COMPOSITIO MATHEMATICA

JAN-HENDRIK EVERTSE

On sums of S-units and linear recurrences

Compositio Mathematica, tome 53, nº 2 (1984), p. 225-244

<http://www.numdam.org/item?id=CM_1984__53_2_225_0>

Compositio Mathematica 53 (1984) 225–244.

ON SUMS OF S-UNITS AND LINEAR RECURRENCES

Jan-Hendrik Evertse

§1. Introduction

In 1961 Chowla [1] proved that in any algebraic number field K there are only finitely many pairs of units ϵ_1, ϵ_2 such that $\epsilon_1 - \epsilon_2 = 1$. Schlickewei [15] and Dubois and Rhin [2] proved independently of each other that the equation $x_1 + x_2 + \ldots + x_n = 0$ has only finitely many solutions in rational integers $x_1, x_2, \ldots, x_n$ which are pairwise coprime and each composed of fixed primes. Recently, Shorey [20] showed that if $\{u_k\}_{k=0}^{\infty}$ is a simple linear non-degenerate binary recurrence sequence of rational integers, then the greatest prime factor of u_r/u_s tends to infinity if $r \to \infty$, $r > s$, $u_s \neq 0$. It is our intention to generalize these results by a uniform approach based on Schlickewei's p-adic version of the method of Thue-Siegel-Roth-Schmidt. Part of our results has been obtained independently by van der Poorten and Schlickewei [14].

Throughout this paper, K will denote an algebraic number field of degree D with ring of integers O_K. By a prime on K we mean an equivalence class of non-trivial valuations on K. We distinguish between infinite primes which contain archimedean valuations and finite primes which contain non-archimedean valuations. We denote the set of all infinite primes on K by S_∞. There is a well-known correspondence between finite primes and prime ideals. The letter p is used for primes on $\mathbb{Q}$, the letter v for primes on K. The infinite prime on $\mathbb{Q}$ is denoted by p_0 and $|.|_{p_0}$ is the ordinary absolute value. If q is a prime number in $\mathbb{Q}$, the corresponding finite prime is also denoted by q and $|.|_q$ denotes the q-adic valuation defined in the usual way. The completions of $\mathbb{Q}$, K at the primes p, v respectively, are denoted by $\mathbb{Q}_p$, K_v respectively. Thus $\mathbb{Q}_{p_0} = \mathbb{R}$. For every prime v on K lying above a prime p on $\mathbb{Q}$ we choose a valuation $\|.\|_v$ such that

$$\|\alpha\|_v = |\alpha|_p^{[K_v:\mathbb{Q}_p]} \qquad \text{for all} \quad \alpha \in \mathbb{Q}.$$

By this choice, the so-called product-formula holds,

$$\prod_v \|\alpha\|_v = 1 \qquad \text{for all} \quad \alpha \in K, \alpha \neq 0, \tag{1}$$

where $\prod_v$ means that the product is taken over all primes v on K.

Let n be an integer with $n \geq 1$. Points in the vector space K^{n+1} are denoted by $\boldsymbol{x} = (x_0, x_1, \ldots, x_n)$. let $\sigma_1, \sigma_2, \ldots, \sigma_D$ be the embeddings of K in $\mathbb{C}$. Put

$$\|\boldsymbol{x}\| = \max_{\substack{0 \leq k \leq n \\ 1 \leq j \leq D}} |\sigma_j(x_k)|. \tag{2}$$

If we identify pairwise linearly dependent non-zero points in K^{n+1}, we obtain the n-dimensional projective space $\mathbb{P}^n(K)$. Points in $\mathbb{P}^n(K)$, so-called *projective points*, are denoted by $X = (x_0 : x_1 : \ldots : x_n)$, where the homogeneous coordinates are in K and determined up to a multiplicative constant in K. Put

$$H(X) = \prod_v \max(\|x_0\|_v, \|x_1\|_v, \ldots, \|x_n\|_v). \tag{3}$$

By (1) this height is well-defined since it is independent of the multiplicative factor. The functions $\|\boldsymbol{x}\|$ and $H(X)$ are closely related. Schmidt [17] showed that positive constants c_1, c_2 exist, depending only on K, such that for each point $X \in \mathbb{P}^n(K)$ the homogeneous coordinates $x_0, x_1, \ldots, x_n$ can be chosen such that if $\boldsymbol{x} = (x_0, x_1, \ldots, x_n)$,

(i) $x_k \in O_K$ for $k = 0, 1, \ldots, n$

and (4)

(ii) $c_1\|\boldsymbol{x}\|^D \leq H(X) \leq c_2\|\boldsymbol{x}\|^D$. (cf. §3).

In case $K = \mathbb{Q}$ we may take $c_1 = c_2 = 1$ since

$$\|\boldsymbol{x}\| = H(X) \quad \text{if and only if} \quad \gcd(x_0, x_1, \ldots, x_n) = 1. \tag{5}$$

Obviously $\|\boldsymbol{x}\| \geq 1$ for all $\boldsymbol{x} \in O_K^{n+1}$ and $H(X) \geq 1$ for all $X \in \mathbb{P}^n(K)$. It is easy to check that for each $A \geq 1$ there are at most finitely many $\boldsymbol{x} \in O_K^{n+1}$ with $\|_x\| \leq A$. Hence by (4) for each $B \geq 1$ there are at most finitely many $X \in \mathbb{P}^n(K)$ with $H(X) \leq B$.

Let S be a finite set of primes on K, enclosing S_∞. An *S-unit* is by definition and element α of K with $\|\alpha\|_v = 1$ if $v \in S$ and an *S-integer* an element α of K with $\|\alpha\|_v \leq 1$ if $v \in S$. Let c, d be constants with $c > 0$, $d \geq 0$. A projective point $X \in \mathbb{P}^n(K)$ is called (c, d, S)*-admissible* if its homogeneous coordinates $x_0, x_1, \ldots, x_n$ can be chosen such that

(i) all x_k are S-integers (6)

and

$$\text{(ii)} \quad \prod_{v \in S} \prod_{k=0}^{n} \|x_k\|_v \leq c \cdot H(X)^d \tag{6}$$

Clearly, the homogeneous coordinates of $(1, 0, S)$-admissible projective points can be chosen to be all S-units.

THEOREM 1: *Let c, d be constants with $c > 0$, $0 \leq d < 1$, let S be a finite set of primes on K enclosing S_∞ and let n be a positive integer. Then there are only finitely many (c, d, S)-admissible projective points $X = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$ satisfying*

$$x_0 + x_1 + \ldots + x_n = 0 \tag{7}$$

but

$$x_{i_0} + x_{i_1} + \ldots + x_{i_s} \neq 0 \tag{8}$$

for each proper, non-empty subset $\{i_0, i_1, \ldots, i_s\}$ of $\{0, 1, \ldots, n\}$.

Mahler showed that for $n = 2$ (7) has at most finitely many $(1, 0, S)$-admissible solutions in $\mathbb{P}^n(K)$. As far as I know, Lang [4] was the first who published a proof of this result. For related results we refer to Chowla [1], Nagell [8], [9], [10], Györy [3], Schneider [19]. A somewhat weaker result than Theorem 1 has been stated by van der Poorten and Schlickewei [14]. For $K = \mathbb{Q}$ we have the following corollary of Theorem 1.

