On p-adic Decomposable Form Inequalities

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op 5 maart 2015
klokke 13 : 45 uur

door

Junjiang Liu
geboren te Henan, China
in 1988

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. Peter Stevenhagen

Copromotor: Dr. Jan-Hendrik Evertse

Copromotor: Dr. Pascal Autissier (Université Bordeaux I)

Overige leden:

Prof. dr. Yuri F. Bilu (Université Bordeaux I)

Dr. Robin de Jong

Prof. dr. Jeffrey L. Thunder (Northern Illinois University)

Prof. dr. Robert Tijdeman

This work was funded by Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and l'Université Bordeaux I.

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Junjiang Liu

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

On p-adic Decomposable Form Inequalities

Directeurs de recherche : Pascal AUTISSIER, Jan-Hendrik EVERTSE, Peter STEVENHAGEN

Soutenue le : 5 mars 2015 à Leiden

Devant la commission d'examen formée de :

M AUTISSIER, Pascal	Professeur	Université Bordeaux I	Directeur
M BILU, Yuri	Professeur	Université Bordeaux I	Examinateur
M DE JONG, Robin	Docteur	Universiteit Leiden	Rapporteur
M EVERTSE, Jan-Hendrik	Docteur	Universiteit Leiden	Directeur
M STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Examinateur
M THUNDER, Jeffrey Lin	Professeur	Northern Illinois University	Rapporteur
M TIJDEMAN, Robert	Professeur	Universiteit Leiden	Rapporteur

To my parents and Bo

Contents

Partial list of notation:

$\|S\|$	the cardinality of a set S.
$A \subseteq B$	A is a subset of B.
$A \subsetneq B$	A is a proper subset of B.
$\mathbb{Z}$	the ring of integers.
$\mathbb{Z}_{\geq 0}$	non-negative integers.
$\gcd(x_1, \dots, x_n)$	the greatest common divisor of integers $x_1, \dots, x_n$.
$\mathbf{x} \in \mathbb{Z}^n$ primitive	the greatest common divisor of the coordinates of $\mathbf{x}$ is 1.
$\mathcal{P}$	the set of prime numbers of $\mathbb{Z}$.
p	a prime number.
$\mathbb{Z}_p$	the ring of p-adic integers.
$M_{\mathbb{Q}} = \{\infty\} \cup \mathcal{P}$	the set of places of $\mathbb{Q}$.
$\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p_1 \dots p_r}]$	the ring of S-integers where $S = \{\infty\} \cup \{p_1, \dots, p_r\}$ is a finite set of places.
$\mathbb{Q}$	the field of rational numbers.
$\mathbb{Q}_p$	the field of p-adic numbers.
$\|\cdot\|_p$	p-adic absolute value with $\|p\| = p^{-1}$.
$\overline{\mathbb{Q}}_p$	the algebraic closure of $\mathbb{Q}_p$.
$\mathbb{R} = \mathbb{Q}_\infty$	the field of real numbers.
$[x]$	the largest integer not greater than $x \in \mathbb{R}$.
$\mathbb{C} = \overline{\mathbb{Q}}_\infty$	the field of complex numbers.
$\|\cdot\|_\infty$	ordinary absolute value.
$\mathbb{K}$	a number field.
$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$	the multiplicative group of $\mathbb{K}$.
$\dim_{\mathbb{K}}(V)$	the dimension of a $\mathbb{K}$-vector space V.
$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$	the Galois group of a field $\mathbb{L}$ over a field $\mathbb{K}$.
$\|\mathbf{x}\|_\infty$	the L^2 norm of a vector $\mathbf{x} \in \mathbb{C}^n$.
$\\|\mathbf{x}\\|$	the sup-norm of a vector $\mathbf{x} \in \mathbb{C}^n$.
$\|\mathbf{x}\|_p$	the p-sup-norm of a vector $\mathbf{x} \in \overline{\mathbb{Q}}_p^n$.

$H(\mathbf{x})$	the absolute height of a vector $\mathbf{x}$.
$H_{\mathbb{K}}(\mathbf{x}) = H(\mathbf{x})^{[\mathbb{K}:\mathbb{Q}]}$	the field height of a vector $\mathbf{x}$ with coordinates in $\mathbb{K}$.
$\det(X)$	the determinant of a matrix X.
R	a ring.
R^*	the unit group of a ring R.
$\mathrm{GL}_n(R)$	the group of $n \times n$ matrices with coefficients in R and determinant in R^*.
$R[X_1, \ldots, X_n]$	the ring of polynomials in n variables with its coefficients in a ring R.
$\ll, \gg$	Vinogradov symbols.
$a \gg\ll b$	if $a \ll b$ and $b \ll a$.

Introduction

We start with the *Thue equation*

$$F(x,y) = m \text{ in } x, y \in \mathbb{Z} \tag{0.0.1}$$

where $F \in \mathbb{Z}[X,Y]$ is a homogeneous polynomial of degree $d \geq 3$ which is irreducible over $\mathbb{Q}$. Thue's famous result in [17] shows that the number of integer solutions to (0.0.1) is finite. This implies that the number of solutions $N_F(m)$ to the *Thue inequality*

$$|F(x,y)| \leq m \text{ in } x, y \in \mathbb{Z} \tag{0.0.2}$$

is finite. In 1933, Mahler [10] showed that for such F, the number of solutions $N_F(m)$ can be estimated as follows. Denote the area of the region $\{\mathbf{x} \in \mathbb{R}^2 : |F(x,y)| \leq 1\}$ by A_F. Then $m^{2/d}A_F$ is the area of the region $\{\mathbf{x} \in \mathbb{R}^2 : |F(x,y)| \leq m\}$. One has

$$|N_F(m) - m^{2/d}A_F| = O(m^{1/(d-1)}) \text{ as } m \to \infty$$

where the constant implied by the O-symbol depends on d and F.

Now let F be a norm form over $\mathbb{Q}$ of degree d in $n \geq 3$ variables, that is, a homogeneous polynomial of the shape

$$F = cN_{\mathbb{L}/\mathbb{Q}}(L) = cN_{\mathbb{L}/\mathbb{Q}}(\lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n) \tag{0.0.3}$$

where $L = \lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n$, $\mathbb{L} = \mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ is a number field and $c \in \mathbb{Q}^*$ such that $F \in \mathbb{Z}[X_1, \ldots, X_n]$. To F, we associate the $\mathbb{Q}$-vector space,

$$V := \{\lambda_1 x_1 + \cdots + \lambda_n x_n : x_1, \ldots, x_n \in \mathbb{Q}\}.$$

For each subfield $\mathbb{E}$ of $\mathbb{L}$ we define the linear subspace of V,

$$V^{\mathbb{E}} := \{v \in V : \epsilon v \in V \text{ for every } \epsilon \in \mathbb{E}\}.$$

Notice that in fact $\epsilon V^{\mathbb{E}} \subseteq V^{\mathbb{E}}$ for $\epsilon \in \mathbb{E}$. Hence $V^{\mathbb{E}}$ is the largest subspace of V closed under scalar multiplication with $\mathbb{E}$. The norm form F is said to be *non-degenerate* if $\lambda_1, \ldots, \lambda_n$ are linearly independent over $\mathbb{Q}$ and if $V^{\mathbb{E}} = 0$ for each subfield $\mathbb{E}$ of $\mathbb{L}$ which is not equal to $\mathbb{Q}$ or to an imaginary quadratic field. Schmidt's famous result in [14] shows that the number of solutions to the *norm form equations*

$$F(x_1, \ldots, x_n) = m \text{ in } x_1, \ldots, x_n \in \mathbb{Z} \tag{0.0.4}$$

is finite for all m if and only if F is non- degenerate. This implies that for non-degenerate norm forms F, the number of solutions $N_F(m)$ to the *norm form inequality*

$$|F(x_1, \ldots, x_n)| \leq m \text{ in } x_1, \ldots, x_n \in \mathbb{Z} \tag{0.0.5}$$

is finite. Afterwards, Schmidt also gave in [16] an upper bound for the number of solutions of (0.0.5). Later, Evertse showed in [7] that for non-degenerate norm forms F, we have

$$N_F(m) \leq (16d)^{\frac{(n+7)^3}{3}} m^{\frac{n+\sum_{i=2}^{n-1} i^{-1}}{d}} (1 + \log m)^{\frac{n(n+1)}{2}}.$$

Now let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a *decomposable form* of degree d, that is, a homogeneous polynomial which can be factorized into linear forms over some extension of $\mathbb{Q}$. Denote by $\mathbb{A}_F(m)$ the set $\{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\}$ and put $\mathbb{A}_F := \mathbb{A}_F(1)$. Let μ_∞ be the normalized Lebesgue measure on $\mathbb{R}$ such that $\mu_\infty([0,1]) = 1$ and μ_∞^n the product measure on $\mathbb{R}^n$. Note that $\mu_\infty^n(\mathbb{A}_F(m)) = m^{n/d}\mu_\infty^n(\mathbb{A}_F)$. We say F is *of finite type* if $\mu_\infty^n(\mathbb{A}_F) < \infty$ and $\mu_\infty^{\dim T}(\mathbb{A}_{F|_T}) < \infty$ for every non-zero linear subspace T of $\mathbb{Q}^n$. We consider the *decomposable form inequality*

$$|F(\mathbf{x})| \leq m \text{ in } \mathbf{x} \in \mathbb{Z}^n. \tag{0.0.6}$$

Thunder proved in [19] that the number of solutions to (0.0.6) is finite for every m if and only if F is of finite type. More precisely, he proved that for decomposable forms $F \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree d of finite type, one has

Theorem 0.0.1.

$$N_F(m) \ll m^{\frac{n}{d}},$$
$$|N_F(m) - \mu_\infty^n(\mathbb{A}_F(m))| \ll m^{\frac{n-1}{d-a(F)}}(1+\log m)^{n-2}H(F)^{c(F)}$$

where $a(F), c(F)$ *are rational numbers satisfying*

$$1 \leq a(F) \leq \frac{d}{n} - \frac{1}{n(n-1)}\ , \quad \frac{d-n}{d} \leq c(F) < \binom{d}{n}(d-n+1)$$

and constants implied by the Vinogradov symbol $\ll$ *depend only on* n *and* d.

Later, Thunder's concern was to obtain a similar inequality, but with the upper bound of the error term $|N_F(m) - \mu_\infty^n(\mathbb{A}_F(m))|$ depending only on n, d. He managed to do so in several cases. We define the discriminant $D(F)$ of a decomposable form $F \in \mathbb{Z}[X_1, \ldots, X_n]$ in Chapter 4 (4.2.2) and it is an integer. For decomposable forms $F \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree $n+1$ of finite type (which implies $D(F) \neq 0$), Thunder proved in [20] the following Theorem:

Theorem 0.0.2.

$$|N_F(m) - m^{n/(n+1)}\mu_\infty^n(\mathbb{A}_F)| \ll \frac{m^{(n-1)/n}}{|D(F)|^{1/(2n(n+1))}}(1+\log m)^{n-2} + m^{(n-1)/(n+1)}(1+\log m)^{n-1}.$$

where the implicit constant depends only on n.

For decomposable forms in n variables of degree d of finite type with $\gcd(n,d) = 1$, Thunder proved in [22] the following Theorem:

Theorem 0.0.3.

$$|N_F(m) - m^{n/d}\mu_\infty^n(\mathbb{A}_F)| \ll m^{n/(d+1/(n-1)^2)}(1+\log m)^{n-2}.$$

The subject of this thesis is to generalize Theorems 0.0.1, 0.0.2 and 0.0.3 to the p-adic setting. Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d with $d > n$. Let

$S = \{\infty, p_1, \ldots, p_r\}$ be a fixed (once for all) finite subset of $M_{\mathbb{Q}}$ and $S_0 = S \setminus \{\infty\}$. We are interested in the solutions to inequalities of the shape

$$\begin{array}{c} \prod_{p\in S} |F(\mathbf{x})|_p \leq m \ \text{ in } \ \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{with } \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \end{array} \tag{0.0.7}$$

Note that the condition $\gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1$ is necessary for the number of the solutions being finite. Define

$$\mathbb{A}_{F,S}(m) := \Big\{(\mathbf{x}_p)_p \in \prod_{p\in S} \mathbb{Q}_p^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \leq m \ , \ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\},$$

$$N_{F,S}(m) := \Big|\Big\{\mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |F(\mathbf{x})|_p \leq m \ , \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1\Big\}\Big|.$$

Let μ_∞ be the normalized Lebesgue measure on $\mathbb{R} = \mathbb{Q}_\infty$ with $\mu_\infty([0,1]) = 1$ and μ_p be the normalized Haar measure on $\mathbb{Q}_p$ with $\mu_p(\mathbb{Z}_p) = 1$. Define the product measure $\mu^n = \prod_{p\in S} \mu_p^n$ on $\prod_{p\in S} \mathbb{Q}_p^n$.

In the literature, there are few results in this direction. For decomposable forms F satisfying a suitable finiteness condition, Evertse's result in [5] implies

$$N_{F,S}(1) \leq 2(2^{33}d^2)^{n^3|S|}. \tag{0.0.8}$$

In his master's thesis [9], de Jong proved a result for norm forms F as in (0.0.3) satisfying the following three conditions: (a) each n-tuple among the linear factors of F is linearly independent, (b) the Galois group of the normal closure of $\mathbb{L}$ over $\mathbb{Q}$ acts $n-1$ times transitively on the set of conjugates $\{a^{(1)}, \ldots, a^{(r)}\}$ of any primitive element a of $\mathbb{L}$, (c) $d \geq 2n^{5/3}$. Under these conditions, he proved the following asymptotic formula:

$$N_{F,S}(m) = m^{\frac{n}{d}} \mu^n(\mathbb{A}_{F,S}(1)) + O_{F,S}(m^{f(n,d)}) \ \ as \ \ m \to \infty$$

where $f(n,d) < n/d$ is a function depending only on n and d. The constant implied by the $O_{F,S}$-symbol here and below depends only on F and S.

For our p-adic generalizations of Theorems 0.0.1, 0.0.2 and 0.0.3, we mainly care about the exponents on m rather than the exponents on $\log m$. In fact, the exponents on $\log m$

in our results are slightly bigger than Thunder's, which is caused by the estimation of small solutions. For the proofs of our results, we mainly follow Thunder's proofs and make the necessary modifications in the p-adic setting. As one of the main ingredients of the proofs, we use a version of the p-adic Subspace Theorem. (For a more general version, see [6].)

Let $S = \{\infty, p_1, \ldots, p_r\}$ be a finite subset of $M_{\mathbb{Q}}$. For each $p \in S$, let $L_{p1}, \ldots, L_{pn}$ be linearly independent linear forms in n variables with algebraic coefficients such that

$$H_{\mathbb{Q}(\mathbf{L}_{pi})}(\mathbf{L}_{pi}) \leq H, \quad [\mathbb{Q}(\mathbf{L}_{pi}) : \mathbb{Q}] \leq D \text{ for } p \in S, i = 1, \ldots, n,$$

where $\mathbf{L}_{pi}$ is the vector of coefficients of L_{pi}. (See Section 1.1 for the definitions of these quantities.)

Theorem 0.0.4. *Let $0 < \sigma < 1$. Consider the inequality*

$$\prod_{p \in S} \frac{\prod_{i=1}^{n} |L_{pi}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p1}, \ldots, \mathbf{L}_{pn})|_p} < |\mathbf{x}|_\infty^{-\sigma} \text{ in } \mathbf{x} \in \mathbb{Z}^n. \tag{0.0.9}$$

There are proper linear subspaces $T_1, \ldots, T_N$ of $\mathbb{Q}^n$ with

$$N \leq (2^{60n^2} \sigma^{-7n})^{r+1} \log 4D \log\log 4D$$

such that every solution $\mathbf{x} \in \mathbb{Z}^n$ of (0.0.9) with

$$|\mathbf{x}|_\infty \geq H, \quad \mathbf{x} \text{ primitive}$$

lies in $T_1 \cup \cdots \cup T_N$.

The thesis is organized as follows.

In Chapter 1, we introduce some notation, definitions, general facts and basic lemmas.

In Chapter 2, we prove the following results. For $F = \prod_{i=1}^{d} L_i$, let $I(F)$ denote the set of all ordered n-tuples $(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})$ which are linearly independent. If $I(F) \neq \emptyset$, we define

$$a(F) := \max_{(\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_n}) \in I(F)} \max_{1 \leq j \leq n-1} \frac{|\{\mathbf{L}_i \in \text{span}\ \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}|}{j}.$$

Theorem 0.0.5. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$ and $a(F) < \frac{d}{n}$. Then $\mu^n(\mathbb{A}_{F,S}(m)) \ll m^{n/d}$ where the implicit constant depends only on n, d and S.*

For a polynomial F in n variables and an $n \times n$ matrix $M = (a_{ij})_{i,j=1,\ldots,n}$, define

$$F_M(X_1, \ldots, X_n) := F\Big(\sum_{j=1}^{n} a_{1j}X_j, \ldots, \sum_{j=1}^{n} a_{nj}X_j\Big).$$

For a non-zero m-dimensional linear subspace T of $\mathbb{Q}^n$, we choose $M_T \in \mathrm{GL}_n(\mathbb{Z})$ such that $M_T^{-1}(T)$ is the subspace spanned by $\mathbf{e}_1, \ldots, \mathbf{e}_m$ where $\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, \ldots, 0)$, $\ldots, \mathbf{e}_m$ are the first m standard basis vectors of $\mathbb{Q}^n$. We denote by $F|_T$ the decomposable form of degree d in m variables obtained by restricting F_{M_T} to the subspace spanned by $\mathbf{e}_1, \ldots, \mathbf{e}_m$.

Theorem 0.0.6. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then $N_{F,S}(m) \ll m^{n/d}$ where the implicit constant depends only on n, d and S.*

Theorem 0.0.7. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then*

$$N_{F,S}(m) = m^{\frac{n}{d}} \mu^n(\mathbb{A}_{F,S}(1)) + O_{F,S}(m^{\frac{n}{d+(1/2(n-1)^2)}}) \quad as \quad m \to \infty.$$

The conditions of Theorems 0.0.6 and 0.0.7 can be effectively verified in a finitely number of steps. In fact, write $F = c \cdot \prod_{i=1}^{q} N_{\mathbb{K}_i/\mathbb{Q}}(L_i)$ where $c \in \mathbb{Q}^*$, $\mathbb{K}_i$ is a number field of degree d_i and $L_i = a_{i1}X_1 + \cdots + a_{in}X_n$ with $\mathbb{Q}(a_{i1}, \ldots, a_{in}) = \mathbb{K}_i$ for $i = 1, \ldots, q$. Define the $\mathbb{Q}$-algebra $\Omega = \mathbb{K}_1 \times \cdots \times \mathbb{K}_q$. Let

$$V = \{(L_1(\mathbf{x}), \ldots, L_q(\mathbf{x})) : \mathbf{x} \in \mathbb{Q}^n\}.$$

Then V is a $\mathbb{Q}$-vector space contained in Ω. For a $\mathbb{Q}$-subalgebra $\mathcal{B}$ of Ω, we define

$$V^{\mathcal{B}} = \{a \in V : \mathcal{B} \cdot a \subseteq V\}.$$

This is the largest subspace of V which is closed under scalar multiplication by $\mathcal{B}$. In Chapter 3, we prove the following result.

Theorem 0.0.8. *The following statements are equivalent:*

(a) $a(F|_T) < \frac{d}{\dim T}$ *for every linear subspace* T *of dimension at least* 2 *of* $\mathbb{Q}^n$*,*

(b) for every $\mathbb{Q}$*-subalgebra* $\mathcal{B}$ *of* Ω *with* $\dim_{\mathbb{Q}} \mathcal{B} > 1$*, we have* $V^{\mathcal{B}} = \{0\}$*.*

In Chapter 4, we prove the following theorem.

Theorem 0.0.9. *Let* $F \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a decomposable form of degree* $n+1$*. Suppose* $F(\mathbf{x}) \neq 0$ *for every non-zero* $\mathbf{x} \in \mathbb{Z}^n$*. Also suppose* $a(F|_T) < \frac{d}{\dim T}$ *for every linear subspace* T *of dimension at least* 2 *of* $\mathbb{Q}^n$*. Then we have* $D(F) \neq 0$ *and*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll \frac{m^{(n-1)/n}(1+\log m)^{|S|(n+1)}}{(\prod_{p\in S} |D(F)|_p)^{\frac{1}{2n(n+1)}}} + m^{\frac{n-1}{n+1}}(1+\log m)^{|S|(n-1)}$$

where the implied constant depends only on n *and* S*.*

In Chapter 5, we consider the more general case where the degree d of F and the number of variables n are coprime. We prove the following theorem.

Theorem 0.0.10. *Let* $F \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a decomposable form of degree* d*. Suppose* $F(\mathbf{x}) \neq 0$ *for every non-zero* $\mathbf{x} \in \mathbb{Z}^n$*. Also suppose* $a(F|_T) < \frac{d}{\dim T}$ *for every linear subspace* T *of dimension at least* 2 *of* $\mathbb{Q}^n$*. If* $\gcd(n,d) = 1$*, we have*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll m^{n/(d+1/(n-1)^2)}(1+\log m)^{2d|S|}$$

where the implied constant depends only on n*,* d *and* S*.*

We finish this introduction with some open problems.

(a) Remove the coprime condtion $\gcd(n,d) = 1$ in Thunder's Theorem 0.0.3. For instance, Theorem 0.0.3 holds for binary forms of odd degree. Can we prove the same result for binary forms of even degree?

(*b*) The implicit constants in Theorems 0.0.9 and 0.0.10 depend on n, d and the primes in S. In view of (0.0.8), can we replace these by constants depending only on n, d and the cardinality of S? Further, can we give an upper bound for $\mu^n(\mathbb{A}_{F,S}(1))$ depending only on on n, d and the cardinality of S?

Résumé (version longue)

Nous commençons avec l'*équation de Thue*

$$F(x,y) = m \text{ en } x,y \in \mathbb{Z} \tag{0.0.10}$$

où $F \in \mathbb{Z}[X,Y]$ est un polynôme homogène de degré $d \geq 3$ qui est irréductible sur $\mathbb{Q}$. Le célèbre résultat de Thue dans [17] montre que le nombre de solutions entières à (0.0.10) est fini. Cela implique que le nombre de solutions $N_F(m)$ à l'*inégalité de Thue*

$$|F(x,y)| \leq m \text{ en } x,y \in \mathbb{Z} \tag{0.0.11}$$

est fini. En 1933, Mahler [10] a montré que pour ces F, le nombre de solutions $N_F(m)$ peut être estimé comme suit. Notons A_F l'aire de la région $\{\mathbf{x} \in \mathbb{R}^2 : |F(x,y)| \leq 1\}$. Alors $m^{2/d}A_F$ est l'aire de la région $\{\mathbf{x} \in \mathbb{R}^2 : |F(x,y)| \leq m\}$. On a

$$|N_F(m) - m^{2/d}A_F| = O(m^{1/(d-1)}) \text{ lorsque } m \to \infty$$

où la constante implicite dans le symbole O dépend de d et F.

Maintenant, soit F une forme norme sur $\mathbb{Q}$ de degré d en $n \geq 3$ variables, c'est-à-dire un polynôme homogène de la forme

$$F = cN_{\mathbb{L}/\mathbb{Q}}(L) = cN_{\mathbb{L}/\mathbb{Q}}(\lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n) \tag{0.0.12}$$

où $L = \lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n$, $\mathbb{L} = \mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ est un corps de nombres et $c \in \mathbb{Q}^*$ tel que $F \in \mathbb{Z}[X_1, \ldots, X_n]$. À F, nous associons le $\mathbb{Q}$-espace vectoriel

$$V := \{\lambda_1 x_1 + \cdots + \lambda_n x_n : x_1, \ldots, x_n \in \mathbb{Q}\}.$$

Pour chaque sous-corps $\mathbb{E}$ de $\mathbb{L}$, nous définissons le sous-espace linéaire de V,

$$V^{\mathbb{E}} := \{v \in V : \epsilon v \in V \text{ pour chaque } \epsilon \in \mathbb{E}\}.$$

Notez que $\epsilon V^{\mathbb{E}} \subseteq V^{\mathbb{E}}$ pour $\epsilon \in \mathbb{E}$. Par conséquent $V^{\mathbb{E}}$ est le plus grand sous-espace de V fermé sous la multiplication scalaire par $\mathbb{E}$. La forme norme F est dite *non-dégénérée* si $\lambda_1, \ldots, \lambda_n$ sont linéairement indépendants sur $\mathbb{Q}$ et si $V^{\mathbb{E}} = 0$ pour chaque sous-corps $\mathbb{E}$ de $\mathbb{L}$ qui n'est pas égal à $\mathbb{Q}$ ou à un corps quadratique imaginaire. Le célèbre résultat de Schmidt dans [14] montre que le nombre de solutions à l'*équation de forme norme*

$$F(x_1, \ldots, x_n) = m \text{ en } x_1, \ldots, x_n \in \mathbb{Z} \tag{0.0.13}$$

est fini pour tout m si et seulement si F est non dégénérée. Ceci implique que pour les formes normes non-dégénérées F, le nombre de solutions $N_F(m)$ à l'*inégalité de forme norme*

$$|F(x_1, \ldots, x_n)| \leq m \text{ en } x_1, \ldots, x_n \in \mathbb{Z} \tag{0.0.14}$$

est fini. Ensuite, Schmidt a également donné dans [14] une borne supérieure pour le nombre de solutions de (0.0.14). Plus tard, Evertse a montré dans [7] que pour les formes normes non-dégénérées F, nous avons

$$N_F(m) \leq (16d)^{\frac{(n+7)^3}{3}} m^{\frac{n+\sum_{i=2}^{n-1} i^{-1}}{d}} (1 + \log m)^{\frac{n(n+1)}{2}}.$$

Maintenant, soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une *forme décomposable* de degré d, c'est-à-dire un polynôme homogène qui peut être factorisé en formes linéaires sur une extension de $\mathbb{Q}$. Notons $\mathbb{A}_F(m)$ l'ensemble $\{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\}$ et posons $\mathbb{A}_F := \mathbb{A}_F(1)$. Soit μ_∞ la mesure de Lebesgue normalisée sur $\mathbb{R}$ telle que $\mu_\infty([0,1]) = 1$ et μ_∞^n la mesure produit sur $\mathbb{R}^n$. Notez que $\mu_\infty^n(\mathbb{A}_F(m)) = m^{n/d}\mu_\infty^n(\mathbb{A}_F)$. Nous disons que F est *de type fini* si $\mu_\infty^n(\mathbb{A}_F) < \infty$ et $\mu_\infty^{\dim T}(\mathbb{A}_{F|_T}) < \infty$ pour chaque sous-espace vectoriel non nul T de $\mathbb{Q}^n$. Nous considérons l'*inégalité de forme décomposable*

$$|F(\mathbf{x})| \leq m \text{ en } \mathbf{x} \in \mathbb{Z}^n. \tag{0.0.15}$$

Thunder prouve dans [19] que le nombre de solutions à (0.0.15) est fini pour chaque m si et seulement si F est de type fini. Plus précisément, il a prouvé que pour les formes décomposables $F \in \mathbb{Z}[X_1, \ldots, X_n]$ de degré d de type fini, on a

Theorem 0.0.11.

$$N_F(m) \ll m^{\frac{n}{d}},$$
$$|N_F(m) - \mu_\infty^n(\mathbb{A}_F(m))| \ll m^{\frac{n-1}{d-a(F)}}(1+\log m)^{n-2}H(F)^{c(F)}$$

où $a(F), c(F)$ sont des nombres rationnels satisfaisant

$$1 \leq a(F) \leq \frac{d}{n} - \frac{1}{n(n-1)}, \quad \frac{d-n}{d} \leq c(F) < \binom{d}{n}(d-n+1)$$

et les constantes implicites dans le symbole de Vinogradov $\ll$ ne dépendent que de n et d.

Plus tard, la préoccupation de Thunder était d'obtenir une inégalité similaire, mais avec la borne supérieure du terme d'erreur $|N_F(m) - \mu_\infty^n(\mathbb{A}_F(m))|$ fonction uniquement de n, d. Il a réussi à le faire dans plusieurs cas. Nous définissons le discriminant $D(F)$ d'une forme décomposable $F \in \mathbb{Z}[X_1, \dots, X_n]$ au chapitre 4 (4.2.2) et c'est un nombre entier. Pour les formes décomposables $F \in \mathbb{Z}[X_1, \dots, X_n]$ de degré $n+1$ de type fini (ce qui implique $D(F) \neq 0$), Thunder a prouvé dans [20] le théorème suivant:

Theorem 0.0.12.

$$\begin{aligned}|N_F(m) - m^{n/(n+1)}\mu_\infty^n(\mathbb{A}_F)| \ll \; & \frac{m^{(n-1)/n}}{|D(F)|^{1/(2n(n+1))}}(1+\log m)^{n-2} \\ & + M^{(n-1)/(n+1)}(1+\log m)^{n-1}.\end{aligned}$$

où la constante implicite ne dépend que de n.

Pour les formes décomposables en n variables de degré d de type fini avec $\gcd(n, d) = 1$, Thunder a prouvé dans [22] le théorème suivant:

Theorem 0.0.13.

$$|N_F(m) - m^{n/d}\mu_\infty^n(\mathbb{A}_F)| \ll m^{n/(d+1/(n-1)^2)}(1+\log m)^{n-2}.$$

Le sujet de cette thèse est de généraliser les théorèmes 0.0.11, 0.0.12 et 0.0.13 au cadre p-adique. Soit $F \in \mathbb{Z}[X_1, \dots, X_n]$ une forme décomposable de degré d avec $d > n$.

Soit $S = \{\infty, p_1, \ldots, p_r\}$ un sous-ensemble fini fixé (une fois pour toutes) de $M_{\mathbb{Q}}$ et $S_0 = S \setminus \{\infty\}$. Nous sommes intéressés par les solutions aux inégalités de la forme

$$\begin{array}{c} \prod_{p\in S} |F(\mathbf{x})|_p \le m \quad \text{en} \quad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{avec} \quad \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \end{array} \tag{0.0.16}$$

Notez que la condition $\gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1$ est nécessaire pour que le nombre de solutions soit fini. On définit

$$\mathbb{A}_{F,S}(m) := \Big\{(\mathbf{x}_p)_p \in \prod_{p\in S} \mathbb{Q}_p^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m \ , \ |\mathbf{x}_p|_p = 1 \text{ pour } p \in S_0\Big\},$$
$$N_{F,S}(m) := \Big|\Big\{\mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |F(\mathbf{x})|_p \le m \ , \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1\Big\}\Big|.$$

Soit μ_∞ la mesure de Lebesgue normalisée sur $\mathbb{R} = \mathbb{Q}_\infty$ avec $\mu_\infty([0,1]) = 1$ et μ_p la mesure de Haar normalisée sur $\mathbb{Q}_p$ avec $\mu_p(\mathbb{Z}_p) = 1$. On définit la mesure produit $\mu^n = \prod_{p\in S} \mu_p^n$ sur $\prod_{p\in S} \mathbb{Q}_p^n$.

Dans la littérature, il existe peu de résultats dans ce sens. Pour les formes décomposables F satisfaisant une condition de finitude appropriée, le résultat de Evertse dans [5] implique

$$N_{F,S}(1) \le 2(2^{33}d^2)^{n^3|S|}. \tag{0.0.17}$$

Dans sa thèse de master [9], de Jong a démontré un résultat pour les formes normes F comme dans (0.0.12) satisfaisant les trois conditions suivantes: (a) chaque n-uplet parmi les facteurs linéaires de F est linéairement indépendant, (b) le groupe de Galois de la clôture normale de $\mathbb{L}$ sur $\mathbb{Q}$ agit $n-1$ fois transitivement sur l'ensemble des conjugués $\{a^{(1)}, \ldots, a^{(r)}\}$ de chaque élément primitif a de $\mathbb{L}$, (c) $d \ge 2n^{5/3}$. Dans ces conditions, il a prouvé la formule asymptotique suivante:

$$N_{F,S}(m) = m^{\frac{n}{d}} \mu^n(\mathbb{A}_{F,S}(1)) + O_{F,S}(m^{f(n,d)}) \quad \text{lorsque} \quad m \to \infty$$

où $f(n,d) < n/d$ est une fonction ne dépendant que de n et d. La constante implicite dans le symbole $O_{F,S}$ ici et ci-dessous ne dépend que de F et S.

Pour nos généralisations p-adiques des théorèmes 0.0.11, 0.0.12 et 0.0.13, nous nous soucions surtout des exposants sur m plutôt que des exposants sur $\log m$. En fait, les exposants sur $\log m$ dans nos résultats sont légèrement plus grand que ceux de Thunder, ce qui est causé par l'estimation des petites solutions. Pour les preuves de nos résultats, nous suivons principalement les preuves de Thunder et apportons les modifications nécessaires dans le cadre p-adique. Comme l'un des principaux ingrédients des preuves, nous utilisons une version p-adique du Théorème du Sous-espace. (Pour une version plus générale, voir [6].)

La thèse est organisée comme suit.

Dans le Chapitre 1, nous introduisons quelques notations, des définitions, des faits généraux et lemmes de base.

Dans le Chapitre 2, nous montrons les résultats suivants. Pour $F = \prod_{i=1}^{d} L_i$, désignons par $I(F)$ l'ensemble des n-uplets ordonnés $(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})$ qui sont linéairement indépendants. Si $I(F) \neq \emptyset$, nous définissons

$$a(F) := \max_{(\mathbf{L}_{i_1},\ldots,\mathbf{L}_{i_n}) \in I(F)} \max_{1 \le j \le n-1} \frac{|\{\mathbf{L}_i \in \text{ vect } \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}|}{j}.$$

Theorem 0.0.14. *Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme décomposable de degré d. Supposons $F(\mathbf{x}) \neq 0$ pour chaque $\mathbf{x} \in \mathbb{Z}^n$ non nul et $a(F) < \frac{d}{n}$. Alors $\mu^n(\mathbb{A}_{F,S}(m)) \ll m^{n/d}$ où la constante implicite ne dépend que de n, d et S.*

Pour un polynôme F en n variables et une matrice $n \times n$ $M = (a_{ij})_{i,j=1,\ldots,n}$, on définit

$$F_M(X_1, \ldots, X_n) := F\Big(\sum_{j=1}^{n} a_{1j} X_j, \ldots, \sum_{j=1}^{n} a_{nj} X_j\Big).$$

Pour un sous-espace linéaire T de dimension $m \neq 0$ de $\mathbb{Q}^n$, nous choisissons $M_T \in \mathrm{GL}_n(\mathbb{Z})$ tel que $M_T^{-1}(T)$ est le sous-espace engendré par $\mathbf{e}_1, \ldots, \mathbf{e}_m$ où $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\mathbf{e}_2 = (0, 1, \ldots, 0)$, $\ldots, \mathbf{e}_m$ sont les m premiers vecteurs de la base standard de $\mathbb{Q}^n$. On note $F|_T$ la forme décomposable de degré d en m variables obtenue en restreignant F_{M_T} au sous-espace engendré par $\mathbf{e}_1, \ldots, \mathbf{e}_m$.

Theorem 0.0.15. *Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme décomposable de degré d. Supposons $F(\mathbf{x}) \neq 0$ pour chaque $\mathbf{x} \in \mathbb{Z}^n$ non nul. Supposons $a(F|_T) < \frac{d}{\dim T}$ pour chaque sous-espace linéaire T de dimension au moins 2 de $\mathbb{Q}^n$. Alors $N_{F,S}(m) \ll m^{n/d}$ où la constante implicite ne dépend que de n, d et S. De plus,*

$$N_{F,S}(m) = m^{\frac{n}{d}} \mu^n(\mathbb{A}_{F,S}(1)) + O_{F,S}(m^{\frac{n}{d+(1/2(n-1)^2)}}) \quad \textit{lorsque} \quad m \to \infty.$$

Les conditions du théorème 0.0.15 peuvent être vérifiées effectivement en un nombre fini d'étapes. En fait, on écrit $F = c \cdot \prod_{i=1}^{q} N_{\mathbb{K}_i/\mathbb{Q}}(L_i)$ où $c \in \mathbb{Q}^*$, $\mathbb{K}_i$ est un corps de nombres de degré d_i et $L_i = a_{i1}X_1 + \cdots + a_{in}X_n$ avec $\mathbb{Q}(a_{i1}, \ldots, a_{in}) = \mathbb{K}_i$ pour $i = 1, \ldots, q$. On définit la $\mathbb{Q}$-algèbre $\Omega = \mathbb{K}_1 \times \cdots \times \mathbb{K}_q$. Soit

$$V = \{(L_1(\mathbf{x}), \ldots, L_q(\mathbf{x})) : \mathbf{x} \in \mathbb{Q}^n\}.$$

Alors V est un $\mathbb{Q}$-espace vectoriel contenu dans Ω. Pour une $\mathbb{Q}$-sous-algèbre $\mathcal{B}$ de Ω, nous définissons

$$V^{\mathcal{B}} = \{a \in V : \mathcal{B} \cdot a \subseteq V\}.$$

C'est le plus grand sous-espace de V qui est fermé sous la multiplication scalaire par $\mathcal{B}$. Dans le Chapitre 3, nous prouvons le résultat suivant.

Theorem 0.0.16. *Les énoncés suivants sont équivalents:*

(a) $a(F|_T) < \frac{d}{\dim T}$ *pour chaque sous-espace linéaire T de dimension au moins 2 de $\mathbb{Q}^n$,*

(b) pour chaque $\mathbb{Q}$-sous-algèbre $\mathcal{B}$ de Ω avec $\dim_{\mathbb{Q}} \mathcal{B} > 1$, nous avons $V^{\mathcal{B}} = \{0\}$.

Dans le Chapitre 4, nous prouvons le théorème suivant.

Theorem 0.0.17. *Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme décomposable de degré $n+1$. Supposons $F(\mathbf{x}) \neq 0$ pour chaque $\mathbf{x} \in \mathbb{Z}^n$ non nul. Supposons $a(F|_T) < \frac{d}{\dim T}$ pour chaque sous-espace linéaire T de dimension au moins 2 de $\mathbb{Q}^n$. Alors nous avons $D(F) \neq 0$ et*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll \frac{m^{(n-1)/n}(1+\log m)^{|S|(n+1)}}{(\prod_{p \in S} |D(F)|_p)^{\frac{1}{2n(n+1)}}} + m^{\frac{n-1}{n+1}}(1+\log m)^{|S|(n-1)}$$

où la constante implicite ne dépend que de n et S.

Dans le Chapitre 5, nous considérons le cas plus général où le degré d de F et le nombre de variables n sont premiers entre eux. Nous prouvons le théorème suivant.

Theorem 0.0.18. *Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme décomposable de degré d. Supposons $F(\mathbf{x}) \neq 0$ pour chaque $\mathbf{x} \in \mathbb{Z}^n$ non nul. Supposons $a(F|_T) < \frac{d}{\dim T}$ pour chaque sous-espace linéaire T de dimension au moins 2 de $\mathbb{Q}^n$. Si $\gcd(n,d) = 1$, nous avons*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll m^{n/(d+1/(n-1)^2)}(1 + \log m)^{2d|S|}$$

où la constante implicite ne dépend que de n, d et S.

Nous terminons cette introduction avec certains problèmes ouverts.

(a) Retirer la condition de coprimalité $\gcd(n, d) = 1$ dans le théorème de Thunder 0.0.13. Par exemple, le théorème 0.0.13 vaut pour des formes binaires de degré impair. Pouvons-nous prouver le même résultat pour les formes binaires de degré pair?

(b) Les constantes implicites dans les théorèmes 0.0.17 et 0.0.18 dépendent de n, d et les nombres premiers dans S. Compte tenu de (0.0.17), pouvons nous les remplacer par des constantes ne dépendant que de n, d et le cardinal de S? De plus, pouvons nous donner une borne supérieure pour $\mu^n(\mathbb{A}_{F,S}(1))$ ne dépendant que de n, d et le cardinal de S?

Chapter 1

Preliminaries

In this chapter, we have collected definitions, facts and basic lemmas that are used throughout the thesis.

1.1 Decomposable forms

Definition 1.1.1. *A homogeneous polynomial $F \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree d is called a decomposable form if it factorizes into linear forms over some algebraic closure of $\mathbb{Q}$.*

Lemma 1.1.2. *Let $F \in \mathbb{Q}[X_1, \ldots, X_n]$ be any decomposable form. Then it factors into linear forms over some algebraic number field.*

Proof. [3, Chapter 2, Theorem 1] □

For a polynomial F in n variables and an $n \times n$ matrix $T = (a_{ij})_{i,j=1,\ldots,n}$, we define

$$F_T(X_1, \ldots, X_n) := F(\sum_{j=1}^{n} a_{1j}X_j, \ldots, \sum_{j=1}^{n} a_{nj}X_j).$$

Definition 1.1.3. *Two homogeneous polynomials $F, G \in \mathbb{Z}[X_1, \ldots, X_n]$ of the same degree are called equivalent if there exists a matrix $T \in GL_n(\mathbb{Z})$ such that $F = G_T$.*

Definition 1.1.4. *A norm form over* $\mathbb{Q}$ *is a decomposable form of the shape*

$$F = AN_{\mathbb{L}/\mathbb{Q}}(\lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n) = \prod_{i=1}^{d} \big(\sigma_i(\lambda_1)X_1 + \sigma_i(\lambda_2)X_2 + \cdots + \sigma_i(\lambda_n)X_n\big)$$

where $A \in \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ *and* $\sigma_1, \ldots, \sigma_d$ *are the embeddings of* $\mathbb{L}$ *in* $\overline{\mathbb{Q}}$.

Lemma 1.1.5. *Let* $F \in \mathbb{Q}[X_1, \ldots, X_n]$ *be a decomposable form which is irreducible over* $\mathbb{Q}$*. Then* F *is a norm form.*

Proof. [3, Chapter 2, Theorem 2] □

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Let $\mathcal{P}$ be the set of all primes and $M_{\mathbb{Q}} = \mathcal{P} \cup \{\infty\}$. We denote the set of places of $\mathbb{Q}$ by $M_{\mathbb{Q}}$. Let $S = \{\infty, p_1, \ldots, p_r\}$ be a fixed (once for all) finite subset of $M_{\mathbb{Q}}$, where $p_1, .., p_r$ are primes. Put $S_0 = S \setminus \{\infty\}$. We are interested in the solutions to inequalities of the shape

$$\begin{gathered} \textstyle\prod_{p \in S} |F(\mathbf{x})|_p \leq m \ \text{ in } \ \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{with } \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \end{gathered} \tag{1.1.1}$$

Define $I_{F,S}(m)$ to be the set of solutions to (1.1.1) and put $N_{F,S}(m) = |I_{F,S}(m)|$.

By Lemma 1.1.2, every decomposable form $F \in \mathbb{Z}[X_1, \ldots, X_n]$ can be factored into linear forms over some number field. Let $\mathbb{K}$ be the smallest extension of $\mathbb{Q}$ in which F factorizes into linear forms. This field is called the splitting field of F. Write $F = \prod_{i=1}^{d} L_i$ with $L_i \in \mathbb{K}[X_1, \ldots, X_n]$ linear forms. For every $p \in M_{\mathbb{Q}}$, we choose an extension of $|\cdot|_p$ to $\mathbb{K}$. For $p \in M_{\mathbb{Q}}$, let $\mathbb{K}_p$ be the completion of $\mathbb{K}$ at $|\cdot|_p$. Identify $\mathbb{K}$ as a subfield of $\mathbb{K}_p$. We use the same factorization of F for each $p \in S$.

Henceforth, we fix a factorization $F = \prod_{i=1}^{g} F_i = \prod_{i=1}^{d} L_i$, where $F_1, \ldots, F_g \in \mathbb{Z}[X_1, \ldots, X_n]$ are irreducible and $L_1, \ldots, L_d \in \mathbb{K}[X_1, \ldots, X_n]$ are linear forms.

We denote the coefficient vector of a linear form $L(\mathbf{X})$ by $\mathbf{L}$, that is, if $L(\mathbf{X}) = a_1 X_1 + \cdots + a_n X_n$, then $\mathbf{L} = (a_1, \ldots, a_n)$. Conversely, the linear form associated to $\mathbf{M} = (b_1, \ldots, b_n)$ is $M(\mathbf{X}) = b_1 X_1 + \cdots + b_n X_n$.

Let $I(F)$ denote the set of all ordered n-tuples $(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})$ which are linearly independent over $\mathbb{K}$.

We define the L^2-norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n$ by $|\mathbf{x}|_\infty := \sqrt{|x_1|^2 + \cdots + |x_n|^2}$. For $p \in \mathcal{P}$, $\mathbf{x} = (x_1, \ldots, x_n) \in \overline{\mathbb{Q}}_p^n$, we define the p-sup-norm of $\mathbf{x}$ by $|\mathbf{x}|_p = \max\{|x_1|_p, \ldots, |x_n|_p\}$.

For each $p \in S$, define

$$H_p(F) := \prod_{i=1}^{d} |\mathbf{L}_i|_p$$

where $|\cdot|_\infty$ denotes the L^2-norm and $|\cdot|_p$ ($p \in S_0$) denotes the p-sup-norm. Then the *height* of F is given by

$$\mathcal{H}(F) = \prod_{p \in S} H_p(F). \tag{1.1.2}$$

Note that $H_p(F)$ is independent of the factorization of F for each $p \in S$ and so is $\mathcal{H}(F)$.

Define the semi-discriminant $S(F)$ of F by

$$S(F) := \prod_{(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n}) \in I(F)} \det(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n}).$$

It is known that $S(F) \in \mathbb{Q}$ (see, e.g. [19], Lemma 2).

For $p \in S$, define the normalized p-adic semi-discriminant by

$$NS(F)_p := \prod_{(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n}) \in I(F)} \frac{|\det(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})|_p}{\prod_{j=1}^{n} |\mathbf{L}_{i_j}|_p}.$$

Define $b(\mathbf{L}_i)$ as the number of times that $\mathbf{L}_i$ appears in some element of $I(F)$ and put

$$b(F) := \max_{1 \le i \le d} b(\mathbf{L}_i).$$

Since any two linear forms dividing the same factor F_l of F are conjugate to one another, we have $b(\mathbf{L}_{i_1}) = b(\mathbf{L}_{i_2})$ whenever L_{i_1} and L_{i_2} belong to the same factor F_l of F. Put $b(l) := b(\mathbf{L}_i)$ for any linear factor L_i of F_l.

Let $\mathbb{K}$ be an algebraic number field. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{K}^n$, define

$$|\mathbf{x}|_p = (|x_1|_p^2 + \cdots + |x_n|_p^2)^{1/2} \text{ if } p \text{ is archimedean,}$$

$$|\mathbf{x}|_p = \max(|x_1|_p, \ldots, |x_n|_p) \text{ if } p \text{ is nonarchimedean.}$$

The *field height* $H_{\mathbb{K}}(\mathbf{x})$ of $\mathbf{x}$ is defined as

$$H_{\mathbb{K}}(\mathbf{x}) = \prod_{p \in M_{\mathbb{K}}} |\mathbf{x}|_p^{d_p}$$

where $d_p = [\mathbb{K}_p : \mathbb{Q}_p]$ is the local degree.

Lemma 1.1.6. *Let $F = \prod_{i=1}^{d} L_i \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form. Then each L_i is proportional to a linear form L_i' with algebraic coefficients in an algebraic number field of degree at most d. Furthermore,*

$$\mathcal{H}(F) \geq H_{\mathbb{Q}(\mathbf{L}_i')}(\mathbf{L}_i') \geq 1 \text{ for } i = 1, \ldots, d.$$

Proof. This lemma follows from [19, Lemma 2]. For the convenience of the readers, we give the proof.

First, suppose that F is irreducible over $\mathbb{Q}$. We know that $F(\mathbf{X}) = c \cdot N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X}))$ for some number field $\mathbb{K}$ and some $c \in \mathbb{Q}^*$. Then any linear factor L_i of F is proportional to some conjugate of L. Choose for each $p \in S$ an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$. Assume that $F = a \cdot F'$ where $a \in \mathbb{Z}$ and F' is primitive, i.e., the coefficients of F have gcd 1. Then by Gauss's Lemma for each $p \in S_0$, we have

$$H_p(F) = \prod_{i=1}^{d} |\mathbf{L}_i|_p = |aF'|_p = |a|_p.$$

Hence by the product formula

$$\mathcal{H}(F) = H_\infty(F) \cdot \prod_{p \in S_0} H_p(F) = \frac{H_\infty(F)}{|a|} \cdot \prod_{p \in S} |a|_p \geq \frac{H_\infty(F)}{|a|}.$$

By [19, Lemma 2], we have $H_\infty(F)/|a| = H_{\mathbb{K}}(\mathbf{L}) \geq 1$. Hence

$$\mathcal{H}(F) \geq H_{\mathbb{K}}(\mathbf{L}) \geq 1.$$

Second, suppose that $F = \prod_{l=1}^{g} F_l$ where $F_l \in \mathbb{Z}[X_1, \ldots, X_n]$ is an irreducible form. Then any L_i of F is a linear factor of F_{l_i} $(1 \leq l_i \leq g)$ and hence proportional to some L_i'

with algebraic coefficients in a number field of degree at most $\deg(F_{l_i}) \le d$ and satisfying $\mathcal{H}(F_{l_i}) \ge H_{\mathbb{Q}(\mathbf{L}_i')}(\mathbf{L}_i') \ge 1$. Therefore

$$\mathcal{H}(F) = \prod_{l=1}^{g} \mathcal{H}(F_l) \ge \mathcal{H}(F_{l_i}) \ge 1.$$

□

We often use the following well known lemma, which is called Hadamard's inequality.

Lemma 1.1.7. *Let $p \in M_{\mathbb{Q}}$ and $\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n} \in \overline{\mathbb{Q}}_p^n$. Then we have*

$$\frac{|\det(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})|_p}{\prod_{j=1}^{n} |\mathbf{L}_{i_j}|_p} \le 1.$$

Lemma 1.1.8. *Assume that $I(F) \ne \emptyset$. Then we have*

(a) $\prod_{p \in S} NS(F)_p \ge \mathcal{H}(F)^{-b(F)}$.

(b) For each tuple $(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn}) \in I(F)$ $(p \in S)$, we have

$$1 \le \prod_{p \in S} \frac{\prod_{j=1}^{n} |\mathbf{L}_{pj}|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p} \le \mathcal{H}(F)^{\frac{b(F)}{n!}}.$$

Proof. This lemma follows from [19, Lemma 3]. For the convenience of the readers, we give the proof.

