PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 3, March 1999, Pages 665–675
S 0002-9939(99)04728-0

COUNTING THE VALUES TAKEN BY ALGEBRAIC EXPONENTIAL POLYNOMIALS

G. R. EVEREST AND I. E. SHPARLINSKI

(Communicated by David E. Rohrlich)

Abstract. We prove an effective mean-value theorem for the values of a non-degenerate, algebraic exponential polynomial in several variables. These objects generalise simultaneously the fundamental examples of linear recurrence sequences and sums of S-units. The proof is based on an effective, uniform estimate for the deviation of the exponential polynomial from its expected value. This estimate is also used to obtain a non-effective asymptotic formula counting the norms of these values below a fixed bound.

1. Introduction and main results

Let $\mathbb{K}$ denote a finite extension field of the rational field $\mathbb{Q}$ with degree denoted $d = [\mathbb{K} : \mathbb{Q}]$, and let $O_{\mathbb{K}}$ denote the ring of algebraic integers of $\mathbb{K}$. Let $E(\underline{x})$ denote an *algebraic exponential polynomial* in the variable $\underline{x} = (x_1, \dots, x_r)$. This is an expression of the form

$$E(\underline{x}) = \sum_{i=1}^{m} A_i(\underline{x}) \lambda_{i1}^{x_1} \dots \lambda_{ir}^{x_r}, \tag{1}$$

where $A_i(\underline{x}) \in O_{\mathbb{K}}[x_1, \dots, x_r]$, $\lambda_{ij} \in O_{\mathbb{K}}$ for $1 \le i \le m, 1 \le j \le r$.

For each $\underline{x} \in \mathbb{N}^r$, we define

$$|E_{max}(\underline{x})| = \max_i \{|\lambda_{i1}^{x_1} \dots \lambda_{ir}^{x_r}|\}.$$

We suppose throughout that $E(\underline{x})$ is *non-degenerate* in the following sense. That is, for each distinct pair of indices k and l, the numbers $\lambda_{k1}/\lambda_{l1}, \dots, \lambda_{kr}/\lambda_{lr}$ are multiplicatively independent. If $r = 1$, we may write $x = x_1$. Then (1) takes the simpler form

$$E(x) = \sum_{i=1}^{m} A_i(x) \lambda^x. \tag{2}$$

It can easily be shown that $E(x)$ represents the x-th term of an algebraic linear recurrence sequence. Conversely, if $E(x)$ denotes the x-th term of an algebraic linear recurrence sequence, then it can be shown that $E(x)$ is given by an explicit formula of the kind in (2). In this case, if the sequence has order M and the degree of $A_i(x)$ is denoted $n_i - 1$, then $\sum_i n_i = M$. The non-degeneracy condition given

Received by the editors June 20, 1997.
1991 *Mathematics Subject Classification.* Primary 11B83.

©1999 American Mathematical Society

above reduces, in the case where $r = 1$, to the usual notion of non-degeneracy for these sequences.

Considerable interest has been shown in the arithmetic of these exponential polynomials in the case when $r = 1$, see [3], [7], [8], [9], [11], [12], [13]. Often, quite simply stated questions have turned out to be particularly intractable by elementary methods. We give an example. It looks obvious that $E(x)$ should grow like its largest term. Say we order the 'roots'; thus $|\lambda_1| \geq |\lambda_2| \geq \ldots \geq |\lambda_r|$. We would expect the following to hold for all sufficiently large $x \in \mathbb{N}$, $|E(x)| \geq C_0|\lambda_1|^x$. This is obviously true if $|\lambda_1| > |\lambda_2|$. But suppose several roots tie for first place in absolute value?

The general result was only obtained in [4], independently in [6], and at the expense of an extremely profound theorem from diophantine approximation. In the course of matters, it turned out to be easier to work with a massive generalisation of a recurrence sequence, namely, a sum of S-units. Here, S denotes a finite set of valuations of $\mathbb{K}$, containing the archimedean valuations. Let U_S denote the group of S-units of $\mathbb{K}$. In [4], Evertse studied a linear form

$$a_0 + a_1u_1 + \cdots + a_mu_m, \tag{3}$$

where $u_i \in U_S, a_i \in \mathbb{K}^*, i = 1, \ldots, m$. To obtain the result we just alluded to, he had to work with a linear form with the u_i all belonging to a subset of $\mathbb{K}^*$ whose norms were constrained to grow no faster than a small positive power of their heights. This appears to be the minimally general level at which to work in order to obtain smoothly the growth rate for recurrence sequences. A by-product of working at this level of generality is that the multivariable version of the growth result comes free of charge.

