Publ. Math. Debrecen
56 / 3-4 (2000), 609–630

Zeros of linear recurrence sequences

By WOLFGANG M. SCHMIDT (Boulder)

Dedicated to Kálmán Győry on his 60th birthday

Abstract. Let $\{u_n\}_{n\in\mathbb{Z}}$ be a linear recurrence sequence. A classical theorem of Skolem–Mahler–Lech asserts that the set $\mathcal{Z}$ of subscripts n with $u_n = 0$ is a finite union of arithmetic progressions and single numbers. We now show that when the sequence is of order t, then $\mathcal{Z}$ is a union of at most $c(t)$ progressions and single numbers.

1. Introduction

The sequences $\{u_n\}_{n\in\mathbb{Z}}$ of complex numbers form a vector space V under component-wise addition. A polynomial

$$\mathcal{P}(z) = c_0 z^t + \cdots + c_t \tag{1.1}$$

acts on V by setting $\mathcal{P}(\{u_n\}) = \{v_n\}$ with $v_n = c_0 u_n + c_1 u_{n-1} + \cdots + c_t u_{n-t}$ $(n \in \mathbb{Z})$.

When $\mathcal{P}(z)$ is a polynomial of degree t with constant term $c_t \neq 0$, the sequences $\{u_n\}$ with $\mathcal{P}(\{u_n\}) = \{0\}$ (the zero sequence) make up a subspace $V(\mathcal{P})$ of $\mathcal{P}$ of dimension t. If

$$\mathcal{P}(z) = c_0 \prod_{i=1}^{k} (z - \alpha_i)^{t_i} \tag{1.2}$$

Mathematics Subject Classification: 11B37, 11D61.
Key words and phrases: linear recurrence sequences, exponential diophantine equations.
Supported in part by NSF grant DMS–9710314.

with distinct roots $\alpha_1, \dots, \alpha_k$, the space $V(\mathcal{P})$ is spanned by the sequences

$$\{n^j \alpha_i^n\}_{n \in \mathbb{Z}}$$

where $1 \leqq i \leqq k$, $0 \leqq j < t_i$, so that it consists of the sequences

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n \tag{1.3}$$

where P_i is a polynomial of degree $< t_i$ $(i = 1, \dots, k)$.

On the other hand, given a sequence $\{u_n\}$, the polynomials $\mathcal{P}$ with $\mathcal{P}(\{u_n\}) = \{0\}$ make up an ideal in $\mathbb{C}[z]$. A polynomial $\mathcal{P}(z)$ is in the ideal precisely when $z\mathcal{P}(z)$ is. When the ideal is not the zero ideal, it is generated by a unique monic polynomial $\mathcal{P}$, and this polynomial has nonzero constant term c_t. In this case we say that $\{u_n\}$ is a *linear recurrence sequence*, and the polynomial $\mathcal{P}$ is its *companion polynomial*. The *order* of the recurrence sequence is the degree of its companion polynomial. A sequence is of order t precisely if (1.3) holds with distinct nonzero $\alpha_1, \dots, \alpha_k$ and $\sum_{i=1}^k (\deg P_i + 1) = t$. Only the zero sequence has order $t = 0$. A sequence $\{u_n\}$ of order $t > 0$ with companion polynomial (1.1) satisfies the recurrence relation

$$u_n = -c_1 u_{n-1} - \cdots - c_t u_{n-t} \qquad (n \in \mathbb{Z}).$$

The sequence is said to be *nondegenerate* if the quotients α_i/α_j $(i \neq j)$ of the roots of its companion polynomial are not roots of 1.

Let $\{u_n\}$ be a linear recurrence sequence with companion polynomial (1.1) of degree $t > 0$. We are interested in the set $\mathcal{Z} = \mathcal{Z}(\{u_n\})$ of numbers $n \in \mathbb{Z}$ with $u_n = 0$, i.e., with

$$P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n = 0. \tag{1.4}$$

The Skolem–Mahler–Lech Theorem [3] says that $\mathcal{Z}$ is a finite union of arithmetic progressions and of single numbers. Moreover, $\mathcal{Z}$ is finite if the sequence is non-degenerate. Actually, $\mathcal{Z}$ is finite under the weaker hypothesis that for some i_0, no quotient α_{i_0}/α_j with $j \neq i_0$ is a root of 1.

We recently showed [4] that in the nondegenerate case of order $t > 0$, the set $\mathcal{Z}$ has cardinality $|\mathcal{Z}| \leqq c_1(t)$ where $c_1(t)$ depends on t only. In the present paper we will prove the following.

Theorem. *Suppose $\{u_n\}$ is a recurrence of order t. Then $\mathcal{Z}$ is a union of not more than $c_2(t)$ arithmetic progressions and single numbers, where we may take*

$$c_2(t) = \exp\exp\exp(20t). \tag{1.5}$$

If the companion polynomial (1.2) *has $\max_i t_i = a$, then $\mathcal{Z}$ also is the union of at most $c_3(k,a)$ numbers and progressions, where*

$$c_3(k,a) = \exp\exp(30ak^a \log k).$$

Note that in the nondegenerate case, we have replaced the bound $c_1(t) = \exp\exp\exp(3t\log t)$ of [4] by (1.5). When the companion polynomial has only simple roots, so that $a = 1$, we have $c_3(k,1) = \exp\exp(30k\log k) = \exp\exp(30t\log t)$, i.e., a bound which is only double exponential.

We do not claim that the union involves arithmetic progressions which all have the same common difference a, i.e., progressions $n = ax + b_i$, or that our progressions do not intersect. Suppose ζ, ξ are primitive roots of 1 of respective orders r, s where r, s are coprime, and let

$$u_n = 1^n - \zeta^n - \xi^n + (\zeta\xi)^n = (1-\zeta^n)(1-\xi^n) \quad (n \in \mathbb{Z}).$$

This is a sequence of order 4, and $\mathcal{Z}$ is the union of the two progressions rx $(x \in \mathbb{Z})$, and sx $(x \in \mathbb{Z})$. It is an easy exercise to show that given $a > 0$, at least $r + s - 1$ progressions $n = ax + b_i$ $(x \in \mathbb{Z})$ are needed such that their union equals $\mathcal{Z}$.

It will be convenient to introduce the following equivalence relation on $\mathbb{C}^\times$: we set $\alpha \approx \beta$ if α/β is a root of 1. Given

$$f(n) = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n$$

we group together summands $P_i(n)\alpha_i^n$ and $P_j(n)\alpha_j^n$ with $\alpha_i \approx \alpha_j$. After relabeling, we may write (uniquely up to ordering)

$$f(n) = f_1(n) + \cdots + f_g(n)$$

where

$$f_i(n) = P_{i1}(n)\alpha_{i1}^n + \cdots + P_{i,q_i}(n)\alpha_{i,q_i}^n \quad (i = 1,\ldots,g)$$

with $q_1 + \cdots + q_g = k$ and $\alpha_{ij} \approx \alpha_{i\ell}$ when $1 \leqq i \leqq g$, $1 \leqq j$, $\ell \leqq q_i$, but $\alpha_{ij} \not\approx \alpha_{i'\ell}$ when $1 \leqq i \neq i' \leqq g$, $1 \leqq j \leqq q_i$, $1 \leqq \ell \leqq q_{i'}$.

We will now show that if $f(n) = 0$ for every n in an arithmetic progression $\mathcal{A} : n = ax + b$ $(x \in \mathbb{Z})$, then

$$f_1(n) = \cdots = f_g(n) = 0 \tag{1.6}$$

for every $n \in \mathcal{A}$. Pick $m \in \mathbb{N}$ such that $(\alpha_{ij}/\alpha_{i\ell})^m = 1$ for $1 \leqq i \leqq g$, $1 \leqq j$, $\ell \leqq q_i$. The progression $\mathcal{A}$ is a finite union of progressions $\mathcal{A}' : n = amx + b'$ $(x \in \mathbb{Z})$, so that it will suffice to prove our assertion for each progression $\mathcal{A}'$. When $n = amx + b'$ in $\mathcal{A}'$, we have $\alpha_{ij}^n = \alpha_{ij}^{b'} \alpha_{i1}^{amx}$, so that

$$f_i(n) = Q_i(x) \alpha_{i1}^{amx}$$

with $Q_i(x) = \sum_{j=1}^{q_i} \alpha_{ij}^{b'} P_{ij}(amx + b')$. We may infer that

$$Q_1(x)\alpha_{11}^{amx} + \cdots + Q_g(x)\alpha_{g1}^{amx} \tag{1.7}$$

vanishes for each $x \in \mathbb{Z}$. Since $\alpha_{i1} \not\approx \alpha_{i'1}$, for $i \neq i'$, we have $\alpha_{i1}^{am} \not\approx \alpha_{i'1}^{am}$, so that $\{x^\ell \alpha_{i1}^{amx}\}_{x \in \mathbb{Z}}$ for $1 \leqq i \leqq g$, $\ell = 0, 1, \ldots$ are linearly independent recurrence sequences. Therefore (1.7) can vanish for each $x \in \mathbb{Z}$ only if $Q_1 = \cdots = Q_g = 0$. But then (1.6) holds indeed for every $n \in \mathcal{A}'$.

