DIOPHANTINE PROBLEMS WITH LINEAR RECURRENCES VIA THE SUBSPACE THEOREM

CLEMENS FUCHS*

ABSTRACT. In this paper we give an overview over recent developments (initiated by P. Corvaja and U. Zannier in [3]) on Diophantine problems where linear recurring sequences are involved and which were solved by using W.M. Schmidt's Subspace Theorem.

Moreover, as a new application, we show: 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 rational numbers and where $\alpha_1 > \ldots \alpha_t > 0, \beta_1 > \ldots > \beta_s > 0$ are integers with $\alpha_1, \alpha_2 \cdots \alpha_t \beta_1 \cdots \beta_s$ coprime, and let $\epsilon > 0$. Then, we have

$$\text{G.C.D.}(G_n, H_n) < \exp(\epsilon n)$$

for all n large enough.

1. INTRODUCTION

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

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

It is well known that G_n admits an analytic representation, namely for $n \geq 0$

$$G_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{2}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_t$ are the distinct roots of the corresponding characteristic polynomial

$$X^k - A_1 X^{k-1} - \cdots - A_k \tag{3}$$

and 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: $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$.

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

For the sake of simplicity we shall often restrict ourselves to linear recurring sequences (G_n), where all roots of the characteristic polynomial of (G_n) are simple, which means that

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

Date: April 25, 2005.

*This work was supported by the Austrian Science Foundation FWF, grants S8307-MAT and J2407-N12.

2000 *Mathematics Subject Classification:* 11D45,11D61.

for some $c_i, \alpha_i \in \mathbb{C}$. In this case we refer to G_n as to a power sums. The α_i are called the roots and the c_i are called the coefficients of the power sums G_n. If we restrict the roots to come from a multiplicative semigroup $A \subset \mathbb{C}$, then we let $\mathcal{E}_A$ denote to 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.

We need some information about the structure of the ring of power sums $\mathcal{E}_{\mathbb{Z}}^+$ introduced above. In fact, if e.g. 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 [25]) 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 $n \mapsto \gamma_i^n$. Hence, it is easy to decide on arithmetic properties of power sums in the ring of power sums, e.g. whether (G_n) is some q-th power in $\mathcal{E}_A$ or whether (G_n) and (H_n) are coprime (as power sums). This will be important for the results stated below.

Diophantine problems involving linear recurrences (or power sums) have been widely investigated and have a long tradition. However, a new development was started in 1998 by P. Corvaja and U. Zannier, who used the celebrated Subspace Theorem due to W.M. Schmidt to obtain new results. The Subspace Theorem has long been known to be crucial in the investigation of recurrence sequences, but somewhat surprisingly the results collected in this paper have not appeared before that time.

It is the aim of the present paper to give an overview over these results and how they are deduced from the Subspace Theorem. This will be done by first stating an appropriate version of the result and afterward giving a brief sketch of the proof. Of course we will concentrate on the results where the author was involved (his work on it started with [12]). Moreover, we will also show a new result in this direction concerning the G.C.D. of two power sums both with arbitrarily large order.

Before we start with the results it is worth to spend a few more words on the Subspace Theorem: we begin with the most simple statement of the Subspace Theorem which was proved in 1972 and which is a generalisation to higher dimensions of Roth's famous theorem, which says that for a real algebraic number α and for every $\delta > 0$, the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\delta}},$$

has at most finitely many solutions in rational integers p, q.

Theorem 1 (Subspace Theorem, W.M. Schmidt)**.** *Suppose $L_1(\mathbf{x}), \dots, L_n(\mathbf{x})$ are linearly independent linear forms in $\mathbf{x} = (x_1, \dots, x_n)$ with algebraic coefficients. Given $\delta > 0$, there are finitely many proper linear subspaces $T_1, \dots, T_w$ of $\mathbb{R}^n$ such that every integer point $\mathbf{x} \neq \mathbf{0}$ with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \|\mathbf{x}\|^{-\delta},$$

where $\|\mathbf{x}\| := \max\{|x_i| : i = 1, \dots, n\}$, lies in one of these subspaces.

In 1989 Schmidt gave a quantification of this result by giving an explicit upper bound for the number of subspaces involved in the statement. Before we can state this result we introduce the notation of absolute values and heights in number fields.

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 $\sigma : K \hookrightarrow \mathbb{R}$;
(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 $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$;
(iii) $|x|_v = (N\wp)^{-\mathrm{ord}_\wp(x)/[K:\mathbb{Q}]}$ if v corresponds to the prime ideal $\wp$ of O_K.

Here $N\wp = \#(O_K/\wp)$ is the norm of $\wp$ and $\mathrm{ord}_\wp(x)$ the exponent of $\wp$ in the prime ideal decomposition of (x), with $\mathrm{ord}_\wp(0) := \infty$. 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*

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for } x \in K \backslash \{0\}. \tag{5}$$

We define the *K-height* of $x \in K$ to be

$$\mathcal{H}_K(x) = \prod_{v \in M_K} \max\{1, |x|_v\}.$$

Observe that $\mathcal{H}_\mathbb{Q}(x) = |x|$ (the usual absolute value) for $x \in \mathbb{Z}$ and that

$$\mathcal{H}_L(x) = \mathcal{H}_K(x)^{[L:K]},$$

for $x \in K$ and for a finite extension L of K.

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

$$|\mathbf{x}|_v = \max_{1 \le i \le n} |x_i|_v.$$

Now define

$$\mathcal{H}(\mathbf{x}) = \prod_{v \in M_K} \max\{1, |\mathbf{x}|_v\}.$$

Again, in the special cases $x \in \mathbb{Z}^n$, we have $\mathcal{H}(\mathbf{x}) = \|\mathbf{x}\|$. Moreover, we define another height H by taking Euclidean norms at the infinite places, namely

$$H(\mathbf{x}) = \prod_{v \in M_K} |\mathbf{x}|_{v,2},$$

where

$$|\mathbf{x}|_{v,2} = \left(\left(\sum_{i=1}^{n} |x_i|_v^2 \right)^{\frac{1}{2}} \right)^{d(v)} \qquad \text{for } v \text{ infinite,}$$
$$|\mathbf{x}|_{v,2} = |\mathbf{x}|_v \quad \text{for } v \text{ finite,}$$

and where $d(v) = \frac{1}{[K:\mathbb{Q}]}, \frac{2}{[K:\mathbb{Q}]}$ depending on whether v is real infinite or complex infinite, respectively.

Now Schmidt's quantitative Subspace Theorem is as follows: consider the inequality

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\det(L_1, \ldots, L_n)| \|\mathbf{x}\|^{-\delta}, \tag{6}$$

where $0 < \delta < 1$ and where $L_1, \ldots, L_n$ are linearly independent linear forms with coefficients in the number field K. For the set of solutions with

$$\mathbf{x} \in \mathbb{Z}^n, \quad \|\mathbf{x}\| \gg \max\{(n!)^{8/\delta}, H(L_1), \ldots, H(L_n)\},$$

where the height of a linear form is the height of its vector of coefficients, we have the conclusion of Theorem 1 with

$$w \leq \left[(2d)^{2^{26n}\delta^{-2}} \right],$$

where $d = [K : \mathbb{Q}]$.

Later on the Subspace Theorem (and also the quantification) was extended to p-adic numbers and number fields by H.P. Schlickewei. We also state one version of his result (which follows from Theorem 1D' in [28], page 178).

Theorem 2 (Subspace Theorem, Schlickewei)**.** *Let K be an algebraic number field and let $S \subset M_K$ be a finite set of absolute values which contains all the infinite ones. For $v \in S$, let $L_{1,v}, \ldots, L_{n,v}$ be n linearly independent linear forms in n variables with coefficients in K. Let $\delta > 0$ be given. Then the solutions of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v < \mathcal{H}(\mathbf{x})^{-\delta} \tag{7}$$

with $\mathbf{x} \in (O_K)^n$ and $\mathbf{x} \neq \mathbf{0}$ lie in finitely many proper subspaces of K^n.

