The distance between terms of an algebraic recurrence sequence

By *M. Mignotte* at Strasbourg, *T. N. Shorey* at Bombay*) and *R. Tijdeman* at Leiden

---

§ 1. Let $\{u_m\}_{m=0}^{\infty}$ be a sequence of algebraic numbers satisfying a recurrence relation with complex coefficients of order k,

$$u_{m+k} = v_{k-1}u_{m+k-1} + v_{k-2}u_{m+k-2} + \cdots + v_0 u_m, \quad m = 0, 1, 2, \ldots, \tag{1}$$

such that $|u_0| + |u_1| + \cdots + |u_{k-1}| > 0$ and $v_0 \neq 0$. We assume that $\{u_m\}_{m=0}^{\infty}$ does not satisfy a recurrence relation of lower order. Since the recurrence relation of minimal order is unique, this implies that the numbers $v_0, v_1, \ldots, v_{k-1}$ are algebraic (cf. [5] § 18). Let F be the field $\mathbb{Q}(u_0, u_1, \ldots, u_{k-1}, v_0, v_1, \ldots, v_{k-1})$. Hence $u_m \in F$ for all m. Write the companion polynomial of (1) as

$$G(z) = z^k - v_{k-1}z^{k-1} \cdots - v_0 = \prod_{j=1}^{s} (z - w_j)^{\sigma_j}, \tag{2}$$

where $w_1, w_2, \ldots, w_s$ are distinct and $\sigma_1, \sigma_2, \ldots, \sigma_s$ positive integers. Without loss of generality we may assume

$$|w_1| \geqq |w_2| \geqq \cdots \geqq |w_s| > w_{s+1} := 0. \tag{3}$$

Define r by

$$|w_1| = |w_2| = \cdots = |w_r| > |w_{r+1}|. \tag{4}$$

By the minimality of k there exist non-trivial polynomials P_j with coefficients in $F(w_1, w_2, \ldots, w_s)$ and of degrees $\sigma_j - 1$ for $j = 1, 2, \ldots, s$ such that

$$u_m = \sum_{j=1}^{s} P_j(m) w_j^m, \quad m = 0, 1, 2, \ldots. \tag{5}$$

---

*) This research was supported in part by the Netherlands Organization for the Advancement of Pure Research for a stay at the University of Leiden.

In this paper we apply effective methods to the equations

$$u_m = 0 \quad \text{in} \quad m \in \mathbb{Z}, \quad m \geqq 0 \tag{6}$$

and

$$u_m = u_n \quad \text{in} \quad m, n \in \mathbb{Z}, \quad m > n \geqq 0. \tag{7}$$

Moreover, we derive lower bounds for $|u_m|$ and $|u_m - u_n|$. Throughout the paper we shall use the above notations without further reference.

The most general results of this kind have been derived by ineffective methods. The theorem of Skolem-Mahler [17], [6] implies that (6) has only finitely many solutions if none of the numbers $\frac{w_i}{w_j}$ $(1 \leqq i < j \leqq s)$ is a root of unity.

K. Mahler [7] proved that if $u_m \in \mathbb{Z}$ for all m and $s = 2$, $v_1^2 + 4v_0 < 0$, $v_0 \leqq -2$, $(v_1, v_2) = 1$, then for every $\varepsilon > 0$ there exists an m_0 such that

$$|u_m| \geqq |w_1|^{(1-\varepsilon)m} \quad \text{for} \quad m \geqq m_0. \tag{8}$$

Recently some striking results were obtained by the p-adic analogue of the Thue-Siegel-Roth-Schmidt method due to H.-P. Schlickewei [14], [15]. It follows from the Main Theorem on S-units of A. J. van der Poorten and H.-P. Schlickewei [13] that (6) has only finitely many solutions provided that $|w_1| > 1$ and none of the numbers $\frac{w_i}{w_j}$ $(1 \leqq i < j \leqq r)$ is a root of unity. Moreover, for every $\varepsilon > 0$ there exists an m_0 such that (8) holds. In section 5 of [12] van der Poorten noticed consequences for equation (7). J. H. Evertse [4] derived the Main Theorem on S-units independently and applied it to $\frac{u_m}{u_n}$. For $\alpha \in F$, $\alpha \neq 0$ we define $P_F(\alpha)$ to be the maximum of the norms of the prime ideals $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(\alpha) \neq 0$. Further we put $P_F(0) = 0$. Evertse proved that if $s \geqq 2$ and none of the numbers $\frac{w_i}{w_j}$ $(1 \leqq i < j \leqq s)$ is a root of unity, then

$$\lim_{\substack{m \to \infty \\ m > n,\, u_n \neq 0}} P_F\left(\frac{u_m}{u_n}\right) = \infty. \tag{9}$$

The recurrence sequences $\{2^m\}_{m=0}^{\infty}$ and $\{m^2 2^m\}_{m=0}^{\infty}$ show that $\liminf P_F\left(\frac{u_m}{u_n}\right)$ can be finite if $s = 1$. If (9) holds, then the number of solutions of (7) is finite.

Effective methods are only applicable if r is small, but in this case better lower bounds can be derived by Baker's method on linear forms in logarithms and its p-adic analogue. If $r = 1$ and $|w_1| > 1$, then there is a dominant term. Hence (6) has only finitely many solutions and sharp bounds can be given for $|u_m|$. Mignotte [8] proved that if $\{u_m\}_{m=0}^{\infty}$ is an integer sequence and $r \leqq 3$, $\sigma_1 = \cdots = \sigma_r = 1$, then there exist computable numbers c and m_0 such that

$$|u_m| \geqq |w_1|^m m^{-c} \quad \text{for} \quad m \geqq m_0, \tag{10}$$

provided that $\sum_{j=1}^{r} P_j(m) w_j^m \neq 0$. If $r = 2$ and $\sigma_1 = \sigma_2 = 1$, the estimate (10) follows from a result of Stewart [18].

