On the greatest square free factor of terms of a linear recurrence sequence

by

C.L. Stewart*

For Professor Tarlok Shorey on the occasion of his 60$^{\text{th}}$ birthday.

1. Introduction

Let $r_1, \ldots, r_k$ and $u_0, \ldots, u_{k-1}$ be integers and put

$$u_n = r_1 u_{n-1} + \cdots + r_k u_{n-k}, \tag{1}$$

for $n = k,\ k+1, \ldots$. The sequence $(u_n)_{n=0}^{\infty}$ is a linear recurrence sequence. Let $\mathbb{Q}$ denote the field of rational numbers. It is well known, see [2, p. 62] or [11, p. 33], that

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \tag{2}$$

where $f_1, \ldots, f_t$ are non-zero polynomials with degrees less than $\ell_1, \ldots, \ell_t$ respectively and with coefficients from $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ where $\alpha_1, \ldots, \alpha_t$ are the non-zero roots of the characteristic polynomial

$$X^k - r_1 X^{k-1} - \cdots - r_k,$$

and $\ell_1, \ldots, \ell_t$ are their respective multiplicities. The sequence $(u_n)_{n=0}^{\infty}$ is said to be non-degenerate if $t > 1$ and α_i/α_j is not a root of unity for $1 \le i < j \le t$. In 1935 Mahler [3] proved that if u_n is the n-th term of a non-degenerate linear recurrence sequence then

$$|u_n| \to \infty \quad \text{as } n \to \infty. \tag{3}$$

For any integer m let $P(m)$ denote the greatest prime factor of m and let $Q(m)$ denote the greatest square free factor of m with the convention that $P(0) = P(\pm 1) = 1 = Q(\pm 1) = Q(0)$. Thus, if $m = p_1^{h_1} \cdots p_r^{h_r}$ with $p_1, \ldots, p_r$ distinct primes and $h_1, \ldots, h_r$ positive integers, then $Q(m) = p_1 \cdots p_r$.

van der Poorten and Schlickewei [6] and Evertse [1] proved, by means of a p-adic version of Schmidt's Subspace Theorem due to Schlickewei [8], that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate linear recurrence sequence then

$$P(u_n) \to \infty \quad \text{as } n \to \infty. \tag{4}$$

Estimates (3) and (4) are both ineffective. On the other hand if one of the roots of the characteristic polynomial has modulus strictly larger than the others, say

$$|\alpha_1| > |\alpha_i|, \quad i = 2, \ldots, t, \tag{5}$$

*This research was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

then

$$|u_n| > c_1 n^{\ell_1} |\alpha_1|^n,$$

for $n > c_2$ where c_1 is one half of the absolute value of the coefficient of x^{ℓ_1} in the polynomial f_1 and where c_2 is a positive number which is effectively computable in terms of $\alpha_1, \ldots, \alpha_t$ and $f_1, \ldots, f_t$. In 1982 Stewart [13] obtained effective estimates from below for the greatest prime factor and the great square-free factor of u_n in the case that (5) holds. In particular, if $u_n \neq f_1(n)\alpha_1^n$, then, for any $\varepsilon > 0$,

$$P(u_n) > (1 - \varepsilon) \log n \tag{6}$$

and

$$Q(u_n) > n^{1-\varepsilon}, \tag{7}$$

for $n > c_3$, a number which is effectively computable in terms of $\varepsilon,\ \alpha_1, \ldots, \alpha_t$ and $f_1, \ldots, f_t$. Estimates (6) and (7) were established by means of a version, due to Waldschmidt [16], of Baker's theorem on linear forms in the logarithms of algebraic numbers. Shparlinski [12] independently proved (6) in the case that $f_1(n)$ is a non-zero constant and with $1-\varepsilon$ replaced by a small positive number.

The purpose of this note is to show that estimates (6) and (7) may be improved with the help of a recent result of Matveev [4] on linear forms in the logarithms of algebraic numbers.