This would already justify the further study of the behaviour of linear forms such as those he considered. Further impetus is provided by the fact that sums of S-units occur naturally in many places in the theory of diophantine equations. They occur naturally in other areas also; see [10] for a fascinating application in measurable dynamics. We note that an algebraic exponential polynomial of the kind in (1) arises as a special case of the objects studied by Evertse. Some strong results are known about the growth rate of these general sequences. However, most of the general results are non-effective. The exceptions arise in small numbers of variables or where a few terms dominate the rest. In such cases, it is usual for Baker's Theorem to be applicable, and this is effective.

Evertse's theorem used a hard result, known as the Subspace Theorem, proved by Schmidt. This was proved initially only in the archimedean valuation. Schlickewei subsequently generalised this, enabling one to consider also a finite number of non-archimedean valuations. More recently, many of the results obtained for sums of S-units have been improved using a deeper version of the Subspace Theorem known as the Quantitative Subspace Theorem. Using these powerful techniques, one can show that the number of solutions of equations such as the S-unit equation is bounded in a way which depends very minimally upon the starting parameters. See the recent papers [8], [9] and Schmidt's excellent book [11] for details and further references.

In this paper we are going to show how an effective result on the deviation of $|E(\underline{x})|$ from its expected value, coupled with the recent advances in [8], [9], can be applied to obtain effective mean value results for the non-zero values of $E(\underline{x})$. Although it would require some effort to make our results explicit, nonetheless, general effective results for sequences of this kind are most welcome, especially since we seem to be miles away from proving effective results for their growth rates. With current techniques we would require, at the very least, an effective form of Roth's Theorem which is something we prefer not to hold our breath for.

We say that an exponential polynomial $E(\underline{x})$ given by (1) has *constant coefficients* if its polynomial coefficients $A_i(\underline{x})$ are constants $i = 1, \ldots, m$.

Theorem 1. *For a non-degenerate exponential polynomial $E(\underline{x})$ given by (1) and any postive integer N, there is an effective asymptotic formula as $N \to \infty$:*

$$\frac{1}{N^r} \sum_{x_1=1}^{N} \cdots \sum_{x_r=1}^{N} \log |E(\underline{x})| = CN + O\left(N^{1-\tau} \log^{\tau} N\right), \tag{4}$$

where

$$\tau = \begin{cases} 1 - 1/(r+1), & \textit{if } E(\underline{x}) \textit{ has constant coefficients;} \\ 1/2, & \textit{otherwise.} \end{cases}$$

Notes. (i) The set $L = \{L_i(\underline{x}) = x_1 \log |\lambda_{i1}| + \ldots + x_r \log |\lambda_{ir}|\}$ is a collection of real linear forms; let $|\underline{x}|_L$ denote $\max_i\{L_i(\underline{x})\}$. The constant C in (4) denotes the Riemann integral of the function $|\cdot|_L$ over the unit cube $[0,1]^r$. As a limit, this is

$$\lim_{N\to\infty} \frac{1}{N^{r+1}} \sum_{x_1=1}^{N} \cdots \sum_{x_r=1}^{N} |\underline{x}|_L = \lim_{N\to\infty} \frac{1}{N^r} \sum_{x_1=1}^{N} \cdots \sum_{x_r=1}^{N} |\underline{x}/N|_L. \tag{5}$$

Notice how (5) exploits the linearity property of $|\cdot|_L$, namely $|\rho\underline{x}|_L = \rho|\underline{x}|_L$, for all ρ in $\mathbb{R}_+$.

(ii) For the non-archimedean analogue of formula (4), consult [7] if $r = 1$ and [2] for the general case. The differences are that the leading term in (4) is constant, equal to the local integral of the valuation of the exponential polynomial. Also, remarkably, the error term is not bounded effectively. It is rather unusual in number theory for the archimedean version of a result to be better than its non-archimedean counterpart.

(iii) Theorem 1 (and Lemma 2 below) generalise readily to the S-integral situation. Let S denote any finite set of valuations of $\mathbb{K}$, including the archimedean valuations. Suppose we insisted only that the λ_{ij} and the coefficients of the $A_i(\underline{x})$ be S-integers. Then Theorem 1 holds with $|E(\underline{x})|_v$ replacing $|E(\underline{x})|$, where v denotes any valuation of S and $|\cdot|_v$ denotes the corresponding absolute value.