COROLLARY 1. *Let c, d be constants with $c > 0$, $0 \leq d < 1$, let S_0 be a finite set of prime numbers and let n be a positive integer. Then there are only finitely many tuples $\boldsymbol{x} = (x_0, x_1, \ldots, x_n)$ of rational integers such that*

$$x_0 + x_1 + \ldots + x_n = 0; \tag{9}$$

$$x_{i_0} + x_{i_1} + \ldots + x_{i_s} \neq 0 \tag{10}$$

for each proper, non-empty subset $\{i_0, i_1, \ldots, i_s\}$ of $\{0, 1, \ldots, n\}$;

$$\gcd(x_0, x_1, \ldots, x_n) = 1; \tag{11}$$

$$\prod_{k=0}^{n} \left(|x_k| \prod_{p \in S_0} |x_k|_p \leq c . \|\boldsymbol{x}\|^d. \right. \tag{12}$$

The corollary follows by (5) and the fact that there are exactly two tuples $(x_0, \ldots, x_n)$ of rational integers with gcd 1 which can be chosen as homogeneous coordinates of a given projective point in $\mathbb{P}^n(\mathbb{Q})$. Schlickewei [15] and Dubois and Rhin [2] showed that the number of tuples $x = (x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}$ satisfying (9), (12) and $\max(|x_i|_p, |x_j|_p) = 1$ for $i, j \in \{0, 1, \ldots, n\}$ and $i \neq j$ and $p \in S_0$ is finite, where again c, d are constants with $c > 0$, $0 \leq d < 1$.

We shall derive Theorem 1 from

THEOREM 2: *Let n be a non-negative integer and S a finite set of primes on K, enclosing S_∞. Then for every $\epsilon > 0$ a constant C exists, depending only on ϵ, S, K, n such that for each non-empty subset T of S and every vector $\boldsymbol{x} = (x_0, x_1, \ldots, x_n) \in O_K^{n+1}$ with*

$$x_{i_0} + x_{i_1} + \ldots + x_{i_s} \neq 0 \tag{13}$$

for each non-empty subset $\{i_0, \ldots, i_s\}$ of $(0, 1, \ldots, n)$:

$$\left(\prod_{k=0}^{n} \prod_{v \in S} \|x_k\|_v\right) \prod_{v \in T} \|x_0 + x_1 + \ldots + x_n\|_v$$
$$\geq C\left(\prod_{v \in T} \max(\|x_0\|_v, \ldots, \|x_n\|_v)\right) \|\boldsymbol{x}\|^{-\epsilon}. \tag{14}$$

A straightforward application of theorem 2 yields

COROLLARY 2: *Let n, S be as in theorem 2. Then for every $\epsilon > 0$ a constant C_1 exists, depending only on ϵ, S, K, n, such that for each non-empty subset T of S and every vector $X = (x_0, x_1, \ldots, x_n) \in O_K^{n+1}$ with $x_0 x_1 \ldots x_n (x_0 + \ldots + x_n) \neq 0$:*

$$\left(\prod_{k=0}^{n} \prod_{v \in S} \|x_k\|_v\right) \prod_{v \in T} \|x_0 + x_1 + \ldots + x_n\|_v$$

$$\geq C_1\left(\prod_{v \in T} \min(\|x_0\|_v, \ldots, \|x_n\|_v)\right) \|\boldsymbol{x}\|^{-\epsilon}$$

We shall apply theorem 1 to linear recurrence sequences $\{u_k\}_{k=0}^{\infty}$. We assume that no integer k_0 exists such that $u_k = 0$ for $k \geq k_0$. Let n be the smallest integer for which constants $v_1, v_2, \ldots, v_n$ exists such that

$$u_{k+n} = v_1 u_{k+n-1} + v_2 u_{k+n-2} + \ldots + v_n u_k \qquad \text{for} \quad k = 0, 1, 2, \ldots. \tag{15}$$

Then $v_n \neq 0$. It is well-known that polynomials f_i and pairwise distinct numbers α_i exist, depending only on $v_1, v_2, \ldots, v_n, u_0, u_1, \ldots, u_{n-1}$, such that

$$u_k = \sum_{i=1}^{m} f_i(k)\alpha_i^k \qquad \text{for} \quad k = 0, 1, 2, \ldots \tag{16}$$

Without loss of generality we may assume that the polynomials f_i do not vanish identically. The numbers α_i are called the *characteristic roots* of $\{u_k\}_{k=0}^{\infty}$. We call the sequence *degenerate* if at least one of the quotients of two distinct characteristic roots is a root of unity and *non-degenerate* otherwise.

Van der Poorten [13] has applied his version of theorem 1 to deduce several remarkable facts on non-degenerate recurrence sequences $\{u_k\}_{k=0}^{\infty}$ of algebraic numbers. Under very general conditions he proved that (i) for every $\epsilon > 0$ there exists a K such that

$$|u_k| > \left(\max_{i=1,2,\ldots,n} |\alpha_i|\right)^{k(1-\epsilon)} \qquad \text{for} \quad k \geq K,$$

(ii) the maximum of the norms of the prime ideals $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(u_k) \neq 0$ tends to infinity if $k \to \infty$ and (iii) the total multiplicity of $\{u_k\}_{k=0}^{\infty}$ is finite. Here the total multiplicity is defined as the number of pairs (r, s) of non-negative rational integers with $u_r = u_s$ and $r \neq s$. Shorey [20] gave in the case of a binary recurrence sequence of rational integers a lower bound for the greatest prime factor of u_r/u_s subject to the conditions $r > s$, $u_s \neq 0$, which tends to infinity if r does. In Theorem 3 we shall generalize (ii) to prime ideals $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(u_r/u_s) \neq 0$ in the same way as Shorey did, but without an explicit lower bound. Result (iii) is a direct consequence of theorem 3.

For $\alpha \in K$, $\alpha \neq 0$ we define $P_K(\alpha)$ to be the maximum of the norms of the prime ideals $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(\alpha) \neq 0$ if α is not a unit and $P_K(\alpha) = 1$ if α is a unit. Further we put $P_K(0) = 0$.

THEOREM 3: *Let $\{u_k\}_{k=0}^{\infty}$ be a linear non-degenerate recurrence sequence in K with at least two characteristic roots. Then*

$$\lim_{\substack{r \to \infty \\ r > s \\ u_s \neq 0}} P_K\left(\frac{u_r}{u_s}\right) = \infty.$$

The example $u_k = ka^k$ with $a \in \mathbb{Z}$, $a > 2$, where u_{a^l} is a power of a for every positive integer l, shows that the assertion of Theorem 3 does not hold if there is only one characteristic root.

The following two results of van der Poorten [13] are consequences of Theorem 3.

COROLLARY 3: *Let* $\{u_k\}_{k=0}^{\infty}$ *be as in theorem* 3. *Then*

$$\lim_{r\to\infty} P_K(u_r) = \infty$$

This follows from Theorem 3 by keeping some s with $u_s \neq 0$ fixed. This is an improvement and generalization of a result of Pólya ([12], Satz 2′, p. 17) which in fact states that if $\{u_n\}_{n=0}^{\infty}$ is a sequence satisfying the conditions of theorem 3 and if all u_n belong to $\mathbb{Q}$, then $\limsup_{n\to\infty}(P_{\mathbb{Q}}(u_n)) = \infty$.

