choose the integer h so that

$$\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mh}\beta_1^{(k+1)M}<1\,, \tag{28}$$

i.e. we have

$$h>\frac{(k+1)\log\beta_1}{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)\log\alpha}\,.$$

This is possible because of our choice of k.

On the other side, since in any case $|\mathfrak{d}_n|<|G_n|$, we get

$$\mathcal{H}(\boldsymbol{x}_n)\le\prod_{v\in S}|\boldsymbol{x}_n|_v\le\max_{i=1,\dots,N}\{|x_i|\}\,,$$

where we have used our choice of S, the fact that two norms on $\mathbb{Q}^N$ are equivalent and that the x_i are integers. Now we have

$$\left|\mathfrak{c}_{\boldsymbol{j}_i,n}\alpha^{hn}\right|\le\left|H_{\boldsymbol{j}_i,n}\alpha^{hn}\right|\le\tilde{d}\beta_1^{(k+1)n}\alpha^{hn}$$

and

$$\left|\beta_1^{j_1}\cdots\beta_s^{j_s}\beta_l^n\alpha^{(h-i)n}\mathfrak{d}_n\right|\le\tilde{c}\beta_1^{(k+1)n}\alpha^{(h-1)n}\alpha^{(1-\varepsilon)n}\le\tilde{c}\beta_1^{(k+1)n}\alpha^{hn}\,.$$

Thus we can conclude

$$\mathcal{H}(\boldsymbol{x}_n)\le C_{13}\beta_1^{(k+1)n}\alpha^{hn}\,, \tag{29}$$

where the constant $C_{13}:=\max\{\tilde{c},\tilde{d}\}$ does not depend on n.

We now choose $0<\delta<1$ so that

$$\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mh}\beta_1^{(k+1)M}\left(\beta_1^{k+1}\alpha^h\right)^\delta<1\,. \tag{30}$$

This will be possible for small δ in view of (28), namely for

$$\delta<\frac{\log\left(\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mh}\beta_1^{(k+1)M}\right)}{\log(\beta_1^{k+1}\alpha^h)}\,.$$

The verification of (9) of the Quantitative Subspace Theorem 3 will follow from

$$C_{12}\tilde{c}^N\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mhn}\beta_1^{(k+1)Mn}<\left(C_{13}\alpha^{hn}\beta_1^{(k+1)n}\right)^{-\delta}$$

in view of (27) and (29). This is the same as

$$\left(\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mhn}\beta_1^{(k+1)Mn}\left(\beta_1^{k+1}\alpha^h\right)^\delta\right)^n<\left(C_{12}\tilde{c}^NC_{13}^\delta\right)^{-1}\,.$$

This inequality follows from (30) for

$$n>C_{14}:=\frac{\log(C_{12}\tilde{c}^NC_{13}^\delta)}{\log\left(\alpha^{\left((1-\varepsilon)\frac{s+k}{k+1}-1\right)Mh}\beta_1^{(k+1)M}\left(\beta_1^{k+1}\alpha^h\right)^\delta\right)}\,.$$

By the Quantitative Subspace Theorem 3 we can conclude that there exist finitely many non-zero linear forms $\Lambda_1(\boldsymbol{X}),\dots,\Lambda_g(\boldsymbol{X})$ with coefficients in $\mathbb{Q}$ and with

$$g \le C_{15} := \left(2^{60N^2}\delta^{-7N}\right)^{\omega(\alpha\beta_1\cdots\beta_s)}(2+\log\log 2C_{11}),$$

such that each vector $\boldsymbol{x}_n$ is a zero of some Λ_j. Let us consider a hyperplane given by

$$\Lambda(\boldsymbol{X}) = u_1Z_1+\cdots+u_MZ_M+\sum_{i=1}^{N-M} v_iY_i = 0,$$

where the coefficients are rational numbers, not all zero. Substituting from the definition of $\boldsymbol{x}_n$, we get the equation