Theorem 2. *Suppose $E(\underline{x})$ is a non-degenerate exponential polynomial given by (1). Let $N_{\mathbb{K}|\mathbb{Q}} : \mathbb{K} \to \mathbb{Q}$ denote the usual field norm. Let $q > 0$ denote a real parameter, to be thought of as large. Then there is an ineffective asymptotic formula as follows:*

$$N_E(q) = \#\{\underline{x} \in \mathbb{N}^r : |N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))| < q\} = D(\log q)^r + O\left((\log q)^{r-\tau}\right), \tag{6}$$

where

$$\tau = \begin{cases} 1 - 1/(r+1), & \textit{if } E(\underline{x}) \textit{ has constant coefficients;} \\ 1/2, & \textit{otherwise.} \end{cases}$$

Notes. (i) In formula (6), the constant D arises as a volume in the following way. Let $\sigma_l : \mathbb{K} \to \mathbb{C}, \quad l = 1, \ldots, d$, denote the distinct embeddings of $\mathbb{K}$ into the complex numbers. Let $\mathcal{L}$ denote the set of linear forms

$$\{L_{il}(\underline{x}) = x_1 \log |\sigma_l(\lambda_{i1})| + \ldots + x_r \log |\sigma_l(\lambda_{ir})|\}_{1\le i\le m, 1\le l\le d}.$$

Write $|\underline{x}|_{\mathcal{L}} = \max_{i,l}\{L_{il}(\underline{x})\}$. Then D denotes the volume of the fundamental domain $\mathcal{D} = \{\mathbb{R}_+^r : |\underline{x}|_{\mathcal{L}} \le 1\}$.

(ii) We encountered a similar situation in [1], where we obtained a very accurate formula counting the values of the S-norm of a general sum of S-units. Let $\underline{a}\cdot\underline{u} = a_0 + a_1u_1 + \ldots + a_mu_m$, where u_i lie in the group of S-units of a number field $\mathbb{K}$ and $a_i \in \mathbb{K}^*$. Letting N_S denote the S-norm, we derived a formula of the following shape:

$$(7) \qquad \#\{\underline{u} : N_S(\underline{a}\cdot\underline{u}) < q\} = \psi_1(\log q)^N + \psi_2(\log q)^{N-1} + o((\log q)^{N-1}),$$

counting the number of vectors $\underline{u} = (u_1, \ldots, u_m)$ of S-units with $N_S(\underline{a}\cdot\underline{u}) < q$. In (7), N denotes ms, where s is the torsion-free rank of the group of S-units. Now a remark applies which is similar to (iii) following Theorem 1. Assuming $E(\underline{x})$ is a non-degenerate algebraic exponential polynomial, we are able to prove the following asymptotic formula:

$$N_{E,S}(q) = \#\{\underline{x} \in \mathbb{N}^r : N_S(E(\underline{x})) < q\} = D_S(\log q)^r + O\left((\log q)^{r-1+1/(r+1)}\right).$$

Although this formula is not as accurate as the one in (7), it does apply to a much larger class of objects.

(iii) We could (and we will at the beginning of the proof of Theorem 2) have obtained the formula (6) with an error term of $o((\log q)^r)$ simply by applying the standard results from [4] about the growth rate of $|N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))|$. The application of Lemma 2 below gives a fairly substantial improvement of the error term. Unfortunately no effective formula can be given at the moment. The only prospect of this seems to lie with an effective lower bound for $|N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))|$.

2. Auxiliary results

The theorem in [8] implies the following statement.

Lemma 1. *Suppose $E(\underline{x})$ is a non-degenerate exponential polynomial given by (1). Then for any $H \ge 1$ the number T of solutions of the equation*

$$E(\underline{x}) = 0, \qquad 0 \le x_1, \ldots, x_r \le H,$$

is at most

$$T = \begin{cases} O(1), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(H^{r-1}), & \text{otherwise,} \end{cases}$$

where the implied constants depend on d, m, r, the maximal total degree D of the $A_i(\underline{x})$ and the number of prime divisors ω of the fractional ideals (λ_{ij}), $i = 1, \ldots, m$, $j = 1, \ldots, r$.

Proof. We use induction with respect to the number of terms m of the exponential polynomial $E(\underline{x})$. For $m = 1$ the only contribution to the number of zeros comes from a polynomial equation

$$A_1(x_1, \ldots x_r) = 0, \qquad 0 \le x_1, \ldots, x_r \le H.$$

Obviously this equation has at most $O(1)$ solutions if $E(\underline{x})$ has constant coefficients and $O(H^{r-1})$ solutions otherwise.

The induction is provided by the theorem in [8] which implies that all except maybe $O(1)$ solutions of the equation of the lemma satisfy an equation of the form

$$\sum_{i\in\mathcal{I}} A_i(\underline{x})\lambda_{i1}^{x_1}\dots\lambda_{ir}^{x_r} = 0,$$

where $\mathcal{I}$ is a proper subset of the set $\{1,\dots,m\}$. Applying the induction assumption to each of 2^m-1 such subsets we obtain the required estimate. $\square$

We thank H. P. Schlickewei and W. M. Schmidt for the information about their recent work [9] where the dependence on the number of prime ideals is eliminated. However, even this much stronger result still does not allow us to avoid the dependency on λ_{ij} in constants in our paper.

The following statement is an archimedean analogue of Lemma 4 of [13].