In view of the observation just made, our Theorem yields the following result, akin to Lemma 8 of [4].

Corollary. (1.6) *holds for all but at most* $c_2(t)$ *number* $n \in \mathcal{Z}$.

If for some i_0 we have $\alpha_{i_0} \not\approx \alpha_j$ for each $j \neq i_0$, $1 \leqq j \leqq k$, then some f_i equals $P_{i_0}(n)\alpha_{i_0}^n$, hence has at most t zeros. In this case $\mathcal{Z}$ contains no arithmetic progression, hence has cardinality $\leqq c_2(t)$.

The present paper is a sequel to [4], and the proof of the theorem will depend heavily on the machinery introduced in that earlier paper. We will frequently use without mention the fact that when x runs through an arithmetic progression, then so does $ax + b$ when $a > 0$, b in $\mathbb{Z}$ are given. As for notation, $h(\alpha)$ will denote the absolute logarithmic height of a nonzero algebraic number α, and ord β will denote the order of a root of unity β.

2. A specialization argument

By *arithmetic progression* we will, of course, understand a set $\mathcal{A} = \mathcal{A}(a,b) \subset \mathbb{Z}$ where $a > 0$, b are in $\mathbb{Z}$, consisting of numbers $ax+b$ with $x \in \mathbb{Z}$. We will call $a = a(\mathcal{A})$ the *modulus* of $\mathcal{A}$. Suppose a set $\mathcal{Z} \subset \mathbb{Z}$ is a finite union of numbers and of arithmetic progressions. We then write $\nu(\mathcal{Z})$ for the minimum of $u+v$ such that $\mathcal{Z}$ can be expressed as the union of u numbers and v arithmetic progressions. For example, when $\mathcal{Z}$ is finite, $\nu(\mathcal{Z})$ is its cardinality $|\mathcal{Z}|$; on the other hand $\mathcal{Z} = \mathcal{A}(2,0) \cup \mathcal{A}(3,0)$ has $\nu(\mathcal{Z}) = 2$. We write $\nu(\mathcal{Z}) = \infty$ if $\mathcal{Z}$ cannot be expressed as such a union.

In general, $\mathcal{Z}' \supset \mathcal{Z}$ does not imply $\nu(\mathcal{Z}') \geqq \nu(\mathcal{Z})$. We therefore will require the following

Lemma 1. *Suppose $\nu(\mathcal{Z})$ is finite. Then there is a finite set $\mathcal{T} \subset \mathbb{Z}$ with $\mathcal{Z} \cap \mathcal{T} = \emptyset$ such that every set $\mathcal{Z}' \supset \mathcal{Z}$ with $\mathcal{Z}' \cap \mathcal{T} = \emptyset$ has $\nu(\mathcal{Z}') \geqq \nu(\mathcal{Z})$.*

Proof. Suppose $\nu(\mathcal{Z}) = u+v$, and $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$ where $|\mathcal{Z}_1| = u$ and $\mathcal{Z}_2$ is a union of v arithmetic progressions. Clearly $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$ and $\nu(\mathcal{Z}_2) = v$.

Say $\mathcal{Z}_1 = \{n_1, \dots, n_u\}$. When $u = 0$ or 1, set $\mathcal{T}_1 = \emptyset$. When $u > 1$ and $n_i < n_j$, we note that $\mathcal{A}(n_j - n_i, n_i)$ is not contained in $\mathcal{Z}$, for if it were, it clearly would be contained in $\mathcal{Z}_2$, so that $n_i, n_j \in \mathcal{Z}_2$, and we could remove n_i, n_j from $\mathcal{Z}_1$, thus diminishing $u+v$. We may then pick some $t_{ij} \in \mathcal{A}(n_j - n_i, n_i)$ which is not in $\mathcal{Z}$. We now let $\mathcal{T}_1$ be the union of the numbers t_{ij} so obtained. Then

Any arithmetic progression $\mathcal{A}$ with $\mathcal{A} \cap \mathcal{T}_1 = \emptyset$ contains at most one element of $\mathcal{Z}_1$.

Therefore when $v = 0$, the lemma holds with $\mathcal{T} = \mathcal{T}_1$.

Now suppose $v > 0$, and let $\mathcal{Z}_2$ be the union of arithmetic progressions $\mathcal{A}(a_i, b_i)$ $(i = 1, \dots, v)$. Set $q = \operatorname{lcm}(a_1, \dots, a_v)$; then $\mathcal{Z}_2$ is *periodic* with period q, i.e., when $n \in \mathcal{Z}_2$, then $\mathcal{A}(q,n) \subset \mathcal{Z}_2$. Set $\ell = q\nu(\mathcal{Z})$. After a translation, we may suppose that

$$[1, q\ell] \cap \mathcal{Z}_1 = \emptyset.$$

Let $\mathcal{T}_2$ consist of all numbers $n \in [1, q\ell]$ which are not in $\mathcal{Z}$. Suppose $\mathcal{A}$ is an arithmetic progression with modulus $a \leqq \ell$ which is not contained in $\mathcal{Z}_2$. Let $b, b+a, \dots, b+(q-1)a$ with $1 \leqq b \leqq a$ be consecutive elements of $\mathcal{A}$. If all were in $\mathcal{Z}_2$, then by periodicity of $\mathcal{Z}_2$, all of $\mathcal{A}$ would be in $\mathcal{Z}_2$. Therefore at least one of the above q elements of $\mathcal{A}$ is $\notin \mathcal{Z}_2$, hence is in $\mathcal{T}_2$. Therefore

Every arithmetic progression $\mathcal{A}$ with $\mathcal{A} \cap \mathcal{T}_2 = \emptyset$ and modulus $a(\mathcal{A}) \leqq \ell$ is contained in $\mathcal{Z}_2$.

Set $\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2$. Suppose $\mathcal{Z}' \supset \mathcal{Z}$ with $\mathcal{Z}' \cap \mathcal{T} = \emptyset$ is the union of u' numbers and v' arithmetic progressions; say $\mathcal{Z}' = \mathcal{Z}_1' \cup \mathcal{Z}_2'$ where $|\mathcal{Z}_1'| = u'$ and $\mathcal{Z}_2'$ is the union of v' arithmetic progressions $\mathcal{A}_i' = \mathcal{A}_i(a_i', b_i')$ $(i = 1, \ldots, v')$. We have to show that

$$u' + v' \geqq u + v = \nu(\mathcal{Z}). \tag{2.1}$$

If some $\mathcal{A}_i'$ is disjoint from $\mathcal{Z}_2$, its intersection with $\mathcal{Z}$ is empty or consists of a single element of $\mathcal{Z}_1$. Remove $\mathcal{A}_i'$ from $\mathcal{Z}'$, or replace it by this single element of $\mathcal{Z}_1$. In this way $\mathcal{Z}'$ is replaced by a set $\mathcal{Z}'' \supset \mathcal{Z}$ with $\mathcal{Z}'' \cap \mathcal{T} = \emptyset$, and $\mathcal{Z}''$ can be covered by at most $u' + 1$ numbers and $v' - 1$ progressions. If we can show that $(u'+1)+(v'-1) \geqq u+v$, then (2.1) will follow. After some replacements of this kind we may suppose that each $\mathcal{A}_i'$ $(i = 1, \ldots, v')$ intersects $\mathcal{Z}_2$.

We may suppose that $\mathcal{A}_1', \ldots, \mathcal{A}_w'$ have modulus $\leqq \ell$ and $\mathcal{A}_{w+1}', \ldots, \mathcal{A}_{v'}'$ have modulus $> \ell$, where $0 \leqq w \leqq v'$. Then $\mathcal{A}_1', \ldots, \mathcal{A}_w'$ are contained in $\mathcal{Z}_2$. Given $\mathcal{A}_i' = \mathcal{A}(a_i', b_i')$ where $1 \leqq i \leqq w$, each $b_i' + xa_i' \in \mathcal{Z}_2$, and since $\mathcal{Z}_2$ has period q, each $b_i' + xa_i' + yq$ with $x, y \in \mathbb{Z}$ is in $\mathcal{Z}_2$. Therefore, setting $a_i'' = \gcd(a_i', q)$, the progression $\mathcal{A}(a_i'', b_i') \subset \mathcal{Z}_2$. Since clearly $\mathcal{A}_1' \cup \cdots \cup \mathcal{A}_{v'}'$ covers $\mathcal{Z}_2$, this union remains unchanged if we replace $\mathcal{A}_i'$ by $\mathcal{A}(a_i'', b_i')$ for $1 \leqq i \leqq w$. Therefore we may suppose that $a_i' \mid q$ $(i = 1, \ldots, w)$, so that $\mathcal{A}_1', \ldots, \mathcal{A}_w'$ have period q.