It follows from a result of Mignotte [9] that if $r=1$, $|w_1|>1$ and $u_m \in \mathbb{Z}$ for all m, then (7) implies that $P_1(m)\, w_1^m = P_1(n)\, w_1^n$. Parnami and Shorey [10] proved that if $u_m \in \mathbb{Z}$ for all m and $s=2$ and $\dfrac{w_1}{w_2}$ is not a root of unity, then (7) has only finitely many solutions. Further, under the assumptions of the latter result, Shorey [16] proved that

$$\lim_{\substack{m\to\infty \\ m>n,\, u_n\neq 0}} P_0\left(\frac{u_m}{u_n}\right)=\infty .$$

It would be interesting to have an effective proof of this fact for $s>2$.

In this paper we prove

Theorem 1. *Assume $r\leqq 3$ and at least one of the numbers $\dfrac{w_i}{w_j}$ with $1\leqq i<j\leqq r$ is not a root of unity. Then there exist computable numbers $C_1>0$ and $C_2>0$ depending only on the sequence $\{u_m\}_{m=0}^{\infty}$ such that*

$$|u_m| \geqq |w_1|^m \exp\left(-C_1(\log m)^2\right) \tag{11}$$

whenever $m \geqq C_2$.

Corollary 1. *Under the conditions of the theorem all the zeroes of the sequences $\{u_m\}_{m=0}^{\infty}$ can be determined effectively.*

We cannot prove an analogous result for $r=4$, but we have

Theorem 2. *Let $\{u_m\}_{m=0}^{\infty}$ be a sequence of real algebraic numbers. Assume that $s=4$, $|w_1|>1$ and that none of the numbers $\dfrac{w_i}{w_j}$ $(1\leqq i<j\leqq s)$ is a root of unity. Then every solution m of (6) is bounded by a computable number depending only on the sequence $\{u_m\}_{m=0}^{\infty}$.*

We shall apply Theorem 1 to prove the following theorem on $|u_m-u_n|$.

Theorem 3. *Assume $r\leqq 3$, $|w_1|>1$ and at least one of the numbers $\dfrac{w_i}{w_j}$ with $1\leqq i<j\leqq r$ is not a root of unity. Then there exist computable numbers $C_3>0$ and $C_4>0$ depending only on the sequence $\{u_m\}_{m=0}^{\infty}$ such that*

$$|u_m-u_n| \geqq |w_1|^m \mathrm{e}^{-C_3(\log m)^2 \log(n+2)} \tag{12}$$

whenever $m \geqq C_4$ and $m>n$.

Theorem 3 with $s=2$ was proved by Shorey [16].

The proofs of Theorems 1, 2 and 3 depend on the following results.

Theorem 4. *Let A_1, A_2, A_3 be non-zero algebraic numbers of degrees at most D and of heights at most H. Let γ_1, γ_2, γ_3 be non-zero algebraic numbers such that at least one of the numbers $\dfrac{\gamma_i}{\gamma_j}$ $(1\leqq i<j\leqq 3)$ is not a root of unity. Then the equation*

$$A_1\gamma_1^m + A_2\gamma_2^m + A_3\gamma_3^m = 0 \quad (m\in\mathbb{Z},\ m\geqq 0) \tag{13}$$

implies that $m\leqq C_5 \log H$ for some computable number $C_5>0$ depending only on γ_1, γ_2, γ_3 and D.

Theorem 5. *Let A_1, A_2, A_3 be as in Theorem 4. Let $\gamma_1, \gamma_2, \gamma_3$ be distinct algebraic numbers with $|\gamma_1| = |\gamma_2| = |\gamma_3|$. Let $2 \leqq m \in \mathbb{Z}$. Then either (13) or*

$$|A_1\gamma_1^m + A_2\gamma_2^m + A_3\gamma_3^m| \geqq |\gamma_1|^m m^{-C_6 \log H} \tag{14}$$

for some computable number $C_6 > 0$ depending only on $\gamma_1, \gamma_2, \gamma_3$ and D.

The proof of Theorem 5 involves a geometrical idea due to F. Beukers which was also applied in Beukers and Tijdeman [3].

§ 2. In this section, we state the results that we shall require from other sources. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. Put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $[K : \mathbb{Q}] = d$. Let the heights of $\alpha_1, \ldots, \alpha_{n-1}$ and α_n be at most A' and $A (\geqq 2)$ respectively. All the results of this paper depend on the following theorem of Baker [2] on linear forms in logarithms.

Theorem A. *There exists a computable number $C_7 > 0$ depending only on n, d and A' such that, for any δ with $0 < \delta < \frac{1}{2}$, the inequalities*

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < \left(\frac{\delta}{B'}\right)^{C_7 \log A} e^{-\delta B}$$

have no solution in rational integers $b_1, \ldots, b_{n-1}$ and $b_n (\neq 0)$ with absolute values at most B and B' respectively.

(It is assumed that the logarithms have their principal values.)

Putting $\delta = \frac{1}{B}$ and $B' = B$, theorem A includes the following result which is also due to Baker [1].

Theorem B. *There exists a computable number $C_8 > 0$ depending only on n, d and A' such that the inequalities*

$$0 < |\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| < \exp(-C_8 \log A \log B)$$

have no solution in rational integers $b_1, \ldots, b_n$ with absolute values at most $B (\geqq 3)$.