COROLLARY 4: *Let* $\{u_k\}_{k=0}^{\infty}$ *be a linear non-degenerate recurrence sequence of algebraic numbers. Suppose that there do not exist a constant* a *and a root of unity* ρ *such that* $u_k = a\rho^k$ *for all* k. *Then there are only finitely many pairs of non-negative integers* (r, s) *with* $r \neq s$ *and* $u_r = u_s$.

If $u_k = f(k)\rho^k$ for $k = 0, 1, \ldots,$ where f is a non-constant polynomial with complex coefficients and ρ is a root of unity, then there can be only finitely many pairs (r, s) with $r \neq s$ and $u_r = u_s$. This follows from the fact that $\{|u_k|\}_{k=0}^{\infty} = \{|f(k)|\}_{k=0}^{\infty}$ is a strictly increasing sequence from a certain term on. If $u_k = f(k)\alpha^k$ for $k = 0, 1, \ldots,$ where f is a polynomial with algebraic coefficients and α not a root of unity, then we consider instead of $\{u_k\}_{k=0}^{\infty}$ the non-degenerate recurrent sequence $\{v_k\}_{k=0}^{\infty}$ with $v_k = u_k + 1^k$ for $k = 0, 1, \ldots$. So we may assume that $\{u_k\}_{k=0}^{\infty}$ has at least two distinct characteristic roots. Using that in fact all coefficients v_i in (15) are algebraic, all u_k belong to some algebraic number field and now Corollary 4 follows immediately from Theorem 3.

We remark that van der Poorten [13] has claimed that Corollary 4 is also valid if some of the terms u_k are transcendental over $\mathbb{Q}$.

§2. Proof of Theorem 2

As in §1, let K be an algebraic number field of degree D and let O_K be its ring of integers. We mention a theorem, due to Schlickewei [16], which will be used in the proof of theorem 2. As in §1, p_0 denotes the infinite prime on $\mathbb{Q}$. Let $p_1, p_2, \ldots, p_t$ be distinct prime numbers (or finite primes on $\mathbb{Q}$). For each $i \in \{0, 1, \ldots, t\}$ the valuation $|.|_{p_i}$ can be extended to the algebraic closure $\overline{\mathbb{Q}}_{p_i}$ of $\mathbb{Q}_{p_i}$ in a unique way and this extension is also denoted by $|.|_{p_i}$. Furthermore there are D isomorphic embeddings $\sigma_1^{(i)}$, $\sigma_2^{(i)}, \ldots, \sigma_D^{(i)}$ of K in $\overline{\mathbb{Q}}_{p_i}$. Put $K^{(i,j)} = \sigma_j^{(i)}(K)$, $\alpha^{(i,j)} = \sigma_j^{(i)}(\alpha)$ for $\alpha \in K$ and $x^{(i,j)} = (x_0^{(i,j)}, \ldots, x_n^{(i,j)})$ for $x = (x_0, \ldots, x_n) \in K^{n+1}$.

THEOREM 4: *Let n be a non-negative integer. For every j with $1 \leq j \leq D$ and every i with $0 \leq i \leq t$, let $L_0^{(i,j)}, \ldots, L_n^{(i,j)}$ be $n+1$ linearly independent linear forms in $n+1$ variables with coefficients in $\mathbb{Q}_{p_i}$ which are algebraic over $\mathbb{Q}$. Then for all $\epsilon > 0$ there are finitely many proper subspaces $T_1, T_2, \ldots, T_n$ of K^{n+1}, depending only on $n, p_0, \ldots, p_t, \epsilon$, K and the forms $L_k^{(i,j)}$, containing all solutions $\boldsymbol{x} \in O_K^{n+1}$, $\boldsymbol{x} \neq 0$ of the inequality*

$$\prod_{i=0}^{t} \prod_{j=1}^{D} \prod_{k=0}^{n} \left|L_k^{(i,j)}(\boldsymbol{x}^{(i,j)})\right|_{p_i} \leq \|\boldsymbol{x}\|^{-\epsilon}. \tag{17}$$

We shall now prove Theorem 2. Let S be a finite set of primes on K, enclosing S_∞. We assume that S has the property that if it contains one prime lying above some prime p on $\mathbb{Q}$, then it contains all the other primes on K lying above p. Obviously, this is no restriction. Let $p_0, p_1, \ldots, p_t$ be the primes on $\mathbb{Q}$ above which the primes in S ly. We shall proceed by induction on n. For $n = 0$, theorem 2 is trivial. Suppose that theorem 2 has been proved for all integers n with $0 \leq n < m$ (where $m \geq 1$). Our aim is to prove Theorem 2 for $n = m$. Let $\epsilon > 0$ and T a non-empty subset of S. We shall show that the points $\boldsymbol{x} = (x_0, x_1, \ldots, x_n) \in O_K^{n+1}$ which satisfy both

$$x_{i_0} + x_{i_1} + \ldots + x_{i_s} \neq 0 \tag{18}$$

for each non-empty subset $\{i_0, i_1, \ldots, i_s\}$ of $\{0, 1, \ldots, m\}$ and

$$\|x_{i_{0v}}\|_v \geq \|x_{i_{1v}}\|_v \geq \ldots \geq \|x_{i_{mv}}\|_v \qquad \text{for all} \quad v \in S, \tag{19}$$

where for each $v \in S$, $(i_{0v}, i_{1v}, \ldots, i_{mv})$ is a given permutation of $(0, 1, \ldots, m)$, and

$$\left(\prod_{k=0}^{m} \prod_{v \in S} \|x_k\|_v\right) \prod_{v \in T} \|x_0 + x_1 + \ldots + x_m\|_v \leq \left(\prod_{v \in T} \|x_{i_{0v}}\|_v\right) \|\boldsymbol{x}\|^{-\epsilon}$$

do also satisfy (14) for a certain constant C, specified in Theorem 2. This is clearly sufficient to prove Theorem 2.

For each prime $v \in S$, lying above the prime p_i on $\mathbb{Q}$ (where $i \in \{0, 1, \ldots, t\}$), we have that the valuation given by $|\sigma_j^{(i)}(\alpha)|_p$ for $\alpha \in K$ belongs to v for exactly $[K_v : \mathbb{Q}_p]$ embeddings $\sigma_j^{(i)}$. Thus, if $l(v)$ is the set of these embeddings,

$$\|\alpha\|_v = \prod_{\sigma_j^{(i)} \in l(v)} |\sigma_j^{(i)}(\alpha)|_{p_i} \qquad \text{for all} \quad \alpha \in K \tag{21}$$

Let $\mathscr{L}$ be the set of pairs of integers (i, j) with $0 \le i \le t$, $1 \le j \le D$, such that $\sigma_j^{(i)} \in l(v)$ for some $v \in T$. We now define the following linear forms in the variables $x_0, \ldots, x_m$, where v is determined by $\sigma_j^{(i)} \in l(v)$:

$$L_0^{(i,j)}(\boldsymbol{x}) = x_0 + x_1 + \ldots + x_m \qquad \text{for} \quad (i,j) \in \mathscr{L};$$

$$L_0^{(i,j)}(x) = x_{i_{0v}} \qquad \text{for} \quad (i,j) \in \mathscr{L};$$

$$L_k^{(i,j)}(\boldsymbol{x}) = x_{i_{kv}} \qquad \text{for} \quad 0 \le i \le t, \quad 1 \le j \le D, \quad 1 \le k \le m.$$