We claim that $\mathcal{A}_1' \cup \cdots \cup \mathcal{A}_w' = \mathcal{Z}_2$. Say $\mathcal{Z}_2$ has r elements per period of length q, and $\mathcal{A}_1' \cup \cdots \cup \mathcal{A}_w'$ has s elements. Thus $\mathcal{Z}_2$ has "density" r/q, and $\mathcal{A}_1' \cup \cdots \cup \mathcal{A}_w'$ has density s/q. The sequences $\mathcal{A}_{w+1}', \ldots, \mathcal{A}_{v'}'$ have density $< 1/\ell$, so that $\mathcal{Z}_2' = \mathcal{A}_1' \cup \cdots \cup \mathcal{A}_{v'}'$ has density $< (s/q) + (v'/\ell)$. In proving (2.1) we may clearly suppose that $v' \leqq \nu(\mathcal{Z})$, and then $\mathcal{Z}_2'$, hence $\mathcal{Z}'$, has density

$$< (s/q) + (\nu(\mathcal{Z})/q\nu(\mathcal{Z})) = (s+1)/q.$$

Therefore, since $\mathcal{Z}' \supset \mathcal{Z}$ and $\mathcal{Z}$ has density r/q, we see that $s = r$, and our claim is established.

We may conclude that $w \geqq \nu(\mathcal{Z}_2) = v$. The sequences $\mathcal{A}'_{w+1}, \ldots, \mathcal{A}'_{v'}$, together with $\mathcal{Z}'_1$, must cover $\mathcal{Z}_1$. Since each $\mathcal{A}'_i$ contains at most one element of $\mathcal{Z}_1$, we have $(v' - w) + |\mathcal{Z}'_1| \geqq |\mathcal{Z}_1|$, i.e., $v' - w + u' \geqq u$. We may conclude that $u' + v' \geqq u + w \geqq u + v$. $\square$

Consider an equation (1.4) where $P_1, \ldots, P_k$ are of respective degrees $s_1, \ldots, s_k$. The numbers $\alpha_1, \ldots, \alpha_k$ and the coefficients of $P_1, \ldots, P_k$ are not necessarily algebraic. Denote the coefficients of P_j by $c_{j0}, c_{j1}, \ldots, c_{j,s_j}$. By the Skolem–Mahler–Lech Theorem, the solutions $n \in \mathbb{Z}$ of (1.4) make up a set $\mathcal{Z}$ with finite $\nu(\mathcal{Z})$. Construct $\mathcal{T}$ according to Lemma 2.1.

Given $n \in \mathbb{Z}$, the equation (1.4) defines an algebraic variety $V(n)$ in the points $(\boldsymbol{\alpha}, \mathbf{c})$ where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and $\mathbf{c}$ has components $c_{j\ell}$ $(1 \leqq j \leqq k,\ 0 \leqq \ell \leqq s_j)$. Our particular $(\boldsymbol{\alpha}, \mathbf{c})$ lies in the variety

$$V(\mathcal{Z}) = \bigcap_{n \in \mathcal{Z}} V(n).$$

Since $\mathcal{Z} \cap \mathcal{T} = \emptyset$, $(\boldsymbol{\alpha}, \mathbf{c}) \notin W(\mathcal{T})$, where

$$W(\mathcal{T}) = \bigcup_{n \in \mathcal{T}} V(n).$$

In fact $(\boldsymbol{\alpha}, \mathbf{c}) \in V(\mathcal{Z}) \backslash W_0(\mathcal{T})$, where $W_0(\mathcal{T})$ is the union of $W(\mathcal{T})$ and the surface $\alpha_1 \ldots \alpha_k c_{1,s_1} \ldots c_{k,s_k} = 0$.

There is an algebraic specialization $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \in V(\mathcal{Z}) \backslash W_0(\mathcal{T})$, i.e., a point $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}})$ with algebraic coordinates in this set. It gives rise to an equation

$$\widehat{P}_1(n)\hat{\alpha}_1^n + \cdots + \widehat{P}_k(n)\hat{\alpha}_k^n = 0 \tag{2.2}$$

where $\hat{\alpha}_i \neq 0$ and $\deg \widehat{P}_i = s_i$ $(1 \leqq i \leqq k)$. Let $\widehat{\mathcal{Z}}$ consist of solutions $n \in \mathbb{Z}$ of this equation. Since $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \in V(\mathcal{Z})$, we have $\widehat{\mathcal{Z}} \supset \mathcal{Z}$, but since $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \notin W(\mathcal{T})$, no $n \in \mathcal{T}$ is a solution. Therefore $\widehat{\mathcal{Z}} \cap \mathcal{T} = \emptyset$, so that $\nu(\widehat{\mathcal{Z}}) \geqq \nu(\mathcal{Z})$ by the lemma.

Therefore it will suffice to prove our theorem in the situation where $\alpha_1, \ldots, \alpha_k$ and the coefficients of $P_1, \ldots, P_k$ are algebraic. *We will assume from now on that $\alpha_1, \ldots, \alpha_k$ and these coefficients lie in an algebraic number field K.*

3. A Proposition which implies the Theorem

Proposition. *Let* $M_j(\mathbf{X}) = a_{1j}X_1 + \cdots + a_{kj}X_k$ $(j = 1, \ldots, n)$ *be linear forms which are linearly independent over* $\mathbb{Q}$*. We suppose that the coefficients* a_{ij} *are algebraic, we write* $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$ *and assume that each* $\mathbf{a}_i \neq \mathbf{0}$ $(i = 1, \ldots, k)$*. We define* t_i *to be the integer such that* $\mathbf{a}_i = (a_{i1}, \ldots, a_{i,t_i}, 0, \ldots, 0)$ *with* $a_{i,t_i} \neq 0$*. Set* $t = t_1 + \cdots + t_k$*,*

$$T = \min(k^n, e^{12t}), \tag{3.1}$$

$$\hbar = \hbar(T) = e^{-6T^4}. \tag{3.2}$$

Suppose $\alpha_1, \ldots, \alpha_k$ *are nonzero algebraic numbers. Consider numbers* $x \in \mathbb{Z}$ *for which*

$$M_1(\alpha_1^x, \ldots, \alpha_k^x), \ \ldots, \ M_n(\alpha_1^x, \ldots, \alpha_k^x) \tag{3.3}$$

are linearly dependent over $\mathbb{Q}$*. These numbers fall into at most*

$$H(T) = \exp\left((7T)^{6T}\right) \tag{3.4}$$

classes with the following property. For each class C *there is a natural number* m *such that*

(a) *solutions* x, x' *in* C *have* $x \equiv x' \pmod{m}$*,*

(b) *there are* $i \neq j$ *such that either* $\alpha_i \not\approx \alpha_j$ *and* $h(\alpha_i^m/\alpha_j^m) \geqq \hbar$*, or* $\alpha_i \approx \alpha_j$ *and* $\mathrm{ord}(\alpha_i^m/\alpha_j^m) \leqq \hbar^{-1}$.

Deduction of the Theorem. When P is a nonzero polynomial, set $t(P) = 1 + \deg P$, and when $P = 0$ set $t(P) = 0$. When $\mathbf{P} = (P_1, \ldots, P_k)$ is a vector of polynomials, put $t = t(\mathbf{P}) = t(P_1) + \cdots + t(P_k)$. Also set $a = a(\mathbf{P}) = \max_i t(P_i)$. Suppose $P_1, \ldots, P_k$ have algebraic coefficients, and $\alpha_1, \ldots, \alpha_k$ are nonzero algebraic numbers. We will prove by induction on t that the set $\mathcal{Z}$ of solutions $x \in \mathbb{Z}$ of

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0 \tag{3.5}$$

has

$$\nu(\mathcal{Z}) \leqq Z(t, T) = \exp\left((2^t - 1)(7T)^{7T}\right), \tag{3.6}$$

where

$$T = \min(k^a, e^{12t}). \tag{3.7}$$

We clearly may suppose that $k \geqq 2$, $t \geqq 3$, and that $P_1, \dots, P_k$ are not zero. Set $t_i = t(P_i)$ $(i = 1, \dots, k)$. When $P_i(x) = \sum_{j=1}^{a} a_{ij} x^{j-1}$ $(i = 1, \dots, k)$, define linear forms

$$N_j(\mathbf{X}) = N_j(X_1, \dots, X_k) = \sum_{i=1}^{k} a_{ij} X_i \quad (j = 1, \dots, a).$$

Then $\mathbf{a}_i = (a_{i1}, \dots, a_{ia}) = (a_{i1}, \dots, a_{i,t_i}, 0, \dots, 0)$ with $a_{i,t_i} \neq 0$ $(i = 1, \dots, a)$. The forms $N_1, \dots, N_a$ are not necessarily linearly independent over $\mathbb{Q}$. Let $M_1, \dots, M_n$ be a maximal independent (over $\mathbb{Q}$) subset of them. If we replace $N_1, \dots, N_a$ by $M_1, \dots, M_n$, then the numbers t_i $(i = 1, \dots, k)$ and $t = t_1 + \dots + t_k$ induced by them cannot increase.

