On the multiplicity of linear recurrence sequences

Patrick B. Allen

Abstract

We prove a lemma regarding the linear independence of certain vectors and use it to improve on a bound due to Schmidt on the zero-multiplicity of linear recurrence sequences.

1 Linear recurrence sequences

Let $\{u_n\}_{n\in\mathbb{Z}}$ be a linear recurrence sequence of complex numbers satisfying the recurrence relation

$$u_n = c_1 u_{n-1} + \cdots + c_t u_{n-t}, \tag{1}$$

for $c_1, \ldots, c_t \in \mathbb{C}$ with $c_t \neq 0$. We say it is of *order* t if it satisfies (1) but no such relation with fewer than t summands. We define the companion polynomial of our recurrence sequence by

$$\mathcal{P}(z) = z^t - c_1 z^{t-1} - \cdots - c_t.$$

Say our companion polynomial factors over $\mathbb{C}$ as

$$\mathcal{P}(z) = \prod_{i=1}^{k} (z - \alpha_i)^{t_i},$$

with $\alpha_1, \ldots, \alpha_k$ distinct and nonzero. If $\{u_n\}_{n\in\mathbb{Z}}$ is of order t then it is well known that there exists polynomials $P_1, \ldots, P_k$ with $\deg P_i = t_i - 1$, for each $1 \leq i \leq k$, such that

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n, \tag{2}$$

for all integers n. Let $m = \max_{1\leq i\leq k} t_i$ and write

$$P_i(z) = a_{i1} + \cdots + a_{it_i} z^{t_i - 1},$$

for each $1 \leq i \leq k$. We then denote by $\mathbf{a}_i$, $1 \leq i \leq k$, the vector in $\mathbb{C}^m$ given by

$$\mathbf{a}_i = (a_{i1}, \ldots, a_{it_i}, 0, \ldots, 0).$$

Mathematics Subject Classification: 11B37, 11D61

Keywords and Phrases: Linear Recurrence Sequences, Exponential Diophantine Equations

Let $\mathcal{Z}$ denote the set of subscripts $n \in \mathbb{Z}$ such that $u_n = 0$. Note that by (2) $\mathcal{Z}$ is the set of solutions to the equation

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0. \tag{3}$$

By Skolem-Mahler-Lech [2] we know that $\mathcal{Z}$ can be written as the union of finitely many single numbers and arithmetic progressions. If α_i/α_j is not a root of unity for each distinct i and j then we call our recurrence *nondegenerate*. If our recurrence is nondegenerate we have in fact that $\mathcal{Z}$ does not contain any arithmetic progressions. Let $\nu(\mathcal{Z}) = \min\{u + v\}$ such that $\mathcal{Z}$ can be written as the union of u single numbers and v arithmetic progressions. Schlickewei [3] showed that a nondegenerate linear recurrence sequence of order t whose terms are contained in a number field of degree d over $\mathbb{Q}$ satisfies

$$\nu(\mathcal{Z}) \le d^{6t^2} 2^{2^{28t!}}.$$

Schmidt [4] removed the dependence on the degree of the field extension and showed that for any nondegenerate linear recurrence sequence of complex numbers we have

$$\nu(\mathcal{Z}) < \exp\exp\exp(3t\log t).$$

He later [5] improved his result and showed that any linear recurrence sequence of complex numbers satisfies

$$\nu(\mathcal{Z}) < \exp\exp\exp(20t). \tag{4}$$

The purpose of this note is to improve this bound. We prove that

$$\nu(\mathcal{Z}) < \exp\exp(t^{\sqrt{11t}}).$$

To prove (4) Schmidt [5] first showed that for any equation of the form (3) we can find algebraic numbers $\hat{\alpha}_1, \ldots, \hat{\alpha}_k$ and polynomials $\hat{P}_1, \ldots, \hat{P}_k$ with algebraic coefficients and $\deg \hat{P}_i = \deg P_i$ such that if $\mathcal{Z}'$ is the set of solutions to the equation