We shall use the following immediate consequence of theorem B several times. It is case $\delta = \frac{1}{m}$ of [16], lemma 1.

Corollary 2. *Let λ and μ be non-zero algebraic numbers such that $\frac{\lambda}{\mu}$ is not a root of unity. Suppose that a_1 and a_2 are non-zero algebraic numbers of degrees at most D and heights not exceeding $H (\geqq 3)$. Let $n \geqq 2$ be a rational integer. There exist computable numbers $C_9 > 0$ and $C_{10} > 0$ depending only on D, λ and μ such that*

$$|a_1\lambda^n + a_2\mu^n| \geqq (\max\{|\lambda|, |\mu|\})^n H^{-C_9 \log n}$$

whenever $n \geqq C_{10} \log H$.

We shall also require the following p-adic analogue, due to van der Poorten [11].

Theorem C. *Let* $\mathfrak{p}$ *be a prime ideal of* K *lying above a rational prime* p. *Suppose that* $b_1, \ldots, b_{n-1}$ *and* $b_n = -1$ *are rational integers of absolute values at most* B. *There exists a computable number* $C_{11} > 0$ *depending only on* n, d *and* A' *such that for any* δ *with* $0 < \delta < 1$, *the inequalities*

$$\infty > \operatorname{ord}_{\mathfrak{p}} (\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) > \delta B$$

implies that

$$B \leqq C_{11} \delta^{-1} p^d \log(\delta^{-1} p^d) \log A.$$

§ 3. In this section, we shall prove theorems 4 and 5. The constants $g_1, g_2, \ldots$ in the proofs of theorems 4 and 5 are positive computable numbers depending only on $\gamma_1, \gamma_2, \gamma_3$ and D.

Proof of theorem 4. Suppose that the assumptions of theorem 4 are satisfied and (13) is valid. There is no loss of generality in assuming that $\frac{\gamma_1}{\gamma_2}$ is not a root of unity. Further we may assume that $m \geqq g_1 \log H$ with g_1 sufficiently large. Denote by L the field generated over $\mathbb{Q}$ by $A_1, A_2, A_3, \gamma_1, \gamma_2$ and γ_3. Observe that $[L : \mathbb{Q}] \leqq g_2$.

Assume that $\frac{\gamma_1}{\gamma_2}$ is not a unit. Then there exists a prime ideal $\mathfrak{p}$ in the ring of integers of L such that $\operatorname{ord}_{\mathfrak{p}} \left(\frac{\gamma_1}{\gamma_2}\right)$ is non-zero. By permuting the indices of γ_1 and γ_2, we may suppose that $\operatorname{ord}_{\mathfrak{p}} \left(\frac{\gamma_1}{\gamma_2}\right) > 0$. Then, by (13), we see that $A_2 \gamma_2^m + A_3 \gamma_3^m \neq 0$ and

$$m \leqq \operatorname{ord}_{\mathfrak{p}} \left(\left(\frac{\gamma_1}{\gamma_2}\right)^m\right) = \operatorname{ord}_{\mathfrak{p}} (A_2 A_1^{-1}) + \operatorname{ord}_{\mathfrak{p}} \left(-\left(\frac{\gamma_3}{\gamma_2}\right)^m \frac{A_3}{A_2} - 1\right). \tag{15}$$

Observe that

$$\operatorname{ord}_{\mathfrak{p}} (A_2 A_1^{-1}) \leqq g_3 \log H. \tag{16}$$

For $g_1 \geqq 2g_3$, we can apply theorem C with $n = 2$, $d \leqq g_4$, $p \leqq g_4$, $\delta = \frac{1}{2}$, $A' = g_5$, $A = H^{g_6}$ and $B = m$ to conclude that

$$m \leqq g_7 \log H. \tag{17}$$

Thus we may assume that $\frac{\gamma_1}{\gamma_2}$ is a unit. Then, since $\frac{\gamma_1}{\gamma_2}$ is not a root of unity, there exists an embedding σ of L such that $\left|\sigma\left(\frac{\gamma_1}{\gamma_2}\right)\right| > 1$. Therefore $|\sigma(\gamma_1)| > |\sigma(\gamma_2)|$. By taking images under σ on both the sides in (13), we may suppose that $|\gamma_1| > |\gamma_2|$. By (13), $A_1 \gamma_1^m + A_3 \gamma_3^m \neq 0$. Further we may write

$$0 \neq |A_1 \gamma_1^m + A_3 \gamma_3^m| = |A_1 \gamma_1^m| \left|-\left(\frac{\gamma_3}{\gamma_1}\right)^m \frac{A_3}{A_1} - 1\right|. \tag{18}$$

We apply theorem A with $n=3$, $\delta=\min\left(\frac{1}{2}\log\left|\frac{\gamma_1}{\gamma_2}\right|, \frac{1}{4}\right)$, $d\leqq g_4$, $\log A'=g_8$, $\log A=g_9\log H$, $B'=1$ and $B=m+2$ to

$$\left|\mathscr{K}\log(-1)+m\log\left(\frac{\gamma_3}{\gamma_1}\right)+\log\left(\frac{A_3}{A_1}\right)\right|$$

where $\mathscr{K}$ with $|\mathscr{K}|\leqq m+2$ is a rational integer and the logarithms have their principal values. We obtain

$$\left|-\left(\frac{\gamma_3}{\gamma_1}\right)^m\frac{A_3}{A_1}-1\right|\geqq\left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{m}{2}}H^{-g_{10}}. \tag{19}$$

