18

LOWER BOUNDS FOR LINEAR FORMS IN LOGARITHMS

P. Philippon and M. Waldschmidt

1. Introduction

Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers and $\beta_0, \dots, \beta_n$ be algebraic numbers. For $1 \le j \le n$, let $\log \alpha_j$ be any determination of the logarithm of α_j. Assume that the number

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n$$

does not vanish. Our aim is to provide a new lower bound for $|\Lambda|$. For a history of the subject we refer to [1]. See also [11] and [6].

Our estimates improve previously known results on this subject.

If one pays special attention to the dependence on the degree of the algebraic numbers, it is more efficient to work with the absolute logarithmic height. We will do that in the next sections, but here we first give a few corollaries of our main results in terms of the usual height: for an algebraic number α, we denote by $H(\alpha)$ the maximum of the absolute values of the coefficients of the minimal polynomial of α over $\mathbf{Z}$.

Let D be a positive integer and A, A_1, $\dots$, A_n be positive real numbers satisfying

$$D \ge \left[\mathbf{Q}(\alpha_1, \dots, \alpha_n, \beta_0, \dots, \beta_n) : \mathbf{Q}\right],$$

$$A_j \ge \max\{H(\alpha_j), e\}, \qquad 1 \le j \le n,$$

and

$$A = \max\{A_1, \dots, A_n, e^e\}.$$

Theorem 1.1. *Let $B = \max\{H(\beta_j),\ 0 \le j \le n\}$. Assume*

$$A_j \ge \max\{\exp|\log \alpha_j|, e^n\}, \qquad 1 \le j \le n.$$

Then

$$|\Lambda| \ge e^{-U},$$

where

$$U = C_{11}(n) \,.\, D^{n+2} \,.\, \log A_1 \dots \log A_n \,.\, (\log B + \log\log A)$$

and

$$C_{11}(n) \le 2^{8n+53} \,.\, n^{2n}.$$

The main difference with Theorem 1.1 of [11] is that we omit a factor $\log\log A_{n-1}$ when, say, $A_n \ge A_{n-1} \ge \dots \ge A_1 \ge e^n$ (with $A_{n-1} = e^e$ if $n = 1$). The cost is a factor 4 for the constant, but also the assumption $A_1 \ge e^n$.

We turn now to the so-called rational case, where $\beta_0 = 0$ and $\beta_1, \dots, \beta_n$ are rational integers. In this case we write $\beta_i = b_i$, $1 \le i \le n$.

Theorem 1.2. *Let $b_1, \dots, b_n$ be rational integers such that*

$$\alpha_1^{b_1} \dots \alpha_n^{b_n} \ne 1.$$

Let B be a positive real number satisfying

$$B \ge \max\{|b_i|,\ 1 \le i \le n\} \quad \textit{and} \quad B \ge e.$$

Then

$$|\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1| \ge B^{-C_{12}\Omega}$$

with $\Omega = \log A_1 \dots \log A_n$, and C_{12} is a positive effectively computable constant depending only on n and on the degree of $\mathbf{Q}(\alpha_1, \dots, \alpha_n)$ over $\mathbf{Q}$.

Finally, here is a variant of Theorem 1.2 which is useful for instance in the study of Diophantine equations.

Theorem 1.3. *In the situation of Theorem 1.2 assume $e^e \le A_1 \le \dots \le A_{n-1} \le A_n$, and*

$$0 < |\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1| < e^{-\epsilon B}$$

for some $\epsilon > 0$. Then there exists a positive effectively computable constant C_{13}, depending only on n, on the degree of $\mathbf{Q}(\alpha_1, \dots, \alpha_n)$ over $\mathbf{Q}$, and on ϵ, such that

$$\boldsymbol{B < C_{13} \log A_1 \dots \log A_n \log\log A_n}.$$

Moreover, if $b_n = 1$, *then*

$$B < C_{13} \log A_1 \dots \log A_n \log\log A_{n-1}.$$

Here is the plan of this paper. In §2 we state two results (Theorem 2.1 for the "general" case, Theorem 2.2 for the "rational" case), and we deduce from them Theorems 1.1, 1.2 and 1.3.

Compared with previous proofs of similar results, the new feature here is that we apply the zero estimate of [9] (the previous zero estimates, which are referred to in [9], would not be sufficient for our purpose). The main result of [9] is stated in a much more general context, involving commutative algebraic groups. In §3 we state the special case which is needed here in terms of a lower bound for the rank of certain matrices. We need also to know that this zero estimate is not far from the best possible one, which means that we need an upper bound for the rank of these matrices. The proof of the zero estimate is postponed to the appendix. Indeed, for this proof, it is convenient to use the language of algebraic groups, and a reader who wishes to avoid this language can do so provided he takes for granted the Proposition 3.4. The proof of Theorem 2.1 is given in §4, and the proof of Theorem 2.2 in §5. A discussion on the explicit values of the constants is given in §2.

2. The two main results

Apart from the explicit dependence of the constant in terms of n, the two following statements include all previously known lower bounds for linear forms in logarithms which have been obtained so far by Baker's method.

When α is an algebraic number, we denote by $h(\alpha)$ the absolute logarithmic height of α (see for instance [11]).

We consider a non-zero linear form in logarithms of algebraic numbers with algebraic coefficients

$$\Lambda = \beta_0 + \beta_1 \log\alpha_1 + \dots + \beta_n \log\alpha_n,$$

where $\alpha_1, \dots, \alpha_n$ are non-zero algebraic numbers, $\beta_0, \dots, \beta_n$ are algebraic numbers, and $\log\alpha_1, \dots, \log\alpha_n$ are any non-zero determinations of the logarithms of $\alpha_1, \dots, \alpha_n$. Let K be a number field containing $\alpha_1, \dots, \alpha_n$, $\beta_0, \dots, \beta_n$, of degree D over $\mathbf{Q}$.

Let $V_1, \dots, V_n$, V, E be positive real numbers satisfying

$$V_j \geq \max\{h(\alpha_j),\ |\log\alpha_j|/D,\ n/D\},$$
$$V = \max\{V_1, \dots, V_n,\ 1\},$$

and

$$1 < E \leq \min\{e^{DV_j/n},\ eDV_j/|\log\alpha_j|\}, \qquad 1 \leq j \leq n.$$

Our first main result deals with the "general case".

Theorem 2.1. *Let* W *be a positive real number satisfying*

$$W \geq \max_{0 \leq j \leq n}\{h(\beta_j)\}.$$

Then

$$|\Lambda| > \exp\{-C_{21}(n) . D^{n+2} . V_1 \dots V_n .$$
$$(W + \log(EDV)) . (\log(ED)) . (\log E)^{-n-1}\}$$

with

$$C_{21}(n) \leq 2^{8n+51} . n^{2n}.$$

An improvement of our numerical value for $C_{21}(n)$ has been obtained recently by J. Blass, A. M. W. Glass, D. B. Meronk and R. P. Steiner [2].

Our second main result deals with the so-called "rational case".

Theorem 2.2. *Assume* $\beta_0 = 0$ *and* $\beta_i = b_i \in \mathbf{Z}$ *for* $1 \leq i \leq n$. *Let* B, B_n, W *be positive real numbers satisfying*

$$B \geq \max_{1 \leq j \leq n-1} |b_j|, \qquad B_n \geq |b_n|,$$

and

$$W \geq \max\left\{\log\left[\frac{B_n}{V_1} + \frac{B}{V_n} + 1\right];\ \frac{1}{D} . \log E;\ 1\right\},$$

where we assume

$$V_1 \leq V_2 \leq \dots \leq V_n.$$

Then

$$|\Lambda| > \exp\{-C_{22}(n) . D^{n+2} . V_1 \dots V_n . W . (\log(ED)) . (\log E)^{-n-1}\},$$

where $C_{22}(n)$ *is an effectively computable constant which depends only on* n.

If one tries to compute an explicit value for $C_{22}(n)$ just by working out the proof in §5 below, one finds $C_{22}(n) \leq C_{23}.n^{2n^2}$ for some absolute constant C_{23}. However, assuming that the field $\mathbf{Q}(\sqrt{\alpha}_1, \dots \sqrt{\alpha}_n)$

has degree 2^n over $\mathbf{Q}$, Blass, Glass, Meronk and Steiner find $C_{22}(n) \le C_{24}^n . n^n$ (with $C_{24} \le 2^{59}$). From the final descent of [11], one deduces $C_{12}(n) \le C_{25}^n . n^{2n}$ for the constant C_{12} of Theorem 1.2, and one expects that $C_{22}(n) \le C_{26}^n . n^{2n}$ without any assumption on $\mathbf{Q}(\sqrt{\alpha}_1, \dots \sqrt{\alpha}_n)$ (here C_{25} and C_{26} denote effectively computable absolute constants). However, as C.L. Stewart pointed out to the authors of [6], a further argument is necessary in order to achieve such an estimate. Also it was suggested by C. L. Stewart that the zero estimate of [9] could enable one to remove the $\log\log A_{n-1}$ as we did in Theorem 1.1.

Concerning the definition of E, it may be useful to notice that

$$eDV_j/|\log\alpha_j| \le 2^D . e^{2DV_j};$$

indeed, for each non-zero algebraic number $\alpha \ne 0$, of degree $\le d$, and for $\log\alpha \ne 0$, we have

$$|\log\alpha| \ge 2^{-d} . e^{-dh(\alpha)},$$

(using $|e^z - 1| \le |z| . e^{|z|}$ with the Liouville inequality).

Proof of Theorem 1.1. We deduce Theorem 1.1 from Theorem 2.1, with $C_{11}(n) \le 4 . C_{21}(n)$. We assume that the hypotheses of Theorem 1.1 hold, and we choose

$$V_j = \log A_j, \qquad W = \max\{1, \log B\}, \qquad E = eD.$$

Since

$$h(\alpha) \le \frac{1}{d}(\log H(\alpha) + \log d)$$

with $d = [\mathbf{Q}(\alpha) : \mathbf{Q}]$ (cf. [11], p. 260), we check that $V_j \ge h(\alpha_j)$. We use Theorem 2.1, with the fact that $A \ge e^e$ and $n \ge 1$, hence

$$(W + 1 + 2\log D + \log\log A)(1 + 2\log D) \\ < 4(1 + \log D)^{n+1}(\log B + \log\log A).$$

Therefore

$$C_{11}(n) \le 4C_{21}(n) \le 2^{8n+53} . n^{2n}.$$

Proof of Theorem 1.2. We now deduce Theorem 1.2 from Theorem 2.2. We will use the following simple lemma.

