ON RESULTANT INEQUALITIES

JAN-HENDRIK EVERTSE

1. Introduction

Let t be a positive integer, κ a positive real and $f \in \mathbb{Z}[X]$ a polynomial of degree $r > 0$ without multiple zeros. We consider the so-called *resultant inequality*

$$0 < |R(f,g)| \leqslant M(g)^{r-\kappa} \tag{1.1}$$

to be solved in polynomials $g \in \mathbb{Z}[X]$ of degree t, where $R(f,g)$ denotes the resultant of f and g and where $M(g)$ denotes the Mahler measure of g (see formulas (2.1), (2.2) in Section 2 for definitions). If $g = vX - u$ is a polynomial of degree 1 then $R(f,g) = F(u,v)$ where F is the binary form defined by $F(u,v) = v^r f(u/v)$ and $M(g) = \max(|u|,|v|)$. So for $t = 1$ we may rewrite (1.1) as a *Thue inequality*

$$0 < |F(u,v)| \leqslant \max(|u|,|v|)^{r-\kappa} \quad \text{in } u,v \in \mathbb{Z}. \tag{1.2}$$

By a theorem of Roth [10], (1.2) has only finitely many solutions if $\kappa > 2$. Hence (1.1) has only finitely many solutions if $t = 1, \kappa > 2$. From results of Wirsing [17], Schmidt [14] and Ru and Wong [11] it follows that (1.1) has only finitely many solutions if $t \geqslant 2$ and $\kappa > 2t$.

Our purpose is to compute an explicit upper bound for the number of polynomials $g \in \mathbb{Z}[X]$ of degree t satisfying (1.1) for any $t \geqslant 1$, $\kappa > 2t$. With the present state of affairs, it is realistic to estimate only the number of polynomials g which are irreducible and primitive (i.e., whose coefficients have greatest common divisor 1). Indeed, as was pointed out by Hirata-Kohno and the author [4], any explicit upper bound for the number of non-primitive or reducible polynomials g of degree t satisfying (1.1) would yield an effective improvement of Liouville's inequality which is much stronger than what has been achieved so far. In other words, getting an

1991 *Mathematics Subject Classification.* 11J25, 11J68.

Key words and phrases. Resultants, Subspace Theorem, Diophantine approximation, approximation of algebraic numbers by algebraic numbers of bounded degree.

explicit upper bound for the number of non-primitive or reducible solutions of (1.1) is at least as difficult as proving such a strong effective result.

In [3] we derived an explicit upper bound for the number of primitive, irreducible polynomials $g \in \mathbb{Z}[X]$ of degree t satisfying (1.1) but only for $\kappa > 2t\Big(\sum_{k=1}^{t} \frac{1}{2k-1}\Big)$. In the present paper we derive a similar such upper bound for $\kappa > 2t$. The precise statement is given in Theorem 2.1 in Section 2. Whereas in [3] we obtained our result by following Wirsing's method from [17], in the present paper we use techniques from the proof of the quantitative Subspace Theorem. These techniques were developed in their basic form by Schmidt [15] and refined later by Schlickewei and the author, cf. e.g., [2], [5].

The quantitative Subspace Theorem implies for a general class of inequalities including (1.1), that the set of solutions is contained in a finite union $V_1 \cup \cdots \cup V_s$ of proper linear subspaces of the ambient solution space, and moreover it provides an explicit upper bound for s. In this paper, we specialise the arguments of the proof of the quantitative Subspace Theorem to (1.1) and show that in this particular situation, $V_1, \ldots, V_s$ can be chosen to be one-dimensional. As our argument heavily uses properties of resultants, it is not likely that it can be extended to inequalities other than (1.1).

We give two applications. First we give an explicit upper bound for the number of solutions of Thue inequalities in which the unknowns are algebraic integers x, y with $[\mathbb{Q}(x/y) : \mathbb{Q}] = t$ (cf. Corollary 2.2 in Section 2). Second we derive an explicit upper bound for the number of solutions of so-called Wirsing systems (these are systems of inequalities introduced by Wirsing in [17]) (cf. Corollary 2.3 in Section 2). Roughly speaking this means that we give an upper bound for the number of algebraic numbers ζ of degree t such that for $i = 1, \ldots, t$, the i-th conjugate $\zeta^{(i)}$ of ζ is very close to a given algebraic number α_i.

By (2.3) in Section 2 we can express $R(f, g)$ as $F(g_0, \ldots, g_t)$ where $g_0, \ldots, g_t$ are the coefficients of g and where F is a homogeneous polynomial in $\mathbb{Z}[X_0, \ldots, X_t]$ of degree $r = \deg f$. More precisely, F is a *decomposable form*, i.e., F factors into homogeneous linear forms over the algebraic closure of $\mathbb{Q}$. Thus (using that for polynomials g, $M(g)/\max(|g_0|, \ldots, |g_t|)$ is bounded from above and from below by constants depending only on t), we may view (1.1) as a special type of a *decomposable* *form inequality*

$$|F(g_0,\dots,g_t)| \leqslant \big(\max |g_0|,\dots,|g_t|\big)^{r-\kappa} \quad \text{in } g_0,\dots,g_t\in\mathbb{Z}, \tag{1.3}$$

where F is any decomposable form in $\mathbb{Z}[X_0,\dots,X_t]$ of degree r and where $\kappa>0$. Schmidt [13],[14] and Ru and Wong [11] obtained qualitative finiteness results for classes of decomposable form inequalities much more general than (1.1). However, to obtain explicit upper bounds for the number of solutions of decomposable form inequalities other than (1.1) is a notoriously difficult problem.

2. Results

We start with some notation. The Mahler measure of a polynomial $f = f_0(X-\alpha_1)\cdots(X-\alpha_r)\in\mathbb{C}[X]$ is given by

$$M(f) := |f_0|\prod_{i=1}^{r}\max(1,|\alpha_i|). \tag{2.1}$$

The resultant $R(f,g)$ of two polynomials $f,g\in\mathbb{C}[X]$ is defined as follows: write $f=f_0X^r+f_1X^{r-1}+\cdots+f_r$ with $f_0\neq 0$ and $g=g_0X^t+g_1X^{t-1}+\cdots+g_t$ with $g_0\neq 0$; then

$$R(f,g) := \begin{vmatrix} f_0 & f_1 & \cdots & f_r & & & \\ & \ddots & & & \ddots & & \\ & & & f_0 & f_1 & \cdots & f_r \\ g_0 & \cdots & g_t & & & & \\ & \ddots & & \ddots & & & \\ & & \ddots & & \ddots & & \\ & & & & g_0 & \cdots & g_t \end{vmatrix}, \tag{2.2}$$

where the right-hand side is a determinant of order $r+t$ of which the first t rows consist of coefficients of f and the last r rows of coefficients of g. The resultant $R(f,g)$ is characterized by the fact that $R(f,g)=0$ if and only if f, g have a common zero in $\mathbb{C}$. If

$$f=f_0(X-\alpha_1)\cdots(X-\alpha_r),\ \ g=g_0(X-\zeta_1)\cdots(X-\zeta_t),$$

then

$$(2.3) \qquad R(f,g) = f_0^t g_0^r \prod_{i=1}^{r} \prod_{j=1}^{s} (\alpha_i - \zeta_j)$$
$$= g_0^r f(\zeta_1)\cdots f(\zeta_t) = f_0^t g(\alpha_1)\cdots g(\alpha_r)$$

(see [16, §§34,35]). This implies

$$(2.4) \qquad |R(f,g)| \leqslant 2^{rt} M(f)^t \cdot M(g)^r \, .$$

Now let $f \in \mathbb{Z}[X]$ be a fixed polynomial of degree $r > 0$, let t be a positive integer and let $\kappa > 0$. We consider the inequality

$$(2.5) \qquad 0 < |R(f,g)| \leqslant M(g)^{r-\kappa} \quad \text{in polynomials } g \in \mathbb{Z}[X] \text{ of degree } t.$$

It is trivial that for $r < \kappa$ the number of solutions of (2.5) is finite. So henceforth we assume that $r \geqslant \kappa$.

Wirsing [17] proved that (2.5) has only finitely many solutions if f has no multiple zeros and if $\kappa > 2t\cdot(1+\frac{1}{3}+\cdots+\frac{1}{2t-1})$. Later, Schmidt [14] proved that (2.5) has only finitely many solutions if $\kappa > 2t$ and if f has no multiple zeros and no irreducible factors in $\mathbb{Z}[X]$ of degree $\leqslant t$. Finally, Ru and Wong [11, p. 212, Theorem 4.1] proved a general result on decomposable form inequalities which gives as a special case that (2.5) has only finitely many solutions if $\kappa > 2t$ and if f has no multiple zeros.

On the other hand, Schmidt [14] showed that for every $t \geqslant 1$ there are infinitely many integers r for which there exists a polynomial $f \in \mathbb{Z}[X]$ of degree r such that (2.5) has infinitely many solutions for any $\kappa < 2t$. But Schmidt showed also in [14] that there are polynomials f such that (2.5) has only finitely many solutions already when $\kappa > t+1$.

We now discuss quantitative results which give an explicit upper bound for the number of solutions of (2.5). As we explained in Section 1, we will restrict ourselves to polynomials g which are primitive and irreducible.

In [3] we proved the following result. Let t be a positive integer, f a polynomial in $\mathbb{Z}[X]$ of degree $r > 0$ without multiple zeros and

$$\kappa = (2t+\delta)\big(1+\frac{1}{3}+\cdots+\frac{1}{2t-1}\big) \quad \text{with } 0 < \delta < 1.$$

Then there are at most

$$10^{15}(\delta^{-1})^{t+3}(100r)^t \log 4r \log\log 4r$$

primitive, irreducible polynomials $g \in \mathbb{Z}[X]$ of degree t which satisfy (2.5) and for which

$$M(g) \geqslant \left(2^{8r^2 t} \cdot M(f)^{4(r-1)t}\right)^{\delta^{-1}(1+\frac{1}{3}+\cdots+\frac{1}{2t-1})^{-1}}.$$

We mention that we proved this result by making explicit Wirsing's arguments from [17]. In [3] we suggested the possibility to prove a similar result for $\kappa > 2t$, but this was not possible with Wirsing's method.

In the present paper we prove the following result by means of another approach, based on techniques from the proof of the quantitative Subspace Theorem:

Theorem 2.1. *Let $t \geqslant 1$, $0 < \delta < 1$ and let f be a polynomial in $\mathbb{Z}[X]$ of degree $r \geqslant 2t+1$ without multiple zeros. Then the number of polynomials $g \in \mathbb{Z}[X]$ of degree t such that*

$$0 < |R(f,g)| \leqslant M(g)^{r-2t-\delta}, \tag{2.6}$$

$$g \text{ is primitive and irreducible,} \tag{2.7}$$

$$M(g) \geqslant \left(2^{2r^2} M(f)^{4r-4}\right)^{t/\delta} \tag{2.8}$$

is at most

$$2^{7t+60} \cdot t^{2t+21} \cdot (\delta^{-1})^{t+5} \cdot r^t \log 4r \log\log 4r. \tag{2.9}$$

Remark. Put $C(f) := \left(2^{2r^2} M(f)^{4r-4}\right)^{t/\delta}$. The number of polynomials $g = g_0X^t + \cdots + g_t \in \mathbb{Z}[X]$ of degree t with (2.6), (2.7), $M(g) < C(f)$ may be trivially estimated from above by the number of all polynomials $g \in \mathbb{Z}[X]$ of degree t with $M(g) \leqslant C(f)$. By estimating the latter from above using $M(g) \gg \max(|g_0|, \ldots, |g_t|)$, and then adding (2.9), it follows that the total number of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6), (2.7) is $\ll M(f)^{(4r-4)t(t+1)/\delta}$, where the constants implied by $\ll, \gg$ depend on r, t and δ. We do not know of any better estimate in terms of $M(f)$.

On the other hand, one may show that for any pair of integers $r > t > 0$ and for any $\lambda > 0$ there exists an infinite family of polynomials $f \in \mathbb{Z}[X]$ of degree r, such that the number of primitive, irreducible polynomials $g \in \mathbb{Z}[X]$ of degree t with

$$0 < |R(f,g)| \leqslant M(g)^{\lambda} \tag{2.10}$$

grows polynomially with $M(f)$.

In the construction we use an argument similar to Mueller and Schmidt [9, pp. 331–332]. Fix an irreducible polynomial $f_0 \in \mathbb{Z}[X]$ of degree r. Constants implied by $\ll$, $\gg$ will depend on r, t and f_0. Let b be a sufficiently large integer, and let $0 < \theta < 1$. Put $f(X) := f_0(X+b)$. Take a monic, irreducible polynomial h of degree t in $\mathbb{F}_2[X]$. Let S_b be the set of monic polynomials $g_0 \in \mathbb{Z}[X]$ of degree t with $M(g_0) \leqslant b^{\theta}$ whose reduction modulo 2 is equal to h. Then S_b has cardinality $\gg b^{t\theta}$ and moreover, each $g_0 \in S_b$ is primitive and irreducible. Let T_b be the set of polynomials $g(X) = g_0(X+b)$ with $g_0 \in S_b$. Thus, each $g \in T_b$ is a primitive, irreducible polynomial of degree t. Note that by (2.1) we have

$$M(f) \gg\ll b^r\,, \tag{2.11}$$

$$M(g) \gg\ll b^t \quad \text{for } g \in T_b. \tag{2.12}$$

From (2.11) and the lower bound for the cardinality of S_b mentioned above we infer that T_b has cardinality

$$\gg b^{t\theta} \gg M(f)^{t\theta/r}\,. \tag{2.13}$$

Now let $g \in T_b$. Then by (2.3), (2.4), (2.12) and the fact that f_0 is irreducible we have

$$0 < |R(f,g)| = |R(f_0,g_0)| \ll M(g_0)^r \ll b^{\theta r} \ll M(g)^{\theta r/t}\,,$$

where $g(X) = g_0(X+b)$. By taking θ sufficiently small and then b sufficiently large this implies that each $g \in T_b$ satisfies (2.10). Combining the latter with (2.13), (2.11) and letting $b \to \infty$ our assertion follows.

We now state two corollaries of Theorem 2.1. Our first corollary concerns Thue inequalities such as (1.2) but whose unknowns are algebraic integers of bounded degree. To give the correct formulation we have to introduce the absolute norm and height of an algebraic number.

Denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and by $\overline{\mathcal{O}}$ the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$, i.e., the ring of all algebraic integers. All algebraic numbers occurring in this paper are supposed to belong to $\overline{\mathbb{Q}}$. We define the minimal polynomial of $\zeta \in \overline{\mathbb{Q}}$ to be the primitive, irreducible polynomial f in $\mathbb{Z}[X]$ with positive leading coefficient for which $f(\zeta) = 0$. Then the Mahler measure of ζ is defined by $M(\zeta) := M(f)$. Further, we define the absolute norm and absolute height of ζ by

$$\|\zeta\| := |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta)|^{1/[\mathbb{Q}(\zeta):\mathbb{Q}]}, \quad H(\zeta) := M(\zeta)^{1/[\mathbb{Q}(\zeta):\mathbb{Q}]} .$$

For a binary form $F \in \mathbb{C}[X,Y]$ we put $M(F) := M(f)$ where $f(X) := F(X,1)$. For a pair $(\xi,\eta) \in \overline{\mathcal{O}}^2$ with $\xi\eta \neq 0$ we put $H(\xi,\eta) := H(\xi/\eta)$. Lastly, two pairs (ξ_1,η_1), $(\xi_2,\eta_2) \in \overline{\mathcal{O}}^2$ are said to be proportional if $(\xi_2,\eta_2) = (\lambda\xi_1,\lambda\eta_1)$ for some $\lambda \in \overline{\mathbb{Q}}^*$. Then our result reads as follows:

Corollary 2.2. *Let t be an integer $\geqslant 1$, let $0 < \delta < 1$ and let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $r \geqslant 2t+1$ without multiple factors. Then up to proportionality, there are at most*

$$2^{7t+60} \cdot t^{2t+22} \cdot (\delta^{-1})^{t+5} \cdot r^t \log 4r \log\log 4r \tag{2.14}$$

pairs $(\xi,\eta) \in (\overline{\mathcal{O}}\backslash\{0\})^2$ such that

$$0 < \|F(\xi,\eta)\| \leqslant H(\xi,\eta)^{r-2t-\delta}, \tag{2.15}$$

$$[\mathbb{Q}(\xi/\eta) : \mathbb{Q}] = t, \tag{2.16}$$

$$H(\xi,\eta) \geqslant \left(2^{2r^2} M(F)^{4r-4}\right)^{1/\delta}. \tag{2.17}$$

We now turn to Wirsing systems. For each algebraic number $\zeta \in \overline{\mathbb{Q}}$ of degree t we choose an ordering of its conjugates $\zeta^{(1)},\ldots,\zeta^{(t)}$. A *Wirsing system* is a system of inequalities of the shape

$$|\alpha_i - \zeta^{(i)}| \leqslant M(\zeta)^{-\varphi_i} \quad (i \in I) \quad \text{in algebraic numbers } \zeta \text{ of degree } t, \tag{2.18}$$

where I is a subset of $\{1,\ldots,t\}$, α_i $(i \in I)$ are algebraic numbers, and φ_i $(i \in I)$ non-negative reals. A particular instance of (2.18) is

$$|\alpha - \zeta| \leqslant M(\zeta)^{-\varphi} \quad \text{in algebraic numbers } \zeta \text{ of degree } t, \tag{2.19}$$

where α is a fixed algebraic number and φ a non-negative real. Wirsing [17] showed that (2.19) has only finitely many solutions if $\varphi > 2t$ and later Schmidt [12] proved the same for $\varphi > t+1$. In his paper [17], Wirsing showed also that (2.18) has only finitely many solutions if $\sum_{i\in I}\varphi_i > 2t\cdot\left(\sum_{k=1}^{\#I}\frac{1}{2k-1}\right)$. Hirata-Kohno and the author [4] showed that (2.18) has only finitely many solutions already when $\sum_{i\in I}\varphi_i > 2t$. Furthermore they gave examples of tuples $(\alpha_i : i \in I)$ with the property that for any $\varepsilon > 0$ there is a tuple $(\varphi_i : i \in I)$ with $\sum_{i\in I}\varphi_i = 2t-\varepsilon$ such that (2.18) has infinitely many solutions.

In [3] we showed that if

$$\max_{i\in I} M(\alpha_i) \leqslant M, \quad [\mathbb{Q}(\alpha_i : i \in I) : \mathbb{Q}] \leqslant R,$$

$$\sum_{i\in I}\varphi_i \geqslant (2t+\delta)\sum_{k=1}^{\#I}\tfrac{1}{2k-1} \quad \text{with } 0<\delta<1,$$

then (2.18) has at most

$$2\times 10^7\cdot t^7\delta^{-4}\log 4R\log\log 4R \tag{2.20}$$

solutions with $M(\zeta) \geqslant \max\left(M, 4^{t(t+1)/(\sum_{i\in I}\varphi_i-2t)}\right)$. We mention that independently Locher [8] obtained a similar upper bound for the number of solutions of (2.19).

From Theorem 2.1 we deduce the following:

Corollary 2.3. *Let t be a positive integer, let $f\in\mathbb{Z}[X]$ be a polynomial of degree $r\geqslant 2t+1$ with only distinct zeros, let I be a subset of $\{1,\dots,t\}$, let α_i $(i\in I)$ be not necessarily distinct zeros of f and let φ_i $(i\in I)$ be non-negative reals with*

$$\sum_{i\in I}\varphi_i \geqslant 2t+\delta \quad \textit{with } 0<\delta<1. \tag{2.21}$$

Then there are at most

$$2^{8t+66}\cdot t^{2t+22}\cdot(\delta^{-1})^{t+5}\cdot r^t\log 4r\log\log 4r \tag{2.22}$$

algebraic numbers ζ of degree t satisfying

$$|\alpha_i-\zeta^{(i)}| \leqslant M(\zeta)^{-\varphi_i} \quad \textit{for } i\in I, \tag{2.23}$$

$$M(\zeta) \geqslant \max\left(M(f), 4^{t(t+1)/\delta}\right). \tag{2.24}$$

It should be noted that the upper bound (2.22) is much worse than (2.20). Hirata-Kohno discovered another method to estimate from above the number of algebraic numbers ζ of degree t with (2.23), (2.24), based on ideas of Ru and Wong [11] and on techniques used in the proof of the quantitative Subspace Theorem. This is work in preparation; see [6].

We conclude this section with some comments on the proof of Theorem 2.1. With each primitive, irreducible polynomial g of degree t with (2.6)-(2.8) we associate a symmetric convex body $\mathcal{C}(g) \subset \mathbb{R}^{t+1}$. Let $\lambda_1, \dots, \lambda_{t+1}$ be the successive minima of this body. Following the standard method of proof of the Subspace Theorem one shows first that there is an index $k \in \{1, \dots, t\}$ such that λ_k/λ_{k+1} is small in terms of $M(g)$, and next that there is a k-dimensional vector space which contains g and which belongs to a finite collection which is independent of g. Moreover, by making all arguments explicit one may compute an explicit upper bound for the cardinality of this collection of k-dimensional spaces.

We show that in the particular case considered in this paper we can take $k = 1$. More precisely, by an argument heavily depending on properties of resultants we show in an explicit form, that λ_1/λ_2 is small in terms of $M(g)$. Then using the Subspace machinery we prove that each primitive, irreducible polynomial g of degree t with (2.6)-(2.8) is contained in a one-dimensional vector space belonging to a finite collection independent of g, and moreover we obtain an explicit upper bound for the cardinality of this collection. Since each such one-dimensional space contains at most two primitive polynomials, this gives an explicit upper bound for the number of primitive, irreducible polynomials of degree t satisfying (2.6)-(2.8).

3. Preliminaries

For a polynomial $F \in \mathbb{C}[X_1, \dots, X_n]$, put

$$\|F\|_1 := \sum_{i=1}^{s} |c_i|$$

where $c_1, \dots, c_s$ are the non-zero coefficients of F. It is easy to check that

$$\|F+G\|_1 \leqslant \|F\|_1 + \|G\|_1, \quad \|F \cdot G\|_1 \leqslant \|F\|_1 \cdot \|G\|_1 \quad \text{for } F, G \in \mathbb{C}[X_1, \dots, X_n]. \tag{3.1}$$

Let $f = f_0(X-\alpha_1)\cdots(X-\alpha_r) \in \mathbb{C}[X]$. The Mahler measure $M(f)$ is defined by (2.1) and the discriminant of f by

$$D(f) := f_0^{2r-2} \prod_{1\leqslant i<j\leqslant r} (\alpha_i-\alpha_j)^2.$$

We will use that

$$|D(f)|^{1/2} M(f)^{1-r} = \prod_{1\leqslant i<j\leqslant r} \frac{|\alpha_i-\alpha_j|}{\max(1,|\alpha_i|)\max(1,|\alpha_j|)} \tag{3.2}$$

(note that the factors $|f_0|^{r-1}$ in the numerator and denominator cancel each other). Since

$$|\alpha_i-\alpha_j| \leqslant 2\max(1,|\alpha_i|)\max(1,|\alpha_j|)$$

this implies

$$|D(f)| \leqslant 2^{r(r-1)} M(f)^{2r-2}. \tag{3.3}$$

Moreover, for any subset I of $\{(i,j) : i,j = 1,\dots,r,\ i<j\}$ we have

$$\prod_{(i,j)\in I} \frac{|\alpha_i-\alpha_j|}{\max(1,|\alpha_i|)\max(1,|\alpha_j|)} \geqslant 2^{(\#I)-\frac{r(r-1)}{2}} |D(f)|^{1/2} M(f)^{1-r}. \tag{3.4}$$

From the arguments in for instance [7, p. 60] it follows easily that for polynomials $f \in \mathbb{C}[X]$ of degree r we have

$$\|f\|_1 \leqslant 2^r M(f), \quad M(f) \leqslant \|f\|_1. \tag{3.5}$$

Moreover,

$$M(fg) = M(f)M(g) \quad \text{for } f,g \in \mathbb{C}[X]. \tag{3.6}$$

We now prove some more elaborate results.

Lemma 3.1. *Let $f \in \mathbb{C}[X]$ be a polynomial of degree r without multiple zeros. Let $\alpha_1,\dots,\alpha_{t+1}$ be distinct zeros of f where $t<r$. Then there are linear forms*

$C_i = \sum_{j=1}^{t+1} c_{ij} X_j$ $(i = 0, \ldots, t)$ with

$$\text{(3.7)} \qquad |c_{ij}| \leqslant \binom{t}{i} \cdot 2^{\frac{r(r-1)}{2}-t} \cdot M(f)^{r-1} \cdot |D(f)|^{-1/2}$$
$$\text{for } i = 0, \ldots, t,\ j = 1 \ldots t+1,$$

$$\text{(3.8)} \qquad \|C_i\|_1 \leqslant (t+1) \cdot 2^{\frac{r(r-1)}{2}-1} \cdot M(f)^{r-1} \cdot |D(f)|^{-1/2} \quad \text{for } i = 0, \ldots, t,$$

such that for every polynomial $g = g_0 X^t + g_1 X^{t-1} + \cdots + g_t \in \mathbb{C}[X]$ of degree $\leqslant t$ we have

$$\text{(3.9)} \qquad g_i = C_i(g(\alpha_1), \ldots, g(\alpha_{t+1})) \quad \text{for } i = 0, \ldots, t.$$

Proof. Let $g = g_0 X^t + g_1 X^{t-1} + \cdots + g_t \in \mathbb{C}[X]$ be any polynomial of degree $\leqslant t$. Then Lagrange's interpolation formula gives

$$g = \sum_{j=1}^{t+1} g(\alpha_j) \prod_{k=1,\, k\neq j}^{t+1} \left(\frac{X - \alpha_k}{\alpha_j - \alpha_k} \right).$$

Take $C_i = \sum_{j=1}^{t+1} c_{ij} X_j$ where c_{ij} is the coefficient of X^i in $\prod_{k=1,k\neq j}^{t+1} (X - \alpha_k)/(\alpha_j - \alpha_k)$. Then clearly, (3.9) is satisfied. Furthermore, by (3.4) we have

$$\begin{aligned} |c_{ij}| &\leqslant \binom{t}{i} \prod_{k=1,\, k\neq j}^{t+1} \frac{\max(1, |\alpha_j|) \max(1, |\alpha_k|)}{|\alpha_j - \alpha_k|} \\ &\leqslant \binom{t}{i} 2^{\frac{r(r-1)}{2}-t} M(f)^{r-1} |D(f)|^{-1/2} \end{aligned}$$

for $i = 0, \ldots, t$ and $j = 1, \ldots, t+1$. This proves (3.7). Inequality (3.8) is an immediate consequence of (3.7). □

Lemma 3.2. *Let $f = f_0(X - \alpha_1) \cdots (X - \alpha_r) \in \mathbb{C}[X]$ where $f_0 \neq 0$ and where $\alpha_1, \ldots, \alpha_r$ are distinct. Further, let $t < r$ and let $g = g_0 X^t + g_1 X^{t-1} + \cdots + g_t \in \mathbb{C}[X]$*

be a polynomial of degree t. Suppose that $|g(\alpha_1)| \leqslant |g(\alpha_2)| \leqslant \cdots \leqslant |g(\alpha_r)|$. Then

$$|g(\alpha_i)| \leqslant M(g)\cdot 2^t \max(1,|\alpha_i|)^t \quad \text{for } i=1,\dots,r, \tag{3.10}$$

$$|g(\alpha_i)| \geqslant M(g)\cdot (t+1)^{-1}\cdot 2^{\frac{-r(r-1)}{2}}\cdot |D(f)|^{1/2}M(f)^{1-r} \quad \text{for } i=t+1,\dots,r, \tag{3.11}$$

$$\prod_{i\in I}|g(\alpha_i)| \geqslant 2^{-t((\#I)-r)}|R(f,g)|\cdot M(f)^{-t}\cdot M(g)^{(\#I)-r} \quad \text{for each subset } I \text{ of } \{1,\dots,r\}. \tag{3.12}$$

Proof. It is obvious that $|g(\alpha_i)| \leqslant \|g\|_1 \max(1,|\alpha_i|)^t$ for $i=1,\dots,t$. By combining this with (3.5) we obtain (3.10).

It clearly suffices to prove (3.11) for $i=t+1$. Let $C_0,\dots,C_t$ be the linear forms from Lemma 3.1. Then by (3.5), (3.9), (3.7) we have

$$\begin{aligned} M(g) &\leqslant \|g\|_1 = \sum_{i=0}^{t}|g_i| \leqslant \Big(\sum_{i=0}^{t}\sum_{j=1}^{t+1}|c_{ij}|\Big)\cdot|g(\alpha_{t+1})| \\ &\leqslant (t+1)\Big(\sum_{i=0}^{t}\binom{t}{i}\Big)2^{\frac{r(r-1)}{2}-t}\cdot\frac{M(f)^{r-1}}{|D(f)|^{1/2}}\cdot|g(\alpha_{t+1})| \\ &= (t+1)\cdot 2^{\frac{r(r-1)}{2}}\cdot\frac{M(f)^{r-1}}{|D(f)|^{1/2}}\cdot|g(\alpha_{t+1})| \end{aligned}$$

which implies (3.11).

From (2.3), (3.10) we obtain

$$\begin{aligned} \prod_{i\in I}|g(\alpha_i)| &\geqslant |R(f,g)|\cdot\Big(|f_0|^t\prod_{i\notin I}|g(\alpha_i)|\Big)^{-1} \\ &\geqslant |R(f,g)|\cdot\Big(|f_0|^t 2^{t(r-(\#I))}M(g)^{r-(\#I)}\prod_{i\notin I}\max(1,|\alpha_i|)^t\Big)^{-1} \\ &\geqslant |R(f,g)|\cdot\Big(2^{t(r-(\#I))}M(g)^{r-(\#I)}M(f)^t\Big)^{-1} \end{aligned}$$

which implies (3.12). $\square$

Lemma 3.3. *Let r, t be positive integers with $r \geqslant 2t+1$. Let $f = f_0(X-\alpha_1)\cdots(X-\alpha_r) \in \mathbb{C}[X]$ where $f_0 \neq 0$ and $\alpha_1, \ldots, \alpha_r$ are distinct. Further, let $g \in \mathbb{C}[X]$ be a polynomial of degree t with leading coefficient g_0 and let $h \in \mathbb{C}[X]$ be a non-zero polynomial of degree $m \leqslant t$. Then*

$$
\begin{aligned}
(3.13)\quad |R(g,h)| \leqslant\ & 2^{\frac{1}{2}r^3} \cdot |f_0|^{-t} \cdot M(f)^{r(r-1)} \cdot |D(f)|^{-r/2} \times \\
& \times |R(f,g)| \cdot |g_0|^{m-t} M(g)^{2t-r} \cdot \left(\max\left(1, \frac{|h(\alpha_1)|}{|g(\alpha_1)|}, \ldots, \frac{|h(\alpha_r)|}{|g(\alpha_r)|}\right)\right)^t .
\end{aligned}
$$

Proof. Without loss of generality we may assume that

$$
|g(\alpha_1)| \leqslant |g(\alpha_2)| \leqslant \cdots \leqslant |g(\alpha_r)|. \tag{3.14}
$$

Put

$$
\lambda := \max\left(1, \frac{|h(\alpha_1)|}{|g(\alpha_1)|}, \ldots, \frac{|h(\alpha_r)|}{|g(\alpha_r)|}\right). \tag{3.15}
$$

From Lagrange's interpolation formula we infer

$$
g = \sum_{i=1}^{t+1} y_i \prod_{j=1, j\neq i}^{t+1} \Big(\frac{X-\alpha_j}{\alpha_i - \alpha_j}\Big), \quad h = \sum_{i=1}^{t+1} z_i \prod_{j=1, j\neq i}^{t+1} \Big(\frac{X-\alpha_j}{\alpha_i - \alpha_j}\Big) \tag{3.16}
$$

with

$$
y_i = g(\alpha_i), \quad z_i = h(\alpha_i) \quad (i = 1, \ldots, t+1). \tag{3.17}
$$

Write

$$
g = g_0 X^t + g_1 X^{t-1} + \cdots + g_t, \quad h = h_0 X^t + h_1 X^{t-1} + \cdots + h_t
$$

where $g_0 \neq 0$, $h_{t-m} \neq 0$ and $h_i = 0$ for $i > t-m$. Thus $g_i = C_i(\mathbf{y})$, $h_i = C_i(\mathbf{z})$ for $i = 0, \ldots, t$ where $C_0, \ldots, C_t$ are the linear forms from Lemma 3.1 and where $\mathbf{y} = (y_1, \ldots, y_{t+1})$, $\mathbf{z} = (z_1, \ldots, z_{t+1})$.