Theorem 1. *Let α be a real algebraic number with absolute value greater than one and let f be a non-zero polynomial with coefficients which are algebraic numbers. Let δ be a real number with $0 < \delta < 1$, let n be a positive integer and let $u(n)$ be an integer for which*

$$0 < |u(n) - f(n)\alpha^n| < |\alpha|^{\delta n}. \tag{8}$$

There exist positive numbers $C_1,\ C_2$ and C_3, which are effectively computable in terms of $\delta,\ \alpha$ and f, such that if n exceeds C_3 and $f(n)$ is non-zero, then

$$P(u(n)) > C_1 \log n \frac{\log\log n}{\log\log\log n} \tag{9}$$

and

$$Q(u(n)) > n^{C_2 (log \log n)/ \log\log\log n}. \tag{10}$$

In particular, if u_n is the n-th term of a non-degenerate linear recurrence sequence, defined as in (2), $|\alpha_1| > |\alpha_j|$ for $j = 2, \ldots, t$ and $u_n \neq f_1(n)\alpha_1^n$, then estimates (9) and (10) hold with $u(n)$ replaced by u_n.

For any real number x let $[x]$ denote the greatest integer less than or equal to x and let $\langle x \rangle$ denote the nearest integer to x with the proviso that if x is an integer then $\langle x + 1/2 \rangle$ equals x. Further, as in [13] and following an idea of Mignotte [5], we may apply Theorem 1 to integers of the form $[\lambda\theta^n]$ or $\langle \lambda\theta^n \rangle$ where λ and θ are non-zero real algebraic numbers with $|\theta| > 1$ for which $\lambda\theta^n$ is not an integer. In particular, in this case there exist positive numbers $c_4,\ c_5$ and c_6 which are effectively computable in terms of λ and θ, such that for $n > c_4$,

$$P([\lambda\theta^n]) > c_5 \log n \frac{\log\log n}{\log\log\log n},$$

and

$$Q([\lambda\theta^n]) > n^{c_6 (\log\log n)/\log\log\log n}.$$

In the special case of binary recurrence sequences, so $k = 2$ in (1), stronger estimates apply than those which follow from (9) and (10). If u_n is the n-th term of a binary recurrence sequence, then, for $n \geq 0$,

$$u_n = a\alpha^n + b\beta^n, \tag{11}$$

where α and β are the roots of $x^2 - r_1 x - r_2$ and

$$a = \frac{u_0\beta - u_1}{\beta - \alpha} \quad \text{and} \quad b = \frac{u_1 - u_0\alpha}{\beta - \alpha},$$

whenever $\alpha \neq \beta$. The binary recurrence sequence $(u_n)_{n=0}^{\infty}$ is non-degenerate whenever $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

In 1967 Schinzel [7] proved that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence then there exist positive numbers $c_7,\ c_8$ and c_9 such that

$$P(u_n) > c_7 n^{c_8} (\log n)^{c_9},$$

where $c_8 = 1/84$ and $c_9 = 7/12$ if α and β are integers while $c_8 = 1/133$ and $c_9 = 7/19$ otherwise and where c_7 is effectively computable in terms of $r,\ s,\ u_0$ and u_1. Let d denote the degree of α over the rationals. In 1982 Stewart [13] proved that if u_n, as in (11), is the n-th term of a non-degenerate binary recurrence sequence then

$$P(u_n) > c_{10} \left(\frac{n}{\log n}\right)^{1/(d+1)} \tag{12}$$

and

$$Q(u_n) > c_{11} \left(\frac{n}{(\log n)^2}\right)^{1/d} \tag{13}$$

where c_{10} and c_{11} are effectively computable in terms of a and b only. In a letter to the author Shorey [10] pointed out that for those indices n which are odd, the argument given in [13] leads to a dependence of c_{10} and c_{11} on α and β in addition to a and b. However, with some additional work we were able to show that the numbers c_{10} and c_{11} do indeed depend on a and b only. In 1995 Yu and Hung [17] improved both (12) and (13). They proved that if u_n is the n-th term of a non-degenerate binary recurrence sequence, as in (11), then

$$P(u_n) > c_{12} n^{1/(d+1)},$$

and

$$Q(u_n) > c_{13}\left(\frac{n}{\log n}\right)^{1/d},$$

where c_{12} and c_{13} are positive numbers which are effectively computable in terms of $a,\ b$ and the class number of the field obtained by adjoining α to $\mathbb{Q}$.