Lemma 2.3. *Let $t \in \mathbf{C}$ and $r \in \mathbf{R}$ satisfy*

$$0 < r < 1 \quad \textit{and} \quad |e^t - 1| \le r.$$

Then there exists $\kappa \in \mathbf{Z}$ such that

$$|t - 2i\kappa\pi| \le \frac{1}{r} . |\log(1 - r)| . |e^t - 1|.$$

Proof of Lemma 2.3. The principal value of the logarithm satisfies

$$\sup_{|z|=r} \bigl|\log(1 + z)\bigr| = \bigl|\log(1 - r)\bigr|.$$

From Schwarz' lemma we get for $|z| \le r$

$$\bigl|\log(1 + z)\bigr| \le |z| . \frac{1}{r} . \bigl|\log(1 - r)\bigr|.$$

We use this inequality for $z = e^t - 1$, and we define

$$\kappa = \frac{1}{2i\pi} . \bigl(t - \log(e^t)\bigr).$$

This proves Lemma 2.3.

For the proof of Theorem 1.2, we assume, as we may without loss of generality, $A_1 \le A_2 \le \dots \le A_{n-1} \le A_n$ (with $A_{n-1} = e$ if $n = 1$). From Lemma 2.3 we deduce that as soon as

$$\bigl|\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1\bigr| \le 1/3,$$

we have, for the principal value of the logarithm,

$$\bigl|b_1 \log\alpha_1 + \dots + b_n \log\alpha_n - 2i\pi\kappa\bigr| \le \frac{3}{2} \cdot \bigl|\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1\bigr|$$

for some $\kappa \in \mathbf{Z}$. Considering the imaginary parts, we get

$$|\kappa| < (nB + 1)/2.$$

We now choose

$$V_j = 7\log A_j, \quad (1 \le j \le n), \quad V_0 = 2\pi n/D,$$

$$E = e, \quad \text{and} \quad W = \log(DB + 1).$$

Notice that

$$|\log\alpha_j| \le \pi + \log|\alpha_j| \le \pi + \log(A_j + 1) \le \frac{9}{2} \cdot \log A_j.$$

We use Theorem 2.2 with n replaced by $n+1$:

$$\begin{aligned}&\left|2\kappa\pi i - \sum_{j=1}^{n} b_j \log \alpha_j\right| \\ &> \exp\bigl\{-C_{22}(n+1)\,.\,D^{n+3}7^n \log A_1 \dots \log A_n (2\pi n/D) W(1+\log D)\bigr\} \\ &> \exp\bigl\{-C_{28}(n,D) \log A_1 \dots \log A_n \log B\bigr\}.\end{aligned}$$

Theorem 1.2 follows.

Proof of Theorem 1.3. Finally we deduce Theorem 1.3 from Theorem 2.2.

1) From the assumptions of Theorem 1.3 and from Theorem 1.2 we deduce
$$\epsilon B < C_{29}(n,D)\,.\,\log A_1 \dots \log A_n \log B,$$
which yields
$$B < C_{13}(n,D,\epsilon)\,.\,\log A_1 \dots \log A_n \log\log A_n.$$

2) If $b_n = 1$, we follow the proof of Theorem 1.2 above with the definition of W replaced by $W = \log(e + nB/V_n)$. There is no loss of generality to assume $B \ge e\,.\,\log A_n$. Using Theorem 2.2 we obtain
$$\begin{aligned}\exp(-\epsilon B) &> \left|2\kappa\pi i - \sum_{j=1}^{n} b_j \log \alpha_j\right| \\ &> \exp\bigl\{-C_{29}(n,D) \log A_1 \dots \log A_n \log(B/\log A_n)\bigr\},\end{aligned}$$
for some $\kappa \in \mathbf{Z}$ such that $|\kappa| < ((n-1)B+2)/2$. Hence
$$B < C_{13}(n,D,\epsilon)\,.\,\log A_1 \dots \log A_n \log\log A_{n-1}.$$

3. On the rank of certain matrices

In this section $\beta_0, \dots, \beta_n$, $\ell_1, \dots, \ell_n$ denote arbitrary complex numbers with $\beta_n = -1$. We write $\alpha_j = e^{\ell_j}$, $1 \le j \le n$.

The transcendence proofs will involve auxiliary functions of the form
$$F(z_0, z_1, \dots, z_n) = P(z_0, e^{z_1}, \dots, e^{z_n})$$

where $P \in \mathbf{C}[X_0, \dots, X_n]$.

We define derivations $D_0, \dots, D_{n-1}$ on the ring $R = \mathbf{C}[X_0, \dots X_n]$ by setting, for $0 \le i \le n$,
$$\begin{aligned}D_i X_0 &= \delta_{i,0} \qquad \text{(Kronecker symbol)},\\ D_i X_j &= \delta_{i,j}\,.\,X_j, \qquad 1 \le j \le n-1,\end{aligned}$$
and
$$D_i X_n = \beta_i\,.\,X_n.$$

Therefore
$$\begin{aligned}&(\partial/\partial z_0)^{\tau_0} \dots (\partial/\partial z_{n-1})^{\tau_{n-1}} F(z_0, \dots, z_{n-1}, \beta_0 z_0 + \dots + \beta_{n-1} z_{n-1}) \\ &\qquad = D_0^{\tau_0} \dots D_{n-1}^{\tau_{n-1}} P(z_0, e^{z_1}, \dots, e^{z_{n-1}}, e^{\beta_0 z_0 + \dots + \beta_{n-1} z_{n-1}}).\end{aligned}$$

We say that F has a zero of order $\ge T$ in the direction of the hyperplane W:
$$z_n = \beta_0 z_0 + \dots + \beta_{n-1} z_{n-1}$$
at a point $(u_0, \dots, u_n) \in \mathbf{C}^{n+1}$ if
$$D_0^{\tau_0} \dots D_{n-1}^{\tau_{n-1}} P(u_0, \dots, u_n) = 0$$
for all non-negative integers $\tau_0, \dots, \tau_{n-1}$ with $\tau_0 + \dots + \tau_{n-1} \le T$. This means that the function of n variables
$$F(u_0 + z_0, \dots, u_{n-1} + z_{n-1}, u_n + \beta_0 z_0 + \dots + \beta_{n-1} z_{n-1})$$
has a zero order of $\ge T$ at the point $(0, \dots, 0) \in \mathbf{C}^n$.

We need to know whether there exists a non-zero polynomial P of degrees say
$$\deg_{X_i} P \le L_i, \qquad 0 \le i \le n$$
such that F has a zero of order $\ge T$ in the direction of W at all points
$$(s, s\ell_1, \dots, s\ell_n), \qquad 0 \le s < S$$
for some given non-negative integers L_0, L_1, …, L_n, T, S.

By linear algebra, a sufficient condition for the existence of such a P is
$$L_0 \dots L_n > \binom{T+n}{n}\,.\,S.$$

The following easy remark will be used several times.

Remark 3.1. Assume $L_0 < TS$, $L_i < T$, $1 \le i \le n-1$, and $L_n = 0$. Then there is no non-zero polynomial P of degrees $\le L_i$ such that

$$D_0^{\tau_0} \dots D_{n-1}^{\tau_{n-1}} P(s, \alpha_1^s, \dots, \alpha_n^s) = 0$$

for $0 \le \tau_i < T$, $(0 \le i \le n-1)$, $0 \le s < S$; (see [1], [11], [10]).

We denote by $\mathcal{A}$ the matrix whose entries are

$$\sum_{\tau_0'+\tau_0''=\tau_0} \frac{\tau_0!}{\tau_0'! \,.\, \tau_0''!} \cdot (\lambda_n\beta_0)^{\tau_0'} . s^{\lambda_0-\tau_0''} \cdot \frac{\lambda_0!}{(\lambda_0-\tau_0'')!} \prod_{i=1}^{n-1} (\lambda_i + \lambda_n\beta_i)^{\tau_i} \prod_{i=1}^{n} e^{\lambda_i \ell_i s},$$

where the index of row is

$$(\tau_0, \dots, \tau_{n-1}, s), \quad \text{with } \tau_0 + \dots + \tau_{n-1} < T,\ 0 \le s < S,$$

and the index of column is

$$(\lambda_0, \dots, \lambda_n), \quad \text{with } 0 \le \lambda_i \le L_i,\ 0 \le i \le n.$$

The existence of a non-zero polynomial P as above amounts to saying that $\mathcal{A}$ has rank $< (L_0+1)\dots(L_n+1)$.

We begin by giving upper bounds for the rank of $\mathcal{A}$, and then we will explain that these upper bounds are essentially best possible.

We need to introduce a few notations. Let r be an integer, $0 \le r \le n$, and let $\lambda^{(1)}, \dots, \lambda^{(r)}$ be linearly independent elements of $\mathbf{Z}^n$, with

$$\lambda^{(\rho)} = (\lambda_1^{(\rho)}, \dots, \lambda_n^{(\rho)}), \qquad 1 \le \rho \le r.$$

Let us write

$$\mathcal{L} = (\lambda^{(1)}, \dots, \lambda^{(r)}),$$

and let $\varphi_{r,n}$ denote the set composed of all increasing sequences of r elements from $\{1, \dots, n\}$; for each θ in $\varphi_{r,n}$, we will denote by $\mathcal{L}_\theta$ the minor of $\mathcal{L}$ whose columns are indexed by $\theta_1, \dots, \theta_r$. Define

$$\sigma_0(\mathcal{L}) = \sigma_0 = \begin{cases} r & \text{if } (\beta_1, \dots, \beta_n) \in \mathbf{C}\lambda^{(1)} + \dots + \mathbf{C}\lambda^{(r)}, \\ r+1 & \text{otherwise,} \end{cases}$$

and

$$H(\mathcal{L}; x_1, \dots, x_n) = (n-r)! \sum_{\theta \in \varphi_{r,n}} |\det \mathcal{L}_\theta| . \prod_{i \notin \theta} x_i.$$

In this paragraph we will denote by $\mathcal{I}$ the ideal, associated to the matrix $\mathcal{L}$, generated by the r polynomials

$$\prod_{i=1}^{n} X_i^{\lambda_i^{(j)}} - 1; \qquad 1 \le j \le r$$

in $\mathbf{C}[X_1, \dots, X_n]$. We will need an upper estimate for the maximal number of monomials in $X_1, \dots, X_n$ of given degrees which are linearly independent modulo the above ideal $\mathcal{I}$. The following lemma will do the job.