If $m = t$, i.e., $h_0 \neq 0$, we can express $R(g,h)$ as a determinant of order $2t$ of the shape (2.2), with $g_0, \ldots, g_t$ on the first t rows and $h_0, \ldots, h_t$ on the last t rows. It is easy to check that for arbitrary $m \leqslant t$ we have

$$g_0^{t-m}R(g,h) = \begin{vmatrix} g_0 & \cdots & g_t & & \\ & \ddots & & \ddots & \\ & & g_0 & \cdots & g_t \\ h_0 & \cdots & h_t & & \\ & \ddots & & \ddots & \\ & & h_0 & \cdots & h_t \end{vmatrix},$$

where the first t rows consist of coefficients of g and the last t rows of coefficients of h. Hence

$$g_0^{t-m}R(g,h) = U(\mathbf{y},\mathbf{z}) := \begin{vmatrix} C_0(\mathbf{y}) & \cdots & C_t(\mathbf{y}) & & \\ & \ddots & & \ddots & \\ & & C_0(\mathbf{y}) & \cdots & C_t(\mathbf{y}) \\ C_0(\mathbf{z}) & \cdots & C_t(\mathbf{z}) & & \\ & \ddots & & \ddots & \\ & & C_0(\mathbf{z}) & \cdots & C_t(\mathbf{z}) \end{vmatrix}. \tag{3.18}$$

By expanding U we get a polynomial expression

$$U(\mathbf{y},\mathbf{z}) = \sum_{(\mathbf{a},\mathbf{b})\in I} c(\mathbf{a},\mathbf{b}) y_1^{a_1}\cdots y_{t+1}^{a_{t+1}} z_1^{b_1}\cdots z_{t+1}^{b_{t+1}}, \tag{3.19}$$

where the sum is taken over a finite set I of tuples of non-negative integers $(\mathbf{a},\mathbf{b}) = (a_1,\dots,a_{t+1},b_1,\dots,b_{t+1})$ with

$$a_1+\cdots+a_{t+1} = t, \quad b_1+\cdots+b_{t+1} = t \tag{3.20}$$

and where $c(\mathbf{a},\mathbf{b}) \in \mathbb{C}\backslash\{0\}$ for $(\mathbf{a},\mathbf{b}) \in I$. Moreover, we have

$$a_i + b_i \geqslant 1 \quad \text{for } i = 1,\dots,t+1,\ (\mathbf{a},\mathbf{b}) \in I. \tag{3.21}$$

To prove this we view $y_1,\dots,y_{t+1},z_1,\dots,z_{t+1}$ for a while as indeterminates. Pick $i \in \{1,\dots,t+1\}$ and substitute $y_i = 0$, $z_i = 0$ in U. Then by (3.17) we have $g(\alpha_i) = 0$, $h(\alpha_i) = 0$ which implies $U(\mathbf{y},\mathbf{z}) = g_0^{t-m}R(g,h) = 0$. So by substituting $y_i = 0$, $z_i = 0$ in U we obtain a polynomial which is identically 0. Therefore, each monomial of U must contain at least one of the variables y_i, z_i. This implies (3.21).

We first estimate from above $|y_1^{a_1}\cdots y_{t+1}^{a_{t+1}}z_1^{b_1}\cdots z_{t+1}^{b_{t+1}}|$ for $(\mathbf{a},\mathbf{b})\in I$. We have

$$\begin{aligned}
&|y_1^{a_1}\cdots y_{t+1}^{a_{t+1}}z_1^{b_1}\cdots z_{t+1}^{b_{t+1}}|\\
&\quad\leqslant \lambda^{b_1+\cdots+b_{t+1}}|g(\alpha_1)|^{a_1+b_1}\cdots|g(\alpha_{t+1})|^{a_{t+1}+b_{t+1}}\quad\text{by (3.17),(3.15)}\\
&\quad\leqslant \lambda^t|g(\alpha_1)\cdots g(\alpha_{t+1})|\cdot|g(\alpha_{t+1})|^{(a_1+b_1)+\cdots+(a_t+b_t)-t-1}\quad\text{by (3.20),(3.21),(3.14)}\\
&\quad= \lambda^t|g(\alpha_1)\cdots g(\alpha_{t+1})|\cdot|g(\alpha_{t+1})|^{t-1}\quad\text{by (3.20)}\\
&\quad\leqslant \lambda^t|g(\alpha_1)\cdots g(\alpha_{2t})|\quad\text{by (3.14)}\\
&\quad\leqslant \lambda^t\left((t+1)\cdot 2^{\frac{r(r-1)}{2}}\cdot\frac{M(f)^{r-1}}{|D(f)|^{1/2}}\right)^{r-2t}|g(\alpha_1)\cdots g(\alpha_r)|\cdot M(g)^{2t-r}
\end{aligned}$$

by (3.14), (3.11), and finally

$$\begin{aligned}
&|y_1^{a_1}\cdots y_{t+1}^{a_{t+1}}z_1^{b_1}\cdots z_{t+1}^{b_{t+1}}|\\
&\quad\leqslant\left((t+1)\cdot 2^{\frac{r(r-1)}{2}}\cdot\frac{M(f)^{r-1}}{|D(f)|^{1/2}}\right)^{r-2t}|f_0|^{-t}|R(f,g)|\cdot M(g)^{2t-r}\cdot\lambda^t
\end{aligned}\tag{3.22}$$

by (2.3).

It remains to estimate the coefficients of U. By repeatedly applying (3.1), using that the determinantal expression (3.18) for U is the sum of $(t+1)^{2t}$ products each consisting of t terms $C_i(\mathbf{y})$ and t terms $C_i(\mathbf{z})$ and then inserting (3.8) we obtain

$$\begin{aligned}
\|U\|_1 &\leqslant (t+1)^{2t}\Big(\max_{0\leqslant k\leqslant t}\|C_k\|_1\Big)^{2t}\\
&\leqslant \Big((t+1)^2\cdot 2^{\frac{r(r-1)}{2}-1}\cdot M(f)^{r-1}\cdot|D(f)|^{-1/2}\Big)^{2t}.
\end{aligned}$$

Together with (3.18), (3.19), (3.22), $r\geqslant 2t+1\geqslant 3$ this implies

$$\begin{aligned}
&|g_0|^{t-m}|R(g,h)|=|U(\mathbf{y},\mathbf{z})|\leqslant\|U\|_1\cdot\max_{(\mathbf{a},\mathbf{b})\in I}|y_1^{a_1}\cdots y_{t+1}^{a_{t+1}}z_1^{b_1}\cdots z_{t+1}^{b_{t+1}}|\\
&\quad\leqslant\Big((t+1)^2 2^{\frac{r(r-1)}{2}-1}M(f)^{r-1}\cdot|D(f)|^{-1/2}\Big)^r\cdot|f_0|^{-t}|R(f,g)|\cdot M(g)^{2t-r}\cdot\lambda^t\\
&\quad< 2^{\frac{1}{2}r^3}\left(M(f)^{r-1}\cdot|D(f)|^{-1/2}\right)^r|f_0|^{-t}|R(f,g)|\cdot M(g)^{2t-r}\cdot\lambda^t.
\end{aligned}$$

This proves Lemma 3.3. □

4. Geometry of numbers

In what follows, t, r are positive integers with $r \geqslant 2t+1$, δ is a real with $0 < \delta < 1$ and

$$f = f_0X^r + f_1X^{r-1} + \cdots + f_r = f_0(X-\alpha_1)\cdots(X-\alpha_r) \in \mathbb{Z}[X]$$

is a polynomial for which $f_0 \neq 0$ and $\alpha_1, \ldots, \alpha_r$ are distinct.

In what follows we fix a polynomial $g = g_0X^t + g_1X^{t-1} + \cdots + g_t \in \mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7) and, instead of (2.8), the stronger condition

$$M(g) \geqslant 2^{16r^5/\delta} M(f)^{16r^4/\delta}. \tag{4.1}$$

Define the quantity $\xi = \xi(g)$ by

$$|R(f,g)| = M(g)^{r-2t-\xi}. \tag{4.2}$$

Then (2.6) implies

$$\xi \geqslant \delta\,. \tag{4.3}$$

We associate with g a set of indices $\{i_1, \ldots, i_{t+1}\} \subset \{1, \ldots, r\}$ such that

$$\begin{cases} |g(\alpha_{i_1})|, \ldots, |g(\alpha_{i_t})| \text{ are the } t \text{ smallest values among } |g(\alpha_1)|, \ldots, |g(\alpha_r)|, \\ i_1 < i_2 < \ldots < i_t, \\ i_{t+1} \text{ is the smallest index from } \{1, \ldots, r\} \backslash \{i_1, \ldots, i_t\}. \end{cases} \tag{4.4}$$

Notice that i_{t+1} is determined by $i_1, \ldots, i_t$. Thus, when g varies then $\{i_1, \ldots, i_{t+1}\}$ runs through a collection of subsets of $\{1, \ldots, r\}$ of cardinality at most $\binom{r}{t}$.

Further we define linear forms

$$L_i = \alpha_i^t X_0 + \alpha_i^{t-1} X_1 + \cdots + X_t \quad (i = 1, \ldots, r). \tag{4.5}$$

Thus if $\mathbf{h} = (h_0, \ldots, h_t)$ is the coefficient vector of a polynomial $h = h_0X^t + \cdots + h_t$ of degree $\leqslant t$ we have

$$L_i(\mathbf{h}) = h(\alpha_i) \quad \text{for } i = 1, \ldots, r. \tag{4.6}$$

With the polynomial g chosen above we associate the set

$$\mathcal{C}(g) := \{\mathbf{x} \in \mathbb{R}^{t+1} : |L_i(\mathbf{x})| \leqslant |g(\alpha_i)| \text{ for } i = 1, \ldots, r\}\,. \tag{4.7}$$

It is easy to show that $\mathcal{C}(g)$ is a compact, convex subset of $\mathbb{R}^{t+1}$ which is symmetric about $\mathbf{0}$. We shall prove below that $\mathcal{C}(g)$ has positive volume. Notice that if $\mathbf{g} = (g_0, \dots, g_t)$ is the coefficient vector of g then $\mathbf{g} \in \mathcal{C}(g)$.

We denote by

$$\lambda_1 = \lambda_1(g), \dots, \lambda_{t+1} = \lambda_{t+1}(g)$$

the successive minima of $\mathcal{C}(g)$. Further, let $\mathbf{h}_1 = \mathbf{h}_1(g), \dots, \mathbf{h}_{t+1} = \mathbf{h}_{t+1}(g)$ be linearly independent vectors in $\mathbb{Z}^{t+1}$ with $\mathbf{h}_i \in \lambda_i \mathcal{C}(g)$ for $i = 1, \dots, t+1$. Thus

$$|L_i(\mathbf{h}_j)| \leqslant \lambda_j \cdot |g(\alpha_i)| \quad \text{for } i = 1, \dots, r;\ j = 1, \dots, t+1. \tag{4.8}$$

One may show that $\mathrm{vol}(\mathcal{C}(g)) \gg\ll |g(\alpha_{i_1}) \cdots g(\alpha_{i_{t+1}})|$ where $\mathrm{vol}(\mathcal{C}(g))$ denotes the volume of $\mathcal{C}(g)$, $\{i_1, \dots, i_{t+1}\}$ is the set of indices defined by (4.4) and where the constants implied by $\gg$, $\ll$ depend on f. Then Minkowski's theorem on successive minima of convex bodies implies that $|g(\alpha_{i_1}) \cdots g(\alpha_{i_{t+1}})| \cdot \lambda_1 \cdots \lambda_{t+1} \gg\ll 1$. We will prove a more precise version of this estimate below. As a preparation we need the following:

Lemma 4.1. *Let $\{L_{j_1}, \dots, L_{j_{t+1}}\}$ be a linearly independent subset of $\{L_1, \dots, L_r\}$. Then*

$$2^{(t(t+1)-r(r-1))/2} M(f)^{1-r} \leqslant |\det(L_{j_1}, \dots, L_{j_{t+1}})| \leqslant 2^{t(t+1)/2} M(f)^t. \tag{4.9}$$

Proof. Put $D := |\det(L_{j_1}, \dots, L_{j_{t+1}})|$. By Vandermonde's indentity we have $D = \prod_{1 \leqslant k < l \leqslant t+1} |\alpha_{j_k} - \alpha_{j_l}|$. This implies on the one hand, noting that the leading coefficient f_0 of f is a non-zero integer,

$$\begin{aligned} D &\leqslant \prod_{1 \leqslant k < l \leqslant t+1} \Big(2 \max(1, |\alpha_{j_k}|) \max(1, |\alpha_{j_l}|) \Big) \\ &= 2^{t(t+1)/2} \Big(\prod_{k=1}^{t+1} \max(1, |\alpha_{j_k}|) \Big)^t \leqslant 2^{t(t+1)/2} M(f)^t \end{aligned}$$

and on the other hand, by (3.4),

$$\begin{aligned} D &\geqslant \prod_{1 \leqslant k < l \leqslant t+1} \frac{|\alpha_{j_k} - \alpha_{j_l}|}{\max(1, |\alpha_{j_k}|) \max(1, |\alpha_{j_l}|} \geqslant 2^{(t(t+1)-r(r-1))/2} |D(f)|^{1/2} M(f)^{1-r} \\ &\geqslant 2^{(t(t+1)-r(r-1))/2} M(f)^{1-r} \end{aligned}$$

where we have used that $D(f)$ is a non-zero integer. $\square$

Lemma 4.2. *Let $\{i_1,\dots,i_{t+1}\}$ be the set of indices defined by (4.4). Then*

$$2^{-r^2/2}M(f)^{1-r}\leqslant|g(\alpha_{i_1})\cdots g(\alpha_{i_{t+1}})|\cdot\lambda_1\cdots\lambda_{t+1}\leqslant 2^{2r^2}M(f)^{2r}. \tag{4.10}$$

Proof. Put $\Lambda:=|g(\alpha_{i_1})\cdots g(\alpha_{i_{t+1}})|\cdot\lambda_1\cdots\lambda_{t+1}$. We first deduce the lower bound for Λ. Notice that the determinant $\det(L_{i_j}(\mathbf{h}_k))_{j,k=1,\dots,t+1}$ is the sum of $(t+1)!$ terms of the shape $\pm\prod_{j=1}^{t+1}L_{i_j}(\mathbf{h}_{\sigma(j)})$ where σ is a permutation of $1,\dots,t+1$. By (4.8), each such term has absolute value at most $\prod_{j=1}^{t+1}\big(|g(\alpha_{i_j})|\lambda_{\sigma(j)}\big)=\Lambda$. Together with Lemma 4.1 this implies

$$\begin{aligned}1 &\leqslant |\det(\mathbf{h}_1,\dots,\mathbf{h}_{t+1})|=|\det(L_{i_1},\dots,L_{i_{t+1}})|^{-1}\cdot|\det(L_{i_j}(\mathbf{h}_k))_{j,k=1,\dots,t+1}|\\ &\leqslant 2^{(r(r-1)-t(t+1))/2)}M(f)^{r-1}\cdot(t+1)!\cdot\Lambda\\ &\leqslant 2^{r^2/2}M(f)^{r-1}\Lambda\end{aligned}$$

from which the lower bound for Λ immediately follows.