Let us remark that the best version (concerning the dependancy on the parameters) of the quantitative Subspace Theorem is due to Evertse (cf. [8]). Recently, Evertse and Schlickewei proved a much more general result taking into account all algebraic numbers and not only those lying in a fixed number field (cf. [10, 9]).

Now we come back to Diophantine problems where linear recurrences are involved. The following results are well known and the most classical consequences of the Subspace Theorem (they are obtained by the fact that a recurrence is just a linear combination of a fixed number of S-units): let

(G_n) be a non-degenerate linear recurrence and assume that also $\alpha_1, \ldots, \alpha_t$ are not roots of unity. Denote by $N(a)$ for every complex number a the number of integers n with

$$G_n = a$$

(this number is called the a-multiplicity of (G_n)). From the Theorem of Skolem-Mahler-Lech (cf. [20]) it follows that then $N(a)$ is finite. Schlickewei [26] proved that if $\alpha_1, \ldots, \alpha_t$ and the coefficients of $P_1, \ldots, P_t$ generate an algebraic number field K of degree q, then for every $a \in K$ we have

$$N(a) \leq q^{6d^2} 2^{2^{28d!}}.$$

Recently, Schmidt proved that for arbitrary non-degenerate linear recurrences of complex numbers we have

$$N(0) \leq \exp(\exp(\exp(20d)))$$

(cf. [29, 30]). Moreover, Evertse, Schlickewei and Schmidt [11] proved for power sums (i.e. simple linear recurrences), where the coefficients and roots are non-zero complex numbers and where neither $\alpha_1, \ldots, \alpha_t$, nor any quotient α_i/α_j $(1 \leq i < j \leq t)$ is a root of unity, we have

$$N(a) \leq \exp\left((t+2)(6t)^{4t}\right)$$

for every $a \in \mathbb{C}$.

These results show that the Subspace Theorem is a major tool to consider Diophantine problems with linear recurrences.

The rest of the paper is organized as follows: in Section 2 we show how the Subspace Theorem can be used to solve the equation $G_n = y^q$ and generalisations as $f(G_n^{(1)}, \ldots, G_n^{(d)}, y) = 0$ for power sums. Moreover, we will consider generalisations of these results to the corresponding Diophantine inequalities. In Section 3 we will consider the equation $H_n = yG_n$ and study upper bounds for the G.C.D. of two power sums (G_n) and (H_n). In Section 4 we present a new result on the G.C.D. of two power sums and we will give a complete proof of this result in Section 5.

2. The equation $G_n = y^q$ and generalisations

First we deal with Diophantine equations, where linear recurring sequences are involved. Such equations were earlier investigated by several authors, e.g. in the special case

$$G_n = Ey^q, \quad E \in \mathbb{Z}\backslash\{0\} \tag{8}$$

including the question of how many squares are in classical sequences as the Fibonacci sequence. A survey on this equation can be found in [22, 23] and in more general form in [13, 17]. The first results have been proved just by using elementary and algebraic tools. Later, the results were obtained with the applications of lower bounds for linear forms in logarithms of algebraic numbers.

We mention here also Pisot's q-th root conjecture (cf. [24]), which states that if all the values of G_n are q-th powers in a given number field K, then G_n is identically a q-th power of a recurrence. This conjecture was finally verified by Zannier [32]. However, this result does not solve the question on the finiteness of the solutions of (8).

Corvaja and Zannier (cf. [3]) were able to attack this problem for power sums. They considered linear recurrences defined by

$$G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n, \tag{9}$$

where $t \geq 2, c_1, c_2, \ldots, c_t$ are non-zero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers. They used the Subspace Theorem to show that for every integer $q \geq 2$ the equation

$$G_n = y^q \tag{10}$$

has only finitely many solutions $(n, y) \in \mathbb{N}^2$ assuming that G_n is not identically a perfect qth power for all n in a suitable arithmetic progression. Observe that, as remarked in the Introduction, it is easy to decide effectively whether this is the case or not.

Tichy and the author [17] gave a quantitative version of the above result of Corvaja and Zannier by using the quantitative Subspace Theorem due to Evertse [8].

Theorem 3 (p. 12, [17])**.** *Let $(G_n) \in \mathcal{E}_{\mathbb{Z}}^+$ be a linear recurring sequence defined by (9) where $t \geq 2, c_1, c_2, \ldots, c_t$ are nonzero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers and such that for given $q \geq 2$ there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$. Then the number of solutions $(n, y) \in \mathbb{N}^2$ of the equation*

$$G_n = y^q$$

is finite and can be bounded above by an explicitly computable number depending on $q, c_1, c_2, \ldots, c_t, \alpha_1, \ldots, \alpha_t$.

Sketch of the Proof: We approximate the quantity $G_n^{1/q}$ by defining

$$H_m := (c_1\alpha_1^r)^{1/q} \cdot \alpha_1^m \cdot \left[1 + \sum_{j=1}^{R} \binom{1/q}{j} \cdot \left(\sum_{i=2}^{t} \frac{c_i\alpha_i^{mq+r}}{c_1\alpha_1^{mq+r}}\right)^j\right],$$

where $R \geq 1$ and where $n = mq + r$, $n \in \mathbb{N}$, $r \in \{0, \ldots, q-1\}$. This quantity is obtained by using the binomial series for expanding $G_n^{1/q}$ after putting first out the dominant root α_1 and by truncating this series at the index R. We write

$$H_m = \sum_{i=1}^{h} d_i \left(\frac{e_i}{b}\right)^m,$$

where $d_i \in \mathbb{Q}\left((c_1\alpha_1^r)^{1/q}\right)^*$, e_i, b are integers, $b > 0$, and the e_i/b are nonzero distinct rational numbers. We have obtained an approximation for the solutions y_{mq+r} as linear combination of S-units for a finite set S of absolute values which we define in a second. From this we can construct a small linear form with respect to the usual infinite absolute value. This will always be our main strategy.

Define the linear forms $L_{i,v}$ for $v \in S = \{\infty \text{ and primes dividing } e_i \text{ or } b\}$ and $i = 1, \dots, h$ as follows:

$$L_{0,\infty} := X_0 - \sum_{i=1}^{h} d_i X_i \quad \text{and} \quad L_{i,v} := X_i$$

for $(i, v) \neq (0, \infty)$. Applying the Subspace Theorem (Theorem 2) now yields the result by a standard argument (see also the end of the proof in Section 5). □

Later on, Corvaja and Zannier [4] generalized their result (in fact for power sums defined over $\mathbb{Q}$ this result was already contained in [3]). Let K be an algebraic number field and let (G_n) be a non-degenerate linear recurring sequence defined by (4) where $t \geq 2, c_i$ are non-zero elements of K for all $i = 2, \dots, t$ and where $\alpha_1, \dots, \alpha_t$ are elements of K with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \dots, t$. Let $f(x, y) \in K[x, y]$ be monic in y and suppose that there do not exist non-zero algebraic numbers d_j, β_j for $j = 1, \dots, k$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j \beta_j^n\right) = 0 \tag{11}$$

for all n in an arithmetic progression. Then the number of solutions $(n, y) \in \mathbb{N} \times K$ of the equation

$$f(G_n, y) = 0 \tag{12}$$

is finite. The author [13] gave a quantitative version of this result, which is a little bit more general in the assumptions.