Consequently, by (18), (19) and $|A_1|\geqq(DH)^{-1}$, we conclude that

$$|A_1\gamma_1^m+A_3\gamma_3^m|\geqq|\gamma_1|^m\left|\frac{\gamma_1}{\gamma_2}\right|^{-\frac{m}{2}}H^{-g_{11}}. \tag{20}$$

Further, by $|A_2|\leqq DH$, we have

$$|A_2\gamma_2^m|\leqq DH|\gamma_2|^m. \tag{21}$$

Now it follows from (13), (20) and (21) that

$$\left|\frac{\gamma_1}{\gamma_2}\right|^{\frac{m}{2}}\leqq H^{g_{12}}$$

which, together with $\left|\frac{\gamma_1}{\gamma_2}\right|>1$, implies that $m\leqq g_{13}\log H$. This completes the proof of theorem 4.

Proof of theorem 5. Without loss of generality, we may assume $|A_2|\leqq|A_1|\leqq|A_3|$ and $A_1\gamma_1^m+A_2\gamma_2^m+A_3\gamma_3^m\neq0$. Put

$$v_m=-\frac{A_1}{A_3}\left(\frac{\gamma_1}{\gamma_3}\right)^m-\frac{A_2}{A_3}\left(\frac{\gamma_2}{\gamma_3}\right)^m-1,\quad m=1,2,\ldots. \tag{22}$$

Then v_m is of the form

$$v_m=a_1\alpha_1^m-a_2\alpha_2^m-1 \tag{23}$$

with $a_1, a_2, \alpha_1, \alpha_2$ algebraic, $0<|a_2|\leqq|a_1|\leqq1$, $\alpha_1\neq\alpha_2$ and $|\alpha_1|=|\alpha_2|=1$. Note that $v_m\neq0$ and that the heights of a_1 and a_2 do not exceed $g_{14}H^2$. Let η be any positive number with $\eta<\frac{1}{2}$. We distinguish two cases:

(i) $\underline{|a_1|+|a_2|\leqq1+\eta}$. Put $|a_1\alpha_1{}^m|=|a_1|=r_1$. If $|v_m|<\min\left(r_1,\frac{1}{2}\right)$, then, by (23),

$$r_1-\mathrm{Re}(a_1\alpha_1^m)\leqq r_1-\mathrm{Re}\,v_m-\mathrm{Re}(a_2\alpha_2^m)-1\leqq|a_1|+|v_m|+|a_2|-1\leqq|v_m|+\eta.$$

Hence

$$(\mathrm{Im}(a_1\alpha_1^m))^2 = r_1^2 - (\mathrm{Re}(a_1\alpha_1^m))^2 \leqq (|v_m|+\eta)\cdot 2r_1.$$

It follows that

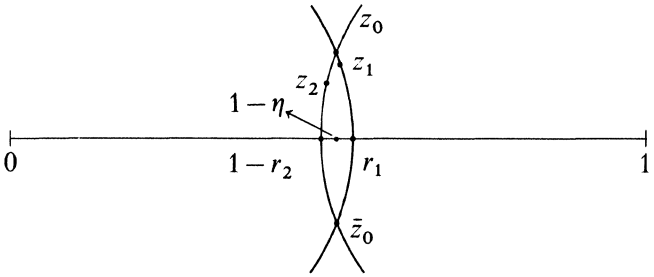
$$|r_1 - a_1\alpha_1^m| \leqq |r_1 - \mathrm{Re}(a_1\alpha_1^m)| + |\mathrm{Im}(a_1\alpha_1^m)|$$
$$\leqq (|v_m|+\eta) + 2\sqrt{|v_m|+\eta} \leqq 3\sqrt{|v_m|+\eta}.$$

Thus

$$|v_m| \geqq \min\left(r_1, \frac{1}{2}, \frac{1}{9}|r_1 - a_1\alpha_1^m|^2 - \eta\right). \tag{24}$$

(ii) $|a_1|+|a_2|>1+\eta$. Put $r_1=|a_1|$, $r_2=|a_2|$. Note that $z_1 := a_1\alpha_1^m$ is on the circle $|z|=r_1$ and that $z_2 = a_2\alpha_2^m + 1$ is on the circle $|z-1|=r_2$. These circles intersect in two points, z_0 and $\bar{z_0}$. We may assume that $(\mathrm{Im}\, z_0)(\mathrm{Im}\, z_1) \geqq 0$. Because of symmetry it is no restriction to assume that $\mathrm{Im}\, z_0 > 0$. Put $z_0 = x+iy$. By $x^2+y^2=r_1^2$, $(1-x)^2+y^2=r_2^2$ and $y \leqq r_2 \leqq r$ we have

$$1 = x + (1-x) = \sqrt{r_1^2 - y^2} + \sqrt{r_2^2 - y^2}$$
$$= r_1\sqrt{1-\frac{y^2}{r_1^2}} + r_2\sqrt{1-\frac{y^2}{r_2^2}} \geqq r_1\left(1-\frac{y^2}{r_1^2}\right) + r_2\left(1-\frac{y^2}{r_2^2}\right).$$



We infer, by $r_2 > 1+\eta-r_1 \geqq \eta$,

$$\eta < r_1 + r_2 - 1 \leqq \frac{y^2}{r_1} + \frac{y^2}{r_2} \leqq \frac{2y^2}{r_2} \leqq \frac{2y^2}{\eta}. \tag{25}$$