We now prove the upper bound for Λ. Assume, as we may, that $\alpha_1,\dots,\alpha_{r_1}$ are real numbers and that $\alpha_{r_1+1},\dots,\alpha_r$ are non-real, where $r=r_1+2r_2$ and $\alpha_{i+r_2}=\overline{\alpha_i}$ for $i=r_1+1,\dots,r_1+r_2$. Let $\tilde{L}_i:=|g(\alpha_i)|^{-1}L_i$ for $i=1,\dots,r$. Then there are linear forms $M_1,\dots,M_r$ in $t+1$ variables with real coefficients such that

$$\left\{\begin{array}{rcl}\tilde{L}_i &=& M_i\quad(i=1,\dots,r_1)\\ \tilde{L}_i &=& M_i+\sqrt{-1}\cdot M_{i+r_2}\quad(i=r_1+1,\dots,r_1+r_2),\\ \tilde{L}_{i+r_2} &=& M_i-\sqrt{-1}\cdot M_{i+r_2}\quad(i=r_1+1,\dots,r_1+r_2).\end{array}\right. \tag{4.11}$$

Clearly, if for some $\mathbf{x}\in\mathbb{R}^{t+1}$ we have $|M_i(\mathbf{x})|\leqslant 2^{-1/2}$ for $i=1,\dots,r$ then $|\tilde{L}_i(\mathbf{x})|\leqslant 1$, whence $|L_i(\mathbf{x})|\leqslant|g(\alpha_i)|$ for $i=1,\dots,r$. Therefore,

$$\mathcal{C}(g)\supseteq\mathcal{D}_0:=\{\mathbf{x}\in\mathbb{R}^{t+1}:\ |M_i(\mathbf{x})|\leqslant 2^{-1/2}\text{ for }i=1,\dots,r\}. \tag{4.12}$$

By $\operatorname{rank}\{L_1,\dots,L_r\}=t+1$ and (4.11) we have $\operatorname{rank}\{M_1,\dots,M_r\}=t+1$. Let $j_1,\dots,j_{t+1}$ be indices for which $\Delta:=|\det(M_{j_1},\dots,M_{j_{t+1}})|$ is maximal. Then $\Delta>0$ and therefore $M_1,\dots,M_r$ are linear combinations of $M_{j_1},\dots,M_{j_{t+1}}$. Write

$$M_i=\sum_{k=1}^{t+1}c_{ik}M_{j_k}\quad\text{for }i=1,\dots,r.$$

For $k=1,\dots,t+1$ and for any linear form L in $t+1$ variables, let $\Delta_k(L)$ be the absolute value of the determinant obtained by replacing M_{i_k} by L in the determinant $\det(M_{i_1},\dots,M_{i_{t+1}})$. By Cramer's rule, (4.11), and the choice of $j_1,\dots,j_{t+1}$, we have

$$|c_{ik}| = \Delta_k(M_i)/\Delta \leqslant 1 \quad \text{for } i=1,\dots,r.$$

Hence if for some $\mathbf{x}\in\mathbb{R}^{t+1}$ we have $|M_{j_k}(\mathbf{x})| \leqslant 2^{-1/2}(t+1)^{-1}$ for $k=1,\dots,t+1$, then $|M_i(\mathbf{x})| \leqslant 2^{-1/2}$ for $i=1,\dots,r$. Together with (4.12) this implies

$$\mathcal{C}(g) \supseteq \mathcal{D}_0 \supseteq \mathcal{D} := \{\mathbf{x}\in\mathbb{R}^{t+1} : |M_{j_k}(\mathbf{x})| \leqslant 2^{-1/2}(t+1)^{-1} \text{ for } k=1,\dots,t+1\}$$

and therefore, the volume of $\mathcal{C}(g)$ is bounded from below by

$$\mathrm{vol}\,(\mathcal{C}(g)) \geqslant \mathrm{vol}\,(\mathcal{D}) = 2^{(t+1)/2}(t+1)^{-t-1}\Delta^{-1}.$$

Now Minkowski's theorem on successive minima implies that

$$\lambda_1\cdots\lambda_{t+1} \leqslant 2^{t+1}(\mathrm{vol}\,(\mathcal{C}(g)))^{-1} \leqslant \left(\sqrt{2}(t+1)\right)^{t+1}\Delta\,. \tag{4.13}$$

We estimate Δ from above. Assume that among $\{j_1,\dots,j_{t+1}\}$ there are precisely s indices $>r_1$. By (4.11) we have $M_i=\tilde{L}_i$ for $i=1,\dots,r_1$, $M_i=\frac{1}{2}(\tilde{L}_i+\tilde{L}_{i+r_2})$ for $i=r_1+1,\dots,r_2$, $M_i=\frac{1}{2\sqrt{-1}}(\tilde{L}_{i-r_2}-\tilde{L}_i)$ for $i=r_1+r_2+1,\dots,r$, therefore,

$$\det(M_{j_1},\dots,M_{j_{t+1}}) = \sum_{K=(k_1,\dots,k_{t+1})} \varepsilon_K \det(\tilde{L}_{k_1},\dots,\tilde{L}_{k_{t+1}})$$

where the sum is taken over all 2^s tuples $K=(k_1,\dots,k_{t+1})$ such that $k_h=j_h$ if $1\leqslant j_h\leqslant r_1$, $k_h\in\{j_h,j_h+r_2\}$ if $r_1+1\leqslant j_h\leqslant r_1+r_2$ and $k_h\in\{j_h-r_2,j_h\}$ if $r_1+r_2+1\leqslant j_h\leqslant r$, and where $|\varepsilon_K|=2^{-s}$ for each of these tuples K. Therefore, there is a tuple $K=(k_1,\dots,k_{t+1})$ such that $\Delta\leqslant|\det(\tilde{L}_{k_1},\dots,\tilde{L}_{k_{t+1}})|$. By (3.10), (3.11) (with $\{i_1,\dots,i_t\}$ in place of $\{1,\dots,t\}$) we have for any two indices $j,k\in\{1,\dots,r\}\backslash\{i_1,\dots,i_t\}$,

$$|g(\alpha_j)| \leqslant 2^t\cdot(t+1)\cdot 2^{r(r-1)/2}M(f)^r\cdot|g(\alpha_k)|$$

and so by (4.4),

$$|g(\alpha_{i_1})\cdots g(\alpha_{i_{t+1}})| \leqslant 2^t\cdot(t+1)\cdot 2^{r(r-1)/2}M(f)^r\cdot|g(\alpha_{k_1})\cdots g(\alpha_{k_{t+1}})|\,.$$

Together with Lemma 4.1 this implies

$$\begin{aligned}\Delta &\leqslant |\det(\tilde{L}_{k_1},\dots,\tilde{L}_{k_{t+1}})| = |\det(L_{k_1},\dots,L_{k_{t+1}})|\cdot|g(\alpha_{k_1})\cdots g(\alpha_{k_{t+1}})|^{-1}\\ &\leqslant 2^{(t(t+1)/2}M(f)^t\cdot 2^t\cdot(t+1)\cdot 2^{r(r-1)/2}M(f)^r\cdot|g(\alpha_{i_1})\cdots g(\alpha_{i_{t+1}})|^{-1}\\ &= (t+1)\cdot 2^{(r(r-1)+(t+1)(t+2))/2}M(f)^{r+t}\cdot|g(\alpha_{i_1})\cdots g(\alpha_{i_{t+1}})|^{-1}.\end{aligned}$$

By combining this with (4.13) and using $r\geqslant 2t+1$ we obtain the upper bound for Λ in (4.10). □

The following lemma is our key observation. Its proof is the only place where we use our assumption that g is irreducible.

Lemma 4.3. *(i)* $\lambda_1=1$, $\mathbf{h}_1=\pm\mathbf{g}$ *where* $\mathbf{g}$ *is the coefficient vector of* g*;*
(ii) $\lambda_2\geqslant M(g)^{15\xi/16t}$*, where* ξ *is the number defined by (4.2).*

Proof. Let $\mathbf{h}=(h_0,\dots,h_{t+1})\in\mathbb{Z}^{t+1}\backslash\{0\}$. Define $\lambda(\mathbf{h})$ to be the smallest positive real λ such that $\mathbf{h}\in\lambda\mathcal{C}(g)$, i.e., the smallest real λ such that $|L_i(\mathbf{h})|\leqslant\lambda|g(\alpha_i)|$ for $i=1,\dots,r$. Then in view of (4.6) we have

$$\lambda(\mathbf{h})=\max_{i=1,\dots,r}\frac{|h(\alpha_i)|}{|g(\alpha_i)|}\tag{4.14}$$

where $h=h_0X^t+\dots+h_t$. Suppose $\mathbf{h}$ is linearly independent of $\mathbf{g}$. Then the corresponding polynomials g,h are linearly independent. But g is irreducible, hence the polynomials g,h do not have a common zero, that is, $R(g,h)\neq 0$. Since g,h have integer coefficients this implies $|R(g,h)|\geqslant 1$. By combining this with the upper bound for $|R(g,h)|$ from Lemma 3.3, observing that $|f_0|\geqslant 1$, $|D(f)|\geqslant 1$, $|g_0|\geqslant 1$ since $f,g\in\mathbb{Z}[X]$, we obtain

$$\begin{aligned}1 &\leqslant 2^{\frac{1}{2}r^3}M(f)^{r(r-1)}\cdot|R(f,g)|\cdot M(g)^{2t-r}\cdot\max(1,\lambda(\mathbf{h}))^t\\ &\leqslant 2^{\frac{1}{2}r^3}M(f)^{r(r-1)}M(g)^{-\xi}\max(1,\lambda(\mathbf{h}))^t \quad\text{by (4.2)}\\ &\leqslant M(g)^{-15\xi/16}\max(1,\lambda(\mathbf{h}))^t \quad\text{by (4.3), (4.1)}.\end{aligned}$$

Therefore,

$$\lambda(\mathbf{h})\geqslant M(g)^{15\xi/16t}>1.\tag{4.15}$$

Since $\mathbf{g} \in \mathcal{C}(g)$ we have $\lambda(\mathbf{h}_1) = \lambda_1 \leqslant 1$. So by (4.15), $\mathbf{h}_1$ is linearly dependent on $\mathbf{g}$. Since g is primitive, this implies $\mathbf{h}_1 = \pm\mathbf{g}$ and $\lambda_1 = \lambda(\mathbf{g}) = 1$. Further, $\mathbf{h}_2$ is linearly independent of $\mathbf{h}_1$, hence of $\mathbf{g}$, and therefore (4.15) gives that $\lambda_2 = \lambda(\mathbf{h}_2) \geqslant M(g)^{15\xi/16t}$. □

5. Reciprocal vectors and linear forms

We keep the notation and assumptions from the previous sections. In particular, g is a polynomial in $\mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7), (4.1). Let $\mathbf{h}_1, \dots, \mathbf{h}_{t+1}$ be the linearly independent vectors in $\mathbb{Z}^{t+1}$ associated with the successive minima of $\mathcal{C}(g)$, i.e., the vectors satisfying (4.8). Write $\mathbf{h}_i = (h_{i0}, \dots, h_{it})$ $(i = 1, \dots, t+1)$,

$$H = \begin{pmatrix} h_{10} & \cdots & h_{1t} \\ \vdots & & \vdots \\ h_{t+1,0} & \cdots & h_{t+1,t} \end{pmatrix}, \qquad (\det H) \cdot (H^{-1})^T = \begin{pmatrix} h^*_{10} & \cdots & h^*_{1t} \\ \vdots & & \vdots \\ h^*_{t+1,0} & \cdots & h^*_{t+1,t} \end{pmatrix}$$

where A^T denotes the transpose of a matrix A, and put

$$\mathbf{h}^*_i := (h^*_{i0}, \dots, h^*_{it}) \quad (i = 1, \dots, t+1). \tag{5.1}$$

Recall that up to sign, h^*_{ij} is the determinant of the $t \times t$-matrix obtained by removing the i-th row and j-th column from H. Therefore $\mathbf{h}^*_i \in \mathbb{Z}^{t+1}$ for $i = 0, \dots, t$. Define the scalar product of two vectors $\mathbf{x} = (x_0, \dots, x_{t+1})$, $\mathbf{y} = (y_0, \dots, y_{t+1})$ by $\mathbf{x} \cdot \mathbf{y} = x_0 y_0 + \cdots + x_t y_t$. Then we have

$$\mathbf{h}_i \cdot \mathbf{h}^*_j = \delta_{ij} \det H \quad \text{for } i, j = 1, \dots, t+1,$$

where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise. Therefore, $\mathbf{h}_i$ is perpendicular to the span of the vectors $\mathbf{h}^*_j$ $(j \neq i)$. In particular, by Lemma 4.3, (i) we have that $\mathbf{g}$ is perpendicular to the span of $\mathbf{h}^*_2, \dots, \mathbf{h}^*_{t+1}$, i.e. the one-dimensional vector space generated by $\mathbf{g}$ is determined by this span. Since g is primitive, this implies that

$$\text{up to sign, } g \text{ is uniquely determined by the span of } \mathbf{h}^*_2, \dots, \mathbf{h}^*_{t+1}. \tag{5.2}$$

Let $\{i_1, \dots, i_{t+1}\}$ be the set of indices defined by (4.4) and let $L_1, \dots, L_r$ be the linear forms given by (4.5) so that in particular $L_{i_j} = \alpha^t_{i_j} X_0 + \alpha^{t-1}_{i_j} X_1 + \cdots + X_t$ for

$j = 1, \dots, t+1$. Write

$$L = \begin{pmatrix} \alpha_{i_1}^t & \alpha_{i_1}^{t-1} & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ \alpha_{i_{t+1}}^t & \alpha_{i_{t+1}}^{t-1} & \cdots & 1 \end{pmatrix}, \qquad (\det L)\cdot (L^{-1})^T = \begin{pmatrix} b_{10} & \cdots & b_{1t} \\ \vdots & & \vdots \\ b_{t+1,0} & \cdots & b_{t+1,t} \end{pmatrix}$$

and define the linear forms

$$L_j^* = \sum_{k=0}^{t} b_{jk} X_k \quad (j = 1, \dots, t+1). \tag{5.3}$$

Lemma 5.1. *We have*

$$|L_j^*(\mathbf{h}_k^*)| \leqslant t! \cdot 2^{2r^2} M(f)^{2r} \cdot \big(|g(\alpha_{i_j})| \cdot \lambda_k \big)^{-1} \quad \textit{for } j, k = 1, \dots, t+1. \tag{5.4}$$

Proof. Let $A = LH^T$. Then

$$\begin{aligned} \Big(L_{i_m}(\mathbf{h}_n) \Big)_{1 \leqslant m,n \leqslant t+1} &= A\,, \\ \Big(L_m^*(\mathbf{h}_n^*) \Big)_{1 \leqslant m,n \leqslant t+1} &= (\det L)(L^T)^{-1} \cdot (\det H) H^{-1} = (\det A)(A^{-1})^T \end{aligned}$$

where in both cases m is the row index and n the column index. It follows that for $j, k \in \{1, \dots, t+1\}$ we have

$$L_j^*(\mathbf{h}_k^*) = \pm \det (L_{i_m}(\mathbf{h}_n))_{m,n}$$

where the indices m, n run over $\{1, \dots, t+1\} \backslash \{j\}$, $\{1, \dots, t+1\} \backslash \{k\}$, respectively. The determinant is the sum of $t!$ terms of the shape $\pm \prod_{m=1,\, m \neq j}^{t+1} L_{i_m}(\mathbf{h}_{\sigma(m)})$ where σ is a bijection from $\{1, \dots, t+1\} \backslash \{j\}$ to $\{1, \dots, t+1\} \backslash \{k\}$. In view of (4.8), (4.10), each such term has absolute value at most

$$\begin{aligned} \prod_{m=1,\, m \neq j}^{t+1} \big(|g(\alpha_{i_m})| \cdot \lambda_{\sigma(m)} \big) &= \Big(\prod_{m=1}^{t+1} |g(\alpha_{i_m})| \cdot \lambda_m \Big) \cdot \big(|g(\alpha_{i_j})| \cdot \lambda_k \big)^{-1} \\ &\leqslant 2^{2r^2} M(f)^{2r} \big(|g(\alpha_{i_j})| \cdot \lambda_k \big)^{-1}. \end{aligned}$$

Now (5.4) easily follows. □

6. Estimates for certain linear forms

For a linear form $L = c_0X_0 + \cdots + c_tX_t$ with coefficients in $\overline{\mathbb{Q}}$ we define the field $\mathbb{Q}(L) := \mathbb{Q}(c_0/c_i, \ldots, c_t/c_i)$ where c_i is any non-zero coefficient of L. Thus $\mathbb{Q}(cL) = \mathbb{Q}(L)$ for any $c \in \overline{\mathbb{Q}}^*$. Further, we define the linear form $\sigma(L) := \sigma(c_0)X_0 + \cdots + \sigma(c_t)X_t$ for any isomorphism σ defined on $\mathbb{Q}(c_0, \ldots, c_t)$.