These linear forms have coefficients in $\mathbb{Q}$ and for fixed i, j, the forms $\{L_k^{(i,j)}\}_{k=0}^m$ are linearly independent. Furthermore, for all $x \in O_K^{n+1}$ satisfying (18), (19), (20) we have by (21),

$$\prod_{i=0}^{t} \prod_{j=1}^{D} \prod_{k=0}^{m} |L_k^{(i,j)}(\boldsymbol{x}^{(i,j)})|_{p_j} = \left(\prod_{k=0}^{m} \prod_{v \in S} \|x_k\|_v \right) \left(\prod_{v \in T} \|x_{i_{0v}}\|_v \right)^{-1}$$
$$\times \left(\prod_{v \in T} \|x_0 + x_1 + \ldots + x_m\|_v \right)$$
$$\le \|\boldsymbol{x}\|^{-\epsilon}$$

Hence by Theorem 4, the $\boldsymbol{x} \in O_K^{n+1}$ satisfying (18), (19), (20) already belong to finitely many proper subspaces of K^{n+1}. For each subspace it is possible to express some of the variables x_i in the other variables x_i. Hence there exist finitely many tuples $(\beta_{j_0}, \beta_{j_1}, \ldots, \beta_{j_u})$ of numbers in K, where $0 \le u \le m$ such that each solution $\boldsymbol{x} \in O_K^{n+1}$ of (18), (19), (20) satisfies at least one of the relations

$$x_0 + x_1 + \ldots + x_m = \beta_{j_0} x_{j_0} + \beta_{j_1} x_{j_1} + \ldots + \beta_{j_u} x_{j_u} \quad (0 \le u < m). \tag{22}$$

We may assume that no subsums of the right-hand side are equal to zero by cancelling some of the terms $\beta_{j_l} x_{j_l}$ if possible. We now show that all points $\boldsymbol{x} \in O_K^{n+1}$ satisfying (18), (19), (20), (22) also satisfy (14) with a constant C depending only on ϵ, m, K, S, the permutations in (19) and the tuple $(\beta_{j_0}, \ldots, \beta_{j_u})$. Since we have only finitely many permutations of $(0, 1, \ldots, m)$ and a finite set of tuples $(\beta_{j_0}, \ldots, \beta_{j_u})$ which depends only on m, K, S, ϵ and the permutations in (19), this suffices. Let $\mathscr{V}_1 = \{j_0, j_1, \ldots, j_u\}$, $\mathscr{V}_2 = \{0, 1, \ldots, m\} - \mathscr{V}_1$, let T_1 be the subset of T such that $i_{0v} \in \mathscr{V}_1$ and T_2 the subset of T such that $i_{0v} \in \mathscr{V}_2$. The constants c_3, c_4, ... will depend only on ϵ, K, S, m, the permutations in (19) and the tuple $(\beta_{j_0}, \ldots, \beta_{j_u})$. Let δ be a number in K such that $\delta\beta_{j_0}, \ldots, \delta\beta_{j_u}$ are algebraic integers and put $z_l = \delta\beta_{j_l} x_{j_l}$ for $l = 0, 1, \ldots, u$, $z = (z_0, z_1, \ldots,$

z_u). By (22) and the induction hypothesis we have

$$\left(\prod_{k=0}^{m}\prod_{v\in S}\|x_k\|_v\right)\prod_{v\in T}\|x_0+x_1+\dots+x_m\|_v$$

$$\geq c_3\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\prod_{l=0}^{u}\prod_{v\in S}\|z_l\|_v\left(\prod_{v\in T}\|z_0+\dots+z_u\|_v\right)$$

$$\geq c_4\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\left(\prod_{v\in T}\max(\|z_0\|_v,\dots,\|z_u\|_v)\right)\|z\|^{-\epsilon/2}$$

$$\geq c_5\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\left(\prod_{v\in T}\max_{k\in\mathscr{V}_1}\|x_l\|_v\right)\|\boldsymbol{x}\|^{-\epsilon/2}. \tag{23}$$

If $T_1 = T$ then (23) implies inequality (14) since $\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v \geq 1$. If $T_1 \subsetneqq T$, then, by (22) and the induction hypothesis,

$$\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\left(\prod_{v\in T_2}\max_{k\in\mathscr{V}_1}\|x_k\|_v\right)$$

$$\geq c_6\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\cdot$$

$$\cdot\left(\prod_{v\in T_2}\|(\beta_{j_0}-1)x_{j_0}+(\beta_{j_1}-1)x_{j_1}+\dots+(\beta_{j_u}-1)x_{j_u}\|_v\right)$$

$$=c_6\left(\prod_{k\in\mathscr{V}_2}\prod_{v\in S}\|x_k\|_v\right)\prod_{v\in T_2}\Big\|\sum_{k\in\mathscr{V}_2}x_k\Big\|_v$$

$$\geq c_7\left(\prod_{v\in T_2}\max_{i\in\mathscr{V}_2}\|x_k\|_v\right)\|\boldsymbol{x}\|^{-\epsilon/2}.$$

Together with (23) this implies that

$$\left(\prod_{k=0}^{m}\prod_{v\in S}\|x_k\|_v\right)\prod_{v\in T}\|x_0+\dots+x_m\|_v$$

$$\geq c_8\left(\prod_{v\in T_1}\max_{k\in\mathscr{V}_1}\|x_k\|_v\right)\left(\prod_{v\in T_2}\max_{k\in\mathscr{V}_2}\|x_k\|_v\right).\|\boldsymbol{x}\|^{-\epsilon}$$

$$=c_8\left(\prod_{v\in T}\max(\|x_0\|_v,\dots,\|x_m\|_v)\right)\|\boldsymbol{x}\|^{-\epsilon},$$

where empty products must be taken equal to 1. This completes the proof of Theorem 2. □

§3. Proof of Theorem 1

As before, K is an algebraic number field of degree D, S a finite set of primes on K enclosing S_∞ and c, d positive constants with $c > 0$, $0 \le d < 1$. Constants $c_9, c_{10}, \ldots$ will depend only on K, s, n, c, d. Let $X = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$ be a projective point satisfying (6), (7), (8). By an argument of Schmidt [17], (p. 63), there are positive constants c_9, c_{10}, c_{11} and a $\lambda \in K$ with $\lambda \neq 0$ such that

$$\lambda x_i \in O_K \qquad \text{for} \quad i = 0, 1, \ldots, m,$$

$$N\big((\lambda x_0, \ldots, \lambda x_n)\big) \le c_9,$$

(where $N(\mathfrak{a})$ denotes the absolute norm of the ideal $\mathfrak{a}$) i.e.

$$\prod_{v \notin S_\infty} \max(\|\lambda x_0\|_v, \ldots, \|\lambda x_n\|_v) \ge c_9^{-1} \tag{25}$$

and if $\sigma_1, \sigma_2, \ldots, \sigma_D$ are the embeddings of K in $\mathbb{C}$,

$$c_{10} \le \frac{\max\big(|\sigma_i(x_0)|, \ldots, |\sigma_i(x_n)|\big)}{\max\big(|\sigma_j(x_0)|, \ldots, |\sigma_j(x_n)|\big)} \le c_{11} \quad \text{for} \quad i, j \in \{1, 2, \ldots, D\}. \tag{26}$$