$$\hat{P}_1(x)\hat{\alpha}_1^x + \cdots + \hat{P}_k(x)\hat{\alpha}_k^x = 0,$$

then

$$\nu(\mathcal{Z}') \ge \nu(\mathcal{Z}).$$

Hence we may assume that $\alpha_1, \ldots, \alpha_k$ and all the coefficients of the $P_1, \ldots, P_k$ belong to some number field K. For $\eta \in K$ and σ an embedding of K into $\mathbb{C}$ we denote by $\eta^{(\sigma)}$ the image of η under σ. If $\mathbf{v} = (v_1, \ldots, v_m) \in K^m$ we set

$$\mathbf{v}^{(\sigma)} = (v_1^{(\sigma)}, \ldots, v_m^{(\sigma)}).$$

We may also assume that $t \ge 3$ since $t = 2$ implies we have either an equation of the form

$$(a_1x + a_0)\alpha^x = 0,$$

which has at most one zero, or we have

$$a_1\alpha_1^x + a_2\alpha_2^x = 0,$$

which can be rewritten as

$$\left(\frac{\alpha_1}{\alpha_2}\right)^x = -\frac{a_2}{a_1}. \tag{5}$$

If α_1/α_2 is not a root of unity then (5) has at most one solution $x \in \mathbb{Z}$. If α_1/α_2 is a root of unity then we see that

$$\mathcal{Z} = \{qy + b : y \in \mathbb{Z}\}$$

where $q = \operatorname{ord}(\alpha_1/\alpha_2)$ and $0 \le b < q$. In either case we have

$$\nu(\mathcal{Z}) = 1.$$

Let $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be as above. For $\sigma_1, \ldots, \sigma_m$ embeddings of K into $\mathbb{C}$ and $i_1, \ldots, i_m \in \{1, \ldots, k\}$ denote by

$$\Delta\begin{pmatrix}\sigma_1, \ldots, \sigma_m \\ i_1, \ldots, \imath_m\end{pmatrix}$$

the determinant of the matrix with columns $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_m}^{(\sigma_m)}$. Also set

$$\mathcal{A}\begin{pmatrix}\sigma_1, \ldots, \sigma_m \\ i_1, \ldots, i_m\end{pmatrix} = \alpha_{i_1}^{(\sigma_1)} \cdots \alpha_{i_m}^{(\sigma_m)}.$$

The bound (4) was obtained by showing that

$$\nu(\mathcal{Z}) < \exp(2^t (7T)^{7T}), \tag{6}$$

where T is an upper bound on the number of nonzero summands of

$$\sum_{i_1=1}^{k} \cdots \sum_{i_m=1}^{k} \Delta\begin{pmatrix}\sigma_1, \ldots, \sigma_m \\ i_1, \ldots, i_m\end{pmatrix} \mathcal{A}\begin{pmatrix}\sigma_1, \ldots, \sigma_m \\ i_1, \ldots, i_m\end{pmatrix}.$$

Schmidt then showed that one may estimate T by means of a lemma dealing with the linear independence of certain vectors. Using Lemma 2 of [5] Schmidt deduced that we may take

$$T = \mathrm{e}^{12t}.$$

We are able to improve on Lemma 2. In fact by the Lemma in §2 of this paper we can take

$$T = t^{\sqrt{2t}}.$$

Then, since we may assume $t \ge 3$, (6) yields

$$\begin{aligned}\nu(\mathcal{Z}) &< \exp\exp(7t^{\sqrt{2t}}(\sqrt{2t}\log t + \log 7) + t\log 2) \\ &< \exp\exp(t^{\sqrt{11t}}).\end{aligned}$$

For a more complete treatment see [1].