For a prime number p, we denote by $|\cdot|_p$ the standard p-adic absolute value, normalised such that $|p|_p = p^{-1}$ and we choose an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$ which we denote also by $|\cdot|_p$. Then for a linear form $L = c_0X_0 + \cdots + c_tX_t \in \overline{\mathbb{Q}}[X_0, \ldots, X_t]$ we put

$$\begin{aligned} \|L\| &:= \Big(|c_0|^2 + \cdots + |c_t|^2\Big)^{1/2}, \\ \|L\|_p &:= \max(|c_0|_p, \ldots, |c_t|_p) \quad \text{for each prime number } p \end{aligned}$$

and subsequently we define the absolute height of L by choosing a number field K containing the coefficients of L and putting

$$H(L) := \prod_\sigma \Big\{ \|\sigma(L)\| \cdot \prod_p \|\sigma(L)\|_p \Big\}^{1/[K:\mathbb{Q}]} \tag{6.1}$$

where the products are taken over all primes p and over all isomorphic embeddings σ of K into $\overline{\mathbb{Q}}$. This is easily shown to be independent of the choice of K. Further we have $H(cL) = H(L)$ for every $c \in \overline{\mathbb{Q}}^*$.

Now let $L_1^*, \ldots, L_{t+1}^*$ be the linear forms defined by (5.3). If the coefficients of L_j^* are not all real we write

$$L_j^* = \Re(L_j^*) + \sqrt{-1} \cdot \Im(L_j^*)$$

where both $\Re(L_j^*)$ and $\Im(L_j^*)$ are linear forms with real coefficients. We can express $\det(L_1^*, \ldots, L_{t+1}^*)$ as a linear combination of at most 2^{t+1} determinants $\sum_k \varepsilon_k \Delta_k$ where each ε_k is a power of $\sqrt{-1}$ and where each Δ_k is a determinant of $t+1$ linear forms, the j-th of which is L_j^* if all coefficients of L_j^* are real, and either one of the linear forms $\Re(L_j^*)$, $\Im(L_j^*)$ if not all coefficients of L_j^* are real. Therefore, we may choose linear forms $M_1^*, \ldots, M_{t+1}^*$, with $M_j^* = L_j^*$ if all coefficients of L_j^* are real and $M_j^* \in \{\Re(L_j^*), \Im(L_j^*)\}$ otherwise, such that

$$|\det(M_1^*, \ldots, M_{t+1}^*)| \geqslant 2^{-t-1} |\det(L_1^*, \ldots, L_{t+1}^*)| \,. \tag{6.2}$$

Lastly, we define normalised linear forms

$$N_j^* := \|M_j^*\|^{-1} \cdot M_j^* \quad (j = 1, \dots, t+1). \tag{6.3}$$

Notice that each linear form N_j^* has real coeficients. Below we have collected some other properties of the linear forms M_j^*, N_j^*.

Lemma 6.1. *We have*

$$|\det(M_1^*, \dots, M_{t+1}^*)| \geqslant 2^{-r^2t/2} M(f)^{-(r-1)t}; \tag{6.4}$$

$$\|M_j^*\| \leqslant (t+1)^{(t+1)/2} M(f)^t \quad \textit{for } j = 1, \dots, t+1; \tag{6.5}$$

$$\|M_j^*\| \geqslant 2^{-r^2t} M(f)^{-2rt} \quad \textit{for } j = 1, \dots, t+1. \tag{6.6}$$

Proof. We first prove (6.4). From definition (5.3) it follows that $\det(L_1^*, \dots, L_{t+1}^*) = \det(L_{i_1}, \dots, L_{i_{t+1}})^t$. Together with (6.2), Lemma 4.1, $r \geqslant 2t+1$, this implies

$$\begin{aligned} |\det(M_1^*, \dots, M_{t+1}^*)| &\geqslant 2^{-t-1} \cdot |\det(L_{i_1}, \dots, L_{i_{t+1}})|^t \\ &\geqslant 2^{-t-1} \Big(2^{(t(t+1)-r(r-1))/2} M(f)^{1-r} \Big)^t \\ &\geqslant 2^{-r^2t/2} M(f)^{-(r-1)t}. \end{aligned}$$

This proves (6.4).

We prove (6.5). Fix $j \in \{1, \dots, t+1\}$. By (4.5) we have

$$\|L_i\| \leqslant \big(1 + |\alpha_i|^2 + \dots + |\alpha_i|^{2t}\big)^{1/2} \leqslant \sqrt{t+1} \cdot \max(1, |\alpha_i|)^t \quad \text{for } i = 1, \dots, r.$$

By inserting this into Hadamard's inequality

$$\|L_j^*\| \leqslant \prod_{k=1,\, k \neq j}^{t+1} \|L_{i_k}\|$$

(which follows easily from the Gram-Schmidt orthogonalisation procedure) we obtain

$$\|L_j^*\| \leqslant (t+1)^{(t+1)/2} M(f)^t.$$

Using the obvious inequality $\|M_j^*\| \leqslant \|L_j^*\|$, inequality (6.5) follows.

We prove (6.6). Fix again $j \in \{1, \ldots, t+1\}$. By combining Hadamard's inequality $|\det(M_1^*, \ldots, M_{t+1}^*)| \leqslant \|M_1^*\| \cdots \|M_{t+1}^*\|$ with (6.4), (6.5) we obtain

$$\begin{aligned}
\|M_j^*\| &\geqslant |\det(M_1^*, \ldots, M_{t+1}^*)| \cdot \Big(\prod_{k=1,\, k\neq j}^{t+1} \|M_k^*\| \Big)^{-1} \\
&\geqslant 2^{-r^2 t/2} M(f)^{-(r-1)t} \cdot \Big((t+1)^{(t+1)/2} M(f)^t \Big)^{-t} \\
&\geqslant 2^{-r^2 t} M(f)^{-2rt} .
\end{aligned}$$

This proves (6.6). □

Lemma 6.2. *We have*

$$[\mathbb{Q}(N_j^*) : \mathbb{Q}] \leqslant r^{2t} \quad \textit{for } j = 1, \ldots, t+1; \tag{6.7}$$

$$H(N_j^*) \leqslant 2 \cdot (t+1)^{t/2} M(f)^t \quad \textit{for } j = 1, \ldots, t+1; \tag{6.8}$$

$$|\det(N_1^*, \ldots, N_{t+1}^*)| \geqslant 2^{-r^2(t+1)} M(f)^{-2r(t+1)} . \tag{6.9}$$

Proof. We prove (6.7). Fix $j \in \{1, \ldots, t+1\}$. The coefficients of L_j^* are $t \times t$-determinants, whose elements are coefficients of the linear forms L_{i_k} ($k = 1, \ldots, t+1$, $k \neq j$). Hence the coefficients of L_j^* belong to the field generated by the numbers α_{i_k} ($k \neq j$). Now N_j^* is a scalar multiple of either L_j^* or $L_j^* \pm \overline{L}_j^*$, where the coefficients of $\overline{L}_j^*$ are the complex conjugates of the coefficients of L_j^*. The coefficients of $\overline{L}_j^*$ belong to the field generated by the complex conjugates of the numbers α_{i_k} ($k \neq j$), which are also zeros of f. Therefore, N_j^* is proportional to a linear form with coefficients from a field which is generated by at most $2t$ zeros of f. This implies (6.7).

We prove (6.8). Recall that $M(f) = |f_0| \prod_{i=1}^r \max(1, |\alpha_i|)$. We will use

$$\prod_{i=1}^r \max(1, |\alpha_i|) \cdot \prod_p \prod_{i=1}^r \max(1, |\alpha_i|_p) \leqslant M(f) . \tag{6.10}$$

Indeed, by Gauss' lemma and since $f \in \mathbb{Z}[X]$ we have for every prime number p,

$$|f_0|_p \prod_{i=1}^r \max(1, |\alpha_i|_p) \leqslant 1$$

and together with the product formula $\big(\prod_p |f_0|_p \big)^{-1} = |f_0|$ this implies (6.10).

Fix again $j \in \{1, \ldots, t+1\}$. Let K be a finite normal extension of $\mathbb{Q}$ containing $\alpha_1, \ldots, \alpha_r$, $\sqrt{-1}$ and the coefficients of $N_1^*, \ldots, N_{t+1}^*$. Let σ be an automorphism of K. First notice that

$$\|L_i\| \leqslant (t+1)^{1/2} \max(1, |\alpha_i|)^t \quad \text{for } i = 1, \ldots, r.$$

Together with Hadamard's inequality and the fact that σ permutes $\alpha_1, \ldots, \alpha_r$ this implies

$$\begin{aligned} (6.11) \qquad \|\sigma(L_j^*)\| &\leqslant \prod_{k=1, k\neq j}^{t+1} \|\sigma(L_{i_k})\| \leqslant (t+1)^{t/2} \prod_{k=1, k\neq j}^{t+1} \max(1, |\sigma(\alpha_{i_k})|)^t \\ &\leqslant (t+1)^{t/2} \prod_{i=1}^{r} \max(1, |\alpha_i|)^t. \end{aligned}$$

Recall that N_j^* is a scalar multiple of $\tilde{N}_j^*$ where $\tilde{N}_j^*$ is either L_j^* or $L_j^* \pm \overline{L}_j^*$. Note that $\|\sigma(\overline{L}_j^*)\|$ is bounded above by the right-hand side of (6.11) since $\sigma(\overline{L}_j^*) = \tau(L_j^*)$ for some automorphism τ of K. So in either case, by the triangle inequality,

$$(6.12) \qquad \|\sigma(\tilde{N}_j^*)\| \leqslant 2 \cdot (t+1)^{t/2} \prod_{i=1}^{r} \max(1, |\alpha_i|)^t.$$

Now let p be a prime number. Then for $i = 1, \ldots, r$ we have

$$\|L_i\|_p \leqslant \max(1, |\alpha_i|_p)^t.$$

By precisely the same reasoning as above, but using the ultrametric inequality instead of Hadamard's inequality and the triangle inequality, one obtains

$$\|\sigma(L_j^*)\|_p \leqslant \prod_{k=1, k\neq j}^{t+1} \|\sigma(L_{i_k})\|_p \leqslant \prod_{k=1, k\neq j}^{t+1} \max(1, |\sigma(\alpha_{i_k})|_p)^t \leqslant \prod_{i=1}^{r} \max(1, |\alpha_i|_p)^t\,,$$

$$(6.13) \qquad \|\sigma(\tilde{N}_j^*)\|_p \leqslant \prod_{i=1}^{r} \max(1, |\alpha_i|_p)^t.$$

Now by combining (6.12), (6.13), (6.10) we obtain

$$\begin{aligned} H(N_j^*) = H(\tilde{N}_j^*) &= \prod_\sigma \left\{ \|\sigma(\tilde{N}_j^*)\| \cdot \prod_p \|\sigma(\tilde{N}_j^*)\|_p \right\}^{1/[K:\mathbb{Q}]} \\ &\leqslant 2 \cdot (t+1)^{t/2} \cdot \prod_{i=1}^r \Big(\max(1, |\alpha_i|) \prod_p \max(1, |\alpha_i|_p) \Big)^t \\ &\leqslant 2 \cdot (t+1)^{t/2} M(f)^t \end{aligned}$$

where in the products σ runs through the isomorphic embeddings of K into $\overline{\mathbb{Q}}$ and p through the prime numbers. This proves (6.8).

Lastly, (6.9) is proved by observing that

$$|\det(N_1^*, \dots, N_{t+1}^*)| = \frac{|\det(M_1^*, \dots, M_{t+1}^*)|}{\|M_1^*\| \cdots \|M_{t+1}^*\|}$$

and then proceeding as in the proof of (6.6). □

Lemma 6.3. *Let* $\mathbf{h}_1^*, \dots, \mathbf{h}_{t+1}^*$ *be the vectors defined by (5.1). Then we have*

$$|N_j^*(\mathbf{h}_k^*)| \leqslant 2^{2r^3} M(f)^{2r^2} \cdot \big(|g(\alpha_{i_j})| \cdot \lambda_k \big)^{-1} \quad \textit{for } j, k = 1, \dots, t+1. \tag{6.14}$$

Proof. Fix $j, k \in \{1, \dots, t+1\}$. Since $M_j^*(\mathbf{h}_k^*)$ is either the real or imaginary part of $L_j^*(\mathbf{h}_k^*)$ we have $|M_j^*(\mathbf{h}_k^*)| \leqslant |L_j^*(\mathbf{h}_k^*)|$. Together with Lemma 5.1, (6.6) this implies

$$\begin{aligned} |N_j^*(\mathbf{h}_k^*)| &= \|M_j^*\|^{-1} \cdot |M_j^*(\mathbf{h}_k^*)| \leqslant \|M_j^*\|^{-1} \cdot |L_j^*(\mathbf{h}_k^*)| \\ &\leqslant 2^{r^2 t} M(f)^{2rt} \cdot t! \cdot 2^{2r^2} M(f)^{2r} \cdot \big(|g(\alpha_{i_j})| \cdot \lambda_k \big)^{-1} \end{aligned}$$

and since $r \geqslant 2t+1$ this implies (6.14). □

7. Davenport's Lemma

We start with a variation on Davenport's lemma.

