ACTA ARITHMETICA
113.4 (2004)

Diophantine equations $E(\mathbf{x}) = P(\mathbf{x})$ with E exponential, P polynomial

by

Wolfgang M. Schmidt (Boulder, CO)

Dedicated to Robert Tijdeman on his sixtieth birthday

1. Introduction. A theorem of Laurent [2] tells us that polynomial-exponential equations of a fairly general type have only finitely many solutions in integers. It would be desirable to have a version of this theorem with bounds on the number of solutions, which do not depend on the coefficients of the equation. This has been achieved for purely exponential equations [3], and for equations in one variable [4]. In the present paper we will indicate such bounds for certain solutions of the equation of the title.

More precisely, we will deal with equations

$$E(\mathbf{x}) = P(\mathbf{x}) \tag{1.1}$$

in $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, where P is a polynomial and E is exponential of the type

$$E(\mathbf{x}) = E_1(x_1) + \ldots + E_n(x_n) + c, \tag{1.2}$$

where c is a complex number, and

$$E_l(x) = a_{l1}\alpha_{l1}^x + \ldots + a_{l,k_l}\alpha_{l,k_l}^x \qquad (l = 1, \ldots, n) \tag{1.3}$$

with $k_l > 0$ and $a_{li} \in \mathbb{C}, \alpha_{li} \in \mathbb{C}^\times$, where no α_{li} is a root of unity ($1 \le l \le n$, $1 \le i \le k_l$). A solution of (1.1) will be called *degenerate* if

$$\sum_{l\in\lambda} E_l(x_l) = 0 \tag{1.4λ}$$

for some nonempty subset λ of $\{1, \ldots, n\}$. As will be pointed out in Section 2, it is an easy consequence of Laurent's theorem that there are only finitely many nondegenerate solutions.

2000 *Mathematics Subject Classification*: 11D61, 11D45.
Supported in part by NSF DMS 0074531.

The notation $A \ll B$ will mean that $A \leq c_\circ B$ with an effective constant $c_\circ$ depending only on

$$N := \sum_{l=1}^{n} k_l \quad \text{and} \quad d := \text{total degree of } P. \tag{1.5}$$

Observe that $n \leq N$.

Theorem. *Suppose P has rational coefficients. Then all but $\ll 1$ solutions of* (1.1) *are degenerate.*

On the other hand it is easy to give examples of equations with infinitely many degenerate solutions.

A number α is a *radical* of β if $\alpha^u = \beta$ for some $u \in \mathbb{N}$. When P has rational coefficients, the equation (1.1) yields the relation

$$E(\mathbf{x}) \in \mathbb{Q}. \tag{1.6}$$

In Theorem 1 of [5] it was shown that if no α_{li} is a radical of an algebraic number of degree $\leq N$, then all but $\ll 1$ solutions of (1.6) are degenerate, so that our present Theorem holds in this case. But observe that we now have the weaker hypothesis that no α_{li} is a root of unity. The proof of our Theorem will depend on [5], and on some assertions in [3], [4].

Example. Let α, β in $\mathbb{C}^\times$ be multiplicatively independent, and consider the equation

$$\alpha^{2x_1} - \alpha \cdot \alpha^{3x_2} + \beta^{x_3} - \beta^{5x_4} = x_2 + x_3 - x_1 - x_4. \tag{1.7}$$

The left hand side is as $E(\mathbf{x})$ in (1.2), (1.3), with $c = 0$, $n = 4$, and each $k_l = 1$. When λ is a nonempty subset of $\{1, 2, 3, 4\}$, let $\mathcal{S}(\lambda)$ be the set of solutions which have (1.4λ), but not (1.4λ') for any nonempty set $\lambda' \subsetneqq \lambda$. By the Theorem, all but $\ll 1$ solutions of (1.7) are in $\mathcal{S}(\lambda)$ for some λ. When $\lambda = \{1, 2\}$, so that (1.4λ) becomes $\alpha^{2x_1} - \alpha \cdot \alpha^{3x_2} = 0$, we obtain $2x_1 = 1 + 3x_2$, therefore $x_1 = 3y + 2$, $x_2 = 2y + 1$ with $y \in \mathbb{Z}$. After insertion into (1.7) we have

$$\beta^{x_3} - \beta^{5x_4} = x_3 - x_4 - y - 1. \tag{1.8}$$

The Theorem does not apply to this last equation since the variable y does not occur in the exponential function on the left hand side. As is easily seen, the only solutions are with $\beta^{x_3} - \beta^{5x_4} = 0$, unless β is an algebraic integer. When $\beta \in \mathbb{Z}$ we obtain a 2-parameter family of solutions parametrized by x_3, x_4. On the other hand suppose β is not a radical of a rational or a quadratic. Then all but $\ll 1$ solutions of (1.8) have $\beta^{x_3} - \beta^{5x_4} = 0$ by Theorem 1 of [5], so that $x_3 = 5x_4$ and $4x_4 - y - 1 = 0$, giving a 1-parameter family of solutions parametrized by x_4. As will be shown in Section 3, this conclusion holds under the weaker assumption that β is not a radical of a rational, or a quadratic of norm 1. The assumption cannot be entirely dispensed with. For instance, if β is a quadratic unit of norm -1 (so that it is a radical of a unit of norm 1), the conjugate β' of β equals $-1/\beta$, and

$$\beta^{-5x_4} - \beta^{5x_4} = -\beta'^{5x_4} - \beta^{5x_4} \in \mathbb{Z}$$

when x_4 is odd. We then have the family of solutions with $x_3 = -5x_4$, $x_4 = 2t+1$ where $t \in \mathbb{Z}$.