Put $y_i = \lambda x_i$, $\boldsymbol{y} = \lambda \cdot \boldsymbol{x}$. Then, by (25), (26),

$$c_{12} \|\boldsymbol{y}\|^D \le H(X) \le c_{13} \|\boldsymbol{y}\|^D. \tag{27}$$

Moreover, since the x_i are S-integers and the y_i algebraic integers, by (25),

$$\prod_{v \in S} \|\lambda\|_v \ge \prod_{v \in S} \max(\|y_0\|_v, \ldots, \|y_n\|_n)$$

$$\ge \prod_{v \notin S_\infty} \max(\|y_0\|_v, \ldots, \|y_n\|_v) \ge c_9^{-1},$$

hence

$$\prod_{v \in S} \|\lambda\|_v \le c_9.$$

By (6) this implies that

$$\prod_{k=0}^{n} \prod_{v \in S} \|y_k\|_v \leq c_{14} H(X)^d. \tag{28}$$

Put $\tilde{y} = (y_v, \ldots, y_n)$, $Y = (y_1 : y_2 : \ldots : y_n)$. Since $y_0 + y_1 + \ldots + y_n = 0$ we have

$$H(Y) \leq H(X) \leq c_{15} H(Y) \tag{29}$$

Now we have, by (28), (7), (24), (8), (27), (29) and Theorem 2 with $\epsilon = \frac{1}{2}D(1-d)$,

$$\begin{aligned}
c_{14} H(X)^d &\geq \prod_{k=0}^{n} \prod_{v \in S} \|y_k\|_v \\
&= \left(\prod_{k=1}^{n} \prod_{v \in S} \|y_k\|_v \right) \prod_{v \in S} \|y_1 + y_2 + \ldots + y_n\|_v \\
&\geq c_{16} \left(\prod_{v \in S} \max(\|y_1\|_v, \ldots, \|y_n\|_v) \| y \|^{-\epsilon} \right. \\
&\geq c_{17} H(Y) H(X)^{-\epsilon/D} \geq c_{18} H(X)^{1-\epsilon/D}.
\end{aligned}$$

This implies that

$$H(X)^{(1-d)/2} \leq c_{14}/c_{18}.$$

Since $d < 1$ this proves Theorem 1.

§4. Proof of Theorem 3

In the proof of Theorem 3 we shall use two lemmas which are stated and proved below. In the sequel, K denotes an algebraic number field.

LEMMA 1: *Suppose K has degree D, let $f(X) \in K[X]$ be a polynomial of degree m and T a non-empty set of primes on K. Then there exists a positive constant c_{19}, depending only on K, f such that for all $r \in \mathbb{Z}$ with $r \neq 0$, $f(r) \neq 0$,*

$$\begin{aligned}
c_{19}^{-1} |r|^{-Dm} &\leq \left(\prod_{v} \max(1, \|f(r)\|_v) \right)^{-1} \leq \prod_{v \in T} \|f(r)\|_v \\
&\leq \prod_{v} \max(1, \|f(r)\|_v) \leq c_{19} |r|^{Dm}.
\end{aligned} \tag{30}$$

PROOF: It follows easily from (1) that

$$\prod_{v\in T}\|f(r)\|_v \le \prod_v \max(1, \|f(r)\|_v),$$

$$\prod_{v\in T}\|f(r)\|_v = \prod_{v\notin T}\|f(r)\|_v^{-1} \ge \Big(\prod_v \max(1, \|f(r)\|_v)\Big)^{-1}.$$

Furthermore there exist positive constants c_{20}, c_{21} and a finite set of finite primes T_0, all depending only on K, f such that for all $r \in \mathbb{Z}$ with $r \neq 0, f(r) \neq 0$,

$$\|f(r)\|_v \le c_{20}\|r\|_v^m \qquad \text{for} \quad v \in S_\infty,$$

$$\|f(r)\|_v \le c_{21} \qquad \text{for} \quad v \in T_0,$$

$$\|f(r)\|_v \le 1 \qquad \text{for} \quad v \notin S_\infty \cup T_0.$$

This implies Lemma 1 immediately. □

LEMMA 2: *Let $f(X)$, $g(X) \in K[X]$ be polynomials of degrees m, n respectively such that no rational integer h with $h \neq 0$ exists for which one of the polynomials $f(X+h)$, $g(X)$ divides the other. Let S be a finite set of primes on K and β, γ constants with*

$$\beta > 0,\ 0 \le \gamma < \frac{1}{m+n+2}. \tag{31}$$

Then there are only finitely many pairs of rational integers (r, s) such that

$$0 < |r-s| \le \beta|r|^\gamma \tag{32}$$

and

$$\frac{f(r)}{g(s)} \text{ is an } S\text{-unit}. \tag{33}$$

PROOF: For each pair of polynomials $f(X)$, $g(X) \in K[X]$, let $\mathscr{H}(f, g)$ be the set of rational integers h with $h \neq 0$ which are the difference of a zero of f and a zero of g. It suffices to show that if f, g are both non-constant polynomials, then at most finitely many pairs $(r, s) \in \mathbb{Z}^2$ exist which satisfy (32), (33) and $r - s \notin \mathscr{H}(f, g)$. For assume we have shown this. Let f, g be polynomials in $K[X]$ such that no rational integer h with

$h \neq 0$ exists for which one of the polynomials $f(X+h)$, $g(X)$ divides the other. Let $\mathscr{H}(f, g)$ be non-empty. Take $h \in \mathscr{H}(f, g)$ and consider the pairs $(r, s) \in \mathbb{Z}^2$ with $r-s=h$ for which $f(r)/g(s)$ is an S-unit. The polynomials $f(X)$, $g(X\text{-}h)$ have a nonconstant greatest common divisor $k(X)$ in $K[X]$. Put $f_0(X)=f(X)/k(X)$, $g_0(X)=g(X)/k(X+h)$. Then neither $f_0(X)$, nor $g_0(X)$ is constant and for the pairs (r, s) under consideration we have that $f_0(r)/g_0(s)=f(r)/g(s)$ is an S-unit and $r-s \notin \mathscr{H}(f_0, g_0)$. By our assumption and by the fact that $\mathscr{H}(f, g)$ is finite, this proves Lemma 2 in general.

Let $\mathscr{V}$ be the set of pairs $(r, s) \in \mathbb{Z}^2$ satisfying (32), (33) and $r-s \notin \mathscr{H}(f, g)$, where f, g are non-constant polynomials in $K[X]$. It is our aim to show that $\mathscr{V}$ is finite. We assume that $f(X), g(X) \in O_K[X]$, that all the zeros of f and g are S-units in K and that $S \supset S_\infty$, which are no restrictions. Put $D=[K:\mathbb{Q}]$. Suppose $K \subset \mathbb{C}$ and let $\sigma_1, \sigma_2, \ldots, \sigma_D$ be the embeddings of K in $\mathbb{C}$. The constants c_{22}, c_{23} will be positive and depend only on K, f, g.