$$\alpha^{hn}H_n\sum_{\boldsymbol{j}\in\mathcal{J}} u_{\boldsymbol{j}}\beta_1^{j_1}\cdots\beta_s^{j_s} = G_n\cdot\sum_{i,l,\boldsymbol{j}} v_{i,l,\boldsymbol{j}}\beta_1^{j_1}\cdots\beta_s^{j_s}\beta_l^n\alpha^{(h-i)n}, \tag{31}$$

where the sum runs lexicographically over $\boldsymbol{j}=(j_1,\dots,j_s)\in\mathcal{J}$, $l=1,\dots,s$ and $i=1,\dots,h$ and is valid for some integers $n\in\Sigma$. But this equation can only hold identically, which means for all $n\in\mathbb{N}$, or it has a finite number of solutions $n\in\mathbb{N}$. Therefore, we first assume that all $u_{\boldsymbol{j}}$ are equal to zero, then we have

$$\sum_{i,l,\boldsymbol{j}} v_{i,l,\boldsymbol{j}}\beta_1^{j_1}\cdots\beta_s^{j_s}\beta_l^n\alpha^{(h-i)n} = 0,$$

and at least one of the $v_{i,l,\boldsymbol{j}}$ is different from zero. This can hold for at most $N-M$ many n by Lemma 2. Second, we assume that all $v_{i,l,\boldsymbol{j}}$ are equal to zero, then we have

$$\alpha^{hn}H_n\cdot\sum_{\boldsymbol{j}\in\mathcal{J}} u_{\boldsymbol{j}}\beta_1^{j_1}\cdots\beta_s^{j_s} = 0,$$

which can hold for at most $s+M$ many n by Lemma 2. If there is at least one non-zero coefficient at both sides of (31), then we can conclude (observe that by Lemma 3, G_n and H_n are coprime) that G_n divides

$$\sum_{\boldsymbol{j}\in\mathcal{J}} u_{\boldsymbol{j}}\beta_1^{j_1}\cdots\beta_s^{j_s}$$

in the ring $\mathcal{E}_{\mathbb{Z}}^{+}$, which is impossible by Lemma 3, since α and $\beta_1\cdots\beta_s$ are coprime, or (31) holds for at most N many n.

Finally the number of exceptions can be bounded by

$$C_2 := 1 + C_{15}(s+2N)$$

and C_1 can be choose as $C_1 := \max\{C_4, C_{14}\}$. So, the proof is finished.

Acknowledgement

The author would like to thank Prof. P. Corvaja for suggestions improving the paper. Especially he is grateful for his help in choosing appropriate linear forms in the proof of Theorem 2.

REFERENCES

[1] BUGEAUD, Y.—CORVAJA, P.—ZANNIER, U.: *An upper bound for the* G. C. D. *of* $a^n - 1$ *and* $b^n - 1$, Math. Z. (To appear).

[2] CORVAJA, P.—ZANNIER, U.: *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) **9** (1998), 317–332.

[3] CORVAJA, P.—ZANNIER, U.: *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), 431–451.

[4] EVERTSE, J.-H.: *An improvement of the Quantitative Subspace Theorem*, Compositio Math. **101** (1996), 225–311.

[5] VAN DER POORTEN, A. J.: *Some facts that should be better known, especially about rational functions.* In: Number Theory and Applications. Proc. NATO ASI, Banff/Can. 1988. NATO ASI Ser., Ser. C 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 497–528.

[6] VAN DER POORTEN, A. J.: *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1998), 97–102.

[7] SCHMIDT, W. M.: *Diophantine Approximation.* Lecture Notes in Math. 785, Springer Verlag, Berlin-Heidelberg-New York, 1980.

[8] SCHMIDT, W. M.: *Diophantine Approximations and Diophantine Equations.* Lecture Notes in Math. 1467, Springer Verlag, Berlin, 1991.

[9] SCHMIDT, W. M.: *The zero multiplicity of linear recurrence sequences*, Acta Math. **182** (1999), 243–282.

Received June 14, 2002

Institut für Mathematik
TU Graz
Steyrergasse 30
A-8010 Graz
AUSTRIA

E-mail: clemens.fuchs@tugraz.at