Similar considerations apply when $\lambda = \{3,4\}$. For all other nonempty sets λ we claim that $|\mathcal{S}(\lambda)| \ll 1$. For instance, take $\lambda = \{1,2,3\}$. According to [1] (see also the formulations in Section 2 of [5]), the solutions in $\mathcal{S}(\lambda)$ fall into $\ll 1$ classes, and for solutions in a given class the triples $(\alpha^{2x_1}, -\alpha\cdot\alpha^{3x_2}, \beta^{x_3})$ are proportional to a given triple, i.e., will have $\alpha^{2x_1} = \gamma(-\alpha\cdot\alpha^{3x_2}) = \gamma'\beta^{x_3}$ for some γ, γ'. But these relations for fixed γ, γ' have (by the multiplicative independence of α, β) at most one solution in integers x_1, x_2, x_3. Or take $\lambda = \{1,3\}$, which gives $\alpha^{2x_1} + \beta^{x_3} = 0$, hence $x_1 = x_3 = 0$ by the multiplicative independence of α, β, and we obtain $-\alpha\cdot\alpha^{3x_2} - \beta^{5x_4} = x_2 - x_4$. By our Theorem, both sides vanish for all but $\ll 1$ solutions, and then $x_2 = x_4 = 0$.

2. Laurent's theorem. Let polynomials $P_i(\mathbf{x}) = P_i(x_1,\dots,x_n)$ and exponential functions $\boldsymbol{\alpha}_i^{\mathbf{x}} = \alpha_{i1}^{x_1}\dots\alpha_{in}^{x_n}$ $(1 \le i \le q)$ with nonzero α_{ij} be given. The symbol $\mathcal{P}$ will denote a partition of $\{1,\dots,q\}$, also interpreted as a partition of the set of functions $P_i(\mathbf{x})\boldsymbol{\alpha}_i^{\mathbf{x}}$ $(i = 1,\dots,q)$. The notation $\Lambda \in \mathcal{P}$ will mean that Λ is a subset determined by $\mathcal{P}$. Further $G(\mathcal{P})$ signifies the group of points $\mathbf{x} \in \mathbb{Z}^n$ having $\boldsymbol{\alpha}_i^{\mathbf{x}} = \boldsymbol{\alpha}_j^{\mathbf{x}}$ for every pair i, j of numbers lying in the same set $\Lambda \in \mathcal{P}$.

THEOREM 2.1 (M. Laurent [2]). *Let $\mathcal{S}(\mathcal{P})$ consist of solutions $\mathbf{x} \in \mathbb{Z}^n$ of the system of equations*

$$\sum_{i\in\Lambda} P_i(\mathbf{x})\boldsymbol{\alpha}_i^{\mathbf{x}} = 0 \qquad (\Lambda \in \mathcal{P}), \tag{2.1$\mathcal{P}$}$$

which are not solutions of $(2.1\mathcal{P}')$ for any proper refinement $\mathcal{P}'$ of $\mathcal{P}$. Then $\mathcal{S}(\mathcal{P})$ is finite if $G(\mathcal{P}) = \{\mathbf{0}\}$.

We will derive the (qualitative) result that (1.1) has only finitely many nondegenerate solutions. This equation may be written as

$$\sum_{l,i} a_{li}\alpha_{li}^{x_l} - P(\mathbf{x})\boldsymbol{\alpha}_0^{\mathbf{x}} = 0 \tag{2.2}$$

with $\boldsymbol{\alpha}_0 = (1,\dots,1)$. It is of polynomial-exponential type with $q = N+1$ summands. Each solution lies in a set $\mathcal{S}(\mathcal{P})$ (not necessarily uniquely determined) where $\mathcal{P}$ is a partition of the set of summands. It will be enough to show that for any $\mathcal{P}$, either $\mathcal{S}(\mathcal{P})$ is finite, or its elements are degenerate.

Let $\mathcal{P}$ be given. Write $0 \stackrel{.}{\sim} 0$, and for $1 \le l \le n$ write $l \stackrel{.}{\sim} 0$ (and also $0 \stackrel{.}{\sim} l$) if both $-P(\mathbf{x})\boldsymbol{\alpha}_0^{\mathbf{x}}$ and $a_{li}\alpha_{li}^{x_l}$ lie in Λ for some $\Lambda \in \mathcal{P}$ and some i, $1 \le i \le k_l$. When $1 \le l, m \le n$, write $l \stackrel{.}{\sim} m$ if both $a_{li}\alpha_{li}^{x_l}$ and $a_{mj}\alpha_{mj}^{x_m}$ lie in Λ for some $\Lambda \in \mathcal{P}$ and some i, j with $1 \le i \le k_l$, $1 \le j \le k_m$. On the other hand, for $0 \le l, m \le n$, write $l \sim m$ if there are $l_1, \ldots, l_\nu$ with $l_1 = l$, $l_\nu = m$ and $l_t \stackrel{.}{\sim} l_{t+1}$ $(1 \le t < \nu)$. Then $\sim$ is an equivalence relation on the set $\{0, 1, \ldots, n\}$.