The equation (3.5) may be written as

$$\sum_{j=1}^{a} N_j(\alpha_1^x, \dots, \alpha_k^x) x^{j-1} = 0. \tag{3.8}$$

Each $N_j(\mathbf{X})$ is a linear combination $\sum_{r=1}^{n} c_{jr} M_r(\mathbf{X})$ with rational c_{jr}, so that (3.8) may be expressed as

$$\sum_{r=1}^{n} \left(\sum_{j=1}^{a} c_{jr} x^{j-1} \right) M_r(\alpha_1^x, \dots, \alpha_k^x) = 0. \tag{3.9}$$

There are fewer than a numbers $x \in \mathbb{Z}$ such that each polynomial $\sum_{j=1}^{a} c_{jr} x^{j-1}$ $(r = 1, \dots, n)$ vanishes. For other solutions of (3.9), the numbers $M_r(\alpha_1^x, \dots, \alpha_k^x)$ $(r = 1, \dots, n)$ are linearly dependent over $\mathbb{Q}$. By the Proposition, these numbers fall into at most $H(T)$ classes. Let us consider solutions in a fixed class.

The numbers in such a class are of the form $x = x_0 + my$ with $y \in \mathbb{Z}$. In terms of y, the equation (3.5) becomes

$$\widehat{P}_1(y)\hat{\alpha}_1^y + \dots + \widehat{P}_k(y)\hat{\alpha}_k^y = 0 \tag{3.10}$$

where $\hat{\alpha}_i = \alpha_i^m$, $\widehat{P}_i(y) = \alpha_i^{x_0} P_i(x_0 + my)$ $(i = 1, \dots, k)$.

The Proposition leads to two cases. Let us first consider the case where $i \neq j$, $\alpha_i \approx \alpha_j$ and $\mathrm{ord}(\hat{\alpha}_i/\hat{\alpha}_j) = \mathrm{ord}(\alpha_i^m/\alpha_j^m) \leqq \hbar(T)^{-1}$. We may suppose that $i = k$, $j = k-1$, say, and we set $q = \mathrm{ord}(\hat{\alpha}_k/\hat{\alpha}_{k-1})$. We divide $\mathbb{Z}$ into the arithmetic progressions $\mathcal{A}(q, \ell)$ $(0 \leqq \ell < q)$. When $y = qz + \ell$ is in such a progression, then $\hat{\alpha}_k^y = \hat{\alpha}_k^\ell \hat{\alpha}_{k-1}^{qz}$, and (3.10) becomes

$$P_1^*(z)\alpha_1^{*z} + \cdots + P_{k-1}^*(z)\alpha_{k-1}^{*z} = 0 \tag{3.11}$$

with $\alpha_i^* = \hat{\alpha}_i^q$ $(1 \leqq i \leqq k-1)$, $P_i^*(z) = \hat{\alpha}_i^\ell \widehat{P}_i(qz+\ell)$ for $1 \leqq i \leqq k-2$, but $P_{k-1}^*(z) = \hat{\alpha}_{k-1}^\ell \widehat{P}_{k-1}(qz+\ell) + \hat{\alpha}_k^\ell \widehat{P}_k(qz+\ell)$. Since $t(P_1^*, \ldots, P_{k-1}^*) < t(\mathbf{P})$, the zeros of (3.11) make up at most $Z(t-1, T)$ single numbers and arithmetic progressions. Taking the sum over ℓ in

$$0 \leqq \ell < q \leqq \hbar(T)^{-1} = \exp\left(6T^4\right) < \exp\left((6T)^{6T}\right),$$

we see that the set $\mathcal{Z}_C$ of solutions in our class has

$$\nu(\mathcal{Z}_C) < \exp\left((6T)^{6T}\right) Z\big(t-1, T\big). \tag{3.12}$$

In the other case of the Proposition, some $\alpha_i \not\approx \alpha_j$ have $h(\alpha_i^m/\alpha_j^m) \geqq \hbar$. Then just as in Section 5 of [4], there are polynomial vectors $\mathbf{P}^{(w)} = (P_1^{(w)}, \ldots, P_k^{(w)}) \neq (0, \ldots, 0)$ with $a(\mathbf{P}^{(w)}) \leqq a$, $t(\mathbf{P}^{(w)}) < t(\mathbf{P}) = t$, and where $1 \leqq w \leqq F$, such that every solution of (3.10) satisfies

$$P_1^{(w)}(y)\hat{\alpha}_1^y + \cdots + P_k^{(w)}(y)\hat{\alpha}_k^y = 0 \tag{3.13}$$

for some w: here (as in [4])

$$F = \exp\left((6t)^{5t}\right) + 5E\log E \quad \text{with} \quad E = 16t^2 a/\hbar.$$

Therefore $E < 16T^3\exp(6T^4) < \exp(7T^4)$, $E\log E < \exp(8T^4)$,

$$F < \exp\left((6T)^{5T}\right) + 5\exp(8T^4) < \exp\left((6T)^{6T}\right). \tag{3.14}$$

By our induction on t, the solutions of (3.13) consist of at most $Z(t-1, T)$ single numbers and arithmetic progressions. The single numbers give no problem, but we have to observe that the solutions of (3.10) are just *contained* in these progressions.

Say the progression is $y = az + b$ $(z \in \mathbb{Z})$, and (3.13) becomes

$$\widetilde{P}_1^{(w)}(z)\tilde{\alpha}_1^z + \cdots + \widetilde{P}_k^{(w)}(z)\tilde{\alpha}_k^z = 0 \tag{3.15}$$

with $\tilde{\alpha}_i = \hat{\alpha}_i^a$ and $\widetilde{P}_i^{(w)}(z) = \hat{\alpha}_i^b P_i^{(w)}(az+b)$ $(i = 1, \dots, k)$. Now if $\tilde{\alpha}_1 \dots, \tilde{\alpha}_k$ were distinct, then the validity of (3.15) for each $z \in \mathbb{Z}$ would imply that each $\widetilde{P}_i^{(w)} = 0$, hence each $P_i^{(w)} = 0$, which is not the case. Therefore $\tilde{\alpha}_1, \dots, \tilde{\alpha}_k$ are not all distinct, say $\tilde{\alpha}_{k-1} = \tilde{\alpha}_k$. In terms of z in $y = az + b$, the equation (3.10) becomes

$$\widetilde{P}_1(z)\tilde{\alpha}_1^z + \dots + \widetilde{P}_{k-1}(z)\tilde{\alpha}_{k-1}^z = 0 \tag{3.16}$$

where $\widetilde{P}_i(z) = \hat{\alpha}_i^b \widehat{P}_i(az+b)$ for $1 \leqq i \leqq k-2$, but $\widetilde{P}_{k-1}(z) = \hat{\alpha}_{k-1}^b \widehat{P}_{k-1}(az + b) + \hat{\alpha}_k^b \widehat{P}_k(az+b)$. Since $t(\widetilde{P}_1, \dots, \widetilde{P}_{k-1}) < t(\mathbf{P}) = t$, the solutions to (3.16) make up a set of not more that $Z(t-1, T)$ numbers and progressions. Altogether, the set $\mathcal{Z}_C$ of solutions in our class has

$$\nu(\mathcal{Z}_C) \leqq FZ(t-1,T)^2 < \exp((6T)^{6T})Z(t-1,T)^2 \tag{3.17}$$

by (3.14).

Considering the possible (fewer than a) solutions mentioned at the beginning, and summing over the classes C, we obtain

$$\begin{aligned}\nu(\mathcal{Z}) &< a + H(T)\exp\big((6T)^{6T}\big)Z(t-1,T)^2 \\ &< T + \exp\big((7T)^{6T} + (6T)^{6T}\big)\big(\exp\big((2^{t-1}-1)(7T)^{7T}\big)\big)^2 \\ &< \exp\big((2^t - 1)(7T)^{7T}\big) = Z(t,T).\end{aligned}$$

Hence (3.6) is established.