Theorem 4 (p. 236, [13])**.** *Let K be an algebraic number field and let (G_n) be a linear recurring sequence defined by*

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a non-zero element of K, $P_i(x) \in K[x]$ for all $i = 2, \dots, t$ and where $\alpha_1, \dots, \alpha_t$ are elements of K with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \dots, t$. Let $f(x, y) \in K[x, y]$ be monic in y and suppose that there do not exist non-zero algebraic numbers β_j and polynomials $d_j(n) \in \bar{K}[n]$ for $j = 1, \dots, k$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j(n) \beta_j^n\right) = 0$$

for all n in an arithmetic progression. Then the number of solutions $(n, y) \in \mathbb{N} \times K$ of the equation

$$f(G_n, y) = 0$$

is finite and can be bounded by an explicitly computable number C depending on f and on the coefficients and the initial values of the recurrence.

Sketch of the Proof: We work only in the case $|\alpha_1| > 1$ and consider the Puiseux expansion at $x = \infty$ of the solution $y = y(x)$ of $f(x, y) = 0$.

Now by Puiseux's Theorem we can conclude that

$$f(x, y) = \prod_{j,i} (y - y_{ij}),$$

where

$$y_{ij} = \sum_{k=v_i}^{\infty} a_{ik} \zeta^{jk} \left(\frac{1}{x}\right)^{\frac{k}{e_i}},$$

for $j = 0, \dots, e_i - 1$, $i = 1, 2, \dots, r$. Therefore for each solution (n, y_n) of (12) we get

$$y_n = \sum_{k=v}^{\infty} \beta_k G_n^{-\frac{k}{e}}, \tag{13}$$

for some v, e and β_k, which lie in a fixed finite extension of K.

We have the binomial expansion

$$G_n^{-\frac{k}{e}} = \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right)^r,$$

for some choice of the eth roots of λ_1 and α_1. Thus we can approximate y_n by a finite sum extracted from the Puiseux expansion (13), namely by

$$H_n := \sum_{k=v}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{H} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right)^r,$$

where $H \geq 1$ is an integer to be chosen later.

As before this leads to one small linear form with respect to the usual absolute value. All other linear forms are again the trivial projections. They are small because the expression above is again a linear combination of S-units. The result follows from the Subspace Theorem. □

Scremin [31] proved the following result which is related to what we consider here (in fact it is a consequence on his related result on the Diophantine inequality which we will mention below). Let $f(x, y) \in \overline{\mathbb{Q}}[x, y]$ be monic in y, absolutely irreducible and of degree $d \geq 2$ in y; let $g(n) \in \mathbb{Z}[x]$ be a non constant polynomial; let $G_n \in \overline{\mathbb{Q}}\mathcal{E}_{\mathbb{Z}}$ not constant. Then the equation

$$f(G_n, y) = g(n)$$

has only finitely many solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$.

Recently, Scremin and the author [15] generalised these results to the equation

$$G_n^{(0)} y^d + \ldots + G_n^{(d-1)} y + G_n^{(d)} = 0. \tag{14}$$

First we need some notation. Let $d \geq 2$ be an integer and let $G_n^{(0)}, \ldots, G_n^{(d)} \in \overline{\mathbb{Q}}\mathcal{E}_{\mathbb{Z}}^+$, i.e. we have

$$\begin{aligned} G_n^{(0)} &= a_1^{(0)} \alpha_1^{(0)^n} + a_2^{(0)} \alpha_2^{(0)^n} + \ldots + a_{t^{(0)}}^{(0)} \alpha_{t^{(0)}}^{(0)^n}, \\ &\vdots \\ G_n^{(d)} &= a_1^{(d)} \alpha_1^{(d)^n} + a_2^{(d)} \alpha_2^{(d)^n} + \ldots + a_{t^{(d)}}^{(d)} \alpha_{t^{(d)}}^{(d)^n}, \end{aligned}$$

where $a_i^{(j)}$ are algebraic and $\alpha_i^{(j)}$ are positive integers such that $\alpha_1^{(j)} > \alpha_2^{(j)} > \ldots > \alpha_{t^{(j)}}^{(j)}$ for all $i = 1, \ldots t^{(j)}$ and $j = 0, \ldots, d$.

Let $f(x_0, \ldots, x_d, y) = x_0 y^d + \ldots + x_{d-1} y + x_d$. So the above equation becomes

$$f(G_n^{(0)}, \ldots, G_n^{(d)}, y) = 0.$$

We will show how to this equation another equation in some normal form can be associated. First, we set (for a positive real determination of the roots)

$$\alpha := \max_{i=1,\ldots,d} \left(\frac{\alpha_1^{(i)}}{{\alpha_1^{(0)}}^{\frac{d-i}{d}}} \right)^{\frac{1}{i}}.$$

Moreover, let

$$y = \frac{\alpha^n}{{\alpha_1^{(0)}}^{\frac{n}{d}}} z.$$

Then consider

$$\frac{1}{\alpha^{dn}} f\left(G_n^{(0)}, \ldots, G_n^{(d)}, \frac{\alpha^n}{{\alpha_1^{(0)}}^{\frac{n}{d}}} z \right). \tag{15}$$

This is a polynomial in z with coefficients in $\overline{\mathbb{Q}}\mathcal{E}_A$, where A is the multiplicative group generated by

$$\alpha, {\alpha_1^{(0)}}^{\frac{1}{d}} \text{ and the roots of } G_n^{(0)}, \ldots, G_n^{(d)},$$

i.e. the coefficients of this polynomial are again power sums. Observe that all the roots which appear in these power sums are ≤ 1, because of our construction and that one of the roots which appears as coefficient of z^d is 1. Let $\gamma_1, \ldots, \gamma_r$ denote the different roots of these power sums (the coefficients of (15) as a polynomial in z), which are strictly less than 1. We identify the

expressions γ_i^n in (15) by a new variable x_i. Therefore we get a polynomial (linear in $x_1, \ldots, x_r$) $g(x_1, \ldots, x_r, z) \in \overline{\mathbb{Q}}[x_1, \ldots, x_r, z]$ such that

$$g(\gamma_1^n, \ldots, \gamma_r^n, z) = \frac{1}{\alpha^{dn}} f\left(G_n^{(0)}, \ldots, G_n^{(d)}, \frac{\alpha^n}{{\alpha_1^{(0)}}^{\frac{n}{d}}} z\right).$$

This polynomial is some kind of normal form for our equation under consideration. We denote by $D(G_n^{(1)}, \ldots, G_n^{(d)})$ the discriminant of g with respect to z evaluated at $(0, \ldots, 0)$.

We are now able to formulate our next result, which states that the equation (14) has only finitely many solutions in integers, apart from "trivial" cases which can be classified and which come from functional identities in the ring of power sums.

Theorem 5 (p. 154, [15]). *Let $d \geq 2$ and let $G_n^{(0)}, \ldots, G_n^{(d)} \in \overline{\mathbb{Q}}\mathcal{E}_{\mathbb{Z}}^+$. Assume that*

$$D(G_n^{(1)}, \ldots, G_n^{(d)}) \neq 0. \tag{16}$$

Then there exist finitely many recurrences $H_n^{(1)}, \ldots, H_n^{(s)}$ with algebraic coefficients and algebraic roots, arithmetic progressions $\mathcal{P}_1, \ldots, \mathcal{P}_s$, and a finite set $\mathcal{N}$ of integers, such that for the set S of solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$ of the equation

$$f(G_n^{(0)}, \ldots, G_n^{(d)}, y) = G_n^{(0)} y^d + \ldots + G_n^{(d-1)} y + G_n^{(d)} = 0$$

we have

$$S = \bigcup_{i=1}^{s} \{(n, H_n^{(i)}) \,:\, n \in \mathcal{P}_i\} \cup \{(n, y) \,:\, n \in \mathcal{N}, y \in \mathbb{Z}\} \cup M,$$

where M is a finite set.

Sketch of the Proof: The solutions (n, y_n) of the equation give rise to solutions (n, z_n) of the equation $g(\gamma_1^n, \ldots, \gamma_r^n, z_n) = 0$. We consider infinitely many solutions (n, z_n) where $n \in \Sigma$ and Σ is a sequence of positive integers. From the construction of g it follows that the sequence (z_n) must be bounded and therefore lie in some neighbourhood of the solutions of

$$g(0, \ldots, 0, z) = 0,$$

at least if n is large enough.