(a) First, there is no loss of generality to assume that F is primitive. Indeed, let $F = aF'$ with F' primitive and $a \in \mathbb{Z}$, and assume that (a) is true for F'. Then we have $b(F) = b(F')$,

$$\prod_{p \in S} NS(F)_p = \prod_{p \in S} NS(F')_p,$$

and also

$$\mathcal{H}(F)^{-b(F)} = (\prod_{p \in S} |a|_p)^{-b(F)} \cdot \mathcal{H}(F')^{-b(F)} \le \mathcal{H}(F')^{-b(F)} = \mathcal{H}(F')^{-b(F')}.$$

Hence

$$\prod_{p\in S} NS(F)_p = \prod_{p\in S} NS(F')_p \geq \mathcal{H}(F')^{-b(F')} \geq \mathcal{H}(F)^{-b(F)}.$$

Now assume that F is primitive. Recall that $S(F) \in \mathbb{Q}$. For $p \in M_{\mathbb{Q}} \setminus S$, we have

$$\begin{aligned}
|S(F)|_p &= \prod_{(i_1,\ldots,i_n)\in I(F)} |\det(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})|_p \\
&\leq \prod_{(i_1,\ldots,i_n)\in I(F)} |\mathbf{L}_{i_1}|_p \cdot |\mathbf{L}_{i_2}|_p \cdots |\mathbf{L}_{i_n}|_p = \prod_{l} |F_l|_p^{b(l)} = 1
\end{aligned}$$

and then by the product formula,

$$\prod_{p\in S} |S(F)|_p = \frac{1}{\prod_{p\in M_{\mathbb{Q}}\setminus S} |S(F)|_p} \geq 1.$$

Hence

$$\begin{aligned}
\prod_{p\in S} NS(F)_p = \prod_{p\in S} \frac{|S(F)|_p}{\prod_{I(F)} \prod_{j=1}^{n} |\mathbf{L}_{i_j}|_p} &= \frac{\prod_{p\in S} |S(F)|_p}{\prod_{p\in S} \prod_{i=1}^{d} |\mathbf{L}_i|_p^{b(\mathbf{L}_i)}} \\
\geq \frac{1}{\prod_{p\in S} \prod_{l=1}^{g} H_p(F_l)^{b(l)}} &= \frac{1}{\prod_{l=1}^{g} H_\infty(F_l)^{b(l)}} \\
\geq \frac{1}{H_\infty(F)^{b(F)}} &= \frac{1}{\mathcal{H}(F)^{b(F)}}
\end{aligned}$$

(b) Apply Hadamard's inequality. For each $\{(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn}) : p \in S\}$ in $I(F)$ we have

$$1 \leq \prod_{p\in S} \frac{\prod_{j=1}^{n} |\mathbf{L}_{pj}|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p} \leq \Big(\prod_{p\in S} NS(F)_p\Big)^{\frac{-1}{n!}} \leq \mathcal{H}(F)^{\frac{b(F)}{n!}}.$$

□

1.2 Measures, geometry of numbers

In this section, let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d such that $F(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Q}^n \setminus \{0\}$. Let S be a finite subset of $M_{\mathbb{Q}}$ including ∞. Define

$$\mathbb{Z}_S := \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for } p \notin S\}$$

and $\mathbb{A}_S^n := \prod_{p\in S}\mathbb{Q}_p^n$. We identify $\mathbb{Q}^n$ with a subset of $\mathbb{A}_S^n$ via the diagonal embedding.

Let μ_∞ be the normalized Lebesgue measure on $\mathbb{R} = \mathbb{Q}_\infty$ such that $\mu_\infty([0,1]) = 1$. Let μ_∞^n be the product measure on $\mathbb{R}^n$. For $p \in S_0$, let μ_p be the normalized Haar measure on $\mathbb{Q}_p$ such that $\mu_p(\mathbb{Z}_p) = 1$. Let μ_p^n be the product measure on $\mathbb{Q}_p^n$. Define the product measure $\mu^n = \prod_{p\in S}\mu_p^n$ on $\mathbb{A}_S^n$.

Define

$$\mathbb{A}_{F,S}(m) := \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S}|F(\mathbf{x}_p)|_p \le m\ ,\ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\}.$$

We view $\mathbb{Z}_S^n$ as a subset of $\mathbb{A}_S^n$ by identifying $\mathbf{x} \in \mathbb{Z}_S^n$ with $(\mathbf{x})_{p\in S} \in \mathbb{A}_S^n$. With this identification, we may interpret the set of the solutions of (1.1.1) as $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$.

1.2.1 Counting lattice points

We prove a general result on counting the number of lattice points in a symmetric convex body. Here, by a lattice we mean a free $\mathbb{Z}$-module of rank n in $\mathbb{Q}^n$. For $p \in \mathcal{P}$, we view $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$. For a lattice M, we define

$$M_p = \mathbb{Z}_pM = \Big\{\sum_{i\in I}\zeta_i\mathbf{m}_i : \zeta_i \in \mathbb{Z}_p,\ \mathbf{m}_i \in M, I \text{ finite}\Big\}.$$

Lemma 1.2.1. *(a) Let M be a lattice and p be a prime, then M_p is a free $\mathbb{Z}_p$-module of rank n.*

(b) If $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ is a $\mathbb{Z}_p$-basis of M_p, then $|\det(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)|_p = |\det M|_p$.

Proof. Obvious.

□

Let $A_p \in GL(n, \mathbb{Q}_p)$ for $p \in S_0$ and $A_q = \mathrm{Id}$ for $q \in \mathcal{P}\setminus S_0$ where Id is the $n\times n$ unit matrix. Define

$$M = \{\mathbf{x} \in \mathbb{Q}^n : |A_p\mathbf{x}|_p \le 1 \text{ for } p \in \mathcal{P}\}.$$

The following lemma is well-known. For the convenience of the readers, we give the proof.

Lemma 1.2.2. *(a) M is a lattice.*

(b) We have $M_p = \{\mathbf{x} \in \mathbb{Q}_p^n : |A_p\mathbf{x}|_p \le 1\}$ for $p \in \mathcal{P}$.

(c) $|\det M| = \prod_{p\in S_0} |\det(A_p)|_p$.

Proof. (a) For $p \in \mathcal{P}$, write $A_p = (a_{ij})_{i,j}$ and $A_p^{-1} = (b_{ij})_{i,j}$. Define $C_p = \max_{i,j}\{|a_{ij}|_p, |b_{ij}|_p\}$. Then $C_p > 0$ for $p \in S_0$ and $C_p = 1$ for $p \in \mathcal{P} \setminus S$. Choose $\alpha \in \mathbb{Q}^*$ such that $|\alpha|_p = C_p^{-1}$ for $p \in \mathcal{P}$. For every $\mathbf{x} \in \mathbb{Q}_p^n$ and $p \in \mathcal{P}$, we have

$$|A_p\mathbf{x}|_p \le (\max_{i,j} |a_{ij}|_p) \cdot |\mathbf{x}|_p \le C_p|\mathbf{x}|_p \ ,$$
$$|\mathbf{x}|_p = |(A_p^{-1} \cdot A_p)\mathbf{x}|_p = |A_p^{-1}(A_p\mathbf{x})|_p \le C_p|A_p\mathbf{x}|_p \ .$$

Hence $C_p^{-1}|\mathbf{x}|_p \le |A_p\mathbf{x}|_p \le C_p|\mathbf{x}|_p$ for $p \in \mathcal{P}$. Then for $m \in M$, we have

$$|\alpha m|_p = C_p^{-1}|m|_p \le |A_p m|_p \le 1 \text{ for } p \in \mathcal{P}.$$

Hence $\alpha m \in \mathbb{Z}^n$. So $M \subseteq \alpha^{-1}\mathbb{Z}^n$.

On the other hand, for $\mathbf{x} \in \alpha\mathbb{Z}^n$, we have $|\alpha^{-1}\mathbf{x}|_p \le 1$ for $p \in \mathcal{P}$. Hence

$$|A_p\mathbf{x}|_p \le C_p|\mathbf{x}|_p \le |\alpha^{-1}\mathbf{x}|_p \le 1 \text{ for } p \in \mathcal{P}.$$

This implies $\alpha\mathbb{Z}^n \subseteq M$. So $\alpha\mathbb{Z}^n \subseteq M \subseteq \alpha^{-1}\mathbb{Z}^n$ which implies that M is a lattice.

(b) Let $p \in \mathcal{P}$ and define $R_p := \{\mathbf{x} \in \mathbb{Q}_p^n : |A_p\mathbf{x}|_p \le 1\}$. By definition

$$M_p = \mathbb{Z}_p M = \Big\{ \sum_{\text{finite}} \zeta_i \mathbf{m}_i : \zeta_i \in \mathbb{Z}_p,\ \mathbf{m}_i \in M \Big\}.$$

Since $|A_p\mathbf{m}_i|_p \le 1$ for $\mathbf{m}_i \in M$, we have $|A_p\mathbf{m}|_p \le 1$ for $\mathbf{m} \in M_p$. Hence $M_p \subseteq R_p$.

We need to prove $R_p \subseteq M_p$. Let $\mathbf{x} \in R_p$. There is $\mathbf{x}' \in \mathbb{Q}^n$ such that $|\mathbf{x} - \mathbf{x}'|_p \le |\alpha|_p$ and $|A_p(\mathbf{x} - \mathbf{x}')|_p \le 1$. Hence $|A_p\mathbf{x}'|_p \le 1$ and $\mathbf{x} - \mathbf{x}' \in \alpha\mathbb{Z}_p^n \subseteq M_p$. So it suffices to prove that $\mathbf{x}' \in M_p$. By the Chinese Remainder Theorem, there is $\beta \in \mathbb{Q}$ such that

$$|\beta - 1|_p < 1 \quad , \quad |\beta|_q |A_q\mathbf{x}'|_q \le 1 \text{ for } q \ne p.$$

So $|\beta|_p = 1$. Now we have $|A_p(\beta\mathbf{x}')|_p = |A_p\mathbf{x}'|_p \le 1$ and $|A_q(\beta\mathbf{x}')|_q \le 1$ for $q \ne p$. Hence $\beta\mathbf{x}' \in M$. Since $\beta \in \mathbb{Z}_p^*$, it follows that $\mathbf{x}' \in M_p$. Therefore, also $\mathbf{x} \in M_p$.

(c) For each $p \in \mathcal{P}$,

$$M_p = \left\{\mathbf{x} \in \mathbb{Q}_p^n : |A_p\mathbf{x}|_p \le 1\right\} = \left\{\mathbf{x} \in \mathbb{Q}_p^n : A_p\mathbf{x} \in \mathbb{Z}_p^n\right\} = A_p^{-1}\mathbb{Z}_p^n.$$

This implies that the columns of A_p^{-1} serve as a $\mathbb{Z}_p$-basis of M_p. Hence

$$|\det M|_p = |\det A_p^{-1}|_p = |\det A_p|_p^{-1}.$$

Since $\det M \in \mathbb{Q}$, we have

$$|\det M| = \prod_{p\in\mathcal{P}} |\det M|_p^{-1} = \prod_{p\in S_0} |\det M|_p^{-1} = \prod_{p\in S_0} |\det A_p|_p.$$

□

The following two lemmas are Lemma 8 and Lemma 9 from Thunder [19]. They allow us to bound the number of lattice points inside a symmetric convex body.

Lemma 1.2.3. *Let $\mathcal{C} \subset \mathbb{R}^n$ be a symmetric convex body and let $\Lambda \subset \mathbb{R}^n$ be a lattice. Suppose there are n linearly independent lattice points in $\mathcal{C} \cap \Lambda$. Then there are $y_1, y_2, \ldots, y_n \in \mathcal{C}$ such that*

$$|\mathcal{C} \cap \Lambda| \le 3^n 2^{n(n-1)/2} \frac{|\det(y_1, y_2, \ldots, y_n)|}{\det \Lambda}.$$

Lemma 1.2.4. *Let $a_1, a_2, \ldots, a_n$ be positive reals and $K_1', K_2', \ldots, K_n' \in \mathbb{C}[X_1, \ldots, X_n]$ linearly independent linear forms with $|\det(\mathbf{K}_1', \ldots, \mathbf{K}_n')| = 1$. Let $\mathcal{C} = \{y \in \mathbb{R}^n : |K_i'(y)| \le a_i,\ i = 1, \ldots, n\}$. Then $\mathcal{C} \cap \mathbb{Z}^n$ either lies in a proper linear subspace of $\mathbb{Q}^n$ or*

$$|\mathcal{C} \cap \mathbb{Z}^n| \le 3^n 2^{n(n-1)/2} n! \prod_{i=1}^n a_i.$$

The volume of $\mathcal{C}$ is at most $2^n n! \prod_{i=1}^n a_i$.

Apply these lemmas to the following situation. Let

$$\mathcal{C} := \{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \le a_{pi} \text{ for } p \in S, i = 1, \dots, n\},$$

where for $p \in S$ $K'_{p1}, \dots, K'_{pn}$ are linearly independent linear forms in $\mathbb{Q}_p[X_1, \dots, X_n]$ with

$$|\det(K'_{p1}, K'_{p2}, \dots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1$$

and the a_{pi} are positive reals.

Lemma 1.2.5. *Let $\mathcal{C}$ be as above. Then we have*

$$\mu^n(\mathcal{C}) \ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi}.$$

Assume that there are n linearly independent points in $\mathcal{C} \cap \mathbb{Q}^n$. Then we have

$$|\mathcal{C} \cap \mathbb{Z}_S^n| \ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi}.$$

The implicit constants implied by the $\ll$ symbols depend only on n, S

Proof. For each $p \in S_0$, we choose $\lambda_{pi} \in \mathbb{Q}_p^*$ such that $a_{pi} \le |\lambda_{pi}|_p < p a_{pi}$. For $p = \infty$, we choose $\lambda_{\infty i} = a_{\infty i}$. Then

$$\mathcal{C} = \{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |\lambda_{pi}^{-1} K'_{pi}(\mathbf{x}_p)|_p \le 1 \text{ for } p \in S, i = 1, \dots, n\}.$$

For $p \in S_0$, let A_p be a matrix with rows $(\lambda_{p1}^{-1}\mathbf{K}'_{p1}, \lambda_{p2}^{-1}\mathbf{K}'_{p2}, \dots, \lambda_{pn}^{-1}\mathbf{K}'_{pn})$. Let $A_q =$ Id, for $q \in \mathcal{P} \setminus S_0$.

Define

$$O := \{\mathbf{x} \in \mathbb{R}^n : |\lambda_{\infty i}^{-1} K'_{\infty i}(\mathbf{x})| \le 1 \ , \ i = 1, \dots, n\},$$
$$\Lambda := \{\mathbf{x} \in \mathbb{Z}_S^n : |A_p(\mathbf{x})|_p \le 1 \ , p \in S_0\}.$$

Then O is a symmetric convex body. By Lemma 1.2.2, Λ is a lattice and clearly

$$\mathcal{C} \cap \mathbb{Z}_S^n = O \cap \Lambda.$$

Suppose there are n linearly independent lattice points in O. Then by Lemma 1.2.3 and Lemma 1.2.4, there are $y_1, y_2, \ldots, y_n \in O$ such that

$$|O \cap \Lambda| \leq 3^n 2^{n(n-1)/2} \frac{|\det(y_1, y_2, \ldots, y_n)|}{\det \Lambda} \leq 3^n 2^{n(n-1)/2} \cdot \frac{n! \prod_{i=1}^n a_{\infty i}}{\det \Lambda}.$$

By Lemma 1.2.2, we have

$$\begin{aligned} |\det \Lambda| &= \prod_{p \in S_0} |A_p|_p = \prod_{p \in S_0} |\det(\lambda_{p1}^{-1}\mathbf{K}'_{p1}, \lambda_{p2}^{-1}\mathbf{K}'_{p2}, \ldots, \lambda_{pn}^{-1}\mathbf{K}'_{pn})|_p \\ &= \prod_{p \in S_0} \frac{|\det(\mathbf{K}'_{p1}, \mathbf{K}'_{p2}, \ldots, \mathbf{K}'_{pn})|_p}{\prod_{i=1}^n |\lambda_{pi}|_p} = \frac{1}{\prod_{p \in S_0} \prod_{i=1}^n |\lambda_{pi}|_p} \geq \frac{1}{\prod_{p \in S_0} \prod_{i=1}^n p a_{pi}}. \end{aligned} \tag{1.2.1}$$

Hence

$$\begin{aligned} |\mathcal{C} \cap \mathbb{Z}_S^n| = |O \cap \Lambda| &\leq 3^n 2^{n(n-1)/2} n! \frac{\prod_{i=1}^n a_{\infty i}}{\det \Lambda} \\ &\leq 3^n 2^{n(n-1)/2} n! \prod_{p \in S_0} p^n \cdot \prod_{p \in S} \prod_{i=1}^n a_{pi}. \end{aligned} \tag{1.2.2}$$

Now we compute the volume of $\mathcal{C}$. For $p \in S_0$, define the $\mathbb{Q}_p$-linear map $\phi_p : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ by $\mathbf{y}_p = \phi_p(\mathbf{x}_p) = A_p \mathbf{x}_p$. Further, let $\phi_\infty = \mathrm{Id}$. This gives a product map $\Phi = \prod_{p \in S} \phi_p : \mathbb{A}_S^n \to \mathbb{A}_S^n$. Then we have

$$\Phi(\mathcal{C}) = \{(\mathbf{y}_p)_{p \in S} \in \mathbb{A}_S^n : |K'_{\infty i}(\mathbf{x}_\infty)|_\infty \leq a_{\infty i} \ , \ |\mathbf{y}_p|_p \leq 1 \text{ for } p \in S_0 \ , \ i = 1, \ldots, n\}.$$

Hence, using (1.2.1)

$$\begin{aligned} \mu_\infty^n(O) = \mu^n(\Phi(\mathcal{C})) &= \prod_{p \in S} |\det \phi_p|_p \cdot \mu^n(\mathcal{C}) = \prod_{p \in S_0} |\det A_p|_p \cdot \mu^n(\mathcal{C}) \\ &= \frac{1}{\prod_{p \in S_0} \prod_{i=1}^n |\lambda_{pi}|_p} \cdot \mu^n(\mathcal{C}) = |\det \Lambda| \cdot \mu^n(\mathcal{C}). \end{aligned}$$

Therefore

$$\mu^n(\mathcal{C}) = \frac{\mu_\infty^n(O)}{|\det \Lambda|} \leq \frac{2^n n! \prod_{i=1}^n a_{\infty i}}{|\det \Lambda|} \leq 2^n n! \prod_{p \in S_0} p^n \cdot \prod_{p \in S} \prod_{i=1}^n a_{pi}.$$

□

1.2.2 Geometry of numbers

In this section, we recall some results from the adelic Geometry of numbers.

Definition 1.2.6. *An n-dimensional symmetric p-adic convex body is a set $\mathcal{C}_p \subset \mathbb{Q}_p^n$ with the following properties:*

(a) $\mathcal{C}_p$ is compact in the topology of $\mathbb{Q}_p^n$ and has 0 as an interior point,

(b) for $\mathbf{x} \in \mathcal{C}_p$, $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$ we have $a\mathbf{x} \in \mathcal{C}_p$,

(c) if $p = \infty$, then for $\mathbf{x}, \mathbf{y} \in \mathcal{C}_\infty$, $\lambda \in \mathbb{R}$ with $0 \leq \lambda \leq 1$ we have $(1-\lambda)\mathbf{x} + \lambda\mathbf{y} \in \mathcal{C}_p$,

(d) if p is finite, then for $\mathbf{x}, \mathbf{y} \in \mathcal{C}_p$ we have $\mathbf{x} + \mathbf{y} \in \mathcal{C}_p$.

Definition 1.2.7. *An n-dimensional S-convex body is a Cartesian product*

$$\mathcal{C} = \prod_{p \in S} \mathcal{C}_p \subset \prod_{p \in S} \mathbb{Q}_p^n = \mathbb{A}_S^n$$

where for $p \in S$, $\mathcal{C}_p$ is an n-dimensional symmetric p-adic convex body.

For $\lambda > 0$ set

$$\lambda\mathcal{C} := \lambda\mathcal{C}_\infty \times \prod_{p \in S_0} \mathcal{C}_p.$$

For $i = 1, \ldots, n$, we define the *i-th successive minimum* λ_i of $\mathcal{C}_p$ to be the minimum of all $\lambda \in \mathbb{R}_{\geq 0}$ such that $\lambda\mathcal{C}_p \cap \mathbb{Z}_S^n$ contains at least i $\mathbb{Q}$-linearly independent points. From the definition of p-adic convex body and from the fact that $\mathbb{Z}_S^n$ is discrete in $\mathbb{A}_S^n$, it follows that these minima exist and

$$0 < \lambda_1 \leq \cdots \leq \lambda_n < \infty.$$

For $p \in S$, let $M_{p1}, \ldots, M_{pn}$ be linearly independent linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$. Define

$$\mathcal{C}_p := \left\{ \mathbf{x} \in \mathbb{Q}_p^n : \max_{1 \leq i \leq n} |M_{pi}(\mathbf{x})|_p \leq 1 \right\}.$$

Then $\mathcal{C}_p$ is a symmetric p-adic convex body and $\prod_{p \in S} \mathcal{C}_p$ is a n-dimensional S-convex body.

Let $\lambda_1, \ldots, \lambda_n$ denote the successive minima of $\prod_{p \in S} \mathcal{C}_p$.

Lemma 1.2.8.

$$\lambda_1 \cdots \lambda_n \ll \prod_{p \in S} |\det(\mathbf{M}_{p1}, \dots, \mathbf{M}_{pn})|_p$$

Proof. See Lemma 6 in [6]. □

For a linear form $L = a_1 X_1 + \cdots + a_n X_n$ with $a_1, \dots, a_n \in \overline{\mathbb{Q}}_p$ and $\sigma \in Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, define $\sigma(L) := \sigma(a_1)X_1 + \cdots + \sigma(a_n)X_n$.

Definition 1.2.9. *For $p \in M_{\mathbb{Q}}$, a set $\mathcal{L} = \{L_1, \dots, L_d\}$ of linear forms with coefficients in $\overline{\mathbb{Q}}_p$ (resp. a finite extension $\mathbb{E}_p$ of $\mathbb{Q}_p$) is called $\mathbb{Q}_p$-symmetric (resp. $Gal(\mathbb{E}_p/\mathbb{Q}_p)$-symmetric) if for every $\sigma \in Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (resp. $\sigma \in Gal(\mathbb{E}_p/\mathbb{Q}_p)$)*

$$\sigma(\mathcal{L}) := \{\sigma(L_1), \dots, \sigma(L_d)\} = \mathcal{L}.$$

We also need the following lemma. Let $d \geq n$ be an integer. For $p \in S$, let

$$\mathcal{L}_p = \{L_{p1}, \dots, L_{pd}\} \subset \overline{\mathbb{Q}}_p[X_1, \dots, X_n]$$

be a $\mathbb{Q}_p$-symmetric set of linear forms of maximal rank n. Define

$$\mathcal{C}_p := \Big\{\mathbf{x} \in \mathbb{Q}_p^n : \max_{1 \leq i \leq d} |L_{pi}(\mathbf{x})|_p \leq 1\Big\}.$$

Let $\lambda_1, \dots, \lambda_n$ be the successive minima of $\prod_{p \in S} \mathcal{C}_p$. Further let

$$R_p = R_p(\mathcal{L}_p) := \max_{1 \leq i_1, \dots, i_n \leq d} |\det(L_{pi_i}, \dots, L_{pi_n})|_p$$

where the maximum is taken over all tuples $i_1, \dots, i_n$ from $\{1, \dots, d\}$.

Lemma 1.2.10.

$$\lambda_1 \cdots \lambda_n \ll \prod_{p \in S} R_p$$

Proof. See [6, Lemma 6]. □

1.3 Basic properties of the volume of $\mathbb{A}_{F,S}(m)$

Recall that

$$\mathbb{A}_{F,S}(m) = \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \leq m, |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\}.$$

In this section, we show how the volume of $\mathbb{A}_{F,S}(m)$ changes under some actions defined below. In fact, we can consider a slightly more general situation by letting F vary at each $p \in S$.

Let $S = \{\infty, p_1, \ldots, p_r\}$. For each $p \in S$, take $T_p \in GL_n(\mathbb{Q}_p)$ and let $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ be a decomposable form of degree d. Define

$$\mathbb{A}(F_p : p \in S, m) := \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F_p(\mathbf{x}_p)|_p \leq m \ , \ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\}.$$

Write

$$\mathbb{A}(F_p : p \in S) := \mathbb{A}(F_p : p \in S, 1).$$

The first fact we notice is that the volume of $\mathbb{A}(F_p : p \in S, m)$ is homogeneous in m.

Lemma 1.3.1. *For $m \in \mathbb{R}_{\geq 0}$, we have*

$$\mu^n\big(\mathbb{A}(F_p : p \in S, m)\big) = m^{n/d}\mu^n\big(\mathbb{A}(F_p : p \in S)\big).$$

Remark 1.3.2. The statement is also true if $\mu^n(\mathbb{A}(F_p : p \in S))$ is infinite.

Proof of Lemma 1.3.1. We can write $\mathbb{A}(F_p : p \in S, m)$ as a disjoint union

$$\mathbb{A}(F_p : p \in S, m) = \coprod_{z_1,\ldots,z_r \in \mathbb{Z}_{\geq 0}} \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} |F_\infty(\mathbf{x}_\infty)| \leq m p_1^{z_1} \ldots p_r^{z_r}, \\ |F_p(\mathbf{x}_{p_i})|_{p_i} = p_i^{-z_i} (i = 1, \ldots, r) \end{array} \right\}.$$

Therefore

$$\begin{aligned}
\mu^n\big(\mathbb{A}(F_p : p \in S, m)\big) &= \sum_{z_1\geq 0,\ldots,z_r\geq 0} \mu_\infty^n\{|F_\infty(\mathbf{x}_\infty)| \leq m p_1^{z_1} \ldots p_r^{z_r}\} \prod_{i=1}^r \mu_{p_i}^n\{|F_p(\mathbf{x}_{p_i})|_{p_i} = p_i^{-z_i}\} \\
&= \sum_{z_1\geq 0,\ldots,z_r\geq 0} m^{n/d}\mu_\infty^n\{|F_\infty(\mathbf{x}_\infty)| \leq p_1^{z_1} \ldots p_r^{z_r}\} \prod_{i=1}^r \mu_{p_i}^n\{|F_p(\mathbf{x}_{p_i})|_{p_i} = p_i^{-z_i}\} \\
&= m^{n/d} \cdot \mu^n\big(\mathbb{A}(F_p : p \in S)\big).
\end{aligned}$$

□

The next lemma tells us how $\mu^n(\mathbb{A}(F_p : p \in S))$ changes under the action of $T_p \in GL_n(\mathbb{Q}_p), p \in S$.

Lemma 1.3.3. *Let $T_p \in GL_n(\mathbb{Q}_p)$ for each $p \in S$. Then*

$$\mu^n\Big(\mathbb{A}((F_p)_{T_p} : p \in S)\Big) = \Big(\prod_{p\in S} |\det(T_p)|_p^{-1}\Big) \cdot \mu^n(\mathbb{A}(F_p : p \in S).$$

Proof. Let $\mathbf{k} = (k_p : p \in S) \in \mathbb{Z}^{r+1}$ with $k_\infty = 0$ and $|S_0| = r$. Put $\mathbf{k}' = (k_p : p \in S_0)$. Define

$$\mathbb{A}(\mathbf{k}') = \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F_p(\mathbf{x}_p)|_p \leq 1\ ,\ |T_p^{-1}(\mathbf{x}_p)|_p = p^{k_p} \text{ for } p \in S_0\Big\}.$$

Then we can write

$$\mathbb{A}(F_p : p \in S) = \coprod_{\mathbf{k}'\in\mathbb{Z}^r} \mathbb{A}(\mathbf{k}').$$

Let $a = \prod_{p\in S_0} p^{k_p}$. For each $p \in S$, define a map $\phi_{k_p} : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ by $\phi_{k_p}(\mathbf{x}_p) = aT_p^{-1}(\mathbf{x}_p)$. This gives a product map $\phi_{\mathbf{k}} = \prod_{p\in S} \phi_{k_p} : \mathbb{A}_S^n \to \mathbb{A}_S^n$. For each $p \in S$, put $\mathbf{y}_p = aT_p^{-1}(\mathbf{x}_p)$. Then we have

$$\phi_{\mathbf{k}}(\mathbb{A}(\mathbf{k}')) = \Big\{(\mathbf{y}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F_p(T_p(\mathbf{y}_p))|_p \leq 1\ ,\ |\mathbf{y}_p|_p = |a|_p \cdot p^{k_p} = 1 \text{ for } p \in S_0\Big\}$$

So we have

$$\coprod_{\mathbf{k}'\in\mathbb{Z}^r} \phi_{\mathbf{k}}(\mathbb{A}(\mathbf{k}')) = \mathbb{A}((F_p)_{T_p} : p \in S).$$

Therefore

$$\begin{aligned}\mu^n\Big(A((F_p)_{T_p} : p \in S)\Big) &= \sum_{\mathbf{k}'\in\mathbb{Z}^r} \mu^n\Big(\phi_{\mathbf{k}}(\mathbb{A}(\mathbf{k}')\Big) = \sum_{\mathbf{k}'\in\mathbb{Z}^r}\prod_{p\in S} |\det \phi_{k_p}|_p \mu_p^n(\mathbb{A}(\mathbf{k}'))\\ &= \sum_{\mathbf{k}'\in\mathbb{Z}^r}\prod_{p\in S} |a^n \det T_p^{-1}|_p \mu_p^n(\mathbb{A}(\mathbf{k}')) = \sum_{\mathbf{k}'\in\mathbb{Z}^r}\prod_{p\in S} |\det T_p|_p^{-1} \mu_p^n(\mathbb{A}(\mathbf{k}'))\\ &= (\prod_{p\in S} |\det T_p|_p)^{-1} \cdot \mu^n(\mathbb{A}(F_p : p \in S)).\end{aligned}$$

□

Corollary 1.3.4. *Let $\lambda_p \in \mathbb{Q}_p^*$ for $p \in S$. Then*

$$\mu^n(A(\lambda_p F_p : p \in S)) = (\prod_{p \in S} |\lambda_p|_p)^{-n/d} \cdot \mu^n(A(F_p : p \in S)).$$

Proof. Let $T_\infty = ((\prod_{p\in S} |\lambda_p|_p)^{1/d}) \cdot \mathrm{Id} \in \mathrm{GL_n}(\mathbb{R})$ and $T_p = \mathrm{Id} \in GL_n(\mathbb{Q}_p)$ for $p \in S_0$. By Lemma 1.3.3, we have

$$\begin{aligned}\mu^n(A(\lambda_p F_p : p \in S)) &= (\prod_{p \in S} |\det T_p|_p)^{-1} \cdot \mu^n(A((F_p : p \in S)) \\ &= (\prod_{p \in S} |\lambda_p|_p)^{-n/d} \cdot \mu^n(A(F_p : p \in S)).\end{aligned}$$

□

1.4 Analysis of the small solutions

In this section, we use the sup-norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ defined by

$$\|\mathbf{x}\| := \max\{|x_1|, \ldots, |x_n|\}.$$

Given $B_0 > 0$, we define

$$\mathbb{A}_{F,S}(m, B_0) := \{(\mathbf{x}_p)_p \in \mathbb{A}_{F,S}(m) : \|\mathbf{x}_\infty\| \le B_0\}.$$

We estimate the difference between the volume $\mu^n(\mathbb{A}_{F,S}(m, B_0))$ and the number of integer points in $\mathbb{A}_{F,S}(m, B_0)$, i.e., $|\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n|$. First, we need the following generalization of [19, Lemma 14].

Lemma 1.4.1. *Let $F_1, \ldots, F_r \in \mathbb{R}[X_1, \ldots, X_n]$. Suppose that F_i has total degree d_i for $i = 1, \ldots, r$. Let $B_0, m_1, \ldots, m_r$ be positive reals and*

$$\mathcal{A} := \{\mathbf{x} \in \mathbb{R}^n : |F_i(\mathbf{x})| \le m_i \ , i = 1, \ldots, r\}.$$

Assume that $\mathcal{A} \subseteq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \le B_0\}$. Then we have

$$\left|\mu_\infty^n(\mathcal{A}) - |\mathcal{A} \cap \mathbb{Z}^n| \ \right| \le n 2^r d_1 \cdots d_r \cdot (2B_0 + 1)^{n-1}.$$

Proof. The proof is by induction on n.

Let $n = 1$. If $F \in \mathbb{R}[X]$ and $\deg F = d$, we know that the set

$$\{x \in \mathbb{R} : |F(x)| \leq m\} = \{x \in \mathbb{R} : F^2(x) \leq m^2\}$$

is a disjoint union of at most $2d$ closed intervals. So

$$\mathcal{A} = \{x \in \mathbb{R} : |F_i(x)| \leq m_i \ , i = 1, \ldots, r\}$$

is a disjoint union of at most $2^r d_1 \cdots d_r$ closed intervals. For each interval I we know that $|\mu_\infty(I) - |I \cap \mathbb{Z}| \ | \leq 1$. Hence

$$\Big| \ \mu_\infty(\mathcal{A}) - |\mathcal{A} \cap \mathbb{Z}^n| \ \Big| \leq 2^r d_1 \cdots d_r.$$

Let $n \geq 2$. Let v^n be the counting measure of $\mathbb{Z}^n$, that is $v^n(\mathcal{B}) = |\mathcal{B} \cap \mathbb{Z}^n|$ for a subset $\mathcal{B}$ of $\mathbb{Z}^n$. For $\mathbf{x} = (x_1, \ldots, x_n)$, let $\mathbf{x}' = (x_1, \ldots, x_{n-1})$ and define

$$\begin{aligned}
&\mathcal{A}(\mathbf{x}') := \{x_n \in \mathbb{R} : (\mathbf{x}', x_n) \in \mathcal{A}\}, \\
&\mathcal{A}' := \{\mathbf{x}' \in \mathbb{R}^{n-1} : \mathcal{A}(\mathbf{x}') \neq \emptyset\}, \\
&\mathcal{A}(x_n) := \{\mathbf{x}' \in \mathbb{R}^{n-1} : (\mathbf{x}', x_n) \in \mathcal{A}\}, \\
&\mathcal{A}'' := \{x_n \in \mathbb{R} : \mathcal{A}(x_n) \neq \emptyset\}.
\end{aligned}$$

By our assumption $\mathcal{A} \subseteq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq B_0\}$, we have

$$\mathcal{A}(\mathbf{x}') \subseteq [-B_0, B_0] \ , \ \mathcal{A}' \subseteq [-B_0, B_0]^{n-1} \ , \ \mathcal{A}(x_n) \subseteq [-B_0, B_0]$$

and $\mathcal{A}'' \subseteq [-B_0, B_0]$. Hence we can apply the induction hypothesis to

$$\begin{aligned}
&\mathcal{A}(\mathbf{x}') := \{x_n \in \mathbb{R} : |F_{i,\mathbf{x}'}(x_n)| \leq m_i, i = 1, \ldots, r\} \\
&\quad \text{with } \deg F_{i,\mathbf{x}'}(X_n) \leq \deg F_i = d_i \text{ for } i = 1, \ldots, r
\end{aligned}$$

and

$$\begin{aligned}
&\mathcal{A}(x_n) := \left\{\mathbf{x}' \in \mathbb{R}^{n-1} : |F_{i,x_n}(\mathbf{x}')| \leq m_i, i = 1, \ldots, r\right\} \\
&\quad \text{with } \deg F_{i,x_n}(X_1, \ldots, X_{n-1}) \leq \deg F_i = d_i \text{ for } i = 1, \ldots, r.
\end{aligned}$$

By the Fubini-Tonelli Theorem (see [2, 41.1]), we have

$$
\begin{aligned}
&|\mu_\infty^n(\mathcal{A}) - |\mathcal{A}\cap\mathbb{Z}^n|\,| = |\mu_\infty^n(\mathcal{A}) - v^n(\mathcal{A})| \\
&= \Big| \int_{\mathcal{A}''} \Big\{ \int_{\mathbf{x}'\in\mathcal{A}(x_n)} d\mu_\infty^{n-1}(\mathbf{x}') \Big\} d\mu_\infty^1(x_n) - \int_{\mathcal{A}'} \Big\{ \int_{x_n\in\mathcal{A}(\mathbf{x}')} dv^1(x_n) \Big\} dv^{n-1}(\mathbf{x}') \Big| \\
&= \Big| \int_{\mathcal{A}''} \mu_\infty^{n-1}(\mathcal{A}(x_n)) d\mu_\infty^1(x_n) - \int_{\mathcal{A}''} \Big\{ \int_{\mathbf{x}'\in\mathcal{A}(x_n)} dv^{n-1}(\mathbf{x}') \Big\} d\mu_\infty^1(x_n) \\
&\qquad + \int_{\mathcal{A}'} \Big\{ \int_{x_n\in\mathcal{A}(\mathbf{x}')} d\mu_\infty^1(x_n) \Big\} dv^{n-1}(\mathbf{x}') - \int_{\mathcal{A}'} v^1(\mathcal{A}(\mathbf{x}')) dv^{n-1}(\mathbf{x}') \Big|.
\end{aligned}
$$

This leads to

$$
\begin{aligned}
&|\mu_\infty^n(\mathcal{A}) - |\mathcal{A}\cap\mathbb{Z}^n|\,| \\
&\le \Big| \int_{\mathcal{A}''} \mu_\infty^{n-1}(\mathcal{A}(x_n)) d\mu_\infty^1(x_n) - \int_{\mathcal{A}''} v^{n-1}(\mathcal{A}(x_n)) d\mu_\infty^1(x_n) + \\
&\qquad + \int_{\mathcal{A}'} \mu_\infty^1(\mathcal{A}(\mathbf{x}')) dv^{n-1}(\mathbf{x}') - \int_{\mathcal{A}'} v^1(\mathcal{A}(\mathbf{x}')) dv^{n-1}(\mathbf{x}') \Big| \\
&\le \Big| \int_{\mathcal{A}''} \big(\mu_\infty^{n-1}(\mathcal{A}(x_n)) - v^{n-1}(\mathcal{A}(x_n))\big) d\mu_\infty^1(x_n) \Big| + \Big| \int_{\mathcal{A}'} \big(\mu_\infty^1(\mathcal{A}(\mathbf{x}')) - v^1(\mathcal{A}(\mathbf{x}'))\big) dv^{n-1}(\mathbf{x}') \Big| \\
&\le \int_{\mathcal{A}''} \Big|\mu_\infty^{n-1}(\mathcal{A}(x_n)) - v^{n-1}(\mathcal{A}(x_n))\Big| d\mu_\infty^1(x_n) + \int_{\mathcal{A}'} \Big|\mu_\infty^1(\mathcal{A}(\mathbf{x}')) - v^1(\mathcal{A}(\mathbf{x}'))\Big| dv^{n-1}(\mathbf{x}') \\
&\le \int_{\mathcal{A}''} (n-1)2^r d_1\cdots d_r(2B_0+1)^{n-2} d\mu_\infty^1(x_n) + \int_{\mathcal{A}'} (2^r d_1\cdots d_r) dv^{n-1}(\mathbf{x}') \\
&\le (n-1)2^r d_1\cdots d_r(2B_0+1)^{n-2}\cdot 2B_0 + 2^r d_1\cdots d_r\cdot(2B_0+1)^{n-1} \\
&\le n2^r d_1\cdots d_r(2B_0+1)^{n-1}.
\end{aligned}
$$

□

Remark 1.4.2. We obtain a slightly weaker version of Thunder's Lemma 14 in [19] by putting $F_1(\mathbf{X}) = F(\mathbf{X}), F_2(\mathbf{X}) = X_1, F_3(\mathbf{X}) = X_2, \ldots, F_{n+1} = X_n$ and $m_1 = m, m_2 = \cdots = m_r = B_0$.

We also need a lemma of Schlickewei.

Lemma 1.4.3. *Let Λ be any lattice in $\mathbb{R}^n$ and $|\cdot|_\infty$ a Euclidean norm on $\mathbb{R}^n$. Then Λ has a basis $\{a_1, \dots, a_n\}$ with the property that for any $\mathbf{x} = y_1 a_1 + \cdots + y_n a_n$ with $y_1, \dots, y_n \in \mathbb{R}$, we have*

$$|\mathbf{x}|_\infty \geq 2^{-(3/2)n} \max\{|y_1||a_1|_\infty, \dots, |y_n||a_n|_\infty\}.$$

Proof. See [13, Lemma 2.2]. □

Combining the previous two lemmas, we obtain the following:

Lemma 1.4.4. *Let $F \in \mathbb{R}[X_1, \dots, X_n]$ be a polynomial of total degree d. Let m, B_0 and $m_i, i = 1, \dots, n$ be positive reals. Let*

$$\mathcal{A} = \{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m \ , |x_i| \leq m_i \ , i = 1, \dots, n\}.$$

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n and $\|\cdot\|$ be the sup-norm on $\mathbb{R}^n$. Assume

$$\mathcal{A} \subseteq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq B_0\} \ \textit{and} \ \inf\{\|\mathbf{x}\| : 0 \neq \mathbf{x} \in \Lambda\} = \theta > 0.$$

Then

$$\left| \ \frac{\mu_\infty^n(\mathcal{A})}{|\det \Lambda|} - |\mathcal{A} \cap \Lambda| \ \right| \leq nd \cdot (2\frac{\sqrt{n}4^n B_0}{\theta} + 1)^{n-1}.$$

Proof. Choose a basis $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ of Λ as in Lemma 1.4.3 and let A be the matrix with columns $\mathbf{a}_1, \dots, \mathbf{a}_n$. For the set $\mathcal{A}' = A^{-1}\mathcal{A} = \{\mathbf{y} \in \mathbb{R}^n : A\mathbf{y} \in \mathcal{A}\}$, we have

$$\mathcal{A}' = \{\mathbf{y} \in \mathbb{R}^n : |F(A\mathbf{y})| \leq m \ , | < \mathbf{a}_i, \mathbf{y} > | \leq m_i' \text{ for } i = 1, \dots, n\}$$

where $<,>$ is the usual inner product of vectors. By Lemma 1.4.3, for each $\mathbf{y} = \sum_{i=1}^n y_i \mathbf{a}_i \in \mathcal{A}'$ we have that

$$|y_i| \leq \frac{4^n |\mathbf{x}|_\infty}{|\mathbf{a}_i|_\infty} \leq \frac{\sqrt{n}4^n \|\mathbf{x}\|}{\|\mathbf{a}_i\|} \leq \frac{\sqrt{n}4^n B_0}{\theta}.$$

Hence $\mathcal{A}' \subseteq \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{y}\| \leq \sqrt{n}4^n B_0/\theta\}$. We know that

$$\mu_\infty^n(\mathcal{A}') = \mu_\infty^n(\mathcal{A})/|\det \Lambda| \quad , \quad \mathcal{A}' \cap \mathbb{Z}^n = \mathcal{A} \cap \Lambda.$$

Now an application of Lemma 1.4.1 to $\mathcal{A}'$ gives

$$\left|\frac{\mu_\infty^n(\mathcal{A})}{|\det\Lambda|} - |\mathcal{A}\cap\Lambda|\ \right| = |\mu_\infty^n(\mathcal{A}') - |\mathcal{A}'\cap\mathbb{Z}^n|\ | \le nd\cdot(2\frac{\sqrt{n}4^nB_0}{\theta}+1)^{n-1}.$$

□

We use Lemma 1.4.4 to analyze the set $\mathbb{A}_{F,S}(m,B_0)$. Without loss of generality, we assume that F is primitive.

For $p\in S_0$, let $\mathbb{E}_p$ be the splitting field of F over $\mathbb{Q}_p$. Choose a factorization $F = L_{p1}\cdots L_{pd}$ with $L_{pi}=a_{pi,1}x_1+\cdots+a_{pi,n}x_n\in\mathbb{E}_p[X_1,\ldots,X_n]$. We can fix the factorization such that

$$|\mathbf{L}_{pi}|_p = \max\{|a_{pi,1}|_p,\ldots,|a_{pi,n}|_p\} = 1\ (i=1,..,d).$$

Let e_p be the ramification index of $\mathbb{E}_p/\mathbb{Q}_p$. Then $e_p\Big|[\mathbb{E}_p:\mathbb{Q}_p]$ and hence $e_p\le d!$. For every $\mathbf{x}_p\in\mathbb{Z}_p^n$ with $|\mathbf{x}_p|_p=1$, there are $z_{p1},\ldots,z_{pd}\in\mathbb{Z}_{\ge 0}$ such that

$$|L_{pi}(\mathbf{x}_p)|_p = p^{-z_{pi}/e_p},\ i=1,\ldots,d.$$

For a tuple $\underline{z} := (z_{pi}: p\in S_0, i=1,\ldots,d)\in\mathbb{Z}_{\ge 0}^{dr}$, we define

$$\mathbb{A}_{F,S}(m,B_0,\underline{z}) = \left\{(\mathbf{x}_p)_p\in\mathbb{A}_{F,S}(m,B_0) : |L_{pi}(\mathbf{x}_p)|_p = p^{-z_{pi}/e_p}\ (p\in S_0, i=1,\ldots,d)\right\}.$$

Then $\mathbb{A}_{F,S}(m,B_0)=\coprod_{\underline{z}\in\mathbb{Z}_{\ge 0}^{dr}}\mathbb{A}_{F,S}(m,B_0,\underline{z})$.

Define $m(\underline{z}) = m\cdot\prod_{p\in S_0}p^{(\sum_{i=1}^d z_{pi})/e_p}$. Then

$$(\mathbf{x}_p)_p\in\mathbb{A}_{F,S}(m,B_0,\underline{z})\quad\text{implies}\quad|F(\mathbf{x}_\infty)|\le m(\underline{z}).$$

For each $\mathbf{x}\in\mathbb{A}_{F,S}(m,B_0,\underline{z})\cap\mathbb{Z}^n$ and $q\in\mathcal{P}\setminus S_0$, we have $|F(\mathbf{x})|_q\le 1$. By the product formula, we have $\prod_{p\in M_\mathbb{Q}}|F(\mathbf{x})|_p = 1$, hence $\prod_{p\in S}|F(\mathbf{x})|_p\ge 1$. Therefore

$$\prod_{p\in S_0}p^{(\sum_{i=1}^d z_{pi})/e_p}\le|F(\mathbf{x})|\le n^{d/2}H_\infty(F)\cdot B_0^d = \mathcal{H}(F)\cdot B_0^d.$$

This implies

$$\sum_{p\in S_0}\sum_{i=1}^d\frac{z_{pi}}{e_p}\le\log\left(n^{d/2}\mathcal{H}(F)\cdot B_0^d\right)/\log 2,$$

hence

$$\sum_{p\in S_0}\sum_{i=1}^{d} z_{pi} \le d!\cdot \frac{\log\left(n^{d/2}\mathcal{H}(F)\cdot B_0^d\right)}{\log 2} \tag{1.4.1}$$

Let $\mathcal{Z}$ be the set of tuples $\underline{z} = (z_{pi} : p \in S_0, 1 \le i \le d) \in \mathbb{Z}_{\ge 0}^{dr}$ that satisfy condition (1.4.1). Then $\mathbb{A}_{F,S}(m, B_0, \underline{z}) \cap \mathbb{Z}^n \ne \emptyset$ implies that $\underline{z} \in \mathcal{Z}$. Note that

$$|\mathcal{Z}| \le \left(d! \log\left(n^{d/2}\mathcal{H}(F)\cdot B_0^d\right)/\log 2\right)^{dr} \ll \left(1 + \log\left(\mathcal{H}(F)B_0\right)\right)^{dr} \tag{1.4.2}$$

where the implicit constant depends only on n, d and $|S|$. So we can write $\mathbb{A}_{F,S}(m, B_0)\cap\mathbb{Z}^n$ as a finite disjoint union

$$\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n = \coprod_{\underline{z}\in\mathcal{Z}} (\mathbb{A}_{F,S}(m, B_0, \underline{z}) \cap \mathbb{Z}^n).$$

Lemma 1.4.5. *With the notation above, we have*

$$\left|\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z})) - |\mathbb{A}_{F,S}(m, B_0, \underline{z}) \cap \mathbb{Z}^n|\right| \ll (B_0 + 1)^{n-1}$$

where the implicit constant depends only on n, d and $|S|$.

Proof. Write $\mathbb{A}_{F,S}(m, B_0, \underline{z})$ as follows:

$$\mathbb{A}_{F,S}(m, B_0, \underline{z}) = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} |F(\mathbf{x}_\infty)| \le m(\underline{z}), \|\mathbf{x}_\infty\| \le B_0, \\ |L_{pi}(\mathbf{x}_p)|_p = p^{-z_{pi}/e_p}, 1 \le i \le d, p \in S_0, \\ |\mathbf{x}_p|_p = 1, p \in S_0. \end{array} \right\}$$

Let $L_{p,d+1} = X_1, \ldots, L_{p,d+n} = X_n$ and $z_{p,d+1} = \cdots = z_{p,d+n} = 0$ for $p \in S$. Then

$$\mathbb{A}_{F,S}(m, B_0, \underline{z}) = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} |F(\mathbf{x}_\infty)| \le m(\underline{z}), \|\mathbf{x}_\infty\| \le B_0, \\ |L_{pi}(\mathbf{x}_p)|_p = p^{-z_{pi}/e_p}\ ,\ i = 1, \ldots, d+n, p \in S_0. \end{array} \right\}$$

Put $I_0 = \{(p, i) : p \in S_0, 1 \le i \le d + n\}$. For $I \subset I_0$, define

$$\mathbb{A}_{F,S}(m, B_0, \underline{z}, I) = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} |F(\mathbf{x}_\infty)| \le m(\underline{z}), \|\mathbf{x}_\infty\| \le B_0, \\ |L_{p,i}(\mathbf{x}_p)|_p < p^{-z_{pi}/e_p}((p, i) \in I), \\ |L_{p,i}(\mathbf{x}_p)|_p \le p^{-z_{p,i}/e_p}((p, i) \in I_0 \setminus I). \end{array} \right\}.$$

Then $\mathbb{A}_{F,S}(m, B_0, \underline{z}) = \mathbb{A}_{F,S}(m, B_0, \underline{z}, \emptyset) - \bigcap_{|I|=1} \mathbb{A}_{F,S}(m, B_0, \underline{z}, I)$. Hence by the rule of inclusion-exclusion

$$\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z})) = \mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, \emptyset)) - \textstyle\sum_{|I|=1} \mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)) \\ + \textstyle\sum_{|I|=2} \mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)) - \cdots$$

and

$$|\mathbb{A}_{F,S}(m, B_0, \underline{z})| = |\mathbb{A}_{F,S}(m, B_0, \underline{z}, \emptyset)| - \textstyle\sum_{|I|=1} |\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)| \\ + \textstyle\sum_{|I|=2} |\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)| - \cdots$$

where both sums are over all subsets of I_0. Therefore

$$\Big|\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z})) - |\mathbb{A}_{F,S}(m, B_0, \underline{z}) \cap \mathbb{Z}^n|\,\Big| \\ \leq \sum_{I \subseteq I_0} \Big|\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)) - |\mathbb{A}_{F,S}(m, B_0, \underline{z}, I) \cap \mathbb{Z}^n|\,\Big|.$$

The set I_0 has at most $2^{|I_0|} = 2^{(d+n)r}$ subsets. Hence we are left to show that for each non-empty subset $I \subseteq I_0$

$$|\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)) - |\mathbb{A}_{F,S}(m, B_0, \underline{z}, I) \cap \mathbb{Z}^n|\,| \ll (B_0 + 1)^{n-1}.$$

Note that the set

$$\left\{ \mathbf{x} \in \mathbb{Z}^n : \begin{array}{c} |L_{pi}(\mathbf{x})|_p < p^{-z_{pi}/e_p}, (pi) \in I; \\ |L_{pi}(\mathbf{x})|_p \leq p^{-z_{pi}/e_p}, (pi) \in I_0 \setminus I; \\ |\mathbf{x}|_p \leq 1, p \in \mathcal{P} \setminus S \end{array} \right\}$$

defines a lattice $\Lambda = \Lambda(\underline{z}, I) \subseteq \mathbb{Z}^n$. So we have $\theta = \inf\{\|\mathbf{x}\| : 0 \neq \mathbf{x} \in \Lambda\} \geq 1$. Define $S = S(\underline{z}, B_0) = \{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m(\underline{z}), \|\mathbf{x}\| \leq B_0\}$. Then

$$\mathbb{A}_{F,S}(m, B_0, \underline{z}, I) \cap \mathbb{Z}^n = S \cap \Lambda.$$

Since

$$\mu^n(\mathbb{A}_{F,S}(m, B_0, \underline{z}, I)) = \mu^n_\infty(S)/|\det \Lambda|,$$

we are left to show that for each lattice $\Lambda \in \mathbb{Z}^n$

$$\left| \frac{\mu^n_\infty(S)}{|\det \Lambda|} - |S \cap \Lambda|\, \right| \ll (B_0 + 1)^{n-1}.$$

But this follows from Lemma 1.4.4. □

With the lemma above, we finally arrive at the next Proposition which allows us to estimate the difference between the volume $\mu^n(\mathbb{A}_{F,S}(m, B_0))$ and the cardinality of $\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n$.

