BULL. AUSTRAL. MATH. SOC. 11B37, 11Q25
VOL. 44 (1991) [215-223]

ZEROS OF RECURRENCE SEQUENCES

A.J. VAN DER POORTEN AND H.P. SCHLICKEWEI

We give an upper bound for the number of zeros of recurrence sequences defined over an algebraic number field in terms of their order, the degree of their field of definition and the number of prime ideal divisors of the characteristic roots of the sequence.

1. INTRODUCTION

Let $\mathbf{K}$ be a number field of degree

$$[\mathbf{K}:\mathbb{Q}]=d. \tag{1.1}$$

We consider linear recurrence sequences

$$a_{h+n}=s_1a_{h+n-1}+\cdots+s_na_h \qquad (h=0,1,2,\dots) \tag{1.2}$$

of order n. Here we suppose that the coefficients s_j and the initial values $a_0,\dots,a_{n-1}$ are elements of some subfield $\mathbf{F}\subseteq\mathbf{K}$ and that $s_n\neq 0$, and not all the initial values are zero. Let

$$X^n-s_1X^{n-1}-\cdots-s_n=\prod_{i=1}^{m}(X-\alpha_i)^{n_i} \tag{1.3}$$

be the companion polynomial to the recurrence sequence. We suppose that the roots $\alpha_1,\dots,\alpha_m$ all belong to $\mathbf{K}$; thus $\mathbf{K}$ is an extension of $\mathbf{F}$ of degree at most $n!$ over $\mathbf{F}$. It is well known that the terms a_h are given by generalised power sums

$$a_h=\sum_{i=1}^{m}A_i(h)\alpha_i^h,$$

where for each i the coefficient $A_i(h)$ is a polynomial with coefficients in $\mathbf{K}$ and of degree $\leqslant n_i-1$.

Received 20th September, 1990.
Research of the first author and the visit of the second author to Macquarie University partially supported by the Australian Research Council.

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

We shall study the equations

$$(1.4) \qquad a_h = 0 \qquad (h = 0, 1, 2, \ldots).$$

The number of solutions of (1.4) is called the zero-multiplicity of the recurrence sequence.

If equation (1.4) *has infinitely many solutions* $h \in \mathbb{N}$, *then*, by the Skolem-Mahler-Lech Theorem we know that *those solutions form a finite union of arithmetic progressions after a certain stage.*

We may infer that *if a recurrence relation with companion polynomial* (1.4) *generates a sequence* (a_h) *with infinitely many zeros then there exists a pair* i, j $(1 \leqslant i < j \leqslant m)$ *such that* α_i/α_j *is a root of unity.*

On the other hand, if for each pair i, j $(1 \leqslant i < j \leqslant m)$ the quotient α_i/α_j is not a root of unity, we call the sequence *nondegenerate.*

It has been conjectured that the zero-multiplicity of a nondegenerate recurrence sequence $(a_h)_{h=0}^{\infty}$ is bounded above by a constant $c_1 = c_1(d, n)$ depending only on the degree d of the field of definition and on the order n.

For binary recurrence sequences (that is, for $n = 2$) it is easy to see that the 0-multiplicity of a nondegenerate recurrence sequence is at most 1. There is the additional question, to wit the 0-multiplicity of a recurrence sequence $(a_h - a)$ with a constant — that is, the a-multiplicity of the sequence (a_h). In the binary case Kubota [**3**] shows that when $\mathbf{F} = \mathbb{Q}$ the a-multiplicity is at most 4 and Beukers and Tijdeman [**2**] have given a bound for arbitrary number fields.

Recently, Beukers [**1**] has shown that the 0-multiplicity of a nondegenerate ternary recurrence sequence of rational numbers is at most 6.

In general the conjecture remains open.

It is our present purpose to prove a semi-uniform result for the general case. Accordingly, let $\omega = \omega(\alpha_1, \ldots, \alpha_m)$ denote the number of prime ideals occurring in the decomposition of the fractional ideals (α_i) in $\mathbf{K}$.

We show that

THEOREM 1. *Let* (a_h) *be a nondegenerate recurrence sequence given by* (1.2). *Then there is an effectively computable constant* $c_2 = c_2(d, n, \omega)$ *depending only on* d, n *and* ω *such that the sequence has zero-multiplicity not exceeding* c_2. *We may take*

$$(1.5) \qquad c_2 = \bigl(4(d + \omega)\bigr)^{2(d+1)}(n - 1).$$

Let m be a natural number and for i with $1 \leqslant i \leqslant m$ let n_i be natural numbers satisfying

$$\sum_{i=1}^{m} n_i = n.$$

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

Theorem 1 is an immediate consequence of

THEOREM 2. *Suppose that for each* i $(1 \leqslant i \leqslant m)$ A_i *is a polynomial of degree* $n_i - 1$ *with coefficients in* $\mathbf{K}$. *Suppose moreover that for each pair* i, j $(1 \leqslant i < j \leqslant m)$ *the quotient* α_i/α_j *is not a root of unity. Then the number of solutions* $h \in \mathbb{Z}$ *of the equation*

$$\sum_{i=1}^{m} A_i(h)\alpha_i^h = 0 \tag{1.6}$$

is bounded above by $c_2(d, n, \omega)$, *with* c_2 *as in* (1.5).