Lemma 2. *Let $N_1,\dots,N_r,H$ denote non-negative integers, with $|\underline{N}| = \max_i\{N_i\}$ for $\underline{N} = (N_1,\dots,N_r)$. There are effectively computable constants C_1,C_2,C_3, independent of $\underline{N}$ and H with the following property:*

$$\#\{0\le y_i < H : |E(\underline{N}+\underline{y})| < |E_{max}(\underline{N})|e^{-C_1H-C_2\log|\underline{N}|}\}$$

$$\le \begin{cases} C_3, & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ C_3H^{r-1}, & \text{otherwise.}\end{cases} \tag{8}$$

Proof. It will be easier to re-write the definition of $E(\underline{x})$ as a sum of monomials of the form

$$m(\underline{x})\underline{\lambda}^{\underline{x}} = x_1^{n_1}\dots x_r^{n_r}\lambda_1^{x_1}\dots\lambda_r^{x_r}. \tag{9}$$

With this notation, write $E(\underline{x})$ in the following way:

$$E(\underline{x}) = \sum_{i=1}^{M} A_i m_i(\underline{x})\underline{\lambda}_i^{\underline{x}}. \tag{10}$$

In (10), the coefficients A_i are non-zero algebraic integers, $A_i\in O_{\mathbb{K}}$.

By Lemma 1, we see that there is some number

$$T = \begin{cases} O(1), & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ O(H^{r-1}), & \text{otherwise,}\end{cases}$$

such that any other non-zero exponential polynomial

$$F(\underline{x}) = \sum_{i=1}^{M} B_i m_i(\underline{x})\underline{\lambda}_i^{\underline{x}}, \qquad B_i\in O_{\mathbb{K}}, \tag{11}$$

has at most T zeros. The constants implicit in the definition of T depend upon the exponential polynomial E only.

Suppose it is possible to find $Q = T+1$ integer vectors $\underline{x}_i = \underline{N}+\underline{y}_i$, $\underline{y}_i = (y_{i1},\dots,y_{ir})$, $i = 1,\dots,Q$, in the range $0\le y_{ij} < H$, $i=1,\dots,Q$, $j = 1,\dots,r$, which satisfy the property within the brackets in (8). Denote $Y = \{\underline{y}_1,\dots,\underline{y}_Q\}$.

Now we construct a sequence $\underline{z}_1,\dots,\underline{z}_M$ recursively. On the first step, we select an arbitrary $\underline{z}_1\in Y$ with $m_1(N+\underline{z}_1)\underline{\lambda}_1^{\underline{z}_1}\ne 0$. This choice is possible because the last equation is an equation with a non-zero exponential polynomial of the shape (11) and $|Y| > T$.

Assume that $\underline{z}_1, \dots, \underline{z}_k \in Y$, $k < M$, are already selected in such a way that

$$\det \begin{pmatrix} m_1(\underline{N}+\underline{z}_1)\underline{\lambda}_1^{\underline{z}_1} & \dots & m_k(\underline{N}+\underline{z}_1)\underline{\lambda}_k^{\underline{z}_1} \\ \dots & \dots & \dots \\ m_1(\underline{N}+\underline{z}_k)\underline{\lambda}_1^{\underline{z}_k} & \dots & m_k(\underline{N}+\underline{z}_k)\underline{\lambda}_k^{\underline{z}_k} \end{pmatrix} \neq 0.$$

We select $\underline{z}_{k+1} \in Y$ such that

$$\det \begin{pmatrix} m_1(\underline{N}+\underline{z}_1)\underline{\lambda}_1^{\underline{z}_1} & \dots & m_{k+1}(\underline{N}+\underline{z}_1)\underline{\lambda}_{k+1}^{\underline{z}_1} \\ \dots & \dots & \dots \\ m_1(\underline{N}+\underline{z}_k)\underline{\lambda}_1^{\underline{z}_k} & \dots & m_{k+1}(\underline{N}+\underline{z}_k)\underline{\lambda}_{k+1}^{\underline{z}_k} \\ m_1(\underline{N}+\underline{z}_{k+1})\underline{\lambda}_1^{\underline{z}_{k+1}} & \dots & m_{k+1}(\underline{N}+\underline{z}_{k+1})\underline{\lambda}_{k+1}^{\underline{z}_{k+1}} \end{pmatrix} \neq 0.$$

This is possible because of the choice of $\underline{z}_1, \dots, \underline{z}_k$; the last determinant is a non-zero exponential polynomial of the shape (11) and $|Y| > T$.