We assume that $\mathscr{V}$ is infinite for some pair of constants β, γ satisfying (31). Let

$$f(X)=A(X-a_1)^{e_1}(X-a_2)^{e_2}\ldots(X-a_p)^{e_p},$$

$$g(X)=B(X-b_1)^{f_1}(X-b_2)^{f_2}\ldots(X-b_q)^{f_q}$$

where the a_i are distinct, the b_j are distinct, the e_i and the f_j are positive integers with $\sum_{i=1}^{p} e_i=m$, $\sum_{j=1}^{1} f_j=n$. First of all we have for $(r, s) \in \mathscr{V}$, if $N(\mathfrak{a})$ denotes the absolute norm of the ideal $\mathfrak{a}$, on noting that $r-s \notin \mathscr{H}(f, g)$,

$$\begin{aligned} N\big((r-a_i, s-b_j)\big) &\leq N\big((r-s+b_j-a_i)\big) \\ &\leq \prod_{k=1}^{D} |r-s+\sigma_k(b_j-a_i)| \\ &\leq c_{22}|r-s|^D \qquad \text{for} \quad \begin{array}{l} i=1,2,\ldots,p\ , \\ j=1,2,\ldots,q, \end{array} \end{aligned}$$

hence

$$N\big((f(r), g(s))\big) \leq c_{23}|r-s|^{Dmn}.$$

Since $f(r)/g(s)$ is an S-unit this implies by (1), and $f(X), g(X) \in O_K[X]$

that

$$\max\Big(\prod_{v\in S}\|f(r)\|_v,\ \prod_{v\in S}\|g(s)\|_v\Big)$$

$$= \max\Big(\prod_{v\notin S}\|f(r)\|_v^{-1},\ \prod_{v\notin S}\|g(s)\|_v^{-1}\Big)$$

$$= \Big(\prod_{v\notin S}\max(\|f(r)\|_v, \|g(s)\|_v)\Big)^{-1}$$

$$\leq \Big(\prod_{v\notin S_\infty}\max(\|f(r)\|_v, \|g(s)\|_v)\Big)^{-1}$$

$$= N((f(r), g(s))) \leq c_{23}|r-s|^{Dmn}.$$

By permuting the a_i, b_j if necessary we may therefore assume that an infinite subset $\mathscr{V}_1$ of $\mathscr{V}$ exist such that for $(r, s)\in\mathscr{V}_1$:

$$\prod_{v\in S}\|r-a_1\|_v \leq c_{24}\big(|r-s|^{Dmn}\big)^{1/m} = c_{24}|r-s|^{Dn},$$

$$\prod_{v\in S} s - b_{1v} \leq c_{24}|r-s|^{Dm}. \tag{34}$$

Put $\zeta_0 = \zeta_0^{(r,s)} = s - r + a_1 - b_1$, $\zeta_1 = \zeta_1^{(r,s)} = r - a_1$, $\zeta_2 = \zeta_2^{(r,s)} = b_1 - s$, $Z = Z^{(r,s)} = (\zeta_0 : \zeta_1 : \zeta_2)$. Then $Z\in\mathbb{P}^2(K)$,

$$\zeta_0 + \zeta_1 + \zeta_2 = 0 \tag{35}$$

and by (34), since $r - s\notin\mathscr{H}(f, g)$,

$$\prod_{i=0}^{2}\prod_{v\in S}\|\zeta_i\|_v \leq c_{25}|r-s|^{D(m+n+1)}. \tag{36}$$

Since $f(r)\neq 0$, $g(s)\neq 0$, $r - s\notin H(f, g)$ for $(r, s)\in\mathscr{V}_1$, we have by (1)

$$H(Z) = \prod_v \max(\|\zeta_0\|_v, \|\zeta_1\|_v, \|\zeta_2\|_v)$$

$$\geq \prod_{v\in S_\infty}\|r-a_1\|_v\cdot\prod_{v\notin S_\infty}\|s-r+a_1-b_1\|_v$$

$$= \prod_{v\in S_\infty}\big(\|r-a_1\|_v\|s-r+a_1-b_1\|_v^{-1}\big) \geq c_{26}|r|^D|r-s|^{-D}. \tag{37}$$

Put $d=(m+n+1)\gamma/(1-\gamma)$. Then, by (31), $0 \le d < 1$. Formulas (36), (32) and (37) yield that for $(r, s) \in \mathscr{V}_1$:

$$\prod_{i=0}^{2} \prod_{v \in S} \|\zeta_i\|_v \le c_{25}\beta^{D(m+n+1)}|r|^{D\gamma(m+n+1)} = c_{25}\beta^{D(m+n+1)}|r|^{Dd(1-\gamma)}$$

$$\le c_{25}\beta^{D(m+n+1+d)}\left(|r|^D|r-s|^{-D}\right)^d$$

$$\le c_{25}c_{26}^{-d}\beta^{D(m+n+1+d)}H(Z)^d.$$

Together with (35), the fact that ζ_0, ζ_1, ζ_2 are non-zero S-integers and Theorem 1, this yields that there at most finitely many such projective points Z. Therefore, there must be an infinite subset $\mathscr{V}_2$ of $\mathscr{V}_1$ such that $Z^{(r,s)} = Z_0$ for $(r, s) \in \mathscr{V}_2$, where Z_0 is a fixed projective point in $\mathbb{P}^2(\mathrm{K})$; Choose two pairs (r_1, s_1), (r_2, s_2) in $\mathscr{V}_2$ with $|r_2| > |r_1|$. By (32), (31) this is possible. Now we have by (32),

$$\left|\zeta_2^{(r_1,s_2)}\right| = \left|\frac{\zeta_1^{(r_1,s_1)}}{\zeta_0^{(r_1,s_1)}}\right| \cdot \left|\zeta_0^{(r_2,s_2)}\right|$$

$$\le c_{27}\beta\left|\frac{\zeta_1^{(r_1,s_1)}}{\zeta_0^{(r_1,s_1)}}\right| \cdot \left|\zeta_1^{(r_2,s_2)}\right|^{\gamma}.$$

By (31), this implies that $\left|\zeta_1^{(r_2,s_2)}\right|$, whence $|r_2|$, can be bounded above in terms of r_1, s_1, f, g, k, β, γ. Together with (32) this contradicts the fact that $\mathscr{V}_2$ is infinite. Therefore our assumption that $\mathscr{V}$ is infinite was false and together with the remarks made at the beginning of the proof, this proves Lemma 2. □

PROOF OF THEOREM 3: Let K be an algebraic number field and let $\{u_k\}_{k=0}^{\infty}$ be a non-degenerate linear recurrence sequence with $u_k \in K$, having at least two characteristic roots. We have

$$u_k = \sum_{i=1}^{m} f_i(k)\alpha_i^k \qquad \text{for} \quad k = 0, 1, 2, \ldots, \tag{38}$$

where $m \ge 2$, f_i is a non-zero polynomial for $i = 1, 2, \ldots, m$ and the α_i are distinct algebraic numbers such that α_i/α_j is not a root of unity for $i \ne j$. We assume that $f_i(X) \in K[X]$, and $\alpha_i \in K$ for $i = 1, 2, \ldots, m$ which is no restriction in the proof of theorem 3. Further c_{28}, c_{29}, $\ldots$ will denote positive constants depending only on K, α_1, α_2, $\ldots$, α_m, f_1, $\ldots$, f_m.