A result implying the same parameters has been obtained recently by Schlickewei [9]. However, in [9] the upper bound depends doubly exponentially on $n!$ and $d!$. The method of proof employed in this paper uses only p-adic analysis in contrast to [9], where diophantine approximation (the Subspace Theorem) is the main tool.

The advantage of the current approach as compared to [9], apart from the fact that it gives a better bound, is the rather simple proof. However the method applied in [9] has the strength that it may be generalised to count the number of solutions of multivariable exponential polynomial equations

$$\sum_{i=1}^{m} A_i(h_1, \dots, h_k)\alpha_{i1}^{h_1} \cdots \alpha_{ik}^{h_k} = 0 \tag{1.7}$$

We do not see that the method of the present paper allows one to attack equations (1.7) with $k \geqslant 2$.

Our proof uses Straßmann's Theorem on the number of zeros of p-adic power series in a given disc. This has been applied in our context already by Laxton [4], Mignotte [5], van der Poorten [6] and Robba [7].

2. p-ADIC ANALYSIS

Let p be a rational prime. Denote by $\mathbb{Q}_p$ the p-adic completion of $\mathbb{Q}$ and let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. We denote the valuation of $\mathbb{C}_p$ by $|\ |_p$, normalised so that $|p|_p = p^{-1}$.

Let $\mathfrak{p}$ be a prime ideal in the number field $\mathbf{K}$ which lies above p. Then we may embed the completion $\mathbf{K}_\mathfrak{p}$ of $\mathbf{K}$ with respect to $\mathfrak{p}$ in $\mathbb{C}_p$. We denote by $\mathbf{O}_\mathfrak{p}$ the ring of integers of $\mathbf{K}_\mathfrak{p}$ consisting of those elements $a \in \mathbf{K}_\mathfrak{p}$ having $|a|_p \leqslant 1$. Recall the classic theorem of Straßmann.

LEMMA 1. (Straßmann [10]) *Let*

$$F(t) = \sum_{h=0}^{\infty} b_h t^h \tag{2.1}$$

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

be a nonzero power series in $\mathbb{C}_p$ *with coefficient* b_h *in* $\mathbf{O}_p$. *Assume that* $F(t)$ *converges in the circle* $\{t : |t|_p \leqslant 1\}$ *and suppose that some coefficient* a_h *has* $|a_h|_p = 1$. *Set*

$$k = \max\{n : |a_h|_p = 1\}. \tag{2.2}$$

Then there is a factorisation

$$F(t) = P(t)U(t), \tag{2.3}$$

where $|U(t)|_p = 1$ *for* $|t|_p \leqslant 1$ *and* $P(t)$ *is a polynomial of degree* k. *In particular,* $F(t)$ *has not more than* k *zeros in the circle* $\{t : |t|_p \leqslant 1\}$.

For a proof see, for example, van der Poorten [**6**].

In the sequel it will be convenient to use exponential valuations. Accordingly, given $\alpha \in \mathbb{C}_p$ with $|\alpha|_p = p^{-\nu_p(\alpha)}$ we write $\operatorname{ord}_p(\alpha) = \nu_p(\alpha) = -\log|\alpha|_p$.

LEMMA 2. (van der Poorten [**6**]) *Suppose* $\varepsilon > 0$ *is given. Let* $\phi_1, \dots, \phi_m$ *be distinct elements of* $\mathbf{K}_p$ *having*

$$\operatorname{ord}_p(\phi_i) > \varepsilon + \frac{1}{p-1} \qquad (i = 1, \dots, m). \tag{2.4}$$

Let $B_1(t), \dots, B_m(t)$ *be nonzero polynomials in* $\mathbf{K}_p[t]$ *of degree* $n_1 - 1, \dots, n_m - 1$ *respectively. Set*

$$F(t) = \sum_{i=1}^{m} B_i(t) e^{\phi_i t}$$

and write $n = \sum_{i=1}^{m} n_i$.