Lemma 3.2. *The maximal number of monomials in $X_1, \dots, X_n$ of degrees $\le L_1, \dots, L_n$ which are linearly independent modulo $\mathcal{I}$, is bounded above by*

$$((4\sqrt{n})^{n-r}/(n-r)!)H(\mathcal{L}; L_1, \dots, L_n).$$

Proof. Put $\Lambda = \mathbf{Z}(1/L_1, 0, \dots, 0) + \dots + \mathbf{Z}(0, \dots, 0, 1/L_n)$ in $\mathbf{R}^n$,

$$\mathcal{C} = \{z \in \mathbf{R};\ |z_i| \le 1,\ 1 \le i \le n\},$$

and $\Lambda' = \mathbf{Z}\tilde\lambda^{(1)} + \dots + \mathbf{Z}\tilde\lambda^{(r)}$ where $\tilde\lambda^{(j)} = (\lambda_1^{(j)}/L_1, \dots, \lambda_n^{(j)}/L_n)$. It is clear that two monomials $X_1^{\mu_1} \dots X_n^{\mu_n}$ and $X_1^{\nu_1} \dots X_n^{\nu_n}$ are congruent modulo $\mathcal{I}$ as soon as $\mu - \nu \in \Lambda'$, where $\mu = (\mu_1/L_1, \dots, \mu_n/L_n)$ and $\nu = (\nu_1/L_1, \dots, \nu_n/L_n)$. Let p be the orthogonal projection of $\mathbf{R}^n$ on the orthogonal of $\Lambda' \otimes_{\mathbf{Z}} \mathbf{R}$; then $p(\Lambda)$ is a discrete subgroup of $\mathbf{R}^n$. If $\tilde\lambda^{(r+1)}, \dots, \tilde\lambda^{(n)}$ is a basis of $p(\Lambda)$, it follows from Lemma 3 of [3] that

$$\det {}^t\mathcal{M}\mathcal{M} = [\overline{\Lambda}' : \Lambda']^2/(L_1 \dots L_n)^2 \det {}^t\tilde{\mathcal{L}}\tilde{\mathcal{L}},$$

where $\tilde{\mathcal{L}} = (\tilde\lambda^{(1)}, \dots, \tilde\lambda^{(r)})$, $\mathcal{M} = (\tilde\lambda^{(r+1)}, \dots, \tilde\lambda^{(n)})$ and $\overline{\Lambda}' = (\Lambda' \otimes_{\mathbf{Z}} \mathbf{R}) \cap \Lambda$. The maximal number, say $\mathcal{N}$, of monomials in $X_1, \dots, X_n$ of degrees $\le L_1, \dots, L_n$ which are linearly independent modulo $\mathcal{I}$ is at most $[\overline{\Lambda}' : \Lambda']$ times the number of points of $p(\Lambda)$ in $p(\mathcal{C})$. Since $p(\mathcal{C})$ is contained in the ball $\{z \in \mathbf{R}^{n-r};\ |z| \le \sqrt{n}\}$, and since the diameter of a fundamental parallelogram of $p(\Lambda)$ is $\le \sqrt{n}$, we get the upper bound

$$\mathcal{N} \le (4\sqrt{n})^{n-r}[\overline{\Lambda}' : \Lambda']/(\det {}^t\mathcal{M}\mathcal{M}^{\frac{1}{2}}) \le (4\sqrt{n})^{n-r} L_1 \dots L_n (\det {}^t\tilde{\mathcal{L}}\tilde{\mathcal{L}})^{\frac{1}{2}}.$$

It remains to compare $\det {}^t\tilde{\mathcal{L}}\tilde{\mathcal{L}}$ with $H(\mathcal{L}; L_1, \dots, L_n)$. But

$$\det {}^t\tilde{\mathcal{L}}\tilde{\mathcal{L}} = \sum_{\theta \in \varphi_{r,n}} (\det \tilde{\mathcal{L}}_\theta)^2 = \sum_{\theta \in \varphi_{r,n}} \left(\frac{\det \mathcal{L}_\theta}{L_{\theta_1} \dots L_{\theta_r}} \right)^2,$$

by the Cauchy-Binet formula (cf. [5], pp. 23–24). Finally

$$\begin{aligned} L_1 \dots L_n (\det {}^t\tilde{\mathcal{L}}\tilde{\mathcal{L}})^{1/2} &= L_1 \dots L_n \Big[\sum_{\theta \in \varphi_{r,n}} \left(\frac{\det \mathcal{L}_\theta}{L_{\theta_1} \dots L_{\theta_r}} \right)^2 \Big]^{1/2} \\ &\leq L_1 \dots L_n \sum_{\theta \in \varphi_{r,n}} \frac{|\det \mathcal{L}_\theta|}{L_{\theta_1} \dots L_{\theta_r}} \\ &\leq H(\mathcal{L}; L_1, \dots, L_n)/(n-r)!, \end{aligned}$$

which conclude the proof of Lemma 3.2.

Remark. We could also deduce Lemma 3.2 with $(4\sqrt{n})^{n-r}/(n-r)!$ replaced by 4^{n-r} using Nesterenko's result in [8] (compare with [10]).

Lemma 3.3. *For each $\mathcal{L}$ as above, the rank of the matrix $\mathcal{A}$ is at most*

$$\frac{(4\sqrt{n})^{n-r}}{(n-r)!} \cdot \binom{T+\sigma_0}{\sigma_0} . S . H(\mathcal{L}; L_1, \dots, L_n).$$

Proof. The linear system associated to the matrix $\mathcal{A}$ can be written

$$(*) \qquad D_0^{\tau_0} \circ \dots \circ D_{n-1}^{\tau_{n-1}} P(s, e^{s\ell_1}, \dots, e^{s\ell_n}) = 0 \qquad (\tau_0 + \dots + \tau_{n-1} < T; 0 \leq s \leq S),$$

where P stands for the general polynomial of degrees $L_0, \dots, L_n$.

We will use the following remark. Let $Q \in \mathbf{C}[X_1, \dots, X_n]$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{C}^n$ be such that

$$Q(x_1\alpha_1, \dots, x_n\alpha_n) = 0$$

for all $(x_1, \dots, x_n) \in \mathbf{C}^n$ satisfying

$$\prod_{i=1}^n x_i^{\lambda_i^{(j)}} = 1, \qquad 1 \leq j \leq r.$$

Then the function

$$G(z) = Q(\alpha_1 e^{z_1}, \dots, \alpha_n e^{z_n})$$

vanishes on the orthogonal V_0 in $\mathbf{C}^n$ of $\mathbf{C}\lambda^{(1)} + \dots + \mathbf{C}\lambda^{(r)}$. Therefore, for all $\zeta = (\zeta_1, \dots, \zeta_n) \in V_0$, we have

$$\sum_{i=1}^n \zeta_i \frac{\partial}{\partial z_i} G(0) = 0,$$

which can be written

$$\sum_{i=1}^n \zeta_i X_i \frac{\partial}{\partial X_i} Q(\alpha) = 0.$$

For each $\zeta = (\zeta_1, \dots, \zeta_n) \in \mathbf{C}^n$, we define a derivation Δ_ζ on $\mathbf{C}[X_0, \dots, X_n]$ by

$$\Delta_\zeta = \sum_{i=1}^n \zeta_i X_i \frac{\partial}{\partial X_i}.$$

We denote by W_0 the orthogonal in $\mathbf{C}^n$ of $\mathbf{C}(\beta_1, \dots, \beta_n)$. Notice that $\dim W_0 = n-1$ and $\dim W_0/W_0 \cap V_0 = \sigma_0 - 1$. We choose a basis $f_{\sigma_0+1}, \dots, f_n$ of $W_0 \cap V_0$, we complete it as a basis $f_2, \dots, f_n$ of W_0, and we write

$$D'_1 = D_0, \quad D'_i = \Delta_{f_i} \qquad 2 \leq i \leq n.$$

The system (*) is clearly equivalent to

$$D'^{\tau_1}_1 \circ \dots \circ D'^{\tau_n}_n P(s, e^{s\ell_1}, \dots, e^{s\ell_n}) = 0, \quad \tau_1 + \dots + \tau_n < T, \ 0 \leq s \leq S.$$

We now consider the following linear system

$$(**) \qquad D'^{\tau_1}_1 \circ \dots \circ D'^{\tau_{\sigma_0}}_{\sigma_0} P(s, x_1 e^{s\ell_1}, \dots, x_n e^{s\ell_n}) = 0,$$

where $\tau_1 + \dots + \tau_{\sigma_0} < T$, $0 \leq s \leq S$, $\prod_{i=1}^n x_i^{\lambda_i^{(j)}} = 1$ and P is as above. Since $D'_{\sigma_0+1}, \dots, D'_n$ are associated with vectors orthogonal to $\mathbf{C}\lambda^{(1)} + \dots + \mathbf{C}\lambda^{(r)}$, the rank of of the system (**) is at least the rank of (*), and we only consider the derivatives in σ_0 directions. On the other hand we need to eliminate the $x_i's$. Rewriting each equation of (**) as a polynomial $Q_{s,\tau}$ in $x_1, \dots, x_n$ modulo the equations $\prod_{i=1}^n x_i^{\lambda_i^{(j)}} = 1$, $1 \leq j \leq r$, each condition $Q_{s,\tau} \equiv 0$ gives, thanks to Lemma 3.2, at most

$$\big((4\sqrt{n})^{n-r}/(n-r)!\big) H(\mathcal{L}; L_1, \dots, L_n)$$

equations. It is then clear that the rank of (**) is bounded by

$$\big((4\sqrt{n})^{n-r}/(n-r)!\big) \binom{T+\sigma_0}{\sigma_0} . S . H(\mathcal{L}; L_1, \dots, L_n),$$

hence the Lemma 3.3.

Remark. If we choose for $\mathcal{L}$ the canonical basis of $\mathbf{C}^n$, we find the trivial upper bound $\binom{T+n}{n}.S$ for the rank of $\mathcal{A}$. Notice that a basis of W is $e_0,\ldots,e_{n-1}$, with $e_0=(1,0,\ldots,0)$ and $e_i=(0,\delta_{i1},\ldots,\delta_{i,n-1},\beta_i)$, $1\le i\le n-1$, hence $e_1,\ldots,e_{n-1}$ is a basis of W_0; for this special case, in the preceding proof if we choose $f_i=e_{i+1}$, then $D'_i=D_{i+1}$.