Case A: *There is just one equivalence class.* We claim that $G(\mathcal{P}) = \{\mathbf{0}\}$, which by Laurent's theorem implies the finiteness of $\mathcal{S}(\mathcal{P})$. We have $l \stackrel{.}{\sim} 0$ for some l, $1 \le l \le n$. Then $\mathbf{x} \in G(\mathcal{P})$ has $\alpha_{li}^{x_l} = \boldsymbol{\alpha}_0^{\mathbf{x}} = 1$ for some i, therefore $x_l = 0$ since α_{li} is not a root of unity. Say $m \stackrel{.}{\sim} l$ with $1 \le m \le n$. Then $\alpha_{mj}^{x_m} = \alpha_{li}^{x_l} = 1$ for some i, j, hence $x_m = 0$. Continuing in this way we see that $0 = x_l = x_m = \ldots$, so that indeed $G(\mathcal{P}) = \{\mathbf{0}\}$.

Case B: *There is more than one equivalence class.* Let $\lambda = \{l_1, \ldots, l_\nu\}$ be an equivalence class not containing 0. All the $a_{li}\alpha_{li}^{x_l}$ with $l \in \lambda$, $1 \le i \le k_l$ belong to sets $\Lambda \in \mathcal{P}$ which do not contain $-P(\mathbf{x}) = -P(\mathbf{x})\boldsymbol{\alpha}_0^{\mathbf{x}}$ or any $a_{mj}\alpha_{mj}^{x_m}$ with $m \notin \lambda$. Let these sets be $\Lambda_1, \ldots, \Lambda_s$. For $\mathbf{x} \in \mathcal{S}(\mathcal{P})$, the sum of the $a_{li}\alpha_{li}^{x_l}$ with $1 \le i \le k_l$ and l belonging to some Λ_t, is zero. The union of $\Lambda_1, \ldots, \Lambda_s$ is the union of the $a_{li}\alpha_{li}^{x_l}$ with $1 \le i \le k_l$ and $l \in \lambda$. Therefore (1.4λ) holds, and $\mathbf{x}$ is degenerate. ∎

3. Rational values of $\beta^x - \beta^y$. Suppose β is not a radical of a rational, or of a quadratic of norm 1. To prove a certain assertion made in the Introduction it will be enough to show that the set of integer pairs (x, y) with $x \ne y$ and $\beta^x - \beta^y$ rational has cardinality $\ll 1$.

In view of Theorem 1 of [5] we may assume β to be algebraic. Say β is of degree D, with conjugates $\beta^{(1)} = \beta, \beta^{(2)}, \ldots, \beta^{(D)}$. Suppose at first that for some σ, $1 < \sigma \le D$, the numbers $\beta, \beta^{(\sigma)}$ are multiplicatively independent. The rationality of $\beta^x - \beta^y$ implies the equation

$$\beta^x - \beta^y - \beta^{(\sigma)x} + \beta^{(\sigma)y} = 0. \tag{3.1}$$

When $\mathcal{P}$ is a partition of the set of the four summands on the left hand side, define $\mathcal{S}(\mathcal{P})$ as in the preceding section. If $\Lambda_0 = \{\beta^x, -\beta^y\}$ is a set of $\mathcal{P}$, then $\beta^x - \beta^y = 0$, hence $x = y$. We will show that for any partition $\mathcal{P}$ not containing Λ_0, $|\mathcal{S}(\mathcal{P})| \ll 1$. When $\mathcal{P}$ is no *proper* partition, so that for $(x, y) \in \mathcal{S}(\mathcal{P})$ no proper subsum of (3.1) vanishes, then by [1], the solutions in $\mathcal{S}(\mathcal{P})$ fall into $\ll 1$ classes, with solutions in a given class having $\beta^x = \gamma_1\beta^y = \gamma_2\beta^{(\sigma)x} = \gamma_3\beta^{(\sigma)y}$ with fixed $\gamma_1, \gamma_2, \gamma_3$. By the multiplicative independence of $\beta, \beta^{(\sigma)}$, there can be at most one such pair (x, y). On the other hand, if $\mathcal{P}$ consists of $\Lambda_1 = \{\beta^x, -\beta^{(\sigma)x}\}$ and $\Lambda_2 = \{-\beta^y, \beta^{(\sigma)y}\}$, then again $x = y = 0$ for $(x, y) \in \mathcal{S}(\mathcal{P})$; and the same holds if $\Lambda_3 = \{\beta^x, \beta^{(\sigma)y}\} \in \mathcal{P}$.

We are left with the case when $\beta, \beta^{(\sigma)}$ are multiplicatively dependent for each σ. Say for some σ we have $\beta^u = \beta^{(\sigma)v}$ with $(u,v) \neq (0,0)$. Extend σ to an element of the Galois group of the normal closure N of $\mathbb{Q}(\beta)$. We obtain $\beta^{u^2} = (\beta^u)^{(\sigma)v} = \beta^{(\sigma^2)v^2}$, then $\beta^{u^3} = \beta^{(\sigma^3)v^3}, \ldots, \beta^{u^E} = \beta^{(\sigma^E)v^E} = \beta^{v^E}$, where $E = \deg N$. Since β is not a root of unity this gives $u^E = v^E$, therefore $u = \pm v$. Introducing the equivalence relation $\approx$ on $\mathbb{C}^\times$ with $\varrho \approx \sigma$ if ϱ/σ is a root of unity, we may conclude that for each σ, either $\beta \approx \beta^{(\sigma)}$ or $\beta \approx 1/\beta^{(\sigma)}$.