Then the number of zeros of $F(t)$ *in the disc* $|t|_p \leqslant 1$ *does not exceed*

$$(n-1)\left(1 + \frac{1}{\varepsilon(p-1)}\right). \tag{2.5}$$

PROOF: For completeness we detail the proof. Denote by D the differential operator $D = d/dt$. Then F satisfies the differential equation

$$D^n F = f_1 D^{n-1} F + f_2 D^{n-2} F + \cdots + f_n D^0 F, \tag{2.6}$$

where the f_i are given by

$$\prod_{i=1}^{m} (X - \phi_i)^{n_i} = X^n - f_1 X^{n-1} - \cdots - f_{n-1} X - f_n. \tag{2.7}$$

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

We expand F as a power series

$$F(t)=\sum_{h=0}^{\infty} b_h t^h=\sum_{h=0}^{\infty}\frac{c_h}{h!}t^h \text{ in } |t|_p\leqslant 1 .$$

The differential equation (2.6) now entails that the c_h satisfy the recurrence relation

$$c_{h+n}=f_1c_{h+n-1}+\cdots+f_nc_h \qquad (h=0,1,\ldots). \tag{2.8}$$

After multiplying F by a constant if necessary we may suppose without loss of generality that

$$\min\{\operatorname{ord}_p b_h : h=0,1,\ldots\}=0 .$$

Set

$$R=\varepsilon+\frac{1}{p-1} .$$

By (2.4), that is $\operatorname{ord}_p(\phi_i)>R$, it follows from (2.7) that

$$\operatorname{ord}_p f_j>jR \qquad (j=1,\ldots,n). \tag{2.9}$$

By the recurrence relation we have

$$\operatorname{ord}_p c_n\geqslant \min_{1\leqslant j\leqslant n}\{\operatorname{ord}_p f_jc_{n-j}\} .$$

Thus using (2.9) we get

$$\operatorname{ord}_p c_n>\min_{1\leqslant j\leqslant n}\{jR+\operatorname{ord}_p c_{n-j}\} . \tag{2.10}$$

On the other hand, since $c_h=h!b_h$ and $\operatorname{ord}_p b_h\geqslant 0$

$$\operatorname{ord}_p c_h\geqslant \operatorname{ord}_p h!=\frac{h-s_p(h)}{p-1}\geqslant 0 ,$$

where $s_p(h)$ denotes the sum of the digits of h expressed in base p. Thus, in particular, (2.10) implies

$$\operatorname{ord}_p c_n>\min_{1\leqslant j\leqslant n}\left\{jR+\frac{n-j-s_p(n-j)}{p-1}\right\}\geqslant R .$$

Again applying the recurrence relation (2.8) for $h=1,2,\ldots$ and using (2.9) we obtain by induction

$$\operatorname{ord}_p c_{h+n-1}>hR \text{ for } h=1,2,\ldots .$$

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

We conclude that for $h = 1, 2, \dots$

$$\begin{aligned}\operatorname{ord}_p b_{h+n-1} &> hR - \operatorname{ord}_p\big((h+n-1)!\big)\\ &= hR - \frac{h+n-1-s_p(h+n-1)}{p-1}\\ &\geqslant hR - \frac{h+n-2}{p-1}\\ &= h\varepsilon - \frac{n-2}{p-1}.\end{aligned}$$

It follows that

$$\operatorname{ord}_p a_{h+n-1} > 0 \text{ once } h > \frac{n-2}{\varepsilon(p-1)}.$$

Thus we can apply Lemma 1 and infer that F has at most

$$n - 1 + \frac{n-2}{\varepsilon(p-1)}$$

zeros in the disc $|t|_p \leqslant 1$, as asserted.

3. Application to exponential polynomials.

We resume the notation of the introduction and now turn to a study of the solutions $h \in \mathbb{Z}$ of the equation (1.6). Accordingly $\mathbf{K}$ is a number field of degree d over $\mathbb{Q}$. We choose a rational prime p so that

(3.1) *none of the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_\omega$ from the decomposition in $\mathbf{K}$ of the ideals (α_i) divides (p).*

Let $e = e_p$ and $f = f_p$ denote respectively the ramification index and the residue class degree of $\mathbf{K}_\mathfrak{p}$ over $\mathbb{Q}_p$.

Our choice of p implies that

$$|\alpha_i|_p = 1 \text{ for each } i \quad (1 \leqslant i \leqslant m).$$

But then

$$|\alpha_i^{p^f-1} - 1|_p \leqslant p^{-1/e} \qquad (i = 1, \dots, m). \tag{3.2}$$

However, we have $e \leqslant d/f$. Therefore, if we choose p with

$$p > d + 1 \tag{3.3}$$

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

then (3.2) yields

$$(3.4) \qquad |\alpha_i^{p^f-1}-1|_p < p^{-1/p(p-1)-1/(p-1)} \qquad (i=1,\dots,m).$$

Given $h \in \mathbb{Z}$ we set

$$h = r + (p^f-1)k$$

where $0 \leqslant r < p^f - 1$. Equation (1.6) splits into p^f-1 equations

$$(3.5) \qquad \sum_{i=1}^{m} A_i\big(r+(p^f-1)k\big)\alpha_i^r\big(\alpha_i^{p^f-1}\big)^k = 0 \quad k \in \mathbb{Z}.$$

Given r with $0 \leqslant r < p^f - 1$ we may define B_i and ϕ_i by

$$B_i(k) = A_i\big(r+(p^f-1)k\big)\alpha_i^r \text{ and } \alpha_i^{p^f-1} = e^{\phi_i}.$$

Then (3.5) may be rewritten as

$$(3.6) \qquad \sum_{i=1}^{m} B_i(k)e^{\phi_i k} = 0 \qquad k \in \mathbb{Z}.$$

We note that since none of the ratios α_i/α_j is a root of unity the ϕ_i are pairwise distinct.