Finally we obtain,

(12)
$$\begin{pmatrix} m_1(\underline{N}+\underline{y}_1)\underline{\lambda}_1^{\underline{y}_1} & \dots & m_M(\underline{N}+\underline{y}_1)\underline{\lambda}_M^{\underline{y}_1} \\ \dots & \dots & \dots \\ m_1(\underline{N}+\underline{y}_M)\underline{\lambda}_1^{\underline{y}_M} & \dots. & m_M(\underline{N}+\underline{y}_M)\underline{\lambda}_M^{\underline{y}_M} \end{pmatrix} \begin{pmatrix} A_1\underline{\lambda}_1^{\underline{N}} \\ \dots \\ A_M\underline{\lambda}_M^{\underline{N}} \end{pmatrix} = \begin{pmatrix} E(\underline{N}+\underline{y}_1) \\ \dots \\ E(\underline{N}+\underline{y}_M) \end{pmatrix},$$

where

$$\Delta = \det \begin{pmatrix} m_1(\underline{N}+\underline{y}_1)\underline{\lambda}_1^{\underline{y}_1} & \dots & m_M(\underline{N}+\underline{y}_1)\underline{\lambda}_M^{\underline{y}_1} \\ \dots & \dots & \dots \\ m_1(\underline{N}+\underline{y}_M)\underline{\lambda}_1^{\underline{y}_M} & \dots & m_M(\underline{N}+\underline{y}_M)\underline{\lambda}_M^{\underline{y}_M} \end{pmatrix} \neq 0.$$

Noticing that all algebraic conjugates (over $\mathbb{K}$) of Δ do not exceed $e^{C_4H+C_5\log|\underline{N}|}$, we obtain

$$\Delta \geq e^{-C_4dH-C_5d\log|\underline{N}|}.$$

Applying Cramer's Rule we see that for the vector $(E(\underline{N}+\underline{z}_i))_{1\leq i\leq M}$ the largest entry is bounded below by a quantity of the shape $|E_{max}(\underline{N})|e^{-C_6H-C_7\log|\underline{N}|}$. This contradicts our starting assumption by violating the inequality satisfied by $|E_{max}(\underline{N})|$. This completes the proof of the lemma. □

For the proof of Theorem 2 we need the following (perhaps well-known) statement.

Lemma 3. *Let $Q > 0$ denote a large real parameter. Then*

(13) $$\#\{\underline{x} \in \mathbb{N}^r : |\underline{x}|_L \leq Q\} = DQ^r + O(Q^{r-1}).$$

Proof. This is a standard fact from the geometry of numbers; $|\underline{x}|_L$ represents the largest of a finite collection of linear forms with positive coefficients. We could just apply the result on p. 128 of [5]. The condition of Lipschitz-parametrizability follows because the faces of the domain are defined by linear forms. Note that the constant D is the volume of the fundamental domain $\mathcal{D} = \{\underline{x} \in \mathbb{R}_+^r : |\underline{x}|_L \leq 1\}$. □

3. Proofs of the main results

This section starts with a proof of Theorem 1.

Proof of Theorem 1. Let H denote a positive integer. We are going to prove the following effective asymptotic formula,

$$\frac{1}{N^r}\sum_{x_1=1}^{N}\cdots\sum_{x_r=1}^{N}\log|E(\underline{x})| = CN + O\left(H\log N + NH^{-\rho}\right), \tag{14}$$

where

$$\rho = \begin{cases} r, & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ 1, & \text{otherwise.} \end{cases}$$

Clearly, Theorem 1 (formula (4)) follows by taking

$$H = \begin{cases} [N^{1/(r+1)}\log^{-1/(r+1)} N], & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ [N^{1/2}\log^{-1/2} N], & \text{otherwise.} \end{cases}$$

The proof of formula (14) comes by breaking the summatory range in each variable into intervals of length H. In each interval, we may use Lemma 2 to replace $|E(\underline{x})|$ by its value at an endpoint together with an error term of size $O(H\log N)$, with a number of exceptional values of $\underline{x}$ which is bounded as in (8). For each i with $1 \le i \le r$, write $x_i = a_iH + b_i$ and $\underline{x} = \underline{a}H + \underline{b}$. Fixing $\underline{a}$ for the moment, consider the sum

$$\sum_{b_1=1}^{H}\cdots\sum_{b_r=1}^{H}\log|E(\underline{a}H + \underline{b})|. \tag{15}$$

By Lemma 2, this is

$$\begin{aligned} &\sum_{b_1=1}^{H}\cdots\sum_{b_r=1}^{H}(\log|E_{max}(\underline{a}H)| + O(H\log N)) \\ &\quad + \begin{cases} O(N), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(NH^{r-1}), & \text{otherwise.} \end{cases} \end{aligned} \tag{16}$$

The last part of this formula comes from the exceptional points in Lemma 2. For these, we can only estimate $\log|E(\underline{a}H + \underline{b})|$ by $O(N)$. Thus the formula in (16) simplifies to

$$\begin{aligned} &H^{r+1}\log|E_{max}(\underline{a})| + O(H^{r+1}\log N) \\ &\quad + \begin{cases} O(N), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(NH^{r-1}), & \text{otherwise.} \end{cases} \end{aligned} \tag{17}$$