Lemma 7.1. *Let $L_1, \dots, L_n$ be linearly independent linear forms in n variables with coefficients in $\mathbb{R}$, let $\mathbf{h}_1, \dots, \mathbf{h}_n$ be linearly independent vectors from $\mathbb{R}^n$ and let $\mu_1, \dots, \mu_n$ be reals with $0 < \mu_1 \leqslant \mu_2 \leqslant \dots \leqslant \mu_n$. Suppose that*

$$|L_j(\mathbf{h}_k)| \leqslant \mu_k \quad \text{for } j, k = 1, \dots, n. \tag{7.1}$$

Then there are a permutation κ of $\{1, \dots, n\}$ and vectors

$$\mathbf{v}_j = \mathbf{b}_i + \sum_{k=1}^{j-1} \xi_{jk} \mathbf{b}_k \tag{7.2}$$

with $\xi_{jk} \in \mathbb{Z}$ for $j = 1, \dots, n$ and $k = 1, \dots, j-1$, such that

$$|L_j(\mathbf{v}_k)| \leqslant 2^{2n} \min(\mu_{\kappa(j)}, \mu_k) \quad \text{for } j, k = 1, \dots, n. \tag{7.3}$$

Proof. cf. [1, p. 40, Lemma 3.3.5]. □

We keep the notation from the previous sections so that in particular g is a polynomial in $\mathbb{Z}[X]$ with (2.6), (2.7), (4.1) and $N_1^*, \dots, N_{t+1}^*$ are the linear forms defined by (6.3). Then we have:

Lemma 7.2. *There are a permutation κ of $\{1, \dots, t+1\}$ and linearly independent vectors $\mathbf{v}_1^*, \dots, \mathbf{v}_{t+1}^* \in \mathbb{Z}^{t+1}$ with the following properties:*

$$|N_j^*(\mathbf{v}_k^*)| \leqslant 2^{3r^3} M(f)^{2r^2} |g(\alpha_{i_j})|^{-1} \cdot \min(\lambda_{\kappa(j)}^{-1}, \lambda_k^{-1}) \quad \text{for } j, k = 1, \dots, t+1; \tag{7.4}$$

(7.5) *up to sign, g is determined by the span of $\mathbf{v}_2^*, \dots, \mathbf{v}_{t+1}^*$.*

Proof. We apply Lemma 7.1 with $n = t+1$ and with

$$L_j = |g(\alpha_{i_{t+2-j}})| \cdot N_{t+2-j}^*, \quad \mu_j = 2^{2r^3} M(f)^{2r^2} \lambda_{t+2-j}^{-1}, \quad \mathbf{h}_j = \mathbf{h}_{t+2-j}^*$$

for $j = 1, \dots, t+1$. Lemma 6.3 implies that condition (7.1) is satisfied. It follows that there are a permutation κ of $\{1, \dots, t+1\}$ and vectors $\mathbf{v}_j^* = \mathbf{h}_j^* + \sum_{k=j+1}^{t+1} \xi_{jk} \mathbf{h}_k^*$

with $\xi_{jk} \in \mathbb{Z}$ for $j = 1, \ldots, t+1$ and $k = j+1, \ldots, t+1$, such that

$$\begin{aligned} |g(\alpha_{i_j})| \cdot |N_j^*(\mathbf{v}_k^*)| &\leqslant 2^{2r^3+2t+2} M(f)^{2r^2} \cdot \min(\lambda_{\kappa(j)}^{-1}, \lambda_k^{-1}) \\ &\leqslant 2^{3r^3} M(f)^{2r^2} \cdot \min(\lambda_{\kappa(j)}^{-1}, \lambda_k^{-1}) \end{aligned}$$

for $j, k = 1, \ldots, t+1$ where we have used that $r \geqslant 2t+1$. This proves (7.4). Using (5.2) and the fact that the span of $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$ is equal to the span of $\mathbf{h}_2^*, \ldots, \mathbf{h}_{t+1}^*$ we obtain (7.5). Lastly, $\mathbf{v}_1^*, \ldots, \mathbf{v}_{t+1}^*$ are linearly independent since they have the same span as $\mathbf{h}_1^*, \ldots, \mathbf{h}_{t+1}^*$ and since the latter vectors are linearly independent. □

8. Construction of a parallelepiped

We keep the notation from the previous sections. In particular, g is a polynomial in $\mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7), (4.1).

We wish to construct a parallelepiped $\Pi \subset \mathbb{R}^{t+1}$ which contains the vectors $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$ from Lemma 7.2 but which does not contain any vector from $\mathbb{Z}^{t+1}$ which is linearly independent of $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$. Thus the vector space V generated by $\Pi \cap \mathbb{Z}^{t+1}$ is equal to the span of $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$ and by (7.5) this means that V uniquely determines $\pm g$. A possible candidate is

$$\Pi := \{\mathbf{x} \in \mathbb{R}^{t+1} : |N_j^*(\mathbf{x})| \leqslant A_j \quad \text{for } j = 1, \ldots, t+1\}$$

where

$$(8.1) \qquad \begin{cases} A_j := 2^{3r^3} M(f)^{2r^2} \big(|g(\alpha_{i_j})| \cdot \lambda_{\kappa(j)}\big)^{-1} \quad (j = 1, \ldots, t+1;\ j \neq j_0), \\ A_{j_0} := 2^{3r^3} M(f)^{2r^2} \big(|g(\alpha_{i_{j_0}})| \cdot \lambda_2\big)^{-1} \\ \qquad = 2^{3r^3} M(f)^{2r^2} \big(|g(\alpha_{i_{j_0}})| \cdot \lambda_1\big)^{-1} \cdot (\lambda_1/\lambda_2) \end{cases}$$

with $\kappa(j_0) = 1$.

Indeed, from (7.4) it follows at once that Π contains $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$. Suppose Π contains also a vector $\mathbf{v}_1^* \in \mathbb{Z}^{t+1}$ (not necessarily the same vector as in Lemma 7.2) which is linearly independent of $\mathbf{v}_2^*,\dots,\mathbf{v}_{t+1}^*$. Then by Lemma 4.2, Lemma 4.3, (4.3),

$$\begin{aligned} 1 &\leqslant |\det(\mathbf{v}_1^*,\dots,\mathbf{v}_{t+1}^*)| \ll \mathrm{vol}(\Pi) \ll A_1\cdots A_{t+1} \\ &\ll \prod_{j=1}^{t+1}\left(|g(\alpha_{i_j})|\cdot\lambda_{\kappa(j)}\right)^{-1}\cdot(\lambda_1/\lambda_2) \ll \lambda_1/\lambda_2 \\ &\ll M(g)^{-15\xi/16t} \ll M(g)^{-15\delta/16t} \end{aligned}$$

where the constants implied by $\ll$ depend only on f. For $M(g)$ sufficiently large this gives a contradiction, i.e., such a vector $\mathbf{v}_1^*$ cannot exist.

However, for our method of proof to work, we need instead of Π a parallelepiped of the shape $\{\mathbf{x}\in\mathbb{R}^{t+1} : |N_j^*(\mathbf{x})| \leqslant M(g)^{\rho_j\xi} \text{ for } j=1,\dots,t+1\}$ where each ρ_j is independent of g. To construct such a parallelepiped we need the following combinatorial lemma.

Lemma 8.1. *There is a set $P\subset\mathbb{R}^{t+1}$ independent of g of cardinality at most*

$$(6t(t+1)^2\delta^{-1})^{t+1} \tag{8.2}$$

with the following property: if $A_1,\dots,A_{t+1}$ are the reals given by (8.1), then there is a tuple $(\rho_1,\dots,\rho_{t+1})\in P$ such that

$$M(g)^{(\rho_j-\frac{1}{2t(t+1)})\xi} < A_j \leqslant M(g)^{\rho_j\xi}\quad (j=1,\dots,t+1), \tag{8.3}$$

$$\rho_j \leqslant \tfrac{2t+1}{\delta}\quad (j=1,\dots,t+1), \tag{8.4}$$

$$\rho_1+\cdots+\rho_{t+1} \leqslant -\tfrac{1}{3t}. \tag{8.5}$$

Proof. First observe that for $j=1,\dots,t+1$

$$\begin{aligned} A_j &\leqslant 2^{3r^3}M(f)^{2r^2}|g(\alpha_{i_j})|^{-1} \quad \text{by Lemma 4.3 (i)} \\ &\leqslant 2^{3r^3}M(f)^{2r^2}\cdot 2^{t(r-1)}|R(f,g)|^{-1}M(f)^tM(g)^{r-1} \quad \text{by (3.12)} \\ &= 2^{3r^3+t(r-1)}M(f)^{2r^2+t}M(g)^{2t-1+\xi} \quad \text{by (4.2)} \\ &\leqslant (M(g)^\xi)^{\frac{2t-1}{\delta}+\frac{37}{36}} \quad \text{by (4.3), (4.1), } r\geqslant 2t+1\geqslant 3, \end{aligned}$$

and

$$
\begin{aligned}
A_j &\geqslant 2^{3r^3} M(f)^{2r^2} \prod_{k=1}^{t+1} \Big(|g(\alpha_{i_k})| \cdot \lambda_{\kappa(k)} \Big)^{-1} \cdot \prod_{k=1,\, k\neq j}^{t+1} |g(\alpha_{i_k})| \\
&\qquad\qquad\qquad\qquad\qquad \text{by Lemma 4.3 (i)} \\
&\geqslant 2^{3r^3} M(f)^{2r^2} 2^{2r^2} M(f)^{-2r} \cdot 2^{-t(r-t)} |R(f,g)| \cdot M(f)^{-t} M(g)^{t-r} \\
&\qquad\qquad\qquad\qquad\qquad \text{by Lemma 4.2, (3.12)} \\
&\geqslant M(g)^{-t-\xi} \geqslant (M(g)^{\xi})^{-\frac{t}{\delta}-1} \quad \text{by (4.2), (4.3),}
\end{aligned}
$$

so altogether,

$$
(M(g)^{\xi})^{-\frac{t}{\delta}-1} \leqslant A_j \leqslant (M(g)^{\xi})^{\frac{2t-1}{\delta}+\frac{37}{36}} \quad \text{for } j = 1, \dots, t+1. \tag{8.6}
$$

For $j = 1, \dots, t+1$, let f_j be the integer given by

$$
(M(g)^{\xi})^{f_j - 1} < A_j^{2t(t+1)} \leqslant (M(g)^{\xi})^{f_j} \tag{8.7}
$$

and put

$$
\rho_j := \frac{f_j}{2t(t+1)}.
$$

Notice that by (8.6), (8.7) we have for $j = 1, \dots, t+1$,

$$
-\left(\tfrac{t}{\delta}+1\right) \cdot 2t(t+1) < f_j \leqslant 1 + \left(\tfrac{2t-1}{\delta} + \tfrac{37}{36}\right) \cdot 2t(t+1)\,. \tag{8.8}
$$

It is clear that (8.3) is satisfied. By (8.8) we have

$$
\rho_j \leqslant \tfrac{2t-1}{\delta} + \tfrac{37}{36} + \tfrac{1}{2t(t+1)} \leqslant \tfrac{2t+1}{\delta}
$$

which implies (8.4). Further,

$$
\begin{aligned}
&(M(g)^{\xi})^{\rho_1+\cdots+\rho_{t+1}} \\
&\quad \leqslant A_1\cdots A_{t+1}\cdot (M(g)^{\xi})^{1/2t} \quad \text{by (8.3)} \\
&\quad \leqslant \left(2^{3r^3}M(f)^{2r^2}\right)^{t+1}\prod_{j=1}^{t+1}\left(|g(\alpha_{i_j})|\cdot\lambda_{\kappa(j)}\right)^{-1}\cdot(\lambda_1/\lambda_2)\cdot(M(g)^{\xi})^{1/2t} \quad \text{by (8.1)} \\
&\quad \leqslant \left(2^{3r^3}M(f)^{2r^2}\right)^{t+1}\cdot 2^{r^2/2}M(f)^{r-1}\cdot(M(g)^{\xi})^{-15/16t}\cdot(M(g)^{\xi})^{1/2t} \\
&\qquad\qquad\qquad\qquad \text{by Lemma 4.2, Lemma 4.3} \\
&\quad \leqslant 2^{4r^4}M(f)^{3r^3}(M(g)^{\xi})^{-7/16t}\leqslant (M(g)^{\xi})^{\frac{1}{12t}-\frac{7}{16t}}\leqslant (M(g)^{\xi})^{-1/3t} \\
&\qquad\qquad\qquad\qquad \text{by } r\geqslant 2t+1\geqslant 3,\ (4.3),\ (4.1)
\end{aligned}
$$

which implies (8.5).

Lastly, from (8.8) we infer that each integer f_j can be chosen from a set independent of g of cardinality at most

$$1+\left(\tfrac{3t-1}{\delta}+\tfrac{73}{36}\right)\cdot 2t(t+1)\leqslant 6t(t+1)^2\delta^{-1}.$$

Hence, each number ρ_j can be chosen from a set of cardinality at most $6t(t+1)^2\delta^{-1}$ which is independent of g and therefore, the tuple $(\rho_1,\dots,\rho_{t+1})$ can be chosen from a set of cardinality at most $\left(6t(t+1)^2\delta^{-1}\right)^{t+1}$ which is independent of g. This completes the proof of Lemma 8.1. $\square$

Lemma 8.2. *Let $(\rho_1,\dots,\rho_{t+1})$ be the tuple from Lemma 8.1 and define the parallelepiped*

$$\Pi(g):=\{\mathbf{x}\in\mathbb{R}^{t+1}\,:\,|N_j^*(\mathbf{x})|\leqslant (M(g)^{\xi})^{\rho_j}\quad \textit{for } j=1,\dots,t+1\}.$$

Then $\mathbf{v}_2^*,\dots,\mathbf{v}_{t+1}^*\in\Pi(g)\cap\mathbb{Z}^{t+1}$. Moreover, $\Pi(g)\cap\mathbb{Z}^{t+1}$ does not contain any vector which is linearly independent of $\mathbf{v}_2^*,\dots,\mathbf{v}_{t+1}^*$.

Proof. By (7.4), (8.1), (8.3) we have for $j=1,\dots,t+1$ and $k=2,\dots,t+1$,

$$|N_j^*(\mathbf{v}_k^*)|\leqslant A_j\leqslant (M(g)^{\xi})^{\rho_j}.$$

Hence $\mathbf{v}_k^* \in \Pi(g) \cap \mathbb{Z}^{t+1}$ for $k = 2, \ldots, t+1$.

Assume that $\Pi(g) \cap \mathbb{Z}^{t+1}$ contains a vector $\mathbf{v}_1^*$ which is linearly independent of $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$. Then

$$\begin{aligned} 1 &\leqslant |\det(\mathbf{v}_1^*, \ldots, \mathbf{v}_{t+1}^*)| = |\det(N_1^*, \ldots, N_{t+1}^*)|^{-1} \cdot |\det(N_j^*(\mathbf{v}_k^*)_{j,k=1,\ldots,t+1}| \\ &\leqslant 2^{r^2(t+1)} M(f)^{2r(t+1)} \cdot (t+1)! \cdot (M(g)^{\xi})^{\rho_1+\cdots+\rho_{t+1}} \quad \text{by (6.9)} \\ &\leqslant 2^{r^2(t+1)} M(f)^{2r(t+1)} \cdot (t+1)! \cdot M(g)^{-\xi/3t} < 1 \quad \text{by (8.5), (4.3), (4.1).} \end{aligned}$$

Thus the assumption that $\Pi(g) \cap \mathbb{Z}^{t+1}$ contains a vector which is linearly independent of $\mathbf{v}_2^*, \ldots, \mathbf{v}_{t+1}^*$ leads to a contradiction. □

In the proposition below we have collected the facts from Sections 4-8 which are needed in the proof of Theorem 2.1:

Proposition 8.3. *For every polynomial $g \in \mathbb{Z}[X]$ of degree t with (2.6), (2.7), (4.1) there exists a parallelepiped*

$$\Pi(g) = \{\mathbf{x} \in \mathbb{R}^{t+1} : |N_j^*(\mathbf{x})| \leqslant (M(g)^{\xi})^{\rho_j} \quad (j = 1, \ldots, t+1)\} \tag{8.9}$$

with the following properties:

(i) $N_1^*, \ldots, N_{t+1}^*$ are linearly independent linear forms with algebraic coefficients satisfying

$$[\mathbb{Q}(N_j^*) : \mathbb{Q}] \leqslant r^{2t}, \quad H(N_j) \leqslant 2 \cdot (t+1)^{t/2} M(f)^t, \quad \|N_j\| = 1 \tag{8.10}$$

for $j = 1, \ldots, t+1$.