We need another upper bound for the rank of $\mathcal{A}$. Let r be an integer, $0<r\le n$, and let $\lambda^{(1)},\ldots,\lambda^{(r)}$ be linearly independent elements of $\mathbf{Z}^n$. Define $\mathcal{L}=(\lambda^{(1)},\ldots,\lambda^{(r)})$,

$$\sigma_1(\mathcal{L})=\sigma_1=\begin{cases} r-1 & \text{if } \sigma_0=r \text{ and } \beta_0=0,\\ r & \text{otherwise.}\end{cases}$$

Define a mapping

$$\varphi:(\mathbf{C}^\times)^n\longrightarrow(\mathbf{C}^\times)^r$$

by

$$\varphi(u_1,\ldots,u_n)=\Big[\prod_{i=1}^n u_i^{\lambda_i^{(1)}},\ldots,\prod_{i=1}^n u_i^{\lambda_i^{(r)}}\Big],$$

and put

$$E(S)=\varphi(\Gamma(S)),$$

where

$$\Gamma(S)=\{(e^{\ell_1 s},\ldots,e^{\ell_n s}),\ 0\le s\le S\}.$$

Lemma 3.4. *For each $\mathcal{L}$ as above, the rank of the matrix $\mathcal{A}$ is at most*

$$\frac{(4\sqrt{n})^{n-r}}{(n-r)!}\cdot\binom{T+\sigma_1}{\sigma_1}.\operatorname{Card}E(S).(L_0+1).H(\mathcal{L};L_1,\ldots,L_n).$$

Proof. Let V_1 denote the orthogonal in $\mathbf{C}^{n+1}$ of $\{0\}\times(\mathbf{C}\lambda^{(1)}+\ldots+\mathbf{C}\lambda^{(r)})$. Hence $\dim W/W\cap V_1=\sigma_1$. For each $\zeta=(\zeta_0,\ldots,\zeta_n)\in\mathbf{C}^{n+1}$, we define a derivation Δ_ζ on $\mathbf{C}[X_0,\ldots,X_n]$ by

$$\Delta_\zeta=\zeta_0\frac{\partial}{\partial X_0}+\sum_{i=1}^n\zeta_iX_i\frac{\partial}{\partial X_i}.$$

Let now $D'_{\sigma_1+1},\ldots,D'_n$ be derivatives associated with a basis of $W\cap V_1$, and $D'_1,\ldots,D'_{\sigma_1}$ derivatives associated with vectors completing the previous as a basis of W. We consider the following linear system

$$(**)\qquad D'^{\tau_1}_1\circ\ldots\circ D'^{\tau_{\sigma_1}}_{\sigma_1}P(x_0,x_1e^{s\ell_1},\ldots,x_ne^{s\ell_n})=0,$$

where $\tau_1+\ldots+\tau_{\sigma_1}<T$, $0\le s\le S$, $\prod_{i=1}^n x_i^{\lambda_i^{(j)}}=1$ and P is the general polynomial of degrees $L_0,\ldots,L_n$ in $X_0,\ldots,X_n$. First let's remark that it is equivalent to restrict s to $\operatorname{card}E(S)$ values in the range $\{0,\ldots,S\}$. Since $D'_{\sigma_1+1},\ldots,D'_n$ are associated with vectors orthogonal to $\mathbf{C}\lambda^{(1)}+\ldots+\mathbf{C}\lambda^{(r)}$, the rank of the system $(**)$ is larger than the rank of $(*)$. Rewriting each equation of $(**)$ as a polynomial $Q_{s,\tau}$ in $x_0,\ldots,x_n$ modulo the equations $\prod_{i=1}^n x_i^{\lambda_i^{(j)}}=1$, $1\le j\le r$, each condition $Q_{s,\tau}\equiv0$ gives, thanks again to Lemma 3.2, at most

$$((4\sqrt{n})^{n-r}/(n-r)!)H(\mathcal{L};L_1,\ldots,L_n).(L_0+1)$$

equations. It is then clear that the rank of $(**)$ is bounded by

$$((4\sqrt{n})^{n-r}/(n-r)!)\binom{T+\sigma_1}{\sigma_1}.\operatorname{card}E(S).(L_0+1).H(\mathcal{L};L_1,\ldots,L_n),$$

hence the Lemma 3.4.

Here is the main result of this section: the zero estimate.

Proposition 3.5. *Assume that the rank of $\mathcal{A}$ is $(L_0+1)\ldots(L_n+1)$. Then there exists an integer r, $0\le r\le n$, and there exist $\lambda^{(1)},\ldots,\lambda^{(r)}$ linearly independent in $\mathbf{Z}^n$, such that if we set*

$$T_1=[T/(n+1)]\quad\textit{and}\quad S_1=[S/(n+1)],$$

then either

(i) $$\binom{T_1+\sigma_0}{\sigma_0}.S_1.H(\mathcal{L};L_1,\ldots,L_n)\le(n+1)!.L_0\ldots L_n$$

or

(ii) $r>0$ *and*

$$\binom{T_1+\sigma_1}{\sigma_1}.\operatorname{Card}E(S_1).H(\mathcal{L};L_1,\ldots,L_n)\le\frac{(n+1)!}{n+1-r}.L_1\ldots L_n.$$

Proof. See appendix.

We need some further simple properties of H. For the rest of this section, we assume $L_i\ge1$, $1\le i\le n$, and we denote by a and b two positive numbers satisfying

$$T\ge a\max_{1\le j\le n}L_j$$

and

$$TS \ge bL_0.$$

Lemma 3.6. *We have the following inequalities.*

(i) $$\frac{T^{r+1}}{(r+1)!}\,.\,S\,.\,H(\mathcal{L},\mathbf{L}) \ge a^r b\frac{(n-r)!}{(r+1)!}L_0\ldots L_n.$$

(ii) $$\frac{T^r}{r!}\,.\,H(\mathcal{L},\mathbf{L}) \ge a^r\frac{(n-r)!}{r!}L_1\ldots L_n.$$

Proof. We have

$$H(\mathcal{L},\mathbf{L}) \ge (n-r)!\,L_1\ldots L_n/(\max_{1\le i\le n} L_i)^r.$$

This completes the proof of Lemma 3.6.

Lemma 3.7. *Define* $A = \max\{|\ell_j|,\ 1 \le j \le n\}$, $L = \max\{|\lambda_i^{(j)}|,$ $1\le j\le r,\ 1\le i\le n\}$. *Assume* $\sigma_1 = r-1$, $\operatorname{Card} E(S) < S$ *and that* $\beta_1,\ldots,\beta_n$ *are algebraic numbers in a field of degree* $\le D$. *Then either the number*

$$\Lambda = \beta_1\ell_1 + \ldots + \beta_n\ell_n$$

vanishes or

$$|\Lambda| \ge \exp\Big\{-D\Big[\sum_{j=1}^{n} h(\beta_j) + \log(n^{n+2}ASL^n)\Big]\Big\}.$$

Proof. Since $\sigma_1 = r-1$ we have $\beta_0 = 0$ and

$$\beta_i = \sum_{j=1}^{r} c_j\lambda_i^{(j)}, \qquad 1 \le i \le n,$$

for some $c_j \in \overline{\mathbf{Q}}$. The assumption on $E(S)$ means that there exists $s\in\mathbf{Z}$, $1\le s\le S$, such that

$$\prod_{i=1}^{n}\alpha_i^{\lambda_i^{(j)}s} = 1 \qquad \text{for } 1\le j\le r.$$

Define $k_j \in \mathbf{Z}$, $1\le j\le r$, by

$$\sum_{i=1}^{n}\lambda_i^{(j)}s\ell_i = 2\pi k_j\sqrt{-1}.$$

Hence

$$\Lambda = \sum_{i=1}^{n}\beta_i\ell_i = \sum_{j=1}^{r} c_j 2\pi k_j\sqrt{-1}/s$$

and

$$|\Lambda| = 2\pi\Big|\sum_{j=1}^{r} c_jk_j/s\Big|.$$

It is therefore sufficient to use Liouville inequality (e.g. Lemma 2.2 of [11]). We have

$$2\pi|k_j| \le S.\sum_{i=1}^{n}|\lambda_i^{(j)}|\,.\,|\ell_i| \le ALSn.$$

Now we compute the c_j by solving the system

$$\beta_i = \sum_{j=1}^{r} c_j\lambda_i^{(j)},\ 1\le i\le n,$$

which gives

$$c_j = \Delta_j/\Delta,$$

where Δ and Δ_j are certain determinants; Δ is a non-zero integer of absolute value at most $(rL)^r$, and Δ_j are linear combinations of $\beta_1,\ldots,\beta_n$ with integral coefficients of absolute values at most $(rL)^{r-1}$. So

$$\sum_{j=1}^{r} c_jk_j = \Big(\sum_{i=1}^{n} a_i\beta_i\Big)/\Delta,$$

where a_i are integers of absolute values at most $n^{r+1}ASL^r$, and

$$|\Lambda| \ge \Big|\sum_{i=1}^{n} a_i\beta_i\Big|/\Delta S.$$

The desired estimate easily follows from Lemma 2.2 of [11].

4. Proof of Theorem 2.1

We use the notations of [11]. We first refine Proposition 3.1 of [11].

Let c_0, c_0', c_1, c_2, c_3, c_4 be positive real numbers satisfying the inequalities (3.1), (3.2) and (3.3) of [11]. We also assume $c_0 \le 29$ and $c_3 \le 2^{10}$.

We assume $V_1 \geq n/D$, and we define

$$E_1 = \min\{\exp(qDV_1/n), \min_{1\leq j\leq n}\{2qDV_j|\log\alpha_j|^{-1}\}\},$$

$$E^* = \max\{2^{5n+4}q^{n+1}n^{2n}DE_1^n, E_1^{n^2}\},$$

$$W^* = \max\{W, n\,.\,\log(2^{11}nq^2DV_n^+), \frac{q}{nD}\,.\,\log E_1\},$$

$$U_1 = 2^{22}n^2q^{n+1}D^2\max\{W^*, V_n^+, W^*V_n^+(\log E_1)^{-1}, \log E_1\}$$

and

$$U_2 = c_0'c_1c_2^nc_3c_4q^{3n}(q-1)n^{2n+1}(n!)^{-1}D^{n+2}V_1\dots V_n \qquad W^*(\log E^*)(\log E_1)^{-n-1},$$

and

$$U = \max\{U_1, U_2\}.$$

Proposition 4.1. *With the assumptions of Theorem* 2.1, *let* $K = \mathbf{Q}(\alpha_1,\dots,\alpha_n,\beta_0,\dots,\beta_{n-1})$, *and assume q is a prime number such that*

$$[K(\alpha_1^{1/q},\dots,\alpha_n^{1/q}):K] = q^n.$$

Assume also $\beta_n = -1$. *Then*

$$|\Lambda| > e^{-U}.$$

We go back to the proof in §3 of [11]. We replace V_{n-1}^* by E^*. We replace (3.7) of [11] by

$$\log E^* \leq (19/2)qn^2D\log E_1.$$

We replace (3.10) of [11] by

$$q^32^{5n+8}n^{2n+1}E_1 \leq (E^*)^{1+1/n},$$

and (3.14) of [11] by

$$3q^{n+2}\,.\,2^{5n+10}n^{2n+1}E_1S \leq (L_{-1}+1)(E^*)^{1+2/n},$$

because $C_3 \leq 2^{10}$. The inequality (3.17) of [11] is satisfied for $0 \leq t \leq T$ and $|z| \leq q^{n+2}2^{5n+7}n^{2n+1}E_1S$.

Next we take Q in the interval $1 \leq Q \leq q^33^{5n+82}n^{2n+1}$, and in (3.18) of [11] we replace qL_n by $q^32^{5n+82}n^{2n+1}$.

This means that if we set

$$N = q^22^{5n+8}n^{2n+1},$$

then we replace L_n by N in (3.10), (3.14), (3.17) and (3.18) of [11]. In §3.4 of [11] we restrict J to the interval

$$0 \leq J \leq \left[\frac{\log N}{\log q}\right]+1.$$

All the estimates in §3.3 of [11] will remain valid; however there are two important modifications which we now explain: the construction of the auxiliary function, and the contradiction.

a) *Preliminaries to the proof of Proposition* 4.1

In [11], we use the polynomials

$$\Delta(X,k) = (X+1)\dots(X+k)/k!\,.$$

Let us set $\tilde{L}_0 = (L_0+1)(L_{-1}+1)$. Then the polynomials

$$\Delta(z+\lambda_{-1}, L_{-1}+1)^{\lambda_0+1}, \qquad 0 \leq \lambda_{-1} \leq L_{-1},\ 0 \leq \lambda_0 \leq L_0$$

give a basis of a space of polynomials of degree $\leq \tilde{L}_0$. This change of basis gives trivial changes in the matrix which we will consider. We will use the results of our §3 above, but now the space of polynomials we consider is of dimension $\tilde{L}_0$ (instead of L_0+1 in our §3 above).