Proposition 1.4.6. *With the notation above, we have*

$$| \ \mu^n\big(\mathbb{A}_{F,S}(m, B_0)\big) - |\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n| \ | \ll (B_0+1)^{n-1}\Big(1 + \log\big(\mathcal{H}(F)B_0\big)\Big)^{dr}$$

where the implicit constant depends only on n, d *and* $|S|$.

Proof. Since $\mathbb{A}_{F,S}(m, B_0) = \coprod_{\underline{z} \in \mathbb{Z}^{dr}_{\geq 0}} \mathbb{A}_{F,S}(m, B_0, \underline{z})$, we have

$$\begin{aligned}
&\Big| \ \mu^n\big(\mathbb{A}_{F,S}(m, B_0)\big) - |\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n| \ \Big| \\
\leq &\sum_{\underline{z} \in \mathcal{Z}} \Big| \ \mu^n\big(\mathbb{A}_{F,S}(m, B_0, \underline{z})\big) - |\mathbb{A}_{F,S}(m, B_0, \underline{z}) \cap \mathbb{Z}^n| \ \Big| \\
\ll &\sum_{\underline{z} \in \mathcal{Z}} (B_0+1)^{n-1} \ll (B_0+1)^{n-1}\Big(1 + \log\big(\mathcal{H}(F)B_0\big)\Big)^{dr}
\end{aligned}$$

where in the estimates we have used (1.4.2) and Lemma 1.4.5. □

Chapter 2

Asymptotic estimates for the number of solutions of decomposable form inequalities

2.1 Statements of the Theorems

Same as in Chapter 1, we define

$$S = \{\infty, p_1, \ldots, p_r\},\ S_0 = S \setminus \{\infty\} \text{ where } p_1, \ldots, p_r \text{ are prime integers,}$$

$$F = \prod_{i=1}^{d} L_i \in \mathbb{Z}[X_1, \ldots, X_n] \text{ is a decomposable form of degree } d,$$

$$L_1, \ldots, L_d \in \overline{\mathbb{Q}}[X_1, \ldots, X_n] \text{ are linear forms,}$$

$$I(F) := \text{ the set of all ordered linearly independent } n\text{-tuples among } \mathbf{L}_1, \ldots, \mathbf{L}_d,$$

$$b(\mathbf{L}_i) := \text{ the number of times that } \mathbf{L}_i \text{ appears in some element of } I(F),$$

$$b(F) := \max_{1 \le i \le d} b(\mathbf{L}_i),$$

$$a(F) := \max_{(\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_n}) \in I(F)} \max_{1 \le j \le n-1} \frac{|\{\mathbf{L}_i \in \text{span } \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}|}{j},$$

$$\mathbb{A}_{F,S}(m) := \Big\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m \ , \ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0 \Big\},$$

$$\mathbb{A}_{F,S} := \mathbb{A}_{F,S}(1),$$

$$N_{F,S}(m) := \Big| \big\{ \mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |F(\mathbf{x})|_p \le m \ , \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1 \big\} \Big|.$$

In this chapter, we prove the following theorems. From now on, all the implicit constants depends only on n, d and S, unless explicitly stated otherwise.

Theorem 2.1.1. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$ and $a(F) < \frac{d}{n}$. Then $\mu^n(\mathbb{A}_{F,S}(m)) \ll m^{n/d}$.*

Remark 2.1.2. By Lemma 1.3.1, we know that $\mu^n(\mathbb{A}_{F,S}(m))$ is homogeneous in m. Hence for Theorem 2.1.1, it suffices to prove $\mu^n(\mathbb{A}_{F,S}(m)) \ll m^{n/d}$ for some positive real m of our choice.

Theorem 2.1.3. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then $N_{F,S}(m) \ll m^{n/d}$.*

Theorem 2.1.4. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then*

$$N_{F,S}(m) = m^{\frac{n}{d}} \mu^n(\mathbb{A}_{F,S}) + O_{F,S}(m^{\frac{n}{d+1/2(n-1)^2}}) \quad \text{as} \quad m \to \infty.$$

Remark 2.1.5. By the notation $O_{F,S}$, we mean that the implicit constant in Theorem 2.1.4 depends on F and S. In some cases, we can get rid of the dependence on F. (See Chapter 4 and Chapter 5.)

Remark 2.1.6. The conditions on F in Theorem 2.1.3 are effectively decidable. (See Chapter 3.)

2.2 Auxiliary Lemmas

Lemma 2.2.1. *Let $p \in S$ and let $L_1, L_2, \ldots, L_n$ be n linearly independent linear forms with coefficients in $\overline{\mathbb{Q}}_p$. For $\mathbf{x} \in \mathbb{Q}_p^n \setminus \{0\}$, We have*

$$\max_{1\le i\le n} \frac{|L_i(\mathbf{x})|_p}{|\mathbf{L}_i|_p} \ge n^{-d(p)\cdot n/2} \cdot |\mathbf{x}|_p \cdot \frac{|\det(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n)|_p}{\prod_{i=1}^n |\mathbf{L}_i|_p}$$

where $d(\infty) = 1$ and $d(p) = 0$ for $p \in S_0$.

Proof. For the case $p = \infty$, see [19, Lemma 4].

Now let $p \in S_0$. First, the inequality to be proved remains unaffected if we multiply $\mathbf{x}, \mathbf{L}_1, \ldots, \mathbf{L}_n$ with arbitrary scalars. So without loss of generality, we may assume that $|\mathbf{x}|_p = 1$ and $|\mathbf{L}_i|_p = 1$ for $i = 1, \ldots, d$. Then the inequality to be proved is

$$\max_{1\le i\le n} |L_i(\mathbf{x})|_p \ge |\det(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n)|_p.$$

Let T be the matrix with rows $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n$ and put

$$m = \min_{|\mathbf{y}|_p=1} |T\mathbf{y}|_p \quad , \quad M = \max_{|\mathbf{y}|_p=1} |T\mathbf{y}|_p$$

where the minimum and maximum are taken over $\mathbf{y} \in \mathbb{Q}_p^n$. Choose $\mathbf{x}_1 \in \mathbb{Z}_p^n$ such that $|T(\mathbf{x}_1)|_p = m$. Then $|\mathbf{x}_1|_p = 1$, hence there are $\mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_n \in \mathbb{Z}_p^n$ such that

$$|\det(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)|_p = 1.$$

Therefore,

$$\begin{aligned} |\det T|_p &= |\det T|_p \cdot |\det(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)|_p = |\det(T\mathbf{x}_1, T\mathbf{x}_2, \ldots, T\mathbf{x}_n)|_p \\ &\le \prod_{i=1}^n |T\mathbf{x}_i|_p = m \prod_{i=2}^n |T\mathbf{x}_i|_p \le mM^{n-1}. \end{aligned}$$

By assumption, we have

$$M = \max_{|\mathbf{y}|_p=1} |T\mathbf{y}|_p = \max_{|\mathbf{y}|_p=1} \max_i \{|L_i\mathbf{y}|_p\} \le \max_{|\mathbf{y}|_p=1} \max_i \{|\mathbf{L}_i|_p |\mathbf{y}|_p\} = 1$$

and

$$m = \min_{|\mathbf{y}|_p=1} |T\mathbf{y}|_p \leq |T\mathbf{x}|_p = \max_i \{|L_i(\mathbf{x})|_p\}.$$

Hence

$$|\det(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n)|_p = |\det T|_p \leq mM^{n-1} \leq m \leq \max_{1\leq i\leq n} |L_i(\mathbf{x})|_p.$$

□

We also need the following elementary lemma from linear programming.

Lemma 2.2.2. *Let $n > 0$ be an integer and $A > 0$. Let $a_1 \leq a_2 \leq \cdots \leq a_n$ be a non-decreasing sequence of real numbers and define*

$$\mathcal{T} = \left\{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n_{\geq 0} : \sum_{i=1}^{n} x_i = nA,\ \sum_{i=1}^{j} x_i \leq jA,\ j = 1, \ldots, n\right\}.$$

Then

$$\min_{(x_1,x_2,\ldots,x_n)\in\mathcal{T}} (x_1a_1 + x_2a_2 + \cdots + x_na_n) = \sum_{i=1}^{n} Aa_i.$$

Proof. See [19, Lemma 1]. □

Lemma 2.2.3. *Let $n > 0$ be an integer and $A > 0$. For any real numbers $\lambda_1, \ldots, \lambda_n$ with $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$, we have*

$$\prod_{i=1}^{n} \lambda_i^{x_i} \geq \left(\prod_{i=1}^{n} \lambda_i\right)^A \text{ for all } (x_1, x_2, \ldots, x_n) \in \mathcal{T}.$$

Proof. By Lemma 2.2.2,

$$\log(\prod_{i=1}^{n} \lambda_i^{x_i}) = \sum_{i=1}^{n} x_i \log \lambda_i \geq \sum_{i=1}^{n} A \log \lambda_i = \log(\prod_{i=1}^{n} \lambda_i^{A}).$$

□

Lemma 2.2.4. *Suppose $I(F) \neq \emptyset$ and $a(F) < d/n$, then for every $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$ there are n-tuples $(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn}) \in I(F)$ $(p \in S)$ such that*

$$\prod_{p \in S} \frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn})|_p} \ll \Big(\prod_{p \in S} \frac{|F(\mathbf{x}_p)|_p}{|\mathbf{x}_p|_p^{d-na(F)}} \Big)^{1/a(F)} \cdot \mathcal{H}(F)^{c(F)} \tag{2.2.1}$$

where

$$c(F) = \frac{b(F)(d-(n-1)a(F))/n! - 1}{a(F)}. \tag{2.2.2}$$

Proof. Let $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$. Assume $\prod_{p \in S} |F(\mathbf{x}_p)|_p \neq 0$, otherwise there is nothing to prove.

Let $p \in S$. Define $\lambda_{p1}, \dots, \lambda_{pn}$ as follows. Let

$$\lambda_{p1} := \min_{1 \le i \le d} \{ |L_i(\mathbf{x}_p)|_p / |\mathbf{L}_i|_p \}$$

and choose $L_{p1} \in \{L_1, \dots, L_d\}$ such that $|L_{p1}(\mathbf{x}_p)|_p / |\mathbf{L}_{p1}|_p = \lambda_{p1}$. For $j = 2, \dots, n$, Let

$$\lambda_{pj} := \min \{ |L_l(\mathbf{x}_p)|_p / |\mathbf{L}_l|_p \}$$

where the minimum is taken over all linear forms L_l such that $\mathbf{L}_l$ is not in the $\mathbb{Q}_p$-span of $\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{p,j-1}$. Choose L_{pj} from these L_l such that $\lambda_{pj} = |L_{pj}(\mathbf{x}_p)|_p / |\mathbf{L}_{pj}|_p$.

Let a_{p1} denote the number of vectors $\mathbf{L}_l$ which are linearly dependent on $\mathbf{L}_{p1}$ over $\mathbb{Q}_p$. Let a_{pj} denote the number of vectors $\mathbf{L}_l$ which are in the span of $\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pj}$ but not in the span of $\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{p,j-1}$. Then $\sum_{i=1}^j a_{pi}$ is the number of $\mathbf{L}_l$ which are in the span of $\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pj}$ for $j = 1, \dots, n$. By the definition of $a(F)$, we have $\sum_{i=1}^j a_{pi} \le j a(F)$ for $j = 1, \dots, n-1$. So $\sum_{i=1}^{n-1} a_{pi} \le (n-1)a(F)$ and $\sum_{i=1}^n a_{pi} = d$. Now let

$$\begin{aligned} a'_{p,n-1} &= a_{p,n-1} + \big((n-1)a(F) - (\textstyle\sum_{i=1}^{n-1} a_{pi})\big) \\ a'_{pn} &= a_{pn} - \big((n-1)a(F) - (\textstyle\sum_{i=1}^{n-1} a_{pi})\big) = d - (n-1)a(F) \\ a'_{pj} &= a_{pj} \text{ for } j = 1, \dots, n-2. \end{aligned}$$

Thus, we have $\sum_{i=1}^{n-1} a'_{pi} = (n-1)a(F)$, $\sum_{i=1}^n a'_{pi} = d$, $a'_{p,n-1} \ge a_{p,n-1}$, $a'_{pn} \le a_{pn}$ for

$p \in S$. This leads to

$$\frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p}{\mathcal{H}(F)} = \prod_{p\in S}\prod_{i=1}^{n}\frac{|L_i(\mathbf{x}_p)|_p}{|\mathbf{L}_i|_p} \geq \prod_{p\in S}\prod_{j=1}^{n}\lambda_{pj}^{a_{pj}}$$
$$\geq \prod_{p\in S}\prod_{j=1}^{n}\lambda_{pj}^{a'_{pj}} = \prod_{p\in S}\left(\lambda_{pn}^{d-(n-1)a(F)}\cdot\prod_{i=1}^{n-1}\lambda_{pi}^{a'_{pi}}\right)$$

and by Lemma 2.2.3

$$\geq \prod_{p\in S}\lambda_{pn}^{d-na(F)}\cdot\prod_{p\in S}\prod_{i=1}^{n}\lambda_{pi}^{a(F)} = \prod_{p\in S}\lambda_{pn}^{d-na(F)}\left(\prod_{j=1}^{n}\frac{|L_{pj}(\mathbf{x}_p)|_p}{|\mathbf{L}_{pj}|_p}\right)^{a(F)}.$$

By Lemma 2.2.1, this is

$$\gg \prod_{p\in S}|\mathbf{x}_p|_p^{d-na(F)}\cdot\prod_{p\in S}\left(\frac{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn})|_p}{\prod_{j=1}^{n}|\mathbf{L}_{pj}|_p}\right)^{d-na(F)}\cdot\prod_{p\in S}\left(\prod_{j=1}^{n}\frac{|L_{pj}(\mathbf{x}_p)|_p}{|\mathbf{L}_{pj}|_p}\right)^{a(F)}$$
$$\gg \prod_{p\in S}|\mathbf{x}_p|_p^{d-na(F)}\cdot\prod_{p\in S}\left(\frac{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn})|_p}{\prod_{j=1}^{n}|\mathbf{L}_{pj}|_p}\right)^{d-(n-1)a(F)}\cdot\prod_{p\in S}\left(\frac{\prod_{j=1}^{n}|L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn})|_p}\right)^{a(F)}.$$

By Lemma 1.1.8, this is

$$\gg \prod_{p\in S}|\mathbf{x}_p|_p^{d-na(F)}\cdot\prod_{p\in S}\left(\frac{\prod_{j=1}^{n}|L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn})|_p}\right)^{a(F)}\cdot\mathcal{H}(F)^{-b(F)(d-(n-1)a(F))/n!}.$$

This implies (2.2.1). □

Definition 2.2.5. *We say that two decomposable forms $F, G \in \mathbb{Z}[X_1,\dots,X_n]$ are S-equivalent if there exist $T \in GL(n,\mathbb{Z}_S)$ and $t \in \mathbb{Z}_S^*$ such that $G = t\cdot F_T$.*

Lemma 2.2.6. *Let $F \in \mathbb{Z}[X_1,\dots,X_n]$ be a decomposable form such that $I(F) \neq \emptyset$ and $\mathcal{H}(F) \leq \mathcal{H}(G)$ for any decomposable form $G \in \mathbb{Z}[X_1,\dots,X_n]$ that is S-equivalent to F. Suppose $F(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}$. Then for every $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$, there are n-tuples $(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn}) \in I(F)$ $(p \in S)$ such that*

$$\prod_{p\in S}\frac{\prod_{j=1}^{n}|L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\dots,\mathbf{L}_{pn})|_p} \ll \frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p^{n/d}}{\mathcal{H}(F)^{1/d}}.$$

Proof. We only need to show the lemma for those $(\mathbf{x}_p)_p$ such that $\prod_{p\in S} |F(\mathbf{x}_p)|_p \neq 0$, since otherwise there is nothing to prove.

For $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$, consider the convex body

$$\mathcal{C} := \left\{ (\mathbf{y}_p)_p \in \mathbb{A}_S^n \ : \ \frac{|L_i(\mathbf{y}_p)|_p}{|L_i(\mathbf{x}_p)|_p} \leq 1 \ (p \in S, \quad i = 1, \ldots, d) \right\}.$$

Let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ be the successive minima of $\mathcal{C}$. By Lemma 1.2.10, we have an upper bound for their product:

$$\lambda_1 \cdot \lambda_2 \cdots \lambda_n \ll \prod_{p\in S} \max_{(i_1,i_2,\ldots,i_n)\in I(F)} \frac{|\det(\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \ldots, \mathbf{L}_{i_n})|_p}{\prod_{j=1}^n |L_{i_j}(\mathbf{x}_p)|_p}.$$

For each $p \in S$, we choose a tuple $(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn}) \in I(F)$ such that $|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p$ is maximal. Then

$$\prod_{p\in S} \frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p} \ll \frac{1}{\lambda_1\lambda_2\cdots\lambda_n}.$$

Now we need to give a lower bound for $\lambda_1 \cdot \lambda_2 \cdots \lambda_n$. By a Theorem of K. Mahler in [11], we have a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ of $\mathbb{Z}_S^n$ such that

$$\mathbf{a}_i \in \max\{1, i/2\} \cdot \lambda_i\mathcal{C} \text{ for } i = 1, \ldots, n.$$

Since $\mathbf{a}_1 \in \lambda_1\mathcal{C}$, we have

$$|L_i(\mathbf{a}_1)|_p \leq \lambda_1^{d(p)} |L_i(\mathbf{x}_p)|_p \ \text{ for } i = 1, \ldots, d, \ p \in S$$

where $d(\infty) = 1$ and $d(p) = 0$ for $p \in S_0$. Since $\mathbf{a}_1 \in \mathbb{Z}_S^n$, we have

$$1 \leq \prod_{p\in S} |F(\mathbf{a}_1)|_p \leq \lambda_1^d \prod_{p\in S} |F(\mathbf{x}_p)|_p.$$

Hence

$$\lambda_1 \geq \left(\prod_{p\in S} |F(\mathbf{x}_p)|_p \right)^{-1/d}. \tag{2.2.3}$$

We need a larger lower bound for λ_n. Let $G = t \cdot F_T$ with $t \in \mathbb{Z}_S^*$ and $T \in GL(n, \mathbb{Z}_S)$. Let $\mathbf{a}_1, \dots, \mathbf{a}_n$ be the columns of T. By the minimality of $\mathcal{H}(F)$, we have

$$\begin{aligned}
\mathcal{H}(F) &\le \mathcal{H}(G) = \mathcal{H}(tF_T) \\
&= \prod_{p \in S} |t|_p \prod_{i=1}^{d} |L_i(X_1 \cdot \mathbf{a}_1 + \cdots + X_n \cdot \mathbf{a}_n)|_p \\
&\ll \prod_{p \in S} \prod_{i=1}^{d} \max_{1 \le j \le n} |L_i(\mathbf{a}_j)|_p \\
&= \prod_{i=1}^{d} \max_{1 \le j \le n} |L_i(\mathbf{a}_j)|_\infty \cdot \prod_{p \in S_0} \prod_{i=1}^{d} \max_{1 \le j \le n} |L_i(\mathbf{a}_j)|_p \\
&\ll \prod_{i=1}^{d} (\lambda_j |L_i(\mathbf{x}_\infty)|_\infty) \cdot \prod_{p \in S_0} \prod_{i=1}^{d} |L_i(\mathbf{x}_p)|_p \\
&\le \lambda_n^d \prod_{p \in S} |F(\mathbf{x}_p)|_p.
\end{aligned}$$

Hence

$$\lambda_n \gg \left(\frac{\mathcal{H}(F)}{\prod_{p \in S} |F(\mathbf{x}_p)|_p} \right)^{1/d}.$$

Together with the lower bound for λ_1 in (2.2.3), this gives

$$\prod_{p \in S} \frac{\prod_{j=1}^{n} |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn})|_p} \ll \frac{1}{\prod_{i=1}^{n} \lambda_i} \le \frac{1}{\lambda_1^{n-1} \lambda_n} \ll \frac{\prod_{p \in S} |F(\mathbf{x}_p)|_p^{n/d}}{\mathcal{H}(F)^{1/d}}.$$

$\square$

We have proved two lemmas for points $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$ giving inequalities of the shape

$$\prod_{p \in S} \frac{\prod_{j=1}^{n} |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn})|_p} \ll A.$$

As it will turn out to be inconvenient to work with linear forms L_i whose coefficients lie outside $\mathbb{Q}_p$, we must reduce these inequalities to similar ones with linear forms with coefficients in $\mathbb{Q}_p$.

We first need a simple lemma from algebraic number theory (see e.g. [12]). Let $\mathbb{K}_p$ be a finite extension of $\mathbb{Q}_p$ of degree d. Let $O_p = \{x \in \mathbb{K}_p : \ |x|_p \leq 1\}$. It is well-known that O_p is a free $\mathbb{Z}_p$-module of rank d. Let $\{w_1, w_2, \ldots, w_d\}$ be a $\mathbb{Z}_p$-basis of O_p. Let $\sigma_l : \mathbb{K}_p \to \overline{\mathbb{Q}}_p, l = 1, \ldots, d$ be the $\mathbb{Q}_p$ embeddings of $\mathbb{K}_p$ into $\overline{\mathbb{Q}}_p$. Let $\Omega = (\sigma_l(w_j))_{l,j=1,\ldots,d}$.

Lemma 2.2.7.

$$|\det \Omega|_p^2 \geq (pd)^{-d}.$$

Proof. Let $D_{\mathbb{K}_p/\mathbb{Q}_p}$ be the discriminant of $\mathbb{K}_p$ over $\mathbb{Q}_p$. Then $D_{\mathbb{K}_p/\mathbb{Q}_p} = (\det \Omega)^2$.

The different $\mathfrak{D}_{\mathbb{K}_p/\mathbb{Q}_p}$ of $\mathbb{K}_p$ over $\mathbb{Q}_p$ is given by

$$\mathfrak{D}^{-1}_{\mathbb{K}_p/\mathbb{Q}_p} := \{x \in \mathbb{K}_p : Tr_{\mathbb{K}_p/\mathbb{Q}_p}(xy) \in \mathbb{Z}_p \text{ for all } y \in O_p\}.$$

The different $\mathfrak{D}_{\mathbb{K}_p/\mathbb{Q}_p}$ is an ideal of O_p and $D_{\mathbb{K}_p/\mathbb{Q}_p} = N_{\mathbb{K}_p/\mathbb{Q}_p}(\mathfrak{D}_{\mathbb{K}_p/\mathbb{Q}_p})$.

Let $\mathfrak{p} = \{x \in \mathbb{K}_p : |x|_p < 1\}$. Then $\mathfrak{p}$ is the maximal ideal of O_p. Let $f = [O_p/\mathfrak{p} : \mathbb{Z}_p/(p)]$. We have $N_{\mathbb{K}_p/\mathbb{Q}_p}(\mathfrak{p}) = p^f$. Let e be the ramification index of $\mathbb{K}_p$ over $\mathbb{Q}_p$. Assume $\mathfrak{D}_{\mathbb{K}_p/\mathbb{Q}_p} = \mathfrak{p}^r$ for some r and $e = p^a e'$ with $p \nmid e', a \geq 0$. Then by [12, Chapter 3, Thm 2.6] we have

$$D_{\mathbb{K}_p/\mathbb{Q}_p} = N_{\mathbb{K}_p/\mathbb{Q}_p}(\mathfrak{D}_{\mathbb{K}_p/\mathbb{Q}_p}) = N_{\mathbb{K}_p/\mathbb{Q}_p}(\mathfrak{p})^r = p^{fr} \text{ and}$$

$$e - 1 \leq \ r \ \leq e - 1 + a \cdot e \leq e(1 + a).$$

Therefore

$$|\det \Omega|_p^2 = |D_{\mathbb{K}_p/\mathbb{Q}_p}|_p = p^{-fr} \geq p^{-fe(1+a)} = p^{-d}(p^a)^{-d} = p^{-d}e^{-d} \geq (pd)^{-d}.$$

□

Lemma 2.2.8. *Let $\mathbb{K}_p$ be a finite extension of $\mathbb{Q}_p$ of degree d. Let $L_1, L_2, \ldots, L_n \in \mathbb{K}_p[X_1, \ldots, X_n]$ be linearly independent linear forms. Then there exist linearly independent linear forms $M_1, M_2, \ldots, M_n \in \mathbb{Q}_p[X_1, \ldots, X_n]$ such that for every $\mathbf{x} \in \mathbb{Q}_p^n$ we have*

$$\frac{\prod_{j=1}^n |M_j(\mathbf{x})|_p}{|\det(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)|_p} \leq (pd)^{nd/2} \cdot \frac{\prod_{i=1}^n |L_i(\mathbf{x})|_p}{|\det(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n)|_p}.$$

Proof. Recall that O_p is a free $\mathbb{Z}_p$-module of rank d and $\{w_1, w_2, \ldots, w_d\}$ is a $\mathbb{Z}_p$-basis of O_p. So for every $x \in O_p$, there exist unique $a_1, a_2, \ldots, a_d \in \mathbb{Z}_p$ such that $x = \sum_{j=1}^{d} a_j w_j$. Then $L_k = \sum_{j=1}^{d} w_j W_{kj}$ with $W_{kj} = \sum_{i=1}^{n} a_{kij} X_i \in \mathbb{Q}_p[X_1, \ldots, X_n]$.

Recall that $\sigma_l : \mathbb{K}_p \to \overline{\mathbb{Q}}_p, l = 1, \ldots, n$ are the $\mathbb{Q}_p$ embeddings. We extend them in a natural way to embeddings $\mathbb{K}_p[X_1, \ldots, X_n] \to \overline{\mathbb{Q}}_p[X_1, \ldots, X_n]$. Then

$$\sigma_l(L_i) = \sigma_l(\sum_{j=1}^{d} w_j W_{ij}) = \sum_{j=1}^{d} \sigma_l(w_j) W_{ij} \text{ for } i, l = 1, \ldots, d.$$

Write

$$\Omega = (\sigma_l(w_j))_{l,j=1,\ldots,d} \text{ and } \Omega^{-1} = (m_{lj})_{l,j=1,\ldots,d}.$$

Let $C := \max_{i,j} |m_{i,j}|_p$. Since $w_j \in O_p$, we have $|\sigma_l(w_j)|_p = |w_j|_p \leq 1$ for all l, j. Hence

$$C = \frac{\max_{l,j}\{|\Omega_{lj}|_p\}}{|\det \Omega|_p} \leq \frac{1}{|\det \Omega|_p}$$

where Ω_{lj} is the minor of Ω associated with m_{lj}. Then for every $\mathbf{x} \in \mathbb{Q}_p^n$, we have

$$\max\{|W_{i1}(\mathbf{x})|_p, |W_{i2}(\mathbf{x})|_p, \ldots, |W_{id}(\mathbf{x})|_p\} \leq C \cdot \max_l |\sigma_l(L_i(\mathbf{x}))|_p = C \cdot |L_i(\mathbf{x})|_p.$$

By Lemma 2.2.7, we have

$$|\det \Omega|_p^2 \geq (pd)^{-d}, \text{ implying } C \leq (pd)^{d/2}.$$

Hence, for $i = 1, \ldots, n$ we have

$$\max_{1 \leq j \leq d} |W_{ij}(\mathbf{x})|_p \leq C \cdot |L_i(\mathbf{x})|_p \leq (pd)^{\frac{d}{2}} |L_i(\mathbf{x})|_p.$$

Moreover,

$$\begin{aligned}
0 < |\det(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n)|_p &= |\det(\sum_{j=1}^{d} w_j \mathbf{W}_{1j}, \sum_{j=1}^{d} w_j \mathbf{W}_{2j}, \ldots, \sum_{j=1}^{d} w_j \mathbf{W}_{nj})|_p \\
&= \Big| \sum_{j_i=1}^{d} \sum_{j_2=1}^{d} \cdots \sum_{j_n=1}^{d} w_{j_1} w_{j_2} \cdots w_{j_n} \cdot \det(\mathbf{W}_{1,j_1}, \mathbf{W}_{2,j_2}, \ldots, \mathbf{W}_{n,j_n}) \Big|_p \\
&\leq \max_{1 \leq j_1, j_2, \ldots, j_n \leq d} |w_{j_1} w_{j_2} \cdots w_{j_n}|_p \cdot |\det(\mathbf{W}_{1,j_1}, \mathbf{W}_{2,j_2}, \ldots, \mathbf{W}_{n,j_n})|_p \\
&\leq \max_{1 \leq j_1, j_2, \ldots, j_n \leq d} |\det(\mathbf{W}_{1,j_1}, \mathbf{W}_{2,j_2}, \ldots, \mathbf{W}_{n,j_n})|_p.
\end{aligned}$$

Choose $(\mathbf{M}_1\ ,\mathbf{M}_2,\ldots,\mathbf{M}_n)$ among

$$\{(\mathbf{W}_{1,j_1},\mathbf{W}_{2,j_2},\ldots,\mathbf{W}_{n,j_n}) : 1 \leq j_1, j_2, \ldots, j_n \leq d\}$$

such that

$$|\det(\mathbf{M}_1\ ,\mathbf{M}_2,\ldots,\mathbf{M}_n)|_p = \max_{1\leq j_1,j_2,\ldots,j_n\leq d} |\det(\mathbf{W}_{1,j_1},\mathbf{W}_{2,j_2},\ldots,\mathbf{W}_{n,j_n})|_p.$$

Then $M_1\ ,M_2,\ldots,M_n \in \mathbb{Q}_p[X_1,\ldots,X_n]$ are linearly independent linear forms and we have

$$\frac{\prod_{i=1}^n |M_i(\mathbf{x})|_p}{|\det(\mathbf{M}_1,\mathbf{M}_2,\ldots,\mathbf{M}_n)|_p} \leq \frac{(pd)^{nd/2}\cdot\prod_{i=1}^n |L_i(\mathbf{x})|_p}{|\det(\mathbf{L}_1,\mathbf{L}_2,\ldots,\mathbf{L}_n)|_p}.$$

□

Lemma 2.2.9. *[Archimedean Orthogonalization]*
Let $\{M_1, M_2, \ldots, M_n\} \subseteq \mathbb{C}^n[X_1,\ldots,X_n]$ be a set of n linearly independent linear forms. Then there is a collection $\mathcal{L}$ of cardinality at most $n!$, consisting of linearly independent sets of linear forms $\{N_1, N_2, \ldots, N_n\} \subseteq \mathbb{C}^n[X_1,\ldots,X_n]$ with

(a) $|\mathbf{N}_1|_\infty = |\mathbf{N}_2|_\infty = \cdots = |\mathbf{N}_n|_\infty = 1$ *and* $|\det(\mathbf{N}_1,\mathbf{N}_2,\ldots,\mathbf{N}_n)| = 1$,

(b) For every $\mathbf{x} \in \mathbb{R}^n$ there exists a set of linear forms $\{N_1, N_2, \ldots, N_n\} \in \mathcal{L}$ with

$$\prod_{i=1}^n |N_i(\mathbf{x})|_\infty \leq \frac{n!\cdot\prod_{i=1}^n |M_i(\mathbf{x})|_\infty}{|\det(\mathbf{M}_1,\mathbf{M}_2,\ldots,\mathbf{M}_n)|_\infty}.$$

Proof. This follows from the proof of [19, Lemma 7]. □

Lemma 2.2.10. *[Non-archimedean Orthogonalization]*
Let p be a prime. Let $\{M_1, M_2, \ldots, M_n\} \subseteq \mathbb{Q}_p^n[X_1,\ldots,X_n]$ be a set of n linearly independent linear forms. Then there is a collection $\mathcal{L}$ of cardinality at most $n!$, consisting of sets of linearly independent linear forms $\{N_1, N_2, \ldots, N_n\} \subseteq \mathbb{Q}_p^n[X_1,\ldots,X_n]$ such that

(a) $|\mathbf{N}_1|_p = |\mathbf{N}_2|_p = \cdots = |\mathbf{N}_n|_p = 1$ *and* $|\det(\mathbf{N}_1,\mathbf{N}_2,\ldots,\mathbf{N}_n)|_p = 1$,

(b) for every $\mathbf{x} \in \mathbb{Q}_p^n$ there exists a set of linear forms $\{N_1, N_2, \dots, N_n\} \in \mathcal{L}$ with

$$\prod_{i=1}^{n} |N_i(\mathbf{x})|_p \le \frac{\prod_{i=1}^{n} |M_i(\mathbf{x})|_p}{|\det(\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_n)|_p}.$$

Proof. The proof is by induction on n. For $n = 1$, the assertion is trivial.

Let $n \ge 2$. Take $\mathbf{x} \in \mathbb{Q}_p^n$. We may assume without loss of generality that $|\mathbf{M}_1|_p = |\mathbf{M}_2|_p = \cdots = |\mathbf{M}_n|_p = 1$ and $|\mathbf{x}|_p = 1$. Further, we may assume that $|M_1(\mathbf{x})|_p = \min_{1\le j\le n} |M_j(x)|_p$. Take $N_1 := M_1$.

Since $|\mathbf{M}_1|_p = 1$, we can augment $\mathbf{M}_1$ to a basis of $\mathbb{Z}_p^n$, $\{\mathbf{M}_1, \mathbf{O}_2, \dots, \mathbf{O}_n\}$, say. Then there is a matrix $C \in GL(n, \mathbb{Z}_p)$ such that

$$C\mathbf{M}_1 = \mathbf{e}_1 \ , \ C\mathbf{O}_2 = \mathbf{e}_2 \ , \ \dots \ , \ C\mathbf{O}_n = \mathbf{e}_n \tag{2.2.4}$$

where $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ denotes the standard basis of $\mathbb{Q}_p^n$. Hence $|\det C|_p = 1$.

Define

$$\mathbf{M}'_1 = C\mathbf{M}_1 = \mathbf{e}_1 \ , \ \mathbf{M}'_2 = C\mathbf{M}_2 \ , \ \dots \ , \ \mathbf{M}'_n = C\mathbf{M}_n.$$

Let $\mathbf{x}' = (C^T)^{-1}\mathbf{x}$ where C^T is the transpose of C. Then

$$< \mathbf{M}'_i, \mathbf{x}' > = < C\mathbf{M}_i, (C^T)^{-1}\mathbf{x} > = < \mathbf{M}_i, \mathbf{x} > \ \ (i = 1, \dots, n).$$

Hence

$$\frac{\prod_{i=1}^{n} | < \mathbf{M}_i, \mathbf{x} > |_p}{|\det(\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_n)|_p} = \frac{|x'_1|_p \prod_{i=2}^{n} | < \mathbf{M}'_i, \mathbf{x}' > |_p}{|\det(\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_n)|_p |\det C|_p} = \frac{|x'_1|_p \prod_{i=2}^{n} | < \mathbf{M}'_i, \mathbf{x}' > |_p}{|\det(\mathbf{e}_1, \mathbf{M}'_2, \dots, \mathbf{M}'_n)|_p} \tag{2.2.5}$$

Write $\mathbf{x}' = (x_1, \dots, x_n)$ and $\mathbf{M}'_i = (m_{i1}, m_{i2}, \dots, m_{in})$ for $i = 1, \dots, n$. Let $\mathbf{M}''_i := \mathbf{M}'_i - m_{i1}\mathbf{e}_1$ for $i = 2, \dots, n$. Then

$$\begin{aligned} | < \mathbf{M}''_i, \mathbf{x}' > |_p &= | < (\mathbf{M}'_i - m_{i1}\mathbf{e}_1), \mathbf{x}' > |_p \le \max\{| < \mathbf{M}'_i, \mathbf{x}' > |_p, \ | < m_{i1}\mathbf{e}_1, \mathbf{x}' > |_p\} \\ &\le \max\{| < \mathbf{M}_i, \mathbf{x} > |_p, \ | < \mathbf{M}_1, \mathbf{x} > |_p\} \\ &= | < \mathbf{M}_i, \mathbf{x} > |_p, \end{aligned}$$

since $|<\mathbf{M}'_i,\mathbf{x}'>|_p = \ |<\mathbf{M}_i,\mathbf{x}>|_p$ and

$$|<m_{i1}\mathbf{e}_1,\mathbf{x}'>|_p = \ |<\mathbf{M}'_1,\mathbf{x}'>|_p = \ |<\mathbf{M}_1,\mathbf{x}>|_p \le |<\mathbf{M}_i,\mathbf{x}>|_p.$$

So

$$\frac{|x'_1|_p\prod_{i=2}^n|<\mathbf{M}'_i,\mathbf{x}'>|_p}{|\det(\mathbf{e}_1,\mathbf{M}'_2,\ldots,\mathbf{M}'_n)|_p} \ge \frac{|x'_1|_p\prod_{i=2}^n|<\mathbf{M}''_i,\mathbf{x}'>|_p}{|\det(\mathbf{e}_1,\mathbf{M}''_2,\ldots,\mathbf{M}''_n)|_p}. \tag{2.2.6}$$

Let $\tilde{\mathbf{M}}_i = (m_{i2},\ldots,m_{in})$ for $i=2,\ldots,n$ and $\tilde{\mathbf{x}} = (x_2,\ldots,x_n)$. Then

$$|<\mathbf{M}''_i,\mathbf{x}'>|_p = \ |<\tilde{\mathbf{M}}_i,\tilde{\mathbf{x}}>|_p \ \ , \ \ |\det(\mathbf{e}_1,\mathbf{M}''_2,\ldots,\mathbf{M}''_n)|_p = |\det(\tilde{\mathbf{M}}_2,\ldots,\tilde{\mathbf{M}}_n)|_p \ .$$

Since $M_1,M_2,\ldots,M_n$ are linearly independent, we know that $e_1,M''_2,\ldots,M''_n$ are linearly independent and hence $\tilde{M}_2,\ldots,\tilde{M}_n$ are linearly independent. Then by the induction hypothesis, there exists a collection $\tilde{\mathcal{L}}$ of cardinality $\le (n-1)!$, consisting of tuples $(\tilde{N}_2,\tilde{N}_3,\ldots,\tilde{N}_n)$ of linear forms in $\mathbb{Q}_p[X_2,\ldots,X_n]$ with

$$|\tilde{\mathbf{N}}_2|_p = |\tilde{\mathbf{N}}_3|_p = \cdots = |\tilde{\mathbf{N}}_n|_p = 1 \text{ and } |\det(\tilde{\mathbf{N}}_2,\tilde{\mathbf{N}}_3,\ldots,\tilde{\mathbf{N}}_n)|_p = 1,$$

For every $\mathbf{y}\in\mathbb{Q}_p^{n-1}$, there exists $(\tilde{N}_2,\tilde{N}_3,\ldots,\tilde{N}_n)\in\tilde{\mathcal{L}}$ such that

$$\prod_{i=2}^n|\tilde{N}_i(\mathbf{y})|_p \le \frac{\prod_{i=2}^n|\tilde{M}_i(y)|_p}{|\det(\tilde{\mathbf{M}}_2,\tilde{\mathbf{M}}_3,\ldots,\tilde{\mathbf{M}}_n)|_p}.$$

Take the tuples $(\tilde{N}_2,\tilde{N}_3,\ldots,\tilde{N}_n)$ corresponding to $\mathbf{y}=\tilde{\mathbf{x}}$. Then

$$\frac{|x'_1|_p\prod_{i=2}^n|<\mathbf{M}''_i,\mathbf{x}'>|_p}{|\det(\mathbf{e}_1,\mathbf{M}''_2,\ldots,\mathbf{M}''_n)|_p} = \frac{|x'_1|_p\prod_{i=2}^n|<\tilde{\mathbf{M}}_i,\tilde{\mathbf{x}}>|_p}{|\det(\tilde{\mathbf{M}}_2,\tilde{\mathbf{M}}_3,\ldots,\tilde{\mathbf{M}}_n)|_p} \ge |x'_1|_p\prod_{i=2}^n \ |<\tilde{\mathbf{N}}_i,\tilde{\mathbf{x}}>|_p. \tag{2.2.7}$$

Let $\mathbf{N}'_i = (0,\tilde{\mathbf{N}}_i)\in\mathbb{Z}_p^n$ for $i=2,\ldots,n$. Then

$$|\mathbf{N}'_i|_p = |\tilde{\mathbf{N}}_i|_p = 1, \ |<\mathbf{N}'_i,x'>|_p = |<\tilde{\mathbf{N}}_i,\tilde{x}>|_p,$$
$$|\det(\mathbf{e}_1,\mathbf{N}'_2,\ldots,\mathbf{N}'_n)|_p = |\det(\tilde{\mathbf{N}}_2,\tilde{\mathbf{N}}_3,\ldots,\tilde{\mathbf{N}}_n)|_p = 1.$$

Finally, put $N_1 = M_1$ and $N_i = C^{-1}N'_i$ for $2\le i\le n$ where C is the matrix defined by (2.2.4). Then

$$|\mathbf{N}_i|_p = |\mathbf{N}'_i|_p = 1 \ , \ |\det(\mathbf{N}_1,\mathbf{N}_2,\ldots,\mathbf{N}_n)|_p = |\det C^{-1}|_p|\det(\mathbf{e}_1,\mathbf{N}'_2,\ldots,\mathbf{N}'_n)|_p = 1.$$

Hence

$$|x_1'|_p \prod_{i=2}^{n} |\tilde{N}_i(\tilde{\mathbf{x}})|_p \geq |N_1(\mathbf{x})|_p \prod_{i=2}^{n} |N_i'(\mathbf{x}')|_p = |N_1(\mathbf{x})|_p \prod_{i=2}^{n} |N_i'((C^T)^{-1}\mathbf{x})|_p$$
$$= |N_1(\mathbf{x})|_p \prod_{i=2}^{n} |C^{-1} N_i'(\mathbf{x})|_p = \prod_{i=1}^{n} |N_i(\mathbf{x})|_p. \qquad (2.2.8)$$

Now (2.2.5), (2.2.6), (2.2.7) and (2.2.8) give

$$\frac{\prod_{i=1}^{n} |M_i(\mathbf{x})|_p}{|\det(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)|_p} \geq \prod_{i=1}^{n} |N_i(\mathbf{x})|_p.$$

□

Lemmas 2.2.8 and 2.2.10 can be combined as follows:

Lemma 2.2.11. *Let $p \in S_0$ and let $\mathbb{K}_p$ be a finite extension of $\mathbb{Q}_p$ of degree d. Let $L_{p1}, L_{p2}, \ldots, L_{pn}$ be linearly independent linear forms in $K_p[X_1, \ldots, X_n]$. Then there exists a collection $\mathcal{L}$ of cardinality at most $n!$, consisting of sets of linearly independent linear forms $\{N_{p1}, N_{p2}, \ldots, N_{pn}\}$ in $\mathbb{Q}_p^n[X_1, \ldots, X_n]$ with:*

(a) $|\mathbf{N}_{p1}|_p = \cdots = |\mathbf{N}_{pn}|_p = 1$ *and* $|\det(\mathbf{N}_{p1}, \mathbf{N}_{p2}, \ldots, \mathbf{N}_{pn})|_p = 1,$

(b) For every $\mathbf{x} \in \mathbb{Q}_p^n$, there exists $\{N_{p1}, N_{p2}, \ldots, N_{pn}\} \in \mathcal{L}$ such that

$$\prod_{i=1}^{n} |N_{pi}(\mathbf{x})|_p \leq (pd)^{nd/2} \cdot \frac{\prod_{i=1}^{n} |L_{pi}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p}.$$

Lemma 2.2.12. *[Main Lemma]*
For $p \in S$, let $K_{p1}, K_{p2}, \ldots, K_{pn} \in \overline{\mathbb{Q}}_p[X_1, \ldots, X_n]$ be linearly independent linear forms in n variables. Let $A > 0$, $C > B > 0$ and $D > 1$. Consider the set

$$\mathcal{M} = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p \in S} \frac{\prod_{i=1}^{n} |K_{pi}(\mathbf{x}_p)|_p}{|\det(K_{p1}, K_{p2}, \ldots, K_{pn})|_p} \leq A \ , \\ \\ B \leq |\mathbf{x}_\infty|_\infty \leq C \ , \ |\mathbf{x}_p|_p = 1 \ , \ p \in S_0 \end{array} \right\}.$$

If $BC^{n-1} \geq n^{n/2} n! \left(\prod_{p\in S_0} (pd)^{nd/2} \right) \cdot AD^{|S|\cdot(n-1)}$, *then the set* $\mathcal{M}$ *can be covered by at most*

$$|S|(n-1)n^{2|S|} \cdot \left(\log_D \left(\frac{BC^{n-1}}{n^{n/2} n! \prod_{p\in S_0} (pd)^{nd/2} \cdot A} \right) \right)^{|S|(n-1)-1}$$

sets of the form

$$\mathcal{C} = \{ (\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \leq a_{pi} \ (p \in S, i = 1, \ldots, n) \}$$

where $K'_{p1}, K'_{p2}, \ldots, K'_{pn}$ *are linear forms in* $\mathbb{Q}_p[X_1, \ldots, X_n]$ *with*

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1$$

and the a_{pi} *are positive reals with*

$$\prod_{p\in S} \prod_{i=1}^{n} a_{pi} < n^{n/2} n! \prod_{p\in S_0} (pd)^{nd/2} \cdot \frac{CA}{B} D^{|S|\cdot(n-1)+1}.$$

Otherwise, $\mathcal{M}$ *can be covered by at most* $(n!)^{|S|}$ *sets of that form.*

Proof. By Lemma 2.2.9 and Lemma 2.2.11, we can cover $\mathcal{M}$ by at most $(n!)^{|S|}$ sets of the shape

$$\mathcal{M}' = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} \prod_{i=1}^{n} |K'_{pi}(\mathbf{x}_p)|_p \leq n! \prod_{p\in S_0} (pd)^{nd/2} \cdot A \\ \\ B \leq |\mathbf{x}_\infty|_\infty \leq C \ , \ |\mathbf{x}_p|_p = 1 \ , \ p \in S_0 \end{array} \right\}$$

where $K'_{p1}, K'_{p2}, \ldots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$ with

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1.$$

By Lemma 2.2.1, for every $(\mathbf{x}_p)_p \in \mathcal{M}'$ there exist $i_p \in \{1, \ldots, n\}$ for $p \in S$ such that

$$|K'_{\infty,i_\infty}(\mathbf{x}_\infty)|_\infty \geq n^{-n/2} |\mathbf{x}_\infty|_\infty \ , \ |K'_{p,i_p}(\mathbf{x}_p)|_p \geq |\mathbf{x}_p|_p \ , \ p \in S_0 \ .$$

Thus, for $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$ we have

$$\prod_{p\in S}\prod_{i\neq i_p}|K'_{pi}(\mathbf{x}_p)|_p \leq \frac{n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A}{n^{-n/2}|\mathbf{x}_\infty|_\infty\cdot\prod_{p\in S_0}|\mathbf{x}_p|_p} \leq n^{n/2}n!\prod_{p\in S_0}(pd)^{nd/2}\cdot\frac{A}{B}.$$

We fix the linear forms K'_{pi} and subdivide the corresponding set $\mathcal{M}'$. Define reals $\{n_{pi} : p \in S, i \neq i_p\}$ by

$$|K'_{\infty i}(\mathbf{x}_\infty)| = D^{-n_{\infty i}}C \text{ for } i \neq i_\infty\ ,\ |K'_{pi}(\mathbf{x}_p)|_p = D^{-n_{pi}} \text{ for } p \in S_0,\quad i \neq i_p.$$

Note that

$$\sum_{p\in S}\sum_{i\neq i_p} n_{pi} \geq \log_D\left(\frac{BC^{n-1}}{n^{n/2}n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A}\right).$$

Hence

$$\sum_{p\in S}\sum_{i\neq i_p}[n_{pi}] > \sum_{p\in S}\sum_{i\neq i_p}(n_{pi}-1) \geq \log_D\left(\frac{BC^{n-1}}{n^{n/2}n!\prod_{p\in S_0}(pd)^{nd/2}\cdot AD^{|S|\cdot(n-1)}}\right).$$

Denote this last quantity by Q. We see that $Q \geq 0$ if and only if

$$BC^{n-1} \geq n^{n/2}n!\prod_{p\in S_0}(pd)^{nd/2}\cdot AD^{|S|\cdot(n-1)}.$$

Suppose $Q \geq 0$. We choose non-negative integers $z_{pi} \leq [n_{pi}]$ for each $i \neq i_p$ such that

$$\sum_{p\in S}\sum_{i\neq i_p} z_{pi} = [Q].$$

Since $z_{pi} \leq n_{pi}$, we have

$$|K'_{\infty i}(\mathbf{x}_\infty)| \leq D^{-z_{\infty i}}C \text{ for } i \neq i_\infty\ ,\ |K'_{pi}(\mathbf{x}_p)|_p \leq D^{-z_{pi}} \text{ for } p \in S_0,\quad i \neq i_p.$$

In order to unify notation, we put $z_{pi_p} = 0$ for $p \in S$. Further, if $Q < 0$, we put $z_{pi} := 0$ for $p \in S,\ i = 1, \dots, n$. This leads to a subdivision of $\mathcal{M}'$ into sets of the shape

$$\mathcal{C} := \{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : |K'_{\infty i}(\mathbf{x}_\infty)| \leq D^{-z_{\infty i}}C,\ |K'_{pi}(\mathbf{x}_p)|_p \leq D^{-z_{pi}}\ (p \in S_0, 1 \leq i \leq n)\} \tag{2.2.9}$$

where $K'_{p1}, K'_{p2}, \ldots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$ with

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1\ ,\ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1$$

and the z_{pi} are integers with

$$\sum_{p \in S} \sum_{i=1}^{n} z_{pi} = \max\{[Q], 0\}.$$

Let $a_{\infty i} = D^{-z_{\infty i}} C$ and $a_{pi} = D^{-z_{pi}}$. Then we have

$$\prod_{p \in S} \prod_{i=1}^{n} a_{pi} \leq C^n D^{-[Q]} < C^n D^{1-Q} \leq \frac{CA}{B} \cdot n^{n/2} n! \prod_{p \in S_0} (pd)^{nd/2} \cdot D^{|S| \cdot (n-1)+1}.$$

The number of tuples $\underline{z} = (z_{pi})_{p \in S, i=1,\ldots,n}$ of nonnegative integers with $z_{pi_p} = 0$ for $p \in S$ satisfying

$$\sum_{p \in S} \sum_{i \neq i_p} z_{pi} = [Q]$$

is at most $([Q] + |S|(n-1) - 1)^{|S|(n-1)-1} / (|S|(n-1)-1)!$. Counting the n different possibilities for each i_p, we see that the total number of possible $\underline{z}$ is at most

$$\frac{n^{|S|} \cdot ([Q] + |S|(n-1) - 1)^{|S|(n-1)-1}}{(|S|(n-1)-1)!} < \frac{n^{|S|} \cdot (Q + |S|(n-1))^{|S|(n-1)-1}}{(|S|(n-1)-1)!}.$$

So if $Q \geq 0$, this number is equal to

$$\frac{n^{|S|}}{(|S|(n-1)-1)!} \cdot \left(\log_D \left(\frac{BC^{n-1}}{n^{n/2} n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A} \right) \right)^{|S|(n-1)-1}.$$

Counting the $(n!)^{|S|}$ different sets $\mathcal{M}'$, we see that $\mathcal{M}$ can be divided into at most

$$|S|(n-1) \cdot n^{2|S|} \cdot \left(\log_D \left(\frac{BC^{n-1}}{n^{n/2} n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A} \right) \right)^{|S|(n-1)-1}$$

sets of the type $\mathcal{C}$ as in (2.2.9), where we have used

$$(|S|(n-1))! = \big((n-1) + \cdots + (n-1)\big)! \geq (n-1)! \cdots (n-1)! = ((n-1)!)^{|S|}.$$

□

We will also need the following variation.