We shall derive a lower bound for $|v_m| = |z_1 - z_2|$. Observe that

$$|z_1 - 1|^2 = r_1^2 + 1 - 2\,\mathrm{Re}\, z_1,$$
$$|z_2 - 1|^2 = |z_0 - 1|^2 = r_1^2 + 1 - 2\,\mathrm{Re}\, z_0.$$

Hence

$$2|\mathrm{Re}\, z_1 - \mathrm{Re}\, z_0| = |\,|z_1-1|^2 - |z_2-1|^2\,| \leqq |z_1 - z_2|\cdot(|z_1|+|z_2|+2),$$

which implies

$$|\mathrm{Re}\, z_1 - \mathrm{Re}\, z_0| \leqq 3|z_1 - z_2|. \tag{26}$$

From $|z_0| = |z_1|$ and (26) we obtain

$$|(\mathrm{Im}\, z_1)^2 - (\mathrm{Im}\, z_0)^2| = |(\mathrm{Re}\, z_1)^2 - (\mathrm{Re}\, z_0)^2| \leqq 6|z_1 - z_2|. \tag{27}$$

On the other hand, by $\mathrm{Im}\, z_1 \geqq 0$ and $\mathrm{Im}\, z_0 = y > 0$,

$$|(\mathrm{Im}\, z_1)^2 - (\mathrm{Im}\, z_0)^2| \geqq |\mathrm{Im}\, z_1 - \mathrm{Im}\, z_0|\, y. \tag{28}$$

On combining (28), (27) and (25) we see that

$$\left|\mathrm{Im}\, z_1 - \mathrm{Im}\, z_0\right| \leqq \frac{6\sqrt{2}}{\eta}\left|z_1 - z_2\right|. \tag{29}$$

By (26) and (29),

$$|z_1 - z_0| \leqq \left(3 + \frac{9}{\eta}\right)|z_1 - z_2|,$$

or, equivalently,

$$|v_m| \geqq \frac{\eta}{3\eta + 9}|a_1 \alpha_1^m - z_0|. \tag{30}$$

Subsequently we show that z_0 is an algebraic number of degree at most $g_{15} H^{g_{16}}$. By $z_0 \overline{z_0} = a_1 \overline{a_1}$ and $(1 - z_0)(1 - \overline{z_0}) = (1 - a_2)(1 - \overline{a_2})$ we have $z_0 + \overline{z_0} = a_2 + \overline{a_2} - a_2 \overline{a_2} + a_1 \overline{a_1}$. Thus

$$(z - z_0)(z - \overline{z_0}) = z^2 - (a_2 + \overline{a_2} - a_2 \overline{a_2} + a_1 \overline{a_1})\, z + a_1 \overline{a_1}.$$

This proves that z_0 is algebraic indeed and that z_0 can be expressed in a_1 and a_2 by using only sums, products and square roots. On using simple estimates for the heights of sums, products, quotients and square roots of algebraic numbers it becomes clear that we may assume without loss of generality that the heights of the numbers a_1, a_2, $r_1 = (a_1 \overline{a_1})^{\frac{1}{2}}$, $r_1 - 1$, $\frac{r_1^2}{9}$, $\frac{a_1}{r_1}$, $\frac{a_2}{r_1 - 1}$, z_0, $z_0 - 1$, $\frac{a_1}{z_0}$ and $\frac{a_2}{z_0 - 1}$ are at most $g_{17} H^{g_{18}}$. Hence these numbers are in absolute values at least $g_{19}^{-1} H^{-g_{18}}$. We use these estimates in the sequel without further reference.

Case (i). If $a_1 \alpha_1^m = r_1 = 1$, then $v_m = -a_2 \alpha_2^m$ and hence

$$|v_m| = |a_2|\, |\alpha_2|^m = |a_2| \geqq \frac{1}{g_{19} H^{g_{18}}} \geqq \exp(-g_{20} \log m \log H). \tag{31}$$

If $a_1 \alpha_1^m = r_1 < 1$, then $v_m = r_1 - 1 - a_2 \alpha_2^m$. On applying theorem B we obtain

$$\begin{aligned} |v_m| = |r_1 - 1|\, |\alpha_2^m \frac{a_2}{r_1 - 1} - 1| &\geqq \frac{1}{g_{19} H^{g_{18}}} \exp(-g_{21} \log m \log H) \\ &\geqq \exp(-g_{22} \log m \log H). \end{aligned} \tag{32}$$

If $a_1 \alpha_1^m \neq r_1$, then we find by applying theorem B,

$$\frac{1}{9}|r_1 - a_1 \alpha_1^m|^2 = \frac{r_1^2}{9}\left|\alpha_1^m \left(\frac{a_1}{r_1}\right) - 1\right| \geqq 2\exp(-g_{23} \log m \log H)$$

where g_{23} is chosen so large that the right hand side is less than one. Put

$$\eta = \exp(-g_{23} \log m \log H).$$

Then $\eta < \frac{1}{2}$ and, by (24),

$$|v_m| \geqq \min(r_1, \eta) \geqq \exp(-g_{24} \log m \log H). \tag{33}$$

Case (ii). If $a_1 \alpha_1^m = z_0$, then $v_m = z_0 - 1 - a_2 \alpha_2^m$ and hence, by theorem B,

$$|v_m| = |z_0 - 1| \left| \alpha_2^m \frac{a_2}{z_0 - 1} - 1 \right| \geqq \exp(-g_{25} \log m \log H). \tag{34}$$

If $a_1 \alpha_1^m \neq z_0$, then, by (30), $\eta < 1$ and theorem B,

$$|v_m| \geqq \frac{\eta |z_0|}{12} \left| \alpha_1^m \left(\frac{a_1}{z_0} \right) - 1 \right| \geqq \exp(-g_{26} \log m \log H). \tag{35}$$

By (31)—(35) and $|\gamma_1| = |\gamma_3|$ we deduce

$$|A_1 \gamma_1^m + A_2 \gamma_2^m + A_3 \gamma_3^m| = |A_3| \, |v_m| \, |\gamma_1|^m \geqq |\gamma_1|^m \exp(-g_{27} \log m \log H).$$

This completes the proof of theorem 5.