Suppose at first that $\beta \approx \beta^{(\sigma)}$ for each σ. Then $\beta^u = \beta^{(2)u} = \ldots = \beta^{(D)u}$ for some $u \in \mathbb{N}$, so that β^u is a rational, and β among its radicals. Otherwise, if $\beta \not\approx \beta^{(\sigma)}$, hence $\beta \approx 1/\beta^{(\sigma)}$ for some σ, it is easily seen that this holds for exactly half of the embeddings σ. So D is even, and after suitable numbering, there is a $u \in \mathbb{N}$ with

$$\beta^u = \beta^{(2)u} = \ldots = \beta^{(D/2)u} = 1/\beta^{((D/2)+1)u} = \ldots = 1/\beta^{(D)u}.$$

Therefore β^u is quadratic with conjugate $1/\beta^u$, so that its norm is 1. And β is among its radicals. ∎

4. An auxiliary lemma. We now begin with the proof of our Theorem. When $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{C}^\times)^n$, define $\boldsymbol{\alpha}^{\mathbf{x}}$ as in Section 2. We will deal with functions

$$F(\mathbf{x}) = \sum_{i=1}^{m} P_i(\mathbf{x}) \boldsymbol{\alpha}_i^{\mathbf{x}} \tag{4.1}$$

with polynomials P_i and distinct elements $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_m$ of $(\mathbb{C}^\times)^n$. Say

$$P_i(\mathbf{x}) = \sum_{j=1}^{e_i} c_{ij} M_{ij}(\mathbf{x}) \quad (i = 1, \ldots, m)$$

where $M_{i1}, \ldots, M_{i,e_i}$ are distinct monomials, and $c_{i1}, \ldots, c_{i,e_i}$ are nonzero. We will write $F^* \prec F$ if F^* is a function like F, with the same $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_m$ and the same monomials M_{ij}, but arbitrary coefficients c^*_{ij} $(1 \leq i \leq m$, $1 \leq j \leq e_i)$, some of which may be zero.

For $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_q) \in \overline{\mathbb{Q}}^q \backslash \{\mathbf{0}\}$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$, write $h(\boldsymbol{\beta})$ for its absolute logarithmic height, as defined, e.g., in [3, §2]. Our former notation $h(\beta)$ then becomes $h(\beta, 1)$. When $\boldsymbol{\beta}_i = (\beta_{i1}, \ldots, \beta_{i,q_i})$ $(i = 1, \ldots, s)$, set $h(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_s) = h(\beta_{11}, \ldots, \beta_{1,q_1}, \ldots, \beta_{s1}, \ldots, \beta_{s,q_s})$. The following is similar to Lemma 3.3 in [3].

LEMMA 4.1. *Suppose $F(\mathbf{x})$ is as above, with the coefficients c_{ij}, and the components of each $\boldsymbol{\alpha}_i$ in $\overline{\mathbb{Q}}^\times$. Set $\mathbf{c}_i = (c_{i1}, \ldots, c_{i,e_i})$ $(i = 1, \ldots, m)$ and $q =$*

$e_1+\ldots+e_m$, and let $d(F)$ be the maximal total degree of the monomials M_{ij}. Let $h_\circ$ be a positive real. Then solutions $\mathbf{x} \in \mathbb{Z}^n$ of

$$F(\mathbf{x}) = 0 \tag{4.2}$$

with $x_1 \ldots x_n \neq 0$,

$$h(\boldsymbol{\alpha}_1^{\mathbf{x}}\mathbf{c}_1, \ldots, \boldsymbol{\alpha}_m^{\mathbf{x}}\mathbf{c}_m) \geq h_\circ|\mathbf{x}| \tag{4.3}$$

and maximum norm $|\mathbf{x}| \geq x_\circ(h_\circ, q, d(F))$ lie in $\leq c(q)$ classes, and solutions in a given class $\mathcal{C}$ satisfy

$$F_{\mathcal{C}}^*(\mathbf{x}) = 0$$

where $F_{\mathcal{C}}^* \prec F$, but $F_{\mathcal{C}}^*$ is not a constant multiple of F.

Proof. The equation (4.2) may be written as

$$\begin{aligned}(c_{11}M_{11}(\mathbf{x}) + \ldots + c_{1,e_1}M_{1,e_1}(\mathbf{x}))\boldsymbol{\alpha}_1^{\mathbf{x}} + \ldots \\ + (c_{m1}M_{m1}(\mathbf{x}) + \ldots + c_{m,e_m}M_{m,e_m}(\mathbf{x}))\boldsymbol{\alpha}_m^{\mathbf{x}} = 0.\end{aligned}$$

Introduce vectors $\mathbf{X}, \mathbf{Y}$ with q components:

$$\begin{aligned}\mathbf{X} &= (c_{11}\boldsymbol{\alpha}_1^{\mathbf{x}}, \ \ldots, c_{1,e_1}\boldsymbol{\alpha}_1^{\mathbf{x}}, \ \ldots, c_{m1}\boldsymbol{\alpha}_m^{\mathbf{x}}, \ \ldots, c_{m,e_m}\boldsymbol{\alpha}_m^{\mathbf{x}}), \\ \mathbf{Y} &= (M_{11}(\mathbf{x}), \ldots, M_{1,e_1}(\mathbf{x}), \ldots, M_{m1}(\mathbf{x}), \ldots, M_{m,e_m}(\mathbf{x})).\end{aligned}$$