By a suitable version of the Implicit Function Theorem we conclude

$$z = z_0 + \sum_{|\mathbf{i}|>0} a_{\mathbf{i}} x_1^{i_1} \ldots x_r^{i_r}$$

where $\mathbf{i} = (i_1, \ldots, i_r)$, $|\mathbf{i}| := |i_1 + \ldots + i_r|$ and with $a_{\mathbf{i}} \in \overline{\mathbb{Q}}$, where z_0 satisfies $g(0, \ldots, 0, z_0) = 0$.

Therefore for each solution (n, z_n) we get

$$z_n = z_0 + \sum_{|\mathbf{i}|>0} a_{\mathbf{i}} \gamma_1^{i_1 n} \dots \gamma_r^{i_r n},$$

for some z_0 and coefficients $a_{\mathbf{i}}$, and if n is large enough. Next we approximate z_n by

$$V_n := z_0 + \sum_{0<|\mathbf{i}|<H} a_{\mathbf{i}} \gamma_1^{i_1 n} \dots \gamma_r^{i_r n}.$$

So, again we have an approximation for the solutions as a linear combination of S-units for a certain set S, which in turn leads to a small linear form. The result follows as before by applying the Subspace Theorem. □

Now we turn our interest to Diophantine inequalities. Corvaja and Zannier proved in their paper [3] in 1998 also the following result: let $G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n$, where $t \geq 2, c_1, c_2, \dots, c_t$ are non-zero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers. Then for fixed $\epsilon > 0$ and every integer $q \geq 2$ there exist power sums $H_n^{(1)}, \dots, H_n^{(s)} \in \overline{\mathbb{Q}}\mathcal{E}_{\overline{\mathbb{Q}}}$ such that all solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$ of the Diophantine inequality

$$|y^q - G_n| \ll |G_n|^{1-\frac{1}{d}-\epsilon}$$

apart from finitely many, satisfy $y = H_n^{(i)}$ for a certain $i = 1, \dots, s$. As an immediate consequence, for every $q \geq 2$ the equation $G_n = y^q$ has only finitely many solutions, if we suppose that α_1, α_2 are coprime. It is easy to see that the upper bound is best possible; if we remove ϵ then the conclusion is no longer true.

Scremin [31] studied lower bounds for the quantity $|f(G_n, y)|$, where $f(x, y) \in \overline{\mathbb{Q}}[x, y]$ is absolutely irreducible, monic and of degree $d \geq 2$ in y. He proved the following generalisation of the result of Corvaja and Zannier, namely that for $G_n \in \overline{\mathbb{Q}}\mathcal{E}_{\mathbb{Z}}$ and for fixed $\epsilon > 0$ there exists a finite set of power sums $H_n^{(1)}, \dots, H_n^{(s)} \in \mathcal{E}_{\mathbb{Z}}^+$ such that every solution $(n, y) \in \mathbb{N} \times \mathbb{Z}$, apart from finitely many, of the Diophantine inequality

$$\left| f(G_n, y) \right| < \left| \frac{\partial f}{\partial y}(G_n, y) \right| \cdot |G_n|^{-\epsilon}$$

satisfies $y = H_n^{(i)}$ for a certain $i = 1, \dots, s$.

Scremin and the author again went a step further and considered a generalisation of the equation (14) to the case of inequalities. They proved:

Theorem 6 (p. 168, [16]). *Let $d \geq 2$, $G_n^{(1)}, \dots, G_n^{(d)} \in \overline{\mathbb{Q}}\mathcal{E}_{\mathbb{Z}}^+$. Let $f(x_1, \dots, x_d, y)$ be monic in y. Assume that*

$$D(G_n^{(1)}, \dots, G_n^{(d)}) \neq 0.$$

Finally, let $\epsilon > 0$. Then there exist finitely many recurrences $H_n^{(1)}, \dots, H_n^{(s)} \in \overline{\mathbb{Q}}\mathcal{E}_{\overline{\mathbb{Q}}}$ such that all but finitely many solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$ of the Diophantine inequality

$$\left| f(G_n^{(1)}, \dots, G_n^{(d)}, y) \right| < \alpha^{n(d-1-\epsilon)},$$

have $y = H_n^{(i)}$ for some $i = 1, \dots, s$. Moreover, the set of natural numbers n such that (n, y) is a solution of the inequality is the union of a finite set and a finite number of arithmetic progressions.

Sketch of the Proof: Since $D(G_n^{(1)}, \dots, G_n^{(d)}) \neq 0$, we conclude by the Implicit Function Theorem that

$$g(x_1, \dots, x_r, z) = (z - \varphi_1) \cdot \ldots \cdot (z - \varphi_d)$$

with

$$\begin{aligned} \varphi_1(x_1, \dots, x_r) &= \sum_{|\mathbf{i}| \geq 0} a_{\mathbf{i},1} x_1^{i_1} \cdots x_r^{i_r}, \\ &\vdots \\ \varphi_d(x_1, \dots, x_r) &= \sum_{|\mathbf{i}| \geq 0} a_{\mathbf{i},d} x_1^{i_1} \cdots x_r^{i_r} \end{aligned}$$

where $a_{\mathbf{i},j} \in \overline{\mathbb{Q}}$, $z_i := a_{\mathbf{0},i}, i = 1, \dots, d$ satisfy $g(0, \dots, 0, z_i) = 0$. For each solution (n, z) we get that

$$z - \varphi_j(\gamma_1^n, \dots, \gamma_r^n) = z - \sum_{|\mathbf{i}| \geq 0} a_{\mathbf{i},j} \gamma_1^{i_1 n} \cdots \gamma_r^{i_r n}$$

is small for some $j = 1, \dots, d$ and if n is large enough. Here we need that $|z| \leq c\alpha^n$ for some constant c. All solutions which do not satisfy this trivially fulfill our conclusion (see [16, Proposition 1]).

We consider the sets for $j = 1, \dots, d$

$$M_j = \left\{ (n, z) \, : \, |z - \varphi_j| = \min_{i=1,\dots,d} \{|z - \varphi_i|\} \right\}.$$

Without loss of generality, we assume $(n, z) \in M_1$. For $(n, z) \in M_1$ we now consider

$$\left| g(\gamma_1^n, \dots, \gamma_r^n, z) \right| = |z - \varphi_1| \, |z - \varphi_2| \, \cdots \, |z - \varphi_d|.$$

First we calculate the contribution of the "big" terms. We have

$$|z - \varphi_2| \cdots |z - \varphi_d| \geq \left(\frac{1}{3} \min_{i=2,\dots,d} \{|z_i - z_1|\} \right)^{d-1}.$$

Now we consider the small term $|z-\varphi_1|$. We are going to approximate z by a finite sum extracted from

$$\begin{aligned}\varphi_1 &= z_0+\sum_{|\mathbf{i}|>0} a_{\mathbf{i},1}\gamma_1^{i_1 n}\cdots\gamma_r^{i_r n} = \\ &= z_0+\sum_{0<|\mathbf{i}|\le H} a_{\mathbf{i},1}\gamma_1^{i_1 n}\cdots\gamma_r^{i_r n}+\mathcal{O}\left(\gamma^n\right).\end{aligned}$$

We define

$$V_n := z_0+\sum_{0<|\mathbf{i}|\le H} a_{\mathbf{i},1}\gamma_1^{i_1 n}\cdots\gamma_r^{i_r n},$$

and use the Subspace Theorem to show

$$|z-\varphi_1| > C_1\alpha^{-C_2 n},$$

where C_1, C_2 are certain constants, for all n outside of finitely many subspaces. From this the result follows in the usual way. □

Observe that in [16] we did not use the Subspace Theorem directly to get the last result. Instead we used a technical result by Corvaja and Zannier [5, Theorem 4] which is itself a consequence of the Subspace Theorem.