The definition of ϕ_i and (3.4) imply that the left hand side of (3.6) may be continued to a function

$$F(t) = \sum_{i=1}^{m} B_i(t)e^{\phi_i t}$$

analytic in the disc $|t|_p \leqslant 1$.

We are now in a position to apply Lemma 2. By (3.4) the hypotheses of that lemma are satisfied with

$$\varepsilon = \frac{1}{p(p-1)}.$$

Consequently, the function $F(t)$ in (3.7) does not have more than

$$(n-1)(p+1)$$

zeros in the disc $|t|_p \leqslant 1$ and thus, *a fortiori* the equation (3.6) does not have more than $(n-1)(p+1)$ solutions $k \in \mathbb{Z}$.

Since we have p^f-1 residue classes $j \pmod{p^f-1}$ we may conclude that equation (1.6) has not more than

$$(p^f-1)(n-1)(p+1) \leqslant (p^d-1)(n-1)(p+1)$$

solutions $h \in \mathbb{Z}$.

To summarise, we have shown that

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

LEMMA 3. *Let p be a rational prime satisfying conditions* (3.1) *and* (3.3). *Then the number of solutions $h \in \mathbb{Z}$ of equation* (1.6) *does not exceed*

$$(p^d - 1)(p + 1)(n - 1) . \tag{3.7}$$

4. THE CHOICE OF p

To get our semi-uniform bound we still have to choose p in Lemma 3 appropriately. For this purpose we have to study conditions (3.1) and (3.3).

It obviously suffices to find an integer l so that the interval $[d+2, l]$ contains more than ω rational primes. Thus we have to solve the inequality

$$\pi(l) - \pi(d + 1) > \omega . \tag{4.1}$$

Using the estimate (Rosser and Schoenfeld [**8**, Corollary 1])

$$h/\log h \leqslant \pi(h) \text{ for } h \geqslant 17 \tag{4.2}$$

we see that (4.1) will certainly be satisfied for l with $l \geqslant 17$ and

$$(l/\log l) - (d + 1) > \omega$$

that is for $l \geqslant 17$ having

$$l/\log l > d + \omega + 1 . \tag{4.3}$$

If we choose $l = \bigl(4(d + \omega)\bigr)^2$ then (4.3) is true, and indeed with this choice of l we may find a p satisfying (3.1) and (3.4) having $p < l$.

Using this bound for p in (3.3) we obtain at once Theorem 2 and hence also Theorem 1.

REFERENCES

[1] F. Beukers, 'The zero multiplicity of ternary recurrences' (to appear).

[2] F. Beukers and R. Tijdeman, 'On the multiplicities of binary complex recurrences', *Compositio Math.* **51** (1984), 193–213.

[3] K. K. Kubota, 'On a conjecture by Morgan Ward I, II, III', *Acta Arith.* **33** (1977), 11–28, 29–48, 99–109.

[4] R. R. Laxton, 'Linear p-adic recurrences', *Quart. J. Math. Oxford Ser (2)* **19** (1968), 305–311.

[5] M. Mignotte, 'Suites récurrentes linéaires', *Sém. Delange-Pisot-Poitou 15ᵉ année* n° **G14** (1973/74), p. 9.

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press

[6] A. J. van der Poorten, 'Zeros of p-adic exponential polynomials', *Nederl. Akad. Wetensch. Proc. Ser. A* **79**. *Indag. Math.* **38** (1976), 46–49.

[7] P. Robba, 'Zéros de suites récurrentes linéaires", *Groupe d'étude d'analyse ultramétrique 5e année* n° **13** (1977/78), p. 5.

[8] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[9] H. P. Schlickewei, 'Multiplicities of algebraic linear recurrences' (to appear).

[10] R. Straßmann, 'Uber den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen', *J. für Math.* **159** (1928), 13–28.

School of Mathematics, Physics
Computing and Electronics
Macquarie University NSW 2109
Australia

Abteilung Mathematik
Universität Ulm
Oberer Eselsberg
D 7900 Ulm
Germany

https://doi.org/10.1017/S0004972700029646 Published online by Cambridge University Press