Set $\mathbf{Z} = \mathbf{X} * \mathbf{Y} := (X_1Y_1, \ldots, X_qY_q)$. Then (4.2) becomes

$$Z_1 + \ldots + Z_q = 0. \tag{4.4}$$

$\mathbf{X}$ lies in the multiplicative group $\Gamma \subset (\mathbb{C}^\times)^q$ of rank $\leq n+1$ generated by the vectors $(\boldsymbol{\alpha}_1^{\mathbf{x}}, \ldots, \boldsymbol{\alpha}_1^{\mathbf{x}}, \ldots, \boldsymbol{\alpha}_m^{\mathbf{x}}, \ldots, \boldsymbol{\alpha}_m^{\mathbf{x}})$ with $\mathbf{x} \in \mathbb{Z}^n$, and by $(c_{11}, \ldots, c_{1,e_1}, \ldots, c_{m1}, \ldots, c_{m,e_m})$. Now (4.3) becomes

$$h(\mathbf{X}) \geq h_\circ|\mathbf{x}|.$$

On the other hand, $\mathbf{Y} \in \mathbb{Q}^q$, and since the x_i are nonzero, in fact $\mathbf{Y} \in (\mathbb{Q}^\times)^q$ with

$$h(\mathbf{Y}) \leq d(F)\log|\mathbf{x}| + \log q.$$

Therefore

$$h(\mathbf{Y}) \leq (1/4q^2)h(\mathbf{X}) \tag{4.5}$$

provided $|\mathbf{x}|$ is sufficiently large, say $|\mathbf{x}| \geq x_\circ(h_\circ, q, d(F))$. By the Corollary of Lemma 3.1 in [3], solutions $\mathbf{x}$ of (4.4) with (4.5) have $\mathbf{Z} = \mathbf{Z}(\mathbf{x})$ in the union of at most $c(q)$ proper subspaces of the $(q-1)$-dimensional space given by (4.4). In such a subspace $u_1Z_1 + \ldots + u_qZ_q = 0$ where $(u_1, \ldots, u_q)$ is not proportional to $(1, \ldots, 1)$. A subspace corresponds to some $F^* \prec F$ not proportional to F, and any $\mathbf{x}$ with $\mathbf{Z}(\mathbf{x})$ in the subspace has $F^*(\mathbf{x}) = 0$. ∎

5. A proposition which implies our Theorem. We will consider functions $G_r(\mathbf{x})$ in $\mathbf{x} \in \mathbb{Z}^n$ given by

$$G_r(\mathbf{x}) = \sum_{l=1}^{n}(g_{rl1}\alpha_{l1}^{x_l} + \ldots + g_{rlk}\alpha_{lk}^{x_l}) + Q_r(\mathbf{x}) \qquad (r = 1, \ldots, p)$$

with polynomials Q_r, where all the data, i.e., the g_{rli}, α_{li} and the coefficients of the Q_r, are algebraic. We will suppose that each $\alpha_{li} \neq 0$, and that

$$h(\alpha_{l1}) \geq \hbar > 0 \qquad (l = 1, \ldots, n) \tag{5.1}$$

for some constant $\hbar$. The coefficients g_{rli} are not necessarily nonzero, but write N for the number of those which are, and d for the maximal total degree of $Q_1, \ldots, Q_p$.

Proposition 5.1. *Suppose there is a partition of $\{1, \ldots, n\}$ into nonempty sets $S_1, \ldots, S_p$ such that*

$$g_{rl1} \neq 0 \qquad \textit{for } l \in S_r \;\; (r = 1, \ldots, p). \tag{5.2}$$

Then the solutions $\mathbf{x} \in \mathbb{Z}^n$ of the system of equations

$$G_r(\mathbf{x}) = 0 \qquad (r = 1, \ldots, p) \tag{5.3}$$

lie in the union of at most $c_1(\hbar, N, d)$ hyperplanes of the type $x_l =$ const, and $c_2(N, d)$ classes, with elements of a given class having

$$g_{rmj}\alpha_{mj}^{x_m} = \gamma g_{sli}\alpha_{li}^{x_l} \neq 0$$

for some pairs $(m, j) \neq (l, i)$, some r, s, and some constant γ.

Note that the coefficients of the polynomials Q_r are not required to be rational. The proof of the proposition is postponed to the next section. Here we will deduce our Theorem from the case $p = 1$, the general case of the proposition being needed only for its proof.

In view of Theorem 1 of [5] we may assume the α_{li} $(1 \leq l \leq n, 1 \leq i \leq k_l)$ in the definition (1.2), (1.3) of $E(\mathbf{x})$ to be algebraic. It is not hard to see that we also may suppose the a_{li} to be algebraic: this may be done by a specialization argument, or as follows.

Let $\mathbf{A} = (a_{11}, \ldots, a_{1,k_1}, \ldots, a_{n1}, \ldots, a_{n,k_n}) \in \mathbb{C}^N$ be the "coefficient vector" of E. We signify this by writing $E(\mathbf{x}) = E(\mathbf{A}; \mathbf{x})$. We may write

$$\mathbf{A} = \mathbf{A}_1 + \zeta_2\mathbf{A}_2 + \ldots + \zeta_r\mathbf{A}_r$$

where each $\mathbf{A}_i$ is in $\overline{\mathbb{Q}}^N$, and $1, \zeta_2, \ldots, \zeta_r$ are linearly independent over $\overline{\mathbb{Q}}$. Let ξ be algebraic of degree r over the number field generated by the entries of $\mathbf{A}_1, \ldots, \mathbf{A}_r$, and set

$$\widetilde{\mathbf{A}} = \mathbf{A}_1 + \xi\mathbf{A}_2 + \ldots + \xi^{r-1}\mathbf{A}_r.$$

Since P has coefficients in $\mathbb{Q} \subset \overline{\mathbb{Q}}$, the equation (1.1), i.e., $E(\mathbf{A};\mathbf{x}) = P(\mathbf{x})$, is equivalent to the system $E(\mathbf{A}_1;\mathbf{x}) = P(\mathbf{x})$, $E(\mathbf{A}_2;\mathbf{x}) = \ldots = E(\mathbf{A}_r;\mathbf{x}) = 0$, which in turn is equivalent to $E(\widetilde{\mathbf{A}};\mathbf{x}) = P(\mathbf{x})$. Similarly, (1.4$\lambda$), i.e., $\sum_{l\in\lambda} E_l(\mathbf{A};x_l) = 0$, is equivalent to $\sum_{l\in\lambda} E_l(\widetilde{\mathbf{A}};x_l) = 0$. Therefore it will suffice to prove the Theorem for $E(\widetilde{\mathbf{A}};\mathbf{x})$. We may indeed assume the coefficients a_{li} to be algebraic.