We may write $|E_{max}(\underline{x})| = e^{|\underline{x}|_L}$. Then (17) becomes

$$H^{r+1}|\underline{a}|_L + O(H^{r+1}\log N) + \begin{cases} O(N), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(NH^{r-1}), & \text{otherwise.} \end{cases} \tag{18}$$

Fix a j such that $|\underline{x}|_L = L_j(\underline{x})$. This equation defines a region in $\mathbb{R}_+^r$ which we denote by C_j. Now C_j is a cone and summing the values $L_j(\underline{a})$ for $\underline{a} \in \mathbb{N}^r \cap C_j$ is a straightforward matter. The integers in question are bounded as follows, $|\underline{a}| \le$

$N/H + O(1)$. Therefore, summing the expressions in (18) gives a formula of the shape

$$CN^{r+1} + O\left(N^r H \log N\right) + \begin{cases} O(N^{r+1}H^{-r}), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(N^{r+1}H^{-1}), & \text{otherwise.} \end{cases}$$

Dividing through by N^r gives the formula claimed in (14). $\square$

Proof of Theorem 2. Let H denote a positive integer with $H \geq \log\log q$. We will prove the following asymptotic formula:

$$N_E(q) = D(\log q)^r + \begin{cases} O(H(\log q)^{r-1} + H^{-r}(\log q)^r), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(H(\log q)^{r-1} + H^{-1}(\log q)^r), & \text{otherwise.} \end{cases} \tag{19}$$

This clearly implies Theorem 2 (formula (6)) by taking $H^{r+1} = \log q$ if $E(\underline{x})$ has constant coefficients and $H^2 = \log q$ otherwise.

Initially, we will suppose that $\mathbb{K} = \mathbb{Q}$. Recall the definition of $|\cdot|_L$ from Note (i) following Theorem 1. The basic idea of the proof is to simplify matters by counting values of $|\underline{x}|_L$ rather than values of $|E(\underline{x})|$.

Case where $\mathbb{K} = \mathbb{Q}$.

It will be useful to kick off with the following bounds:

$$C_8|\underline{x}| \leq |\underline{x}|_L \leq C_9|\underline{x}|. \tag{20}$$

In (20), $|\cdot|$ denotes any of the standard Euclidean norms on $\mathbb{Z}^r$. We will fix a choice of norm, the maximum norm, so that hereafter

$$|\underline{x}| = \max_i\{|x_i|\}, \quad \underline{x} = (x_1, \dots, x_r). \tag{21}$$

The proof of (20) is trivial in the case where $\mathbb{K} = \mathbb{Q}$. In particular, the left hand inequality follows because the coefficients of the linear forms in L all have positive coefficients (a feature which does not necessarily hold in the general case).

Using the results in [4], we estimate the growth rate of $|E(\underline{x})|$ as $\underline{x}$ varies over $\mathbb{N}^r$. Let $\epsilon > 0$ be given. From Theorem 2 in [4], a constant $C_{10}(E, \epsilon) > 0$ exists with

$$C_{10}|E_{max}(\underline{x})|^{1-\epsilon} \leq |E(\underline{x})|, \tag{22}$$

for all $\underline{x} \in \mathbb{N}^r$ apart from the finitely many zeros of $E(\underline{x})$. Since the bound $|E(\underline{x})| \leq C_{11}|E_{max}(\underline{x})|^{1+\epsilon}$ is trivial, an ineffective version of (7) with error term $o((\log q)^r)$ follows at once. We show how the invocation of Lemma 2 allows an improvement to the error to be made.

First, it is clear that the bounds in (20) and (22), together with the hypothesis that $|E(\underline{x})| < q$, imply a bound for $|\underline{x}|$ of the shape

$$|\underline{x}| \leq C_{12} \log q = T(q), \tag{23}$$

where in (23), the constant C_{12} is *ineffective.* Now let $H > 0$ denote an integer and suppose, after adjusting C_{12} if necessary, that H divides $T(q)$. Now divide the interval $[0, T(q)]$ into sub-intervals of length H. These define boxes of side H, of the form

$$B(\underline{N}) = [N_1, N_1 + H] \times \cdots \times [N_r, N_r + H], \quad \underline{N} = (N_1, \dots, N_r).$$

Given any of these, say $B(\underline{N})$, we have the estimate

$$\log|E(\underline{x})| = |\underline{x}|_L + O(H + \log|\underline{N}|), \tag{24}$$

which holds for all $\underline{x} \in B(\underline{N})$ apart from at most an exceptional set whose number is bounded as in (8). Applying (23) shows that we may take $|\underline{N}|$ to be $O(\log q)$. So we replace (24) by the estimate

$$\log|E(\underline{x})| = |\underline{x}|_L + O(H + \log\log q) = |\underline{x}|_L + O(H), \tag{25}$$

because we have insisted that $H \geq \log\log q$. Therefore (23) can be replaced by

$$|\underline{x}|_L \leq \log q + C_{14}H = T(q, H). \tag{26}$$

We are going to divide the counting into two parts. Notice that for $|\underline{x}|_L > T(q, H)$, there are at most a finite number of elements of $B(\underline{N}) \cap \mathbb{N}^r$ with $|E(\underline{x})| < q$, and this number is bounded as in (8).