Lemma 2.2.13. *For $p \in S$, let $K_{p1}, K_{p2}, \ldots, K_{pn} \in \overline{\mathbb{Q}}_p[X_1, \ldots, X_n]$ be linearly independent linear forms in n variables. Let $A, C > 0$ and $D > 1$. Consider the set*

$$\mathcal{M} = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{c} \displaystyle\prod_{p \in S} \frac{\prod_{i=1}^n |K_{pi}(\mathbf{x}_p)|_p}{|\det(K_{p1}, K_{p2}, \ldots, K_{pn})|_p} \le A \ , \\ \\ |\mathbf{x}_\infty|_\infty \le C \ , \ |\mathbf{x}_p|_p = 1 \ , \ p \in S_0 \end{array} \right\}.$$

If $C^n \ge n! \left(\prod_{p \in S_0} (pd)^{nd/2} \right) \cdot AD^{|S|n}$, then the set $\mathcal{M}$ can be covered by at most

$$|S|n \cdot \left(\log_D \left(\frac{C^n}{n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A} \right) \right)^{|S|n-1}$$

sets of the form

$$\mathcal{C} = \{ (\mathbf{x}_p)_{p \in S} \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \le a_{pi}, \ (p \in S, 1 \le i \le n) \}$$

where $K'_{p1}, K'_{p2}, \ldots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$ with

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1$$

and the a_{pi} are positive reals with

$$\prod_{p \in S} \prod_{i=1}^n a_{pi} < n! \prod_{p \in S_0} (pd)^{nd/2} \cdot AD^{|S|n+1}.$$

Otherwise, $\mathcal{M}$ can be covered by at most $(n!)^{|S|}$ sets of that form.

Proof. The proof is similar to the proof of Lemma 2.2.12. We first cover $\mathcal{M}$ by at most $(n!)^{|S|}$ sets of the shape

$$\mathcal{M}' = \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{c} \displaystyle\prod_{p \in S} \prod_{i=1}^n |K'_{pi}(\mathbf{x}_p)|_p \le n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A, \\ \\ |\mathbf{x}_\infty|_\infty \le C \ , \ |\mathbf{x}_p|_p = 1 \ , \ p \in S_0 \end{array} \right\}$$

where the $K'_{pi} \in \mathbb{Q}_p[X_1, \ldots, X_n]$ are linear forms with

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1 \text{ for } p \in S.$$

Define reals $\{n_{pi} : p \in S, i = 1, \ldots, n\}$ by

$$|K'_{pi}(\mathbf{x}_p)|_p = D^{-n_{pi}} \ (p \in S, \quad i = 1, \ldots, n).$$

Note that

$$\sum_{p \in S} \sum_{i=1}^{n} n_{pi} \geq \log_D \left(\frac{C^n}{n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A} \right)$$

and so

$$\sum_{p \in S} \sum_{i=1}^{n} [n_{pi}] > \sum_{p \in S} \sum_{i=1}^{n} (n_{pi} - 1) \geq \log_D \left(\frac{C^n}{n! \prod_{p \in S_0} (pd)^{nd/2} \cdot AD^{|S|n}} \right).$$

Denote this last quantity by Q. Then $Q \geq 0$ if and only if

$$C^n \geq n! \prod_{p \in S_0} (pd)^{nd/2} \cdot AD^{|S|n}.$$

If $Q \geq 0$, we find non-negative integers $z_{pi} \leq [n_{pi}]$ for $p \in S, i = 1, \ldots, n$ such that

$$\sum_{p \in S} \sum_{i=1}^{n} z_{pi} = [Q].$$

Since $z_{pi} \leq n_{pi}$, we have

$$|K'_{\infty i}(\mathbf{x}_\infty)| \leq D^{-z_{\infty i}} C, \ 1 \leq i \leq n \ , \ |K'_{pi}(\mathbf{x}_p)|_p \leq D^{-z_{pi}} \ (p \in S_0, \quad 1 \leq i \leq n).$$

If $Q < 0$, we put $z_{pi} = 0$ for $p \in S, i = 1, \ldots, n$.

So we can subdivide $\mathcal{M}'$ into at most $(n!)^{|S|}$ subsets of the form:

$$\mathcal{C} := \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : |K'_{\infty i}(\mathbf{x}_\infty)| \leq D^{-z_{\infty i}} C, |K'_{pi}(\mathbf{x}_p)|_p \leq D^{-z_{pi}} \ (p \in S_0, 1 \leq i \leq n) \right\}$$

with

$$|\det(K'_{p1}, K'_{p2}, \ldots, K'_{pn})|_p = 1 \ , \ |K'_{p1}|_p = \cdots = |K'_{pn}|_p = 1 \ , \ p \in S,$$
$$\textstyle\sum_{p \in S} \sum_{i=1}^{n} z_{pi} = \max\{[Q], 0\}.$$

Let $a_{\infty i} = D^{-z_{\infty i}}C$ and $a_{pi} = D^{-z_{pi}}$. Then we have

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} \le C^n D^{-[Q]} < C^n D^{1-Q} \le n! \prod_{p\in S_0}(pd)^{nd/2}\cdot AD^{|S|\cdot n+1}.$$

The number of tuples $\underline{z} = (z_{pi})_{p\in S, i=1,\dots,n}$ of nonnegative integers satisfying $\sum_{p\in S}\sum_i z_{pi} = [Q]$ is at most

$$([Q]+|S|n-1)^{|S|n-1}/(|S|n-1)! < \frac{(Q+|S|n)^{|S|n-1}}{(|S|n-1)!}.$$

So if $Q \ge 0$, the last number is equal to

$$\frac{1}{(|S|n-1)!}\cdot\left(\log_D\left(\frac{C^n}{n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A}\right)\right)^{|S|n-1}.$$

Taking into consideration the $(n!)^{|S|}$ different sets $\mathcal{M}'$, we see that $\mathcal{M}$ can be divided into is at most

$$|S|n\cdot\left(\log_D\left(\frac{C^n}{n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A}\right)\right)^{|S|n-1}$$

sets of the type $\mathcal{C}$. □

Remark 2.2.14. For $S = \{\infty\}$, Lemma 2.2.12 and 2.2.13 are Thunder's Lemmas 7 and $7'$ in [19].

2.3 Proof of Theorem 2.1.1

In this section, we prove Theorem 2.1.1. Recall our assumptions: $F \in \mathbb{Z}[X_1,\dots,X_n]$ is a decomposable form of degree d such that $I(F) \ne \emptyset$, $a(F) < d/n$ and $F(\mathbf{x}) \ne 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$.

Define $\log^* x = \max(0, \log x)$ for $x \in \mathbb{R}_{\ge 0}$.

Assume $m > 1$. Let

$$\begin{aligned} &B_0 = m^{1/(d-a(F))} > 1,\\ &B_l = e^l B_0\ ,\ C_l = B_{l+1} = e^{l+1}B_0 \text{ for } l \in \mathbb{Z}_{\ge 0},\\ &A_0 = m^{1/a(F)} B_0^{\frac{-(d-na(F))}{a(F)}}\mathcal{H}(F)^{c(F)}\ ,\ A_l = e^{\frac{-(d-na(F))l}{a(F)}}A_0. \end{aligned} \tag{2.3.1}$$

We separate the solutions $\mathbf{x}$ of (1.1.1) into small ones with norm $|\mathbf{x}|_\infty \le B_0$ and large ones with norm $|\mathbf{x}|_\infty > B_0$. Let

$$V_0 := \mu^n\Big(\big\{(\mathbf{x}_p)_p \in \mathbb{A}_{F,S}(m) : |\mathbf{x}_\infty|_\infty \le B_0\big\}\Big),$$
$$V_{l+1} := \mu^n\Big(\big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \textstyle\prod_{p\in S} |F(\mathbf{x}_p)|_p \le m, B_l \le |\mathbf{x}_\infty|_\infty \le C_l\big\}\Big) \text{ for } l \in \mathbb{Z}_{\ge 0}.$$

Note that the difference between V_0 and $\mathbb{A}_{F,S}(m, B_0)$ is in the different norms that we use. Here in V_0 we use the Euclidean norm, while in $\mathbb{A}_{F,S}(m, B_0)$ we use the sup-norm.

Lemma 2.3.1. *Suppose that $I(F) \ne \emptyset$ and that $\mathcal{H}(F) \le \mathcal{H}(G)$ for every decomposable form G that is S-equivalent to F. Suppose that $F(\mathbf{z}) \ne 0$ for all $\mathbf{z} \in \mathbb{Q}^n \setminus \{0\}$. Then*

$$V_0 \ll m^{n/d}\Big(1 + \Big(\frac{\log B_0}{\log(2\mathcal{H}(F))}\Big)^{|S|n-1}\Big).$$

Proof. By Lemma 2.2.6, for every $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$ there are tuples $(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn}) \in I(F)$ $(p \in S)$ such that

$$\prod_{p\in S} \frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn})|_p} \ll \frac{\prod_{p\in S} |F(\mathbf{x}_p)|_p^{n/d}}{(2\mathcal{H}(F))^{1/d}} \le \frac{m^{n/d}}{(2\mathcal{H}(F))^{1/d}}. \tag{2.3.2}$$

We use Lemma 2.2.13 to give a bound for the volume V_0. Put $A = m^{n/d}/(2\mathcal{H}(F))^{1/d}$, $C = B_0$ and $D = (2\mathcal{H}(F))^{1/d(|S|\cdot n+1)}$. Then the set of $(\mathbf{x}_p)_p \in \mathbb{A}_S^n$ satisfying inequality (2.3.2) and $|\mathbf{x}_\infty|_\infty \le B_0$ can be covered by at most

$$\ll 1 + |S|n \cdot \left(\log_D\left(\frac{C^n}{A}\right)\right)^{|S|n-1} \ll 1 + (\log_D C)^{|S|n-1} \ll 1 + \left(\frac{\log B_0}{\log(2\mathcal{H}(F))}\right)^{|S|n-1}$$

sets of the form

$$\mathcal{C} = \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \le a_{pi} \text{ for } p \in S, i = 1, \dots, n\Big\}$$

where $K'_{p1}, K'_{p2}, \dots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \dots, X_n]$ with

$$|\det(\mathbf{K}'_{p1}, \mathbf{K}'_{p2}, \dots, \mathbf{K}'_{pn})|_p = 1\ ,\ |\mathbf{K}'_{p1}|_p = \cdots = |\mathbf{K}'_{p1}|_p = 1 \text{ for } \ p \in S$$

and the a_{pi} are reals with

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} < n!\prod_{p\in S_0}(pd)^{nd/2}\cdot AD^{|S|n+1} \ll m^{n/d}.$$

By Lemma 1.2.5, we have

$$\mu^n(\mathcal{C}) \ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi} \ll m^{n/d}.$$

Hence the volume V_0 is at most the sum of the volumes of the sets $\mathcal{C}$, that is,

$$V_0 \ll m^{n/d}\left(1+\left(\frac{\log B_0}{\log(2\mathcal{H}(F))}\right)^{|S|n-1}\right).$$

□

Lemma 2.3.2. *With the notation above, we have*

$$\sum_{l=0}^{\infty} V_{l+1} \ll m^{1/a(F)} B_0^{\frac{d-na(F)}{a(F)}}\mathcal{H}(F)^{c(F)}(1+\log B_0)^{|S|(n-1)-1}.$$

Proof. By Lemma 2.2.4, for every $(\mathbf{x}_p)_p \in \mathbb{A}_{F,S}(m)$ with $B_l \le |\mathbf{x}_\infty|_\infty \le C_l$ there are tuples $\{(\mathbf{L}_{p1},\mathbf{L}_{p2},\ldots,\mathbf{L}_{pn}) \in I(F)(p\in S)$ such that

$$\begin{aligned}
\prod_{p\in S}\frac{\prod_{j=1}^{n}|L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\ldots,\mathbf{L}_{pn})|_p} &\ll \prod_{p\in S}\left(\frac{|F(\mathbf{x}_p)|_p}{|\mathbf{x}_p|_p^{d-na(F)}}\right)^{1/a(F)}\cdot\mathcal{H}(F)^{c(F)}\\
&= \left(\frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p}{|\mathbf{x}_\infty|_\infty^{d-na(F)}}\right)^{1/a(F)}\cdot\mathcal{H}(F)^{c(F)}\\
&\le \left(\frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p}{B_l^{d-na(F)}}\right)^{1/a(F)}\cdot\mathcal{H}(F)^{c(F)}\\
&\le \left(\frac{m}{B_l^{d-na(F)}}\right)^{1/a(F)}\cdot\mathcal{H}(F)^{c(F)}\\
&= m^{1/a(F)}B_0^{\frac{-(d-na(F))}{a(F)}}\mathcal{H}(F)^{c(F)}e^{\frac{-(d-na(F))l}{a(F)}} = A_l.
\end{aligned}$$

By Lemma 2.2.12 with $A = A_l, B = B_l, C = C_l, D = e$, the set of $(\mathbf{x}_p)_p \in \mathbb{A}_{F,S}(m)$ with $B_l \le |\mathbf{x}_\infty|_\infty < C_l$ satisfying the inequality

$$\prod_{p\in S} \frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \dots, \mathbf{L}_{pn})|_p} \le A_l$$

can be covered by at most

$$\ll |S|(n-1)\cdot n^{2|S|}\cdot \Big(\log^* \Big(\frac{B_l C_l^{n-1}}{n^{n/2} n! \prod_{p\in S_0} (pd)^{nd/2} \cdot A_l} \Big) \Big)^{|S|(n-1)-1} \ll (1+l+\log B_0)^{|S|(n-1)-1}$$

sets of the form

$$\mathcal{C} = \{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \le a_{pi} \text{ for } p \in S, i = 1, \dots, n\}$$

where $K'_{p1}, K'_{p2}, \dots, K'_{pn} \in \mathbb{Q}_p[X_1, \dots, X_n]$ are linear forms with

$$|\det(\mathbf{K}'_{p1}, \mathbf{K}'_{p2}, \dots, \mathbf{K}'_{pn})|_p = 1\ ,\ |\mathbf{K}'_{p1}|_p = \dots = |\mathbf{K}'_{pn}|_p = 1 \text{ for } p \in S$$

and

$$\prod_{p\in S}\prod_{i=1}^n a_{pi} < n^{n/2} n! \prod_{p\in S_0} (pd)^{nd/2} \cdot \frac{C_l A_l}{B_l} D^{|S|\cdot(n-1)+1} \ll \frac{C_l A_l}{B_l} \ll A_l \le e^{-l/(n-1)} A_0.$$

In the last inequality, we have used the facts that if $a(F) < d/n$ then $\frac{d-na(F)}{a(F)} \ge \frac{1}{n-1}$, since $a(F)$ is a fraction of denominator $\le n-1$.

By Lemma 1.2.5, each set $\mathcal{C}$ has volume

$$\mu^n(\mathcal{C}) \ll \frac{C_l A_l}{B_l} D^{|S|\cdot(n-1)+1} \ll e^{-l/(n-1)} A_0.$$

Hence for each $l \ge 0$, we have

$$\begin{aligned} V_{l+1} &\ll e^{-l/(n-1)} A_0 \cdot (1 + l + \log B_0)^{|S|(n-1)-1} \\ &\ll \frac{(1+l)^{|S|(n-1)-1}}{e^{l/(n-1)}} \cdot A_0 (1 + \log B_0)^{|S|(n-1)-1}. \end{aligned}$$

As a consequence

$$\sum_{l=0}^{\infty} V_{l+1} \ll A_0(1+\log B_0)^{|S|(n-1)-1} \cdot \sum_{l=0}^{\infty}(1+l)^{|S|(n-1)-1} e^{-l/(1-n)}$$
$$\ll A_0(1+\log B_0)^{|S|(n-1)-1} = m^{1/a(F)} B_0^{\frac{-(d-na(F))}{a(F)}} \mathcal{H}(F)^{c(F)}(1+\log B_0)^{|S|(n-1)-1}.$$

□

Proof of Theorem 2.1.1. First, by Lemma 1.3.1 we see that $\mu^n(\mathbb{A}_{F,S}(m))$ is homogeneous in m. So if the claim holds for some m of our choice, it also holds for any other m'.

By Lemma 2.3.1 and 2.3.2, we know

$$V_0 \ll m^{n/d}\left(1+\left(\frac{\log B_0}{\log(2\mathcal{H}(F))}\right)^{|S|n-1}\right)$$

and

$$\sum_{l=0}^{\infty} V_{l+1} \ll m^{1/a(F)} B_0^{\frac{-(d-na(F))}{a(F)}} \mathcal{H}(F)^{c(F)}(1+\log B_0)^{|S|(n-1)-1}.$$

Using (2.3.1), we have $m^{1/a(F)} B_0^{\frac{-(d-na(F))}{a(F)}} = m^{\frac{n-1}{d-a(F)}}$. Choose m such that

$$m^{\frac{n-1}{d-a(F)}} \cdot \mathcal{H}(F)^{c(F)} = m^{\frac{n}{d+1/2(n-1)^2}}.$$

Hence we have $\log m \gg\ll \log \mathcal{H}(F)$ and

$$V_0 \ll m^{n/d} \text{ and } \sum_{l=0}^{\infty} V_{l+1} \ll m^{\frac{n}{d+1/2(n-1)^2}} \cdot (1+\log B_0)^{|S|(n-1)-1} \ll m^{n/d}.$$

Therefore

$$\mu^n\big(\mathbb{A}_{F,S}(m)\big) \ll V_0 + \sum_{l=0}^{\infty} V_{l+1} \ll m^{n/d}.$$

This proves Theorem 2.1.1. □

2.4 Large solutions

In this section, we assume that $I(F) \neq \emptyset$ and $a(F) < d/n$. We use the same notation as in (2.3.1):

$$B_0 = m^{1/(d-na(F))} > 1,$$
$$B_l = e^l B_0\ ,\ C_l = B_{l+1} = e^{l+1} B_0 \text{ for } l \in \mathbb{Z}_{\geq 0},$$
$$A_0 = m^{1/a(F)} B_0^{\frac{-(d-na(F))}{a(F)}} \mathcal{H}(F)^{c(F)}\ ,\ A_l = e^{\frac{-(d-na(F))l}{a(F)}} A_0.$$

We focus on the large solutions $\mathbf{x}$ to the inequality (1.1.1) with $|\mathbf{x}|_\infty \geq B_0$. The idea is as follows. We use the p-adic Subspace Theorem to deal with the solutions with $|\mathbf{x}|_\infty \geq C_{l_1}$ for some l_1. We deal with the solutions with $B_0 \leq |\mathbf{x}|_\infty \leq C_{l_1}$ similarly as what we did for $\sum_{l=0}^{\infty} V_{l+1}$.

To be precise: for every solution $\mathbf{x}$ with $|\mathbf{x}|_\infty \geq C_l$, we have by Lemma 2.2.4

$$\begin{aligned}
&\prod_{p\in S} \frac{\prod_{j=1}^{n} |L_{pj}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p} \leq c \cdot \left(\frac{\prod_{p\in S} |F(\mathbf{x})|_p}{|\mathbf{x}|_\infty^{d-na(F)}}\right)^{1/a(F)} \cdot \mathcal{H}(F)^{c(F)} \\
&\leq \frac{1}{|\mathbf{x}|_\infty^{(d-na(F))/(2a(F))}} \cdot c \cdot \left(\frac{m}{C_l^{(d-na(F))/2}}\right)^{1/a(F)} \cdot \mathcal{H}(F)^{c(F)} \\
&\leq |\mathbf{x}|_\infty^{-1/(2(n-1))} \cdot c \cdot \left(\frac{m}{C_l^{(d-na(F))/2}}\right)^{1/a(F)} \cdot \mathcal{H}(F)^{c(F)} \qquad (2.4.1)
\end{aligned}$$

where c is a constant depending only on n, d and S.

Let l_0 be the smallest integer l such that $c \cdot \left(\frac{m}{C_l^{(d-na(F))/2}}\right)^{1/a(F)} \cdot \mathcal{H}(F)^{c(F)} \leq 1$. This implies

$$l_0 \ll 1 + \log m + \log \mathcal{H}(F).$$

Let l_1 be the smallest integer l such that $C_l \geq \max\{m^{1/d} C_{l_0}, m^{1/d}\mathcal{H}(F)\}$. This implies

$$l_0 \leq l_1 \ll 1 + \log m + \log \mathcal{H}(F). \qquad (2.4.2)$$

Define

$$\mathcal{L}_1 = \{\mathbf{x} \in \mathbb{Z}^n : \prod_{p \in S} |F(\mathbf{x})|_p \leq m, B_0 \leq |\mathbf{x}|_\infty \leq C_{l_1}, |\mathbf{x}|_p = 1 \text{ for } p \in S_0\},$$
$$\mathcal{L}_2 = \{\mathbf{x} \in \mathbb{Z}^n : \prod_{p \in S} |F(\mathbf{x})|_p \leq m, |\mathbf{x}|_\infty \geq C_{l_1}, |\mathbf{x}|_p = 1 \text{ for } p \in S_0\}. \tag{2.4.3}$$

Lemma 2.4.1. *$\mathcal{L}_1$ is contained in a union of a finite set Ω of cardinality*

$$|\Omega| \ll m^{1/a(F)} B_0^{\frac{d-na(F)}{a(F)}} \mathcal{H}(F)^{c(F)} (1 + \log B_0)^{|S|(n-1)-1}$$

and at most

$$\ll (1 + \log m + \log \mathcal{H}(F))(1 + \log m + \log \mathcal{H}(F) + \log B_0)^{|S|(n-1)-1}$$

proper linear subspaces of $\mathbb{Q}^n$.

Proof. The proof is similar to the proof of Lemma 2.3.2. We use Lemma 2.2.12 with $A = A_l, B = B_l, C = C_l$ and $D = e$. Then the set of $\mathbf{x}$ in $\mathcal{L}_1$ with $B_l \leq |\mathbf{x}|_\infty < C_l$ satisfying the inequality

$$\prod_{p \in S} \frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p1}, \mathbf{L}_{p2}, \ldots, \mathbf{L}_{pn})|_p} \leq A_l$$

can be covered by at most $\ll (1 + l + \log B_0)^{|S|(n-1)-1}$ sets of the form

$$\mathcal{C} = \left\{(\mathbf{x}_p)_{p \in S} \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \leq a_{pi} \text{ for } p \in S, i = 1, \ldots, n\right\}$$

with

$$\prod_{p \in S} \prod_{i=1}^n a_{pi} \ll e^{-l/(n-1)} A_0.$$

By Lemma 1.2.5, if there are n linearly independent lattice points in $\mathcal{C}$, the number of the integer points in $\mathcal{C}$ is $\ll e^{l/(1-n)} A_0$, which is the same as the upper bound of $\mu^n(\mathcal{C})$.

Let Ω be the union of the sets of integer points occurring in the set $\mathcal{C}$ as above having n linear independent lattice points. Then the cardinality of Ω is at most

$$\ll \sum_{l=0}^{l_1} V_{l+1} \ll \sum_{l=0}^{\infty} V_{l+1} \ll m^{1/a(F)} B_0^{\frac{d-na(F)}{a(F)}} \mathcal{H}(F)^{c(F)} (1+\log B_0)^{|S|(n-1)-1}.$$

We now consider the sets $\mathcal{C}$ that do not contain n linearly independent integer points. Then the set of integer points in such a set $\mathcal{C}$ is contained in a proper linear subspace of $\mathbb{Q}^n$ that is related to $\mathcal{C}$.

Recall that $l_1 \ll 1+\log m+\log \mathcal{H}(F)$. So $\mathcal{L}_1$ can be covered by the set Ω and at most

$$\begin{aligned} &\ll \textstyle\sum_{l=0}^{l_1}(1+l+\log B_0)^{|S|(n-1)-1} \ll (l_1+1)(1+l_1+\log B_0)^{|S|(n-1)-1} \\ &\ll (1+\log m+\log \mathcal{H}(F))(1+\log m+\log \mathcal{H}(F)+\log B_0)^{|S|(n-1)-1} \end{aligned}$$

proper linear subspaces of $\mathbb{Q}^n$. □

Lemma 2.4.2. *$\mathcal{L}_2$ is contained in at most $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$.*

Proof. For any $\mathbf{x}$ in $\mathcal{L}_2$ with $\prod_{p\in S}|F(\mathbf{x})|_p \neq 0$, we have $\prod_{p\in S}|F(\mathbf{x})|_p \geq 1$. So it remains to consider those $\mathbf{x}$ in $\mathcal{L}_2$ with $\prod_{p\in S}|F(\mathbf{x})|_p \geq 1$. Let $\mathbf{x}$ be such a solution with $\mathbf{x}=g\mathbf{x}'$ where $\mathbf{x}'$ is primitive and $\gcd(g,\prod_{i=1}^r p_i)=1$. Then

$$m \geq \prod_{p\in S}|F(\mathbf{x})|_p = g^d \prod_{p\in S}|F(\mathbf{x}')|_p \geq g^d.$$

Thus $g \leq m^{1/d}$. As a consequence $|\mathbf{x}'|_\infty = g^{-1}|\mathbf{x}|_\infty \geq m^{-1/d}C_{l_1} \geq \max\{C_{l_0},\mathcal{H}(F)\}$. Since $|\mathbf{x}'|_\infty \geq C_0$, by inequality (2.4.1) we have

$$\prod_{p\in S}\frac{\prod_{j=1}^n |L_{pj}(\mathbf{x}')|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\ldots,\mathbf{L}_{pn})|_p} < |\mathbf{x}'|_\infty^{-1/(2(n-1))}.$$

By Lemma 1.1.6, we may assume that each $\mathbf{L}_{pi}$ here is defined over a number field of degree at most d. So we have $[\mathbb{Q}(\mathbf{L}_{pi}):\mathbb{Q}] \leq d$ and

$$H_{\mathbb{Q}(\mathbf{L}_{pi})}(\mathbf{L}_{pi}) \leq \mathcal{H}(F) \leq |\mathbf{x}'|_\infty.$$

Therefore we can apply a version of the quantitative Subspace Theorem such as [6, Corollary] which implies that the primitive integer solutions of the inequality above lie in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$. Taking into account of number of possible tuples in $I(F)$, all the $\mathbf{x}$ in $\mathcal{L}_2$ with $|\mathbf{x}|_\infty \geq C_{l_1}$ lie in $\ll 1$ proper subspaces. $\square$

2.5 Proof of Theorems 2.1.3 and 2.1.4

We consider again inequality (1.1.1):

$$\prod_{p\in S} |F(\mathbf{x})|_p \leq m \text{ in } \mathbf{x} \in \mathbb{Z}^n \text{ with } \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1.$$

Assume $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also assume $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$.

In the proof, it will be important to keep the following fact in mind. Considering the integral solutions to the inequality (1.1.1) for F restricted to a proper linear subspace of $\mathbb{Q}^n$ is equivalent to considering integral solutions to a similar inequality in fewer variables.

Proof of Theorem 2.1.3. The proof is by induction on n.

Let $n = 1$ and $F(x) = cx^d$ with $c \in \mathbb{Z}$. We consider the solutions of

$$\prod_{p\in S} |cx^d|_p \leq m \text{ in } x \in \mathbb{Z} \text{ with } |x|_p = 1.$$

For every solution x, we have $m \geq \prod_{p\in S} |cx^d|_p = \prod_{p\in S} |c|_p \cdot |x|^d \geq |x|^d$. So it is clear that $N_{F,S}(m) \ll m^{1/d}$.

Let $n \geq 2$. Assume that the number of integral solutions restricted to any proper linear subspace of $\mathbb{Q}^n$ of dimension $n' < n$ is $\ll m^{n'/d}$. We have to distinguish two cases:

(*a*) $\mathcal{H}(F)^{c(F)} m^{(n-1)/(d-a(F))} \leq m^{\frac{n}{d+1/(2(n-1)^2)}}$. (See (2.2.2) for the definition of $c(F)$.) Then we have $\log(\mathcal{H}(F)) \ll \log m$ and

$$\mathcal{H}(F)^{c(F)} m^{(n-1)/(d-a(F))} (1 + \log B_0)^{|S|(n-1)-1} \ll m^{n/d}$$

where B_0 is defined in (2.3.1).

By Proposition 1.4.6 and Theorem 2.1.1, we have $\mu^n(\mathbb{A}_{F,S}(m)) \ll m^{n/d}$ and

$$\begin{aligned}|\mathbb{A}_{F,S}(m,B_0)\cap\mathbb{Z}^n| &\ll \mu^n(\mathbb{A}_{F,S}(m,B_0)) + B_0^{n-1}\Big(1+\log\big(\mathcal{H}(F)B_0\big)\Big)^{dr}\\ &\ll \mu^n(\mathbb{A}_{F,S}(m)) + B_0^{n-1}\Big(1+\log\big(\mathcal{H}(F)B_0\big)\Big)^{dr} \ll m^{n/d}.\end{aligned}$$

By Lemma 2.4.1 and Lemma 2.4.2, the large solutions of (1.1.1), i.e., those with $|\mathbf{x}|_\infty \geq B_0$ lie in the union of a set of cardinality

$$\ll m^{1/a(F)} B_0^{\frac{d-na(F)}{a(F)}} \mathcal{H}(F)^{c(F)}(1+\log B_0)^{|S|(n-1)-1} \ll m^{n/d}$$

and

$$\ll (1+\log m+\log\mathcal{H}(F))(1+\log m+\log\mathcal{H}(F)+\log B_0)^{|S|(n-1)-1} \ll (1+\log m)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$. Using the induction hypothesis, these subspaces together contain at most

$$\ll m^{(n-1)/d}(1+\log m)^{|S|(n-1)} \ll m^{n/d}$$

solutions. So $N_{F,S}(m) \ll m^{n/d}$.

(*b*) $\mathcal{H}(F)^{c(F)} m^{(n-1)/(d-a(F))} \geq m^{\frac{n}{d+1/(2(n-1)^2)}}$. Then we have $\log(\mathcal{H}(F)) \gg 1+\log m$. Choose l_1 as in (2.4.2). So we have

$$l_1 \ll 1+\log m+\log\mathcal{H}(F).$$

By Lemma 2.2.6, for every solution $\mathbf{x}$ with $|\mathbf{x}|_\infty \leq C_{l_1}$, there are tuples $\{(\mathbf{L}_{p1},\mathbf{L}_{p2},\ldots,\mathbf{L}_{pn}) \in I(F) : p\in S\}$ such that

$$\prod_{p\in S}\frac{\prod_{j=1}^n |L_{pj}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p1},\mathbf{L}_{p2},\ldots,\mathbf{L}_{pn})|_p} \ll \frac{\prod_{p\in S}|F(\mathbf{x})|_p^{n/d}}{(2\mathcal{H}(F))^{1/d}} \leq \frac{m^{n/d}}{(2\mathcal{H}(F))^{1/d}}.$$

Put $A = m^{n/d}/(2\mathcal{H}(F))^{1/d}$, $C = C_{l_1}$ and $D = (2\mathcal{H}(F))^{1/d(|S|\cdot n+1)}$. Then by Lemma 2.2.13 the solutions lie in

$$\begin{aligned}&\ll |S|n\cdot\left(\log_D^*\left(\frac{C^n}{n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A}\right)\right)^{|S|n-1} \ll (\log_D^* C)^{|S|n-1}\\ &\ll \left(\frac{\log C_{l_1}}{\log(2\mathcal{H}(F))}\right)^{|S|n-1} \ll \left(\frac{\log m + l_1}{\log(2\mathcal{H}(F))}\right)^{|S|n-1} \ll 1\end{aligned}$$

sets of the form

$$\mathcal{C} = \{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : |K'_{pi}(\mathbf{x}_p)|_p \le a_{pi} \text{ for } p \in S, i = 1, \dots, n\}$$

where $K'_{p1}, K'_{p2}, \dots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \dots, X_n]$ with

$$|\det(\mathbf{K}'_{p1}, \mathbf{K}'_{p2}, \dots, \mathbf{K}'_{pn})|_p = 1\ ,\ |\mathbf{K}'_{p1}|_p = \cdots = |\mathbf{K}'_{p1}|_p = 1 \text{ for } \ p \in S,$$

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} < n! \prod_{p\in S_0} (pd)^{nd/2} \cdot AD^{|S|n+1} \ll m^{n/d}.$$

If such a set $\mathcal{C}$ contains n linearly independent integral points, then by Lemma 1.2.5 the total number of integral points in $\mathcal{C}$ is $\ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi} \ll m^{n/d}$. Thus, we see that the integral solutions with $|\mathbf{x}|_\infty \le C_{l_1}$ lie in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$ and a set with cardinality $\ll m^{n/d}$.

By Lemma 2.4.2, the integral solutions with $|\mathbf{x}|_\infty \ge C_{l_1}$ also lie in $\ll 1$ proper rational subspaces. By the induction hypothesis, each subspace contributes $\ll m^{(n-1)/d}$ integral solutions.

Therefore $N_{F,S}(m) \ll m^{n/d}$. □

Proof of Theorem 2.1.4. By Lemma 2.3.2, we have

$$\left|\mu^n(\mathbb{A}_{F,S}(m)) - \mu^n(\mathbb{A}_{F,S}(m, B_0))\right| \le \sum_{l=0}^{\infty} V_{l+1} \ll m^{(n-1)/(d-a(F))}\mathcal{H}(F)^{c(F)}(1+\log B_0)^{|S|(n-1)-1}.$$

By Proposition 1.4.6, we have

$$\left| \left|(\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n)\right| - \mu^n(\mathbb{A}_{F,S}(m, B_0))\right| \ll m^{(n-1)/(d-a(F))}(1 + \log(\mathcal{H}(F)B_0))^{dr}.$$

Hence

$$\begin{aligned}
&\left|\mu^n(\mathbb{A}_{F,S}(m)) - \left|(\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n)\right| \right| \\
&\ll m^{(n-1)/(d-a(F))}\mathcal{H}(F)^{c(F)}(1 + \log B_0)^{|S|(n-1)-1} + m^{(n-1)/(d-a(F))}(1 + \log(\mathcal{H}(F)B_0))^{dr} \\
&\ll m^{(n-1)/(d-a(F))}(1 + \log m)^{d|S|} \max\{\mathcal{H}(F)^{c(F)}, (1 + \log \mathcal{H}(F))^{d|S|}\} \\
&= O_{F,S}(m^{\frac{n}{d+1/2(n-1)^2}}) \ \ as \ \ m \to \infty.
\end{aligned}$$

By Lemmas 2.4.1 and 2.4.2, we know that the set of integral solutions with $|\mathbf{x}|_\infty \geq B_0$ is covered by a finite set Ω and at most

$$(1 + \log m + \log \mathcal{H}(F))(1 + \log m + \log \mathcal{H}(F) + \log B_0)^{|S|(n-1)-1}$$

proper linear subspaces of $\mathbb{Q}^n$. By Theorem 2.1.3, we know that the number of solutions in each subspace is at most $m^{(n-1)/d}$. Let $\mathcal{L}_1$, $\mathcal{L}_2$ be the sets defined by (2.4.3). Then

$$\begin{aligned}
&\Big| N_{F,S}(m) - |(\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n)| \Big| \ll |\mathcal{L}_1| + |\mathcal{L}_2| \\
&\ll m^{(n-1)/(d-a(F))}\mathcal{H}(F)^{c(F)}(1 + \log B_0)^{|S|(n-1)-1} + \\
&\qquad + m^{(n-1)/d}(1 + \log m + \log \mathcal{H}(F))(1 + \log m + \log \mathcal{H}(F) + \log B_0)^{|S|(n-1)-1} \\
&\ll m^{(n-1)/(d-a(F))}(1 + \log m)^{d|S|} \max\{\mathcal{H}(F)^{c(F)}, (1 + \log \mathcal{H}(F))^{d|S|}\} \\
&= O_{F,S}(m^{\frac{n}{d+1/2(n-1)^2}}) \quad as \quad m \to \infty.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&\Big| N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m)) \Big| \\
&\leq \Big| N_{F,S}(m) - |\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n| \Big| + \Big| |\mathbb{A}_{F,S}(m, B_0) \cap \mathbb{Z}^n| - \mu^n(\mathbb{A}_{F,S}(m)) \Big| \\
&\ll m^{(n-1)/(d-a(F))}(1 + \log m)^{d|S|} \max\{\mathcal{H}(F)^{c(F)}, (1 + \log \mathcal{H}(F))^{d|S|}\} \\
&= O_{F,S}(m^{\frac{n}{d+1/2(n-1)^2}}) \quad as \quad m \to \infty. \qquad (2.5.1)
\end{aligned}$$

$\square$

Chapter 3

An effective finiteness criterion for decomposable form inequalities

In this chapter, let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d and $S = \{\infty, p_1, \ldots, p_r\}$ where $p_1, \ldots, p_r$ are distinct primes. We assume $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Q}^n$, which implies that $I(F) \neq \emptyset$. Recall that

$$\begin{aligned} a(F) &= \max_{(\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_n}) \in I(F)} \max_{1 \leq j \leq n-1} \frac{|\{\mathbf{L}_i \in \text{span } \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}|}{j} \\ &= \max_{\substack{\emptyset \neq \mathcal{L} \subseteq \{\mathbf{L}_1, \ldots, \mathbf{L}_d\} \\ \text{rank}(\mathcal{L}) < n}} \frac{|\mathcal{L}|}{\text{rank } (\mathcal{L})}. \end{aligned}$$

By Theorem 2.1.3, the inequality

$$\begin{gathered} \textstyle\prod_{p \in S} |F(\mathbf{x})|_p \leq m \quad \text{in} \quad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{with} \quad \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1 \end{gathered}$$

has only finitely many solutions, provided

$$a(F|_T) < \frac{d}{\dim T} \text{ for every linear subspace } T \text{ of dimension at least 2 of } \mathbb{Q}^n.$$

The question that immediately arises is how to effectively test this criterion, that is, whether there is an algorithm that, given the coefficients of F and its linear factors, checks in finitely many steps whether the criterion is satisfied.

Besides $a(F)$, we also define

$$\alpha(F) := \max_{\emptyset \neq \mathcal{L} \subsetneq \{\mathbf{L}_1, \ldots, \mathbf{L}_d\}} \frac{|\mathcal{L}|}{\text{rank } (\mathcal{L})}.$$

We notice that, under the condition $I(F) \neq \emptyset$,

$$a(F|_T) < \frac{d}{\dim T} \iff \alpha(F|_T) < \frac{d}{\dim T}.$$

Hence, throughout this chapter, we equivalently use $a(F)$ and $\alpha(F)$. We answer the question above in two steps. In the first section, we assume F to be a norm form, which is a special type of decomposable form. In this case the question turns out to be standard. We can find the answer in the book [15] of W. Schmidt. In the second section, we have collected some basic facts about finite étale algebras. In the third section, we consider the general case, when F is an arbitrary decomposable form. This turns out to be similar to the norm form case. Our argument is based on arguments from [8].

3.1 Norm forms

In this section, let $\mathbb{K}$ be a number field of degree d. Denote by $\mathbb{L}$ its normal closure over $\mathbb{Q}$ and let $x \to x^{(1)} = x, \ldots, x \to x^{(d)}$ be the embeddings of $\mathbb{K}$ in $\mathbb{L}$. Consider the norm form

$$F = c \cdot N_{\mathbb{K}/\mathbb{Q}}(w_1 X_1 + \cdots + w_n X_n) = c \cdot N_{\mathbb{K}/\mathbb{Q}}(L) = c \cdot L^{(1)} \cdots L^{(d)} \in \mathbb{Q}[X]$$

where $c \in \mathbb{Q}^*$, $\mathbb{K} = \mathbb{Q}(w_1, \ldots, w_n)$, $L = w_1 X_1 + \cdots + w_n X_n$ and $L^{(i)} = \sum_{j=1}^{n} w_j^{(i)} X_j$ for $i = 1, \ldots, d$.

We assume that $F(\mathbf{x}) \neq 0$ for all $\mathbf{x} \in \mathbb{Q}^n \setminus \{0\}$. This implies that $w_1, \ldots, w_n$ are linearly independent over $\mathbb{Q}$. Hence

$$\text{rank}_{\mathbb{L}}\{L^{(1)}, \ldots, L^{(d)}\} = n.$$

Let $G := \text{Gal}(\mathbb{L}/\mathbb{Q})$. We know that G acts transitively on $\{L^{(1)}, \ldots, L^{(d)}\}$. That is for each $\sigma \in G$, there is a permutation $\hat{\sigma}$ of $\{1, \ldots, d\}$ such that

$$\sigma(L^{(i)}) = L^{(\hat{\sigma}(i))} \text{ for } i = 1, \ldots, d$$

and for each $i, j \in \{1, \ldots, d\}$ there is $\sigma \in G$ with $\hat{\sigma}(i) = j$.

For each non-empty subset S of $\{1, \ldots, d\}$, define

$$r(S) := \operatorname{rank}\{L^{(i)} : i \in S\} \quad \text{and} \quad q(S) = \frac{r(S)}{|S|}.$$

Definition 3.1.1. *A non-empty subset S of $\{1, \ldots, d\}$ is called extremal if*

- $q(S) \leq q(S')$ *for all non-empty* $S' \subseteq \{1, \ldots, d\}$,
- $q(S) < q(S')$ *for all non-empty* $S' \subsetneq S$.

Remark 3.1.2. (a) Extremal subsets exist. Indeed, let $q_0 := \min\{q(T) : T \subseteq \{1, \ldots, d\}, T \neq \emptyset\}$ and $\{S_1, S_2, \ldots, S_n\} = \{S : q(S) = q_0\}$. Choose i_0 such that $|S_{i_0}| = \min_{1 \leq i \leq n} |S_i|$. Then S_{i_0} is an extremal subset. Indeed, for every non-empty $T \subsetneq S_{i_0}$ we have $T \notin \{S_1, S_2, \ldots, S_n\}$ since $|T| < |S_{i_0}|$. Hence $q(S_{i_0}) < q(T)$.

(b) We know that $q(\{1, \ldots, d\}) = n/d$. So $\{1, \ldots, d\}$ is extremal if and only if $q(S) > n/d$ for all non-empty $S \subsetneq \{1, \ldots, d\}$.

Lemma 3.1.3. *Suppose that $S_1 \neq S_2$ are two different extremal subsets. Then $S_1 \cap S_2 = \emptyset$.*

Proof. Assume $S_1 \cap S_2 \neq \emptyset$. Let $q(S_1) = q(S_2) = q_0$. Then since

$$|S_1 \cap S_2| + |S_1 \cup S_2| = |S_1| + |S_2|,$$
$$r(S_1 \cap S_2) + r(S_1 \cup S_2) \leq r(S_1) + r(S_2),$$

we have

$$\begin{aligned}
&|S_1 \cap S_2| \cdot q(S_1 \cap S_2) = r(S_1 \cap S_2) \\
&\leq r(S_1) + r(S_2) - r(S_1 \cup S_2) = |S_1|q_0 + |S_2|q_0 - q(S_1 \cup S_2)|S_1 \cup S_2| \\
&\leq |S_1|q_0 + |S_2|q_0 - |S_1 \cup S_2|q_0 = |S_1 \cap S_2|q_0.
\end{aligned}$$

So $q(S_1 \cap S_2) \leq q_0$. This is in contradiction with the extremality of S_1 and S_2. □

Lemma 3.1.4. *Let S be an extremal subset of $\{1, \ldots, d\}$. Then the extremal subsets form a partition of $\{1, \ldots, d\}$ and $q(S) = n/d$.*

Proof. If S is a extremal subset, then so is $\hat{\sigma}(S)$ for each $\sigma \in G$. Indeed, since we have $|S| = |\hat{\sigma}(S)|$ and $r(S) = r(\hat{\sigma}(S))$, we have also $q(S) = q(\hat{\sigma}(S))$.

Since G acts transitively on $\{1, \ldots, d\}$, the collection $\{\hat{\sigma}(S) : \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})\}$ covers the set $\{1, \ldots, d\}$. Let $\hat{\sigma}_1(S), \ldots, \hat{\sigma}_t(S)$ be the distinct sets in this collection. Then

$$\{1, \ldots, d\} = \hat{\sigma}_1(S) \cup \cdots \cup \hat{\sigma}_t(S)$$

and by Lemma 3.1.3, these sets are pairwise disjoint.

Note that for every L_i which lies in the span$\{L_j : j \in S\}$, we have $i \in S$. Since otherwise we would have

$$q(S \cup \{i\}) = \frac{r(S \cup \{i\})}{|S \cup \{i\}|} < \frac{r(S)}{|S|} = q(S)$$

which contradicts the extremality of S. This implies

$$\sum_{i=1}^{t} r(\hat{\sigma}_i(S)) = r(\{1, \ldots, d\}) = n.$$

Hence

$$\frac{n}{d} = \frac{\sum_{i=1}^{t} r(\hat{\sigma}_i(S))}{\sum_{i=1}^{t} |\hat{\sigma}_i(S)|} = \frac{t \cdot r(S)}{t \cdot |S|} = q(S).$$

□

Let S be the necessarily unique extremal subset with $1 \in S$.

Define $G_S = \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) : \hat{\sigma}(S) = S\}$. Let $\mathbb{M}$ be the number field with $\mathbb{Q} \subseteq \mathbb{M} \subseteq \mathbb{L}$ and $\mathrm{Gal}(\mathbb{L}/\mathbb{M}) = G_S$.

Recall that $\{1, \ldots, d\} = \hat{\sigma}_1(S) \cup \cdots \cup \hat{\sigma}_t(S)$ where $\sigma_1, \ldots, \sigma_t \in G$ and $\hat{\sigma}_1(S), \ldots, \hat{\sigma}_t(S)$ are pairwise disjoint. So

$$|G_S| = |\mathrm{Gal}(\mathbb{L}/\mathbb{Q})|/t$$

and hence

$$[\mathbb{M} : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{Q})|/|\mathrm{Gal}(\mathbb{L}/\mathbb{M})| = |\mathrm{Gal}(\mathbb{L}/\mathbb{Q})|/|G_S| = t.$$

Lemma 3.1.5. *Suppose that S is an extremal subset with $1 \in S$. Then $\mathbb{M} \subseteq \mathbb{K}$.*

Proof. We first show that

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) : \hat{\sigma}(1) = 1\}.$$

Indeed, since $L = L^{(1)}$ and $\mathbb{K}$ is generated by the coefficients of L we have

$$\hat{\sigma}(1) = 1 \iff \sigma(L) = L \iff \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}).$$

If $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, then $\hat{\sigma}(1) = 1$ which implies $\hat{\sigma}(S) = S$ by Lemma 3.1.3. Hence $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \leq \mathrm{Gal}(\mathbb{L}/\mathbb{M})$ which implies $\mathbb{M} \subseteq \mathbb{K}$. □

Consider the $\mathbb{Q}$-vector space

$$V = \{x_1 w_1 + \cdots + x_n w_n : x_i \in \mathbb{Q} \text{ for } i = 1, \ldots, n\}.$$

For each subfield $\mathbb{E}$ of $\mathbb{K}$ and every $\mathbb{Q}$-linear subspace W of V, define

$$W^{\mathbb{E}} := \{v \in W : \epsilon \cdot v \in W \text{ for all } \epsilon \in \mathbb{E}\}.$$

Lemma 3.1.6. *Let $\mathbb{E}$ be a subfield of $\mathbb{K}$. Then we have the following:*

(a) $W^{\mathbb{E}}$ is a $\mathbb{Q}$-linear subspace of W.

(b) $(V^{\mathbb{E}})^{\mathbb{E}} = V^{\mathbb{E}}$.

(c) $V^{\mathbb{E}} = V$ if and only if $\mathbb{E} \subseteq \mathbb{M}$. In particular, $V^{\mathbb{M}} = V$.

Proof. (a) Clear.