We assume that theorem 3 is not valid, i.e. there exists a finite set of primes S on K, enclosing S_∞, and an infinite set $\mathscr{W}$ of pairs of integers (r, s) with $r > s \geq 0$ and $u_s \neq 0$, such that u_r/u_s is an S-unit or $u_r = 0$ for $(r, s) \in \mathscr{W}$. We assume that the α_i and the coefficients of the f_i are all S-units which is no restriction. In view of (38) we have

$$\zeta_{r,s} \sum_{i=1}^{m} f_i(r)\alpha_i^r - \beta \sum_{i=1}^{m} f_i(s)\alpha_i^s = 0 \qquad \text{for} \quad (r, s) \in \mathscr{W}, \tag{39}$$

where $\zeta_{r,s}$ is an S-unit, $\beta = 1$ if $u_r \neq 0$, $\beta = 0$ and $\zeta_{r,s} = 1$ if $u_r = 0$. Put $\xi_i = \zeta_{r,s} f_i(r)\alpha_i^r$ for $i = 1, 2, \ldots, m$, $\xi_i = -\beta f_{i-m}(s)\alpha_{i-m}^s$ for $i = m+1, \ldots, 2m$. Then $\xi_1 + \xi_2 + \ldots + \xi_{2m} = 0$. For each pair $(r, s) \in \mathscr{W}$ there is a collection $\mathscr{P}$ of pairwise disjoint non-empty subsets of $\{1, 2, \ldots, 2m\}$, having $\{1, 2, \ldots, 2m\}$ as their union, such that

$$\begin{aligned} &\sum_{i \in S} \xi_i = 0 \qquad \text{for} \quad \mathscr{S} \in \mathscr{P}, \\ &\sum_{i \in T} \xi_i \neq 0 \qquad \text{if} \quad \mathscr{T} \subsetneqq \mathscr{S}, \mathscr{T} \neq \emptyset \qquad \text{for some} \quad \mathscr{S} \in \mathscr{P}. \end{aligned} \tag{40}$$

Since there are only finitely many collections of subsets as described above, we can find such a collection $\mathscr{P}$ such that (40) holds for all pairs (r, s) belonging to an infinite subset $\mathscr{W}_1$ of $\mathscr{W}$. We assume that there are no pairs (r, s) in $\mathscr{W}_1$ with $f_i(r) = 0$ for some $i \in \{1, 2, \ldots, m\}$ which is no restriction.

First of all, we shall prove that each set $\mathscr{S}$ in $\mathscr{P}$ can contain at most one element from $\{1, 2, \ldots, m\}$. Let us assume the contrary i.e. that there is an $\mathscr{S}$ in $\mathscr{P}$ containing integers i, j with $1 \leq i < j \leq m$. Let $\Xi = \Xi^{(r,s)}$ denote the projective point with the $\xi_k (k \in \mathscr{S})$ as homogeneous coordinates. Put

$$c_{28} = \prod_v \max(1, \|\alpha_i/\alpha_j\|_v).$$

Since α_i/α_j is not a root of unity, we have $c_{28} > 1$. By (1) and Lemma 1 we have for $r \geq c_{29}$,

$$\begin{aligned} H(\Xi) &\geq \prod_v \max(\|\zeta_{r,s} f_i(r)\alpha_i^r\|_v, \|\zeta_{r,s} f_j(r)\alpha_j^r\|_v) \\ &= \prod_v \max\left(1, \left\| \frac{f_i(r)\alpha_i^r}{f_j(r)\alpha_j^r} \right\|_v \right) \\ &\geq \prod_v \left(\left(\max(1, \|f_i(r)\|_v) \max(1, \|f_j(r)\|_v)\right)^{-1} \right. \end{aligned}$$

$$\times \max\left(1, \left\|\frac{\alpha_i}{\alpha_j}\right\|_v\right)\Bigg)^r$$

$$\geq c_{30} r^{-c_{31}} c_{28}^r \geq c_{28}^{r/2}.$$

But on the other side we have, since all α_i are S-units,

$$\prod_{i \in S} \prod_{v \in S} \|\xi_i\|_v \leq \max_{1 \leq k \leq m} \left(\prod_{v \in S} \|f_k(r)\|_v^{2m}, \prod_{v \in S} \|f_k(s)\|_v^{2m} \right)$$

$$\leq c_{32} r^{c_{33}}.$$

Since all the ξ_i are S-integers, this implies by Theorem 1, and (40) that there are only finitely many of such projective points $\Xi^{(r,s)}$. But then there are infinitely pairs (r, s) in $\mathscr{W}_1$ which correspond to the same projective point $\Xi^{(r,s)}$. Take two of these pairs, (r_1, s_1), (r_2, s_2) say, with $r_2 > 2r_1$. Then

$$\frac{\zeta_{r_1, s_1} f_i(r_1) \alpha_i^{r_1}}{\zeta_{r_1, s_1} f_j(r_1) \alpha_j^{r_1}} = \frac{\zeta_{r_2, s_2} f_i(r_2) \alpha_i^{r_2}}{\zeta_{r_2, s_2} f_j(r_2) \alpha_j^{r_2}},$$

hence

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{r_2 - r_1} = \frac{f_i(r_1) f_j(r_2)}{f_i(r_2) f_j(r_1)}. \tag{41}$$

Choose a prime v such that $\|\alpha_i/\alpha_j\|_v = : c_{34} > 1$. Then $\|\alpha_i/\alpha_j\|_v^{r_2 - r_1} \geq c_{34}^{r_2/2}$, whereas by Lemma 1,

$$\left\| \frac{f_i(r_1) f_j(r_2)}{f_j(r_1) f_i(r_2)} \right\|_v \leq c_{35} r_2^{c_{36}}.$$

However, for r_2 sufficiently large this contradicts (41). This shows indeed that each set $\mathscr{S}$ in $\mathscr{P}$ can contain at most one element from $\{1, 2, \ldots, m\}$. Of course, there are sets $\mathscr{S}$ containing an element from $\{1, 2, \ldots, m\}$ and since we assumed that $f_i(r) \neq 0$ for $i \in \{1, 2, \ldots, m\}$ and $(r, s) \in \mathscr{W}_1$, these sets must contain also an element i from $\{m+1, \ldots, 2m\}$, for which $\xi_i \neq 0$. Hence $\beta = 1$ and $\mathscr{P}$ consists of m pairwise disjoint subsets of $\{1, 2, \ldots, 2m\}$, each containing exactly one element from $\{1, 2, \ldots, m\}$ and one from $\{m+1, \ldots, 2m\}$. This can be written as

$$\zeta_{r,s} f_i(r) \alpha_i^r = f_{\sigma(i)}(s) \alpha_{\sigma(i)}^s \qquad \text{for} \quad (r, s) \in \mathscr{W}_1 \tag{42}$$

where $\zeta_{r,s}$ is an S-unit and σ a fixed permutation of $\{1, 2, \ldots, m\}$.

In the final part of the proof we shall show that $\mathscr{W}_1$ is finite. This is contradictory to what we have seen before and will complete the proof of theorem 3. We distinguish two cases.