When $\tilde{L}_1,\dots,\tilde{L}_n$ are positive integers, we are interested in the rank of the matrix $\tilde{A}$ whose entries are

$$\sum_{\tau_0'+\tau_0''=\tau_0}\frac{\tau_0!}{\tau_0'!\tau_0''!}\left(\frac{d^{\tau_0'}}{dz_0^{\tau_0'}}\Delta(s+\lambda_{-1}, L_{-1}+1)^{\lambda_0+1}\right)\prod_{r=1}^{n-1}(\lambda_r+\lambda_n\beta_r)^{\tau_r}\prod_{i=1}^{n}\alpha_i^{\lambda_i s},$$

which can be written, with the notations of [11],

$$\Lambda_0(s,\tau)\,.\,\alpha_1^{\lambda_1 s}\dots\alpha_n^{\lambda_n s}.$$

The index of a row is (s,τ), with

$$\tau = (\tau_0,\dots,\tau_{n-1}),\ \tau_0+\dots+\tau_{n-1} < T, \quad \text{and} \quad 0 \leq s < S,\ (s,q) = 1,$$

while the index of a column is $\lambda = (\lambda_{-1}, \lambda_0, \dots, \lambda_n)$ with

$$0 \le \lambda_{-1} \le L_{-1},\ 0 \le \lambda_0 \le L_0, \quad \text{and} \quad 0 \le \lambda_i \le \tilde{L}_i, \qquad 1 \le i \le n.$$

We will choose $\tilde{L}_i = L_i$, $1 \le i \le n-1$, but we will take for $\tilde{L}_n$ the smallest integer such that we can construct the auxiliary function. More precisely, for each real number $\tilde{U} \le U$, we define

$$L_n^\sharp = \tilde{U}/c_1c_2nq^{n+1}DSV_n,$$

and

$$\tilde{L}_n = [L_n^\sharp].$$

Notice that in the case $\tilde{U} = U$, we find $\tilde{L}_n = L_n$, and also in this case

$$(L_{-1}+1)(L_0+1)\dots(L_{n-1}+1)L_n^\sharp \ge c_0(1-\frac{1}{q})\binom{T+n}{n}.S \qquad (4.2)$$

(compare with inequality (3.6) in [11]).

Let $i \in \{0,1\}$, $0 \le r \le n$, with $r > 0$ in case $i = 1$, and $\mathcal{L} = (\lambda^{(1)}, \dots, \lambda^{(r)}) \in \mathbf{Z}^{nr}$, with $\lambda^{(1)}, \dots, \lambda^{(r)}$ linearly independent. We set

$$L^\sharp = (L_1, \dots, L_{n-1}, L_n^\sharp)$$

and

$$\tilde{L} = (L_1, \dots, L_{n-1}, \tilde{L}_n).$$

The function $H(\mathcal{L}; L^\sharp)$ (see §3) is of the form

$$H(\mathcal{L}; L^\sharp) = A(\mathcal{L})\tilde{U} + B(\mathcal{L}).$$

Lemma 4.3. *Assume $\sigma_i = r - i$. Then $B(\mathcal{L}) > 0$.*

Proof. Assume $B(\mathcal{L}) = 0$. This means $\det \mathcal{L}_\theta = 0$ for all $\theta = (\theta_1, \dots, \theta_{r-1}, n)$ with $0 < \theta_1 < \dots < \theta_{r-1} < n$:

$$\mathcal{L}_\theta = \begin{vmatrix} \lambda_{\theta_1}^{(1)} & \dots & \lambda_{\theta_1}^{(r)} \\ \vdots & \ddots & \vdots \\ \lambda_{\theta_{r-1}}^{(1)} & \dots & \lambda_{\theta_{r-1}}^{(r)} \\ \lambda_n^{(1)} & \dots & \lambda_n^{(r)} \end{vmatrix}.$$

As $\lambda^{(1)}, \dots, \lambda^{(r)}$ are linearly independent, we have $\lambda_n^{(1)} = \dots = \lambda_n^{(r)} = 0$. But the assumption $\beta_n = -1$ gives

$$(\beta_1, \dots, \beta_n) \notin \mathbf{C}\lambda^{(1)} + \dots + \mathbf{C}\lambda^{(r)},$$

hence $\sigma_0 = r+1$ if $i = 0$ and $\sigma_1 = r$ if $i = 1$. This completes the proof of Lemma 4.3.

Now we are going to choose $\tilde{U}$ as the smallest positive number such that there exists $i_0 \in \{0,1\}$, r_0, and $\mathcal{L}^0 = (\lambda_0^{(1)}, \dots, \lambda_0^{(r_0)})$, with $\sigma_i^0 = \sigma_i(\mathcal{L}^0) = r_0 - i_0$, satisfying

$$c_0\left(1-\frac{1}{q}\right)\frac{(8\sqrt{n})^{n-r_0}}{(n-r_0)!}\binom{T+\sigma_i^0}{\sigma_i^0}S.H(\mathcal{L}^0, L^\sharp) \le \tilde{L}_0^{1-i_0}.(L_1+1)\dots(L_{n-1}+1)L_n^\sharp. \qquad (4.4)$$

We do this in the following way. We define $C(\mathcal{L})$ by

$$C(\mathcal{L}).c_0.\left(1-\frac{1}{q}\right)\frac{(8\sqrt{n})^{n-r_0}}{(n-r_0)!}\binom{T+\sigma_i}{\sigma_i}.c_1c_2nq^{n+1}DS^2V_n = \tilde{L}_0^{1-i_0}.(L_1+1)\dots(L_{n-1}+1)$$

so that (4.4) can be written

$$A(\mathcal{L}^0).\tilde{U} + B(\mathcal{L}^0) \le C(\mathcal{L}^0).\tilde{U}.$$

We define $\tilde{U}$ as the minimum of

$$B(\mathcal{L})/(C(\mathcal{L}) - A(\mathcal{L}))$$

for $(i, \mathcal{L})$ running over the set of $i \in \{0,1\}$, and $\mathcal{L} = (\lambda^{(1)}, \dots, \lambda^{(r)})$, for which $\sigma_i = r - i$ and $C(\mathcal{L}) > A(\mathcal{L})$. This set is not empty; thanks to (4.2) we can choose for $\mathcal{L}$ the canonical basis of $\mathbf{Z}^n$, with $i = 0$. Of course we choose a value $(i_0, \mathcal{L}^0)$ which gives the minimum, and we get (4.4) with equality. Notice that, if $r_0 = n$, then $\mathbf{Z}\lambda_0^{(1)} + \dots + \mathbf{Z}\lambda_0^{(n)} = \mathbf{Z}^n$ and $i = 0$ (this follows from the definition of H: this is the only case where $H = 1$). If $r_0 < n$, then $\left(1-\frac{1}{q}\right).2^{n-r_0} \ge 1$.

Moreover, from this choice of $\tilde{U}$, we deduce, using Lemma 4.3,

$$A(\mathcal{L}).\tilde{U} + B(\mathcal{L}) \ge C(\mathcal{L}).\tilde{U} \qquad (4.5)$$

for all $(i, \mathcal{L})$ with $\sigma_i = r - i$. This means

$$c_0 \cdot \left(1 - \frac{1}{q}\right) \cdot \frac{(8\sqrt{n})^{n-r}}{(n-r)!} \cdot \binom{T+\sigma_i}{\sigma_i} . S . H(\mathcal{L}, L^\sharp) \geq \tilde{L}_0^{1-i} . (L_1+1) \dots (L_{n-1}+1) . L_n^\sharp. \tag{4.6}$$

Let us show that $L_n^\sharp \geq 1$. Otherwise, the matrix $\tilde{\mathcal{A}}$ (which corresponds to our choice of $\tilde{U}$) does not involve λ_n, and from the Remark 3.1 we deduce that its rank is $\tilde{L}_0 . (L_1+1) \dots (L_{n-1}+1)$. We now use Lemmas 3.3 and 3.4 with $n-1$ variables instead of n (because α_n is not involved) to get a contradiction with (4.4).

Now we have $L_n^\sharp \geq 1$:

$$\tilde{U} \geq c_1 c_2 n q^{n+1} D S V_n,$$

hence $\tilde{L}_n \geq 1$, and we can use Lemmas 3.3 and 3.4 (with $L_0, \dots, L_n$ replaced by $\tilde{L}_0, \dots, \tilde{L}_n$, and $\tilde{L}_i = L_i$ for $1 \leq i \leq n-1$) to deduce:

Lemma 4.7. *The rank of the matrix* $\tilde{\mathcal{A}}$ *is at most*

$$\frac{1}{c_0} \tilde{L}_0 . (L_1+1) \dots (L_{n-1}+1) . (\tilde{L}_n + 1)$$

b) *Construction of the auxiliary function.*

Lemma 4.8. *In Lemma* 3.2 *of* [11] p. 266, *one may restrict* λ *to run over the* $(n+2)$*-tuples* $(\lambda_{-1}, \dots, \lambda_n)$ *with* $0 \leq \lambda_j \leq L_j$, $(-1 \leq j \leq n-1)$ *and* $0 \leq \lambda_n \leq \tilde{L}_n$.

Proof. The proof is the same as in [11], apart from the fact that we use Lemma 4.7 in place of (3.6) of [11].

We now continue the proof as in §3.3 and §3.4 of [11]. We keep the estimates of [11] as they stand; we do not modify the parameters T, S, U, L_{-1}, $\dots$, L_{n-1}, but the parameter L_n is replaced by $\tilde{L}_n$ which may be smaller, and therefore the upper bounds in [11] §3.3 and §3.4 are valid. Also it is important to notice that $L_n^{(J+1)} \leq L_n^{(J)}/q$, hence $L_n^{(J)} \leq q^{-J} \tilde{L}_n$.

c) *End of the proof of Proposition 4.1.*

We write the main inductive argument (p. 268 of [11]) for $J_0 = \left[\frac{\log N}{\log q}\right]$. Then we need to modify the argument in §3.5 of [11], because we cannot claim that $L_n^{(J_0)}$ vanishes.

Let us show that the numbers

$$\varphi_{J_0,\tau}(s) = \sum_{(\lambda)} \sum_{d=1}^{D} p_d^{(J_0)}(\lambda) \xi_d \Lambda_{J_0}(s, \tau) \alpha_1^{\lambda_1 s} \dots \alpha_n^{\lambda_n s}$$

satisfy

$$\varphi_{J_0,\tau}(s) = 0 \quad \text{for } 0 \leq s \leq q^{J_0} S \text{ and } |\tau| \leq q^{-J_0} T. \tag{4.9}$$

This is plain if $(s, q) = 1$, since this is the step before the last in the inductive argument. If q divides s, this has been proved at the last step of the induction (proof of Lemma 3.6 of [11]).