(b) By (a), we have $(V^{\mathbb{E}})^{\mathbb{E}} \subseteq V^{\mathbb{E}}$. For every $v' \in V^{\mathbb{E}}$, we have $\mu(\epsilon \cdot v') = (\mu\epsilon) \cdot v' \in V$ for all $\mu, \epsilon \in \mathbb{E}$. This implies $\epsilon \cdot v' \in V^{\mathbb{E}}$ for all $\epsilon \in \mathbb{E}$. Hence $v' \in (V^{\mathbb{E}})^{\mathbb{E}}$ and therefore $V^{\mathbb{E}} \subseteq (V^{\mathbb{E}})^{\mathbb{E}}$.

(c) This is Lemma $7D$ from [15]. We will prove a more general result for decomposable forms. □

Recall that

$$\alpha(F) = \max_{\emptyset \neq S \subsetneq \{1,\ldots,d\}} \frac{|S|}{r(S)} = \max_{\emptyset \neq S \subsetneq \{1,\ldots,d\}} \frac{1}{q(S)}.$$

Now we formulate our criterion for $a(F)$.

Lemma 3.1.7. *Let $F = c \cdot N_{\mathbb{K}/\mathbb{Q}}(w_1X_1 + \cdots + w_nX_n) \in \mathbb{Z}[X]$ be a norm form of degree d such that $F(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Q}^n \setminus \{0\}$. Let $t \geq 2$ be a integer. Then the following statements are equivalent:*

(a) $a(F) < d/n$.

(b) For every subfield $\mathbb{M}$ with $\mathbb{Q} \subsetneq \mathbb{M} \subseteq \mathbb{K}$, we have $V^{\mathbb{M}} \subsetneq V$.

Proof.

$$\begin{aligned} a(F) < d/n &\iff q(S) > n/d \text{ for every non-empty } S \subsetneq \{1, \dots, d\}, \\ &\iff \{1, \dots, d\} \text{ is an extremal subset (By Remark 3.1.2[(b)]),} \\ &\iff \text{there does not exist an extremal subset } S \text{ with } 1 \in S \text{ and } |S| = d/t, \\ &\iff V^{\mathbb{M}} \subsetneq V \text{ for every subfield } \mathbb{M} \text{ with } \mathbb{Q} \subsetneq \mathbb{M} \subseteq \mathbb{K} \text{ (By Lemma 3.1.6[(c)]).} \end{aligned}$$

□

For a linear subspace T of $\mathbb{Q}^n$ (possibly $\mathbb{Q}^n$ itself), we define

$$V^T = \{x_1w_1 + \cdots + x_nw_n : (x_1, \dots, x_n) \in T\}.$$

We apply Lemma 3.1.7 to obtain the following criterion.

Lemma 3.1.8. *The following are equivalent:*

(a) $a(F|_T) < d/\dim T$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$,

(b) $(V^T)^{\mathbb{E}} \subsetneq V^T$ for every subfield $\mathbb{E}$ with $\mathbb{Q} \subsetneq \mathbb{E} \subseteq \mathbb{K}$ and every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$,

(c) $V^{\mathbb{E}} = \{0\}$ for every $\mathbb{Q} \subsetneq \mathbb{E} \subseteq \mathbb{K}$.

Proof. We only have to show that (b) and (c) are equivalent.

$(b) \Rightarrow (c)$ Assume that there is a subfield $\mathbb{E}_0$ with $\mathbb{Q} \subsetneq \mathbb{E}_0 \subseteq \mathbb{K}$, $V^{\mathbb{E}_0} \neq \{0\}$. Then either $V^{\mathbb{E}_0} = V$ or $V^{\mathbb{E}_0} = V^{T_0} \subsetneq V$ for some non-zero linear subspace T_0 of $\mathbb{Q}^n$. Now by Lemma 3.1.6 we have

$$(V^{T_0})^{\mathbb{E}_0} = (V^{\mathbb{E}_0})^{\mathbb{E}_0} = V^{\mathbb{E}_0} = V^{T_0},$$

contradicting (b).

$(c) \Rightarrow (b)$ Assume that $(V^{T_1})^{\mathbb{E}_1} = V^{T_1} \neq \{0\}$ for some subfield $\mathbb{E}_1$ with $\mathbb{Q} \subsetneq \mathbb{E}_1 \subseteq \mathbb{K}$ and some linear subspace T_1 of $\mathbb{Q}^n$. It is clear that $(V^{T_1})^{\mathbb{E}_1} \subseteq V^{\mathbb{E}_1}$, hence $V^{\mathbb{E}_1} \neq \{0\}$. $\square$

3.2 Finite étale algebras

In this section, we have collected some basic facts about finite étale algebras.

A *finite étale* $\mathbb{Q}$*-algebra* is a $\mathbb{Q}$-algebra that is isomorphic to a direct product of finitely many algebraic number fields. Let $\mathbb{K}_1, \ldots, \mathbb{K}_q$ be algebraic number fields and Ω their direct product, i.e.

$$\Omega = \mathbb{K}_1 \times \cdots \times \mathbb{K}_q = \{(a_1, \ldots, a_q) : a_i \in \mathbb{K}_i \text{ for } i = 1, \ldots, q\}$$

endowed with coordinatewise addition and multiplication.

Let $\mathbb{L}$ be the normal closure of the compositum $\mathbb{K}_1 \ldots \mathbb{K}_q$.

For $i = 1, \ldots, q$, let $d_i := [\mathbb{K}_i : \mathbb{Q}]$ and $\sigma_{i1}, \ldots, \sigma_{id_i}$ the embeddings of $\mathbb{K}_i$ in $\mathbb{L}$. Let $d := d_1 + \cdots + d_q = \dim_{\mathbb{Q}} \Omega$. In this way, we get d $\mathbb{Q}$-algebra homomorphisms

$$\mathbf{a} = (a_1, \ldots, a_q) \rightarrow \sigma_{ij}(a_j) : \Omega \rightarrow \mathbb{L} \quad (i = 1, \ldots, q, j = 1, \ldots, d_i).$$

We denote these homomorphisms by $\sigma_1, \ldots, \sigma_d$ and write $\mathbf{a}^{(i)}$ for $\sigma_i(\mathbf{a})$.

Let $G := \text{Gal}(\mathbb{L}/\mathbb{Q})$. For each $\sigma \in G$ there is a permutation $\hat{\sigma}$ of $\{1, \ldots, d\}$ such that

$$\sigma(\mathbf{a}^{(i)}) = \mathbf{a}^{(\hat{\sigma}(i))} \quad (i = 1, \ldots, q, \sigma \in G, \mathbf{a} \in \Omega).$$

This defines an action of G on the set of indices $\{1, \ldots, d\}$.

For $\sigma \in G$ we define maps $\sigma, \hat{\sigma} : \mathbb{L}^d \rightarrow \mathbb{L}^d$ by

$$\begin{aligned} \sigma(\mathbf{x}) &= (\sigma(x_1), \ldots, \sigma(x_d)) \\ \hat{\sigma}(\mathbf{x}) &= (x_{\hat{\sigma}(1)}, \ldots, x_{\hat{\sigma}(d)}) \qquad \text{for } \mathbf{x} = (x_1, \ldots, x_d) \in \mathbb{L}^d. \end{aligned}$$

Note that for any $\sigma_1, \sigma_2 \in G$, the maps σ_1 and $\hat{\sigma_2}$ commute.

Define

$$\Lambda = \{\mathbf{x} \in \mathbb{L}^d : \sigma(\mathbf{x}) = \hat{\sigma}(\mathbf{x}) \text{ for } \sigma \in G\}.$$

Then Λ is a $\mathbb{Q}$-vector space.

Lemma 3.2.1. *Let S be a subset of Λ. Then*

$$\mathit{rank}_{\mathbb{L}}(S) = \mathit{rank}_{\mathbb{Q}}(S).$$

Proof. Clearly, $\mathrm{rank}_{\mathbb{L}}(S) \leq \mathrm{rank}_{\mathbb{Q}}(S)$.

Assume $\mathrm{rank}_{\mathbb{L}}(S) < \mathrm{rank}_{\mathbb{Q}}(S) = r$. Then there are $\mathbb{Q}$-linearly independent elements $\mathbf{a}_1, \ldots, \mathbf{a}_r$ in S such that

$$\lambda_1 \mathbf{a}_1 + \cdots + \lambda_r \mathbf{a}_r = 0 \text{ with } (\lambda_1, \ldots, \lambda_r) \in \mathbb{L}^r \setminus \{0\}.$$

Without loss of generality, assume $\lambda_1 = 1$. Then for each $\sigma \in G$, we have

$$\sum_{i=1}^{r} \sigma(\lambda_i)\hat{\sigma}(\mathbf{a}_i) = \sigma(\sum_{i=1}^{r} \lambda_i \mathbf{a}_i) = 0$$

which after permuting coordinates gives $\sum_{i=1}^{r} \sigma(\lambda_i)\mathbf{a}_i = 0$. Hence

$$\sum_{i=1}^{r} \Big(\sum_{\sigma \in G} \sigma(\lambda_i) \Big) \mathbf{a}_i = \sum_{\sigma \in G} \sum_{i=1}^{r} \sigma(\lambda_i)\mathbf{a}_i = 0$$

with $\sum_{\sigma \in G} \sigma(\lambda_i) \in \mathbb{Q}$ and $\sum_{\sigma \in G} \sigma(\lambda_1) = |G| \neq 0$. This contradicts the linear independence of $\mathbf{a}_1, \ldots, \mathbf{a}_r$ over $\mathbb{Q}$. □

Define the map

$$\Phi : \Omega \to \mathbb{L}^d, \mathbf{a} \to (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(d)}).$$

If we endow $\mathbb{L}^d$ with coordinatewise multiplication, Φ becomes an injective $\mathbb{Q}$-algebra homomorphism.

Corollary 3.2.2. *We have*

$$\Phi(\Omega) = \Lambda.$$

Proof. Clearly $\Phi(\Omega) \subseteq \Lambda$. Further, $\dim_{\mathbb{Q}} \Phi(\Omega) = d$, and by Lemma 3.2.1,

$$\dim_{\mathbb{Q}} \Lambda = \mathrm{rank}_{\mathbb{Q}} \Lambda = \mathrm{rank}_{\mathbb{L}} \Lambda \leq d.$$

Hence $\Phi(\Omega) = \Lambda$. □

Definition 3.2.3. *A subspace W of $\mathbb{L}^d$ is called special if $\hat{\sigma}^{-1}(\sigma(\mathbf{x})) \in W$ for all $\mathbf{x} \in W, \sigma \in G$.*

Lemma 3.2.4. *Let W be an $\mathbb{L}$-linear subspace of $\mathbb{L}^d$. Then W is special $\iff$ W is generated by $W \cap \Lambda$. Further in this case, we have $\dim_{\mathbb{L}} W = \dim_{\mathbb{Q}} W \cap \Lambda$.*

Proof. For the first implication, let $\mathbf{a}_1, \ldots, \mathbf{a}_r$ be a $\mathbb{Q}$-basis of $W \cap \Lambda$. Let $\mathbf{x} \in W$ and write $\mathbf{x} = \sum_{i=1}^r \lambda_i \mathbf{a}_i$ with $\lambda_i \in \mathbb{L}$ for $i = 1, \ldots, r$. Then

$$\hat{\sigma}^{-1}(\sigma(\mathbf{x})) = \sum_{i=1}^{r} \sigma(\lambda_i)\hat{\sigma}^{-1}(\sigma(\mathbf{a}_i)) = \sum_{i=1}^{r} \sigma(\lambda_i)\mathbf{a}_i \in W \text{ for } \sigma \in G.$$

So W is special. Further, in that case we have by Lemma 3.2.1

$$\dim_{\mathbb{L}} W = \text{ rank }_{\mathbb{L}} W \cap \Lambda = \dim_{\mathbb{Q}} W \cap \Lambda.$$

For the second implication, assume W is special. Let $[\mathbb{L} : \mathbb{Q}] = m$ and take a $\mathbb{Q}$-basis $\{w_1, \ldots, w_m\}$ of $\mathbb{L}$. Write $G = \{\sigma_1, \ldots, \sigma_m\}$. Let $\mathbf{x} \in W$ and put

$$\mathbf{y}_i = \sum_{j=1}^{m} \sigma_j(w_i)\hat{\sigma}_j^{-1}(\sigma_j(\mathbf{x})) \quad \text{for } i = 1, \ldots, m.$$

Then for $\sigma \in G, i = 1, \ldots, d$, we have

$$\begin{aligned} \hat{\sigma}^{-1}(\sigma(\mathbf{y}_i)) &= \sum_{j=1}^{m} \sigma\sigma_j(w_i)\hat{\sigma}^{-1}\sigma\hat{\sigma}_j^{-1}\sigma_j(\mathbf{x}) = \sum_{j=1}^{m} \sigma\sigma_j(w_i)\hat{\sigma}^{-1}\hat{\sigma}_j^{-1}\sigma\sigma_j(\mathbf{x}) \\ &= \sum_{j=1}^{m} \sigma\sigma_j(w_i)\widehat{\sigma\sigma}_j^{-1}\sigma\sigma_j(\mathbf{x}) = \mathbf{y}_i, \end{aligned}$$

hence $\mathbf{y}_i \in \Lambda$. Therefore $\mathbf{y}_i \in W \cap \Lambda$.

It is well-known that the matrix $(\sigma_j(w_i))_{1 \le i,j \le m}$ is invertible. Hence $\mathbf{x}$ is an $\mathbb{L}$-linear combination of $\mathbf{y}_1, \ldots, \mathbf{y}_m$. So W is generated by $W \cap \Lambda$. $\square$

For a $\mathbb{Q}$-linear subspace V of Ω, denote by $\overline{V}$ the $\mathbb{L}$-linear subspace of $\mathbb{L}^d$ generated by $\Phi(V)$.

Lemma 3.2.5. *The map $V \mapsto \overline{V}$ defines a bijection between the $\mathbb{Q}$-linear subspaces of Ω and the special $\mathbb{L}$-linear subspaces of $\mathbb{L}^d$, and we have $\dim_{\mathbb{L}}(\overline{V}) = \dim_{\mathbb{Q}} V$.*

Proof. Let W be a special linear subspace of $\mathbb{L}^d$ and put $V := \Phi^{-1}(W \cap \Lambda)$. We show that $W = \overline{V}$. Indeed, $\Phi(V) = W \cap \Lambda$ and, by Lemma 3.2.4, W is generated by $W \cap \Lambda$.

Conversely, let V be a $\mathbb{Q}$-linear subspace of Ω. Clearly, $\overline{V}$ is special as it is generated by a subset of Λ. We show that $\Phi(V) = \overline{V} \cap \Lambda$. Clearly, $\Phi(V) \subseteq \overline{V} \cap \Lambda$. Further by Lemma 3.2.4,

$$\dim_{\mathbb{L}} \overline{V} = \dim_{\mathbb{Q}} \overline{V} \cap \Lambda$$

while by Lemma 3.2.1, $\dim_{\mathbb{L}} \overline{V} = \mathrm{rank}_{\mathbb{L}} \Phi(V) = \dim_{\mathbb{Q}} \Phi(V)$. Hence $\Phi(V) = \overline{V} \cap \Lambda$.

This shows that the maps $V \mapsto \overline{V}, W \mapsto \Phi^{-1}(W \cap \Lambda)$ are each other's inverses and also $\dim_{\mathbb{L}}(\overline{V}) = \dim_{\mathbb{Q}} V$. □

Definition 3.2.6. *Let V be a $\mathbb{Q}$-linear subspace of Ω. Define*

$$V^{\perp} := \{\mathbf{y} = (y_1, \ldots, y_d) \in \mathbb{L}^d : \sum_{i=1}^{d} y_i \mathbf{a}^{(i)} = 0 \textit{ for all } \mathbf{a} \in V\},$$

$$< \mathbf{x}, \mathbf{y} > := \sum_{i=1}^{d} x_i y_i \textit{ for } \mathbf{x} = (x_1, \ldots, x_d), \mathbf{y} = (y_1, \ldots, y_d) \in \mathbb{L}^d.$$

Let W be a $\mathbb{L}$-linear subspace of $\mathbb{L}^d$. Define

$$W^{\perp} := \{\mathbf{x} \in \mathbb{L}^d :< \mathbf{x}, \mathbf{y} >= 0 \textit{ for all } \mathbf{y} \in W\}.$$

Lemma 3.2.7. *(a) Let V be a $\mathbb{Q}$-linear subspace of Ω. Then*

$$V = \{\mathbf{a} \in \Omega : \sum_{i=1}^{d} y_i \mathbf{a}^{(i)} = 0 \textit{ for all } \mathbf{y} \in V^{\perp}\}$$

and $\dim_{\mathbb{L}} V^{\perp} = d - \dim_{\mathbb{Q}} V$.

(b) $V \mapsto V^{\perp}$ defines a bijection from the $\mathbb{Q}$-linear subspaces of Ω to the special linear subspaces of $\mathbb{L}^d$.

Proof. (a) We have

$$\begin{aligned}\overline{V}^{\perp} &= \{\mathbf{y} \in \mathbb{L}^d :< \mathbf{x}, \mathbf{y} >= 0 \ \text{ for all } \mathbf{x} \in \overline{V}\} \\ &= \{\mathbf{y} \in \mathbb{L}^d :< \Phi(\mathbf{a}), \mathbf{y} >= 0 \ \text{ for all } \mathbf{a} \in V\} \\ &= \{\mathbf{y} \in \mathbb{L}^d : \sum_{i=1}^{d} y_i \mathbf{a}^{(i)} = 0 \ \text{ for all } \mathbf{a} \in V\} = V^{\perp}.\end{aligned}$$

Hence

$$\overline{V} = (\overline{V}^{\perp})^{\perp} = \{\mathbf{x} \in \mathbb{L}^d :< \mathbf{x}, \mathbf{y} >= 0 \ \text{ for all } \mathbf{y} \in \overline{V}^{\perp}\}.$$

Then by elementary linear algebra, we know

$$\begin{aligned}V = \Phi^{-1}(\overline{V} \cap \Lambda) &= \{\mathbf{a} \in \Omega :< \Phi(\mathbf{a}), \mathbf{y} >= 0 \ \text{ for all } \mathbf{y} \in \overline{V}^{\perp}\} \\ &= \{\mathbf{a} \in \Omega : \sum_{i=1}^{d} y_i \mathbf{a}^{(i)} = 0 \ \text{ for all } \ y \in V^{\perp}\}.\end{aligned}$$

(b) For a $\mathbb{Q}$-linear subspace V of Ω, by Lemma 3.2.5 we know that $\overline{V}$ is special. It is easy to show that $\overline{V}^{\perp}$ is also special. By (a), we know that $V^{\perp} = \overline{V}^{\perp}$ and hence is special. We also have $(V^{\perp})^{\perp} = (\overline{V}^{\perp})^{\perp} = \overline{V}$ and therefore

$$\Phi^{-1}((V^{\perp})^{\perp} \cap \Lambda) = \Phi^{-1}(\overline{V} \cap \Lambda) = V.$$

Let W be a special $\mathbb{L}$-linear subspace of $\mathbb{L}^d$. Then $W^{\perp}$ is also special. Let $V = \Phi^{-1}(W^{\perp} \cap \Lambda)$. Then since $W^{\perp}$ is generated by $W^{\perp} \cap \Lambda = \Phi(V)$, we have

$$\begin{aligned}V^{\perp} &= \{\mathbf{y} \in \mathbb{L}^d :< \Phi(\mathbf{a}), \mathbf{y} >= 0 \ \text{ for all } \mathbf{a} \in V\} \\ &= \{\mathbf{y} \in \mathbb{L}^d :< \mathbf{x}, \mathbf{y} >= 0 \ \text{ for all } \mathbf{x} \in W^{\perp}\} = W.\end{aligned}$$

□

Definition 3.2.8. *A symmetric partition of* $\{1, \ldots, d\}$ *is a collection* $\mathcal{P} = \{P_1, \ldots, P_t\}$ *of non-empty subsets of* $\{1, \ldots, d\}$ *such that*

$$\begin{aligned}&P_1 \cup \cdots \cup P_t = \{1, \ldots, d\}, \\ &P_i \cap P_j = \emptyset \text{ for each } i, j \in \{1, \ldots, d\} \text{ with } i \neq j, \\ &\hat{\sigma}(P_i) \in \mathcal{P} \text{ for } i = 1, \ldots, t, \sigma \in G.\end{aligned}$$

We say that *a property holds for each pair* $i \overset{\mathcal{P}}{\sim} j$ if it holds for each pair $\{i, j\} \subseteq \{1, \dots, d\}$ such that i, j belong to the same set of $\mathcal{P}$.

For a symmetric partition $\mathcal{P}$, we define the set

$$\Lambda^{\mathcal{P}} := \{\mathbf{x} = (x_1, \dots, x_d) \in \Lambda : x_i = x_j \text{ for each pair } i \overset{\mathcal{P}}{\sim} j\}$$

and put $\Omega^{\mathcal{P}} := \Phi^{-1}(\Lambda^{\mathcal{P}})$. Then $\Lambda^{\mathcal{P}}$ is a $\mathbb{Q}$-subalgebra of Λ and $\Omega^{\mathcal{P}}$ a $\mathbb{Q}$-subalgebra of Ω.

Conversely, we have the following Lemma.

Lemma 3.2.9. *For each $\mathbb{Q}$-subalgebra B of Ω, there is a symmetric partition $\mathcal{P}$ of $\{1, \dots, d\}$ such that $B = \Omega^{\mathcal{P}}$. Further, $\dim_{\mathbb{Q}} B$ is equal to the number of sets in $\mathcal{P}$.*

Proof. For a vector $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{L}^d$, we define $\operatorname{supp}(\mathbf{x}) := \{i : x_i \neq 0\}$. Let B be a $\mathbb{Q}$-subalgebra of Ω. We call a subset P of $\{1, \dots, d\}$ *a minimal set of* $B^{\perp}$ if $P \neq \emptyset$, there is $\mathbf{x} \in B^{\perp}$ with $\operatorname{supp}(\mathbf{x}) = P$ and there is no non-zero $\mathbf{y} \in B^{\perp}$ with $\operatorname{supp}(\mathbf{y}) \subsetneq \operatorname{supp}(\mathbf{x})$. We call $\mathbf{x} \in B^{\perp}$ *minimal vector* if $\operatorname{supp}(\mathbf{x})$ is minimal.

We first observe that $B^{\perp}$ is generated by its minimal vectors. Indeed, let $\mathbf{x} \in B^{\perp}$ be not minimal. Choose a minimal vector $\mathbf{y} \in B^{\perp}$ such that $\operatorname{supp}(\mathbf{y}) \subsetneq \operatorname{supp}(\mathbf{x})$. By multiplying $\mathbf{y}$ with a scalar we can assume that $\mathbf{x}, \mathbf{y}$ have a coordinate in common, then $\operatorname{supp}(\mathbf{x} - \mathbf{y}) \subsetneq \operatorname{supp}(\mathbf{x})$. By induction we can express $\mathbf{x} - \mathbf{y}$ as a sum of minimal vectors.

Next, we show that each minimal set of $B^{\perp}$ has cardinality 2. Let P be a minimal set. Let $\mathbf{y} \in B^{\perp}$ with $\operatorname{supp}(\mathbf{y}) = P$ and take $\mathbf{b} \in B$. Then for every $\mathbf{a} \in B$, we have

$$\sum_{i \in P} y_i \mathbf{b}^{(i)} \mathbf{a}^{(i)} = 0,$$

hence $\Phi(\mathbf{b}) \cdot \mathbf{y} \in B^{\perp}$. Suppose $|P| \geq 3$ and there are $i, j \in P$ with $\mathbf{b}^{(i)} \neq \mathbf{b}^{(j)}$. Then $\Phi(\mathbf{b}) \cdot \mathbf{y} - \mathbf{b}^{(i)}\mathbf{y} \in B^{\perp}$, but $\operatorname{supp}(\Phi(\mathbf{b}) \cdot \mathbf{y} - \mathbf{b}^{(i)}\mathbf{y}) \subsetneq P$. Hence $\Phi(\mathbf{b}) \cdot \mathbf{y} = \mathbf{b}^{(i)}\mathbf{y}$ which implies that all $\mathbf{b}^{(i)}$ ($i \in P$) are equal. This holds for all $\mathbf{b} \in B$, so the minimal sets of $B^{\perp}$ are pairs, and the minimal vectors corresponding to a pair $\{i, j\}$ are multiples of $\mathbf{a}_{ij} = \mathbf{e}_i - \mathbf{e}_j$.

Now define a partition $\mathcal{P} = \{P_1, \dots, P_t\}$ of $\{1, \dots, d\}$ in such a way that i, j belong to the same set of $\mathcal{P}$ if $\{i, j\}$ is a minimal set of $B^{\perp}$. Then $B^{\perp}$ is generated by the vectors

$\mathbf{e}_i - \mathbf{e}_j$ for each minimal set $\{i,j\}$. If follows that

$$B = \{\mathbf{a} \in \Omega : \mathbf{a}^{(i)} = \mathbf{a}^{(j)} \text{ for each pair } i \overset{\mathcal{P}}{\sim} j\} = \Omega^{\mathcal{P}}.$$

Put

$$W = \{\mathbf{x} \in \mathbb{L}^d : x_i = x_j \text{ for all pairs } i \overset{\mathcal{P}}{\sim} j\}.$$

Then W is special, since $\mathcal{P}$ is a symmetric partition. So by Lemma 3.2.4

$$t = \dim_{\mathbb{L}} W = \dim_{\mathbb{Q}} W \cap \Lambda = \dim_{\mathbb{Q}} \Phi^{-1}(W \cap \Lambda) = \dim_{\mathbb{Q}} B.$$

□

3.3 Decomposable forms

In this section, let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Write

$$F = c \cdot \prod_{i=1}^{q} N_{\mathbb{K}_i/\mathbb{Q}}(L_i)$$

where $c \in \mathbb{Q}^*$, $\mathbb{K}_i$ is a number field of degree d_i and $L_i = a_{i1}X_1 + \cdots + a_{in}X_n$ with $\mathbb{Q}(a_{i1}, \ldots, a_{in}) = \mathbb{K}_i$ for $i = 1, \ldots, q$.

Assume $F(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Q}^n \setminus \{0\}$. Then $a_{i1}, \ldots, a_{in}$ are linearly independent over $\mathbb{Q}$ for $i = 1, \ldots, q$.

Let $\mathbb{L}$ be the normal closure of the compositum $\mathbb{K}_1 \cdots \mathbb{K}_q$ and define $G := \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

By writing $N_{\mathbb{K}_i/\mathbb{Q}}(L_i)$ as the product of the conjugates of L_i we obtain

$$F = c \cdot \prod_{i=1}^{q} N_{\mathbb{K}_i/\mathbb{Q}}(L_i) = c \cdot \prod_{i=1}^{d} L^{(i)}$$

where $L^{(i)} \in \mathbb{L}[X_1, \ldots, X_n]$ for $i = 1, \ldots, d$. Then G acts on $\{L^{(1)}, \ldots, L^{(d)}\}$, that is, every $\sigma \in G$ gives a permutation $\hat{\sigma}$ of $\{1, \ldots, d\}$ such that

$$\sigma(L^{(i)}) = L^{(\hat{\sigma}(i))} \ (i = 1, \ldots, d).$$

Definition 3.3.1. *Let I be a non-empty subset of $\{1, \ldots, d\}$. Then we call I (in)dependent if $\{L^{(i)} : i \in I\}$ is linearly (in)dependent over $\mathbb{L}$.*

Denote the rank of $\{L^{(i)} : i \in I\}$ over $\mathbb{L}$ by $r(I)$. Define $q(I) = \frac{r(I)}{|I|}$.

Definition 3.3.2. *A non-empty subset I of $\{1, \ldots, d\}$ is called extremal if*

- *$q(I) \leq q(S)$ for all non-empty $S \subseteq \{1, \ldots, d\}$;*
- *$q(I) < q(S')$ for all non-empty $S' \subsetneq I$.*

Remark 3.3.3. Using the same arguments as Remark 3.1.2 and Lemmas 3.1.3 and 3.1.4, we obtain that

(a) Extremal subsets always exist.

(b) $q(\{1, \ldots, d\}) = d/n$.

(c) If $I_1 \neq I_2$ are two distinct extremal subsets, then $I_1 \cap I_2 = \emptyset$.

(d) If I is an extremal subset, then $\hat{\sigma}(I)$ is also an extremal subset for each $\sigma \in G$.

Lemma 3.3.4. *Let $P_1, \ldots, P_t$ be the extremal subsets of $\{1, \ldots, d\}$ and $\mathcal{P} = \{P_1, \ldots, P_t\}$. Then*

(a) $\mathcal{P}$ is a symmetric partition of $\{1, \ldots, d\}$.

(b) $r(P_1) + \cdots + r(P_t) = n$.

(c) $q(P_i) = n/d$ for $i = 1, \ldots, t$.

Proof. Let $P_1, \ldots, P_t$ be the extremal subsets of $\{1, \ldots, d\}$ and $q(P_1) = \cdots = q(P_t) = q_0$. Let $S = \cup_{i=1}^{t} P_i$. By Remark 3.3.3, we know that $\hat{\sigma}(S) = S$ for every $\sigma \in G$.

Recall that $F = c \cdot \prod_{i=1}^{q} N_{\mathbb{K}_i/\mathbb{Q}}(L_i) = c \cdot \prod_{i=1}^{d} L^{(i)}$. Suppose that $N_{\mathbb{K}_i/\mathbb{Q}}(L_i) = \prod_{j \in T_i} L^{(j)}$. Then if one of the indices $j \in T_i$ belongs to S then T_i is contained in S. We first show that

$$r(T_i) = \text{rank}_{\mathbb{L}}\{L^{(j)} : j \in T_i\} = n \text{ for } i = 1, \ldots, q.$$

Recall that $\{L^{(j)} : j \in T_i\}$ are the conjugates of $L_i = a_{i1}X_1 + \cdots + a_{in}X_n$ and that $a_{i1}, \ldots, a_{in}$ are linearly independent over $\mathbb{Q}$. Hence we can augment $\{a_{i1}, \ldots, a_{in}\}$ to a $\mathbb{Q}$-basis $\{a_{i1}, \ldots, a_{id_i}\}$ of $\mathbb{K}_i$. Let $T_i = \{1, \ldots, d_i\}$. Then

$$\det \begin{pmatrix} a_{i1}^{(1)} \ldots a_{id_i}^{(1)} \\ \vdots \quad\quad \vdots \\ a_{i1}^{(d_i)} \ldots a_{id_i}^{(d_i)} \end{pmatrix} \neq 0$$

So

$$\operatorname{rank} \begin{pmatrix} a_{i1}^{(1)} \ldots a_{in}^{(1)} \\ \vdots \quad\quad \vdots \\ a_{i1}^{(d_i)} \ldots a_{in}^{(d_i)} \end{pmatrix} = n.$$

Hence the set of linear forms $\{L_i^{(k)} = a_{i1}^{(k)}X_1 + \cdots + a_{in}^{(k)}X_n : k = 1, \ldots, d_i\}$ has rank n. So $r(T_i) = n$ for $i = 1, \ldots, q$, which implies $r(S) = n$. Therefore,

$$\frac{n}{d} \leq \frac{r(S)}{|S|} = \frac{r(P_1) + \cdots + r(P_t)}{|P_1| + \cdots + |P_t|} = q_0.$$

But $q_0 \leq q(\{1, \ldots, d\}) = n/d$, so we have $q_0 = n/d$ and $|S| = d$. This implies $(a), (b)$ and (c).

□

Define the finite étale $\mathbb{Q}$-algebra $\Omega = \mathbb{K}_1 \times \cdots \times \mathbb{K}_q$. Let

$$V = \{(L_1(\mathbf{x}), \ldots, L_q(\mathbf{x})) : \mathbf{x} \in \mathbb{Q}^n\}.$$

Then V is a $\mathbb{Q}$-vector space contained in Ω. Since the coefficients of each L_i are linearly independent over $\mathbb{Q}$, we have $\dim_{\mathbb{Q}}(V) = n$.

For $\mathbf{a} = (L_1(\mathbf{x}), \ldots, L_q(\mathbf{x})) \in V$, let $\mathbf{a}^{(i)} = L^{(i)}(\mathbf{x})$. Then

$$V^{\perp} = \{\mathbf{y} = (y_1, \ldots, y_d) \in \mathbb{L}^d : \sum_{i=1}^{d} y_i \mathbf{a}^{(i)} = 0 \text{ for } \mathbf{a} \in V\}$$

and $V^{\perp}$ is an $\mathbb{L}$-linear subspace of $\mathbb{L}^d$.

Lemma 3.3.5. *Let $\mathcal{P} := \{P_1, \ldots, P_t\}$ be a symmetric partition of extremal subsets of $\{1, \ldots, d\}$. Then we have*

$$\sum_{i \in P_j} y_i \mathbf{a}^{(i)} = 0 \quad (j = 1, \ldots, t) \quad \textit{for all} \ \ \mathbf{y} \in V^{\perp}, \mathbf{a} \in V. \tag{3.3.1}$$

Proof. By part (b) of Lemma 3.3.4, we have

$$r(P_1) + \cdots + r(P_t) = n.$$

Let I_j be a maximal independent subset of P_j. So $\{L^{(i)} : i \in I_j\}$ is $\mathbb{L}$-linearly independent and $L^{(i)}$ $(i \in P_j \backslash I_j)$ are linear combinations of $\{L^{(i)} : i \in I_j\}$, for $j = 1, \ldots, t$. Then $\bigcup_{j=1}^{t} \{L^{(i)} : i \in I_j\}$ is $\mathbb{L}$-linearly independent and has cardinality n. Without loss of generality, let $\cup_{j=1}^{r} I_j = \{1, \ldots, n\}$. So $L^{(1)}, \ldots, L^{(n)}$ are $\mathbb{L}$-linearly independent and $L^{(n+1)}, \ldots, L^{(d)}$ are linear combinations of $L^{(1)}, \ldots, L^{(n)}$.

Then for each $i \in P_k \cap \{n+1, \ldots, d\}$ and $k = 1, \ldots, t$, we can write

$$L^{(i)} = \sum_{j \in I_k} a_{ij} L^{(j)} \text{ with } a_{ij} \in \mathbb{L}.$$

Define vectors

$$\mathbf{a}_i = (a_{i1}, \ldots, a_{in}, 0, \ldots, -1, \ldots, 0), \ i = n+1, \ldots, d$$

where -1 is the i-th coordinate of $\mathbf{a}_i$ and $a_{ij} = 0$ if $j \notin I_k$. Then $\{\mathbf{a}_{n+1}, \ldots, \mathbf{a}_d\}$ forms a basis of $V^{\perp}$. Now (3.3.1) is satisfied for $\mathbf{y} \in \{\mathbf{a}_{n+1}, \ldots, \mathbf{a}_d\}$ hence for all $\mathbf{y} \in V^{\perp}$. □

For a symmetric partition $\mathcal{P} := \{P_1, \ldots, P_t\}$ of $\{1, \ldots, d\}$, define

$$\mathcal{B} := \Omega^{\mathcal{P}} = \big\{\mathbf{a} \in \Omega : \mathbf{a}^{(i_1)} = \mathbf{a}^{(i_2)} \text{ if } \{i_1, i_2\} \in P_i \text{ for some } i\big\}.$$

Then $\mathcal{B}$ is a $\mathbb{Q}$-subalgebra of Ω. For every $\mathbf{b} \in \mathcal{B}$ and each $j = 1, \ldots, t$, we know that $\mathbf{b}^{(i)}$ is fixed for all $i \in P_j$. Hence, by (3.3.1) we have

$$\sum_{i \in P_j} y_i \mathbf{b}^{(i)} \mathbf{a}^{(i)} = \mathbf{b}^{(i)} (\sum_{i \in P_j} y_i \mathbf{a}^{(i)}) = 0 \ \ (j = 1, \ldots, t) \text{ for all } \mathbf{y} \in V^{\perp}, \mathbf{a} \in V.$$

Hence $\mathcal{B} \cdot V \subseteq V$. By Lemma 3.2.9, we know that $\dim_{\mathbb{Q}} \mathcal{B} = t$.

Recall that

$$\alpha(F) = \max\{\frac{1}{q(I)} : I \subsetneq \{1, \ldots, d\}, I \neq \emptyset\}.$$

Lemma 3.3.6. *The following statements are equivalent:*

(a) $a(F) \geq \frac{d}{n}$.

(b) There exists a $\mathbb{Q}$*-subalgebra* $\mathcal{B}$ *of* Ω *with* $\dim_{\mathbb{Q}} \mathcal{B} > 1$ *such that* $\mathcal{B} \cdot V \subseteq V$.

Proof. By definition $a(F) \geq \frac{d}{n}$ is equivalent to $\{1, \ldots, d\}$ not being extremal, hence equivalent to that the symmetric partition of extremal subsets of $\{1, \ldots, d\}$ contains $t > 1$ sets. By Lemma 3.2.9, this in turn is equivalent to the existence of a $\mathbb{Q}$-subalgebra $\mathcal{B}$ of Ω with $\dim_{\mathbb{Q}} \mathcal{B} = t > 1$ such that $\mathcal{B} \cdot V \subseteq V$. □

Let T be a subspace of $\mathbb{Q}^n$. Define

$$W := \{L_1(\mathbf{x}), \ldots, L_q(\mathbf{x}) : \mathbf{x} \in T\}.$$

Lemma 3.3.7. *The following are equivalent:*

(a) There exists a subspace T *of dimension at least* 2 *of* $\mathbb{Q}^n$ *such that* $a(F|_T) \geq \frac{d}{\dim T}$.

(b) There exists a $\mathbb{Q}$*-subalgebra* $\mathcal{B}$ *of* Ω *such that* $\dim_{\mathbb{Q}} \mathcal{B} > 1$ *and* $\mathcal{B} \cdot W \subseteq W$.

Proof. Apply Lemma 3.3.6. □

To a $\mathbb{Q}$-subalgebra $\mathcal{B}$ of Ω, we associate $V^{\mathcal{B}} = \{\mathbf{a} \in V : \mathcal{B} \cdot \mathbf{a} \subseteq V\}$. It is easy to show that

$$V^{\mathcal{B}} := \bigcup_{\{W \subseteq V :\ \mathcal{B} \cdot W \subseteq W\}} W.$$

We finally arrive at our effective criterion.

Theorem 3.3.8. *Let* $F \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a decomposable form of degree d. The following statements are equivalent:*

(a) $a(F|_T) < \frac{d}{\dim T}$ *for every linear subspace* T *of dimension at least* 2 *of* $\mathbb{Q}^n$*,*

(b) for every non-trivial $\mathbb{Q}$*-subalgebra* $\mathcal{B}$ *of* Ω *with* $\dim_{\mathbb{Q}} \mathcal{B} > 1$*, we have* $V^{\mathcal{B}} = \{0\}$*.*

Proof. By Lemma 3.3.6 and Lemma 3.3.7, it is enough to show that the assertion

$$V^{\mathcal{B}} = \{0\} \text{ for every } \mathbb{Q}\text{-subalgebra } \mathcal{B} \text{ of } \Omega \text{ with } \dim_{\mathbb{Q}} \mathcal{B} > 1$$

is equivalent to

$$\mathcal{B} \cdot W \subsetneq W \text{ for non-zero } \mathbb{Q}\text{-linear subspace } W \text{ of } V \text{ and}$$
$$\text{every } \mathbb{Q}\text{-subalgebra } \mathcal{B} \text{ of } \Omega \text{ with } \dim_{\mathbb{Q}} \mathcal{B} > 1.$$

If $V^{\mathcal{B}_0} \neq \{0\}$ for some $\mathcal{B}_0$, then either $V^{\mathcal{B}_0} = V$ or $V^{\mathcal{B}_0} = W_0$ for some subspace W_0. Since $\mathcal{B}_0 V^{\mathcal{B}_0} = V^{\mathcal{B}_0}$, we have either $\mathcal{B}_0 V = V$ or $\mathcal{B}_0 W_0 = W_0$.

If $\mathcal{B}_1 \cdot W_1 = W_1 \neq \{0\}$ for some proper linear subspace W_1 of $\mathbb{Q}^n$ and some $\mathbb{Q}$-subalgebra $\mathcal{B}_1$ of Ω with $\dim_{\mathbb{Q}} \mathcal{B}_1 > 1$, then $\{0\} \neq W_1^{\mathcal{B}_1} \subseteq V^{\mathcal{B}_1}$. □

Remark 3.3.9. Criterion (b) can be checked effectively as follows. Let $\mathbf{x}_1, \ldots, \mathbf{x}_d$ be a $\mathbb{Q}$-basis of Ω. The $\mathbb{Q}$-algebra Ω has finitely many $\mathbb{Q}$-subalgebras. Compute a $\mathbb{Q}$-basis for each $\mathbb{Q}$-subalgebra $\mathcal{B}$ of Ω, as $\mathbb{Q}$-linear combinations of $\mathbf{x}_1, \ldots, \mathbf{x}_d$. Given a $\mathbb{Q}$-subalgebra $\mathcal{B}$ with basis $\mathbf{y}_1, \ldots, \mathbf{y}_b$, we have

$$V^{\mathcal{B}} = \{\mathbf{a} \in V : \mathbf{y}_i \cdot \mathbf{a} \in V \text{ for } i = 1, \ldots, b\}.$$

Then it can be checked by straightforward linear algebra whether $V^{\mathcal{B}} = 0$.

Chapter 4

Decomposable form in n variables of degree $n+1$

Recall that Theorem 2.1.4 in Chapter 2 provides an asymptotic formula for the number of solutions of a decomposable form inequality in n variables of degree d. Unfortunately in this formula, the error term depends on the coefficients of F.

A lot of work on removing the dependence of the error term on F has been done by Thunder. We recall some results of his below. The following notation is needed. Consider the inequality

$$|F(\mathbf{x})| \leq m \quad \text{in} \quad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n.$$

Define the discriminant $D(F)$ of a decomposable form $F = aL_1, \ldots, L_d \in \mathbb{Z}[X_1, \ldots, X_n]$ to be

$$D(F) = a^{2\binom{d-1}{n-1}} \prod_{1 \leq i_1 < \cdots < i_n \leq d} \left(\det(\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_n})\right)^2.$$

Put $\mathbb{A}_F(m) = \{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\})$ and $\mathbb{A}_F = \mathbb{A}_F(1)$. Denote the volume of $\mathbb{A}_F$ by $\mu_\infty^n(\mathbb{A}_F)$ and the number of integer solutions in $\mathbb{A}_F(m)$ by $N_F(m)$.

Theorem 4.0.10 (Thunder [18]). *Let $F \in \mathbb{Z}[X, Y]$ be a binary cubic form in two vari-*

ables that is irreducible over $\mathbb{Q}$. Then

$$|N_F(m) - m^{2/3}\mu_\infty^2(\mathbb{A}_F)| \leq 9 + \frac{2008m^{1/2}}{|D(F)|^{1/12}} + 3156m^{1/3} \text{ for all } m \geq 1.$$

Later, Thunder proved a Theorem concerning decomposable forms $F \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree $n+1$ of finite type (hence $D(F) \neq 0$).

Theorem 4.0.11 (Thunder [20])**.**

$$|N_F(m) - m^{n/n+1}\mu_\infty^n(\mathbb{A}_F)| \ll \frac{m^{(n-1)/n}}{|D(F)|^{1/(2n(n+1))}}(1+\log m)^{n-2} + \\ + m^{(n-1)/(n+1)}(1+\log m)^{n-1}.$$

where the implicit constant depends only on n.

The goal of this Chapter is to prove a p-adic generalization of Theorem 4.0.11, removing the dependence on F of the error term in Theorem 2.1.4. Thunder's main idea is to find an equivalent form G of F such that it is possible to give a upper bound for $\mathcal{H}(G)$ in terms of its discriminant $D(F)$. In our proof, we first give the p-adic generalization of this idea.

4.1 Statement of the Theorem

Let $F(\mathbf{X}) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $n+1$. Let $S = \{\infty, p_1, \ldots, p_r\}$ be a finite subset of $M_{\mathbb{Q}}$. We consider the inequality

$$\prod_{p \in S} |F(\mathbf{x})|_p \leq m \text{ in } \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$$
$$\text{with } \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \tag{4.1.1}$$

Recall the notation

$$
\begin{aligned}
&I(F) := \text{ the set of all ordered linearly independent } n\text{-tuples among } \mathbf{L}_1, \dots, \mathbf{L}_d,\\
&a(F) := \max_{(\mathbf{L}_{i_1},\dots,\mathbf{L}_{i_n})\in I(F)} \max_{1\le j\le n-1} \frac{|\{\mathbf{L}_i \in \text{span } \{\mathbf{L}_{i_1},\dots,\mathbf{L}_{i_j}\}\}|}{j},\\
&\mathbb{A}_S^n = \prod_{p\in S} \mathbb{Q}_p^n,\\
&\mathbb{A}_{F,S}(m) := \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m \ , \ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\},\\
&N_{F,S}(m) := \Big|\Big\{\mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |F(\mathbf{x})|_p \le m \ , \ \gcd(x_1, x_2, \dots, x_n, p_1 \cdots p_r) = 1\Big\}\Big|.
\end{aligned}
$$

Recall that μ_∞ is the normalized Lebesgue measure on $\mathbb{R} = \mathbb{Q}_\infty$ such that $\mu_\infty([0,1]) = 1$ and that μ_p is the normalized Haar measure on $\mathbb{Q}_p$ such that $\mu_p(\mathbb{Z}_p) = 1$. Define the product measure $\mu^n = \prod_{p\in S} \mu_p^n$ on $\mathbb{A}_S^n$.

For each $p \in S$, we can decompose F as

$$F = a_p L_{p,1} \cdots L_{p,n+1}$$

where $a_p \in \mathbb{Q}_p^*$ and $\{L_{p,1}, \dots, L_{p,n+1}\}$ are linear forms in $\overline{\mathbb{Q}}_p[X_1, \dots, X_n]$ such that the decomposition is $\mathbb{Q}_p$-symmetric. It means that each element of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ permutes the linear forms $L_{p1}, \dots, L_{p,n+1}$.

For $p \in S$, put $\Delta_p^F = \Delta_{p1} \cdots \Delta_{p,n+1}$ where

$$\Delta_{pi} = \det(\mathbf{L}_{p1}, \cdots, \widehat{\mathbf{L}_{pi}}, \cdots, \mathbf{L}_{p,n+1}) \text{ for } i = 1, \dots, n+1.$$

Then

$$\sum_{j=1}^{n+1} (-1)^j \Delta_{pj} \cdot \mathbf{L}_{pj} = 0. \tag{4.1.2}$$

In what follows, the constants implied by the occurring Vinogradov symbols $\ll$ and $\gg$ will be effectively computable and depend only on n and S. We prove the following Theorem.

Theorem 4.1.1. *Let $F \in \mathbb{Z}[X_1, \dots, X_n]$ be a decomposable form of degree $n+1$. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then we have $D(F) \neq 0$ and*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll \frac{m^{(n-1)/n}(1 + \log m)^{|S|(n+1)}}{(\prod_{p \in S} |D(F)|_p)^{\frac{1}{2n(n+1)}}} + m^{\frac{n-1}{n+1}}(1 + \log m)^{|S|(n-1)}.$$

4.2 About discriminants of decomposable forms

In this section, we collect some facts about discriminants of decomposable forms. We can be more general by letting F vary for each $p \in S$ and $\mathbb{K}$ be a field with char$\mathbb{K} = 0$.

Definition 4.2.1. *Let $F = aL_1, \dots, L_d \in \mathbb{K}[X_1, \dots, X_n]$ be a decomposable form where $a \in \mathbb{K}^*$ and $L_1, \dots, L_d \in \overline{\mathbb{K}}[X_1, \dots, X_n]$ are linear forms. We say that F is in general position if $\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n}) \neq 0$ for each $\{i_1, \dots, i_n\} \subseteq \{1, \dots, d\}$.*

Definition 4.2.2. *The discriminant $D(F)$ of a decomposable form $F = aL_1, \dots, L_d \in \mathbb{K}[X_1, \dots, X_n]$ in general position is defined to be*

$$D(F) = a^{2\binom{d-1}{n-1}} \cdot \prod_{1 \le i_1 < \cdots < i_n \le d} \left(\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})\right)^2.$$

It is easy to check that $D(F)$ is independent of the choice of $a, L_1, \dots, L_d$.

Lemma 4.2.3. *Let $F \in \mathbb{K}[X_1, \dots, X_n]$ be a decomposable form of degree d. Then*

(a) $D(F) \in \mathbb{K}^*$.

(b) $D(\lambda F) = (\lambda)^{2\binom{d-1}{n-1}} D(F)$ *for* $\lambda \in \mathbb{K}^*$.

(c) $D(F_T) = (\det T)^{2\binom{d}{n}} D(F)$ *for* $T \in GL_n(\mathbb{K})$.

Proof. (b) and (c) are straightforward.

(a) For every $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ there is a permutation $\hat{\sigma}$ of $\{1,\ldots,d\}$ such that $\sigma(L_i) = \lambda_i L_{\hat{\sigma}(i)}$ with $\lambda_i \in \overline{\mathbb{K}}^*$ and $\lambda_1 \cdots \lambda_d = 1$. Hence

$$\begin{aligned}\sigma(D(F)) &= a^{2\binom{d-1}{n-1}} \prod_{1\le i_1<\cdots<i_n\le d} (\lambda_{i_1}\cdots\lambda_{i_n})^2 \Big(\det(\mathbf{L}_{\hat{\sigma}(i_1)},\ldots,\mathbf{L}_{\hat{\sigma}(i_n)})\Big)^2 \\ &= (a\lambda_1\cdots\lambda_d)^{2\binom{d-1}{n-1}} \prod_{1\le i_1<\cdots<i_n\le d} \Big(\det(\mathbf{L}_{\hat{\sigma}(i_1)},\ldots,\mathbf{L}_{\hat{\sigma}(i_n)})\Big)^2 \\ &= a^{2\binom{d-1}{n-1}} \prod_{1\le i_1<\cdots<i_n\le d} \Big(\det(\mathbf{L}_{i_1},\ldots,\mathbf{L}_{i_n})\Big)^2 = D(F).\end{aligned}$$

□

Let $(F_p : p \in S)$ be a system of decomposable forms with $F_p \in \mathbb{Q}_p[X_1,\ldots,X_n]$ of degree d. For each $T_p \in GL_n(\mathbb{Q}_p)$, define $(F_p)_{T_p}(\mathbf{X}) = F_p(T_p\mathbf{X})$.