Since $t \leqq T$, we have in fact

$$\nu(\mathcal{Z}) < \exp\big(2^T(7T)^{7T}\big).$$

We have $T \leqq T_1 := e^{12t}$. Here (since we may suppose $t \geqq 2$ in our theorem) $T_1 \geqq e^{24}$, and

$$\nu(\mathcal{Z}) < \exp\big(T_1^{8T_1}\big) = \exp\exp(12t \cdot 8e^{12t}) < \exp\exp\exp(20t).$$

On the other hand $T \leqq k^n$, so that $T \leqq T_2 := k^a$, since $n \leqq a$. Here $T_2 \geqq 2$, so that

$$\nu(\mathcal{Z}) < \exp\big(T_2^{30T_2}\big) = \exp\exp(30T_2 \log T_2) = \exp\exp(30ak^a \log k). \quad \square$$

4. A lemma on linear independence

Lemma 2. *Let K be a field, and $\mathbf{a}_1, \dots, \mathbf{a}_k$ vectors in K^n. Suppose*

$$\mathbf{a}_i = (a_{i1}, \dots, a_{i,t_i}, 0, \dots, 0) \qquad (i = 1, \dots, k)$$

where $t_i = 0$ (so that $\mathbf{a}_i = \mathbf{0}$) or $t_i > 0$, $a_{i,t_i} \neq 0$. Set $t = t_1 + \dots + t_k$. Then there are fewer than e^{12t} ordered n-tuples $i_1, \dots, i_n$ (with $1 \leqq i_1, \dots, i_n \leqq k$) for which $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_n}$ are linearly independent.

Remark. The conclusion is trivially true when $\mathbf{a}_1, \dots, \mathbf{a}_k$ do not span K^n, in particular when $k < n$.

Proof. We may suppose that each $\mathbf{a}_i \neq \mathbf{0}$, so that each $t_i > 0$. Let $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_n}$ be linearly independent. For $1 \leqq j \leqq m = [\log n / \log 2] + 2$, let S_j be the set of numbers ℓ, $1 \leqq \ell \leqq n$, with $n/2^j < t_{i_\ell} \leqq n/2^{j-1}$. Then $S_1, \dots, S_m$ are pairwise disjoint, and their union is $\{1, \dots, n\}$. We have $t_{i_\ell} \leqq n/2^{j-1}$ for $\ell \in S_j \cap S_{j+1} \cup \dots \cup S_m$, so that the independence of $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_n}$ implies $|S_1| + \dots + |S_{j-1}| \geqq n - n/2^{j-1}$ $(2 \leqq j \leqq m)$. Given $S_1, \dots, S_{j-1}$, the set S_j is contained in the set $\{1, \dots, n\} \backslash (S_1 \cup \dots \cup S_{j-1})$ of cardinality $\leqq n/2^{j-1}$. This gives at most $2^{n/2^{j-1}}$ choices for S_j. Altogether the number of possibilities for all the sets $S_1, \dots, S_m$ is less than $2^{n+(n/2)+\cdots} = 4^n$.

Now supppose $S_1, \dots, S_m$ are given. When $\ell \in S_j$, how many choices are there for i_ℓ? For such ℓ, $t_{i_\ell} > n/2^j$, and since the number of subscripts i with $t_i > n/2^j$ is $< (2^j/n)t$, the number of choices for our i_ℓ is $< (2^j/n)t$. Since $|S_j| \leqq n/2^{j-1}$, we see that given j, the number of choices for all the i_ℓ with $\ell \in S_j$ is

$$< (2^j t/n)^{n/2^{j-1}}.$$

Taking the product over j, $1 \leqq j \leqq m$, we obtain

$$< (t/n)^{2n} (2 \cdot 2^{2/2} \cdot 2^{3/4} \cdot 2^{4/8} \dots)^n < (8t/n)^{2n}.$$

The number of possibilities for $S_1, \dots, S_m$ was $< 4^n$, so that altogether we get fewer than

$$(16t/n)^{2n}$$

n-tuples $i_1, \dots, i_n$. The function $f(x) = (16t/x)^x$ takes its maximum at $x_0 = 16t/e$, so that

$$(16t/n)^{2n} = f(n)^2 \leqq f(x_0)^2 = e^{32t/e} < e^{12t}. \qquad \square$$

5. Denominators of certain rational numbers

Let $q \in \mathbb{N}$ be given, and R the system of numbers u/q with $1 \leqq u \leqq q$, $\gcd(u, q) = 1$. This system has $n = \phi(q)$ elements, so that we may set $R = \{\rho_1, \ldots, \rho_n\}$, say. For $1 \leqq i,\ j \leqq n$, let r_{ij} be the denominator of $\rho_i - \rho_j$, i.e., r_{ij} is the least natural number with $r_{ij}(\rho_i - \rho_j) \in \mathbb{Z}$. Write $N(\varepsilon)$ for the number of triples i, j, k in $1 \leqq i, j, k \leqq n$ with

$$\operatorname{lcm}(r_{ij}, r_{ik}) \leqq \varepsilon n. \tag{5.1}$$

By a special case of Theorem A in [4], $N(\varepsilon) \leqq \zeta(2-\kappa)\varepsilon^\kappa n^3$ for any $0 < \kappa < 1$, where ζ is the Riemann zeta function.

Here we will have to deal with the number $M(\varepsilon)$ of triples i, j, k with

$$\operatorname{lcm}(r_{ij}, r_{ik}) \leqq \varepsilon q. \tag{5.2}$$

Lemma 3. *For $0 < \kappa < 1$*

$$M(\varepsilon) \leqq c(\kappa)\varepsilon^\kappa n^3. \tag{5.3}$$

For instance, when $\kappa = 1/2$, we may take $c(\kappa) = 11$.

Proof. $\operatorname{lcm}(r_{ij}, r_{ik})$ is the least common denominator of $\rho_i - \rho_j$, $\rho_i - \rho_k$. The least common denominator of $(u/q) - (v/q)$, $(u/q) - (w/q)$ is q/d where $d = \gcd(u - v, u - w, q)$. So if S denotes the set of numbers z in $1 \leqq z \leqq q$ with $\gcd(z, q) = 1$, then $M(\varepsilon)$ is the number of triples u, v, w in S with

$$\gcd(u - v, u - w, q) \geqq 1/\varepsilon. \tag{5.4}$$

When $\gcd(r, q) = 1$, the left hand side of (5.4) is unchanged if u, v, w are replaced by numbers congruent to $ru, rv, rw \pmod q$. Therefore $M(\varepsilon) = nM_1(\varepsilon)$, where $M_1(\varepsilon)$ is the number of pairs v, w in S with

$$\gcd(1 - v, 1 - w, q) \geqq 1/\varepsilon.$$

Given h, let $M_2(h)$ be the number of pairs v, w in S such that

$$h \mid \gcd(1 - v, 1 - w, q). \tag{5.5}$$

Then

$$M_1(\varepsilon) \leqq \sum_{h \geqq 1/\varepsilon} M_2(h) = \sum_{\substack{h|q \\ h \geqq 1/\varepsilon}} M_2(h).$$

The Euler totient function has $\phi(h) \geqq c_1(\kappa) h^{(1+\kappa)/2}$ for $0 < \kappa < 1$, and in particular one may take $c_1(1/2) = (2/27)^{1/4}$ (see, e.g., [2], Theorem 327, and the proof given there). Now suppose $h \mid q$, and let h', q' be their respective square free parts, i.e., the products of primes dividing h, q respectively. Then $\phi(q)/q = \phi(q')/q'$ and $\phi(h)/h = \phi(h')/h'$. Define t, t' by $q = ht$, $q' = h't'$, so that $\phi(q') = \phi(h')\phi(t')$. We obtain

$$\begin{aligned}(\phi(t')/t')(q/h) &= (\phi(q')/\phi(h'))(t/t') \\ &= (\phi(q)/\phi(h))(q'/q)(h/h')(t/t') = \phi(q)/\phi(h) \\ &\leqq c_1(\kappa)^{-1}\phi(q) h^{-(1+\kappa)/2} = c_1(\kappa)^{-1} n h^{-(1+\kappa)/2}.\end{aligned} \tag{5.6}$$

(5.5) yields $v = 1 + hx$, and $v \in S$ further implies $0 \leqq x < q/h$ and $(1 + hx, q) = 1$, so that $(1 + hx, t') = 1$. Since $(h, t') = 1$, the last relation allows $\phi(t')$ values of x in an interval of length t', hence $(\phi(t')/t')(q/h)$ values of x in $0 \leqq x < q/h$. This, then, is the number of possible values for v. It is also the number of possibilities for w, so that

$$M_2(h) = \big((\phi(t')/t')(q/h)\big)^2 \leqq c_1(\kappa)^{-2} n^2 h^{-1-\kappa}$$

by (5.6), and therefore

$$M_1(\varepsilon) \leqq c_1(\kappa)^{-2} n^2 \sum_{h \geqq 1/\varepsilon} h^{-1-\kappa}.$$

Suppose $0 < \varepsilon < 1/2$. The last sum may be estimated by an integral from $(1/\varepsilon) - 1$ to ∞, and since $(1/\varepsilon) - 1 \geqq 1/2\varepsilon$, it is $\leqq \kappa^{-1}(2\varepsilon)^\kappa$. We obtain

$$M(\varepsilon) = n M_1(\varepsilon) \leqq c_1(\kappa)^{-2} \kappa^{-1} 2^\kappa \varepsilon^\kappa n^3.$$

When $\varepsilon \geqq 1/2$, we have $\varepsilon^\kappa > 1/2$, so that trivially $M(\varepsilon) \leqq n^3 < 2\varepsilon^\kappa n^3$. Thus (5.3) is established.