From Remark 3.1 above (or from the argument in §3.5 of [1]) we have $L_n^{(J_0)} \geq 1$, hence $L_n^{(J)} \geq q^J$ for $1 \leq J \leq J_0$. We define

$$J_1 = \left[J_0 - \frac{\log(5n)}{\log q}\right];$$

thus

$$q^{J_0 - J_1} \geq 5n \quad \text{and} \quad q^{J_1} \geq q^{J_0}/5nq \geq N/5nq^2.$$

We now use the zero estimate (Proposition 3.4 above). Define

$$T_1 = \left[[q^{-J_1}T]/(n+1)\right], \qquad S_1 = \left[q^{J_1}S/(n+1)\right].$$

From (4.9) we deduce that there exists an integer r, $0 \leq r \leq n$, and there exist $\lambda^{(1)}, \dots, \lambda^{(r)}$ linearly independent in $\mathbf{Z}^n$, such that either

$$\binom{T_1+\sigma_0}{\sigma_0} . S_1 . H(\mathcal{L}; L_1^{(J_1)}, \dots, L_n^{(J_1)}) \leq (n+1)! \prod_{j=-1}^{n} (L_j^{(J_1)}+1), \tag{4.10}$$

or $r > 0$ and

$$\binom{T_1+\sigma_1}{\sigma_1} . \operatorname{Card} E(S_1) . H(\mathcal{L}; L_1^{(J_1)}, \dots, L_n^{(J_1)}) \leq \frac{(n+1)!}{n-r+1} . \prod_{j=1}^{n} (L_j^{(J_1)}+1), \tag{4.11}$$

where $\mathcal{L}$ stands for $(\lambda^{(1)}, \dots, \lambda^{(r)})$.

It is readily checked that

$$S_1 \,.\, \binom{T_1+\sigma_i}{\sigma_i} \geq \frac{4}{5} \cdot \frac{T^{\sigma_i} \,.\, S}{q^{J_1(\sigma_i-1)} \,.\, (n+1)^{\sigma_i+1} \,.\, \sigma_i!}$$

and

$$\binom{T_1+\sigma_i}{\sigma_i} \geq \frac{4}{5} \cdot \frac{T^{\sigma_i}}{q^{J_1\sigma_i} \,.\, (n+1)^{\sigma_i} \,.\, \sigma_i!}$$

for $i=0$ and $i=1$. We write

$$\frac{H(\mathcal{L}; L^{(J_1)})}{\prod_{j=-1}^{n} L_j^{(J_1)}} \geq q^{J_1 r} \cdot \frac{H(\mathcal{L}; \tilde{L})}{\prod_{i=0}^{n} \tilde{L}_j},$$

where $\tilde{L}$ stands for $(\tilde{L}_1, \ldots, \tilde{L}_n)$. Since $L_j^{(J_1)} \geq 5n$, $1 \leq j \leq n$, we have $L_j^{(J_1)} + 1 \leq (1 + 1/5n) L_j^{(J_1)}$, hence

$$\prod_{j=1}^{n} (L_j^{(J_1)} + 1) \leq \frac{5}{4} \cdot \prod_{j=1}^{n} L_j^{(J_1)}.$$

Therefore (4.10) gives

$$q^{J_1(r-\sigma_0+1)} \,.\, \frac{T^{\sigma_0}}{\sigma_0!} \,.\, S \,.\, H(\mathcal{L}; \tilde{L}) \leq \frac{7}{4} \cdot (n+1)^{\sigma_0+1} (n+1)! \,.\, \prod_{j=0}^{n} \tilde{L}_j, \tag{4.12}$$

while (4.11) gives

$$q^{J_1(r-\sigma_1)} \,.\, \frac{T^{\sigma_1}}{\sigma_1!} \cdot \operatorname{Card} E(S_1) \,.\, H(\mathcal{L}; \tilde{L}) \leq \frac{7}{4} \cdot (n+1)^{\sigma_1} \frac{(n+1)!}{n-r+1} \cdot \prod_{j=1}^{n} \tilde{L}_j. \tag{4.13}$$

Our assumption $\log E_1 \leq qDV_1/n$ gives

$$T/\tilde{L}_j \geq \tfrac{1}{2} \,.\, c_2 n^2 q^2 D V_j / \log E_1 > 14 \,.\, n^3,$$

while the assumption $E^* \geq E_1^{n^2}$ gives

$$TS/\tilde{L}_0 \geq \tfrac{1}{2} \,.\, c_4 n q D \log E^* / \log E_1 > 14 \,.\, n^3.$$

We consider different cases depending on whether $i=0$ or $i=1$, and $\sigma_i = r - i + 1$ or $\sigma_i = r - i$.

α) Assume (4.12) holds with $\sigma_0 = r+1$. We get

$$\frac{T^{r+1}}{(r+1)!} \,.\, S .\, H(\mathcal{L}; \tilde{L}) \leq \frac{7}{4} .(n+1)^{r+3} n! .\, \prod_{j=0}^{n} \tilde{L}_j.$$

However, it is readily checked that

$$(n+1)^{r+3} n! (r+1)! \leq 2^{2r+3} n^{3r+3} (n-r)!, \tag{4.14}$$

and we get a contradiction with lemma 3.6 (i) with $a > 14n^3$, $b > 14n^3$.

β) Assume (4.13) holds with $\sigma_1 = r$. We get

$$\begin{aligned} \frac{T^r}{r!} \,.\, H(\mathcal{L}; \tilde{L}) &\leq \frac{7}{4} \cdot \frac{(n+1)^{r+1}}{n-r+1} \,.\, n! \,.\, \prod_{j=1}^{n} \tilde{L}_j \\ &< \frac{7}{2(n+1)} (4n^3)^r \cdot \frac{(n-r)!}{r!} \cdot \prod_{j=1}^{n} \tilde{L}_j, \end{aligned}$$

(from (4.14) with r replaced by $r-1$) which contradicts Lemma 3.6 (ii) with $a > 14n^3$.

γ) Assume (4.12) holds with $\sigma_0 = r$. We get

$$q^{2J_1} \cdot \frac{T^r}{r!} \,.\, S \,.\, H(\mathcal{L}; \tilde{L}) \leq \frac{7}{4} \cdot (n+1)^{r+2} n! \,.\, \prod_{j=0}^{n} \tilde{L}_j.$$

We use our choice of N, with the bounds

$$(n+1)^{r+2} n! \,.\, \frac{(8\sqrt{n})^{n-r}}{(n-r)!} \leq 2^{5n} n^{2n}$$

and $C_0 \leq 29$; we get a contradiction with (4.6).

δ) Assume (4.13) holds with $\sigma_1 = r-1$. From Lemma 3.7 we deduce $\operatorname{Card} E(S_1) = S_1$, hence we get

$$q^{2J_1} \cdot \frac{T^{r-1}}{(r-1)!} \,.\, S \,.\, H(\mathcal{L}; \tilde{L}) \leq 2 \,.\, (n+1)^{r+1} n! \,.\, \prod_{j=1}^{n} \tilde{L}_j.$$

Once more, we get a contradiction with (4.6).

This completes the proof of Proposition 4.1.

d) *End of the proof of Theorem 2.1.*

We now deduce from Proposition 4.1 that in Proposition 3.8, p. 274 of [11] one may replace $\log(EDV_{n-1}^{+})$ by $\log(ED)$, provided that $V_1 \geq n/D$.

This is clear if $n \leq 12$, because in this case we still have, with our value of E^*,

$$\log E^* \leq n\log(2^{13}q^2n)\,.\,\log(ED).$$

If $n \geq 13$, we have

$$\log E^* \leq n^2(1+\log q)\,.\,\log(ED),$$

and

$$\log(2^{13}nq^2) < (3+\log q)\sqrt{n},$$

while

$$(3+\log q)(1+\log q) < 2q^2/(q-1),$$

and this is sufficient for our estimates of [11] p. 275.

Finally, it follows that in the theorem p. 258 of [11], one may replace $\log(EDV_{n-1}^{+})$ by $\log(ED)$, provided that $V_1 \geq n/D$. This completes the proof of Theorem 2.1.

5. Proof of Theorem 2.2

We introduce parameters $c_0, c_1, \dots, c_5$ which satisfy the following requirements: c_0 is a sufficiently large absolute constant, and

$$c_5 \geq c_0^2 2^n(n+1)^{n+2}n!, \quad c_1 \geq c_0 \log c_5,$$

$$c_2 \geq c_0c_5, \quad c_3 \geq c_0c_5, \quad c_4 \geq c_0c_5.$$

We could of course choose $c_2 = c_3 = c_4$, but the above notations will enable us to use the computations already made in [11]; also, if one wishes to provide good numerical values, it may be better to have more freedom.

We will denote by $f_1, \dots, f_8$ positive numbers which can be explicitly computed in terms of n and $c_0, \dots, c_5$, and which satisfy the property that $c_0c_1f_i$ are bounded by an absolute constant independent of c_0.

Next we define

$$S = \left[c_3DW(\log E)^{-1}\right],$$

$$U = c_0c_1c_2^nc_3c_4\,.\,\frac{n^n}{n!}\,.\,D^{n+2}V_1\dots V_nW\big(\log(DE)\big)(\log E)^{-n-1},$$

and

$$T = [U/c_1c_3DW],$$

$$L_{-1} = [W],$$

$$L_{-2} = \left[U/c_1c_4D\log(DE)(L_{-1}+1)\right],$$

$$L_0 = (L_{-1}+1)(L_{-2}+1).$$

Further, for each real number $\tilde{U} \geq c_0$, we define real numbers $L_1^\sharp, \dots, L_n^\sharp$, and integers $\tilde{L}_1, \dots, \tilde{L}_n$ by

$$L_j^\sharp = \tilde{U}/c_1c_2nDSV_j, \qquad 1 \leq j \leq n,$$

and

$$\tilde{L}_j = \left[L_j^\sharp\right], \qquad 1 \leq j \leq n.$$

We denote by $L_1, \dots, L_n$ the values of $\tilde{L}_1, \dots, \tilde{L}_n$ corresponding to $\tilde{U} = U$.

We assume $0 < |\Lambda| < e^{-U}$, and we shall eventually reach a contradiction.

Let us recall that

$$\Delta(z;k;\ell,m) = \frac{d^m}{dz^m}\big(\Delta(z;k)\big)^\ell,$$

where

$$\Delta(z;k) = (z+1)(z+2)\dots(z+k)/k!, \quad \Delta(z;0) = 1.$$

We introduce the functions

$$\Lambda(z;\tau) = \Delta(z+\lambda_{-1}; L_{-1}+1; \lambda_{-2}+1; \tau_0)\,.\,\prod_{r=1}^{n-1}\Delta(b_n\lambda_r - b_r\lambda_n; \tau_r)$$

for $0 \leq \lambda_j \leq \tilde{L}_j$, $(j = -2, -1, 1, \dots, n)$, $\tau = (\tau_0, \dots, \tau_{n-1})$, and $z \in \mathbb{C}$. Notice that the dependence in λ_{-2}, λ_{-1}, λ_1, $\dots$, λ_n is hidden in the notation $\Lambda(z;\tau)$.