Furthermore, Shorey [9] in 1983 proved that there exist positive numbers c_{14} and c_{15} which are effectively computable in terms of $a,\ b,\ \alpha$ and β such that if u_n is the n-th term of a non-degenerate binary recurrence sequence, as in (11), and n exceeds c_{15} then

$$Q(u_n) > n^{c_{14}(\log n)/\log\log n}. \tag{14}$$

Estimate (14) had been established earlier by Stewart [14] when u_n is the n-th term of a Lucas or Lehmer sequence. A Lucas sequence is a non-degenerate binary recurrence sequence with initial terms $u_0 = 0$ and $u_1 = 1$. For a more extensive history of these topics see [15].

2. Preliminary lemma

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ Let D denote the degree of K over $\mathbb{Q}$. We shall define the height $H(\beta)$ of an algebraic number β by

$$H(\beta) = |a_d| \prod_{i=1}^{d} \max\{1, |\beta_i|\},$$

where

$$a_d X^d + \cdots + a_0 = a_d \prod_{i=1}^{d} (X - \beta_i)$$

is the minimal polynomial of β in $\mathbb{Z}[X]$. Let $\log\alpha_1, \ldots, \log\alpha_n$ be non-zero values of the logarithms of $\alpha_1, \ldots, \alpha_n$ and suppose that

$$A_j \geq \max\{H(\alpha_j), \exp(|\log\alpha_j|), 2\}$$

for $j = 1, \ldots, n$. Let $b_1, \ldots, b_n$ be integers and put

$$B = \max\{|b_1|, \ldots, |b_n|, 2\}.$$

Define Λ by

$$\Lambda = b_1 \log\alpha_1 + \cdots + b_n \log\alpha_n.$$

In 2000 Matveev [4] proved the following result.

Lemma 1. *There exists a positive number C, which is effectively computable, such that if $\Lambda \neq 0$ then*

$$|\Lambda| > \exp(-C^n D^{n+2} \log D \log A_1 \ldots \log A_n \log B).$$

Proof. This follows from Corollary 2.3 of [4]. In fact, Matveev gives an estimate for $|\Lambda|$ in an explicit form from which it would be easy to determine C. □

3. Proof of Theorem 1

We shall follow the proof of Theorem 4 of [13]. By replacing $f(n)$ by $-f(n)$ if necessary, we may assume that α is a positive real number. Let K be the field obtained by adjoining α and the coefficients of f to $\mathbb{Q}$. Let D be the degree of K over $\mathbb{Q}$. Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of δ, α and f. We shall suppose throughout that n exceeds a sufficiently large number c_1.

The proof proceeds by a comparison of estimates for $|\log R|$, where

$$R = \frac{u(n)}{f(n)\alpha^n}.$$

Put $h(n) = u(n) - f(n)\alpha^n$. We have $R = 1 + (h(n)/f(n)\alpha^n)$ and for n sufficiently large

$$|\log R| \leq \frac{2|h(n)|}{|f(n)|\alpha^n},$$

since $|\log(1+x)| \leq 2|x|$ whenever $|x| \leq 1/2$. Thus, from (8),

$$|\log R| \leq \alpha^{-((1-\delta)/2)n}. \tag{15}$$

Suppose that

$$u(n) = (-1)^{a_0} p_1^{a_1} \cdots p_t^{a_t},$$

with $p_1, \ldots, p_t$ distinct prime numbers, $a_1, \ldots, a_t$ positive integers and a_0 from $\{0, 1\}$. Then $\log R = a_0 \log(-1) + a_1 \log p_1 + \cdots + a_t \log p_t - \log f(n) - n \log \alpha$. Note that by (8) $u(n) \neq f(n)\alpha^n$ and so $R \neq 1$. Thus $\log R \neq 0$. Further note that by (8)

$$\max(|a_1|, \ldots, |a_t|) < c_2 n.$$

Furthermore

$$\log H(f(n)) < c_3 \log n.$$

Therefore, by Lemma 1,

$$|\log R| > \exp(-c_4^{t+1} D^{t+2} \log D \log p_1 \cdots \log p_t (\log n)^2). \tag{16}$$