When $\kappa = 1/2$, the value of $c(1/2)$ given above yields $M(\varepsilon) \leqq (27/2)^{1/2} \cdot 2 \cdot 2^{1/2} \varepsilon^{1/2} n^3 < 11 \varepsilon^{1/2} n^3$. We therefore may take $c(1/2) = 11$. □

In [4] a triple i, j, k was called ε-*bad* when (5.1) holds. We now (given our special system R) will consider i, j, k to be ε-*bbad* if (5.2) holds. Thus $M(\varepsilon)$ is the number of ε-*bbad* triples. When $\ell \geqq 3$ and $u_1, \ldots, u_\ell$ is an ℓ-tuple of integers with $1 \leqq u_1, \ldots, u_\ell \leqq n$, we will call this ℓ-tuple ε-*bbad* if some triple u_i, u_j, u_k with distinct i, j, k is ε-tuples is ε-*bbad*.

Corollary. *The number of* ε-*bbad* ℓ-*tuples is*

$$< 2\varepsilon^{1/2}\ell^3 n^\ell.$$

Proof. By the case $\kappa = 1/2$ of Lemma 3, the number of ε-*bbad* triples is $< 11\varepsilon^{1/2}n^3$. Therefore given i, j, k with $1 \leqq i < j < k \leqq \ell$, the number of ℓ-tuples $u_1, \ldots, u_\ell$ for which u_i, u_j, u_k is ε-*bbad* is $< 11\varepsilon^{1/2}n^3 \cdot n^{\ell-3} = 11\varepsilon^{1/2}n^\ell$. The number of triples i, j, k in question is $\binom{\ell}{3}$, so that the number of ε-*bbad* ℓ-tuples is

$$< 11\binom{\ell}{3}\varepsilon^{1/2}n^\ell < 2\varepsilon^{1/2}\ell^3 n^\ell. \qquad \square$$

As in [4], for α, β, γ in $\mathbb{C}^\times$, let $G(\alpha : \beta : \gamma)$ be the subgroup of $\mathbb{C}^\times$ generated by α/β and α/γ.

Suppose β is a primitive q-th root of 1, so that $\deg\beta = \phi(q) = n$. The set of conjugates $\beta^{[1]}, \ldots, \beta^{[n]}$ of β consists of the numbers $\exp(2\pi i u/q)$ with $1 \leqq u \leqq q$, $(u, q) = 1$. Clearly an ℓ-tuple of integers $u_1, \ldots, u_\ell$ with $1 \leqq u_1, \ldots, u_\ell \leqq n$ is ε-*bbad* precisely if for some triple u_i, u_j, j_k with distinct i, j, k in $1 \leqq i, j, k \leqq \ell$ we have

$$G\big(\beta^{[u_i]} : \beta^{[u_j]} : \beta^{[u_k]}\big) \leqq \varepsilon q.$$

Suppose $\mathbb{Q}(\beta) \subset K$, and let $\xi \mapsto \xi^{(\sigma)}$ ($\sigma = 1, \ldots, D$) signify the embeddings $K \hookrightarrow \mathbb{C}$. Given $\ell \geqq 3$, an ℓ-tuple $\mu_1, \ldots, \mu_\ell$ of numbers in $1 \leqq \mu \leqq D$ will be called ε-*bbad* if there are distinct numbers i, j, k in $1 \leqq i, j, k \leqq \ell$ such that

$$G\big(\beta^{(\mu_i)} : \beta^{(\mu_j)} : \beta^{(\mu_k)}\big) \leqq \varepsilon q. \tag{5.7}$$

Since for each u in $1 \leqq u \leqq n$ there are D/n numbers μ in $1 \leqq \mu \leqq D$ with $\beta^{(\mu)} = \beta^{[u]}$, the number of ε-*bbad* ℓ-tuples is less than

$$2\varepsilon^{1/2}\ell^3 n^\ell (D/n)^\ell = 2\varepsilon^{1/2}\ell^3 D^\ell. \tag{5.8}$$

6. The cases $k = 1$ and $n = 1$ of the Proposition

When $k = 1$, $M_j(X) = b_j X$ where $b_1, \dots, b_n$ are linearly independent over $\mathbb{Q}$. Then $b_1\alpha_1^x, \dots, b_n\alpha_1^x$ are linearly independent for every $x \in \mathbb{Z}$.

When $n = 1$, $M_1(\mathbf{X}) = a_1X_1 + \cdots + a_kX_k$ with nonzero coefficients. The number $M_1(\alpha_1^x, \dots, \alpha_k^x)$ is dependent when it is zero, i.e., when

$$a_1\alpha_1^x + \cdots + a_k\alpha_k^x = 0.$$

If x is a solution of this equation, there is a subset $\mathcal{S}(x) \subset \{1, \dots, k\}$ such that $1 \in \mathcal{S}(x)$ and

$$\sum_{i \in \mathcal{S}(x)} a_i\alpha_i^x = 0, \tag{6.1}$$

but no subsum of (6.1) vanishes, i.e., (6.1) fails to hold when $\mathcal{S}(x)$ is replaced by a set $\mathcal{S}'$ with $\emptyset \neq \mathcal{S}' \subsetneqq \mathcal{S}(x)$. By Lemma 8 of [4], for all but at most

$$G(k) = \exp\left((7k)^{4k}\right) \tag{6.2}$$

solutions x, the set $\mathcal{S}(x)$ has the property that $\alpha_i \approx \alpha_j$ for any $i, j \in \mathcal{S}(x)$. We put such exceptional solutions x into a class by itself; condition (b) of the Proposition will be satisfied by taking m sufficiently large.

Now let $\mathcal{S} \neq \emptyset$ be a subset of $\{1, \dots, k\}$ such that $\alpha_i \approx \alpha_j$ for $i, j \in \mathcal{S}$. We will consider solutions having $\mathcal{S}(x) = \mathcal{S}$. For convenience of notation, we will suppose $\mathcal{S} = \{1, \dots, \ell\}$, so that (6.1) becomes

$$a_1\alpha_1^x + \cdots + a_\ell\alpha_\ell^x = 0. \tag{6.3}$$

There is no solution when $\ell = 1$; hence we may suppose $\ell \geqq 2$. Since no subsum of (6.3) vanishes, we know from Lemma 3 in [4] (which is an immediate consequence of a theorem of Evertse [1]) that there are vectors $\mathbf{c}^{(w)} = (c_1^{(w)}, \dots, c_\ell^{(w)})$ where

$$1 \leqq w \leqq B(\ell) = \ell^{3\ell^2} \leqq k^{3k^2}$$

such that $\alpha_1^x, \dots, \alpha_\ell^x$ is proportional to some $\mathbf{c}^{(w)}$. Consider solutions with fixed w. When x, x' are such solutions, $(\alpha_1/\alpha_2)^2 = c_1^{(w)}/c_2^{(w)}$, and similarly for x', so that

$$(\alpha_1/\alpha_2)^{x-x'} = 1.$$

When m is the order of α_1/α_2, then $x \equiv x' \pmod{m}$, and $\alpha_1^m/\alpha_2^m = 1$, so that $\mathrm{ord}(\alpha_1^m/\alpha_2^m) = 1$.

The number of sets $\mathcal{S}$ is $< 2^k$, the number of choices for w is $\leqq k^{3k^2}$, so that we obtain $< 2^k \cdot k^{3k^2}$ classes. The total number of classes is

$$< G(k) + 2^k \cdot k^{3k^2} < \exp\left((7k)^{6k}\right) = \exp\left((7T)^{6T}\right) = H(T),$$

since $n = 1$ yields $T = k$.

7. Proof of the Proposition

We may suppose that $k > 1$, $n > 1$. Let K be a field containing $\alpha_1, \dots, \alpha_k$ and the coefficients of our linear forms. Set $D = \deg K$, and let $\xi \mapsto \xi^{(\sigma)}$ $(\sigma = 1, \dots, D)$ signify the embeddings $K \hookrightarrow \mathbb{C}$. For $1 \leqq \sigma_1, \dots, \sigma_n \leqq D$ and $1 \leqq i_1, \dots, i_n \leqq k$, set

$$\mathcal{A}\begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix} = \alpha_{i_1}^{(\sigma_1)} \dots \alpha_{i_n}^{(\sigma_n)},$$

$$\Delta\begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix} = \det(\mathbf{a}_{i_1}^{(\sigma_1)}, \dots, \mathbf{a}_{i_n}^{(\sigma_n)})$$

as in [4]. Given $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ write

$$f_{\boldsymbol{\sigma}}(x) = \sum_{i_1=1}^{k} \cdots \sum_{i_n=1}^{k} \Delta\begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix} \left(\mathcal{A}\begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix}\right)^x. \tag{7.1}$$

Then according to (10.2) of [4], whenever the n quantities (3.3) are linearly dependent over $\mathbb{Q}$, we have

$$f_{\boldsymbol{\sigma}}(x) = 0 \tag{7.2}$$

for each $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$.