§ 4. In this section, we shall prove theorems 1 and 3. The proofs of the theorems depend on the following result.

Lemma 1. *Let $P(X)$ be a non-constant polynomial with algebraic numbers as coefficients and w a non-zero algebraic number. For non-negative integers m and n with $m > n$, the equation*

$$P(m) \, w^m = P(n) \, w^n \tag{36}$$

implies that m is bounded by a computable number depending only on P and w.

Proof of lemma 1. Let P and w be as in lemma 1. Suppose that m and n with $m > n$ are non-negative integers satisfying (36). Denote by $f_1, f_2, \ldots$ positive computable numbers depending only on P and w. We may assume that $m \geqq f_1$ with f_1 sufficiently large. Denote by L_1 the field generated over $\mathbb{Q}$ by w and the coefficients of P. Write $v = \deg P \geqq 1$.

Suppose w is a root of unity. Then $w^\mu = 1$ for some positive integer μ. Consequently, by (36),

$$Q(m) = Q(n) \tag{37}$$

where

$$Q(X) = (P(X))^\mu.$$

Observe that $Q(X)$ is a polynomial of degree $\rho = \mu v \geqq 1$. By (37), we see that $\rho \geqq 2$ and

$$m^{\rho - 1} \leqq \frac{m^\rho - n^\rho}{m - n} \leqq f_2 m^{\rho - 2}$$

which implies that $m \leqq f_2$.

Thus we may assume that w is not a root of unity. We, first, prove that

$$m-n \leqq f_3 \log m. \tag{38}$$

If w is not a unit, there exists a prime ideal $\mathfrak{p}$ in the ring of integers of L_1 such that $\mathrm{ord}_{\mathfrak{p}}(w)$ is non-zero. Counting the power of the prime ideal $\mathfrak{p}$ on both the sides in (36), we obtain (38). Suppose w is a unit. Then, since w is not a root of unity, there exists an embedding σ of L_1 such that $|\sigma(w)|>1$. Further, by taking images under σ on both the sides in (36), we have

$$|\sigma(w)|^{m-n} = \left|\frac{\sigma(P(n))}{\sigma(P(m))}\right|$$

and inequality (38) follows from a Liouville-type argument.

Re-writing (36), we have

$$w^{m-n}-1 = \frac{P(n)-P(m)}{P(m)}. \tag{39}$$

Observe that

$$|P(n)-P(m)| \leqq f_4(m-n)\, m^{\nu-1}$$

and, by taking f_1 large enough,

$$|P(m)| \geqq f_5 m^{\nu}.$$

Thus we obtain from (39) and (38), since w is not a root of unity,

$$0<|w^{m-n}-1| \leqq f_6 m^{-1} \log m.$$

Now we apply theorem B with $n=1$, $d=f_7$, $\log A = f_8$ and, by (38), $B=m-n+1 \leqq 2f_3 \log m$ to conclude that

$$|w^{m-n}-1| \geqq (\log m)^{-f_9}.$$

Consequently $m \leqq f_6 (\log m)^{f_9+1}$ which implies that $m \leqq f_{10}$. This completes the proof of lemma 1.

Corollary 3. *Let $P(X) \not\equiv 0$ be a polynomial with algebraic numbers as coefficients and w a non-zero algebraic number. Suppose that w is not a root of unity. For non-negative integers m and n with $m>n$, equation* (36) *implies that m is bounded by a computable number depending only on P and w.*

Corollary 1 with "$|w|>1$" in place of "w not a root of unity" is sufficient for our purpose.

Proof of corollary 3. In view of lemma 1, we may assume that $\deg P = 0$. Then equation (36) implies that w is a root of unity. This completes the proof of corollary 3.

The constants $c_1, c_2, \ldots$ in the proofs of theorems 1—3 are positive computable numbers depending only on the sequence $\{u_m\}_{m=0}^{\infty}$.

Proof of theorem 1. Let $\{u_m\}_{m=0}^{\infty}$ be as in theorem 1. We may assume that $m \geqq c_1$ with c_1 sufficiently large. Put

$$\Lambda = P_1(m)\, w_1^m + \cdots + P_r(m)\, w_r^m.$$

Observe that

$$|u_m| \geqq |\Lambda| - \delta,$$

where, in view of (3),

$$\delta = m^{c_2} |w_{r+1}|^m.$$

Thus, in view of (4), it suffices to show that

$$|\Lambda| \geqq |w_1|^m \exp\left(-c_3 (\log m)^2\right), \quad m \geqq c_1. \tag{40}$$

If $r = 1$, estimate (40) follows immediately. If $r = 2$, we apply corollary 2, with $n = m$, $a_1 = P_1(m)$, $a_2 = P_2(m)$, $\lambda = w_1$, $\mu = w_2$ and $\log H = c_4 \log m$ to obtain (40). Thus we may suppose $r = 3$. We apply theorem 4 with $A_i = P_i(m)$, $\gamma_i = w_i$ for $1 \leqq i \leqq 3$ and $\log H = c_5 \log m$ to conclude that

$$\Lambda \neq 0$$

if c_1 is sufficiently large. Then, by theorem 5 with the same choice of the parameters, we obtain (40). This completes the proof of theorem 1.