(ii) $\rho_1, \ldots, \rho_{t+1}$ are real numbers satisfying

$$\rho_j \leqslant \frac{2t+1}{\delta} \quad (j = 1, \ldots, 2t+1), \qquad \rho_1 + \cdots + \rho_{t+1} \leqslant -1/3t\,. \tag{8.11}$$

(iii) The tuple $(N_1^*, \ldots, N_{t+1}^*; \rho_1, \ldots, \rho_{t+1})$ belongs to a set independent of g of cardinality at most

$$\binom{r}{t} \cdot \left(6t(t+1)^2\delta^{-1}\right)^{t+1}. \tag{8.12}$$

(iv) Let $V(g)$ be the $\mathbb{R}$-vector space generated by $\Pi(g)\cap\mathbb{Z}^{t+1}$. Then

$$\dim V(g)=t; \tag{8.13}$$

$$\text{up to sign, } g \text{ is uniquely determined by } V(g). \tag{8.14}$$

Proof. (8.10) follows immediately from (6.7), (6.8), (6.3) and (8.11) from (8.4), (8.5). This proves (i) and (ii).

In Section 6 we constructed $N_1^*,\dots,N_{t+1}^*$ from the linear forms $L_{i_1},\dots,L_{i_{t+1}}$. Therefore, $N_1^*,\dots,N_{t+1}^*$ depend only on the set of indices $\{i_1,\dots,i_{t+1}\}$ defined by (4.4). Hence for the tuple of linear forms $(N_1^*,\dots,N_{t+1}^*)$ we have at most $\binom{r}{t}$ possibilities. By multiplying this with the upper bound (8.2) for the number of posibilities of $(\rho_1,\dots,\rho_{t+1})$ we obtain (iii).

Lastly, Lemma 8.2 implies that $V(g)$ is the span of $\mathbf{v}_2^*,\dots,\mathbf{v}_{t+1}^*$. Since these vectors are linearly independent this implies (8.13). Statement (8.14) follows from (7.5). This proves (iv). □

9. The large solutions

We will estimate the number of polynomials g of degree t with (2.6), (2.7) having large Mahler measure. Apart from Proposition 8.3 we need a result from [2] which we recall below.

Let $0<\varepsilon<1$, $t\geqslant 1$, let $N_1,\dots,N_{t+1}$ be linearly independent linear forms in $\overline{\mathbb{Q}}[X_0,\dots,X_t]$ and let $c_1,\dots,c_{t+1}$ be reals such that

$$[\mathbb{Q}(N_j):\mathbb{Q}]\leqslant D,\quad H(N_j)\leqslant H,\quad ||N_j||=1\quad\text{for } j=1,\dots,t+1, \tag{9.1}$$

$$c_j\leqslant 1\quad (j=1,\dots,t+1),\qquad c_1+\cdots+c_{t+1}\leqslant-\varepsilon. \tag{9.2}$$

Then for every real $Q\geqslant 1$ we define the parallelepiped

$$\Pi(Q)=\Pi(\{N_j\},\{c_j\},Q)=\{\mathbf{x}\in\mathbb{R}^{t+1}\,:\,|N_j(\mathbf{x})|\leqslant Q^{c_j}\quad (j=1,\dots,t+1)\} \tag{9.3}$$

and we denote by $V(Q)$ the real vector space generated by $\Pi(Q)\cap\mathbb{Z}^{t+1}$.

Lemma 9.1. *There is a collection $\{V_1, \ldots, V_m\}$ of t-dimensional linear subspaces of $\mathbb{R}^{t+1}$ of cardinality*

$$m \leqslant C := 2^{30}(t+1)^8\varepsilon^{-4}\log 4D \log\log 4D \tag{9.4}$$

such that for every Q with

$$\dim V(Q) = t\,, \tag{9.5}$$

$$Q > (2H)^{e^C} \tag{9.6}$$

we have $V(Q) \in \{V_1, \ldots, V_m\}$.

Proof. This is a special case of Theorem C of [2], cf. pp. 260-261. □

We now show:

Proposition 9.2. *The number of polynomials $g \in \mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7) and*

$$\log M(g) \geqslant \exp(2^{55}t^{18}\delta^{-4}\log 4r \log\log 4r)\log(2M(f)) \tag{9.7}$$

is at most

$$2^{7t+59}t^{2t+21}\delta^{-t-5}\cdot r^t \log 4r \log\log 4r\,. \tag{9.8}$$

Proof. Inequality (9.7) implies (4.1). Therefore, for each polynomial $g \in \mathbb{Z}[X]$ of degree t with (2.6), (2.7), (9.7) there is a parallelepiped $\Pi(g)$ with the properties specified in Proposition 8.3. For the moment we consider only polynomials $g \in \mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7), (9.7) which correspond to a fixed tuple $(N_1^*, \ldots, N_{t+1}^*; \rho_1, \ldots, \rho_{t+1})$. Thus let g be such a polynomial and put

$$Q \;:=\; (M(g)^{\xi})^{(2t+1)/\delta}\,, \tag{9.9}$$

$$c_j^* \;:=\; \frac{\delta}{2t+1}\rho_j \quad (j = 1, \ldots, t+1). \tag{9.10}$$

Then the parallelepiped $\Pi(g)$ defined by (8.9) is equal to

$$\Pi(Q) := \{\mathbf{x} \in \mathbb{R}^{t+1} : |N_j^*(\mathbf{x})| \leqslant Q^{c_j^*} \quad (j = 1, \ldots, t+1)\}$$

while $V(g)$ is equal to the space $V(Q)$ spanned by $\Pi(Q)\cap\mathbb{Z}^{t+1}$. So by (8.13), $\dim V(Q)=t$. Further, by (8.11) we have

$$c_j^*\leqslant 1\quad (j=1,\dots,t+1),\qquad c_1^*+\cdots+c_{t+1}^*\leqslant -\frac{\delta}{3t(2t+1)}\,. \tag{9.11}$$

We apply Lemma 9.1 with $N_j=N_j^*$, $c_j=c_j^*$ $(j=1,\dots,t+1)$. Thus (8.10) implies (9.1) with

$$D=r^{2t},\quad H=2(t+1)^{t/2}M(f)^t\,.$$

Further, (9.11) implies (9.2) with

$$\varepsilon=\frac{\delta}{3t(2t+1)}\,.$$

By substituting these values for D,ε into the quantity C defined by (9.4) we get

$$\begin{aligned} C &= 2^{30}(t+1)^8\big(3t(2t+1)\delta^{-1}\big)^4\log(4r^{2t})\log\log(4r^{2t}) \\ &< 2^{54}t^{18}\delta^{-4}\log 4r\log\log 4r\,, \end{aligned} \tag{9.12}$$

where in the last inequality we have used $t+1\leqslant 2t$, $2t+1\leqslant 3t$ and $\log(4r^{2t})\log\log(4r^{2t})\leqslant 6t^2\log 4r\log\log 4r$ for $t\geqslant 1$, $r\geqslant 2t+1$. Further, by (9.9), (4.3), (9.7) we have

$$\begin{aligned} Q &\geqslant M(g)^{2t+1}\geqslant (2M(f))^{(2t+1)\exp(2^{55}t^{18}\delta^{-4}\log 4r\log\log 4r)} \\ &\geqslant \big(4(t+1)^{t/2}M(f)^t\big)^{\exp(2^{54}t^{18}\delta^{-4}\log 4r\log\log 4r)} \\ &\geqslant (2H)^{e^C} \end{aligned}$$

with the value of H chosen above. Thus, Q satisfies (9.5), (9.6).

Now Lemma 9.1 implies that the space $V(Q)$ belongs to a collection of cardinality at most C which is independent of g. Hence the space $V(g)$ belongs to this collection. But by (8.14), the space $V(g)$ uniquely determines g up to sign. It follows that there are at most $2C$ polynomials $g\in\mathbb{Z}[X]$ of degree t satisfying (2.6), (2.7), (9.7) which correspond to a fixed tuple $(N_1^*,\dots,N_{t+1}^*;\rho_1,\dots,\rho_{t+1})$, where C is given by (9.12).

Thus, the total number of polynomials $g\in\mathbb{Z}[X]$ of degree t with (2.6), (2.7), (9.7) is at most $2C$ times the upper bound (8.12) for the number of possibilities for

$(N_1^*, \dots, N_{t+1}^*; \rho_1, \dots, \rho_{t+1})$, that is,

$$\begin{aligned} &2C \cdot \binom{r}{t} \cdot \big(6t(t+1)^2\delta^{-1}\big)^{t+1} \\ &\quad\leqslant 2^{55} t^{18} \delta^{-4} \log 4r \log\log 4r \cdot (er/t)^t \cdot \big(24t^3\delta^{-1}\big)^{t+1} \\ &\quad\leqslant 2^{7t+59} t^{2t+21} \delta^{-t-5} \cdot r^t \log 4r \log\log 4r \end{aligned}$$

where we have used that $e^t \cdot 24^{t+1} < 2^{7t+4}$ for $t \geqslant 1$. This proves Proposition 9.2. □

10. A gap principle

We derive a gap principle to estimate the number of polynomials g with (2.6)-(2.8) which do not satisfy (9.7). We need the following combinatorial lemma.

Lemma 10.1. *Let θ be a real with $0 < \theta < 1$ and let t be an integer $\geqslant 1$. There exists a set $P \subset \mathbb{R}^t$ of cardinality at most*

$$4\Big(e^2\big(\tfrac{1}{2} + \tfrac{1+\theta^{-1}}{t}\big)\Big)^{t-1}, \tag{10.1}$$

consisting of tuples $(\rho_1, \dots, \rho_t)$ with

$$\rho_1 \geqslant \rho_2 \geqslant \cdots \geqslant \rho_t \geqslant 0, \quad 1 - \theta \leqslant \sum_{i=1}^{t} \rho_i \leqslant 1, \tag{10.2}$$

such that for every tuple of reals $(F_1, \dots, F_t, \Lambda)$ with

$$0 < F_1 \leqslant F_2 \leqslant \cdots \leqslant F_t \leqslant 1, \quad F_1 \cdots F_t \leqslant \Lambda \tag{10.3}$$

there is a tuple $(\rho_1, \dots, \rho_1) \in P$ such that $F_i \leqslant \Lambda^{\rho_i}$ for $i = 1, \dots, t$.

Proof. cf. [3, p. 79, Lemma 14]. □

Let f be the polynomial and δ the real number from Theorem 2.1. Thus, $f = f_0 \prod_{i=1}^r (X - \alpha_i)$ with $f_0 \neq 0$ and with $\alpha_1, \dots, \alpha_r$ distinct. If ζ is an algebraic number of degree t then we order the conjugates $\zeta^{(1)},\dots,\zeta^{(t)}$ of ζ in such a way that

$$\min_{i=1,\dots,r}\frac{|\alpha_i-\zeta^{(1)}|}{\max(1,|\alpha_i|)}\leqslant\min_{i=1,\dots,r}\frac{|\alpha_i-\zeta^{(2)}|}{\max(1,|\alpha_i|)}\leqslant\cdots\leqslant\min_{i=1,\dots,r}\frac{|\alpha_i-\zeta^{(t)}|}{\max(1,|\alpha_i|)}\,. \tag{10.4}$$

If $g\in\mathbb{Z}[X]$ is an irreducible polynomial of degree t, let $\zeta^{(1)},\dots,\zeta^{(t)}$ be the zeros of g, ordered according to (10.4). We first prove the following result.

Lemma 10.2. *There exists a set S of cardinality at most*

$$7r^t(63\delta^{-1})^{t-1} \tag{10.5}$$

consisting of tuples $(i_1,\dots,i_t;\varphi_1,\dots,\varphi_t)$ where $i_1,\dots,i_t\in\{1,\dots,r\}$ and where $\varphi_1,\dots,\varphi_t$ are non-negative reals satisfying

$$\varphi_1+\cdots+\varphi_t\geqslant 2t+\delta/2\,, \tag{10.6}$$

such that for every polynomial $g\in\mathbb{Z}[X]$ with (2.6)-(2.8) there is a tuple $(i_1,\dots,i_t;\varphi_1,\dots,\varphi_t)\in S$ for which

$$\frac{|\alpha_{i_j}-\zeta^{(j)}|}{2\max(1,|\alpha_{i_j}|)\max(1,|\zeta^{(j)}|)}\leqslant M(g)^{-\varphi_j}\quad \text{for } j=1,\dots,t. \tag{10.7}$$

Proof. Let $g\in\mathbb{Z}[X]$ be a polynomial of degree t with (2.6)-(2.8). Choose indices $i_1,\dots,i_t\in\{1,\dots,r\}$ such that

$$\frac{|\alpha_{i_j}-\zeta^{(j)}|}{\max(1,|\alpha_{i_j}|)}=\min_{i=1,\dots,r}\frac{|\alpha_i-\zeta^{(j)}|}{\max(1,|\alpha_i|)}\quad\text{for } j=1,\dots,t. \tag{10.8}$$

By formula (7.3) on [3, p. 81] we have

$$\frac{|R(f,g)|}{M(f)^tM(g)^r}\geqslant C^{-1}\prod_{i=1}^{t}\frac{|\alpha_{i_j}-\zeta^{(j)}|}{2\max(1,|\alpha_{i_j}|)\max(1,|\zeta^{(j)})|}$$

$$\text{with } C=\Big(2^{1+r(r-1)/2}M(f)^{r-1}\Big)^t.$$

Together with (2.6), (2.8) this implies

$$\prod_{i=1}^{t}\frac{|\alpha_{i_j}-\zeta^{(j)}|}{2\max(1,|\alpha_{i_j}|)\max(1,|\zeta^{(j)})|}\leqslant M(g)^{-2t-3\delta/4}. \tag{10.9}$$

We apply Lemma 10.1 with

$$F_j = \frac{|\alpha_{i_j} - \zeta^{(j)}|}{2\max(1,|\alpha_{i_j}|)\max(1,|\zeta^{(j)})|} \quad (j=1,\dots,t), \qquad \Lambda = M(g)^{-2t-3\delta/4},$$

$$\theta = 1 - \frac{2t+\delta/2}{2t+3\delta/4} = \frac{\delta}{8t+3\delta}.$$

Then clearly, $0 < \theta < 1$. Further, (10.4), (10.8), (10.9) imply (10.3). Hence the conditions of Lemma 10.1 are satisfied. Let P be the set from Lemma 10.1, let $(\rho_1,\dots,\rho_t) \in P$ be the tuple for which $F_j \leqslant \Lambda^{\rho_j}$ for $j = 1,\dots,t$ and put $\varphi_j = \rho_j(2t + 3\delta/4)$. Then clearly, (10.7) holds. Further, (10.2) and our choices of θ, Λ and φ_j $(j = 1,\dots,t)$ imply (10.6).

Lastly, with our choice of θ the set P of Lemma 10.1 has cardinality at most

$$4\left(e^2\left(\tfrac{1}{2} + \tfrac{1}{t}\bigl(1 + \tfrac{8t+3\delta}{\delta}\bigr)\right)\right)^{t-1} \leqslant 4\left(e^2\left(\tfrac{1}{2} + \tfrac{4}{t} + \tfrac{8}{\delta}\right)\right)^{t-1}$$

$$\leqslant 4\left(e^2\left(\tfrac{1}{2} + \tfrac{8}{\delta}\right)\right)^{t-1} \cdot \left(1 + \tfrac{1}{2t}\right)^{t-1} \leqslant 7\bigl(63\delta^{-1}\bigr)^{t-1}.$$

Since for each index i_j we have r possibilities and since φ_j is determined by ρ_j, we have at most $7r^t(63\delta^{-1})^{t-1}$ possibilities for the tuple $(i_1,\dots,i_t;\,\varphi_1,\dots,\varphi_t)$. This proves Lemma 10.2. □

We recall the following gap principle for Wirsing systems.