Let $q = q(\boldsymbol{\sigma})$ be the number of nonzero summands in (7.1). Then $q \leqq k^n$, but also $q \leqq e^{12t}$ by Lemma 2. Therefore $q(\boldsymbol{\sigma}) \leqq T$, where T is defined by (3.1).

As in [4], there are $\sigma_2, \dots, \sigma_n$ and $u_1, \dots, u_n$ such that

$$\Delta\begin{pmatrix} 1, \sigma_2, \dots, \sigma_n \\ u_1, u_2, \dots, u_n \end{pmatrix} \neq 0.$$

As in §10 of [4], define a set $\mathcal{S}$ of n-tuples such that this holds for every $\boldsymbol{\sigma} = (\sigma_1 = 1, \sigma_2, \ldots, \sigma_n) \in \mathcal{S}$. Define sets $\mathcal{I}(\boldsymbol{\sigma})$ as in [4]. They have cardinality $\leqq T$.

Suppose $|\mathcal{I}(\boldsymbol{\sigma})| = 1$ for some $\boldsymbol{\sigma} \in \mathcal{S}$. Then (7.2) has at most

$$G(q) \leqq G(T) \leqq H(T)$$

solutions x where $G(q) = \exp((7q)^{4q})$: This follows from the Corollary to Lemma 8 of [4], and corresponds to the inequality in the paragraph below (10.6) of [4].

We may then suppose that $|\mathcal{I}(\boldsymbol{\sigma})| > 1$ for each $\boldsymbol{\sigma} \in \mathcal{S}$. The number of n-tuples $(i_1, \ldots, i_n)$ is k^n. Further $\mathcal{I}(\boldsymbol{\sigma})$ is a set of at most T such n-tuples. Therefore the number of possibilities for $\mathcal{I}(\boldsymbol{\sigma})$ is $\leqq k^{nT}$. As in [4], we construct a set $\mathcal{I}$ of n-tuples $(i_1, \ldots, i_n)$, and sets $\mathcal{S}'_2, \mathcal{S}'_3(\sigma_2), \ldots, \mathcal{S}'_n(\sigma_2, \ldots \ldots, \sigma_{n-1})$. Here $|\mathcal{I}| \leqq T$. In place of (10.8) of [4], we may conclude that each set $\mathcal{S}'_j(\ldots)$ has cardinality

$$|\mathcal{S}'_j(\ldots)| > D/(nk^{nT}) \geqq D/T^{1+T^2} \geqq D/T^{(5/4)T^2} \tag{7.3}$$

where we used that $n \geqq 2$, $k \geqq 2$, $T \geqq \max(4, n, k)$. With $\mathcal{S}'$ constructed as in [4],

$$\mathcal{I}(\boldsymbol{\sigma}) = \mathcal{I} \quad \text{when} \quad \boldsymbol{\sigma} \in \mathcal{S}'.$$

For $2 \leqq j \leqq n$, let $\mathcal{T}_j$ be the set of numbers $i_j \neq u_j$ in $1 \leqq i_j \leqq k$ such that

$$(i_1, \ldots, i_{j-1}, i_j, u_{j+1}, \ldots, u_n) \in \mathcal{I} \tag{7.4}$$

for certain $i_1, \ldots, i_{j-1}$. (When $j = n$, (7.4) becomes $(i_1, \ldots, i_{n-1}, i_n) \in \mathcal{I}$.) Lemma 17 of [4] holds in the following modified form.

Lemma 4. *Suppose $i_j \in \mathcal{T}_j$ and $\alpha_{i_j} \not\approx \alpha_{u_j}$. Then*

$$h(\alpha_{i_j}/\alpha_{u_j}) > 1/\big(8T^7 \deg(\alpha_{i_j}/\alpha_{u_j})\big).$$

Proof. (10.12) of [4] becomes $n_K(\alpha_{i_j}/\alpha_{u_j}) > D/T^{(5/4)T^2}$ by (7.3). The Corollary to Lemma 11 of [4] yields

$$h(\alpha_{i_j}/\alpha_{u_j}) > 1/\big(4\big(\log T^{(5/4)T^2}\big)^3 \deg(\alpha_{i_j}/\alpha_{u_j})\big).$$

Here (since $T \geqq 4$),

$$4\big(\log T^{(5/4)T^2}\big)^3 < 8(T^2\log T)^3 < 8T^7. \qquad \square$$

For $2 \leqq j \leqq n$, let $\mathcal{T}_j^*$ be the set of numbers $\alpha_{i_j}/\alpha_{u_j}$ with $i_j \in \mathcal{T}_j$. Say $\mathcal{T}_j^* = \{\beta_1, \dots, \beta_r\}$. In analogy to (10.13), (10.14) of [4] we have

$$n_K(\beta_s) > D/T^{(5/4)T^2}, \quad h(\beta_s) > 1/(8T^7 \deg\beta_s) \tag{7.5}$$

for each s, $1 \leqq s \leqq r$, with $\beta_s \not\approx 1$. Lemma 18 of [4] now becomes

Lemma 5. *Set $\ell = 3T$, and suppose*

$$D > e^{3T^4}. \tag{7.6}$$

Let $2 \leqq j \leqq n$ and $\sigma_1, \dots, \sigma_{j-1}$ with $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}_2'$, $\dots$, $\sigma_{j-1} \in \mathcal{S}_{j-1}'(\sigma_2, \dots, \sigma_{j-2})$ be given. There is a subset $\mathcal{S}_j'' = \mathcal{S}_j''(\sigma_1, \dots, \sigma_{j-1})$ of $\mathcal{S}_j'(\sigma_1, \dots, \sigma_{j-1})$ of cardinality

$$|\mathcal{S}_j''(\sigma_1, \dots, \sigma_{j-1})| = \ell$$

such that for any triple of distinct numbers ϕ, ψ, ω in $\mathcal{S}_j''(\sigma_1, \dots, \sigma_{j-1})$, and for $1 \leqq s \leqq r$,

$$|G(\beta_s^{(\phi)} : \beta_s^{(\psi)} : \beta_s^{(\omega)})| > \begin{cases} T^{-11T^3} \deg\beta_s & \text{when } \beta_s \not\approx 1, \\ T^{-11T^3} \operatorname{ord}\beta_s & \text{when } \beta_s \approx 1. \end{cases} \tag{7.7}$$

Proof. For brevity, put $\mathcal{S}_j' = \mathcal{S}_j'(\sigma_2, \dots, \sigma_{j-1})$. When $r = 0$, the condition (7.7) is vacuous. Since $\mathcal{S}_j'$ has cardinality $> D/T^{(5/4)T^2} > 3T = \ell$ by (7.3), (7.6), there is certainly a subset of cardinality ℓ.

Suppose $r > 0$. Set

$$\varepsilon = T^{-10T^3}. \tag{7.8}$$

Note that

$$108 r \varepsilon^{1/2} T^3 T^{(5/4)T^2 \ell} < 108 \varepsilon^{1/2} T^{4+4T^3} < \varepsilon^{1/2} T^{5T^3} = 1 \tag{7.9}$$

since $T \geqq 4$, and that

$$2\ell^2 T^{(5/4)T^2\ell} < 18T^{2+4T^3} < T^{5T^3} < e^{3T^4} < D \tag{7.10}$$

by (7.6).