The main restriction in all these results is that we have to assume the existence of a simple dominant root. Of course we conjecture that the results are true without this assumption. This is the major open problem in this subject area.

3. The equation $H_n = yG_n$ and the G.C.D. of G_n, H_n

At first sight this case seems to be much easier then the equations studied in the previous section. In fact it is possible to completely solve this equation. Also other more general questions, as on the G.C.D. of G_n, H_n, are of interest and can be answered (at least partially).

In order to motivate what is going on in this case we mention the so-called Hadamard Quotient theorem (proved by van der Poorten, cf. [25]), 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 the Subspace Theorem a stronger result. They proved that if $(G_n), (H_n)$ are as above and if $H_n = yG_n$ has infinitely many solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$ then there exists a recurring sequence (I_n) such that $H_n = G_n \cdot I_n$ for all $n \in \mathbb{N}$. Thus again, the infinitude of solutions can be explained by a function relation in the ring of

power sums. This result can be found in [3].

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. [4]). They proved:

Theorem 7 (Corvaja and Zannier)**.** *Let $(G_n), (H_n)$ be linear recurrences and let $\mathcal{R}$ be a finitely generated subring of $\mathbb{C}$. Assume that for infinitely many $n \in \mathbb{N}$, we have $G_n \neq 0$ and $H_n/G_n \in \mathcal{R}$. Then there exist a nonzero polynomial $P(X) \in \mathbb{C}[X]$ and positive integers q, r such that both sequences $n \mapsto P(n)H_{qn+r}/G_{qn+r}$ and $n \mapsto G_{qn+r}/P(n)$ are linear recurrences.*

The main problem in the proof was to get rid of the notorious dominant root condition and this was done by an ingenious application of the Subspace Theorem. They achieved this in the following way: first it is still possible to approximate H_n/G_n by using simultaneously all the roots with maximal absolute value; then they constructed several other small linear forms, out from the first one by multiplying the given small linear form by suitable powers of monomials in the dominant roots. We do not go more into details, since the proof of our original result in this paper follows essentially this line of proof, so we refer to Section 5.

Bugeaud, Corvaja and Zannier [1] used the Subspace Theorem 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

$$\text{G.C.D.}(a^n - 1, b^n - 1) \ll a^{\frac{n}{2}}. \tag{17}$$

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 $\epsilon > 0$. Then, provided n is sufficiently large, we have

$$\text{G.C.D.}(a^n - 1, b^n - 1) < \exp(\epsilon n). \tag{18}$$

This result is remarkable, especially because it was the first time that in the proof not only one but several small linear forms were used to which the Subspace Theorem was applied afterwords (see the sketch of the proof of Theorem 9).

Bugeaud, Corvaja and Zannier remarked that their method holds in a more general context. Taking this into account the author [14] proved the following result:

Theorem 8 (p. 23, [14])**.** *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

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

for all n aside of a finite set of exceptions, which 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, $i = 1, \ldots, t, j = 1, \ldots, s$.

Sketch of the Proof: 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. We show that

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

can hold for $n > C_1$ only for a finite number of n, whose cardinality can be bounded by C_2. From this the result will follow.

We expand G_n^{-1} and approximate $z(n)$ by the power sum

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

where $h \geq 1$ is an integer. Now an application of the Subspace Theorem proves the result. □

Moreover, we get the following better result for "coprime" power sums (G_n) and (H_n) where (H_n) is of arbitrary large order:

Theorem 9 (p. 25, [14])**.** *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 $\alpha > 1, \beta_1 > \cdots > \beta_s > 0$ are integers with $\alpha, \beta_1 \beta_2 \cdots \beta_s$ coprime. Furthermore, let $\epsilon > 0$. Then, provided $n > C_1$, we have*

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

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 $c_i, d_j, \alpha, \beta_j$, $i = 1, 2, j = 1, \ldots, s$ and ϵ.

Sketch of the Proof: We fix a k and let

$$\mathcal{J} = \{\mathbf{j} = (j_1, \ldots, j_s) \,:\, j_1 + \ldots + j_s = k\}$$

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

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

We write

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

where $\mathfrak{c}_{\mathbf{j},n}, \mathfrak{d}_n$ are integers.

Now we define

$$\phi_{\mathbf{j}}(n) := z_{\mathbf{j}}(n) - H_{\mathbf{j},n} \cdot \sum_{i=1}^{h} (-1)^{i-1} \frac{c_2^{i-1}}{c_1^i} \alpha^{-ni} =$$

$$= z_{\mathbf{j}}(n) - \beta_1^{j_1 n} \cdots \beta_s^{j_s n} \sum_{i=1}^{h} \sum_{l=1}^{s} (-1)^{i-1} d_l \frac{c_2^{i-1}}{c_1^i} \beta_l^n \alpha^{-ni},$$

for every index $\mathbf{j} = (j_1, \ldots, j_s)$ with $j_1 + \ldots + j_s = k$. We apply the Subspace Theorem by considering several "small" linear forms coming from the above approximation of the values $z_{\mathbf{j}}(n)$ for all $\mathbf{j} \in \mathcal{J}$ with k large enough (the above approximations were obtained by expanding G_n^{-1} in the definition of $z_{\mathbf{j}}(n)$ above).

Finally, this second parameter k can be chosen in such a way, that the theorem follows by an application of the Subspace Theorem. □

Let us mention some very recent generalisations of these type of results. Corvaja and Zannier proved (in [6]) that for every fixed $\epsilon > 0$ the inequality

$$\text{G.C.D.}(u-1, v-1) < (\max\{|u|, |v|\})^{\epsilon}$$

holds for all pairs of multiplicatively independent S-units $u, v \in \mathbb{Z}$ for a finite set of absolute values including the infinite ones. We remark that this result was used to confirm a conjecture of Győry, Sárközy and Stewart from [19] (for further results in this direction see also [18, 2]). In [7] they generalised this statement for other pairs of rational functions then $u-1, v-1$ and gave a reformulation in the language of heights in order to get an extension to number fields. Their results imply that if $p(x,y), q(x,y) \in \overline{\mathbb{Q}}[x,y]$ are non-constant coprime polynomials and suppose that not both of them vanish at $(0,0)$ and let a, b be multiplicatively independent integers. Then for every $\epsilon > 0$ we have that

$$\text{G.C.D.}(p(a^n, b^n), q(a^n, b^n)) < \exp(\epsilon n)$$

for all n large enough.

In [21] Luca studied the G.C.D.$(u-1, v-1)$ where $u, v \in \mathbb{Z}$ are "near" S-units. His result implies that if $f(x), f_1(x), g(x), g_1(x)$ are non-zero polynomials with integer coefficients and a, b are multiplicatively independent integers as before, then for every $\epsilon > 0$ the inequality

$$\text{G.C.D.}(f(n)a^n + g(n), f_1(n)b^n + g_1(n)) < \exp(\epsilon n)$$

holds for all n large enough.

Both results were obtained by using the ideas from [1].

4. New result on the G.C.D.

The aim of this section is to present a new result which is a generalisation of Theorem 9 to the case where also G_n is a power sums of arbitrarily large order. The proof uses again the Subspace Theorem but in a more involved

way with several nontrivial small linear forms (also with respect to different absolute values).

The main result is the following theorem:

Theorem 10. *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 rational numbers and where $\alpha_1 > \cdots > \alpha_t > 0, \beta_1 > \cdots > \beta_s > 0$ are integers with $\alpha_1, \alpha_2 \cdots \alpha_t \beta_1 \cdots \beta_s$ coprime. Furthermore, let $\epsilon > 0$. Then, we have*

$$\text{G.C.D.}(G_n, H_n) < \exp(\epsilon n)$$

for all n large enough.