For a function of the type (1.2), (1.3), write $n = n(E)$, and $N = N(E)$ with N given by (1.5), and set $d(P)$ for the total degree of a polynomial P. For $n \le N$ let $R_d(N,n)$ be the maximal number of nondegenerate solutions of equation (1.1), over E, P as in the Theorem, with $n(E) \le n$, $N(E) \le N$, $d(P) \le d$, and with algebraic data. The Theorem will follow if we can show that $R_d(1,1) \le 1$, $R_d(N,1) \ll R_d(N-1,1)$ when $N > 1$, and $R_d(N,n) \ll R_d(N-1,n) + R_d(N,n-1)$ when $n > 1$.

A function E given by (1.2), (1.3) will be called *proper* if each α_{li} is algebraic, we have $a_{l1} \ne 1$, and absolute logarithmic heights

$$h(\alpha_{l1}) \ge \mathrm{Dob}(N) \qquad (l = 1,\ldots,n)$$

where $\mathrm{Dob}(N) = 1/(4N(\log^+ N)^3)$ with $\log^+ N = \max(1, \log N)$. By Theorem 2 of [5], there are maps ${}_1T,\ldots,{}_tT$ with $t \le t_0(N)$, say ${}_jT : \mathbb{Z}^{m_j} \to \mathbb{Z}^n$ with $0 \le m_j \le n$, such that every nondegenerate solution $\mathbf{x}$ of (1.6), i.e., of $E(\mathbf{x}) \in \mathbb{Q}$, is of the form

$$\mathbf{x} = {}_jT\mathbf{y} \tag{5.4}$$

for some j and some $\mathbf{y} \in \mathbb{Z}^{m_j}$. Furthermore, for each j with $m_j > 0$ the function ${}_j\widetilde{E}(\mathbf{y}) := E({}_jT\mathbf{y})$ is again of the general type (1.2), (1.3), and is proper.

Observe that for j with $m_j = 0$ there is just one $\mathbf{x}$ coming from (5.4), and these together lead to at most $t_0(N) \ll 1$ solutions. We are therefore reduced to studying equations

$${}_j\widetilde{E}(\mathbf{y}) = P({}_jT\mathbf{y})$$

where $m_j > 0$. The maps ${}_jT$ described in [5] are linear (not necessarily homogeneous) with integer coefficients, so that $P({}_jT\mathbf{y})$ again has rational coefficients. They further have the property that when $\mathbf{x} = {}_jT\mathbf{y}$ is a nondegenerate solution of $E(\mathbf{x}) \in \mathbb{Q}$, then $\mathbf{y}$ is a nondegenerate solution of ${}_j\widetilde{E}(\mathbf{y}) \in \mathbb{Q}$. We thus may restrict ourselves to proper functions $E(\mathbf{x})$.

We now apply the proposition with $\hbar = \mathrm{Dob}(N)$, $p = 1$, $\mathbb{G}_1(\mathbf{x}) = E(\mathbf{x}) - P(\mathbf{x})$. Some of the solutions of (1.1), i.e., of $\mathbb{G}_1(\mathbf{x}) = 0$, lie in the union of $\ll 1$ hyperplanes $x_l = \text{const}$. When $n = 1$, these simply give $\ll 1$ solutions, and when $n > 1$, then $E_l(x_l)$ may be absorbed into the constant in (1.2), so that we get $\ll R_d(N, n-1)$ nondegenerate solutions. The remaining solutions of (1.1) lie in $\ll 1$ classes, with elements of a given class having

$$a_{mj}\alpha_{mj}^{x_m} = \gamma a_{li}\alpha_{li}^{x_l} \tag{5.5}$$

for some $(l,i) \neq (m,j)$ and some γ. There clearly can be no such class unless $N > 1$.

When $m = l$, the summands $a_{li}\alpha_{li}^{x_l}$ and $a_{lj}\alpha_{lj}^{x_l}$ in (1.3) can be combined to $(1+\gamma)a_{li}\alpha_{li}^{x_l}$, so that k_l can be reduced, or we even have $E_l(x_l) = 0$, so that $\mathbf{x}$ is degenerate. Thus the number of nondegenerate solutions in our class is at most $R_d(N-1,n)$. Or, when $n > 1$, we may also have $m \neq l$ in (5.5). For $\mathbf{x}, \mathbf{x}'$ in the same class, (5.5) yields $\alpha_{mj}^{x_m - x'_m} = \alpha_{li}^{x_l - x'_l}$, and since α_{mj}, α_{li} are not roots of unity, this either determines x_l, x_m uniquely, or $x_l = uz + x'_l$, $x_m = wz + x'_m$ with fixed nonzero u, w, and $z \in \mathbb{Z}$. Substitution into $E(\mathbf{x}) - P(\mathbf{x})$ gives a function in at most $n-1$ variables, so that the number of nondegenerate solutions in our class is $\leq R_d(N, n-1)$. ■

6. Proof of Proposition 5.1. Order the monomials in $\mathbf{x}$ as $M_1 = 1$, $M_2, M_3, \ldots$ such that the total degrees do not decrease. When Q is a nonzero polynomial, write $\varrho(Q)$ for the maximum number ϱ such that M_ϱ occurs in Q with nonzero coefficient. Call Q *normalized* if this coefficient is 1. Set $\varrho(Q) = 0$ when $Q = 0$.