We deduce, from (15) and (16), on taking logarithms, that

$$c_5 \left(\frac{n}{(\log n)^2} \right) < c_6^t \log p_1 \cdots \log p_t. \tag{17}$$

By the arithmetic-geometric mean inequality

$$\prod_{i=1}^{t} \log p_i \leq \left(\frac{\log\left(\prod_{i=1}^{t} p_i\right)}{t} \right)^t. \tag{18}$$

Since $\prod_{i=1}^{t} p_i = Q(u(n))$ it follows from (17) and (18) that

$$\log n - 2\log\log n + \log c_5 < t \log\left(\frac{\log Q(u(n))}{t}\right) + c_7 t,$$

and so, for n sufficiently large,

$$\left(\frac{\log n}{t}\right) - c_8 \frac{\log\log n}{t} < \log\left(\frac{\log Q(u(n))}{t}\right) + c_7$$

hence

$$c_9 t e^{((\log n)/t) - c_8 (\log\log n)/t} < \log Q(u(n)). \tag{19}$$

We assume first that t is less than $(\log n)/\log\log\log n$. Put

$$h(t) = t e^{(\log n - c_8 \log\log n)/t}$$

and notice that h is decreasing for t in the range from 1 to $\log n - c_8 \log\log n$. Thus for n sufficiently large $(\log n)/\log\log\log n$ is less than $\log n - c_8 \log\log n$ and so, by (19),

$$e^{c_{10}(\log n \log\log n)/\log\log\log n} < Q(u(n)), \tag{20}$$

as required. On the other hand if t is at least $(\log n)/\log\log\log n$ then the product of the first t primes exceeds $e^{(\log n \log\log n)/2\log\log\log n}$ for n sufficiently large and therefore

$$e^{(\log n \log\log n)/2\log\log\log n} < Q(u(n)). \tag{21}$$

Thus (10) follows from (20) and (21).

For any positive integer m

$$Q(m) \leq \prod_{p \leq P(m)} p < e^{c_{11} P(m)} \tag{22}$$

and thus (9) follows from (10) and (22). $\square$

References

[1] J.H. Evertse, On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225–244.

[2] D.J. Lewis, Diophantine equations: p-adic methods, *Studies in Number Theory* **6**, ed. W.J. Leveque, Englewood Cliffs, New Jersey, 1969.

[3] K. Mahler, Eine arithmetische Eigenschaft der rekurrierenden Reihen, *Mathematica* (Leiden) **3** (1934–35), 153–156.

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

[5] M. Mignotte, Tagungsbericht Math. Inst., Oberwolfach 1977.

[6] A.J. van der Poorten and H.P. Schlickewei, The growth conditions for recurrence sequences, *Macquarie Math. Reports* 82–0041 (1982).

[7] A. Schinzel, On two theorems of Gelfond and some of their applications, *Acta Arith.* **13** (1967), 177–236.

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

[9] T.N. Shorey, The greatest square free factor of a binary recursive sequence, *Hardy Ramanujan Journal* **6** (1983), 23–36.

[10] T.N. Shorey, personal communication.

[11] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics **87**, Cambridge Univ. Press, Cambridge, 1986.

[12] I.E. Shparlinski, Prime divisors of recurrent sequences, *Isv. Vyssh. Uchebn. Zaved. Math.* **215** (1980), 101–103.

[13] C.L. Stewart, On divisors of terms of linear recurrence sequences, *J. reine angew. Math.* **333** (1982), 12–31.

[14] C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers III, *J. London Math. Soc.* **28** (1983), 211–217.

[15] C.L. Stewart, On the greatest prime factor of terms of a linear recurrence sequence, *Rocky Mountain J. Math.* **15** (1985), 599–608.

[16] M. Waldschmidt, A lower bound for linear forms in logarithms, *Acta Arith.* **37** (1980), 257–283.

[17] Kunrui Yu and Ling-kei Hung, On binary recurrence sequences, *Indag. Mathem., N.S.* **6** (1995), 341–354.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
email: cstewart@uwaterloo.ca