Recall that

$$\mathbb{A}(F_p : p \in S) := \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F_p(\mathbf{x}_p)|_p \le 1\ ,\ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\}.$$

Lemma 4.2.4. *Let $(F_p : p \in S)$ with $F_p \in \mathbb{Q}_p[X_1,\ldots,X_n]$ for $p \in S$ be a system of decomposable forms of degree d in general position. Let $\lambda_p \in \mathbb{Q}_p^*$ and $T_p \in GL_n(\mathbb{Q}_p)$ for $p \in S$. Then*

$$\Big(\prod_{p\in S} |D(\lambda_p F_{T_p})|_p^{\frac{1}{2\binom{d}{n}}}\Big) \cdot \mu^n\big(\mathbb{A}(\lambda_p F_{T_p} : p \in S)\big) = \Big(\prod_{p\in S} |D(F_p)|_p^{\frac{1}{2\binom{d}{n}}}\Big) \cdot \mu^n\big(\mathbb{A}(F_p : p \in S)\big)$$

(where possibly both sides of the identity are infinite).

Proof. This is a combination of Lemmas 1.3.3, 1.3.4 and 4.2.3. □

Lemma 4.2.5. *For $p \in S$, let $F_p \in \mathbb{Q}_p[X_1,\ldots,X_n]$ be a homogeneous polynomial of degree d. Assume that $|F_p|_p = 1$ for $p \in S_0$. Then*

$$\mu^n\left(\left\{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \prod_{p\in S} |F_p(\mathbf{x}_p)|_p \le 1, |\mathbf{x}_p|_p = 1\ (p \in S_0)\right\}\right) =$$

$$\mu_\infty^n\Big(\{(\mathbf{x}_\infty \in \mathbb{R}^n : |F_\infty(\mathbf{x}_\infty)| \le 1\}\Big) \cdot \prod_{p\in S_0}\left(\sum_{r_p=0}^{d-1} p^{r_p n/d} \cdot \mu_p^n\big(\{\mathbf{y}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-r_p}\}\big)\right)$$

Proof. We can express the set under consideration as a disjoint union

$$\coprod_{\mathbf{k}=(k_p)_{p\in S_0}\in(\mathbb{Z}_{\geq 0})^{|S_0|}} \left\{ (\mathbf{x}_p)_{p\in S}\in\mathbb{A}_S^n : \begin{array}{l} |F_\infty(\mathbf{x}_\infty)|\leq \prod_{p\in S_0} p^{k_p} \\ |F_p(\mathbf{x}_p)|_p = p^{-k_p}, |\mathbf{x}_p|_p = 1 \text{ for } p\in S_0 \end{array} \right\}.$$

Thus, the measure to be computed can be expressed as

$$\sum_{\mathbf{k}\in(\mathbb{Z}_{\geq 0})^{|S_0|}} \mu_\infty^n\big(\{\mathbf{x}_\infty\in\mathbb{R}^n : |F_\infty(\mathbf{x}_\infty)|\leq \prod_{p\in S_0} p^{k_p}\}\big)\cdot \prod_{p\in S_0}\mu_p^n\left(\left\{\mathbf{x}_p\in\mathbb{Q}_p^n : \begin{array}{l} |F_p(\mathbf{x}_p)|_p = p^{-k_p} \\ |\mathbf{x}_p|_p = 1 \end{array}\right\}\right)$$

$$= \mu_\infty^n\big(\{\mathbf{x}_\infty\in\mathbb{R}^n : |F_\infty(\mathbf{x}_\infty)|\leq 1\}\big)\cdot\prod_{p\in S_0}\sum_{k_p=0}^\infty (p^{k_p})^{n/d}\mu_p^n\left(\left\{\mathbf{x}_p\in\mathbb{Q}_p^n : \begin{array}{l} |F_p(\mathbf{x}_p)|_p = p^{-k_p} \\ |\mathbf{x}_p|_p = 1 \end{array}\right\}\right)$$

We have to rewrite the sums occurring in the product. Write $k_p = dl_p + r_p$ with $0\leq r_p\leq d-1$. Then

$$\mu_p^n\left(\left\{\mathbf{x}_p\in\mathbb{Q}_p^n : \begin{array}{l} |F_p(\mathbf{x}_p)|_p = p^{-k_p} \\ |\mathbf{x}_p|_p = 1 \end{array}\right\}\right) = p^{-nl_p}\cdot\mu_p^n\left(\left\{\mathbf{y}_p\in\mathbb{Q}_p^n : \begin{array}{l} |F_p(\mathbf{y}_p)|_p = p^{-r_p} \\ |\mathbf{y}_p|_p = p^{l_p} \end{array}\right\}\right).$$

So

$$\begin{aligned} &\sum_{k_p=0}^\infty (p^{k_p})^{n/d}\mu_p^n\left(\left\{\mathbf{x}_p\in\mathbb{Q}_p^n : \ |F_p(\mathbf{x}_p)|_p = p^{-k_p}, |\mathbf{x}_p|_p = 1 \ \right\}\right) \\ &= \sum_{r_p=0}^{d-1}\sum_{l_p=0}^\infty (p^{k_p})^{n/d}p^{-nl_p}\mu_p^n\left(\left\{\mathbf{y}_p\in\mathbb{Q}_p^n : \ |F_p(\mathbf{y}_p)|_p = p^{-r_p}, |\mathbf{y}_p|_p = p^{l_p} \ \right\}\right) \\ &= \sum_{r_p=0}^{d-1} p^{r_pn/d}\mu_p^n\left(\left\{\mathbf{y}_p\in\mathbb{Q}_p^n : \ |F_p(\mathbf{y}_p)|_p = p^{-r_p}, |\mathbf{y}_p|_p \geq 1 \ \right\}\right) \\ &= \sum_{r_p=0}^{d-1} p^{r_pn/d}\mu_p^n\left(\left\{\mathbf{y}_p\in\mathbb{Q}_p^n : \ |F_p(\mathbf{y}_p)|_p = p^{-r_p} \ \right\}\right) \end{aligned}$$

since if $|\mathbf{y}_p|\leq 1/p$ then $|F(\mathbf{y}_p)|_p\leq p^{-d}$ contradicting $|F(\mathbf{y}_p)|_p = p^{-r_p}$. This implies the lemma. ◻

Let $p \in S_0$. Further, let $F \in \mathbb{Q}_p[X_1, \ldots, X_n]$ be a decomposable form of degree $n+1$ with $|F|_p = 1$ and $D(F) \neq 0$. We compare

$$A_{p,r}(F) := \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |F(\mathbf{x}_p)|_p = p^{-r} \right\} \right)$$

with $|D(F)|_p$. Notice that for $T \in \mathrm{GL}_n(\mathbb{Q}_p)$, we have

$$A_{p,r}(F_T) = |\det T|_p^{-1} A_{p,r}(F).$$

We prove the following:

Lemma 4.2.6. $A_{p,r}(F)|D(F)|_p^{\frac{1}{2(n+1)}} \ll 1$ *where the implicit constant is effectively computable and depends only on* n *and* p.

Proof. Let $\mathbb{E}_p$ be the splitting field of F over $\mathbb{Q}_p$. Denote by e the ramification index of $\mathbb{E}_p$. Then e divides $[\mathbb{E}_p : \mathbb{Q}_p]$, so $e \leq (n+1)!$.

We factor F as $F = L_1 \ldots L_{n+1}$ with L_i a linear form in $\mathbb{E}_p[X_1, \ldots, X_n]$.

Let $\delta_i := \det(\mathbf{L}_{i+1}, \ldots, \mathbf{L}_{n+1}, \mathbf{L}_1, \ldots, \mathbf{L}_{i-1})$ and put $L_i' = \delta_i L_i$ for $i = 1, \ldots, n+1$. Then

$$L_1' + \cdots + L_{n+1}' = 0, \tag{4.2.1}$$

$$L_1' \cdots L_{n+1}' = \pm D(F)^{1/2} F, \tag{4.2.2}$$

the coefficients of $L_1', \ldots, L_{n+1}'$ are integral over $\mathbb{Z}_p$, (4.2.3)

$\{L_1', \ldots, L_{n+1}'\}$ is up to sign $\mathrm{Gal}(\mathbb{E}_p/\mathbb{Q}_p)$-symmetric (4.2.4)

(see 1.2.9 for definition).

Only (4.2.3) and (4.2.4) require some explanation. As for (4.2.3), by the ultrametric inequality and Gauss Lemma, we have

$$|\mathbf{L}_i'|_p = |\det(\mathbf{L}_{i+1}, \ldots, \mathbf{L}_{n+1}, \mathbf{L}_1, \ldots, \mathbf{L}_{i-1})|_p |\mathbf{L}_i|_p \leq |F|_p = 1 \ (i = 1, \ldots, n+1).$$

As for (4.2.4), for every $\sigma \in \mathrm{Gal}(\mathbb{E}_p/\mathbb{Q}_p)$ there is a permutation $\hat{\sigma}$ of $\{1, \ldots, n+1\}$ such that $\sigma(L_i') = \lambda_{\sigma,i} L_{\hat{\sigma}(i)}'$ for some $\lambda_{\sigma,i} \in \mathbb{E}_p$, where $\lambda_{\sigma,1} \cdots \lambda_{\sigma,n=1} = 1$. Thus,

$$\sigma_{L_i'} = \det(\lambda_{\sigma,i+1} L_{\hat{\sigma}(i+1)}, \ldots, \lambda_{\sigma,i-1} L_{\hat{\sigma}(i-1)}) \lambda_{\sigma,i} L_{\hat{\sigma}(i)} = \pm L_{\hat{\sigma}(i)} \text{ for } \sigma \in \mathrm{Gal}(\mathbb{E}_p/\mathbb{Q}_p).$$

Let $|D(F)|^{1/2} = p^{-s/e}$. Notice that for $\mathbf{x} \in \mathbb{Q}_p^n$ with $|F_p(\mathbf{x})|_p = p^{-r}$ we have

$$\begin{aligned}\max\{|L'_1(\mathbf{x})|_p, \ldots, |L'_{n+1}(\mathbf{x})|_p\} &\geq |L'_1(\mathbf{x}) \cdots L'_{n+1}(\mathbf{x})|_p^{\frac{1}{n+1}} \\ &= \left(|D(F)|_p^{1/2} F(\mathbf{x})\right)^{\frac{1}{n+1}} = p^{\frac{-(er+s)}{e(n+1)}}.\end{aligned}$$

So in fact,

$$\max\{|L'_1(\mathbf{x})|_p, \ldots, |L'_{n+1}(\mathbf{x})|_p\} = p^{\frac{l-(er+s)}{e(n+1)}} \text{ with } l \in \mathbb{Z}_{\geq 0}. \tag{4.2.5}$$

Further, we may write

$$|L'_i(\mathbf{x})|_p = p^{\frac{l-(er+s)-m_i}{e(n+1)}} \text{ with } m_i \in \mathbb{Z}_{\geq 0} \text{ for } i = 1, \ldots, n+1. \tag{4.2.6}$$

We have collected some properties of the integers $m_1, \ldots, m_{n+1}$:

$$m_1 + \cdots + m_{n+1} = (n+1)l \text{ (by (4.2.2))}, \tag{4.2.7}$$

$$\text{at least two among } m_1, \ldots, m_{n+1} \text{ are 0 (by (4.2.1), (4.2.5))}, \tag{4.2.8}$$

$$m_i = m_j \text{ if there is } \sigma \in \mathrm{Gal}(\mathbb{E}_p/\mathbb{Q}_p) \text{ with } \hat{\sigma}(i) = j. \tag{4.2.9}$$

We consider the set of $\mathbf{x} \in \mathbb{Q}_p^n$ satisfying (4.2.6) for some tuple of integers $\mathbf{m} = (m_1, \ldots, m_{n+1})$ with (4.2.7), (4.2.8) and (4.2.9). Since $\{L'_1, \ldots, L'_{n+1}\}$ is up to sign, a $\mathrm{Gal}(\mathbb{E}_p/\mathbb{Q}_p)$-symmetric system, we have

$$\begin{aligned}&\mu_p^n\left(\left\{\mathbf{x} \in \mathbb{Q}_p^n : |L'_i(\mathbf{x}_p)| = p^{\frac{l-(er+s)-m_i}{e(n+1)}} \text{ for } i = 1, \ldots, n+1\right\}\right) \\ &\leq \mu_p^n\left(\left\{\mathbf{x} \in \mathbb{Q}_p^n : |L'_i(\mathbf{x}_p)| \leq p^{\frac{l-(er+s)-m_i}{e(n+1)}} \text{ for } i = 1, \ldots, n+1\right\}\right) \\ &\ll \min_{1 \leq j \leq n+1} \frac{p^{\frac{nl-n(er+s)-\sum_{i \neq j} m_i}{e(n+1)}}}{|\det(\mathbf{L}_{j+1}, \ldots, \mathbf{L}_{n+1}, \mathbf{L}_1, \ldots, \mathbf{L}_{j-1})|_p} \\ &\ll \frac{p^{\frac{-ns}{e(n+1)}}}{|D(F)|_p^{1/2}} \cdot p^{\frac{-l}{e(n+1)}} = |D(F)|_p^{\frac{-1}{2(n+1)}} \cdot p^{\frac{-l}{e(n+1)}}.\end{aligned}$$

Summing over all $l \in \mathbb{Z}_{\geq 0}$ and all tuples $\mathbf{m}$ with (4.2.7), (4.2.8) and (4.2.9), we get

$$\begin{aligned}
&\mu_p^n(\{\mathbf{x} \in \mathbb{Q}_p^n : |F(\mathbf{x})|_p = p^{-r}\}) \\
&\ll |D(F)|_p^{\frac{-1}{2(n+1)}} \sum_{l=0}^{\infty} \left(\sum_{\mathbf{m} \text{ with } (4.2.7),\ (4.2.8),\ (4.2.9)} 1 \right) p^{\frac{-l}{e(n+1)}} \\
&\ll |D(F)|_p^{\frac{-1}{2(n+1)}} \sum_{l=0}^{\infty} \binom{(n+1)l+n}{n} p^{\frac{-l}{e(n+1)}} \\
&\ll |D(F)|_p^{\frac{-1}{2(n+1)}} \sum_{l=0}^{\infty} \binom{l+n}{n} p^{\frac{-l}{e(n+1)^2}} = \left(1 - p^{\frac{-1}{e(n+1)^2}}\right)^{-(n+1)} |D(F)|_p^{\frac{-1}{2(n+1)}} \\
&\ll |D(F)|_p^{\frac{-1}{2(n+1)}}.
\end{aligned}$$

□

Lemma 4.2.7. *For $p \in S$, let $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ be a decomposable form of degree $n+1$ with $D(F_p) \neq 0$. Assume that $|F_p|_p = 1$ for $p \in S_0$. Then*

$$(\prod_{p \in S} |D(F_p)|_p)^{1/(2(n+1))} \mu^n(\mathbb{A}(F_p : p \in S)) \leq C$$

where C is an effectively computable number depending only on n and S.

Proof. Combine Theorem of Bean and Thunder in [1] (for $p = \infty$) with Lemma 4.2.5 and Lemma 4.2.6 (for $p \in S_0$). □

Remark 4.2.8. This is a p-adic generalization of the result of Bean and Thunder [1] on n-variable decomposable forms of degree $n+1$ with non-zero discriminant. In the case $S = \{\infty\}$, Bean and Thunder [1] proved a more general result: for arbitrary decomposable forms $F \in \mathbb{C}[X_1, \ldots, X_n]$ of degree d, we have

$$|D(F)|^{\frac{(d-n)!n!}{2d!}} \mu_\infty^n(\mathbb{A}_F) \leq C$$

where C is an effectively computable number depending only on n. It is still open to generalize their result in the p-adic setting.

4.3 Auxiliary Lemmas

In this section, let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form in n variables of degree $n+1$ in general position. Assume that $I(F) \neq \emptyset$ and $F(\mathbf{x}) \neq 0$ for $\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}$.

Recall that: we say that two decomposable forms $F, G \in \mathbb{Z}[X_1, \ldots, X_n]$ are S-*equivalent* if there exist $T \in GL(n, \mathbb{Z}_S)$ and $t \in \mathbb{Z}_S^*$ such that $G = t \cdot F_T$. For the definition of $\mathcal{H}(G)$, see 1.1.2.

Lemma 4.3.1. *There exists a decomposable form $G \in \mathbb{Z}[X_1, \ldots, X_n]$ in the S-equivalent class of F such that*

$$\mathcal{H}(G) \leq c_1 \cdot (\prod_{p \in S} |D(G)|_p)^{\frac{2}{n+1}}$$

where c_1 is an effectively computable constant depending only on n and S.

Proof. For $p \in S$, we choose a factorization $F = a_p L_{p,1} \cdots L_{p,n+1}$ where $a_p \in \mathbb{Q}_p^*$ and $\{L_{p,1}, \ldots, L_{p,n+1}\}$ is a $\mathbb{Q}_p$-symmetric system of linear forms.

For $p = \infty$, we assume that

$$\begin{aligned} &\mathbf{L}_{\infty i} \in \mathbb{C}^n \ (i = 1, \ldots, 2r),\ \mathbf{L}_{\infty i} \in \mathbb{R}^n \ (i = 2r+1, \ldots, n+1) \\ &\overline{\mathbf{L}}_{\infty i} = \mathbf{L}_{\infty, i+r} \ (i = 1, \ldots, r). \end{aligned} \tag{4.3.1}$$

If r is even, put

$$\begin{aligned} &\mathbf{M}_{\infty 1} = \mathrm{Re}(\Delta_{\infty 1}\mathbf{L}_{\infty 1}), \mathbf{M}_{\infty 2} = \mathrm{Im}(\Delta_{\infty 1}\mathbf{L}_{\infty 1}), \ldots, \mathbf{M}_{\infty, 2r-1} = \mathrm{Re}(\Delta_{\infty r}\mathbf{L}_{\infty r}), \\ &\mathbf{M}_{\infty, 2r} = \mathrm{Im}(\Delta_{\infty r}\mathbf{L}_{\infty r}),\ \mathbf{M}_{\infty i} = \Delta_{\infty i}\mathbf{L}_{\infty i} \ (i = 2r+1, \ldots, n+1). \\ &\mathbf{M}_{pi} = \Delta_{pi}\mathbf{L}_{pi} \ \ (p \in S_0, i = 1, \ldots, n+1). \end{aligned} \tag{4.3.2}$$

If r is odd, put

$$\begin{aligned} &\mathbf{M}_{\infty 1} = \mathrm{Im}(\Delta_{\infty 1}\mathbf{L}_{\infty 1}), \mathbf{M}_{\infty 2} = \mathrm{Re}(\Delta_{\infty 1}\mathbf{L}_{\infty 1}), \ldots, \mathbf{M}_{\infty, 2r-1} = \mathrm{Im}(\Delta_{\infty r}\mathbf{L}_{\infty r}), \\ &\mathbf{M}_{\infty, 2r} = \mathrm{Re}(\Delta_{\infty r}\mathbf{L}_{\infty r}),\ \mathbf{M}_{\infty i} = \Delta_{\infty i}\mathbf{L}_{\infty i} \ (i = 2r+1, \ldots, n+1), \\ &\mathbf{M}_{pi} = \Delta_{pi}\mathbf{L}_{pi} \ \ (p \in S_0, i = 1, \ldots, n+1). \end{aligned} \tag{4.3.3}$$

With these choices, we have $\mathrm{rank}\{\mathbf{M}_{p2}, \ldots, \mathbf{M}_{p,n+1}\} = n$ for $p \in S$. Consider the following symmetric convex body:

$$\mathcal{C} := \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \begin{array}{l} |M_{\infty i}(\mathbf{x}_\infty)| \leq 1 \quad (i = 2, \ldots, n+1), \\ |M_{pi}(\mathbf{x}_p)|_p \leq 1 \quad (i = 2, \ldots, n+1,\ p \in S_0) \end{array} \right\}.$$

Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of $\mathcal{C}$ with respect to $\mathbb{Z}_S^n$.

By a Theorem of K. Mahler in [11], $\mathbb{Z}_S^n$ has a basis $\{\mathbf{a}_1, \cdots, \mathbf{a}_n\}$ such that

$$\begin{array}{l} |M_{\infty i}(\mathbf{a}_j)| \leq \max\{1, j/2\}\lambda_j \quad \text{for } i = 2, \ldots, n+1,\ j = 1, \ldots, n, \\ |\Delta_{pi} L_{pi}(\mathbf{a}_j)|_p \leq 1 \quad \text{for } i = 2, \ldots, n+1,\ p \in S_0, \quad j = 1, \ldots, n. \end{array}$$

By Lemma 3.3.5 in [4, Chap. 4], there exist a permutation σ of $\{1, \cdots, n\}$ and another basis $\{\mathbf{a}'_1, \cdots, \mathbf{a}'_n\}$ of $\mathbb{Z}_S^n$ such that

$$|M_{\infty,i+1}(\mathbf{a}'_j)| \leq n4^n \min\{\lambda_{\sigma(i)}, \lambda_j\} \quad \text{for } i = 1, \ldots, n, \quad j = 1, \ldots, n. \tag{4.3.4}$$

Further, $\mathbf{a}'_1, \ldots, \mathbf{a}'_n$ are $\mathbb{Z}$-linear combinations of $\mathbf{a}_1, \ldots, \mathbf{a}_n$. As a consequence

$$|M_{p,i+1}(\mathbf{a}'_j)|_p \leq 1 \quad \text{for } i = 1, \ldots, n, \quad p \in S_0, \quad j = 1, \ldots, n. \tag{4.3.5}$$

Denote the matrix with columns $\mathbf{a}'_1, \cdots, \mathbf{a}'_n$ by

$$T := (\mathbf{a}'_1, \cdots, \mathbf{a}'_n). \tag{4.3.6}$$

Write $G = u \cdot F_T$ where $T \in GL_n(\mathbb{Z}_S)$ and $u \in \mathbb{Z}_S^*$ such that G is primitive. Then

$$D(G) = u^{2n} \cdot \det(T)^2 D(F)$$

and hence

$$\prod_{p \in S} |D(G)|_p = \prod_{p \in S} |D(F)|_p = \prod_{p \in S} |a|_p^{2n} |\Delta_p^F|_p^2. \tag{4.3.7}$$

Consider again $\mathcal{C}$. By Lemma 1.2.10 we know that

$$\lambda_1 \cdots \lambda_n \ll \prod_{p \in S} |\det(\mathbf{M}_{p2}, \ldots, \mathbf{M}_{p,n+1})| \ll \prod_{p \in S} |\Delta_p^F|_p \tag{4.3.8}$$

and also

$$\lambda_1 \cdots \lambda_n \gg \prod_{p \in S} |\Delta_p^F|_p. \qquad (4.3.9)$$

We bound λ_1 from below and λ_n from above. There is a non-zero $\mathbf{x} \in \mathbb{Z}_S^n$ such that

$$\begin{array}{l} |M_{\infty,i+1}(\mathbf{x})| \leq \lambda_1 \ \text{ for } i = 1, \ldots, n. \\ |M_{p,i+1}(\mathbf{x})|_p \leq 1 \ \text{ for } i = 1, \ldots, n, \ p \in S_0. \end{array}.$$

By our assumption that $F(\mathbf{x}) \neq 0$ for $\mathbf{x} \in \mathbb{Q}^n \setminus \{0\}$, we have $\prod_{p \in S} |F(\mathbf{x})|_p \geq 1$.

Since

$$|\Delta_{\infty,i+r} L_{\infty,i+r}(\mathbf{x})| = |\Delta_{\infty i} L_{\infty i}(\mathbf{x})| = |M_{\infty,2i-1}(\mathbf{x}) + \sqrt{-1} \cdot M_{\infty,2i}(\mathbf{x})| \ll \lambda_1 \text{ for } i = 2, \ldots, r$$

we have

$$|\Delta_{\infty 1} L_{\infty 1}(\mathbf{x})| \leq \sum_{j=2}^{n+1} |\Delta_{\infty j} L_{\infty j}(\mathbf{x})| \ll \lambda_1,$$

therefore

$$\begin{aligned} \prod_{p \in S} |\Delta_p^F|_p &\leq \prod_{p \in S} |\Delta_p^F F(\mathbf{x})|_p \\ &= \prod_{p \in S} |a_p|_p \cdot \Big(|\Delta_{\infty 1} L_{\infty 1}(\mathbf{x})| \prod_{j=2}^{n+1} |\Delta_{\infty j} L_{\infty j}(\mathbf{x})| \Big) \cdot \prod_{p \in S_0} (|\Delta_{p1} L_{p1}(\mathbf{x})|_p \prod_{j=2}^{n+1} |\Delta_{pj} L_{pj}(\mathbf{x})|_p) \\ &\ll \prod_{p \in S} |a_p|_p \cdot n\lambda_1 \cdot (\lambda_1)^{2r-1} \cdot (\lambda_1)^{n+1-2r} \\ &\ll \prod_{p \in S} |a_p|_p \cdot (\lambda_1)^{n+1}. \end{aligned}$$

This implies

$$\lambda_1 \gg \Big(\frac{\prod_{p \in S} |\Delta_p^F|_p}{\prod_{p \in S} |a_p|_p} \Big)^{\frac{1}{n+1}} \qquad (4.3.10)$$

and

$$\lambda_n \ll \frac{\prod_{p \in S} |\Delta_p^F|_p}{\lambda_1 \cdots \lambda_{n-1}} \leq \frac{\prod_{p \in S} |\Delta_p^F|_p}{\lambda_1^{n-1}} \ll (\prod_{p \in S} |\Delta_p^F|_p)^{\frac{2}{n+1}} (\prod_{p \in S} |a_p|_p)^{\frac{n-1}{n+1}}. \qquad (4.3.11)$$

Since

$$|M_{\infty,i+1}(\mathbf{a}'_j)| \ll \min\{\lambda_{\sigma(i)}, \lambda_j\} \ \text{ for } i = 1,\dots,n, \quad j = 1,\dots,n,$$

we have

$$\begin{aligned} &|M_{\infty 1}(\mathbf{a}'_j)| \le \textstyle\sum_{i=1}^n |M_{\infty,i+1}(\mathbf{a}'_j)| \ll \lambda_j \ \text{ for } j = 1,\dots,n, \\ &|M_{\infty,i+1}(\mathbf{a}'_j)| \ll \lambda_{\sigma(i)} \ \text{ for } i = 1,\dots,n, \ j = 1,\dots,n, \end{aligned}$$

and hence

$$\begin{aligned} &|(M_{\infty 1}(\mathbf{a}'_1),\dots,M_{\infty 1}(\mathbf{a}'_n))|_\infty \ll \lambda_n, \\ &|(M_{\infty,i+1}(\mathbf{a}'_1),\dots,M_{\infty,i+1}(\mathbf{a}'_n))|_\infty \ll \lambda_{\sigma(i)} \ \text{ for } i = 1,\dots,n. \end{aligned}$$

This leads to

$$\begin{aligned} &\prod_{p\in S} |\Delta_p^F|_p \cdot \mathcal{H}(G) = \prod_{p\in S} |a_p|_p \cdot \prod_{p\in S} \Big(\prod_{i=1}^{n+1} \big(|\Delta_{pi} L_{pi}(\mathbf{a}'_1),\dots,\Delta_{pi} L_{pj}(\mathbf{a}'_n)\big)|_p \Big) \\ &\le \prod_{p\in S} |a_p|_p \cdot \prod_{p\in S_0} \prod_{i=1}^{n+1} \max\left\{ |M_{pi}(\mathbf{a}'_1)|_p,\dots,|M_{pi}(\mathbf{a}'_n)|_p \right\} \\ &\quad \cdot \prod_{i=1}^{r} \Big| \sum_{j=1}^n M_{\infty,2i-1}(\mathbf{a}'_j) X_j + \sqrt{-1} \cdot \sum_{j=1}^n M_{\infty,2i}(\mathbf{a}'_j) X_j \Big|_\infty \cdot \sum_{i=2r+1}^{n+1} \Big| \sum_{j=1}^n M_{\infty,i}(\mathbf{a}'_j) X_j \Big|_\infty \\ &\ll \prod_{p\in S} |a_p|_p \cdot \lambda_n^2 \cdot \prod_{i=n-r+2}^{n} \lambda_i^2 \cdot \prod_{j=r+1}^{n-r+1} \lambda_j \\ &\ll \prod_{p\in S} |a_p|_p \cdot \frac{\lambda_n^2 \prod_{i=1}^n \lambda_i^2}{\prod_{i=1}^r \lambda_i^2 \cdot \prod_{i=r+1}^{n-r+1} \lambda_i} \le \prod_{p\in S} |a_p|_p \cdot \frac{\lambda_n^2 \prod_{i=1}^n \lambda_i^2}{\lambda_1^{n+1}} \end{aligned}$$

By (4.3.8), (4.3.10) and (4.3.11), the last expression is at most

$$\ll \prod_{p\in S} |a_p|_p \cdot (\prod_{p\in S} |\Delta_p^F|_p)^{\frac{4}{n+1}} (\prod_{p\in S} |a_p|_p)^{\frac{2n-2}{n+1}} \cdot (\prod_{p\in S} |\Delta_p^F|_p)^2 \cdot \frac{\prod_{p\in S} |a_p|_p}{\prod_{p\in S} |\Delta_p|_p}.$$

Hence we get

$$\mathcal{H}(G) \ll (\prod_{p\in S} |a_p|_p)^{\frac{4n}{n+1}} \cdot (\prod_{p\in S} |\Delta_p|_p)^{\frac{4}{n+1}}$$

and then an application of (4.3.7) completes the proof. □

From now on, we will work with the decomposable form G as in Lemma 4.3.1. Since F, G are $\mathbb{Z}_S$-equivalent, we have $N_{F,S}(m) = N_{G,S}(m)$ and $\mu^n(\mathbb{A}_{F,S}(m)) = \mu^n(\mathbb{A}_{G,S}(m))$ by Lemma 4.2.4. So for proving Theorem 4.1.1, we may as well work with G.

Recall that we have chosen a decomposition $F = a_p L_{p1} \cdots L_{p,n+1}$ for each $p \in S$. These lead to decompositions $G = uF_T = a'_p \cdot L'_{p1} \cdots L'_{p,n+1}$ where $a'_p = ua_p \in \mathbb{Q}_p^*$ and $L'_{pi}(X) = \sum_{j=1}^{n} L_{pi}(\mathbf{a}'_j) X_j$. Note that formula (4.1.2) still holds for G.

Lemma 4.3.2. *Let $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S$ such that $\mathbf{x}_p \neq 0$ for each $p \in S$. Then there is a set of indices $\mathcal{J} := \{j_p \in \{1, .., n+1\} : p \in S\}$ such that*

$$\prod_{p\in S} \frac{\prod_{i\neq j_p} |L'_{pi}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}'_{pi})_{i\neq j_p}|_p} \leq c_2 \cdot \prod_{p\in S} \frac{|G(\mathbf{x}_p)|_p}{|\mathbf{x}_p|_p |D(G)|_p^{1/2(n+1)}}$$

where c_2 is an effectively computable constant depending only on n and S.

Proof. Put $\mathbf{y}_p = T\mathbf{x}_p$ for $p \in S$ where T is given by (4.3.6). Using (4.3.7), it suffices to show that

$$\prod_{p\in S} \frac{\prod_{i\neq j_p} |L_{pi}(\mathbf{y}_p)|_p}{|\det(\mathbf{L}_{pi})_{i\neq j_p}|_p} \ll \prod_{p\in S} \frac{|F(\mathbf{y}_p)|_p}{|T^{-1}\mathbf{y}_p|_p |D(F)|_p^{1/2(n+1)}}. \tag{4.3.12}$$

Define the linear forms $M'_{pi} := M_{pi}T = \sum_{j=1}^{n} M_{pi}(\mathbf{a}'_j) X_j$ $(p \in S, i = 1, \ldots, n+1)$ where the linear forms M_{pi} $(p \in S, i = 1, \ldots, n+1)$ have been defined by (4.3.2). Recall that by our choice of σ and $\mathbf{a}'_1, \ldots, \mathbf{a}'_n$ in (4.3.4), we have

$$\begin{aligned} |\mathbf{M}'_{\infty,i+1}|_\infty &\ll \lambda_{\sigma(i)} \quad (i = 1, \ldots, n), \\ |\mathbf{M}'_{p,i+1}|_p &\ll 1 \quad (p \in S_0, i = 1, \ldots, n). \end{aligned} \tag{4.3.13}$$

Further, by (4.3.9) we have

$$\lambda_1 \ldots \lambda_n \gg\ll \prod_{p\in S} |\det(\mathbf{M}_{p2}, \ldots, \mathbf{M}_{p,n+1})|_p = \prod_{p\in S} |\det(\mathbf{M}'_{p2}, \ldots, \mathbf{M}'_{p,n+1})|_p. \tag{4.3.14}$$

hence

$$\prod_{p\in S} \prod_{i=1}^{n} |\mathbf{M}'_{p,i+1}|_p \ll \prod_{i=1}^{n} \lambda_{\sigma(i)} \ll \prod_{p\in S} |\det(\mathbf{M}'_{p2}, \ldots, \mathbf{M}'_{p,n+1})|_p.$$

On the other hand, by Hadamard's inequality we have

$$\prod_{p\in S} |\det(\mathbf{M}'_{p2}, \mathbf{M}'_{p3}, \ldots, \mathbf{M}'_{p,n+1})|_p \ll \prod_{p\in S}\prod_{i=1}^{n} |\mathbf{M}'_{p,i+1}|_p.$$

So in fact,

$$\prod_{p\in S} |\det(\mathbf{M}'_{p2}, \mathbf{M}'_{p3}, \ldots, \mathbf{M}'_{p,n+1})|_p \gg\ll \prod_{p\in S}\prod_{i=1}^{n} |\mathbf{M}'_{p,i+1}|_p. \tag{4.3.15}$$

By Lemma 2.2.1, there is a set of indices $\{i_p \in \{2, \ldots, n+1\} : p \in S\}$ such that

$$\prod_{p\in S} \frac{|M'_{i_p}(\mathbf{x}_p)|_p}{|\mathbf{M}'_{i_p}|_p} \gg \prod_{p\in S} \frac{|\mathbf{x}_p|_p |\det(\mathbf{M}'_{p2}, \mathbf{M}'_{p3}, \ldots, \mathbf{M}'_{p,n+1})|_p}{\prod_{i=1}^{n} |\mathbf{M}'_{p,i+1}|_p}. \tag{4.3.16}$$

Thus (4.3.15) and (4.3.16) imply

$$\prod_{p\in S} |M_{i_p}(\mathbf{y}_p)|_p = \prod_{p\in S} |M'_{i_p}(\mathbf{x}_p)|_p \gg \prod_{p\in S} |\mathbf{x}_p|_p |\mathbf{M}'_{i_p}|_p = \prod_{p\in S} |T^{-1}\mathbf{y}_p|_p |\mathbf{M}'_{i_p}|_p. \tag{4.3.17}$$

By (4.3.13), we also have

$$\prod_{p\in S} \prod_{\substack{i\neq 1 \\ i+1\neq i_p}}^{n} |\mathbf{M}'_{p,i+1}| \ll \prod_{i=2}^{n} \lambda_{\sigma(i)} \ll \prod_{i=2}^{n} \lambda_i$$

and together with (4.3.14), (4.3.15) this implies

$$\prod_{p\in S} |\mathbf{M}'_{p,i_p}|_p \gg \lambda_1.$$

Together with (4.3.10), this implies

$$\prod_{p\in S} |\mathbf{M}'_{p,i_p}|_p \gg \left(\frac{\prod_{p\in S} |\Delta_p^F|_p}{\prod_{p\in S} |a_p|_p}\right)^{\frac{1}{n+1}}.$$

Inserting this into (4.3.17), we obtain

$$\prod_{p\in S} |M_{i_p}(\mathbf{y}_p)|_p \gg \left(\frac{\prod_{p\in S} |\Delta_p^F|_p}{\prod_{p\in S} |a_p|_p}\right)^{\frac{1}{n+1}} \prod_{p\in S} |T^{-1}\mathbf{y}_p|_p.$$

For each $p \in S$ there is a $j_p \in \{1, \ldots, n+1\}$ such that $|M_{p,i_p}(\mathbf{y}_p)| \leq |\Delta_{p,j_p} L_{p,j_p}(\mathbf{y}_p)|_p$. So we have

$$\prod_{p \in S} |\Delta_{pj_p} L_{pj_p}(\mathbf{y}_p)|_p \gg \left(\frac{\prod_{p \in S} |\Delta_p^F|_p}{\prod_{p \in S} |a_p|_p}\right)^{\frac{1}{n+1}} \prod_{p \in S} |T^{-1}\mathbf{y}_p|_p.$$

By multiplying this on both sides with

$$\prod_{p \in S} (|a_p|_p \prod_{i \neq j_p} |\Delta_{pi} L_{pi}(\mathbf{y}_p)|_p)$$

we get

$$\prod_{p \in S} |\Delta_p^F F(\mathbf{y}_p)|_p \gg \prod_{p \in S} |a_p|_p^{n/(n+1)} \cdot \prod_{p \in S} \frac{\prod_{i \neq j_p} |L_{pi}(\mathbf{y}_p)|_p}{|\det(L_{pi})_{i \neq j_p}|_p} \cdot \prod_{p \in S} |\Delta_p^F|_p^{1+1/(n+1)} \cdot \prod_{p \in S} |T^{-1}\mathbf{y}_p|_p$$

which implies (4.3.12). □

4.4 Proof of Theorem 4.1.1

We separate the proof into two cases: the small discriminant case and the large discriminant case.

4.4.1 The small discriminant case

Assume

$$\prod_{p \in S} |D(G)|_p \leq m^{2(n+1)}.$$

Put

$$B_0 = \frac{m^{\frac{1}{n}}}{(\prod_{p \in S} |D(G)|_p)^{\frac{1}{2n(n+1)}}}.$$

Note that $B_0 \geq 1$.

For $l \in \mathbb{Z}_{\geq 0}$, let

$$B_l = e^l B_0,\ C_l = e \cdot B_l,\ A_l = c_2 \frac{B_0^n}{B^l}$$

where c_2 is the constant from Lemma 4.3.2.

We recall that

$$\mathbb{A}_{G,S}(m,B_0)=\left\{(\mathbf{x}_p)_p\in\mathbb{A}_{G,S}(m):|\mathbf{x}_\infty|_\infty\le B_0\right\}.$$

By Proposition 1.4.6, we have

$$\Big||\mathbb{A}_{G,S}(m,B_0)\cap\mathbb{Z}^n|-\mu^n(\mathbb{A}_{G,S}(m,B_0))\Big|\ll B_0^{n-1}(1+\log(\mathcal{H}(G)B_0))^{(n+1)\cdot|S_0|}. \quad (4.4.1)$$

Now by Lemma 4.3.2, for each $(\mathbf{x}_p)_p\in\mathbb{A}_{G,S}(m)$ with $\mathbf{x}_p\neq 0$ for $p\in S$ and $|\mathbf{x}_\infty|_\infty\ge B_l$, there is a set of indicies $\mathcal{J}:=\{j_p:p\in S\}$ such that

$$\prod_{p\in S}\frac{\prod_{i\neq j_p}|L'_{pi}(\mathbf{x}_p)|_p}{|\det(L'_{pi})_{i\neq j_p}|_p}\le c_2\prod_{p\in S}\frac{|G(\mathbf{x}_p)|_p}{|\mathbf{x}_p|_p|D(G)|_p^{1/2(n+1)}}\le c_2\frac{m}{\|\mathbf{x}_\infty\|\cdot\prod_{p\in S}|D(G)|_p^{1/2(n+1)}}\le c_2\frac{B_0^n}{B_l}=A_l.$$

Note that

$$\begin{aligned}&|S|(n-1)\cdot n^{2|S|}\cdot(\log(\frac{B_lC_l^{n-1}}{n^{n/2}n!\prod_{p\in S_0}(pd)^{nd/2}\cdot A_l}))^{|S|(n-1)-1}\\&\le|S|\cdot n^{2|S|+1}\cdot(\log(B_0e^{2l+(n-1)(l+1)}))^{|S|(n-1)-1}\\&\le|S|\cdot n^{2|S|+1}\cdot(\log B_0+(n+1)(l+1))^{|S|(n-1)-1}\end{aligned}$$

and

$$|S|\cdot n^{2|S|+1}\cdot(\log B_0+(n+1)(l+1))^{|S|(n-1)-1}\ge(n!)^{|S|}.$$

Using Lemma 2.2.12 and counting the possibilities of j_p ($p\in S$), we deduce that for every $l\ge 0$ the set

$$\mathcal{S}_l:=\left\{(\mathbf{x}_p)_p\in\mathbb{A}_S^n:\prod_{p\in S}\frac{\prod_{i\neq j_p}|L'_{pi}(\mathbf{x}_p)|_p}{|\det(L'_{pi})_{i\neq j_p}|_p}\le A_l,\ B_l\le|\mathbf{x}_\infty|_\infty\le C_l\right\}$$

can be covered by at most

$$(n+1)^{|S|}\cdot|S|\cdot n^{2|S|+1}\cdot(\log B_0+(n+1)(l+1))^{|S|(n-1)-1}$$

sets of the form

$$\mathcal{C}:=\{(\mathbf{x}_p)_p\in\mathbb{A}_S^n:|N'_{pi}(\mathbf{x}_p)|_p\le a_{pi},\ i=1,\dots,n,\ p\in S\} \quad (4.4.2)$$

where $N'_{p1}, N'_{p2}, \dots, N'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \dots, X_n]$ with

$$|\det(\mathbf{N}'_{p1}, \mathbf{N}'_{p2}, \dots, \mathbf{N}'_{pn})|_p = 1, \; |\mathbf{N}'_{p1}|_p = \cdots = |\mathbf{N}'_{pn}|_p = 1 \;\text{ for } p \in S$$

and the a_{pi} $(p \in S, i = 1, \dots, n)$ are reals with

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} < \frac{C_l A_l}{B_l} \cdot n^{n/2} n! \prod_{p\in S_0} (pd)^{nd/2} \cdot e^{|S|\cdot(n-1)+1} \ll e^{-l} A_0.$$

Further, Lemma 1.2.5 implies

$$\mu^n(\mathcal{C}) \ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi} \ll e^{-l} A_0.$$

Hence

$$\begin{aligned}\sum_{l=0}^{\infty} \mu^n(\mathcal{S}_l) &\ll \sum_{l=0}^{\infty} (\log B_0 + (n+1)(l+1))^{|S|(n-1)-1} \cdot e^{-l} A_0 \\ &\ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot A_0.\end{aligned}$$

Therefore we have

$$|\mu^n(A_{G,S}(m)) - \mu^n(\mathbb{A}_{G,S}(m, B_0))| \ll \sum_{l=0}^{\infty} \mu^n(\mathcal{S}_l) \ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot A_0$$

and

$$\begin{aligned}&\left|\mu^n(A_{G,S}(m)) - |\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n|\right| \\ &\le \left|\mu^n(A_{G,S}(m)) - \mu^n(\mathbb{A}_{G,S}(m, B_0))\right| + \left||\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n| - \mu^n(\mathbb{A}_{G,S}(m, B_0))\right| \\ &\ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot A_0 + B_0^{n-1}(1 + \log(\mathcal{H}(G) B_0))^{(n+1)\cdot|S_0|} \\ &\ll B_0^{n-1}(1 + \log(\mathcal{H}(G) B_0))^{|S|(n+1)}. \qquad (4.4.3)\end{aligned}$$

We next estimate the cardinality of the set

$$\mathcal{L} := \left\{ \mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |G(\mathbf{x})|_p \le m, |\mathbf{x}|_\infty \ge B_0, |\mathbf{x}|_p = 1 \text{ for } p \in S_0 \right\}.$$

Lemma 4.4.1. *The set $\mathcal{L}$ can be covered by a union of a finite set Ω of cardinality*

$$|\Omega| \ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot B_0^{n-1}$$

and

$$\ll (1 + \log m)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$.

Proof. Similarly as in Lemma 2.4.1, we can estimate the cardinality of Ω by

$$|\Omega| \ll \sum_{l=0}^{\infty} \mu^n(\mathcal{S}_l) \ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot B_0^{n-1}.$$

Let

$$l_0 = [2\log(c_2 \cdot B_0^n)], \quad l_1 = l_0 + [\log(c_1 \cdot m^5)]$$

where c_1 is the constant from Lemma 4.3.1.

Define

$$\mathcal{L}_1 = \{\mathbf{x} \in \mathbb{Z}^n : \prod_{p \in S} |G(\mathbf{x})|_p \leq m, B_0 \leq |\mathbf{x}|_\infty \leq C_{l_1}, |\mathbf{x}|_p = 1 \text{ for } p \in S_0\},$$
$$\mathcal{L}_2 = \{\mathbf{x} \in \mathbb{Z}^n : \prod_{p \in S} |G(\mathbf{x})|_p \leq m, |\mathbf{x}|_\infty \geq C_{l_1}, |\mathbf{x}|_p = 1 \text{ for } p \in S_0\}. \quad (4.4.4)$$

For any $\mathbf{x}$ in $\mathcal{L}_2$ such that $\prod_{p \in S} |G(\mathbf{x})|_p \neq 0$, we have $\prod_{p \in S} |G(\mathbf{x})|_p \geq 1$. Let $\mathbf{x}$ be such a solution and write $\mathbf{x} = g\mathbf{x}'$ with $\mathbf{x}'$ is primitive and $\gcd(g, \prod_{i=1}^r p_i) = 1$. Then

$$m \geq \prod_{p \in S} |G(\mathbf{x})|_p = g^{n+1} \prod_{p \in S} |G(\mathbf{x}')|_p \geq g^{n+1}.$$

Thus $g \leq m^{1/(n+1)}$.

By Lemma 4.3.1 we have

$$\mathcal{H}(G) \leq c_1 \cdot (\prod_{p \in S} |D(G)|_p)^{\frac{2}{n+1}} \leq m^4.$$

Hence $|\mathbf{x}'|_\infty = g^{-1}|\mathbf{x}|_\infty \geq m^{-1/(n+1)}C_{l_1} \geq m^{-1/(n+1)}c_1 \cdot m^5 C_{l_0} \geq \max\{C_{l_0}, \mathcal{H}(G)\}$.

Using Lemma 4.3.2, there is a set of indices $\mathcal{J} := \{j_p : p \in S\}$ such that

$$\prod_{p\in S} \frac{\prod_{i\neq j_p} |L'_{pi}(\mathbf{x}')|_p}{|\det(L'_{i,p})_{i\neq j_p}|_p} \leq c_2 \cdot \frac{B_0^n}{|\mathbf{x}'|_\infty} \leq c_2 \cdot \frac{B_0^n}{|\mathbf{x}'|_\infty^{1/2} C_{l_0}^{1/2}} \leq |\mathbf{x}'|_\infty^{-1/2}. \tag{4.4.5}$$

By Lemma 1.1.6, we may assume that each linear form L'_{pi} occurring here is defined over a number field of degree at most d. So we have

$$[\mathbb{Q}(\mathbf{L}'_{pi}) : \mathbb{Q}] \leq d \text{ and } H_{\mathbb{Q}(\mathbf{L}'_{pi})}(\mathbf{L}'_{pi}) \leq \mathcal{H}(G) \leq |\mathbf{x}'|_\infty$$

where $\mathbb{Q}(\mathbf{L}'_{pi})$ is the extension of $\mathbb{Q}$ generated by the coordinates of $\mathbf{L}'_{pi}$. Therefore we can apply a version of the quantitative Subspace Theorem such as [6, Corollary] which implies that the primitive integer solutions the inequality (4.4.5) with

$$|\mathbf{x}'|_\infty \geq \max\{C_{l_0}, \mathcal{H}(G)\}$$

lie in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$. Taking into account of the number of possible tuples $\{j_p : p \in S\}$, we conclude that the elements of $\mathcal{L}_2$ lie in $\ll 1$ proper subspaces.

A similar estimate as that for $\mu^n(\mathcal{S}_l)$ gives that the elements $\mathbf{x} \in \mathcal{L}_1$ with $B_l \leq |\mathbf{x}|_\infty \leq C_l$ lie in the union of at most

$$(\log B_0 + (n+1)(l+1))^{|S|(n-1)-1}$$

convex sets $\mathcal{C}$ of the form (4.4.2). The set of integer points in each such kind of set $\mathcal{C}$ is contained in a proper linear subspace of $\mathbb{Q}^n$ that is related to $\mathcal{C}$. Hence the solutions $\mathbf{x}$ with $B_0 \leq |\mathbf{x}|_\infty \leq C_{l_1}$ that are not counted in Ω lie in the union of

$$\ll \sum_{l=0}^{l_1} (\log B_0 + (n+1)(l+1))^{|S|(n-1)-1} \ll (\log B_0 + (n+1)(l_1+1))^{|S|(n-1)-1}$$
$$\ll (1 + \log m)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$. □

By Theorem 2.1.3, we know that the number of integral solutions of (4.1.1) in a proper subspace is $\ll m^{\frac{n-1}{n+1}}$. Hence Lemma 4.4.1 implies

$$|\mathcal{L}| \ll (\log B_0 + 1)^{|S|(n-1)-1} \cdot B_0^{n-1} + (1 + \log m)^{|S|(n-1)} m^{(n-1)/(n+1)}. \qquad (4.4.6)$$

Combining (4.4.3) and (4.4.6), we conclude our proof of Theorem 4.0.10 for the small discriminant case.

4.4.2 The large discriminant case

Fix ϵ with $0 < \epsilon < 1$. One may take $\epsilon = n/(n+1)$.

Assume

$$(\prod_{p \in S} |D(G)|_p)^{1-\epsilon} \geq m^2.$$

Then $\prod_{p\in S} |D(G)|_p \geq m^2$.

Choose λ with $0 < \lambda < \epsilon/4$ and let $B_0 = m^{1/(n+1)}/\mathcal{H}(G)^{\lambda}, B_l = d^l B_0, C_l = eB_l$. So $B_0 \leq m^{1/n+1}$.