Proof of theorem 3. Let $\{u_m\}_{m=0}^{\infty}$ be as in theorem 3 and $m > n \geqq 0$ be rational integers. We may assume that $m \geqq c_6$ with c_6 sufficiently large. Let $c_6 > c_2$ so that estimate (11) is valid. We may suppose that

$$|u_m| < 2|u_n|, \tag{41}$$

otherwise

$$|u_m - u_n| \geqq |u_m| - |u_n| \geqq \frac{|u_m|}{2}$$

and (12) follows from (11). Further, since $m > n$, observe that

$$|u_n| \leqq m^{c_7} |w_1|^n. \tag{42}$$

Now it follows from (41), (11), (42) and $|w_1| > 1$ that

$$m - n \leqq c_8 (\log m)^2. \tag{43}$$

Consequently, by taking c_6 large enough, we have

$$n \geqq \frac{m}{2}.$$

For $1 \leqq i \leqq r$, put

$$B_i = P_i(m)\, w_i^{m-n} - P_i(n)$$

and

$$\Lambda_1 = B_1 w_1^n + \cdots + B_r w_r^n. \tag{44}$$

Observe that

$$|u_m - u_n| \geqq |\Lambda_1| - \delta_1$$

where

$$\delta_1 = m^{c_9} \max\{1, |w_{r+1}|^m\}.$$

Consequently, by (4) and $|w_1| > 1$, it suffices to prove that

$$|\Lambda_1| \geqq |w_1|^m \exp(-c_{10}(\log m)^2 \log n). \tag{45}$$

In view of (43), observe that $B_1, \ldots, B_r$ are algebraic numbers of heights not exceeding $\exp(c_{11}(\log m)^2)$. By taking c_6 sufficiently large, we obtain from corollary 3 and $|w_r| = \cdots = |w_1| > 1$ that $B_1 \cdots B_r \neq 0$. Consequently, by a Liouville argument, it follows that

$$|B_1| \geqq \exp(-c_{12}(\log m)^2). \tag{46}$$

If $r = 1$, estimate (45) follows from (44), (46) and (43). Suppose $r = 2$. We apply corollary 2 with $a_1 = B_1$, $a_2 = B_2$, $\lambda = w_1$, $\mu = w_2$ and $\log H = c_{11}(\log m)^2$ to obtain

$$|\Lambda_1| \geqq |w_1|^n \exp(-c_{13}(\log m)^2 \log n). \tag{47}$$

Here we use that, if c_6 is large enough, then (43) implies that $n \geqq c_{11} \log H$ where c_{11} is the constant occurring in theorem D. Now combine (47) and (43) to obtain (45). Thus we may assume $r = 3$. Then apply theorem 4 with $A_i = B_i$, $\gamma_i = w_i$ for $1 \leqq i \leqq 3$ and $\log H = c_{11}(\log m)^2$ to conclude that

$$\Lambda_1 \neq 0$$

if c_6 is sufficiently large. By theorem 5 with the same choice of the parameters we obtain (47) which, together with (43), implies (45). This completes the proof of theorem 3.

§ 5. *Proof of theorem* 2. Let $\{u_m\}_{m=0}^{\infty}$ be as in theorem 2. In view of corollary 1, we may assume $r = 4$. Further, since $\{u_m\}_{m=0}^{\infty}$ is a sequence of real algebraic numbers, observe that $v_0, v_1, \ldots, v_{k-1}$ are real algebraic numbers. By considering the sequence $\{v^m u_m\}_{m=0}^{\infty}$ where v is the least positive integer such that $vw_1, \ldots, vw_4$ are algebraic integers, we see that there is no loss of generality in assuming that the coefficients of the companion polynomial to $\{u_m\}_{m=0}^{\infty}$ are real algebraic integers. Since none of the $\frac{w_i}{w_j}$ with $1 \leqq i, j \leqq 4$ and $i \neq j$ is ± 1, it follows that $w_1, \ldots, w_4$ are non-real algebraic integers. Further, by permuting the indices of $w_1, \ldots, w_4$, there is no loss of generality in supposing that

$$w_1 = \overline{w_3}, \quad w_2 = \overline{w_4}. \tag{48}$$

Put $L_2 = F(w_1, \ldots, w_4)$ and denote by h the class number of L_2. For an integer $m \geqq 0$, suppose that (6) is satisfied. We may assume that $m \geqq c_{14}$ with c_{14} sufficiently large.

Suppose $\frac{w_1}{w_3}$ is a unit. Then, since $\frac{w_1}{w_3}$ is not a root of unity, there exists an embedding σ of L_2 such that $|\sigma(w_1)| > |\sigma(w_3)|$. Further (6) implies $\sigma(u_m) = 0$ which, by theorem 1, is not possible if c_{14} is large enough.