Our auxiliary functions will be of the form

$$f_\tau(z) = \sum_{(\lambda)} p(\lambda)\Lambda(z;\tau)\alpha_1^{\gamma_1 z}\dots\alpha_{n-1}^{\gamma_{n-1} z},$$

where $\gamma_j = \lambda_j - \lambda_n b_j/b_n$, $(1 \leq j \leq n)$, and

$$\varphi_\tau(z) = \sum_{(\lambda)} p(\lambda)\Lambda(z;\tau)\alpha_1^{\lambda_1 z}\dots\alpha_n^{\lambda_n z};$$

here, λ stands for $(\lambda_{-2}, \lambda_{-1}, \lambda_1 \dots, \lambda_n)$.

We need analytical and arithmetical estimates on $\Lambda(z;\tau)$ (cf. [11], and [6]).

Lemma 5.1. *For $|z| \le c_5 ES$ and $|\tau| \le T$,*

$$\left|\Lambda(z;\tau)\right| \le e^{f_1 U/D}.$$

Moreover, for $s \in \mathbf{Z}$, $0 \le s \le c_5 S$, and $|\tau| < T$, $\Lambda(s;\tau)$ is a rational number with a denominator at most $e^{f_2 U/D}$.

Now we consider the matrix $\mathcal{B}$ whose entries are

$$\Lambda(s;\tau)\alpha_1^{\lambda_1 s} \dots \alpha_n^{\lambda_n s}$$

where the index of row is

$$(\tau_0, \dots, \tau_{n-1}, s), \quad \text{with } |\tau| = \tau_0 + \dots + \tau_{n-1} < T,\ 0 \le s < S,$$

and the index of column is

$$(\lambda_{-2}, \lambda_{-1}, \lambda_1, \dots, \lambda_n), \quad \text{with } 0 \le \lambda_j \le \tilde{L}_j.$$

We recall that the polynomials

$$\left(\Delta(z+r;k)\right)^{\ell}, \qquad 0 \le r \le R-1,\ 1 \le \ell \le L$$

(with $k > R > 0$, $L > 0$) are linearly independent and of degrees $\le kL$.

First step. We choose for $\tilde{U}$ the smallest positive real number with the following property:

There exist $i \in \{0,1\}$, $r \in \mathbf{Z}$, $0 \le r \le n$, with $r > 0$ if $i = 1$, and there exist $\lambda^{(1)}, \dots, \lambda^{(r)}$ linearly independent in $\mathbf{Z}^n$, such that

$$c_0(4\sqrt{n})^{n-r}\binom{T+\sigma_i}{\sigma_i}.\operatorname{Card} E(S).L_0^i.H(\mathcal{L}; L_1^\sharp, \dots, L_n^\sharp)$$
$$\le L_0^{1-i} L_1^\sharp \dots L_n^\sharp,$$

where $\mathcal{L} = (\lambda^{(1)}, \dots, \lambda^{(r)})$, and where we set $\operatorname{Card} E(S) = S$ in case $i = 0$. Note that for $\tilde{U}$ we have

$$c_0(4\sqrt{n})^{n-r}\binom{T+\sigma_i}{\sigma_i}.\operatorname{Card} E(S).H(\mathcal{L}; L_1^\sharp, \dots, L_n^\sharp)$$
$$\ge L_0^{1-i} L_1^\sharp \dots L_n^\sharp,$$

with all $\mathcal{L}$ and $i = 0$, 1 and we have equality with at least one $\mathcal{L}$ and one $i \in \{0,1\}$. From Lemma 3.3 or Lemma 3.4, accordingly to $i = 0$ or $i = 1$, we deduce the existence of a non-zero polynomial of degree $\le L_0 . [L_1^\sharp] \dots [L_n^\sharp]$ satisfying

$$D_0^{\tau_0} \dots D_{n-1}^{\tau_{n-1}} P(s, \alpha_1^s, \dots, \alpha_n^s) = 0.$$

And from Remark 3.1 we deduce $[L_n^\sharp] \ne 0$ hence$\tilde{L}_j \ge 1$ for $1 \le j \le n$.

Step 2. Among the numbers $\alpha_1^{i_1} \dots \alpha_n^{i_n}$, $0 \le i_j \le [\mathbf{Q}(\alpha_j) : \mathbf{Q}]$, $1 \le j \le n$, $i_1 + \dots + i_n \le D$, we choose a basis $\xi_1, \dots, \xi_D$ of the field $\mathbf{Q}(\alpha_1, \dots, \alpha_n)$ over $\mathbf{Q}$. Then there exist rational integers $p_d(\lambda)$, $1 \le d \le D$, $0 \le \lambda_j \le \tilde{L}_j$, $j = -2, -1, 1, \dots, n$, not all zero, bounded in absolute value by $\exp(f_3 U/D)$, such that if we set

$$p(\lambda) = \sum_{d=1}^{D} p_d(\lambda)\xi_d,$$

then for all $(n+1)$-tuple $(\tau_0, \dots, \tau_{n-1}, s) \in \mathbf{N}^{n+1}$ satisfying $|\tau| < T$ and $0 \le s < S$, the equation $\varphi_\tau(s) = 0$ holds.

Proof: We follow the proof of Lemma 3.2 of [11]. The equation $\varphi_\tau(s) = 0$ can be written

$$\sum_{(\lambda)} \sum_{d=1}^{D} p_d(\lambda)\xi_d \Lambda(s,\tau)\alpha_1^{\lambda_1 s} \dots \alpha_n^{\lambda_n s} = 0.$$

The rank of the linear system obtained when $|\tau| < T$ and $0 \le s < S$ vary is equal to the rank of $\mathcal{B}$ which is bounded above, thanks to Lemma 3.3 or Lemma 3.4, according to $i = 0$ or $i = 1$, by

$$(4\sqrt{n})^{n-r}\binom{T+\sigma_i}{\sigma_i}.\operatorname{Card} E(S).(L_0+1)^i.H(\mathcal{L}; L_1^\sharp, \dots, L_n^\sharp)$$

for any $\mathcal{L}$ and $i = 0, 1$ and where we set $\operatorname{Card} E(S) = S$ in case $i = 0$. Hence by the choice of $\tilde{U}$ in step 1, $\operatorname{rank}\mathcal{B}$ is less than $2L_0 L_1^\sharp \dots L_n^\sharp / c_0$. We select $\operatorname{rank}\mathcal{B}$ equations from the above linear system and we apply Lemma 2.1 of [11] to this sub-system, with

$$d = D,$$
$$n = D(L_0+1)([L_1^\sharp]+1)\dots([L_n^\sharp]+1),$$
$$m \le 2L_0 L_1^\sharp \dots L_n^\sharp / c_0,$$

and finally,

$$X \le \exp(f_3 U/2D),$$

thanks to Lemma 5.1.

Step 3. For $|z| < c_5 S$ and $|\tau| < T$, we have

$$|f_\tau(z) - \varphi_\tau(z)| \le |\Lambda|.e^{f_4 U}.$$

Proof: See Lemma 3.3 of [11] with $J = 0$.

Step 4. For $s \in \mathbf{Z}$, $1 \le s < c_5 S$, and $|\tau| < T$, we have either $\varphi_\tau(s) = 0$ or

$$\log|\varphi_\tau(s)| > -f_5 U.$$

Proof. See part 1 of Lemma 3.4 in [11] with $J = 0$.

Step 5. For $|z| < c_5 S$ and $|\tau| < T/2$, we have

$$\log|f_\tau(z)| \le -(\frac{1}{2c_1} - f_8)U.$$

Proof: This is essentially Lemma 3.5 of [11], again with $J = 0$. We use the extrapolation procedure of Baker together with Steps 2 and 3. In the estimate which is provided by Lemma 2.3 of [11], the main term comes from the quantity $(T/2)S\log(R/4r)$; we choose $r = c_5 S$, $R = Er$, and this gives the term $U/2c_1$.

We also need an upper bound for $|f_\tau|_R = \sup\{|f_\tau(z)|;\ |z| = R\}$; this estimate involves

$$\sum_{j=1}^{n} L_j R|\log\alpha_j| \le e c_5 U/c_1 c_2$$

which is less than $f_8 U/2$. We also need an upper bound for $(T/2)S\log(18r/S)$, and we use our assumption $c_1 \ge c_0 \log c_5$.

Step 6. For $|\tau| < T/2$ and $0 \le s < c_5 S$, $s \in \mathbf{Z}$, we have

$$\varphi_\tau(s) = 0.$$

This is an easy consequence of the three preceding steps; see [11] Lemma 3.6 with $J = 0$.

Step 7. We now reach the desired contradiction. We use Proposition 3.5. with $T_1 = [T/2(n+1)]$ and $S_1 = [c_5 S/(n+1)]$: there exists $i = 0$ or 1, and there exists $\mathcal{L}$ such that

$$\binom{T_1 + \sigma_i}{\sigma_i} . \operatorname{Card} E(S_1) . H(\mathcal{L}; \tilde{L}) \le (n+1)! . L_0^{1-i} \tilde{L}_1 \ldots \tilde{L}_n. \qquad (5.2)$$

We notice that, for $0 \le \sigma \le n$, we have

$$\binom{T_1 + \sigma}{\sigma} . S_1 \ge \binom{T + \sigma}{\sigma} . S . c_5/c_0 2^\sigma (n+1)^{\sigma+1}.$$

Notice also that $T/\tilde{L}_j \ge 8n^3$ $(1 \le j \le n)$ and $TS/L_0 \ge 8n^3$. Therefore Lemma 3.6 gives $\sigma_0 = r - 1$ if $i = 0$, and $\sigma_1 = r$ if $i = 1$. Next, Lemma 3.7 yields $\operatorname{Card} E(S_1) = S_1$ if $i = 1$. Now from (5.2) we deduce

$$c_5 . \binom{T + \sigma_i}{\sigma_i} . S . H(\mathcal{L}; \tilde{L}) \le c_0 (n+1)!\, 2^{\sigma_i} (n+1)^{\sigma_i + 1} . L_0^{1-i} \tilde{L}_1 \ldots \tilde{L}_n,$$

and for $c_5 \ge c_0^2 (n+1)^{n+2} n!\, 2^n$, this gives a contradiction with the first step (minimality of $\tilde{U}$).