This theorem includes examples as

$$\text{G.C.D.}(2^n + 3^n, 5^n + 7^n) < \exp(\epsilon n),$$

for all n large enough, which seem not to be covered by the previous results mentioned above.

Remark 1. The condition $\alpha_1, \alpha_2 \cdots \alpha_t \beta_1 \cdots \beta_s$ coprime assure that the sequences (G_n) and (H_n) are coprime as elements in the ring of power sums $\mathcal{E}_{\mathbb{Z}}^+$.

Remark 2. In the proof we use once again (as in the proof of [14, Theorem 2]) several small linear forms for the application of the Subspace Theorem. In fact the proof uses even more from the proof by Corvaja and Zannier of the main result in [4]. Moreover, we use nontrivial linear forms not only for one absolute value, but for several absolute values.

Remark 3. Of course it is possible, by using quantitative versions of the Subspace Theorem (e.g. due to Evertse [8]), to give the following more precise statement. There are explicitly computable positive constants C_1, C_2 such that the claimed inequality is true for all $n > C_1$ with finitely many exceptions whose cardinality can be bounded by C_2.

5. Proof of Theorem 10

For the reader's convenience we state a version of the Subspace Theorem due to Schlickewei in a simplified version which is enough for our application:

Proposition 1 (Subspace Theorem)**.** *Let S be a finite set of absolute values of $\mathbb{Q}$, including the infinite one and normalized in the usual way (i.e. $|p|_v = p^{-1}$ if $v|p$). Extend each $v \in S$ to $\overline{\mathbb{Q}}$ in some way. For $v \in S$ let $L_{1,v}, \ldots, L_{N,v}$ be N linearly independent linear forms in N variables with algebraic coefficients and let $\delta > 0$. Then the solutions $\mathbf{x} := (x_1, \ldots, x_N) \in \mathbb{Z}^N$*

to the inequality

$$\prod_{v\in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x})|_v < \|\mathbf{x}\|^{-\delta},$$

where $\|\mathbf{x}\| := \max\{|x_i| : i = 1,\dots,N\}$*, are contained in finitely many proper subspaces of* $\mathbb{Q}^N$*.*

This theorem follows from [28, Theorem 1E, p. 178] (but a complete proof requires also [27]).

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

First observe that by [14, Lemma 2] it follows that $G_n = 0$ can only hold for finitely many n. So, we will exclude this case in the further considerations.

We now 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. Thus we have

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

We suppose that

$$\mathfrak{d}_n \le \alpha_1^{(1-\epsilon)n} \tag{19}$$

for infinitely many n and we proceed to derive a contradiction which clearly proves

$$\text{G.C.D.}(G_n, H_n) \le C_1\alpha_1^{\epsilon n}$$

from which our claim follows.

Now, let us denote by $p_1,\dots,p_r$ the different prime divisors of α_1. By our assumption that α_1 is coprime to $\alpha_2\cdots\alpha_t\beta_1\cdots\beta_s$ it follows that

$$1 = |\alpha_2|_{p_i} = \ldots = |\alpha_t|_{p_i} = |\beta_1|_{p_i} = \ldots = |\beta_s|_{p_i} > |\alpha_1|_{p_i} \tag{20}$$

for all $i = 1,\dots,r$.

We fix a positive integer f and write

$$\begin{aligned}&(a_2\alpha_2^n + \ldots + a_t\alpha_t^n)^f\\ &\quad = (G_n - a_1\alpha_1^n)^f = G_n\left(\sum_{i=0}^{f-1}\binom{f}{i}G_n^{f-1-i}(-1)^i a_1^i\alpha_1^{in}\right) + (-1)^f a_1^f\alpha_1^{fn}.\end{aligned}$$

This implies

$$\prod_{i=1}^{r}\left|(a_2\alpha_2^n + \ldots + a_t\alpha_t^n)^f\, z_n - H_n\sum_{i=0}^{f-1}\binom{f}{i}G_n^{f-1-i}(-1)^i a_1^i\alpha_1^{in}\right|_{p_i} \le C_2\alpha_1^{(1-f)n}.$$

Observe that it is clear that

$$\prod_{i=1}^{r} |z_n|_{p_i} \leq \prod_{i=1}^{r} |G_n|_{p_i}^{-1} \leq |G_n| \leq C_1 \alpha_1^n,$$

since by the product formula we have

$$\prod_{p \in \mathbb{P}} |x|_p \cdot |x| = 1 \Longrightarrow |x| = \prod_{p \in \mathbb{P}} |x|_p^{-1} \geq \prod_{i=1}^{r} |x|_{p_i}^{-1}$$

for all rational integers x.

We now fix two other positive integers h, k; later on we shall impose that f, h, k satisfy suitable inequalities.

Let us denote by $\mathcal{J} = \{\mathbf{j} = (i_2, \ldots, i_t, j_1, \ldots, j_s) \in \mathbb{N}^{t-1+s} \ : \ i_2 + \ldots + i_t \leq h, j_1 + \ldots + j_s \leq k\}$. If we write $\mathbf{j}_i$ we mean the i-th vector in $\mathcal{J}$ with respect to the lexicographical ordering. The cardinality of $\mathcal{J}$ is given by

$$M := |\mathcal{J}| = \begin{pmatrix} t-1+h \\ t-1 \end{pmatrix} \begin{pmatrix} s+k \\ s \end{pmatrix}.$$

For every $\mathbf{j} \in \mathcal{J}$ we consider the quantity

$$\begin{aligned} \phi_{\mathbf{j}}(n) \ := \ & (a_2 \alpha_2^n + \ldots + a_t \alpha_t^n)^f \, \alpha_2^{i_2 n} \cdots \alpha_t^{i_t n} \beta_1^{j_1 n} \cdots \beta_s^{j_s n} z_n \\ & - \alpha_2^{i_2 n} \cdots \alpha_t^{i_t n} \beta_1^{j_1 n} \cdots \beta_s^{j_s n} H_n \sum_{i=0}^{f-1} \binom{f}{i} G_n^{f-1-i} (-1)^i a_1^i \alpha_1^{in}. \end{aligned}$$

By the above inequality and (20) we have

$$\prod_{i=1}^{r} |\phi_{\mathbf{j}}(n)|_{p_i} \leq C_2 \alpha_1^{(1-f)n} \tag{21}$$

for all $\mathbf{j} \in \mathcal{J}$.

Now, let S be a set of absolute values of $\mathbb{Q}$ containing the infinite absolute value and all primes dividing α_1 or $\alpha_2 \cdots \alpha_t \beta_1 \cdots \beta_s$. Especially, it contains the primes $p_1, \ldots, p_r$. Moreover, we put

$$N_1 := \begin{pmatrix} t-1+f+h \\ t-1 \end{pmatrix} \begin{pmatrix} s+k \\ s \end{pmatrix}$$

and

$$N_2 := f \begin{pmatrix} t-1+f+h \\ t-1 \end{pmatrix} \begin{pmatrix} s+k+1 \\ s \end{pmatrix}.$$

Finally, set $N := N_1 + N_2$. Observe that N_1 denotes the number of possible quantities of the form

$$\alpha_2^{i_2} \cdots \alpha_t^{i_t} \beta_1^{j_1} \cdots \beta_s^{j_s} z_n$$

with $i_2 + \ldots + i_t \le f + h$ and $j_1 + \ldots + j_s \le k$, whereas N_2 denotes the number of possible different quantities of the form

$$\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_t^{i_t}\beta_1^{j_1}\cdots\beta_s^{j_s}$$

with $i_1 < f, i_2 + \ldots + i_t \le f + h, j_1 + \ldots + j_s \le k + 1$. In particular, we can write $\phi_{\mathbf{j}}(n)$ as a linear combination of at most N nonzero terms of the mentioned types. Let us choose an ordering (in such a way that the first N_1 terms are those quantities involving z_n) for the above quantities and denote the terms with $x_1(n), \ldots, x_{N_1}(n), x_{N_1+1} \ldots, x_N(n)$. Thus we can write

$$\phi_{\mathbf{j}}(n) = A_{\mathbf{j},1}x_1(n) + \ldots + A_{\mathbf{j},N}x_N(n)$$

for every $\mathbf{j} \in \mathcal{J}$.