2 A lemma on linear independence

The following lemma improves on Lemma 2 of [5] by replacing the bound e^{12t} with $t^{\sqrt{2t}}$. If K is a subfield of $\mathbb{C}$ and σ is an embedding $K \hookrightarrow \mathbb{C}$ we denote by $\eta^{(\sigma)}$ the image of $\eta \in K$ under σ. If $\mathbf{v} = (v_1, \ldots, v_m) \in K^m$ we set

$$\mathbf{v}^{(\sigma)} = (v_1^{(\sigma)}, \ldots, v_m^{(\sigma)}).$$

Lemma. *Let m be a positive integer, K a subfield of $\mathbb{C}$ and $\mathbf{a}_1, \ldots, \mathbf{a}_k$ vectors in K^m. Fix m, not necessarily distinct, embeddings $\sigma_1, \ldots, \sigma_m$ of K into $\mathbb{C}$. For $1 \leq i \leq k$ write*

$$\mathbf{a}_i = (a_{i1}, \ldots, a_{it_i}, 0, \ldots, 0)\,,$$

where either $t_i = 0$, hence $\mathbf{a}_i = \mathbf{0}$, or $t_i > 0$ and $a_{t_i} \neq 0$. Set $t = t_1 + \ldots + t_k$. Then there are at most $t^{\sqrt{2t}}$ ordered m-tuples $(i_1, \ldots, i_m)$, with $i_1, \ldots, i_m \in \{1, \ldots, k\}$, such that $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_m}^{(\sigma_m)}$ are linearly independent.

Proof. Note first that the result is trivial if $k < m$ so we may assume $k \geq m$. Also note that the embedding σ_i, for any $1 \leq i \leq n$, will not have any effect on the numbers $t_1, \ldots, t_k$. If $\mathbf{a}_i = \mathbf{0}$ then $\mathbf{a}_i$ doesn't contribute at all to the number of m-tuples that we are counting and t_i doesn't contribute to t. Hence we may assume $\mathbf{a}_i \neq \mathbf{0}$ for each $1 \leq i \leq k$. In particular we may assume $t \geq k$. Suppose $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_m}^{(\sigma_m)}$ are linearly independent. Then there can be at most one $\mathbf{a}_i$ with $t_i = 1$. If there exists $\mathbf{a}_i$ such that $t_i = 1$ then there is at most one $\mathbf{a}_i$ such that $t_i = 2$ and so on. Hence if there exist any m-tuples $(i_1, \ldots, i_m)$ such that $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_m}^{(\sigma_m)}$ are linearly independent then we must have

$$t \geq 1 + 2 + \cdots + m = \frac{m(m+1)}{2},$$

hence $m < \sqrt{2t}$. Clearly there are at most k^m such m-tuples and we have

$$k^m < t^{\sqrt{2t}}.$$

□

With the exception of the constant $\sqrt{2}$ the above result is best possible. Say $k = m$, $\sigma_1 = \cdots = \sigma_m$ and we have m linearly independent vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m$. Then the number of such m-tuples is $m!$. By Stirling's Approximation for every positive number ε there is a positive integer $m_0(\varepsilon)$ such that for $m > m_0(\varepsilon)$,

$$m! > \mathrm{e}^{(1-\varepsilon)m\log m},$$

and so, since $t \leq km = m^2$,

$$m! > t^{\frac{1}{2}(1-\varepsilon)\sqrt{t}}.$$

Acknowledgements

The results of this paper form part of my M.Math. thesis which was written at the University of Waterloo under the supervision of C. L. Stewart.

References

[1] ALLEN, P. B., Multiplicities of linear recurrence sequences, M.Math. Thesis, University of Waterloo, Waterloo, Canada.

[2] LECH, C., A note on recurring series, *Ark. Math.* **2** (1953), 417-421.

[3] SCHLICKEWEI, H. P., Multiplicities of rcurrence sequences, *Acta. Math.* **176** (1996), 171-243.

[4] SCHMIDT, W. M., The zero multiplicity of linear recurrence sequences, *Acta Math.* **182** (1999), 243-282.

[5] SCHMIDT, W. M., Zeros of linear recurrence sequences, *Publ. Math. Debrecen* **56** (2000), 609-630.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT LOS ANGELES, BOX 951555, LOS ANGELES, CA, 90095-1555
E-mail address: pballen@math.ucla.edu