We reckon the first part of the sum to be the following:

$$\sum_{\underline{N}} \#\{\underline{x} \in B(\underline{N}) \cap \mathbb{N}^r : |E(\underline{x})| \leq q, \quad |\underline{x}|_L \leq T(q, H)\}. \tag{27}$$

Applying Lemma 2 to (27) gives

$$\begin{aligned}&\sum_{\underline{N}} \#\{\underline{x} \in B(\underline{N}) \cap \mathbb{N}^r : |\underline{x}|_L \leq T(q, H)\}\\ &\qquad + \begin{cases} O(\#\{B(\underline{N}) : |\underline{N}|_L \leq T(q, H)\}), & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ O(H^{r-1}\#\{B(\underline{N}) : |\underline{N}|_L \leq T(q, H)\}), & \text{otherwise.}\end{cases}\end{aligned} \tag{28}$$

Note how the uniformity of the error term played a crucial role in (28). The number of boxes $B(\underline{N})$ with $|\underline{N}|_L \leq T(q, H)$ is approximately $(T(q, H)/H)^r$. Using Lemma 3 and the explicit definition of $T(q, H)$ (in (26)) we deduce the following formula for (28):

$$\begin{aligned}&\#\{\underline{x} \in \mathbb{N}^r : |\underline{x}|_L \leq T(q, H)\}\\ &\qquad + \begin{cases} O\left((T(q, H)/H)^r\right), & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ O((T(q, H)^r/H), & \text{otherwise}\end{cases}\\ &= D(\log q)^r + \begin{cases} O(H(\log q)^{r-1} + H^{-r}(\log q)^r), & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ O(H(\log q)^{r-1} + H^{-1}(\log q)^r), & \text{otherwise.}\end{cases}\end{aligned} \tag{29}$$

For the second part of the sum we recall that in each $B(\underline{N})$, provided $|\underline{x}|_L > T(q, H)$, the contribution is bounded as in (8). Write $R(q, H)$ for the set of $\underline{x}$ with $T(q, H) < |\underline{x}|_L \leq T(q)$. Then the second part of the sum (that is, the contribution from those $\underline{x}$ with $|\underline{x}|_L > T(q, H)$) can be estimated as

$$\begin{cases} O(\sum_{\underline{x} \in R(q,H)} 1), & \text{if } E(\underline{x}) \text{ has constant coefficients;}\\ O(H^{r-1}\sum_{\underline{x} \in R(q,H)} 1), & \text{otherwise.}\end{cases} \tag{30}$$

The total number of boxes counted in (30) is approximately

$$[(T(q) - T(q, H))/H]^r = O((\log q/H)^r).$$

Thus the term in (30) is

$$\begin{cases} O(H^{-r}(\log q)^r), & \text{if } E(\underline{x}) \text{ has constant coefficients;} \\ O(H^{-1}(\log q)^r), & \text{otherwise.} \end{cases} \tag{31}$$

The expression in (31) fits nicely into the last part of the error term in (29), completing the proof of formula (19).

General Case.

First, we can provide an estimate to replace that in (22). As before, $\sigma_l : \mathbb{K} \to \mathbb{C}, \quad l = 1, \dots, d$, denotes the distinct embeddings of $\mathbb{K}$ into the complex numbers. For any vector $\underline{a} = (a_1, \dots, a_M) \in O_{\mathbb{K}}^M$ define the height $H(\underline{a})$ to be

$$H(\underline{a}) = \prod_l \max\{|\sigma_l(a_1)|, \dots, |\sigma_l(a_M)|\}. \tag{32}$$

Using the results in [4], we are able to estimate $|N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))|$, by comparing it with $H_E(\underline{x}) = H((\underline{\lambda}_1^x, \dots, \underline{\lambda}_M^x))$. Using Theorem 2 in [4], we deduce the existence of positive constants C_{15} and C_{16} with

$$C_{15} H_E(\underline{x})^{1-\epsilon} \le |N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))| \le C_{16} H_E(\underline{x}). \tag{33}$$

In (33), the right hand inequality is trivial and follows from the triangle inequality. Secondly, we can use Lemma 2 to deduce the existence of constants C_{17}, C_{18} and C_{19} which are effective and uniform such that for any box $B(\underline{N})$ as in the proof of the case $\mathbb{K} = \mathbb{Q}$

$$\#\{\underline{x} \in B(\underline{N}) : |N_{\mathbb{K}|\mathbb{Q}}(E(\underline{x}))| \le H_E(\underline{x}) e^{-C_{17}H - C_{18} \log |\underline{N}|}\} \tag{34}$$

is bounded by C_{19} if $E(\underline{x})$ has constant coefficients and by $C_{19} H^{r-1}$ otherwise. This follows simply by multiplying together the inequalities in Lemma 2, one for each of the distinct embeddings.