Appendix: Algebraic subgroups of a torus

Let us consider an algebraic group G which is the product of the n-th power of the multiplicative group $\mathbf{G}_m$ with the additive group $\mathbf{G}_a$. We embed $\mathbf{G}_a$ and $\mathbf{G}_m$ in the projective line $\mathbf{P}^1$ in the natural way, that is we identify $\mathbf{G}_a$ with the affine line and $\mathbf{G}_m$ with this affine line but one point. Any algebraic subgroup G' of G is then a quasi-projective subvariety of the multiprojective space $\mathbf{P} = \prod_{i=0}^n \mathbf{P}^1_{(i)}$. There exist notions of multidegrees on $\mathbf{P}$ which we recall now.

Let V be a quasi-projective subvariety of $\mathbf{P}$ of dimension d and $\theta = (\theta_1, \ldots, \theta_d)$ an increasing sequence of $\{0, \ldots, n\}$. There exists a hypersurface of $\prod_{i=1}^d \mathbf{P}^1_{(\theta_i)}$ with the following property: for each point P of $\prod_{i=1}^d \mathbf{P}^1_{(\theta_i)}$ outside this hypersurface, the number of points in V whose projection is P is finite and independent of P. We denote this number by $\deg_\theta V$. The characteristic function of V is then the following homogeneous polynomial of degree d in the variables $X_0, \ldots, X_n$

$$\mathcal{H}(V; X_0, \ldots, X_n) = d! \sum_\theta \deg_\theta V . X_{\theta_1} \ldots X_{\theta_d},$$

where θ runs over the set $\varphi_{d,n+1}$ of all increasing sequences of d elements of $\{0,\dots,n\}$.

We will see soon that this polynomial, which occurs in the zeros estimate of [9], is closely related to the polynomial H introduced in §3. Then we will establish Proposition 3.5.

First we recall that any algebraic subgroup of $G = \mathbb{G}_a \times \mathbb{G}_m^n$ splits in a product $G'_0 \times G'_1$ where G'_0 (resp. G'_1) is a subgroup of $\mathbb{G}_a$ (resp. $\mathbb{G}_m^n$). So we consider two cases, either $G'_0 = \{0\}$ and we will say that we are in case I, or $G'_0 = \mathbb{G}_a$ and we will say that we are in case II. In case I it follows from Lemma 3.4 of [9]

$$\mathcal{H}(G';X_0,\dots,X_n) = \mathcal{H}(G'_1;X_1,\dots,X_n),$$

while in case II we have, with $d+1 = \dim G'$,

$$\mathcal{H}(G';X_0,\dots,X_n) = (d+1)\,.\,X_0\,.\,\mathcal{H}(G'_1;X_1,\dots,X_n).$$

Lemma A.1. *For any connected algebraic subgroup* G' of G *there exists* $\mathcal{L} = (\lambda^{(1)},\dots,\lambda^{(r)})$, *with* $r = n - \dim G'$ *in case* I *and* $r = n+1-\dim G'$ *in case* II, *and* $\lambda^{(i)} \in \mathbb{Z}^n$ *such that*

$$\mathcal{H}(G';X_0,\dots,X_n) = (\dim G'\,.\,X_0)^i H(\mathcal{L};X_1,\dots,X_n),$$

where $i = 0$ *in case* I *and* $i = 1$ *in case* II.

Proof: From the remark above, it is enough to prove

$$\mathcal{H}(G'_1;X_1,\dots,X_n) = H(\mathcal{L};X_1,\dots,X_n),$$

for some $\mathcal{L}$. Note that $n-r$ is always the dimension of G'_1. And according to the definitions of the functions $\mathcal{H}$ and H it all comes down to verify the equalities

$$\deg_\theta G'_1 = |\det \mathcal{L}_{\theta'}|,$$

where $\theta \in \varphi_{n-r,n}$ and θ' stands for the complement of θ in $\varphi_{r,n}$. This is Proposition 4 of [3], we repeat the proof here for the convenience of the reader. By symmetry it is enough to deal with the index $\theta = (r+1,\dots,n)$. Let Λ be the subgroup of $\mathbb{Z}^n$ of rank r which is orthogonal to $T_{G'_1}$. By Theorem I (p.11) of [4] we can find, as in [7], p.434, generators $\lambda^{(1)},\dots,\lambda^{(r)}$ of Λ such that $\lambda_j^{(i)} = 0$ for $i > j$. If $\mathcal{L}$ is a basis of Λ the quantity $|\det \mathcal{L}_{\theta'}|$ is invariant by a change of basis, so we have $|\det \mathcal{L}_{\theta'}| = |\lambda_1^{(1)}|\dots|\lambda_r^{(r)}|$. But G'_1 is defined in G_1 by the equations

$$X_i^{\lambda_i^{(i)}} = \prod_{j>i} X_j^{-\lambda_j^{(i)}}, \quad i = 1,\dots,r,$$

so, if we fix $X_{r+1},\dots,X_n$ each non zero, the number $\deg_\theta G'_1$ of points in G'_1 over $X_{r+1},\dots,X_n$ is equal to $|\lambda_1^{(1)}|\dots|\lambda_r^{(r)}|$, and we deduce the equality

$$\deg_\theta G'_1 = |\det \mathcal{L}_{\theta'}|,$$

which establishes the lemma.

Proof of Proposition 3.5. If the rank of the matrix $\mathcal{A}$ is strictly less than $(L_0+1)\dots(L_n+1)$ there exists a polynomial P of degrees $L_0,\dots,L_n$ which vanishes at each point $(s, e^{s\ell_1},\dots,e^{s\ell_n})$ for $s = 0,\dots,S$ with order at least T with respect to the derivatives $D_0,\dots,D_{n-1}$. The main zeros estimate of [9] (Theorem 2.1) applied to this situation exhibits a connected algebraic subgroup G' of G satisfying

$$\binom{T_1 + \dim W/W\cap G'}{\dim W/W\cap G'}\,.\,\mathrm{card}(\Sigma+G')/G'.\mathcal{H}(G';L_0,\dots,L_n)$$

$$(***) \qquad\qquad \le (n+1)!\,L_0\dots L_n,$$

where Σ stands for the set $\{(s, e^{s\ell_1},\dots,e^{s\ell_n})\,;\, 0 \le s \le S_1\}$ and W stands for the image of the analytic subgroup

$$(z_0,\dots,z_{n-1}) \longrightarrow (z_0, e^{z_1},\dots,e^{z_{n-1}}, e^{\beta_0 z_0+\dots+\beta_{n-1}z_{n-1}}).$$

Let Λ be the subgroup of $\mathbb{Z}^n$ of rank r which is orthogonal to $T_{G'_1}$ and $\mathcal{L}$ a basis of Λ. In Case I, i.e. $G'_0 = \{0\}$, we have $\dim G' = n-r$ and we compute $\mathrm{card}(\Sigma+G')/G' = S_1$ and $\dim W/W\cap G' = r$ if $G' \subseteq W$ or $= r+1$ if $G' \not\subseteq W$. In Case II (i.e. $G'_0 = \mathbb{G}_a$) we have $\dim G' = n+1-r$ so that $\mathrm{card}(\Sigma+G')/G' = \mathrm{card}\,E(S_1)$ and $\dim W/W\cap G' = r-1$ if $G' \subseteq W$ or $= r$ if $G' \not\subseteq W$. Putting these calculations together with Lemma A.1, Proposition 3.5 follows at once from $(***)$.

References

[1] Baker A., The theory of linear forms in logarithms, in: *Transcendence theory; advances and applications*, A. Baker and D. W. Masser ed., Academic Press (1977), Chap. 1, p.1–27.

[2] Blass J., Glass A., Meronk D. and Steiner R., A lower bound for linear forms in logarithms, to appear.

[3] Bertrand D., and Philippon P., Sous-groupes algébriques de groupes algébriques commutatifs, *Illinois J. Math.*, to appear.

[4] Cassels J. W. S., *An introduction to the geometry of numbers,* Springer (1959).

[5] Gramain F., Sur le lemme de Siegel (d'après E. Bombieri et J. Vaaler), in *Problèmes diophantiens* 1983/84, *fasc. 1*, No 2, D. Bertrand and M. Waldschmidt ed, *Publications Math. Paris VI* No 64, (1984).

[6] Loxton J., Mignotte M., van der Poorten A., and Waldschmidt M., A lower bound for linear forms in the logarithms of algebraic numbers, *C. R. Math. Acad. Sci. Canada = Math. Report Acad. Sci.*, **11** (1987), 119–124.

[7] Masser D. W., and Wüstholz G., Fields of large transcendence degree, *Inv. Math.* **72**, (1983), 407–464.

[8] Nesterenko Y. V., Estimates for the characteristic function of a prime ideal, *Math. Sbornik* **123** (165) No 1, (1984) *Math. USSR Sbornik* **51** No 1, (1985), 9–32.

[9] Philippon P., Lemmes de zéros dans les groupes algébriques commutatifs, *Bulletin Soc. Math. France* **114**, tome III, (1986), 355–383.

[10] Philippon P., and Waldschmidt M., Formes linéaires de logarithmes sur les groupes algébriques commutatifs, *Illinois J. Math.*, to appear.

[11] Waldschmidt M., A lower bound for linear forms in logarithms, *Acta Arithmetica* **37**, (1980), 257–283.

19

REDUCIBILITY OF LACUNARY POLYNOMIALS, IX

A. Schinzel

The aim of this paper is to extend the results of the papers [1] and [4] concerning reducibility of trinomials and quadrinomials over **Q** to the case where their coefficients are arbitrary algebraic numbers. We shall use the following notation.

If **K** is a field, $f \in \mathbf{K}[x_1, \dots, x_k]$ then

$$f \overset{\text{can}}{\underset{\mathbf{K}}{=\!=}} \text{const} \prod_{\sigma=1}^{s} f_\sigma^{e_\sigma}$$

means, besides the equality, that the polynomials $f_\sigma \in \mathbf{K}[x_1, \dots, x_k]$ are irreducible over **K** and prime to each other. Constants are considered neither reducible nor irreducible.

If $\phi = f \prod_{i=1}^{k} x_i^{\alpha_i}$, where f is a polynomial prime to $x_1 x_2 \dots x_k$ and α_i are integers, then we set

$$J\phi = f.$$

A polynomial g such that

$$Jg(x_1^{-1}, \dots, x_k^{-1}) = \pm g(x_1, \dots, x_k)$$

is called reciprocal. Let

$$J\phi \overset{\text{can}}{\underset{\mathbf{K}}{=\!=}} \text{const} \prod_{\sigma=1}^{s} f_\sigma^{e_\sigma}.$$

We set

$$K\phi = \text{const}\, \Pi_1 f_\sigma^{e_\sigma}$$

where Π_1 is extended over all f_σ that do not divide $J(x_1^{\delta_1} \dots x_k^{\delta_k} - 1)$ for any integer vector $[\delta_1, \dots, \delta_k] \neq \mathbf{0}$. Moreover if $\mathbf{K} = \mathbf{Q}$ we set

$$L\phi = \text{const}\, \Pi_2 f_\sigma^{e_\sigma}$$

where Π_2 is extended over all f_σ that are non-reciprocal. The leading coefficients of $K\phi$ and $L\phi$ are assumed equal to that of $J\phi$. In particular,