We will do downward induction from $p = n$ to $n-1, n-2, \ldots, 1$. Given a function

$$G(\mathbf{x}) = \sum_{l=1}^{n} (g_{l1}\alpha_{l1}^{x_l} + \ldots + g_{lk}\alpha_{lk}^{x_l}) + Q(\mathbf{x})$$

with the $\alpha_{li} \neq 0$ and Q a polynomial, write $N(G)$ for the number of nonzero coefficients g_{li}. Now set

$$N = \sum_{r=1}^{p} N(G_r), \quad \varrho = \sum_{r=1}^{p} \varrho(Q_r), \quad \mu = N + \varrho.$$

Given p, Proposition 5.1 will be proved by induction on μ. Observe that $n \leq N \leq \mu$.

Case A: *Some* $Q_r = 0$, *say* $Q_1 = 0$. We will then deal with the equation $G_1(\mathbf{x}) = 0$ of purely exponential type. For a partition $\mathcal{P}$ of the set of nonzero summands of G_1 (this set is nonempty by the hypothesis), we have $\mathcal{S}(\mathcal{P}) = \emptyset$ if $\mathcal{P}$ contains a singleton, i.e., a one-element set. We thus may suppose that for some set $\Lambda \in \mathcal{P}$, two summands $g_{1li}\alpha_{li}^{x_l}$ and $g_{1mj}\alpha_{mj}^{x_m}$ with $(l,i) \neq (m,j)$ and nonzero g_{1li}, g_{1mj} belong to Λ. Invoking [1] we see that solutions in $\mathcal{S}(\Lambda)$ fall into $\ll 1$ classes, and $g_{1mj}\alpha_{mj}^{x_m} = \gamma g_{1li}\alpha_{li}^{x_l}$ with fixed γ for solutions $\mathbf{x}$ in a given class.

Case B: *Each* $Q_r \neq 0$. After multiplying the G_r's ($r = 1, \ldots, p$) by suitable constants we may assume each Q_r to be normalized.

Suppose $l \in S_r$, so that (5.2) holds. Since $h(\alpha_{l1}) \geq \hbar$ by (5.1), there is, e.g., by Lemma 6 of [5], an integer u_l such that

$$h(g_{rl1}\alpha_{l1}^{x_l-u_l}) \geq \frac{1}{4}\, h(\alpha_{l1})|x_l| \geq \frac{1}{4}\,\hbar|x_l|$$

for $x_l \in \mathbb{Z}$. Therefore $h(g_{rl1}\alpha_{l1}^{x_l}) \geq \frac{1}{4}\hbar|x_l+u_l| = h_\circ|x_l+u_l|$ with

$$h_\circ = \frac{1}{4}\,\hbar.$$

Setting $\widehat{g}_{rli} = g_{rli}\alpha_{li}^{-u_l}$, $\widehat{x}_l = x_l + u_l$ we have $g_{rli}\alpha_{li}^{x_l} = \widehat{g}_{rli}\alpha_{li}^{\widehat{x}_l}$ $(i = 1, \ldots, k)$ and

$$h(\widehat{g}_{rl1}\alpha_{l1}^{\widehat{x}_l}) \geq h_\circ|\widehat{x}_l|$$

for any $x_l \in \mathbb{Z}$. We may express the functions $G_1, \ldots, G_p$ in terms of $\widehat{x}_l$ instead of x_l. We carry this out for each $l \in S_r$, and then for each r, $1 \leq r \leq p$. These substitutions will not affect the numbers $N(G_r)$, $\varrho(Q_r)$, hence not N, ϱ or μ. Each Q_r will still be normalized. Also, the truth of the desired conclusion of the proposition will not be affected. We therefore may suppose after suitable substitutions that

$$h(g_{rl1}\alpha_{l1}^{x_l}) \geq h_\circ|x_l| \quad (1 \leq r \leq p,\, l \in S_r). \tag{6.1}$$

When dealing with systems of equations (5.3) with given p and μ which satisfy (6.1), and with normalized nonzero polynomials Q_r, we will do induction on $\sigma = \sum_{r=1}^{p} \sigma(Q_r)$, where $\sigma(Q)$ denotes the number of nonzero coefficients of a polynomial Q. We thus will have another layer of induction.

Without loss of generality we may restrict our attention to solutions $\mathbf{x}$ of (5.3) with

$$|\mathbf{x}| = |x_1|.$$

But $1 \in S_r$ for some r, and $1 \in S_1$ without loss of generality. Now (6.1) yields $h(g_{111}\alpha_{11}^{x_1}) \geq h_\circ|x_1| = h_\circ|\mathbf{x}|$, which is $h(g_{111}\alpha_{11}^{x_1}, 1) \geq h_\circ|\mathbf{x}|$ in other notation. In view of this, and since Q_1, being normalized, has some coefficient 1, the vector whose components are the $g_{1li}\alpha_{li}^{x_l}$ and the coefficients of Q_1, has height $\geq h_\circ|\mathbf{x}|$. Thus (4.3) holds, and Lemma 4.1 applies. Some solutions of $G_1(\mathbf{x}) = 0$ may lie on a hyperplane $x_l = 0$ for some l. Next, there may be solutions with $|\mathbf{x}| < x_\circ(h_\circ, q, d(Q_1))$. In the present situation $q = N(G_1) + \sigma(Q_1)$ is bounded in terms of N, d, n, where $n \leq N$, so that such solutions certainly lie in not more than $c_3(\hbar, N, d)$ hyperplanes $x_1 = \text{const}$. In view of Lemma 4.1, the remaining solutions fall into at most $c(q) \leq c_4(N, d)$ classes.