Lemma 10.3. *Let $t > 0$, $0 < \varepsilon < 1$, let $\alpha_1,\dots,\alpha_t$ be algebraic numbers and let $\varphi_1,\dots,\varphi_t$ be non-negative reals with $\sum_{j=1}^t \varphi_j \geqslant 2t + \varepsilon$. Further, let A, B be reals with*

$$B \geqslant A \geqslant 4^{t(t+1)/\varepsilon}. \tag{10.10}$$

Choose for every algebraic number ζ of degree t an ordering of its conjugates $\zeta^{(1)},\dots,\zeta^{(t)}$.
Then the number of algebraic numbers ζ of degree t satisfying

$$\frac{|\alpha_j - \zeta^{(j)}|}{2\max(1,|\alpha_j|)\max(1,|\zeta^{(j)}|)} \leqslant M(\zeta)^{-\varphi_j} \quad \textit{for } j = 1,\dots,t, \tag{10.11}$$

$$A \leqslant M(\zeta) < B \tag{10.12}$$

is at most

$$t \cdot \left(1 + \frac{\log(2\log B/\log A)}{\log(1+\varepsilon/t)}\right). \tag{10.13}$$

Proof. cf. [3, p. 60, Lemma 2 (i)]. □

We finally arrive at the following gap principle for the resultant inequality:

Proposition 10.4. *Let A, B be reals with*

$$B \geqslant A \geqslant \left(2^{2r^2} M(f)^{4r-4}\right)^{t/\delta}. \tag{10.14}$$

Then the number of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6)-(2.8) and with

$$A \leqslant M(g) < B$$

is at most

$$14t(63\delta^{-1})^{t-1} r^t \cdot \left(1 + \frac{\log(2\log B/\log A)}{\log(1+\delta/2t)}\right). \tag{10.15}$$

Proof. Instead of primitive, irreducible polynomials $g \in \mathbb{Z}[X]$ of degree t we may count algebraic numbers ζ of degree t. For each algebraic number ζ of degree t there are precisely two primitive irreducible polynomials $g \in \mathbb{Z}[X]$ with $g(\zeta) = 0$ (taking into consideration the sign) and for these we have $M(g) = M(\zeta)$.

By Lemma 10.2, each polynomial $g \in \mathbb{Z}[X]$ of degree t with (2.6)-(2.8) satisfies one of at most $N_1 := 7r^t(63\delta^{-1})^{t-1}$ systems of inequalities of the shape (10.7). To each of these systems we can apply Lemma 10.3 with $\varepsilon = \delta/2$. For this choice of ε, (10.14) implies (10.10). It follows that the number of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6)-(2.8) and with $A \leqslant M(g) < B$ is at most $2N_1N_2$, where N_2 is the quantity from (10.13) with $\delta/2$ in place of ε. This proves Proposition 10.4. □

11. Proof of Theorem 2.1

Put

$$C^* := 2^{55} t^{18} \delta^{-4} \log 4r \log\log 4r \,.$$

Let R_1 denote the set of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6),(2.7) and

$$\left(2^{2r^2} M(f)^{4r-4}\right)^{t/\delta} \leqslant M(g) < (2M(f))^{e^{C^*}}$$

and let R_2 denote the set of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6),(2.7) and

$$M(g) \geqslant (2M(f)^{e^{C^*}} \,.$$

Thus, $R_1 \cup R_2$ is the set of all polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6), (2.7), (2.8).

We estimate the cardinality of R_1. We apply Proposition 10.4 with

$$A = \left(2^{2r^2} M(f)^{4r-4}\right)^{t/\delta}, \quad B = (2M(f))^{e^{C^*}} .$$

Note that with this choice of A and B we have $B^2 \leqslant A^{e^{C^*}}$. Further, $\log(1+\delta/2t) \geqslant \delta/4t$. By inserting this into (10.15) we obtain that R_1 has cardinality at most

$$\begin{aligned} &14t \cdot r^t (63\delta^{-1})^{t-1} \cdot (1 + 4t\delta^{-1} C^*) \\ &\qquad \leqslant 2^{6t+55} t^{20} \delta^{-t-4} \cdot r^t \log 4r \log\log 4r \,. \end{aligned}$$

By Proposition 9.2, the cardinality of R_2 is bounded above by the quantity in (9.8). Thus we obtain that the total number of polynomials $g \in \mathbb{Z}[X]$ of degree t with (2.6)-(2.8) is at most

$$\begin{aligned} &2^{6t+55} t^{20} \delta^{-t-4} \cdot r^t \log 4r \log\log 4r \;+\; 2^{7t+59} t^{2t+21} \delta^{-t-5} \cdot r^t \log 4r \log\log 4r \\ &\qquad \leqslant 2^{7t+60} t^{2t+21} \delta^{-t-5} \cdot r^t \log 4r \log\log 4r \,. \end{aligned}$$

This completes the proof of Theorem 2.1. $\square$

12. Proof of Corollary 2.2

Let $(\xi,\eta)\in(\overline{\mathcal{O}}\backslash\{0\})^2$ be a pair satisfying (2.15)-(2.17). Let g be the minimal polynomial of $\zeta:=\xi/\eta$. Thus,

$$H(\xi,\eta)=M(\zeta)^{1/t}=M(g)^{1/t}\,. \tag{12.1}$$

Put $f:=F(X,1)$. Let $s:=[\mathbb{Q}(\xi,\eta):\mathbb{Q}]$. Denote by $(\xi^{(i)},\eta^{(i)})$ $(i=1,\dots,s)$ the images of (ξ,η) under the isomorphic embeddings of $\mathbb{Q}(\xi,\eta)$ into $\overline{\mathbb{Q}}$. Write $g=g_0\prod_{j=1}^t(X-\zeta^{(j)})$ where $\zeta^{(1)},\dots,\zeta^{(t)}$ are the conjugates of ζ. Then for each conjugate $\zeta^{(j)}$ of ζ there are precisely s/t indices i such that $\xi^{(i)}/\eta^{(i)}=\zeta^{(j)}$. Thus,

$$\prod_{i=1}^s(\eta^{(i)}X-\xi^{(i)})=\big(\prod_{i=1}^s\eta^{(i)}\big)\cdot\Big(\prod_{j=1}^t(X-\zeta^{(j)})\Big)^{s/t}=d_0g(X)^{s/t},$$

where

$$d_0:=\big(\prod_{i=1}^s\eta^{(i)}\big)g_0^{-s/t}$$

is an integer since the polynomial on the left-hand side has its coefficients in $\mathbb{Z}$ and since g is primitive. Now (2.3) implies

$$\begin{aligned}\|F(\xi,\eta)\| &= \left(\prod_{i=1}^s|F(\xi^{(i)},\eta^{(i)})|\right)^{1/s}=|\prod_{i=1}^s\eta^{(i)}|^{r/s}\cdot|\prod_{j=1}^t f(\zeta^{(j)})|^{1/t}\\ &= |d_0|^{r/s}\cdot|g_0|^{r/t}\cdot|\prod_{j=1}^t f(\zeta^{(j)})|^{1/t}=|d_0|^{r/s}|R(f,g)|^{1/t}\\ &\geqslant |R(f,g)|^{1/t}\,.\end{aligned} \tag{12.2}$$

From (12.1), (12.2) we infer that if $(\xi,\eta)\in(\overline{\mathcal{O}}\backslash\{0\})^2$ is a pair with (2.15)-(2.17), then the minimal polynomial g of ξ/η has degree t and satisfies (2.6)-(2.8). Further, since each such polynomial g has t zeros, there are up to proportionality at most t pairs (ξ,η) giving rise to the same polynomial g. It follows that the number of pairs $(\xi,\eta)\in(\overline{\mathcal{O}}\backslash\{0\})^2$ with (2.15)-(2.17) is up to proportionality at most t times the upper bound (2.9) in Theorem 2.1, which in turn is equal to the upper bound (2.14) in Corollary 2.2. This completes our proof. $\square$

13. Proof of Corollary 2.3

Let $f \in \mathbb{Z}[X]$ be the polynomial of degree $r \geqslant 2t+1$ from Corollary 2.3 such that the numbers α_i $(i \in I)$ are zeros of f. Write $f = f_0 \prod_{i=1}^{r}(X-\beta_j)$ where $\beta_1, \ldots, \beta_r$ are distinct. Thus $\alpha_j = \beta_{i_j} \in \{\beta_1, \ldots, \beta_r\}$ for $i \in I$. Let ζ be an algebraic number of degree t satisfying (2.23) and let $g \in \mathbb{Z}[X]$ be the minimal polynomial of ζ. Write $g = g_0 \prod_{j=1}^{t}(X-\zeta^{(j)})$. Then using (2.3), (2.21) and $|\beta_i - \zeta^{(j)}| \leqslant 2\max(1,|\beta_i|)\cdot\max(1,|\zeta^{(j)}|)$ we obtain

$$
\begin{aligned}
(13.1)\ |R(f,g)| &= |f_0^t g_0^r| \prod_{i=1}^{r}\prod_{j=1}^{s} |\beta_i - \zeta^{(j)}| \\
&\leqslant |f_0^t g_0^r| \prod_{j\in I} |\beta_{i_j} - \zeta^{(j)}| \cdot \prod_{i=1}^{r}\prod_{j=1}^{t} \Big(2\max(1,|\beta_i|)\cdot\max(1,|\zeta^{(j)}|)\Big) \\
&\leqslant M(g)^{-\sum_{j\in I}\varphi_j} \cdot 2^{rt} M(f)^t M(g)^r \\
&\leqslant 2^{rt} M(f)^t M(g)^{r-2t-\delta}.
\end{aligned}
$$

Now let W_1 be the set of algebraic numbers ζ of degree t satisfying (2.23) and

$$
\max\Big(M(f), 4^{t(t+1)/\delta}\Big) \leqslant M(\zeta) < \Big(2^{4r^2} M(f)^{8r-8}\Big)^{t/\delta} \tag{13.2}
$$

and let W_2 be the set of algebraic numbers ζ of degree t satisfying (2.23) and

$$
M(\zeta) \geqslant \Big(2^{4r^2} M(f)^{8r-8}\Big)^{t/\delta}. \tag{13.3}
$$

Thus $W_1 \cup W_2$ is the set of algebraic numbers of degree t with (2.23), (2.24).

To estimate the cardinality of W_1 we apply Lemma 10.3 with

$$
A = \max\Big(M(f), 4^{t(t+1)/\delta}\Big), \quad B = \Big(2^{4r^2} M(f)^{8r-8}\Big)^{t/\delta}, \quad \varepsilon = \delta
$$

(observe that if ζ satisfies (2.23) then ζ also satisfies (10.11) with α_j, φ_j the same as in (2.23) for $j \in I$, and $\alpha_j = 0$, $\varphi_j = 0$ for $j \in \{1, \ldots, t\}\backslash I$).

Thus, using that $B^2 \leqslant A^{32r^2t\delta}$, $r \geqslant 2t+1 \geqslant 3$ we infer that W_1 has cardinality at most

$$
\begin{aligned}
(13.4) \qquad t\left(1+\frac{\log(32r^2t\delta^{-1})}{\log(1+\delta/t)}\right) &\leqslant t\left(1+4t\delta^{-1}\cdot\log(32r^2t\delta^{-1})\right) \\
&\leqslant t+4t^3\delta^{-1}\cdot 3\delta^{-1}\log 4r \leqslant 13t^3\delta^{-2}\log 4r\,.
\end{aligned}
$$

To estimate the cardinality of W_2 we will apply Theorem 2.1 with $\delta/2$ in place of δ.

Let $\zeta \in W_2$ and let g be the minimal polynomial of ζ. We first observe that f and g do not have a common zero. For assume the contrary. Then g is a divisor of f since g is irreducible. But then $M(\zeta) = M(g) \leqslant M(f)$ by (3.6) which contradicts (13.3). Now from our observation, (13.3), (13.1) and $M(\zeta) = M(g)$ it follows that

$$0 < |R(f,g)| \leqslant M(g)^{r-2t-\delta/2}$$

which is (2.6) with $\delta/2$ replacing δ. It is clear that g satisfies (2.7). Further, from (13.3) and $M(g) = M(\zeta)$ it follows that g satisfies (2.8) with $\delta/2$ replacing δ.

So by applying Theorem 2.1 (with $\delta/2$ in place of δ) we infer that if ζ runs through W_2 then its minimal polynomial g runs through a set of cardinality at most

$$2^{7t+60}t^{2t+21}(2\delta^{-1})^{t+5}\log 4r\log\log 4r \;=\; 2^{8t+65}t^{2t+21}\delta^{-t-5}\log 4r\log\log 4r\,.$$

Since each such polynomial g has t zeros we must multiply this with t to obtain an upper bound for the cardinality of W_2, i.e. we must replace t^{2t+21} by t^{2t+22}.

By combining this with the upper bound for the cardinality of W_1 obtained in (13.4) we infer that the total number of algebraic numbers ζ of degree t with (2.23), (2.24) is at most

$$2^{8t+66}t^{2t+22}\delta^{-t-5}\log 4r\log\log 4r\,.$$

Since this is the upper bound (2.22) in Corollary 2.3 we are done. $\square$

References

[1] J.-H. Evertse, The Subspace Theorem of W.M. Schmidt, In: Diophantine Approximation and Abelian Varieties, ed. by B. Edixhoven and J.-H. Evertse, Lecture Notes Math. **1566**, Springer Verlag 1993, Chapter IV.

[2] J.-H. Evertse, An improvement of the Quantitative Subspace Theorem, *Compos. Math.*, **101** (1996) , 225–311.

[3] J.-H. Evertse, The number of algebraic numbers of given degree approximating a given algebraic number, In: Analytic Number Theory, Proc. conf. Kyoto, 1996, ed. by Y. Motohashi, Cambridge Univ. Press 1997, 53-83.

[4] J.-H. Evertse, N. Hirata-Kohno, Wirsing Systems and Resultant Inequalities, In: Number Theory for the Millennium, Proc. Millennial conference on Number Theory, Urbana-Champaign, May 21-26, 2000, ed. by B. Berndt et.al., A.K. Peters, 2002, to appear. http://www.math.leidenuniv.nl/∼evertse/publicaties.shtml

[5] J.-H. Evertse, H.P. Schlickewei, A quantitative version of the absolute Subspace Theorem, *J. reine angew. Math.,* to appear. http://www.math.leidenuniv.nl/∼evertse/publicaties.shtml

[6] N. Hirata-Kohno, On Wirsing systems of Diophantine inequalities, in preparation.

[7] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag 1983.

[8] H. Locher, On the number of good approximations of algebraic numbers by algebraic numbers of bounded degree, *Acta Arith.*, **89** (1999) , 97–122.

[9] J. Mueller, W.M. Schmidt, The generalized Thue inequality, *Compos. Math.*, **96** (1995) , 331–344.

[10] K.F. Roth, Rational approximation to algebraic numbers, *Mathematika*, **2** (1955) , 1–20.

[11] M. Ru, P.M. Wong, Integral points of $\mathbb{P}^n\backslash\{2n+1$ hyperplanes in general position$\}$, *Invent. math.*, **106** (1991) , 195–216.

[12] W.M. Schmidt, Simultaneous approximation to algebraic numbers by rationals, *Acta Math.*, **125** (1970) , 189–201.

[13] W.M. Schmidt, Norm form equations, *Ann. of Math.*, **96** (1972) , 526–551.

[14] W.M. Schmidt, Inequalities for resultants and for decomposable forms, In: Diophantine Approximation and its Applications, Proc. conf. Washington D.C., 1972, ed. by C.F. Osgood, Academic Press, New York 1973, 235-253.

[15] W.M. Schmidt, The Subspace Theorem in Diophantine approximations, *Compos. Math.*, **69** (1989) 121–173.

[16] B.L. van der Waerden, *Algebra I*, 8. Aufl., Heidelberger Taschenbücher, Springer Verlag, 1971.

[17] E. Wirsing, On approximations of algebraic numbers by algebraic numbers of bounded degree, In: Proc. Symp. Pure Math. **20**, A.M.S., Providence, 1971, 213–248.

Universiteit Leiden, Mathematisch Instituut, Postbus 9512, NL-2300 RA Leiden

E-mail address: evertse@math.leidenuniv.nl