By Lemma 4.3.2, for every solution $\mathbf{x}$ of inequality (4.1.1) with $|\mathbf{x}|_\infty \geq B_0$, there are indices $\mathcal{J} := (j_p)_{p\in S}$ such that

$$\begin{aligned}
\prod_{p\in S} \frac{\prod_{i\neq j_p} |L'_{pi}(\mathbf{x})|_p}{|\det(L'_{pi})_{i\neq j_p}|_p} &\leq c_2 \prod_{p\in S} \frac{|G(\mathbf{x})|_p}{|\mathbf{x}|_p |D(G)|_p^{1/2(n+1)}} \leq \frac{c_2 m}{|\mathbf{x}|_\infty \cdot \prod_{p\in S} |D(G)|_p^{1/2(n+1)}} \\
&\leq \frac{c_2 m}{B_0 \prod_{p\in S} |D(G)|_p^{\epsilon/2(n+1)}} \\
&\leq \frac{c_2 m^{\frac{n-1}{n+1}} \mathcal{H}(G)^{\lambda}}{\prod_{p\in S} |D(G)|_p^{\epsilon/2(n+1)}} \leq \frac{c_2 m^{\frac{n-1}{n+1}}}{\prod_{p\in S} |D(G)|_p^{\frac{\epsilon-4\lambda}{2(n+1)}}}.
\end{aligned}$$

Let

$$l_1 = \max \left\{ \log(\prod_{p\in S} |D(G)|_p^{\frac{2\lambda}{(n+1)}}) + 2\log(c_2 \cdot m), \log(c_1 \cdot \prod_{p\in S} |D(G)|_p^{\frac{4(1+\lambda)}{2(n+1)}}) \right\}.$$

Then by Lemma 4.3.1,

$$C_{l_1} \geq B_0 \max\{\mathcal{H}(G)^{\lambda}(c_2 \cdot m)^2, \mathcal{H}(G)^{1+\lambda}\} = m^{1/(n+1)} \max\{(c_2 \cdot m)^2, \mathcal{H}(G)\}.$$

Define the sets $\mathcal{L}_1, \mathcal{L}_2$ as in (4.4.4). We first count the cardinality of $\mathcal{L}_2$. Let $\mathbf{x} \in \mathcal{L}_2$. As before, we write $\mathbf{x} = g\mathbf{x}'$ with x' primitive. Then we have

$$g \leq m^{1/(n+1)} \text{ and } |\mathbf{x}'|_\infty \geq \frac{C_{l_1}}{g} \geq \max\{(c_2 \cdot m)^2, \mathcal{H}(G)\}.$$

Again by Lemma 4.3.2, we have

$$\prod_{p \in S} \frac{\prod_{i \neq j_p} |L'_{i,p}(\mathbf{x}')|_p}{|\det(L'_{i,p})_{i \neq j_p}|_p} \leq \frac{c_2 \cdot m}{|\mathbf{x}'|_\infty \prod_{p \in S} |D(G)|_p^{1/2(n+1)}} \leq \frac{c_2 \cdot m}{|\mathbf{x}'|_\infty} < \frac{1}{|\mathbf{x}|_\infty^{1/2}}. \tag{4.4.7}$$

By the p-adic Subspace Theorem, the set of primitive integer solutions of(4.4.7) lies in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$. Taking into account the number of possible tuples $\{j_p : p \in S\}$, the integer solutions of (4.1.1) with $|\mathbf{x}|_\infty \geq C_{l_1}$ lie in $\ll 1$ proper subspaces. By Theorem 2.1.3 each subspace contains $\ll m^{\frac{n-1}{n+1}}$ solutions of (4.1.1), leading to

$$|\mathcal{L}_2| \ll m^{\frac{n-1}{n+1}}. \tag{4.4.8}$$

We next estimate the cardinality of $\mathcal{L}_1$.

Set

$$A = \frac{c_2 \cdot m^{\frac{n-1}{n+1}}}{\prod_{p \in S} |D(G)|_p^{\frac{\epsilon - 4\lambda}{2(n+1)}}}, \quad B = B_0, \quad C = C_{l_1} \text{ and } D = \prod_{p \in S} |D(G)|_p^{\frac{\epsilon - 4\lambda}{2(n+1)(|S|n+1)}}.$$

Using Lemma 2.2.12 and taking into consideration the number of tuples $\{j_p, p \in S\}$, we deduce that $\mathcal{L}_1$ can be covered by at most

$$\begin{aligned} &\ll \left(\log_D \left(\frac{C^n}{n! \prod_{p \in S_0} (pd)^{nd/2} \cdot A} \right) \right)^{|S|n-1} \\ &\ll \left(\frac{n(\log m + l_1)}{(\epsilon/2 - 2\lambda) \log(\prod_{p \in S} |D(G)|_p)} \right)^{|S|n-1} \\ &\ll (\epsilon/2 - 2\lambda)^{-(|S|n-1)} \end{aligned}$$

sets of the form

$$\mathcal{C} := \{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : |N'_{pi}(\mathbf{x}_p)|_p \le a_{pi} \ \text{ for } i = 1, \ldots, n,\ p \in S\}$$

where $N'_{p1}, N'_{p2}, \ldots, N'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$ with

$$|\det(N'_{p1}, N'_{p2}, \ldots, N'_{pn})|_p = 1,\ |N'_{p1}|_p = \cdots = |N'_{pn}|_p = 1,\ p \in S$$

and the a_{pi} are reals with

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} < A \cdot n! \prod_{p\in S_0} (pd)^{nd/2} \cdot D^{|S|\cdot n+1} \ll m^{\frac{n-1}{n+1}}.$$

By Lemma 1.2.5, a convex set $\mathcal{C}$ that contains n linearly independent integral points contains $\ll m^{\frac{n-1}{n+1}}$ integral points. For the other convex sets, the number of elements of $\mathcal{L}_1$ that are contained in a proper subspace is $\ll m^{\frac{n-1}{n+1}}$ and the number of such proper subspaces is $\ll (\epsilon - 4\lambda)^{-(|S|n-1)}$. So we have

$$|\mathcal{L}_1| \ll (\epsilon - 4\lambda)^{-(|S|n-1)} m^{\frac{n-1}{n+1}}. \tag{4.4.9}$$

It remains to bound the cardinality of $\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n$. According to Lemma 4.2.7, for every decomposable form $G \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree $n+1$ with $D(G) \neq 0$, we have

$$(\prod_{p\in S} |D(G)|_p)^{1/2(n+1)} \mu^n(A_{G,S}(1)) \ll 1.$$

By Lemma 1.3.1 $\mu^n(A_{G,S}(m)) = m^{n/(n+1)} \cdot \mu^n(A_{G,S}(1))$, hence

$$\mu^n(A_{G,S}(m)) \ll \frac{m^{n/(n+1)}}{(\prod_{p\in S} |D(G)|_p)^{1/2(n+1)}} \ll \frac{m^{n/(n+1)}}{m^{1/(n+1)}} = m^{\frac{n-1}{n+1}} \ (m \ge 1). \tag{4.4.10}$$

Using Lemma 1.4.6, we have

$$\begin{aligned} &\big||\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n| - \mu^n(\mathbb{A}_{G,S}(m, B_0))\big| \ll (B_0 + 1)^{n-1}(1 + \log(\mathcal{H}(G)B_0))^{(n+1)|S_0|} \\ &\ll m^{\frac{n-1}{n+1}}(1 + \log m)^{(n+1)|S_0|}. \end{aligned}$$

and hence

$$\begin{aligned}
|\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n| &\ll m^{\frac{n-1}{n+1}} (1 + \log m)^{(n+1)|S_0|} + \mu^n(\mathbb{A}_{G,S}(m, B_0)) \\
&\ll m^{\frac{n-1}{n+1}} (1 + \log m)^{(n+1)|S_0|} + \mu^n(A_{G,S}(m)) \\
&\ll m^{\frac{n-1}{n+1}} (1 + \log m)^{(n+1)|S_0|}. \qquad (4.4.11)
\end{aligned}$$

Combining (4.4.8), (4.4.9) and (4.4.11) and choosing appropriately ϵ, λ, we have

$$N_{G,S}(m) \ll |\mathbb{A}_{G,S}(m, B_0) \cap \mathbb{Z}^n| + |\mathcal{L}_1| + |\mathcal{L}_2| \ll m^{\frac{n-1}{n+1}} (1 + \log m)^{(n+1)|S_0|}$$

and therefore

$$|N_{G,S}(m) - \mu^n(A_{G,S}(m))| \ll N_{G,S}(m) + \mu^n(A_{G,S}(m)) \ll m^{\frac{n-1}{n+1}} (1 + \log m)^{(n+1)|S_0|}.$$

Together with the result in 4.4.1, this completes our proof of Theorem 4.1.1.

Chapter 5

Decomposable form inequalities with coprime degree and number of unknowns

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d and put

$$\mathbb{A}_F(m) = \{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\} \text{ and } \mathbb{A}_F = \mathbb{A}_F(1).$$

We denote the volume of $\mathbb{A}_F$ by $\mu_\infty^n(\mathbb{A}_F)$ and the number of integer solutions in $\mathbb{A}_F(m)$ by $N_F(m)$. Thunder proved the following result:

Theorem 5.0.2 (Thunder [22])**.** *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d of finite type. If n and d are relatively prime, then*

$$|N_F(m) - m^{n/d}\mu_\infty^n(\mathbb{A}_F)| \ll m^{n/(d+1/(n-1)^2)}(1 + \log m)^{n-2}$$

where the implicit constant depends only on n and d.

In this chapter, we prove a p-adic generalization of Theorem 5.0.2. We are interested in the solutions to

$$\begin{array}{c} \prod_{p \in S} |F(\mathbf{x})|_p \leq m \;\text{ in }\; \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{with }\; \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1 \end{array} \tag{5.0.1}$$

Recall the notation

$$\mathbb{A}_{F,S}(m) := \Big\{(\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m \ , \ |\mathbf{x}_p|_p = 1 \text{ for } p \in S_0\Big\},$$

$$N_{F,S}(m) := \Big|\Big\{\mathbf{x} \in \mathbb{Z}^n : \prod_{p\in S} |F(\mathbf{x})|_p \le m \ , \ \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1\Big\}\Big|.$$

Theorem 5.0.3. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \ne 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. If n and d are relatively prime, we have*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll m^{n/(d+1/(n-1)^2)}(1 + \log m)^{2d|S|}$$

where the implicit constant depends only on n, d and S.

5.1 Preliminaries

5.1.1 Notation

Let $F = \prod_{i=1}^d L_i \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form with linear forms $L_1, \ldots, L_d$ with coefficients in $\overline{\mathbb{Q}}$. Let $S = \{\infty, p_1, \ldots, p_r\}$ and $S_0 = S \setminus \{\infty\}$.

Denote $(a_p)_{p\in S} \in \prod_{p\in S} \mathbb{Q}_p$ by $\mathbf{a} \in \mathbb{A}_S$. Define $|\mathbf{a}|_S := \prod_{p\in S} |a_p|_p$. For $\mathbf{a} \in \mathbb{A}_S$, denote $(a_pF)_{p\in S}$ by $\mathbf{a} \cdot F$.

Denote $(T_p)_{p\in S} \in \prod_{p\in S} GL_n(\mathbb{Q}_p)$ by $\mathbf{T} \in GL_n(\mathbb{A}_S)$. For $\mathbf{T} \in GL_n(\mathbb{A}_S)$, denote $(F_{T_p})_{p\in S}$ by $F_{\mathbf{T}}$ and define

$$|\det \mathbf{T}|_S := \prod_{p\in S} |\det T_p|_p.$$

Recall the definition of our heights:

$$H_\infty(F) = \textstyle\prod_{i=1}^d |\mathbf{L}_i|_\infty, H_p(F) = \prod_{i=1}^d |\mathbf{L}_i|_p,$$
$$\mathcal{H}(F) = \textstyle\prod_{p\in S} H_p(F).$$

For a system of polynomials $(F_p : p \in S)$ with $F_p \in \mathbb{Q}_p[X_1, \dots, X_n]$, we also define $\mathcal{H}(F_p : p \in S) := \prod_{p \in S} H_p(F_p)$.

Further, we define

$$m_p(F) := \inf \left\{ \frac{H_p(F_{T_p})}{|\det T_p|_p^{d/n}} : T_p \in \mathrm{GL}_n(\mathbb{Q}_p) \right\},$$
$$m(F_p : p \in S) := \prod_{p \in S} m_p(F_p),$$

and for decomposable forms $F \in \mathbb{Z}[X_1, \dots, X_n]$

$$m(F) := \prod_{p \in S} m_p(F).$$

Lemma 5.1.1. *Let $F \in \mathbb{Z}[X_1, \dots, X_n]$ be a decomposable form. Then*

$$m(F) = \inf \left\{ \prod_{p \in S} H_p(F_{T_p}) : \mathbf{T} = (T_p)_{p \in S} \in GL_n(\mathbb{A}_S) \textit{ with } |\det \mathbf{T}|_S = 1 \right\}.$$

Proof. By definition,

$$m(F) = \prod_{p \in S} m_p(F) = \prod_{p \in S} \inf \left\{ \frac{H_p(F_{T_p})}{|\det T_p|_p^{d/n}} : T_p \in GL_n(\mathbb{Q}_p) \right\}$$
$$= \inf \left\{ \prod_{p \in S} \frac{H_p(F_{T_p})}{|\det T_p|_p^{d/n}} : T_p \in GL_n(\mathbb{Q}_p) \text{ for } p \in S \right\}.$$

For $T_p \in \mathrm{GL}_n(\mathbb{Q}_p)$ $(p \in S)$, let

$$T'_\infty = (\prod_{p \in S} |\det T_p|_p)^{-1} T_\infty \text{ and } T'_p = T_p \ (p \in S_0).$$

Then $\prod_{p \in S} |\det T'_p|_p = 1$ and

$$\prod_{p \in S} H_p(F_{T'_p}) = (\prod_{p \in S} |\det T_p|_p)^{-d/n} \cdot \prod_{p \in S} H_p(F_{T_p}).$$

This proves Lemma 5.1.1.

□

5.1.2 Orthogonality in $\mathbb{Q}_p^n$

In this section, we give a p-adic analogy of Gram-Schmidt process. For the convenience of the readers, we give the proofs.

Definition 5.1.2. *We say that* $\mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Q}_p^n$ *are orthogonal if*

$$|x_1\mathbf{a}_1 + \cdots + x_r\mathbf{a}_r|_p = \max\{|x_1|_p|\mathbf{a}_1|_p, \ldots, |x_r|_p|\mathbf{a}_r|_p\} \text{ for all } x_1, \ldots, x_r \in \mathbb{Q}_p.$$

If in addition $|\mathbf{a}_1|_p = \cdots = |\mathbf{a}_r|_p = 1$*, we say that* $\mathbf{a}_1, \ldots, \mathbf{a}_r$ *are orthonormal.*

Let $r \leq n$ and $I_1, \ldots, I_{\binom{n}{r}}$ be the subsets of $\{1, \ldots, n\}$ of cardinality r, ordered lexicographically, i.e., $I_1 = \{1, \ldots, r\}, I_2 = \{1, \ldots, r-1, r+1\}, \ldots, I_{\binom{n}{r}} = \{n-r+1, \ldots, n\}$. Given vectors $\mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Q}_p^n$, we denote by $\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_r$ the vector $\left(A_1, \ldots, A_{\binom{n}{r}}\right)$, where A_i is the subdeterminant of the $n \times r$ matrix $(\mathbf{a}_1, \ldots, \mathbf{a}_r)$ with rows from I_i.

Lemma 5.1.3. *Let* $\mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Q}_p^n$ *be vectors. Then we have*

(a) $|\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_r|_p \leq |\mathbf{a}_1|_p \ldots |\mathbf{a}_r|_p$,

(b) $|\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_r|_p = |\mathbf{a}_1|_p \ldots |\mathbf{a}_r|_p \iff \mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Q}_p^n$ *are orthogonal.*

Proof. (a) Obvious.

(b) Without loss of generality, we may assume that $|\mathbf{a}_1|_p = \cdots = |\mathbf{a}_r|_p = 1$. It is clear that $|\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_r|_p < 1$ if and only if $\mathbf{a}_1, \ldots, \mathbf{a}_r$ are linearly dependent modulo p. This means that there exist $x_1, \ldots, x_r \in \mathbb{Z}_p$ with $\max\{|x_1|_p, \ldots, |x_r|_p\} = 1$ such that $x_1\mathbf{a}_1 + \cdots + x_r\mathbf{a}_r = 0 \mod p$, i.e.

$$|x_1\mathbf{a}_1 + \cdots + x_r\mathbf{a}_r|_p < 1 = \max\{|x_1|_p, \ldots, |x_r|_p\}.$$

Hence $|\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_r|_p < 1 \iff \mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Q}_p^n$ are not orthogonal.

□

Lemma 5.1.4. *Let* V *be a linear subspace of* $\mathbb{Q}_p^n$ *and* $\mathbf{x} \in \mathbb{Q}_p^n, \mathbf{x} \notin V$. *Let* $\mathbf{y} \in V$ *such that* $|\mathbf{x} - \mathbf{y}|_p = \min\{|\mathbf{x} - \mathbf{z}|_p : \mathbf{z} \in V\}$. *Then* $\mathbf{x} - \mathbf{y}$ *is orthogonal to every* $\mathbf{z} \in V$.

Proof. We have to show that

$$|a(\mathbf{x}-\mathbf{y})-b\mathbf{z}|_p = \max\{|a|_p|\mathbf{x}-\mathbf{y}|_p, |b|_p|\mathbf{z}|_p\} \text{ for all } a,b\in\mathbb{Q}_p,\ \mathbf{z}\in V.$$

It suffices to prove this for $a=b=1$.

Clearly, if $|\mathbf{z}|_p > |\mathbf{x}-\mathbf{y}|_p$, then $|(\mathbf{x}-\mathbf{y})+\mathbf{z}|_p = \max\{|\mathbf{x}-\mathbf{y}|_p, |\mathbf{z}|_p\}$.

Suppose that $|\mathbf{z}|_p \leq |\mathbf{x}-\mathbf{y}|_p$. Then $|\mathbf{x}-\mathbf{y}+\mathbf{z}|_p \leq |\mathbf{x}-\mathbf{y}|_p$ by the ultrametric inequality and $|\mathbf{x}-\mathbf{y}|_p \leq |\mathbf{x}-\mathbf{y}+\mathbf{z}|_p$ by assumption. Hence $|(\mathbf{x}-\mathbf{y})+\mathbf{z}|_p = \max\{|\mathbf{x}-\mathbf{y}|_p, |\mathbf{z}|_p\}$. □

Lemma 5.1.5 (Orthogonalization)**.** *Let $\mathbf{b}_1,\dots,\mathbf{b}_r\in\mathbb{Q}_p^n$ be linearly independent. Then there is a lower triangular matrix $T=(\epsilon_{ij})_{i,j=1,\dots,r}$ with $\epsilon_{ij}\in\mathbb{Q}_p$ such that*

$$\mathbf{a}_i = \sum_{j=1}^{i}\epsilon_{ij}\mathbf{b}_i \ (i=1,\dots,r) \qquad \textit{are orthonormal.} \tag{5.1.1}$$

Proof. The proof is by induction on r.

First, let $r=1$. Take $\epsilon_{11}\in\mathbb{Q}_p$ with $|\epsilon_{11}|_p = |\mathbf{b}_1|_p^{-1}$ and let $\mathbf{a}_1=\epsilon_{11}\mathbf{b}_1$.

Second, let $r\geq 2$. Suppose that Lemma 5.1.5 is true for fewer than r vectors. So there are $(\epsilon_{ij})_{i,j=1,\dots,r-1}$ with $\epsilon_{ij}\in\mathbb{Q}_p$ such that (5.1.1) holds for $i=1,\dots,r-1$. We have to find $\mathbf{a}_r$ of the shape $\mathbf{a}_r = \eta_1\mathbf{a}_1+\cdots+\eta_{r-1}\mathbf{a}_{r-1}+\eta_r\mathbf{b}_r$ with $\eta_1,\dots,\eta_r\in\mathbb{Q}_p$ and $\mathbf{a}_1,\dots,\mathbf{a}_r$ orthonormal.

Let $V=\operatorname{span}\{\mathbf{a}_1,\dots,\mathbf{a}_{r-1}\}=\operatorname{span}\{\mathbf{b}_1,\dots,\mathbf{b}_{r-1}\}$. Choose $\mathbf{y}\in V$ such that $|\mathbf{b}_r-\mathbf{y}|_p$ is minimal, then by Lemma 5.1.4, $\mathbf{b}_r-\mathbf{y}$ is orthogonal to every $\mathbf{z}\in V$. Let $\mathbf{c}_r=\mathbf{b}_r-\mathbf{y}$. Choose $\epsilon_{rr}\in\mathbb{Q}_p$ with $|\epsilon_{rr}|_p=|\mathbf{c}_r|_p$ and put $\mathbf{a}_r=\epsilon_{rr}^{-1}\mathbf{c}_r$. Hence $|\mathbf{a}_r|_p=1$.

It remains to prove that $\mathbf{a}_1,\dots,\mathbf{a}_r$ are orthonormal. By construction of $\mathbf{a}_r$, we have

$$|\eta_1\mathbf{a}_1+\cdots+\eta_r\mathbf{a}_r|_p = \max\{|\eta_r|_p|\mathbf{a}_r|_p, |\eta_1\mathbf{a}_1+\cdots+\eta_{r-1}\mathbf{a}_{r-1}|_p\}.$$

By the induction hypothesis, we have $|\eta_1\mathbf{a}_1+\cdots+\eta_{r-1}\mathbf{a}_{r-1}|_p = \max\{|\eta_1|_p|\mathbf{a}_1|_p,\dots,|\eta_{r-1}|_p|\mathbf{a}_{r-1}|_p\}$ and hence

$$|\eta_1\mathbf{a}_1+\cdots+\eta_r\mathbf{a}_r|_p = \max\{|\eta_r|_p|\mathbf{a}_r|_p,\dots,|\eta_r|_p|\mathbf{a}_r|_p\}.$$

□

5.2 Preparations

Lemma 5.2.1. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form. For $\mathbf{a} \in \mathbb{A}_S$ and $\mathbf{T} \in GL_n(\mathbb{A}_S)$, we have*

(a) $H_p(a_p F) = |a_p|_p H_p(F)$ $(p \in S)$ *and* $\mathcal{H}(\mathbf{a} \cdot F) = |\mathbf{a}|_S \mathcal{H}(F)$,

(b) $m_p(a_p F) = |a_p|_p m_p(F)$ $(p \in S)$ *and* $m(\mathbf{a} \cdot F) = \prod_{p \in S} m_p(a_p F) = |\mathbf{a}|_S m(F)$,

(c) $m_p(F_{T_p}) = |\det T_p|_p^{d/n} m_p(F)$ $(p \in S)$ *and* $m(F_{\mathbf{T}}) = \prod_{p \in S} m(F_{T_p}) = |\det \mathbf{T}|_S^{d/n} m(F)$.

Proof. (a) is obvious. (b) follows directly from (a).

For (c), notice that

$$\begin{aligned} m_p(F_{T_p}) &= \inf \left\{ \frac{H_p((F_{T_p})_{S_p})}{|\det S_p|_p^{d/n}} : S_p \in GL_n(\mathbb{Q}_p) \right\} \\ &= \inf \left\{ \frac{H_p(F_{T_p S_p})}{|\det T_p|_p^{-d/n} |\det T_p S_p|_p^{d/n}} : T_p S_p \in GL_n(\mathbb{Q}_p) \right\} \\ &= |\det T_p|_p^{d/n} m_p(F). \end{aligned}$$

□

Recall that for a system of decomposable forms $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ $(p \in S)$, we have defined

$$\mathbb{A}(F_p : p \in S) = \mathbb{A}(F_p : p \in S)(1) := \left\{ (\mathbf{x}_p)_p \in \mathbb{A}_S^n : \prod_{p \in S} |F_p(\mathbf{x}_p)|_p \leq 1, |\mathbf{x}_p|_p = 1 \ (p \in S_0) \right\}.$$

For each $p \in S$, define

$$\mathbb{A}(F_p)(m) := \left\{ (\mathbf{x}_p)_p \in \mathbb{Q}_p^n : |F_p(\mathbf{x}_p)|_p \leq m \right\} \text{ and } \mathbb{A}(F_p) := \mathbb{A}(F_p)(1).$$

Here and below, constants implied by the Vinogradov symbols and constants c, c_i $(i \geq 1)$, c_i^p $(i \geq 1, p \in S)$ depend only on n, d, S and are all effectively computable.

Lemma 5.2.2. *Let $(F_p : p \in S)$ be a system of non-zero decomposable forms with $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ $(p \in S)$. Then we have*

$$\mu^n(\mathbb{A}(F_p : p \in S)) \gg\ll \prod_{p \in S} \mu_p^n(\mathbb{A}(F_p)).$$

Proof. It suffices to show Lemma 5.2.2 for the case $|F_p|_p = 1$ $(p \in S_0)$. Indeed, let $F_p = a_p \cdot G_p$ $(p \in S)$ with $|G_p|_p = 1$ $(p \in S_0)$. First, by Lemma 1.3.4 we have

$$\mu^n(\mathbb{A}(F_p : p \in S)) = \mu^n(\mathbb{A}(a_p G_p : p \in S)) = \left(\prod_{p \in S} |a_p|_p \right)^{-n/d} \cdot \mu^n(\mathbb{A}(G_p : p \in S)).$$

Second, for each $p \in S_0$ we claim that

$$\mu_p^n(\mathbb{A}(F_p)) \gg\ll |a_p|_p^{-n/d} \mu_p^n(\mathbb{A}(G_p)).$$

Then Lemma 5.2.2 for the case $|G_p|_p = 1$ $(p \in S_0)$ implies Lemma 5.2.2.

Now we prove the claim. Let $|a_p|_p = p^{ad+r}$ with $a, r \in \mathbb{Z}, 0 \leq r < d$. We have

$$\begin{aligned}
\mu_p^n(\mathbb{A}(F_p)) &= \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{x}_p)|_p \leq 1 \right\} \right) = \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq |a_p|_p^{-1} \right\} \right) \\
&= \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-ad-r} \right\} \right) \\
&= p^{-an} \cdot \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-r} \right\} \right) \\
&\gg\ll |a_p|_p^{-n/d} \cdot \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-r} \right\} \right),
\end{aligned}$$

where

$$\mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-r} \right\} \right) \leq \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq 1 \right\} \right) = \mu_p^n(\mathbb{A}(G_p))$$

and

$$\begin{aligned}
\mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-r} \right\} \right) &\geq \mu_p^n \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq p^{-d} \right\} \right) \\
&= p^{-n} \mu_p \left(\left\{ \mathbf{x}_p \in \mathbb{Q}_p^n : |G_p(\mathbf{x}_p)|_p \leq 1 \right\} \right) = p^{-n} \mu_p^n(\mathbb{A}(G_p)).
\end{aligned}$$

Hence the claim is true.

Next we show Lemma 5.2.2 assuming $|F_p|_p = 1$ ($p \in S_0$). We start with rewriting $\mu^n(\mathbb{A}(F_p, p \in S))$. We have

$$\mu^n(\mathbb{A}(F_p, p \in S)) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \mu_\infty^n(\{\mathbf{x}_\infty \in \mathbb{R}^n : |F_\infty(\mathbf{x}_\infty)| \leq p_1^{k_1} \dots p_r^{k_r}\}) \times$$
$$\times \prod_{i=1}^{r} \mu_{p_i}^n(\{\mathbf{x}_{p_i} \in \mathbb{Q}_{p_i}^n : |F_{p_i}(\mathbf{x}_{p_i})|_{p_i} = p_i^{-k_i}, |\mathbf{x}_{p_i}|_{p_i} = 1\})$$
$$= \sum_{k_1=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \Big(\mu_\infty^n\big(\mathbb{A}(F_\infty)(p_1^{k_1} \dots p_r^{k_r})\big) \cdot \prod_{i=1}^{r} \mu_{p_i}^n(\{\mathbf{x}_{p_i} \in \mathbb{Q}_{p_i}^n : |F_{p_i}(\mathbf{x}_{p_i})|_{p_i} = p_i^{-k_i}, |\mathbf{x}_{p_i}|_{p_i} = 1\})\Big)$$
$$= \mu_\infty^n(\mathbb{A}(F_\infty)) \sum_{k_1=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \Big((p_1^{k_1} \dots p_r^{k_r})^{n/d} \cdot \prod_{i=1}^{r} \mu_{p_i}^n(\{\mathbf{x}_{p_i} \in \mathbb{Q}_{p_i}^n : |F_{p_i}(\mathbf{x}_{p_i})|_{p_i} = p_i^{-k_i}, |\mathbf{x}_{p_i}|_{p_i} = 1\})\Big)$$
$$= \mu_\infty^n(\mathbb{A}(F_\infty)) \prod_{i=1}^{r} \Big(\sum_{k_i=0}^{\infty} p_i^{\frac{k_i n}{d}} \mu_{p_i}^n(\{\mathbf{x}_{p_i} \in \mathbb{Q}_{p_i}^n : |F_{p_i}(\mathbf{x}_{p_i})|_{p_i} = p_i^{-k_i}, |\mathbf{x}_{p_i}|_{p_i} = 1\})\Big)$$
$$= \mu_\infty^n(\mathbb{A}(F_\infty)) \prod_{i=1}^{r} C(F_{p_i})$$

where

$$\mathcal{C}(F_p) := \sum_{k=0}^{\infty} p^{\frac{kn}{d}} \mu_p^n\left(\{\mathbf{x}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{x}_p)|_p = p^{-k}, |\mathbf{x}_p|_p = 1\}\right) \text{ for } p \in S_0.$$

We rewrite $\mathcal{C}(F_p)$. Let $k = td + s$ with $t, s \in \mathbb{Z}, 0 \leq s \leq d-1$ and $\mathbf{y}_p = p^{-t}\mathbf{x}_p$. Then

$$\mathcal{C}(F_p) = \sum_{s=0}^{d-1} p^{\frac{sn}{d}} \Big(\sum_{t=0}^{\infty} p^{tn} \mu_p^n\big(\{\mathbf{x}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{x}_p)|_p = p^{-td-s}, |\mathbf{x}_p|_p = 1\}\big)\Big)$$
$$= \sum_{s=0}^{d-1} p^{\frac{sn}{d}} \Big(\sum_{t=0}^{\infty} \mu_p^n\big(\{\mathbf{y}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-s}, |\mathbf{y}_p|_p = p^t\}\big)\Big)$$
$$= \sum_{s=0}^{d-1} p^{\frac{sn}{d}} \mu_p^n\big(\{\mathbf{y}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-s}\}\big) \qquad (\text{ since if } |\mathbf{y}_p| \leq 1/p, |F_p(\mathbf{y}_p)|_p < p^{-s}).$$

Hence

$$\sum_{s=0}^{d-1} \mu_p^n\big(\{\mathbf{y}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-s}\}\big) \leq \mathcal{C}(F_p) \leq p^{\frac{n(d-1)}{d}} \Big(\sum_{s=0}^{d-1} \mu_p^n\big(\{\mathbf{y}_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-s}\}\big)\Big).$$

Further we have

$$\begin{aligned}\mu_p^n(\mathbb{A}(F_p)) &= \mu_p^n(\{(\mathbf{y}_p)_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p \le 1\}) \\ &= \sum_{s=0}^{d-1}\sum_{t=0}^{\infty} \mu_p^n(\{(\mathbf{y}_p)_p \in \mathbb{Q}_p^n : |F_p(\mathbf{y}_p)|_p = p^{-dt-s}\}) \\ &= \sum_{s=0}^{d-1}\sum_{t=0}^{\infty} p^{-tn}\mu_p^n(\{(\mathbf{z}_p)_p \in \mathbb{Q}_p^n : |F_p(\mathbf{z}_p)|_p = p^{-s}\}) \text{ writing } \mathbf{z}_p = p^{-t}\mathbf{y}_p \\ &= \frac{1}{1-p^{-n}}\Big(\sum_{s=0}^{d-1} \mu_p^n(\{(\mathbf{z}_p)_p \in \mathbb{Q}_p^n : |F_p(\mathbf{z}_p)|_p = p^{-s}\})\Big).\end{aligned}$$

So we have

$$\frac{p^n-1}{p^n}\mu_p^n(\mathbb{A}(F_p)) \le \mathcal{C}(F_p) \le \frac{p^n-1}{p^{n/d}}\mu_p^n(\mathbb{A}(F_p)) \text{ for } p \in S_0.$$

This implies that

$$\prod_{p\in S}\mu_p^n(\mathbb{A}(F_p)) \ll \mu^n(\mathbb{A}(F_p : p \in S)) = \mu_\infty^n(\mathbb{A}(F_\infty))\prod_{p\in S_0}\mathcal{C}(F_p) \ll \prod_{p\in S}\mu_p^n(\mathbb{A}(F_p)).$$

□

Lemma 5.2.3. *Let $F \in \mathbb{Z}[X_1,\dots,X_n]$ be a decomposable form. Suppose that $F(\mathbf{z}) \ne 0$ for all $\mathbf{z} \in \mathbb{Q}^n \setminus \{0\}$. Let $\mathbf{T} \in GL_n(\mathbb{A}_S)$ with $|\det \mathbf{T}|_S = 1$. Then there exists $M \in GL_n(\mathbb{Z}_S)$ with $\mathcal{H}(F_M) \ll \mathcal{H}(F_\mathbf{T})^n$ and*

$$\mathcal{H}(F_\mathbf{T})^{-1/d}\prod_{p\in S}|\mathbf{y}_p|_p \ll \prod_{p\in S}|T_p^{-1}M(\mathbf{y}_p)|_p \ll \mathcal{H}(F_\mathbf{T})^{(n-1)/d}\prod_{p\in S}|\mathbf{y}_p|_p \text{ for } (\mathbf{y}_p)_{p\in s} \in \mathbb{A}_S^n.$$

In particular, $\mathcal{H}(F_\mathbf{T}) \gg 1$.

Remark 5.2.4. This implies $m(F) \gg 1$.

Proof of Lemma 5.2.3. For $\mathbf{T} \in GL_n(\mathbb{A}_S)$ as in Lemma 5.2.3, define

$$\mathcal{C}(\mathbf{T}) := \Big\{(T_p\mathbf{a}_p)_{p\in S} : \mathbf{a}_p = (a_{p1},\dots,a_{pn}) \in \mathbb{Q}_p^n \text{ with } |a_{pi}|_p \le 1 \ (i=1,\dots,n) \text{ for } p \in S\Big\}.$$

We know that $\mathcal{C}(\mathbf{T})$ is a symmetric S-convex body in $\mathbb{A}_S^n$ (see 1.2.7). Let $\lambda_1, \ldots, \lambda_n$ denote its successive minima. By a Theorem of K. Mahler in [11], there is a basis $\{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_n\}$ of $\mathbb{Z}_S^n$ such that:

$$\mathbf{z}_i \in \max\{1, i/2\} \cdot \lambda_i \mathcal{C}(\mathbf{T}) \quad (i = 1, \ldots, n).$$

This means that

$$|T_p^{-1}\mathbf{z}_i|_\infty \le \max\{1, i/2\}\lambda_i \quad (i = 1, \ldots, n)\ ,\ |T_p^{-1}\mathbf{z}_i|_p \le 1 \quad (p \in S_0, i = 1, \ldots, n).$$

Let M be the matrix with columns $\mathbf{z}_1, \ldots, \mathbf{z}_n$. Write

$$T_p^{-1}M = (a_{ij}^p)_{i,j=1,\ldots,n}\ ,\ M^{-1}T_p = (b_{ij}^p)_{i,j=1,\ldots,n}.$$

Then

$$\begin{aligned} &|a_{ij}^\infty| \le j\lambda_j \text{ for } i = 1, \ldots, n, j = 1, \ldots, n, \\ &|a_{ij}^p|_p \le 1 \text{ for } i = 1, \ldots, n, j = 1, \ldots, n, p \in S_0. \end{aligned} \tag{5.2.1}$$

Using Cramer's rule, we have

$$\begin{aligned} |b_{ij}^\infty| &\le \frac{(n-1)!\prod_{l=2}^n l\lambda_l}{|\det T_\infty^{-1}M|} \text{ for } i = 1, \ldots, n, j = 1, \ldots, n, \\ |b_{ij}^p|_p &\le \frac{1}{|\det T_p^{-1}M|_p} \text{ for } i = 1, \ldots, n, j = 1, \ldots, n,\ p \in S_0. \end{aligned}$$

Then, by (5.2.1)

$$\begin{aligned} &|\mathbf{L}_i M|_\infty = |\mathbf{L}_i T_\infty \cdot T_\infty^{-1}M|_\infty \ll \lambda_n |\mathbf{L}_i T_\infty|_\infty \ (i = 1, \ldots, d) \\ &|\mathbf{L}_i M|_p \le |\mathbf{L}_i T_p|_p \ (i = 1, \ldots, d, p \in S_0). \end{aligned}$$

Hence

$$\mathcal{H}(F_M) \ll \lambda_n^d \mathcal{H}(F_{\mathbf{T}}), \tag{5.2.2}$$

while by Lemma 1.1.6 $\mathcal{H}(F_M) \ge 1$.

Let $(\mathbf{y}_p)_{p\in S} \in \mathbb{A}_S^n$ and $\mathbf{u}_p = T_p^{-1}M\mathbf{y}_p$ for $p \in S$. Then we have

$$\begin{aligned} &|T_\infty^{-1}M(\mathbf{y}_\infty)|_\infty \ll \lambda_n |\mathbf{y}_\infty|_\infty,\ |T_p^{-1}M(\mathbf{y}_p)|_p \le |\mathbf{y}_p|_p \ (p \in S_0), \\ &|M^{-1}T_\infty(\mathbf{u}_\infty)|_\infty \ll \frac{\prod_{l=2}^n \lambda_l}{|\det T_\infty^{-1}M|}|\mathbf{u}_\infty|_\infty,\ |M^{-1}T_p(\mathbf{u}_p)|_p \le \frac{1}{|\det T_p^{-1}M|_p}|\mathbf{u}_p|_p \ (p \in S_0), \end{aligned}$$

and thus

$$\prod_{p\in S} |T_p^{-1}M(\mathbf{y}_p)|_p \ll \lambda_n \prod_{p\in S} |\mathbf{y}_p|_p, \tag{5.2.3}$$

$$\begin{aligned}\prod_{p\in S} |\mathbf{y}_p|_p = \prod_{p\in S} |M^{-1}T_p(\mathbf{u}_p)|_p &\ll \frac{\prod_{l=2}^{n} \lambda_l}{\prod_{p\in S} |\det T_p^{-1}M|_p} \prod_{p\in S} |\mathbf{u}_p|_p \\ &\ll \prod_{l=2}^{n} \lambda_l \cdot \prod_{p\in S} |T_p^{-1}M(\mathbf{y}_p)|_p. \end{aligned} \tag{5.2.4}$$

Let $F = L_1 \dots L_d$. For $p \in S$, let $\mathbf{t}_1^p, \dots, \mathbf{t}_n^p$ be the columns of the matrix T_p. Then for every $(T_p\mathbf{a}_p)_{p\in S} \in \mathcal{C}(\mathbf{T})$, we have

$$\begin{aligned}\prod_{p\in S} |F(T_p\mathbf{a}_p)|_p = \prod_{p\in S}\prod_{i=1}^{d} |L_i(T_p\mathbf{a}_p)|_p &= \prod_{p\in S}\prod_{i=1}^{d} |L_i(\mathbf{t}_1^p)\cdot a_{p1} + \cdots + L_i(\mathbf{t}_n^p)\cdot a_{pn}|_p \\ \le n^d \prod_{p\in S}\prod_{i=1}^{d} \max_{j=1,\dots,n} |L_i(\mathbf{t}_j^p)|_p &\le n^d \prod_{p\in S} H_p(F_{T_p}) = \mathcal{H}(F_{\mathbf{T}}) \end{aligned} \tag{5.2.5}$$

and thus

$$\prod_{p\in S} |F(\mathbf{x}_p)|_p \ll \mathcal{H}(F_{\mathbf{T}}) \text{ for all } (\mathbf{x}_p)_{p\in S} \in \mathcal{C}(\mathbf{T}).$$

Since $\mathbf{z}_1 \in \lambda_1\mathcal{C}(\mathbf{T}) \cap \mathbb{Z}_S^n$ and $F(\mathbf{z}_1) \neq 0$, we have

$$1 \le \prod_{p\in S} |F(\mathbf{z}_1)|_p \ll \lambda_1^d \mathcal{H}(F_{\mathbf{T}})$$

and hence

$$\lambda_1 \gg \mathcal{H}(F_{\mathbf{T}})^{-1/d}. \tag{5.2.6}$$

By Lemma 1.2.8, we have

$$\lambda_1 \cdots \lambda_n \ll \prod_{p\in S} |\det T_p^{-1}|_p = 1,$$

implying

$$\lambda_2 \cdots \lambda_n \ll \lambda_1^{-1} \ll \mathcal{H}(F_{\mathbf{T}})^{1/d}\ ,\ \lambda_n \ll \lambda_1^{-(n-1)} \ll \mathcal{H}(F_{\mathbf{T}})^{(n-1)/d}. \tag{5.2.7}$$

Finally, (5.2.2) (5.2.3), (5.2.4), (5.2.6) and (5.2.7) imply the lemma. □

Lemma 5.2.5. *Let $(F_p : p \in S)$ be a system of non-zero decomposable forms with $F_p \in \mathbb{Q}_p[X_1, \dots, X_n]$ $(p \in S)$. Suppose that $\mu^n(\mathbb{A}(F_p : p \in S))$ is finite. Then $m(F_p : p \in S)$ is an attained minimum and $\mu^n(\mathbb{A}(F_p : p \in S)) \gg m(F_p : p \in S)^{-n/d}$.*

Proof. By Lemma 5.2.2, we know that $\mu^n(\mathbb{A}(F_p : p \in S)) \gg \prod_{p\in S} \mu_p^n(\mathbb{A}(F_p))$. For each $p \in S_0$, it is easy to see that $\mu_p^n(\mathbb{A}(F_p)) > 0$. Hence, under the assumption that $\mu^n(\mathbb{A}(F_p, p \in S)) < \infty$, we also have $\mu_\infty^n(\mathbb{A}(F_\infty)) < \infty$. Then by [22, Lemma 2], we know that $m_\infty(F_\infty)$ can be attained. For $p \in S_0$, the numbers $H((F_p)_{T_p})$ $(T_p \in \mathrm{GL}_n(\mathbb{Q}_p))$ form a discrete set of positive reals and hence the minimum $m_p(F_p)$ is attained. Therefore $m(F_p : p \in S) = \prod_{p\in S} m_p(F_p)$ is an attained minimum.

For $\mathbf{T} = (T_p)_{p\in S} \in GL_n(\mathbb{A}_S)$, define

$$\mathcal{C}(\mathbf{T}) := \Big\{(T_p\mathbf{a}_p)_{p\in S} : \mathbf{a}_p = (a_{p1}, \dots, a_{pn}) \in \mathbb{Q}_p^n \text{ with } |a_{pi}|_p \le 1 \ (i = 1, \dots, n) \text{ for } p \in S\Big\},$$
$$\mathcal{C}_p(\mathbf{T}) := \Big\{T_p\mathbf{a}_p : \mathbf{a}_p \in \mathbb{Q}_p^n \text{ with } |a_{pi}|_p \le 1 \ (i = 1, \dots, n)\Big\} \ (p \in S).$$

Then

$$\mu^n(\mathcal{C}(\mathbf{T})) = \prod_{p\in S} \mu_p^n(\mathcal{C}_p(\mathbf{T})) = 2^n |\det \mathbf{T}|_S.$$

Let $F_p = L_{p1} \cdots L_{pd}$ where $L_{p1}, \dots, L_{pd}$ are linear forms in $\overline{\mathbb{Q}}_p[X_1, \dots, X_n]$. For each $p \in S$, let $\mathbf{t}_1^p, \dots, \mathbf{t}_n^p$ be the columns of the matrix T_p. Then by (5.2.5), we have for every $(T_p\mathbf{a}_p)_{p\in S} \in \mathcal{C}(\mathbf{T})$

$$\prod_{p\in S} |F_p(T_p\mathbf{a}_p)|_p \le n^d \prod_{p\in S}\prod_{i=1}^{d} \max_{j=1,\dots,n} |L_{pi}(\mathbf{t}_j^p)|_p \le n^d \prod_{p\in S} H_p((F_p)_{T_p}) = n^d \mathcal{H}((F_p)_{T_p} : p \in S).$$

Choose $\lambda_p \in \overline{\mathbb{Q}}_p^*$ $(p \in S)$ such that $|\lambda_p|_p = n^{d\cdot d(p)} H_p((F_p)_{T_p})$ where $d(\infty) = 1$ and $d(p) = 0$ for $p \in S_0$. Then we have

$$\mu^n\left(\mathbb{A}\left(\frac{(F_p)_{T_p}}{\lambda_p} : p \in S\right)\right) \ge \mu^n(\mathcal{C}(\mathbf{T})) = 2^n |\det \mathbf{T}|_S.$$

Further, by Corollary 1.3.4 we have

$$\mu^n\left(\mathbb{A}\left(\frac{(F_p)_{T_p}}{\lambda_p} : p \in S\right)\right) = \left(\prod_{p\in S} |\lambda|_p^{n/d}\right) \cdot \mu^n(\mathbb{A}(F_p : p \in S)).$$

Therefore

$$\mu^n(\mathbb{A}(F_p : p \in S)) \gg \frac{|\det \mathbf{T}|_S}{\mathcal{H}((F_p)_{T_p} : p \in S)^{n/d}} \text{ for every } (T_p)_{p\in S} \in GL_n(\mathbb{A}_S).$$

Taking the supremum over $\mathbf{T}$ of the right hand side, we get

$$\mu^n(\mathbb{A}(F_p : p \in S)) \gg m(F_p : p \in S)^{-n/d}.$$

□

Lemma 5.2.6. *Let p be a prime and $a_1, \ldots, a_d \in \overline{\mathbb{Q}}_p$ with $|a_1 \ldots a_d|_p = 1$. Let $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ be a decomposable form and let $F_p = L_{p1} \cdots L_{pd}$ with $L_{p1}, \ldots, L_{pd}$ linear forms with coefficients in $\overline{\mathbb{Q}}_p$. Then*

$$\max_{1\le i_1<\cdots<i_n\le d} |\det(a_{i_1}\mathbf{L}_{i_1}, \ldots, a_{i_n}\mathbf{L}_{i_n})|_p \gg m_p(F)^{n/d}.$$

Proof. Write $F = a\prod_{i=1}^q N_{\mathbb{K}_i/\mathbb{Q}_p}(L'_i)$ where $a \in \mathbb{Q}_p^*$ and L'_i is a linear form in $\mathbb{K}_i[X_1, \ldots, X_n]$ with $\mathbb{K}_i$ an extension of $\mathbb{Q}_p$ of degree d_i for $i = 1, \ldots, q$.

Choose $a' \in \mathbb{Q}_p$ with $|a'|_p \gg\ll |a|_p^{1/d}$ and let $L''_i = a'L'_i$ $(i = 1, \ldots, q)$. Then $F = c\prod_{i=1}^q N_{\mathbb{K}_i/\mathbb{Q}_p}(L''_i)$ with $|c|_p \gg\ll 1$. Let $F' = c^{-1}F = \prod_{i=1}^d L''_i$. It suffices to prove

$$\max_{1\le i_1<\cdots<i_n\le d} |\det(a_{i_1}\mathbf{L}''_{i_1}, \ldots, a_{i_n}\mathbf{L}''_{i_n})|_p \gg m_p(F')^{n/d} \tag{5.2.8}$$

for all $a_1, \ldots, a_d \in \overline{\mathbb{Q}}_p$ with $|a_1 \ldots a_d|_p = 1$. Hence, we may assume $F = \prod_{i=1}^q N_{\mathbb{K}_i/\mathbb{Q}_p}(L_i)$ without loss of generality.

Let $\mathbb{E}$ be the normal closure of $\mathbb{K}_1 \ldots \mathbb{K}_q$. We have a factorization $F = \prod_{i=1}^q \prod_{j\in I_i} L_j$ where the $L_j (j \in I_i)$ are conjugate linear forms over $\mathbb{Q}_p$ and $\prod_{j\in I_i} L_j = N_{\mathbb{K}_i/\mathbb{Q}_p}(L_i)$ for $i = 1, \ldots, q$.

For $i = 1, \ldots, q$, choose $b_i \in \mathbb{Q}_p$ such that $|b_i|_p \gg\ll (\prod_{j\in I_j} |a_j|_p)^{1/d_i}$ and $b_j = b_i$ for $j \in I_i$.

We know that every $\sigma \in G := \mathrm{Gal}(\mathbb{E}/\mathbb{Q}_p)$ gives a permutation of $\{1, \ldots, d\}$, also denoted by σ, such that $\sigma(I_i) = I_i$ $(i = 1, \ldots, q)$. Further, G acts transitively on each I_i.

If $i_1 \in I_1$, we have $\sigma(i_1) \in I_1$ for every $\sigma \in G$. Also, among the linear forms $\sigma(L_{i_1}) = L_{\sigma(i_1)}$ $(\sigma \in G)$, each conjugate of L_{i_1} occurs $[\mathbb{E} : \mathbb{K}_{i_1}]$ times. Hence each index of I_1 occurs $[\mathbb{E} : \mathbb{K}_{i_1}]$ times among $\{\sigma(i_1)\ (\sigma \in G)\}$ and

$$|\prod_{\sigma\in G} a_{\sigma(i_1)}|_p = |\prod_{j\in I_1} a_j|^{[\mathbb{E}:\mathbb{K}_{i_1}]} \gg\ll |b_{i_1}|_p^{[\mathbb{E}:\mathbb{Q}_p]}.$$

Thus, we have

$$\begin{aligned}
&\max_{\sigma\in G} |\det(a_{\sigma(i_1)}\mathbf{L}_{\sigma(i_1)}, \dots, a_{\sigma(i_n)}\mathbf{L}_{\sigma(i_n)})|_p \\
&= \max_{\sigma\in G} |a_{\sigma(i_1)} \dots a_{\sigma(i_n)}|_p |\det(\mathbf{L}_{\sigma(i_1)}, \dots, \mathbf{L}_{\sigma(i_n)})|_p \\
&\geq \left(\prod_{\sigma\in G} |a_{\sigma(i_1)} \dots a_{\sigma(i_n)}|_p^{\frac{1}{[\mathbb{E}:\mathbb{Q}_p]}}\right) |\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})|_p \\
&\gg |b_{i_1} \dots b_{i_n}|_p |\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})|_p = |\det(b_{i_1}\mathbf{L}_{i_1}, \dots, b_{i_n}\mathbf{L}_{i_n})|_p.
\end{aligned}$$

Hence $\max_{1\leq i_1<\dots<i_n\leq d} |\det(a_{i_1}\mathbf{L}_{i_1}, \dots, a_{i_n}\mathbf{L}_{i_n})|_p \gg |\det(b_{i_1}\mathbf{L}_{i_1}, \dots, b_{i_n}\mathbf{L}_{i_n})|_p$ and we have $|b_1 \dots b_d|_p \gg\ll |a_1 \dots a_d|_p = 1$.