Let $\beta_s \in \mathcal{T}_j^*$ be given. Then if $\beta_s \not\approx 1$, we see from the argument around (10.21) of [4] that the number of ε-*bad* ℓ-tuples $\mu_1, \ldots, \mu_\ell$ with each μ_i in $\mathcal{S}_j'$ is less than $\varepsilon^{1/2}\ell^3 D^\ell$. On the other hand when $\beta_s \approx 1$, then by (5.8) the number of ε-*bbad* ℓ-tuples is less than $2\varepsilon^{1/2}\ell^3 D^\ell$. Summing over s in $1 \leqq s \leqq r$, we see that the number of ℓ-tuples $\mu_1, \ldots, \mu_\ell$ in $\mathcal{S}_j'$ which are ε-*bad* or ε-*bbad* for some β_s is

$$< 2r\varepsilon^{1/2}\ell^3 D^\ell = 54r\varepsilon^{1/2}T^3 D^\ell < \frac{1}{2}\Big(D/T^{(5/4)T^2}\Big)^\ell$$

by (7.9). The number of ℓ-tuples for which at least two elements are equal is

$$\leqq \binom{\ell}{2} D^{\ell-1} < \ell^2 D^{\ell-1} < \frac{1}{2}\Big(D/T^{(5/4)T^2}\Big)^\ell$$

by (7.10). Since $|\mathcal{S}_j'| \geqq D/T^{(5/4)T^2}$, the number of all possible ℓ-tuples in $\mathcal{S}_j'$ is $\geqq (D/T^{(5/4)T^2})^\ell$. Therefore there is an ℓ-tuple of *distinct* numbers in $\mathcal{S}_j'$ which is not ε-*bad* or ε-*bbad* for any of $\beta_1, \ldots, \beta_r$. By the definition of ε-*bad* and ε-*bbad* this means that for any three distinct numbers i, j, k, we have for $\beta_s \not\approx 1$ that

$$\begin{aligned} &|G(\beta_s^{(\mu_i)} : \beta_s^{(\mu_j)} : \beta_s^{(\mu_k)})| > \varepsilon n(\beta_s) \\ &= \varepsilon(\deg \beta_s) D^{-1} n_K(\beta_s) > \varepsilon(\deg \beta_s)/T^{(5/4)T^2} > T^{-11T^3} \deg \beta_s \end{aligned}$$

(in analogy to an estimate below (10.23) in [4]), and using (7.5), (7.8), whereas for $\beta_s \approx 1$ the opposite of (5.7) holds, so that

$$|G(\beta_s^{(\mu_i)} : \beta_s^{(\mu_j)} : \beta_s^{(\mu_k)})| > \varepsilon \operatorname{ord} \beta_s > T^{-10T^3} \operatorname{ord} \beta_s.$$

We now set $\mathcal{S}_j''(\sigma_2, \ldots, \sigma_{j-1}) = \{\mu_1, \ldots, \mu_\ell\}$. Then indeed any three numbers ϕ, ψ, ω in $\mathcal{S}_j''(\ldots)$ have (7.7). $\square$

We will assume from now on that (7.6) holds. This can always be achieved by enlarging K, if necessary.

We define $\mathcal{S}''$ to be the set of n-tuples $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ with $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}_2''$, $\sigma_3 \in \mathcal{S}_3''(\sigma_2), \ldots, \sigma_n \in \mathcal{S}_n''(\sigma_1, \ldots, \sigma_{n-1})$. We will deal with the equation (7.2) with $\boldsymbol{\sigma} \in \mathcal{S}''$. The number of these equations is $|\mathcal{S}''| = \ell^{n-1} < (3T)^n$.

The remainder of our arguments follows Section 11 of [4], with a few changes as follows. Each equation (7.2) splits, with at most $G(q) \leqq G(T)$ exceptions. If we carry this out for each $\boldsymbol{\sigma} \in \mathcal{S}''$, we get

$$|\mathcal{S}''|G(T) < (3T)^n \exp\big((7T)^{4T}\big) < \exp\big((7T)^{5T}\big) \tag{7.11}$$

exceptions. This takes the place of (11.1) in [4].

As in (10.9) of [4], we have $\mathcal{I}(\boldsymbol{\sigma}) = \mathcal{I}$ when $\boldsymbol{\sigma} \in \mathcal{S}'$, hence certainly when $\boldsymbol{\sigma} \in \mathcal{S}''$. Subsets $\mathcal{I}(\boldsymbol{\sigma}, x)$ of $\mathcal{I}$ are defined in terms of the equation (11.4) of [4]. We have $|\mathcal{I}| \leqq T$, so that there are fewer than T tuples $\mathbf{i} = (i_1, \ldots, i_n) \neq (u_1, \ldots, u_n)$ in $\mathcal{I}$. Hence given $\sigma_1, \ldots, \sigma_{n-1}$, there will be an n-tuple $\mathbf{i} = \mathbf{i}(\sigma_1, \ldots, \sigma_{n-1}, x) \neq (u_1, \ldots, u_n)$ such that $\mathbf{i} \in \mathcal{I}(\boldsymbol{\sigma}, x)$ for at least $\ell/T = 3$ of the numbers $\sigma_n \in \mathcal{S}_n''(\sigma_2, \ldots, \sigma_{n-1})$. Let $\mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1}, x)$ consist of 3 such numbers σ_n. Continuing in this way, we construct sets $\mathcal{S}_2^*(x), \mathcal{S}_3^*(\sigma_2, x), \ldots, \mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1}, x)$, a set $\mathcal{S}^*(x)$ and $\mathbf{i}(x)$ such that $\mathbf{i}(x) \in \mathcal{I}(\boldsymbol{\sigma}, x)$ when $\boldsymbol{\sigma} \in \mathcal{S}^*(x)$.

Define systems Σ of 3-element sets as in [4]. When $\mathbf{i} \in \mathcal{I}$, define again a certain class $C(\mathbf{i}, \Sigma)$ of solutions. The number of classes $C(\mathbf{i}, \Sigma)$ is less than

$$T\ell^{3^n} = T(3T)^{3^n}, \tag{7.12}$$

which replaces (11.7) of [4]. When studying solutions x in a given class $C(\mathbf{i}, \Sigma)$, let $j = j(\mathbf{i})$ be the number such that $\mathbf{i} = (i_1, \ldots, i_j, u_{j+1}, \ldots, u_n)$ with $i_j \neq u_j$. In contrast to [4], we can no longer claim that $j > 1$. We can only claim that $j > 1$ if $\alpha_{i_1} \not\approx \alpha_{u_1}$.

The sets $\mathcal{I}(\boldsymbol{\sigma}_\phi, x)$, $\mathcal{I}(\boldsymbol{\sigma}_\psi, x)$, $\mathcal{I}(\boldsymbol{\sigma}_\omega, x)$ are in the set $\mathcal{I}$ of cardinality $\leqq T$. Therefore $C(\mathbf{i}, \Sigma)$ may be divided into

$$2^{3T} \tag{7.13}$$

subclasses $C(\mathbf{i}, \Sigma, \mathcal{I}_\phi, \mathcal{I}_\psi, \mathcal{I}_\omega)$ (where (7.13) replaces the number in (11.10) of [4]). Since each $\mathcal{I}(\mathbf{i}, x)$ is of cardinality $\leqq T$, the estimate (11.11) of [4] may be replaced by

$$T(3T)^{3^n} 2^{3T} B(T)^3 < 2^{4T} T^{9T^2} (3T)^{3^n} < \exp(5T^3 + 3^n T). \tag{7.14}$$

Eventually, just as in [4], we arrive at

$$(\beta_s^{(\phi)}/\beta_s^{(\psi)})^{x-x'} = (\beta_s^{(\phi)}/\beta_s^{(\omega)})^{x-x'} = 1$$

when x, x' lie in the same class. So if $|G(\beta_s^{(\phi)} : \beta_s^{(\psi)} : \beta_s^{(\omega)})| = m$, then $x \equiv x' \pmod{m}$. Further by (7.7),

$$m > \begin{cases} T^{-11T^3} \deg \beta_s & \text{if } \beta_s \not\approx 1, \\ T^{-11T^3} \operatorname{ord} \beta_s & \text{if } \beta_s \approx 1. \end{cases}$$

When $\beta_s \not\approx 1$, we obtain from (7.5) that

$$h(\beta_s^m) = mh(\beta_s) > T^{-11T^3}/8T^7 > e^{-6T^4} = \hbar(T).$$

When $\beta_s \approx 1$, we note that $m \mid \operatorname{ord} \beta_s$, so that

$$\operatorname{ord}(\beta_s^m) = m^{-1} \operatorname{ord} \beta_s < T^{11T^3} < e^{6T^4} = \hbar(T)^{-1}.$$

But β_s is a quotient α_i/α_j, and depending on whether $\alpha_i \not\approx \alpha_j$ or $\alpha_i \approx \alpha_j$, we get $h(\alpha_i^m/\alpha_j^m) > \hbar(T)$ or $\operatorname{ord}(\alpha_i^m/\alpha_j^m) < \hbar(T)^{-1}$.

How many classes do we have? Adding (7.11) to (7.14) we get

$$\exp\left((7T)^{5T}\right) + \exp\left(5T^3 + 3^n T\right) < \exp\left((7T)^{6T}\right) = H(T)$$

classes. □

References

[1] J. H. Evertse, The number of solutions of linear equations in roots of unity, *Acta Arith.* **99.1** (1999), 45–51.

[2] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 3rd edn, *Clarendon Press*, *Oxford*, 1954.

[3] C. Lech, A note on recurring series, *Ark. Math.* **2** (1953), 417–421.

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

WOLFGANG M. SCHMIDT
UNIVERSITY OF COLORADO
BOULDER
USA

(Received September 16, 1999; revised March 14, 2000)