We denote by

$$\mathbf{x}_n = \mathfrak{d}_n(x_1(n), \ldots, x_N(n)) \in \mathbb{Z}^{N_1+N_2}$$

(remember that $\mathfrak{d}_n$ was the denominator of z_n).

We define for every $v \in S$, N linearly independent linear forms in $\mathbf{X} = (X_1, \ldots, X_N)$ as follows: for $i \le M < N_1$ and for all $j = 1, \ldots, r$ put

$$L_{i,p_j}(\mathbf{X}) = A_{\mathbf{j}_i,1}X_1 + \ldots + A_{\mathbf{j}_i,N}X_N;$$

for all other pairs $(j, v) \in \{1, \ldots, N\} \times S$ we set

$$L_{j,v}(\mathbf{X}) = X_j.$$

We want to apply the Subspace Theorem with this choice of the linear forms. Observe that for fixed $v \in S$ the linear forms $L_{1,v}, \ldots, L_{N,v}$ are linearly independent: this is clear for $v \ne p_j, j = 1, \ldots, r$ and for $v = p_j$ we have that

$$L_{i,p_j}(x_1(n), \ldots, x_N(n)) = \mathfrak{d}_n\phi_{\mathbf{j}_i}(n)$$

for $i \le M$. In order to prove that $L_{1,p_j}, \ldots, L_{M,p_j}, X_{M+1}, \ldots, X_N$ are linearly independent it suffices to show this for $L_{1,p_j}(x_1(n), \ldots, x_{N_1}(n), 0, \ldots, 0), \ldots, L_{M,p_j}(x_1(n), \ldots, x_{N_1}(n), 0, \ldots, 0)$. But in this case we have

$$\begin{aligned} &L_{i,p_j}(x_1(n), \ldots, x_{N_1}(n), 0, \ldots, 0) \\ &\quad = (a_2\alpha_2^n + \ldots + a_t\alpha_t^n)^f\,\alpha_2^{i_2 n}\cdots\alpha_t^{i_t n}\beta_1^{j_1 n}\cdots\beta_s^{j_s n}\mathfrak{c}_n, \end{aligned}$$

where $\mathbf{j}_i = (i_2, \ldots, i_t, j_1, \ldots, j_s) \in \mathcal{J}$. It is plain (again e.g. by [14, Lemma 2]) that a linear relation of such quantities holds for at most finitely many n.

We now consider the double product defined by the previously defined linear forms and vectors, namely

$$\prod_{v\in S}\prod_{i=1}^{N} |L_{i,v}(\mathbf{x}_n)|_v\,. \tag{22}$$

This product can be rewritten as

$$\prod_{i=M+1}^{N}\prod_{v\in S}|L_{i,v}(\mathbf{x}_n)|_v\cdot\prod_{i=1}^{M}\prod_{v\in S\setminus\{p_1,\dots,p_r\}}|L_{i,v}(\mathbf{x}_n)|_v\cdot\prod_{i=1}^{M}\prod_{j=1}^{r}|L_{i,p_j}(\mathbf{x}_n)|_{p_j}.$$

We will first handle each of these double products separately.

First, we have for $i>N_1$ that

$$\prod_{v\in S}|L_{i,v}(\mathbf{x}_n)|_v=\prod_{v\in S}|\mathfrak{d}_n\alpha_1^{i_1n}\alpha_2^{i_2n}\cdots\alpha_t^{i_tn}\beta_1^{j_1n}\cdots\beta_s^{j_sn}|_v\le\mathfrak{d}_n,$$

where $i_1,i_2,\dots,i_t,j_1,\dots,j_s$ are suitable integers. Observe that we have used our choice of S and the product formula to obtain $\prod_{v\in S}|\alpha_1^{i_1n}\alpha_2^{i_2n}\cdots\alpha_t^{i_tn}\beta_1^{j_1n}\cdots\beta_s^{j_sn}|_v=1$. For $M<i\le N_1$ we have

$$\prod_{v\in S}|L_{i,v}(\mathbf{x}_n)|_v=\prod_{v\in S}|\mathfrak{c}_n\alpha_2^{i_2n}\cdots\alpha_t^{i_tn}\beta_1^{j_1n}\cdots\beta_s^{j_sn}|_v\le\mathfrak{c}_n\le H_n\le C_3\beta_1^n,$$

where we used the choice of S and the product formula once again.

Further, for $i\le M$ we have

$$\prod_{v\in S\setminus\{p_1,\dots,p_r\}}|L_{i,v}(\mathbf{x}_n)|_v=\prod_{v\in S\setminus\{p_1,\dots,p_r\}}|\mathfrak{c}_n|_v\le\mathfrak{c}_n\le H_n\le C_3\beta_1^n,$$

where we have used that $x_i(n)=\mathfrak{d}_n\alpha_2^{i_2n}\cdots\alpha_t^{i_tn}\beta_1^{j_1n}\cdots\beta_s^{j_sn}z_n$ and $\mathfrak{d}_nz_n=\mathfrak{c}_n$ (as also just before).

Finally, in view of (21), we have for $i\le M$ that

$$\prod_{j=1}^{r}|L_{i,p_j}(\mathbf{x}_n)|_{p_j}=\prod_{j=1}^{r}|\mathfrak{d}_n\phi_{\mathbf{j}_i}(n)|_{p_j}\le\prod_{j=1}^{r}|\phi_{\mathbf{j}_i}(n)|_{p_j}\le C_2\alpha_1^{(1-f)n}.$$

Observe that

$$\prod_{j=1}^{r}|\mathfrak{d}_n|_{p_j}\le 1,$$

since $\mathfrak{d}_n$ is an integer.

Plugging these estimates into (22), we finally obtain

$$\prod_{v\in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x}_n)|_v\le C_4\mathfrak{d}_n^{N_2}\beta_1^{nN_1}\alpha_1^{(1-f)Mn}.$$

Recall that we are assuming $\mathfrak{d}_n\le\alpha_1^{(1-\epsilon)n}$. Consequently,

$$\prod_{v\in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x}_n)|_v\le C_4\left(\alpha_1^{(1-\epsilon)N_2+N_1C_5+(1-f)M}\right)^n. \tag{23}$$

Now we choose k, f and at the end h to assure that the exponent of α_1 in this equation is < 0. Observe that

$$\begin{aligned}(24)\quad (1-\epsilon)N_2 + N_1C_5 + (1-f)M \\ = \quad (1-\epsilon)f\begin{pmatrix} t-1+f+h \\ t-1 \end{pmatrix}\begin{pmatrix} s+k+1 \\ s \end{pmatrix} \\ -f\begin{pmatrix} t-1+h \\ t-1 \end{pmatrix}\begin{pmatrix} s+k \\ s \end{pmatrix} \\ +\left[C_5\begin{pmatrix} t-1+f+h \\ t-1 \end{pmatrix}+\begin{pmatrix} t-1+h \\ t-1 \end{pmatrix}\right]\begin{pmatrix} s+k \\ s \end{pmatrix}.\end{aligned}$$

Since the function $\binom{a+x}{a}$ is a polynomial in x of degree a, we consider first the above quantity as a polynomial in h. The leading coefficient is a polynomial in f whose leading coefficient is a constant multiple (where the positive constant is $\frac{1}{(t-1)!}$ and therefore just depends on t) of

$$(25)\qquad (1-\epsilon)\begin{pmatrix} s+k+1 \\ s \end{pmatrix} - \begin{pmatrix} s+k \\ s \end{pmatrix},$$

which is smaller then zero if we choose

$$k > \frac{(1-\epsilon)s-\epsilon}{\epsilon}.$$

Afterwords we choose f so large that the coefficient of h^{t-1} in (24) is negative, and finally we choose h so large that (24) is negative as a whole.