Thus we may assume that $\frac{w_1}{w_3}$ is not a unit. Further notice that

$$([w_1^h], [w_2^h], [w_3^h], [w_4^h]) = [\Pi]$$

where Π is an algebraic integer in L_2. For $1 \leqq i \leqq 4$, put

$$W_i = w_i^h \Pi^{-1}. \tag{49}$$

Notice that $W_1, \ldots, W_4$ are algebraic integers in L_2 satisfying

$$([W_1], [W_2], [W_3], [W_4]) = [1]. \tag{50}$$

It follows from (49), (48) and $|w_3| = |w_4|$ that

$$W_1 W_3 = W_2 W_4. \tag{51}$$

Since $\frac{w_1}{w_3}$ is not a unit, it follows from (49) that $\frac{W_1}{W_3}$ is not a unit. We know that W_1 and W_3 are algebraic integers. Hence $W_1 W_3$ is not a unit. Thus there exists a prime ideal $\mathfrak{p}$ in the ring of integers of L_2 such that $\mathfrak{p} | W_1 W_3$. Consequently, by (51), $\mathfrak{p} | W_2 W_4$. By permuting the indices of W_1, W_3 and W_2, W_4, there is no loss of generality in assuming that

$$\mathfrak{p} | W_3, \quad \mathfrak{p} | W_4. \tag{52}$$

Write $m = nh + q$ with $0 \leqq q < h$ and $p_i(X) = P_i(X) w_i^q$ for $1 \leqq i \leqq 4$. Then $n + 1 > mh^{-1}$. Consequently we see that

$$n \geqq \frac{m}{2h} \geqq \frac{c_{14}}{2h}. \tag{53}$$

Dividing both the sides of (6) by Π^{-n}, we obtain

$$p_1(m) W_1^n + p_2(m) W_2^n = -p_3(m) W_3^n - p_4(m) W_4^n.$$

By counting the power of prime ideal $\mathfrak{p}$ on both the sides, it follows from (52) that

$$n \leqq c_{15} \log m + \operatorname{ord}_{\mathfrak{p}}(\Delta) \tag{54}$$

where

$$\Delta = p_1(m) W_1^n + p_2(m) W_2^n.$$

By (49) and the fact that $\frac{w_1}{w_2}$ is not a root of unity, we see that $\frac{W_1}{W_2}$ is not a root of unity. Further, by taking c_{14} large enough, it follows from theorem D that $\Delta \neq 0$.

In view of (50) and (52), we find that either $\mathfrak{p} \nmid W_1$ or $\mathfrak{p} \nmid W_2$. For simplicity, assume that $\mathfrak{p} \nmid W_1$. Then

$$\operatorname{ord}_{\mathfrak{p}}(\Delta) \leqq c_{16} \log m + \operatorname{ord}_{\mathfrak{p}}\left(-\left(\frac{W_2}{W_1}\right)^n \frac{p_2(m)}{p_1(m)} - 1\right). \tag{55}$$

We apply theorem C with $n=3$, $d=c_{17}$, $p=c_{18}$, $\delta=\frac{1}{4h}$, $\log A=c_{20}\log m$ and, by (53), $B=n\geqq\frac{m}{2h}$ to conclude that

$$\text{ord}_{\mathfrak{p}}\left(-\left(\frac{W_2}{W_1}\right)^n\frac{p_2(m)}{p_1(m)}-1\right)\leqq\frac{n}{4h}\leqq\frac{m}{4h} \tag{56}$$

if c_{14} is sufficiently large. Combining (54), (53), (55) and (56), we obtain

$$\frac{m}{2h}\leqq(c_{15}+c_{16})\log m+\frac{m}{4h}$$

which implies that $m\leqq c_{21}$. This completes the proof of theorem 3.

References

[1] *A. Baker*, A sharpening of the bounds for linear forms in logarithms. I, Acta Arith. **21** (1972), 117—129.

[2] *A. Baker*, A sharpening of the bounds for linear forms in logarithms. II, Acta Arith. **24** (1973), 33—36.

[3] *F. Beukers* and *R. Tijdeman*, On the multiplicities of binary complex recurrences, Compositio Math. (to appear).

[4] *J. H. Evertse*, On sums of S-units and linear recurrences, Compositio Math. (to appear).

[5] *D. J. Lewis*, Diophantine equations: p-adic methods, Studies in Number Theory, Englewood Cliffs, N. J. 1969, 25—75.

[6] *K. Mahler*, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, Akad. Wetensch. Amsterdam Proc. **38** (1935), 50—60.

[7] *K. Mahler*, A remark on recursive sequences, J. Math. Sci. **1** (1966), 12—17.

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

[9] *M. Mignotte*, Une extension du théorème Skolem-Mahler, C. R. Acad. Sc. Paris **288** (Série A) (1979), 233—235.

[10] *J. C. Parnami* and *T. N. Shorey*, Subsequences of binary recursive sequences, Acta Arith. **40** (1982), 193—196.

[11] *A. J. van der Poorten*, Linear forms in logarithms in the p-adic case, Transcendence Theory: Advances and Applications, London and New York 1977, 29—57.

[12] *A. J. van der Poorten*, Some problems of recurrent interest, Report **81-0037**, Macquarie University, N. S. W., Australia, 1981.

[13] *A. J. van der Poorten* and *H. P. Schlickewei*, The growth conditions for recurrence sequences, Report **82-0041,** Macquarie University, N. S. W., Australia, 1982.

[14] *H. P. Schlickewei*, Linearformen mit algebraischen Koeffizienten, Manuscripta Math. **18** (1976), 147—185.

[15] *H. P. Schlickewei*, The p-adic Thue-Siegel-Roth-Schmidt Theorem, Arch. Math. **29** (1977), 267—270.

[16] *T. N. Shorey*, Linear forms in members of a binary recursive sequence, Acta Arith. (to appear).

[17] *Th. Skolem*, Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. 8. Skand. Mat. Kongr. (1935), 163—188.

[18] *C. L. Stewart*, Divisor Properties of Arithmetical Sequences, Ph. D. thesis, Cambridge 1976.

Université Louis Pasteur, Centre de Calcul de l'Esplanade, 7, rue René Descartes, F-67084 Strasbourg, Cédex

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay-400005, India

Mathematical Institute, Wassenaarseweg 80, NL-Leiden

Eingegangen 16. März 1983