Solutions in a given class $\mathcal{C}$ have $G^*_{\mathcal{C}}(\mathbf{x}) = 0$, hence

$$G_1(\mathbf{x}) = G^*_{\mathcal{C}}(\mathbf{x}) = 0$$

where $G^*_{\mathcal{C}} \prec G_1$, but is not proportional to G_1. Say

$$G^*_{\mathcal{C}} = \sum_{l=1}^{n} (g^*_{l1}\alpha_{l1}^{x_l} + \ldots + g^*_{lk}\alpha_{lk}^{x_l}) + Q^*(\mathbf{x}).$$

(An analogous notation will be used for functions G^{**}, G°, G', G'' introduced below.) We will need the matrix $\mathcal{M}$ with the $|S_1|$ columns

$$\begin{pmatrix} g_{1l1} \\ g^*_{l1} \end{pmatrix} \quad (l \in S_1).$$

Subcase B1: $\mathcal{M}$ *has rank* 1. Then in the pencil of $G_1, G^*_{\mathcal{C}}$ there is a nonzero G^{**} with $g^{**}_{l1} = 0$ for each $l \in S_1$. Suppose first that $\varrho(Q^{**}) = \varrho(Q_1)$, so that M_ϱ with $\varrho = \varrho(Q_1)$ occurs in Q^{**} with a coefficient $\theta \neq 0$. Then $G^\circ = G_1 - \theta^{-1} G^{**}$ has

$$g^\circ_{l1} = g_{1l1} \neq 0 \quad (l \in S_1) \tag{6.2}$$

and $\varrho(Q^\circ) < \varrho(Q_1)$. We now replace $G_1, G_2, \ldots, G_p$ by $G^\circ, G_2, \ldots, G_p$, thus replacing ϱ by a smaller number. Then also μ is diminished. Since (5.2) still holds with g°_{l1} in place of g_{1l1}, induction on μ may be applied. Now suppose that $\varrho(Q^{**}) < \varrho(Q_1)$. Then after subtracting a suitable multiple of G^{**} from G_1, we obtain a function G° which again has (6.2), where M_ϱ with $\varrho = \varrho(Q_1)$ appears in Q° with coefficient 1, but where there are fewer summands, i.e., $N(G^\circ) < N(G_1)$ or $\sigma(Q^\circ) < \sigma(Q_1)$. Again we replace $G_1, G_2, \ldots, G_p$ by $G^\circ, G_2, \ldots, G_p$. When $N(G^\circ) < N(G_1)$, then N and hence μ is diminished, and again induction on μ applies. When $N(G^\circ) = N(G_1)$, then μ remains unchanged. But Q° is normalized, and (6.1) is true with g°_{l1} in place of g_{1l1}. Since $\sigma(Q^\circ) < \sigma(Q_1)$, induction on σ finishes the argument.

Subcase B2: $\mathcal{M}$ *has rank* 2. (This can only happen when $|S_1| \geq 2$, so that $p < n$.) In this case there is a G^{**} in the pencil of $G_1, G^*_{\mathcal{C}}$ with $g^{**}_{111} = 0$, but $g^{**}_{1l1} \neq 0$ for some $l \in S_1$. Set

$$S' = \{l \in S_1 \text{ with } g^{**}_{1l1} = 0\},$$
$$S'' = S_1 \backslash S'_1 = \{l \in S_1 \text{ with } g^{**}_{1l1} \neq 0\}.$$

Then $S_1 = S' \cup S''$ is a partition into two nonempty sets. Setting $G' = G_1$, $G'' = G^{**}$ we have

$$g'_{l1} \neq 0 \quad \text{for } l \in S', \qquad g''_{l1} \neq 0 \quad \text{for } l \in S''.$$

Now $\mathbf{x}$ is a common zero of the system

$$G'(\mathbf{x}) = G''(\mathbf{x}) = G_2(\mathbf{x}) = \ldots = G_p(\mathbf{x}) = 0.$$

Since $S' \cup S'' \cup S_2 \cup \ldots \cup S_p$ is a partition of $\{1, \ldots, n\}$, we may invoke the case $p + 1$ of the proposition. ∎

References

[1] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. 155 (2002), 807–836.

[2] M. Laurent, *Équations exponentielles polynômes et suites récurrentes linéaires*, Astérisque 147–148 (1987), 121–139, 343–344.

[3] H. P. Schlickewei, W. M. Schmidt and M. Waldschmidt, *Zeros of linear recurrence sequences*, Manuscripta Math. 98 (1999), 225–241.

[4] W. M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. 182 (1999), 245–282.

[5] —, *Rationality of exponential functions at integer arguments*, J. Number Theory, to appear.

Department of Mathematics
University of Colorado
Boulder, CO 80309-0395, U.S.A.
E-mail: schmidt@euclid.colorado.edu

Received on 4.9.2003 (4612)