Observe that (as in [4, p. 444]) this inequality is the crucial point of the method to work; it says that in the vector $\mathbf{x}_n$ the number of coordinates which are S-integral and not S-units, i.e. those involving z_n, is not too large.

Finally, we get that

$$(26)\qquad \prod_{v\in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x}_n)|_v \le C_4C_6^n,$$

where $C_6 < 1$ is a suitable positive constant independent of n, for infinitely many n.

In order to apply the Subspace Theorem we need an upper bound for $\|\mathbf{x}_n\|$ which is easily obtained by

$$\|\mathbf{x}_n\| \le C_7\alpha_1^{(f+h)n}\beta_1^{(k+1)n} = C_7C_8^n.$$

The verification of the inequality in the Subspace Theorem (Proposition 1) follows now from

$$C_4C_6^n < \left(C_7C_8^n\right)^{-\delta},$$

which follows for small enough δ (such that $C_6C_8^{\delta} < 1$) if n is large enough.

Now, from the Subspace Theorem (in the form of Proposition 1) it follows that there is a nontrivial linear relation of the form

$$A_1x_1(n) + \ldots + A_Nx_N(n) = 0$$

with $A_1, \ldots, A_d \in \mathbb{Q}$, not all zero, valid for infinitely many n. Thus we obtain a relation of the form $z_nU_n = V_n$, where

$$U_n = \sum_{\mathbf{j}\in\mathcal{J}} u_{\mathbf{j}}\alpha_2^{i_2n}\cdots\alpha_t^{i_tn}\beta_1^{j_1n}\cdots\beta_s^{j_sn}$$

is a power sum with roots in the group generated by $\alpha_2, \ldots, \alpha_t, \beta_1, \ldots, \beta_s$ and V_n is a power sum with roots in the group generated by $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_s$. Observe that (again by [14, Lemma 2]) U_n and V_n must be nontrivial power sums, because if all coefficients in V_n are equal to zero, then there are finitely many possibilities for n only, and the same is true if all coefficients in U_n are zero. Recall that by definition $z_n = H_n/G_n$, thus we have

$$H_nU_n = G_nV_n.$$

Since G_n and H_n are coprime (these follows from [14, Lemma 3]), we conclude that G_n divides U_n in the ring of power sums. This is a contradiction since in G_n there is a root (namely α_1) which is coprime to all roots of U_n and to all other roots of G_n. This contradiction completes our proof. □

References

[1] Y. Bugeaud, P. Corvaja and U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Math. Zeitschrift* **243** (2003), 79-84.

[2] Y. Bugeaud and F. Luca, A quantitative lower bound for the greatest prime factor of $(ab + 1)(bc + 1)(ca + 1)$, *Acta Arith.* **114** (2004), 275-294.

[3] P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math., New Ser.* **9 (3)** (1998), 317-332.

[4] P. Corvaja and U. Zannier, Some new applications of the Subspace Theorem, *Compos. Math.* **131** (2002), no. 3, 319-340.

[5] P. Corvaja and U. Zannier, Finiteness of integral values for the ratio of two linear recurrences, *Invent. Math.* **149** (2002), 431-451.

[6] P. Corvaja and U. Zannier, On the greatest prime factor of $(ab+1)(ac+1)$, *Proc. Amer. Math. Soc.* **131** (2003), 1705-1709.

[7] P. Corvaja and U. Zannier, A lower bound for the height of a rational function at S-unit points, *Monatsh. Math.* **144** (2005), 203-224.

[8] J.-H. Evertse, An improvement of the Quantitative Subspace Theorem, *Compos. Math.* **101 (3)** (1996), 225-311.

[9] J.-H. Evertse and H.P. Schlickewei, The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group, *Number Theory in Progress* Vol. 1 (Zakopane-Kościelisko, 1997), 121-142, de Gruyter, Berlin, 1999.

[10] J.-H. Evertse and H.P. Schlickwei, A quantitative version of the absolute Subspace theorem, *J. reine angew. Math.* **548** (2002), 21-127.

[11] J.-H. Evertse, H.P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Ann. Math.* **155** (2002), 1-30.

[12] C. Fuchs, Quantitative finiteness results for Diophantine equations, PhD-thesis, TU Graz (2002).

[13] C. Fuchs, Exponential-polynomial equations and linear recurring sequences, *Glas. Mat. Ser. III* **38 (58)** (2003), 233-252.
[14] C. Fuchs, An upper bound for the G.C.D. of two linear recurring sequences, *Math. Slovaca* **53** (2003), No. 1, 21-42.
[15] C. Fuchs and A. Scremin, Polynomial-exponential equations involving several linear recurrences, *Publ. Math. Debrecen* **65** (2004), 149-172.
[16] C. Fuchs and A. Scremin, Diophantine inequalities involving several power sums, *Manuscripta Math.* **115** (2004), 163-178.
[17] C. Fuchs and R. F. Tichy, Perfect powers in linear recurring sequences, *Acta Arith.* **107.1** (2003), 9-25.
[18] S. Hernández and F. Luca, On the greatest prime factor of $(ab+1)(ac+1)(bc+1)$, *Bol. Soc. Math. Mexicana* **9** (2003), 235-244.
[19] K. Győry, A. Sárközy and C. L. Stewart, On the number of prime factors of integers of the form $ab+1$, *Acta Arith.* **74** (1996), 365-385.
[20] C. Lech, A note on recurring series, *Ark. Mat.* **2** (1953), 417-421.
[21] F. Luca, On the greatest common divisor of $u-1$ and $v-1$ with u and v near S-units, *Monats. Math.*, to appear.
[22] A. Pethő, Diophantine properties of linear recursive sequences I, Bergum, G. E. (ed.) et al., Applications of Fibonacci numbers. Volume 7: Proceedings of the 7th international research conference on Fibonacci numbers and their applications, Graz, Austria, July 15-19, 1996, Kluwer Academic Publ., Dordrecht (1998), 295-309.
[23] A. Pethő, Diophantine properties of linear recursive sequences II, *Acta Math. Acad. Paed. Nyiregyháziensis* **17** (2001), 81-96.
[24] A. J. van der Poorten, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, *C. R. Acad. Sci. Paris* **306**, Série I (1988), 97-102.
[25] A. J. van der Poorten, Some facts that should be better known, especially about rational functions, *Number Theory and Applications* (Banff, AB, 1988), 497-528, Kluwer Acad. Publ., Dordrecht, 1989
[26] H. P. Schlickewei, Multiplicities of recurrence sequences, *Acta Math.* **176** (1996), *no.* 2, 171-243.
[27] W. M. Schmidt, "Diophantine Approximation", Springer Verlag, LNM **785**, 1980.
[28] W. M. Schmidt, "Diophantine Approximations and Diophantine Equations", Springer Verlag, LNM **1467**, 1991.
[29] W. M. Schmidt, The zero multiplicity of linear recurrence sequences, *Acta Math.* **182** (1999), 243-282.
[30] W. M. Schmidt, Zeros of linear recurrence sequences, *Publ. Math. Debrecen* **56** (2000), 609–630.
[31] A. Scremin, Diophantine inequalities with power sums, *J. Théor. Nombres Bordeaux*, to appear.
[32] U. Zannier, A proof of Pisot's dth root conjecture, *Ann. Math.* **151**, no. 1 (2000), 375-383.

Clemens Fuchs
Institut für Mathematik A
Technische Universität Graz
Steyrergasse 30/II
8010 Graz, Austria
Current Adress: Mathematisch Instituut, Universiteit Leiden,
Niels Bohrweg 1, Postbus 9512, 2300 RA Leiden, The Netherlands
e-mail: fuchs@math.leidenuniv.nl, clemens.fuchs@tugraz.at