Case 1. σ is the identity.
Then we have for $i, j \in \{1, 2, \ldots, m\}$, by (42),

$$\frac{f_i(r)}{f_j(r)}\left(\frac{\alpha_i}{\alpha_j}\right)^r = \frac{f_i(s)}{f_j(s)}\left(\frac{\alpha_i}{\alpha_j}\right)^s \quad \text{for} \quad (r, s) \in \mathscr{W}_1. \tag{43}$$

If all polynomials $f_i(X)$ with $i \in \{1, 2, \ldots, m\}$ are constant this implies that α_i/α_j is a root of unity for all pairs (i, j) with $i, j \in \{1, 2, \ldots, m\}$ and we have excluded this case. Therefore we can choose a polynomial $f_i(X)$ such that $f_i(X)$ is non-constant. Then for every non-zero rational integer h, none of the polynomials $f_i(X+h)$, $f_i(X)$ divides the other. Furthermore, by (42), $f_i(r)/f_i(s)$ is an S-unit for $(r, s) \in \mathscr{W}_1$. Take $j \in \{1, 2, \ldots, m\}$ with $j \neq i$. By (43) and lemma 1, we have, on choosing a prime v such that $\|\alpha_i/\alpha_j\|_v > 1$,

$$\left\|\frac{\alpha_i}{\alpha_j}\right\|_v^{r-s} = \left\|\frac{f_i(s)f_j(r)}{f_i(r)f_j(s)}\right\|_v \leq c_{37} r^{c_{38}},$$

hence

$$0 < r - s \leq c_{39} \log r \qquad \text{for} \quad (r, s) \in \mathscr{W}_1.$$

By Lemma 2 we infer that $\mathscr{W}_1$ is finite indeed.

Case 2. σ is not the identity.
Choose an integer i such that $i \neq \sigma(i)$ and $(r, s) \in \mathscr{W}_1$. Put $\theta_k = \alpha_{\sigma^k(i)}/\alpha_{\sigma^{k+1}(i)}$, $\theta_k = f_{\sigma^{k+1}(i)}(s)/f_{\sigma^k(i)}(r)$. By (42) we have

$$\theta_k^r = \frac{q_k}{q_{k+1}}\theta_{k+1}^s \qquad \text{for} \quad k = 0, 1, 2, \ldots$$

A simple inductive argument shows that

$$\theta_0^{r^k} = \left(\frac{q_0}{q_1}\right)^{r^{k-1}}\left(\frac{q_1}{q_2}\right)^{r^{k-2}s}\cdots\left(\frac{q_{k-1}}{q_k}\right)^{s^{k-1}}\theta_k^{s^k} \qquad \text{for} \quad k = 1, 2, 3, \ldots$$

Let v be the order of σ. Then $\theta_v = \theta_0$, $q_v = q_0$. This implies that

$$\theta_0^{r^v - s^v} = \left(\frac{q_0}{q_1}\right)^{r^{v-1}} \left(\frac{q_1}{q_2}\right)^{r^{v-2}s} \cdots \left(\frac{q_{m-1}}{q_m}\right)^{s^{v-1}}$$

$$= q_0^{r^{v-1}} - s^{v-1} \cdot q_1^{r^{v-2}s - r^{v-1}} \cdot q_2^{r^{v-3}s^2 - r^{v-2}s} \cdots q^{s^{v-1} - r.s^{v-2}}$$

All exponents appearing in the above equality are divisble by $r - s$ and we have

$$\theta_0^{r^{v-1} + r^{v-2}s + \ldots + s^{v-1}} = q_0^{r^{v-2} + \ldots + s^{v-2}} q_1^{-r^{v-2}} q_2^{-r^{v-3}s} \cdots q_{v-1}^{-s^{v-2}}. \tag{44}$$

Now choose a prime v such that $1 < \|\theta_0\|_v = : e^{c_{40}}$. Then by (44) and Lemma 1,

$$e^{c_{40} r^{v-1}} \leq \left(c_{41} \cdot r^{c_{42}}\right)^{r^{v-2}} \leq e^{c_{43} r^{v-2} \log r}.$$

This implies that r is bounded and hence that also in this case $\mathscr{W}_1$ is finite. □

References

[1] S. CHOWLA: Proof of a conjecture of Julia Robinson. *Norske Vid. Selsk. Forh. (Trondheim) 34* (1961) 107–109.

[2] E. DUBOIS and G. RHIN, Sur la majoration de formes linéaires à coefficients algébriques réels et p-adiques. Démonstration d'une conjecture de K. Mahler. *C.R. Acad. Sc. Paris 282,* Série A-1211 (1976).

[3] K. GYORY, On the number of solutions of linear equations in units of an algebraic number field. *Comment. Math. Helv. 54* (1979) 583–600.

[4] S. LANG, Integral points on curves. *Inst. Hautes Etudes Sci. Publ. Math. no. 6* (1960) 27–43.

[5] D.J. LEWIS and K. MAHLER, On the representation of integers by binary forms. *Acta Arith. 6* (1961) 333–363.

[6] K. MAHLER, Zur Approximation algebraischer Zahlen (I). Uber den gröszten Primteiler Binärer Formen. *Math. Ann. 107* (1933) 691–730.

[7] K. MAHLER: *Math. Rev. 42* (1971) 3028.

[8] T. NAGELL, Sur une propriété des unités d'un corps algébrique. *Arkiv för Mat. 5* (1965) 343–356.

[9] T. NAGELL: Quelques problèmes relatifs aux unités algébriques. *Arkiv för Mat. 8* (1969) 115–127.

[10] T. NAGELL: Sur un type particulier d'unités algébriques. *Arkiv för Mat. 8* (1969) 163–184.

[11] M. NEWMAN: Units in arithmetic progression in an algebraic number field. *Proc. Amer. Math. Soc. 43* (1974) 266–268.

[12] G. POLYA, Arithmetische Eigenschaften der Reihenentwicklungen. *J. reine angew. Math. 151* (1921) 1–31.

[13] A.J. VAN DER POORTEN, Some problems of recurrent interest. *Macquarie Math. Reports;* Macquarie Univ., Northride, Australia, 81-0037 (1981).

[14] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI, The growth conditions for recurrence sequences. *Macquarie Math. Reports 82-0041* (1982).
[15] H.P. SCHLICKEWEI Über die diophantische Gleichung $x_1 + x_2 + \ldots + x_n = 0$ *Acta Arith. 33* (1977) 183–185.
[16] H.P. SCHLICKEWEI: The $\not{p}$-adic Thue-Siegel-Roth-Schmidt Theorem. *Arch Math. 29* (1977) 267–270.
[17] W.M. SCHMIDT: Simultaneous approximation to algebraic numbers by elements of a number field *Monatsh. Math. 79* (1975) 55–66.
[18] W.M. SCHMIDT: Diophantine Approximation, *Lecture Notes in Math. 785*, Springer Verlag, Berlin Etc. 1980.
[19] TH. SCHNEIDER: Anwendung eines abgeänderten Roth-Ridoutschen Satzes auf diophantische Gleichungen. *Math. Ann. 169* (1967) 177–182.
[20] T.N. SHOREY, Linear forms in numbers of a binary recursive sequence. *Acta Arith,* to appear.

(Oblatum 17-I-1983)

University of Leiden
Department of Mathematics
Wassenaarseweg 80
Postbus 9512
2300 RA Leiden
The Netherlands