Finally, we stand in need of some kind of geometric information. In the above, we knew that the fundamental domain $\mathcal{D}$ had finite volume, thus implying formula (13). This was true because the coefficients of the linear forms were positive. In the general case, this follows because the expression $H_E(\underline{x})$ is a height function (see [11] for a good discussion of heights). In particular, $H_E(\underline{x})$ has the following property: for any $C_{20} > 0$, there are only finitely many $\underline{x} \in \mathbb{N}^r$ with

$$H_E(\underline{x}) \le C_{20}. \tag{35}$$

In fact (35) follows from a more general property that for any $\underline{x} \in \mathbb{N}^r$,

$$C_{21} |\underline{x}|_L < \log H_E(\underline{x}) < C_{22} |\underline{x}|_L, \tag{36}$$

where C_{21} and C_{22} are positive constants. Now (35) is true because (see [11]) there are only finitely many $\underline{a} \in O_{\mathbb{K}}^M$ with $H(\underline{a})$ below a fixed bound. Write $h_E(\underline{x}) = \log(H_E(\underline{x}))$ as a sum of linear forms; thus

$$h_E(\underline{x}) = \sum_{l=1}^{d} \max\{L_{1l}(\underline{x}), \dots, L_{Ml}(\underline{x})\}. \tag{37}$$

In (37), the notation refers to Note (i), following the statement of Theorem 2. Now the definition of $h_E(\underline{x})$ extends to $\mathbb{R}_+^r$ and we claim that the fundamental domain

$$\mathcal{D} = \{\underline{x} \in \mathbb{R}_+^r : h_E(\underline{x}) \le 1\} \tag{38}$$

has finite volume. To see this, note that $\mathbb{R}_+^r$ is a finite union of cones according to which of the linear forms in (37) are largest. Each of these cones has a fundamental domain of finite volume because if this were not so, the cone would contain infinitely many points of $\mathbb{N}^r$. But this would violate inequality (35). Thus each cone has a fundamental domain of finite volume and therefore $\mathcal{D}$ has finite volume. From this we can use [5], as in Lemma 3, to deduce inequality (13) and the rest of the proof follows verbatim. □

Acknowledgment

Part of this paper was written during a visit by the second author in July 1995 to the University of East Anglia, whose hospitality is gratefully acknowledged. The authors thank Hans-Peter Schlickewei for valuable comments.

References

[1] G. R. Everest, *Counting the values taken by sums of S-units*, J. Number Theory **35** (1990), 269-286. MR **91j:**11015

[2] G. R. Everest, *On the p-adic integral of an exponential polynomial*, Bull. London Math. Soc. **27** (1995), 334-340. MR **96c:**11137

[3] G. R. Everest and I. E. Shparlinski, *Divisor sums of generalised exponential polynomials*, Bull. Canad. Math. Soc. **53** (1996), 35-46. MR **97g:**11021

[4] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), 225-244. MR **86c:**11045

[5] S. Lang, *Algebraic Number Theory*, Addison-Wesley, New York, 1970. MR **44:**181

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

[7] A. J. van der Poorten and I. Shparlinski, *On the number of zeros of exponential polynomials and related questions*, Bull. Austral. Math. Soc. **46** (1992), 401-412.

[8] H.-P. Schlickewei and W. M. Schmidt, *On polynomial-exponential equations*, Math. Ann. **296** (1993), 339-361. MR **94e:**11032

[9] ———, *On polynomial-exponential equations, II* (to appear).

[10] K. Schmidt and T. Ward, *Mixing automorphisms of compact groups and a theorem of Schlickewei*, Invent. Math. **111** (1993), 69-76. MR **95c:**22011

[11] W. M. Schmidt, *Diophantine Approximation and Diophantine Equations, LNM # 1467*, Springer, Berlin, 1991. MR **94f:**11059

[12] T. N. Shorey and R. J. Tijdeman, *Exponential Diophantine Equations*, CUP, 1986. MR **88h:**11002

[13] I. Shparlinski, *On the number of distinct prime divisors of recurrence sequences*, Matem. Zametki **42** (1987), 494–507 (Russian).

School of Mathematics, University of East Anglia, Norwich, NR4 7TJ, Norfolk, United Kingdom

E-mail address: g.everest@uea.ac.uk

School of MPCE, Macquarie University, New South Wales 2109, Australia

E-mail address: igor@mpce.mq.edu.au