Let $L'_i = b_i L_i$ $(i = 1, \dots, d)$ and $F' = b_1 \dots b_d F = \prod_{i=1}^d L'_i$. It suffices to show (5.2.8) with L'_i, F' instead of L_i, F. So it suffices to prove that for $F = \prod_{i=1}^q \prod_{j\in I_i} L_j = \prod_{i=1}^q N_{\mathbb{K}_i/\mathbb{Q}_p}(L_i)$ we have

$$\max_{1\leq i_1<\dots<i_n\leq d} |\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})|_p \gg m_p(F)^{n/d}.$$

For $i = 1, \dots, q$, let $\{w_{i,1}, \dots, w_{i,d_i}\}$ be a $\mathbb{Z}_p$-basis of $O_{\mathbb{K}_i}$ and denote the embeddings of $\mathbb{K}_i$ in $\mathbb{E}$ by $\sigma_{i,1}, \dots, \sigma_{i,d_i}$. Write

$$L_i = \sum_{k=1}^{d_i} w_{ik} M_{ik},\ (i = 1, \dots, q)$$

with $M_{i1}, \dots, M_{ik_i} \in \mathbb{Q}_p[X_1, \dots, X_n]$ linear forms. We have

$$\sigma_{i,l}(L_i) = \sum_{k=1}^{d_i} \sigma_{i,l}(w_{ik}) M_{ik}\ (i = 1, \dots, q, l = 1, \dots, d_i)$$

with $|\sigma_{i,l}(w_{ik})|_p \le 1$ and $|\det(\sigma_{i,l}(w_{ik}))_{l,k=1,\dots,d_i}|_p \gg 1$.

By reindexing, we put

$$L_i = \sum_{k=1}^{d} w_{ik} M_k \quad \text{and} \quad M_i = \sum_{k=1}^{d} w^{ik} L_k \quad \text{for } i = 1, \dots, d.$$

with $|w_{ik}|_p \le 1$ $(i,k = 1, \dots, d)$, $|\det w_{ik}|_p \gg 1$ and $|w^{ik}|_p \ll 1$ for $i,k = 1, \dots, d$.

Let M be the $d \times n$ matrix with rows $\mathbf{M}_1, \dots, \mathbf{M}_d$ and let $\mathbf{m}_1, \dots, \mathbf{m}_n$ be the columns of M. By Lemma 5.1.5, there is a lower triangular matrix $T = (\epsilon_{ij})$ with $\epsilon_{ij} \in \mathbb{Q}_p$ such that $\mathbf{m}'_j = \sum_{j=1}^{i} \epsilon_{ij} \mathbf{m}_j$ $(j = 1, \dots, n)$ are orthonormal. Thus,

$$\begin{aligned} 1 = \max_{j=1,\dots,n} |\mathbf{m}'_j|_p &= \max_{i=1,\dots,d} |\mathbf{M}_i T|_p \gg \max_{j=1,\dots,d} |\mathbf{L}_i T|_p \\ &\gg (\prod_{i=1}^{d} |\mathbf{L}_i T|_p^{1/d}) = H_p(F_T)^{1/d} \ge |\det T|_p^{1/n} m_p(F)^{1/d}. \end{aligned}$$

Hence $|\det T|_p \ll m_p(F)^{-n/d}$.

Further, since $\mathbf{m}'_j = \sum_{j=1}^{i} \epsilon_{ij} \mathbf{m}_j$ $(j = 1, \dots, n)$ are orthonormal, we have

$$\begin{aligned} 1 &= |\mathbf{m}'_1 \wedge \cdots \wedge \mathbf{m}'_n|_p = \max_{1 \le i_1 < \cdots < i_n \le d} |\det(\mathbf{M}_{i_1} T, \dots, \mathbf{M}_{i_n} T)|_p \\ &= |\det T|_p \max_{1 \le i_1 < \cdots < i_n \le d} |\det(\mathbf{M}_{i_1}, \dots, \mathbf{M}_{i_n})|_p \ll |\det T|_p \max_{1 \le i_1 < \cdots < i_n \le d} |\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})|_p \\ &\ll m_p(F)^{-n/d} \cdot \max_{1 \le i_1 < \cdots < i_n \le d} |\det(\mathbf{L}_{i_1}, \dots, \mathbf{L}_{i_n})|_p. \end{aligned}$$

□

Lemma 5.2.7. *For each $p \in S$, let $F_p \in \mathbb{Q}_p[X_1, \dots, X_n]$ be a decomposable form and let $F_p = L_{p1} \cdots L_{pd}$ with $L_{p1}, \dots, L_{pd}$ linear forms with coefficients in $\overline{\mathbb{Q}}_p$. Assume $\mu^n(\mathbb{A}(F_p : p \in S))$ is finite and let*

$$\lambda_{p1}, \dots, \lambda_{pd} \in \overline{\mathbb{Q}}_p \text{ with } \lambda_{p1} \dots \lambda_{pd} = 1 \ (p \in S).$$

Then we have

$$\sqrt{\sum_{1 \le i_1 < \cdots < i_n \le d} |\det(\lambda_{\infty,i_1} \mathbf{L}_{\infty,i_1}, \dots, \lambda_{\infty,i_n} \mathbf{L}_{\infty,i_n})|^2} \ge c_1^{\infty} m_\infty(F_\infty)^{n/d},$$

$$\max_{1 \le i_1 < \cdots < i_n \le d} |\det(\lambda_{p,i_1} \mathbf{L}_{p,i_1}, \dots, \lambda_{p,i_n} \mathbf{L}_{p,i_n})|_p \ge c_1^{p} m_p(F_p)^{n/d} \quad (p \in S_0),$$

where c_1^p denotes an effectively computable positive number depending on n, d, p for each $p \in S$.

Proof. For $p = \infty$, see [22, Lemma 3]. For $p \in S_0$, use Lemma 5.2.6. $\square$

Lemma 5.2.8. *Let $(F_p : p \in S)$ be as in Lemma 5.2.7. Assume $\mu^n(\mathbb{A}(F_p : p \in S))$ is finite and $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S)$. Let $(A_p)_{p\in S} \in \mathbb{A}_S$ with $|A_p|_p < 1$ $(p \in S)$ and $j \in \{1, \dots, n-1\}$. Then there are effectively computable constants c_2^p $(p \in S)$ depending only on n, d, p with $c_2^p > c_1^p$ $(p \in S)$ and with the following property:*

Suppose that for each $p \in S$ there exist $S_p \subseteq \{1, \dots, d\}$ with $|S_p| = [jd/n] + 1$ such that

$$\frac{|\mathbf{L}_{p,i_1} \wedge \cdots \wedge \mathbf{L}_{p,i_{j+1}}|_p}{|\mathbf{L}_{p,i_1}|_p \dots |\mathbf{L}_{p,i_{j+1}}|_p} \leq |A_p|_p \text{ for all } i_1, \dots, i_{j+1} \in S_p. \tag{5.2.9}$$

Then for each $p \in S$, there is a factorization $F_p = \prod_{i=1}^d \lambda_{pi} L_{pi}$ with $\lambda_{p1} \dots \lambda_{pd} = 1$ such that

$$\sqrt{\textstyle\sum_{1\leq i_1<\cdots<i_n\leq d} |\det(\lambda_{\infty,i_1}\mathbf{L}_{\infty,i_1}, \dots, \lambda_{\infty,i_n}\mathbf{L}_{\infty,i_n})|^2} \leq c_2^\infty |A_\infty|^{\frac{n([jd/n]+1)-jd}{(n-j)d}} m_\infty(F_\infty)^{n/d},$$

$$\max_{1\leq i_1<\cdots<i_n\leq d} |\det(\lambda_{p,i_1}\mathbf{L}_{p,i_1}, \dots, \lambda_{p,i_n}\mathbf{L}_{p,i_n})|_p \leq c_2^p |A_p|_p^{\frac{n([jd/n]+1)-jd}{(n-j)d}} m_p(F_p)^{n/d} \quad (p \in S_0).$$

Proof. First, $m_p(F_p) = H_p(F_p)$ for $p \in S$. Indeed. Since $m_p(F_p) \leq H_p(F_p)$ by definition, we have

$$m(F_p : p \in S) = \prod_{p\in S} m_p(F_p) \leq \prod_{p\in S} H_p(F_p) = \mathcal{H}(F_p : p \in S).$$

Then our assumption $\mathcal{H}(F_p : p \in S) = m(F_p : p \in S)$ implies $m_p(F_p) = H_p(F_p)$ $(p \in S)$.

Without loss of generality, we assume that $|\mathbf{L}_1|_p = \cdots = |\mathbf{L}_d|_p = 1$ $(p \in S)$. Thus $m_p(F_p) = H_p(F_p) = 1$ $(p \in S)$.

For $p = \infty$, use [22, Lemma 4]. For $p \in S_0$, choose $a_p, b_p \in \overline{\mathbb{Q}}_p$ such that

$$|a_p|_p = |A_p|_p^{\frac{[jd/n]+1-d}{(n-j)d}} \text{ and } |a_p|_p^{[jd/n]+1} |b_p|_p^{d-[jd/n]-1} = 1.$$

Then

$$|a_p|_p > 1, \ |b_p|_p < 1, \ |a_p|_p^j |b_p|_p^{n-j} = |a_p|_p^n |A_p|_p = |A_p|_p^{\frac{n([jd/n]+1)-jd}{(n-j)d}}.$$

Let $\lambda_{pi} = a_p$ if $i \in S_p$ and $\lambda_{pi} = b_p$ otherwise. For tuples $i_1, \dots, i_n$ with l of them in S_p, we have

$$\begin{aligned} |\det(\lambda_{p,i_1}\mathbf{L}_{i_1}, \dots, \lambda_{p,i_n}\mathbf{L}_{i_n})|_p &\leq |a_p|_p^l |b_p|_p^{n-l} && \text{if } l < j+1, \\ |\det(\lambda_{p,i_1}\mathbf{L}_{i_1}, \dots, \lambda_{p,i_n}\mathbf{L}_{i_n})|_p &\leq |a_p|_p^l |b_p|_p^{n-l} |A_p|_p \leq |a_p|_p^n |A_p|_p && \text{if } l \geq j+1. \end{aligned}$$

□

Combining Lemma 5.2.7, 5.2.8, we see that condition (5.2.9) in Lemma 5.2.8 can hold only if

$$|A_p|_p \geq \left(\frac{c_1^p}{c_2^p} \right)^{\frac{(n-j)d}{n([jd/n]+1)-jd}} \quad \text{for } p \in S. \tag{5.2.10}$$

We now give the definition of $a'(F)$. In fact, we first define $a'(F_p : p \in S)$ for a system of decomposable forms $(F_p : p \in S)$, under the assumption that $\mu^n(\mathbb{A}(F_p : p \in S))$ is finite.

Assume $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S)$. For $j = 1, \dots, n-1$, let $s_j^p(F_p)$ be the cardinality of the largest subset $S_p \subset \{1, \dots, d\}$ such that

$$\frac{|\mathbf{L}_{pi_1} \wedge \cdots \wedge \mathbf{L}_{p,i_{j+1}}|_p}{|\mathbf{L}_{p,i_1}|_p \dots |\mathbf{L}_{p,i_{j+1}}|_p} < \left(\frac{c_1^p}{c_2^p} \right)^{\frac{(n-j)d}{n([jd/n]+1)-jd)}} \quad \text{for all } i_1, \dots, i_{j+1} \in S_p.$$

By Lemma 5.2.8, $s_j^p(F_p) \leq [jd/n]$ for $p \in S$. For each $p \in S$, define

$$s^p(F_p) := \max \left\{ \frac{s_j^p(F_p)}{j} : j = 1, \dots, n-1 \right\}.$$

We define

$$a'(F_p : p \in S) := \max_{\mathbf{T}} \max_{p \in S} \{ s^p((F_p)_{T_p}) \}$$

where the maximum is taken over all $\mathbf{T} = (T_p)_{p \in S} \in GL_n(\mathbb{A}_S)$ with $|\det \mathbf{T}|_S = 1$ such that $m(F_p : p \in S) = \mathcal{H}((F_p)_{T_p} : p \in S)$.

For a decomposable form $F \in \mathbb{Z}[X_1, \dots, X_n]$, under the assumption that $\mu^n(\mathbb{A}_{F,S}) < \infty$, we define

$$a'(F) := \max_{\mathbf{T}} \max_{p \in S} \{ s^p(F_{T_p}) \}$$

where the maximum is taken over all $\mathbf{T} = (T_p)_{p\in S} \in GL_n(\mathbb{A}_S)$ with $|\det \mathbf{T}|_S = 1$ such that $m(F) = \mathcal{H}(F_{\mathbf{T}})$. By definition, $1 \leq s^p(F_{T_p}) \leq d/n$. Also, if $s^p(F_{T_p}) < d/n$, we have

$$s^p(F_{T_p}) \leq \frac{d}{n} - \frac{1}{n(n-1)}.$$

So we have $1 \leq a'(F) \leq d/n$ and

$$a'(F) < \frac{d}{n} \Rightarrow a'(F) \leq \frac{d}{n} - \frac{1}{n(n-1)}.$$

Moreover, if $n \not| jd$ for all $j = 1, \ldots, n-1$ i.e., if n and d are coprime, then $a'(F) < d/n$.

Recall that

$$a(F) := \max_{1\leq j\leq n-1} \max_{(\mathbf{L}_{i_1},\ldots,\mathbf{L}_{i_n})\in I(F)} \frac{|\{\mathbf{L}_i \in \text{span } \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}|}{j}.$$

Since, for every $1 \leq j \leq n-1$, the wedge product of any $j+1$ vectors in span $\{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}$ is 0 for every $(\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_n}) \in I(F)$, we have

$$\max_{(\mathbf{L}_{i_1},\ldots,\mathbf{L}_{i_n})\in I(F)} |\{\mathbf{L}_i \in \text{span } \{\mathbf{L}_{i_1}, \ldots, \mathbf{L}_{i_j}\}\}| \leq s_j^\infty(F)$$

and thus $a(F) \leq a'(F)$.

Lemma 5.2.9. *Let A be an $(N+1)\times(N+1)$ matrix with complex entries. Suppose that all the rows have length ≤ 1. Let $\mathbf{C}$ be a column of A. Then*

$$|\det A| \leq \sqrt{N+1}|\mathbf{C}|_\infty$$

Proof. Let $\mathbf{C} = (c_1, \ldots, c_{N+1})^T$. Then

$$\det A = d_1c_1 + \cdots + d_{N+1}c_{N+1}$$

where up to sign $d_1, \ldots, d_{N+1}$ are determinants of $N \times N$ submatrices of A. The rows of these submatrices are subrows of A, hence have Euclidean length at most 1. So by Hadamard's inequality, $|d_i| \leq 1$ for $i = 1, \ldots, N+1$. Let $D = (d_1, \ldots, d_{N+1})^T$. Then by the Cauchy-Schwarz inequality,

$$|\det A| \leq |\mathbf{D}|_\infty |\mathbf{C}|_\infty \leq \sqrt{N+1}|\mathbf{C}|_\infty.$$

□

Lemma 5.2.10. *For each $p \in S$, let $\mathbf{K}_{p1}, \ldots, \mathbf{K}_{pN} \in \overline{\mathbb{Q}}_p^M$ and $\mathbf{L}_{p1}, \ldots, \mathbf{L}_{p,N+1} \in \overline{\mathbb{Q}}_p^M$ with $|\mathbf{L}_{pi}|_p = 1$ $(i = 1, \ldots, N+1)$ and $N + 1 \leq M$. For $p = \infty$, we have*

$$|\mathbf{K}_{\infty 1} \wedge \cdots \wedge \mathbf{K}_{\infty N}|_\infty \cdot |\mathbf{L}_{\infty 1} \wedge \cdots \wedge \mathbf{L}_{\infty, N+1}|_\infty \leq \sqrt{\binom{M}{N}(N+1)\left(\sum_{j=1}^{N+1} |\mathbf{K}_{\infty 1} \wedge \cdots \wedge \mathbf{K}_{\infty N} \wedge \mathbf{L}_{\infty j}|_\infty^2\right)}.$$

For $p \in S_0$, we have

$$|\mathbf{K}_{p1} \wedge \cdots \wedge \mathbf{K}_{pN}|_p \cdot |\mathbf{L}_{p1} \wedge \cdots \wedge \mathbf{L}_{p,N+1}|_p \leq \max_{j=1,\ldots,N+1} |\mathbf{K}_{p1} \wedge \cdots \wedge \mathbf{K}_{pN} \wedge \mathbf{L}_{pj}|_p.$$

Proof. Let $\mathbf{L}_{pj} = (a_{j1}^p, \ldots, a_{jM}^p)(j = 1, \ldots, N+1, p \in S)$. One may assume that $\mathbf{K}_{p1} = \mathbf{e}_1, \ldots, \mathbf{K}_{pN} = \mathbf{e}_N$ are the first N unit vectors.

For $p = \infty$, it suffices to show that

$$|\mathbf{L}_{\infty 1} \wedge \cdots \wedge \mathbf{L}_{\infty, N+1}|_\infty^2 \leq \binom{M}{N}(N+1) \sum_{j=1}^{N+1} \sum_{k=N+1}^{M} |a_{jk}^\infty|^2. \tag{5.2.11}$$

Since the coordinates of $\mathbf{L}_{\infty 1} \wedge \cdots \wedge \mathbf{L}_{\infty, N+1}$ are the determinants of $(N+1) \times (N+1)$ matrices, it is easy to conclude (5.2.11) by using Lemma 5.2.9.

For $p \in S_0$, it suffices to show that

$$|\mathbf{L}_{p1} \wedge \cdots \wedge \mathbf{L}_{p,N+1}|_p \leq \max_{j=1,\ldots,N+1} \max_{k=N+1,\ldots,M} |a_{jk}|_p, \tag{5.2.12}$$

which is obvious. □

We write $d(\infty) = 1$ and $d(p) = 0$ for $p \in S_0$.

Lemma 5.2.11. *For each $p \in S$, let $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ be a decomposable form and suppose $F_p = L_{p1} \cdots L_{pd}$ with $L_{p1}, \ldots, L_{pd}$ linear forms in $\overline{\mathbb{Q}}_p[X_1, \ldots, X_n]$. Assume $\mu^n(\mathbb{A}(F_p : p \in S))$ is finite and $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S)$. Let $(B_p)_{p \in S} \in \mathbb{A}_S$ with $|B_p|_p > 1$ $(p \in S)$ and $L_{p,i_1(p)}, \ldots, L_{p,i_j(p)}$ are linearly independent. Suppose that for each $p \in S$ there is a set $S_p \subseteq \{1, \ldots, d\}$ with $|S_p| = [jd/n] + 1$ such that*

$$\frac{|\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_j(p)} \wedge \mathbf{L}_{p,l}|_p}{|\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_j(p)}|_p |\mathbf{L}_{p,l}|_p} \leq |B_p|_p \text{ for all } l \in S_p.$$

Then

$$|B_p|_p \geq C(n)^{-d(p)} \left(\frac{c_1^p}{c_2^p}\right)^{\frac{(n-j)d}{n([jd/n]+1)-jd}} \quad \textit{for } p \in S$$

where $C(n) = \max_{1\leq j\leq n} \binom{n}{j}(j+1)^{3/2}$.

Proof. Without loss of generality, we may assume that $|\mathbf{L}_{p1}|_p = \cdots = |\mathbf{L}_{pd}|_p = 1$ $(p \in S)$. Hence $m_p(F) = H_p(F) = 1$ $(p \in S)$.

Let $l_1, \ldots, l_{j+1} \in S_p$ $(p \in S)$. By Lemma 5.2.10, we have

$$\begin{aligned}|\mathbf{L}_{\infty,l_1} \wedge \cdots \wedge \mathbf{L}_{\infty,l_{j+1}}|_\infty^2 &\leq \binom{n}{j}^2 (j+1)^2 \cdot \sum_{k=1}^{j+1} \frac{|\mathbf{L}_{\infty,i_1(\infty)} \wedge \cdots \wedge \mathbf{L}_{\infty,i_j(\infty)} \wedge \mathbf{L}_{\infty,l_k}|_\infty^2}{|\mathbf{L}_{\infty,i_1(\infty)} \wedge \cdots \wedge \mathbf{L}_{\infty,i_j(\infty)}|_\infty^2} \\ &\leq \binom{n}{j}^2 (j+1)^3 |B_\infty|^2 \leq C(n)^2 |B_\infty|^2\end{aligned}$$

where $C(n) = \max_{1\leq j\leq n} \binom{n}{j}(j+1)^{3/2}$ and for $p \in S_0$

$$|\mathbf{L}_{p,l_1} \wedge \cdots \wedge \mathbf{L}_{p,l_{j+1}}|_p \leq \max_{k=1,\ldots,j+1} \frac{|\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_j(p)} \wedge \mathbf{L}_{pl_k}|_p}{|\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_j(p)}|_p} \leq |B_p|_p.$$

Then, using Lemma 5.2.8 and (5.2.10), we complete the proof. □

Lemma 5.2.12. *Let* $(F_p : p \in S)$ *be a system of decomposable forms of degree* d *with* $F_p \in \mathbb{Q}_p[X_1, \ldots, X_n]$ *and* $F_p = L_{p1} \ldots L_{pd}$. *Assume* $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S)$.

(*a*) *For every* $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$, *there are linear independent linear factors* $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ *of* F_p *for* $p \in S$ *such that*

$$\left(\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p}\right)^{a'(F_p:p\in S)} \leq c_3 \frac{\prod_{p\in S} |F_p(\mathbf{x}_p)|_p}{\prod_{p\in S} |\mathbf{x}_p|_p^{d-na'(F_p:p\in S)} \cdot m(F_p : p \in S)}$$

where c_3 *is effectively computable and depends only on* n, d, S.

(*b*)*Let* $F \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a decomposable form of degree* d. *Assume* $m(F) = \mathcal{H}(F_{\mathbf{T}})$ *for some* $\mathbf{T} \in GL_n(\mathbb{A}_S)$ *with* $|\det \mathbf{T}|_S = 1$. *Then for every* $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$, *there are linear independent linear factors* $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ $(p \in S)$ *of* F *such that*

$$\left(\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p}\right)^{a'(F)} \leq c_3 \frac{\prod_{p\in S} |F(\mathbf{x}_p)|_p}{\prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p^{d-na'(F)} \cdot m(F)}.$$

Proof. Note that (b) follows from (a). Indeed, given such $\mathbf{T} \in GL_n(\mathbb{A}_S)$ as in (b) and $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$, apply (a) to $(F_{T_p} : p \in S)$ and $(T_p^{-1}\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$. So we are left to prove (a).

We may assume that $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S) = 1$. Indeed, suppose that $m(F_p : p \in S) = \mathcal{H}(F_p : p \in S) \neq 1$. Let $\mathbf{a} \in \mathbb{A}_S$ such that $|a_p|_p = H_p(F)$ $(p \in S)$ and let $G_p = \frac{F_p}{a_p}$ $(p \in S)$. Then we have $\mathcal{H}_p(G_p : p \in S) = 1, m(G_p : p \in S) = \prod_{p\in S} \frac{m_p(F_p)}{H_p(F_p)} = 1$ and $a'(F_p : p \in S) = a'(G_p : p \in S)$. It is clear that the statement (a) for $(G_p : p \in S)$ implies the statement (a) for $(F_p : p \in S)$.

By homogeneity we may also assume that $|\mathbf{L}_{p1}|_p = \cdots = |\mathbf{L}_{pd}|_p = 1$ $(p \in S)$.

For $j = 1, \ldots, n-1$, choose $C_j^p \in \overline{\mathbb{Q}}_p$ $(p \in S)$ such that

$$|C_j^p|_p = C(n)^{-d(p)} \left(\frac{c_1^p}{c_2^p}\right)^{\frac{(n-j)d}{n([jd/n]+1)-jd}} \quad \text{with } d(\infty) = 1, d(p) = 0 \ (p \in S_0).$$

Let $p \in S$. Choose $i_1(p) \in \{1, \ldots, d\}$ such that $|L_{p,i_1(p)}(\mathbf{x}_p)|_p = \min_{i=1,\ldots,d} |L_{p,i}(\mathbf{x}_p)|_p$ $(p \in S)$ and let $S_1^p \subset \{1, \ldots, d\}$ $(p \in S)$ be the subset of indices l such that

$$|\mathbf{L}_{p,i_1(p)} \wedge \mathbf{L}_{p,l}|_p < |C_1^p|_p \ (p \in S).$$

For $j = 2$, let $|L_{p,i_2(p)}(\mathbf{x}_p)|_p = \min_{i \notin S_1^p} |L_{p,i}(\mathbf{x}_p)|_p$ $(p \in S)$ and let $S_2^p \subseteq \{1, \ldots, d\}$ $(p \in S)$ be the subset of indices l such that

$$\frac{|\mathbf{L}_{p,i_1(p)} \wedge \mathbf{L}_{p,i_2(p)} \wedge \mathbf{L}_{p,l}|_p}{|\mathbf{L}_{p,i_1(p)} \wedge \mathbf{L}_{p,i_2(p)}|_p} < |C_2^p|_p \ (p \in S).$$

Continue in this manner up to S_{n-1}^p. Then by definition, $S_1^p \subseteq \cdots \subseteq S_{n-1}^p$ and

$$|S_j^p| \leq j \cdot a'(F_p : p \in S) \leq [jd/n] < d \text{ for } j = 1, \ldots, n-1.$$

Hence we can choose $L_{p,i_n(p)} \notin S_{n-1}^p$ $(p \in S)$ and let $|S_n^p| = d$.

By this construction, we have $|L_{p,i_1(p)}(\mathbf{x}_p)|_p \leq \cdots \leq |L_{p,i_n(p)}(\mathbf{x}_p)|_p$ and

$$|F_p(\mathbf{x}_p)|_p \geq |L_{p,i_1(p)}(\mathbf{x}_p)|_p^{z_1^p} \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p^{z_n^p} \ (p \in S)$$

where $z_1^p = |S_1^p|$ $(p \in S)$ and $z_j^p = |S_j^p| - |S_{j-1}^p|$ $(j = 2, \ldots, n)$ $(p \in S)$.

Note that $z_1^p + \cdots + z_j^p = |S_j^p| \le ja'(F_p : p \in S)$ $(j = 1, \ldots, n-1)$. Let

$$\epsilon^p := (n-1)a'(F_p : p \in S) - |S_{n-1}^p| \text{ for } p \in S.$$

Then

$$|F_p(\mathbf{x}_p)|_p \ge |L_{p,i_1(p)}(\mathbf{x}_p)|_p^{z_1^p} \cdots |L_{p,i_{n-2}(p)}(\mathbf{x}_p)|_p^{z_{n-2}^p} |L_{p,i_{n-1}(p)}(\mathbf{x}_p)|_p^{z_{n-1}^p + \epsilon^p} |L_{p,i_n(p)}(\mathbf{x}_p)|_p^{z_n^p - \epsilon^p} \ (p \in S).$$

Then Lemma 2.2.2 implies that

$$|F_p(\mathbf{x}_p)|_p \ge \left(\prod_{j=1}^{n} |L_{p,i_j(p)}(\mathbf{x}_p)|_p^{a'(F_p:p\in S)} \right) \cdot |L_{p,i_n(p)}(\mathbf{x}_p)|_p^{d-na'(F_p:p\in S)} \ (p \in S).$$

By Lemma 2.2.1, we have

$$|L_{p,i_n(p)}(\mathbf{x}_p)|_p \ge n^{-d(p)\cdot n/2} \cdot |\mathbf{x}|_p \cdot |\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p \ (p \in S)$$

and thus

$$\left(\frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \right)^{a'(F_p:p\in S)} \le \frac{n^{d(p)(d-na'(F_p:p\in S))\cdot n/2} |F_p(\mathbf{x}_p)|_p \cdot |\mathbf{x}_p|_p^{-d+na'(F_p:p\in S)}}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p^{d-(n-1)a'(F_p:p\in S)}}.$$

Further, for each $p \in S$ we have

$$\begin{aligned} |\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p &\ge |C_{n-1}^p|_p |\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_{n-1}(p)})|_p \\ &\ge |C_{n-1}^p|_p |C_{n-2}^p|_p |\mathbf{L}_{p,i_1(p)} \wedge \cdots \wedge \mathbf{L}_{p,i_{n-2}(p)})|_p \\ &\ge \cdots \ge \prod_{j=1}^{n-1} |C_j^p|_p. \end{aligned}$$

Then Lemma 5.2.12 follows with

$$c_3 = n^{(d-na'(F_p:p\in S))\cdot n/2} \prod_{p\in S} \prod_{j=1}^{n-1} |C_j^p|_p^{-d+(n-1)a'(F_p:p\in S)}.$$

□

5.3 Fundamental propositions

Define $\log^* x := \max\{1, \log x\}$.

Proposition 5.3.1. *Let $F \in \mathbb{Z}[X_1, \dots, X_n]$ be a decomposable form of degree d. Choose $\mathbf{T} = (T_p)_{p\in S} \in GL_n(\mathbb{A}_S)$ such that $\mathcal{H}(F_{\mathbf{T}}) = m(F_{\mathbf{T}})$. Let $1 \le B < C$, $D > 1$, and*

$$\mathcal{M} := \left\{ (\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m, |\mathbf{x}_p|_p = 1 \ (p \in S_0), \\ (\frac{m}{m(F)})^{1/d} B \le \prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\}.$$

Then

(a) $\mu^n(\mathcal{M}) \ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1} \cdot C B^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}.$

(b) $\mathcal{M} \cap \mathbb{Z}^n$ *is contained in the union of*

$$\ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1}$$

proper linear subspaces of $\mathbb{Q}^n$ and a finite set of cardinality

$$\ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1} \cdot C B^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}.$$

Proof. (a) For every $\underline{z} = (z_p)_{p\in S_0} \in \mathbb{Z}^{|S_0|}$, define

$$\mathcal{M}_{\underline{z}} = \left\{ (\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m, \\ |\mathbf{x}_p|_p = 1, |T_p^{-1}\mathbf{x}_p|_p = p^{z_p} \text{ for } p \in S_0, \\ (\frac{m}{m(F)})^{1/d} B \le \prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\}.$$

Then $\mathcal{M} = \coprod_{\underline{z}\in\mathbb{Z}^{|S_0|}} \mathcal{M}_{\underline{z}}$.

For $(\mathbf{x}_p)_{p\in S} \in \mathcal{M}_{\underline{z}}$, let $\mathbf{y}_p = (\prod_{q\in S_0} q^{z_p})\mathbf{x}_p$ for $p \in S$. It is clear that the volume of $\mathcal{M}_{\underline{z}}$ is equal to the volume of

$$\mathcal{M}'_{\underline{z}} := \left\{ (\mathbf{y}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{y}_p)|_p \le m, \\ |\mathbf{y}_p|_p = p^{-z_p}, |T_p^{-1}\mathbf{y}_p|_p = 1 \text{ for } p \in S_0, \\ (\frac{m}{m(F)})^{1/d} B \le \prod_{p\in S} |T_p^{-1}\mathbf{y}_p|_p \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\}.$$

Also, we have

$$|\mathcal{M}_{\underline{z}} \cap \mathbb{Z}^n| = |\mathcal{M}'_{\underline{z}} \cap \mathbb{Z}_S^n| = \left| \left\{ \mathbf{y} \in \mathbb{Z}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{y})|_p \le m, \\ |\mathbf{y}|_p = p^{-z_p}, |T_p^{-1}\mathbf{y}|_p = 1 \text{ for } p \in S_0, \\ (\frac{m}{m(F)})^{1/d} B \le \prod_{p\in S} |T_p^{-1}\mathbf{y}|_p \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\} \right|.$$

Let

$$\begin{aligned} \mathcal{M}' &:= \coprod_{\underline{z}\in\mathbb{Z}^{|S_0|}} \mathcal{M}'_{\underline{z}} = \left\{ (\mathbf{y}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{y}_p)|_p \le m, |T_p^{-1}\mathbf{y}_p|_p = 1 \ (p \in S_0), \\ (\frac{m}{m(F)})^{1/d} B \le \prod_{p\in S} |T_p^{-1}\mathbf{y}_p|_p \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\} \\ &= \left\{ (\mathbf{y}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F_{T_p}(T_p^{-1}\mathbf{y}_p)|_p \le m, |T_p^{-1}\mathbf{y}_p|_p = 1 \ (p \in S_0), \\ (\frac{m}{m(F)})^{1/d} B \le |T_\infty^{-1}\mathbf{y}_\infty|_\infty \le (\frac{m}{m(F)})^{1/d} C \end{array} \right\}. \end{aligned}$$

Then we have $\mu^n(\mathcal{M}) = \mu^n(\mathcal{M}')$ and $|\mathcal{M} \cap \mathbb{Z}^n| = |\mathcal{M}' \cap \mathbb{Z}_S^n|$.

For every $(\mathbf{y}_p)_{p\in S} \in \mathcal{M}'$, by Lemma 5.2.12 there are linear independent linear factors $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)} \in \overline{\mathbb{Q}}_p[X_1, \ldots, X_n]$ of F for $p \in S$ such that

$$\begin{aligned} \prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{y}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{y}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} &\le c_4 \left(\frac{\prod_{p\in S} |F(\mathbf{y}_p)|_p}{\prod_{p\in S} |T_p^{-1}\mathbf{y}_p|_p^{d-na'(F)} m(F)} \right)^{\frac{1}{a'(F)}} \\ &\le c_4 B^{\frac{-d+na'(F)}{a'(F)}} \left(\frac{m}{m(F)} \right)^{n/d} \end{aligned}$$

where $c_4 = \max\{1, c_3^{1/a'(F)}\}$. By homogeneity, we may assume that $m = m(F) = 1$. Then $B \le |T_\infty^{-1}\mathbf{y}_\infty|_\infty \le C$ and

$$\prod_{p\in S} \frac{|(L_{p,i_1(p)})_{T_p}(T_p^{-1}\mathbf{y}_p)|_p \cdots |(L_{p,i_n(p)})_{T_p}(T_p^{-1}\mathbf{y}_p)|_p}{|\det((\mathbf{L}_{p,i_1(p)})_{T_p}, \ldots, (\mathbf{L}_{p,i_n(p)})_{T_p})|_p} \le c_4 B^{\frac{-d+na'(F)}{a'(F)}}. \tag{5.3.1}$$

Applying Lemma 2.2.12 with B, C, D and $A = c_4 B^{\frac{-d+na'(F)}{a'(F)}}$, the set of $(\mathbf{y}_p)_{p\in S} \in \mathbb{A}_S$ with $B \le |T_\infty^{-1}\mathbf{y}_\infty|_\infty \le C$ satisfying (5.3.1) can be covered by at most

$$\ll \left(\log_D^*(\frac{BC^{n-1}}{A})\right)^{|S|(n-1)-1} \ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1}$$

sets of the form

$$\mathcal{C} = \{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |K'_{pi}(T_p^{-1}\mathbf{y}_p)|_p \le a_{pi} \ (p \in S, 1 \le i \le n)\}$$

where $K'_{p1}, K'_{p2}, \dots, K'_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \dots, X_n]$ with

$$|\det(\mathbf{K}'_{p1}, \mathbf{K}'_{p2}, \dots, \mathbf{K}'_{pn})|_p = 1 \ , \ |\mathbf{K}'_{p1}|_p = \cdots = |\mathbf{K}'_{pn}|_p = 1$$

and a_{pi} are positive reals with

$$\prod_{p\in S}\prod_{i=1}^{n} a_{pi} \ll \frac{CA}{B} D^{|S|\cdot(n-1)+1} \ll CB^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1}. \tag{5.3.2}$$

For such a convex set $\mathcal{C}$, by Lemma 1.2.5 and $|\det \mathbf{T}|_S = 1$ we have

$$\mu^n(\mathcal{C}) \ll CB^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}. \tag{5.3.3}$$

Hence we have

$$\mu^n(\mathcal{M}) = \mu^n(\mathcal{M}') \ll \big(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\big)^{|S|(n-1)-1} \times$$
$$\times CB^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}.$$

(b) For a convex set $\mathcal{C}$ with n linearly independent points in $\mathcal{C} \cap \mathbb{Z}_S^n$, we can estimate the cardinality of $\mathcal{C} \cap \mathbb{Z}_S^n$. For each $p \in S$, define

$$\mathcal{C}_p := \{\mathbf{y}_p \in \mathbb{Q}_p^n : |K'_{pi}T_p^{-1}(\mathbf{y}_p)|_p \le a_{pi} \ (i = 1, \dots, n)\}$$

where the a_{pi} satisfy (5.3.2). Then

$$\mathcal{C} = \prod_{p\in S} \mathcal{C}_p \text{ and } \mathcal{C} \cap \mathbb{Z}_S^n = \mathcal{C}_\infty \cap \Lambda$$

where, by Lemma 1.2.2, $\Lambda = \{\mathbf{x} \in \mathbb{Z}_S^n : \mathbf{x} \in \mathcal{C}_p \ (p \in S_0)\}$ is a lattice. By Lemma 1.2.5, we know that

$$|\mathcal{C} \cap \mathbb{Z}_S^n| \le CB^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}. \tag{5.3.4}$$

Hence $\mathcal{M}' \cap \mathbb{Z}^n$ is contained in

$$\ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1}$$

proper linear subspaces of $\mathbb{Q}^n$ and a finite set with cardinality at most

$$\ll \left(\log_D^*(B^{\frac{d-(n-1)a'(F)}{a'(F)}} C^{n-1})\right)^{|S|(n-1)-1} \cdot CB^{\frac{-d+(n-1)a'(F)}{a'(F)}} D^{|S|\cdot(n-1)+1} (\frac{m}{m(F)})^{n/d}.$$

This implies Proposition 5.3.1 (b). $\square$

Proposition 5.3.2. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Assume $a'(F) < d/n$ and let $\mathbf{T} = (T_p)_{p\in S} \in GL_n(\mathbb{A}_S)$ such that $m(F_\mathbf{T}) = \mathcal{H}(F_\mathbf{T})$. Further, let $B_0 \geq 1$ and $D > 1$.*

(a) We have

$$\mu^n\left(\left\{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{x}_p)|_p \leq m, |\mathbf{x}_p| = 1 \ (p \in S_0) \\ \prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p \geq \left(\frac{m}{m(F)}\right)^{1/d} B_0 \end{array}\right\}\right) \ll$$

$$\left(\frac{m}{m(F)}\right)^{n/d} (1+\log_D^* B_0)^{|S|(n-1)-1} B_0^{\frac{-d+na'(F)}{a'(F)}} D^{|S|\cdot(n-1)+2} \cdot \left(\sum_{l=0}^{\infty} (l+1)^{|S|(n-1)-1} D^{\frac{-dl+nla'(F)}{a'(F)}}\right).$$

(b) For any integer $l_1 \geq 0$, the set

$$\left\{\mathbf{z} \in \mathbb{Z}^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{z})|_p \leq m, |\mathbf{z}|_p = 1 \ (p \in S_0) \\ \left(\frac{m}{m(F)}\right)^{1/d} B_0 \leq \prod_{p\in S} |T_p^{-1}\mathbf{z}|_p \leq (\frac{m}{m(F)})^{1/d} B_0 D^{l_1+1} \end{array}\right\}$$

can be covered by a finite set Ω with

$$|\Omega| \ll (\frac{m}{m(F)})^{n/d} (1+\log_D^* B_0)^{|S|(n-1)-1} B_0^{\frac{-d+na'(F)}{a'(F)}} D^{|S|\cdot(n-1)+2} \times$$

$$\times \left(\sum_{l=0}^{l_1} (l+1)^{|S|(n-1)-1} D^{\frac{-dl+nla'(F)}{a'(F)}}\right)$$

and at most

$$\ll (1+\log_D^* B_0)^{|S|(n-1)-1} (l_1+1)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$.

Proof. (a) For $l \geq 0$, let $B_l = D^l B_0,\ C_l = DB_l = D^{l+1}B_0$. By Proposition 5.3.1, we have

$$\mu^n\left(\left\{(\mathbf{x}_p)_{p\in S}\in\mathbb{A}_S^n:\ \begin{array}{l}\prod_{p\in S}|F(\mathbf{x}_p)|_p\leq m,\ |\mathbf{x}_p|=1\ (p\in S_0),\\ (\frac{m}{m(F)})^{1/d}B_l\leq\prod_{p\in S}|T_p\mathbf{x}_p|_p\leq(\frac{m}{m(F)})^{1/d}C_l\end{array}\right\}\right)$$

$$\ll\left(\log_D^*(B_l^{\frac{d-(n-1)a'(F)}{a'(F)}}C_l^{n-1})\right)^{|S|(n-1)-1}\cdot C_l B_l^{\frac{-d+(n-1)a'(F)}{a'(F)}}D^{|S|\cdot(n-1)+1}\left(\frac{m}{m(F)}\right)^{n/d}$$

$$\ll((l+1)(1+\log_D^* B_0))^{|S|(n-1)-1}\cdot B_0^{\frac{-d+na'(F)}{a'(F)}}D^{|S|\cdot(n-1)+2}D^{\frac{-dl+nla'(F)}{a'(F)}}\left(\frac{m}{m(F)}\right)^{n/d}.$$

Hence

$$\mu^n\left(\left\{(\mathbf{x}_p)_{p\in S}\in\mathbb{A}_S^n:\ \begin{array}{l}\prod_{p\in S}|F(\mathbf{x}_p)|_p\leq m,|\mathbf{x}_p|=1\ (p\in S_0),\\ \prod_{p\in S}|T_p\mathbf{x}_p|_p\geq\left(\frac{m}{m(F)}\right)^{1/d}B_0\end{array}\right\}\right)\ll$$

$$\left(\frac{m}{m(F)}\right)^{n/d}(1+\log_D^* B_0)^{|S|(n-1)-1}B_0^{\frac{-d+na'(F)}{a'(F)}}D^{|S|\cdot(n-1)+2}\cdot\left(\sum_{l=0}^{\infty}(l+1)^{|S|(n-1)-1}D^{\frac{-dl+nla'(F)}{a'(F)}}\right).$$

(b) As we have seen in Proposition 5.3.1, for $l = 0, \ldots, l_1$ the set

$$\left\{\mathbf{z}\in\mathbb{Z}^n:\ \begin{array}{l}\prod_{p\in S}|F(\mathbf{z})|_p\leq m,\ |\mathbf{z}|_p=1\ (p\in S_0),\\ (\frac{m}{m(F)})^{1/d}B_l\leq\prod_{p\in S}|T_p^{-1}\mathbf{z}|_p\leq(\frac{m}{m(F)})^{1/d}C_l\end{array}\right\}$$

is contained in at most

$$\ll\left(\log_D^*(B_l^{\frac{d-(n-1)a'(F)}{a'(F)}}C_l^{n-1})\right)^{|S|(n-1)-1}\ll((l+1)(1+\log_D^* B_0))^{|S|(n-1)-1}$$

proper linear subspaces of $\mathbb{Q}^n$ and a finite set Ω_l with

$$|\Omega_l|\ll((l+1)(1+\log_D^* B_0))^{|S|(n-1)-1}\cdot B_0^{\frac{-d+na'(F)}{a'(F)}}D^{|S|\cdot(n-1)+2}D^{\frac{-dl+nla'(F)}{a'(F)}}\left(\frac{m}{m(F)}\right)^{n/d}.$$

Let $\Omega = \bigcup_{l=0}^{l_1}\Omega_l$. Then we have

$$|\Omega|\ll\sum_{l=0}^{l_1}|\Omega_l|\ll\left(\frac{m}{m(F)}\right)^{n/d}(1+\log_D^* B_0)^{|S|(n-1)-1}B_0^{\frac{-d+na'(F)}{a'(F)}}D^{|S|\cdot(n-1)+2}\times$$

$$\times\left(\sum_{l=0}^{l_1}(l+1)^{|S|(n-1)-1}D^{\frac{-dl+nla'(F)}{a'(F)}}\right).$$

□

Lemma 5.3.3. *Let* $\mathbf{T} \in GL_n(\mathbb{A}_S)$ *with* $|\det \mathbf{T}|_S = 1$. *Then*

$$|\{\mathbf{z} \in \mathbb{Z}^n : \prod_{p \in S} |T_p \mathbf{z}|_p \leq A, |\mathbf{z}|_p = 1 \ (p \in S_0)\}| \ll A^n.$$

Proof.

$$\left|\left\{\mathbf{z} \in \mathbb{Z}^n : \begin{array}{l} \prod_{p\in S} |T_p\mathbf{z}|_p \leq A, \\ |\mathbf{z}|_p = 1 \ (p \in S_0) \end{array}\right\}\right| = \left|\left\{\mathbf{x} \in \mathbb{Z}_S^n : \begin{array}{l} \prod_{p\in S} |T_p\mathbf{x}|_p \leq A, \\ |\mathbf{x}|_p = 1 \ (p \in S_0) \end{array}\right\}\right|$$
$$= \left|\left\{\mathbf{x} \in \mathbb{Z}_S^n : \begin{array}{l} \prod_{p\in S} |T_p\mathbf{x}|_p \leq A, \\ |T_p\mathbf{x}|_p = 1 \ (p \in S_0) \end{array}\right\}\right| \leq \left|\left\{\mathbf{x} \in \mathbb{Z}_S^n : \begin{array}{l} |T_\infty\mathbf{x}| \leq A, \\ |T_p\mathbf{x}|_p \leq 1 \ (p \in S_0) \end{array}\right\}\right|.$$

Further, we know that

$$\left\{\mathbf{x} \in \mathbb{Z}_S^n : \begin{array}{l} |T_\infty\mathbf{x}| \leq A, \\ |T_p\mathbf{x}|_p \leq 1 \ (p \in S_0) \end{array}\right\} = \{\mathbf{x} \in \mathbb{R}^n : |T_\infty \mathbf{x}| \leq A\} \cap \Lambda$$

where $\Lambda := \left\{\mathbf{x} \in \mathbb{Z}_S^n : \ |T_p\mathbf{x}|_p \leq 1 \ (p \in S_0)\right\}$ is a lattice. Then by Lemma 1.2.3, we have

$$|\{\mathbf{x} \in \mathbb{R}^n : |T_\infty \mathbf{x}| \leq A\} \cap \Lambda| \ll A^n / |\det \mathbf{T}|_S = A^n$$

and hence Lemma 5.3.3 holds. □

Proposition 5.3.4. *Let* $F \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a decomposable form of degree* d. *Assume* $a'(F) < d/n$ *and* $F(\mathbf{z}) \neq 0$ *for all* $\mathbf{z} \in \mathbb{Q}^n \backslash \{0\}$. *Then for any* $D \geq e$, *the set* $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ *lies in the union of a set* $\mathcal{Z}$ *with*

$$|\mathcal{Z}| \ll \left(\frac{m}{m(F)}\right)^{n/d} D^{|S|\cdot(n-1)+2}$$

and at most

$$\ll (1 + \log_D^* m + \log_D^* m(F))^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$.

Proof. Suppose $m(F) = m(F_{\mathbf{T}}) = \mathcal{H}(F_{\mathbf{T}})$ for some $\mathbf{T} \in GL_n(\mathbb{A}_S)$ with $|\det \mathbf{T}|_S = 1$. By Lemma 5.2.3, there exists $M \in GL_n(\mathbb{Z}_S)$ with $\mathcal{H}(F_M) \leq c_5 m(F)^n$.

Let $\epsilon \in \mathbb{Z}_S^*$ such that $G := \epsilon F_M \in \mathbb{Z}[X_1, \dots, X_n]$. Then

$$N_{F,S}(m) = N_{G,S}(m),\ \mu^n(\mathbb{A}_{F,S}(m)) = \mu^n(\mathbb{A}_{G,S}(m)),\ a'(G) = a'(F)$$

and

$$m(G) = m(\epsilon F_M) = m(F) = \mathcal{H}(F_{\mathbf{T}}) = \mathcal{H}(\epsilon F_{\mathbf{T}}) = \mathcal{H}(G_{M^{-1}\mathbf{T}}).$$

Write $\mathbf{T}' = M^{-1}\mathbf{T} \in GL_n(\mathbb{A}_S)$. So $|\det \mathbf{T}'|_S = 1$ and $m(G) = \mathcal{H}(G_{\mathbf{T}'})$. By Lemma 5.2.3, we have

$$\begin{gathered}\mathcal{H}(G) = \mathcal{H}(F_M) \leq c_5 m(F)^n = c_5 m(G)^n, \\ c_6 m(G)^{-1/d} \prod_{p \in S} |\mathbf{x}_p|_p \leq \prod_{p \in S} |T_p'^{-1}(\mathbf{x}_p)|_p \leq c_7 m(G)^{(n-1)/d} \prod_{p \in S} |\mathbf{x}_p|_p \text{ for } (\mathbf{x}_p)_{p \in S} \in \mathbb{A}_S^n. \end{gathered} \tag{5.3.5}$$

Choose l_1 minimal such that $\sqrt{D^{l_1+1}(m/m(G))^{1/d}} \geq \max\{A, B, C\}$ with

$$\begin{aligned} A &= (c_7 m(G)^{(n-1)/d})^{1/2} c_6^{-1} m(G)^{1/d}, \\ B &= (c_7 m(G)^{(n-1)/d})^{1/2} c_5^{1/2} m^{1/(2d)} m(G)^{n/2}, \\ C &= (c_3 m/m(G))^{\frac{1}{d - na'(F)}}. \end{aligned} \tag{5.3.6}$$

Then we have $l_1 \ll 1 + \log_D^* m + \log_D^* m(G)$.

Let $\mathbf{z} \in \mathbb{A}_{G,S}(m) \cap \mathbb{Z}^n$ with

$$\prod_{p \in S} |T_p'^{-1}\mathbf{z}|_p \geq (\frac{m}{m(G)})^{1/d} D^{l_1+1}. \tag{5.3.7}$$

Then by (5.3.5), we have

$$\sqrt{|\mathbf{z}|_\infty} = \sqrt{\prod_{p \in S} |\mathbf{z}|_p} \geq \max\{c_6^{-1} m(G)^{1/d}, c_5^{1/2} m^{1/(2d)} m(G)^{n/2}\}.$$

Hence again by (5.3.5)

$$m^{1/d}\mathcal{H}(G) \le |\mathbf{z}|_\infty = \prod_{p\in S} |\mathbf{z}|_p \le \prod_{p\in S} |T_p'^{-1}\mathbf{z}|_p^2.$$

For $\mathbf{z} \in \mathbb{A}_{G,S}(m) \cap \mathbb{Z}^n$ with (5.3.7), by Lemma 5.2.12, there are linearly independent linear factors $L_{p,i_1(p)}, \dots, L_{p,i_n(p)}$ of G for $p \in S$ such that

$$\begin{aligned}\left(\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{z})|_p \cdots |L_{p,i_n(p)}(\mathbf{z})|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \dots, \mathbf{L}_{p,i_n(p)})|_p}\right)^{a'(G)} &\le c_3 \frac{\prod_{p\in S} |G(\mathbf{z})|_p}{\prod_{p\in S} |T_p'^{-1}\mathbf{z}|_p m(G)} \le \frac{c_3 m}{\prod_{p\in S} |T_p'^{-1}\mathbf{z}|_p m(G)} \\ &\le \frac{1}{\prod_{p\in S} |T_p'^{-1}\mathbf{z}|_p^{(d-na'(G))/2}} \le \frac{1}{\prod_{p\in S} |\mathbf{z}|_p^{(d-na'(G))/4}}.\end{aligned}$$

Thus

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{z})|_p \cdots |L_{p,i_n(p)}(\mathbf{z})|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \dots, \mathbf{L}_{p,i_n(p)})|_p} \le \frac{1}{\prod_{p\in S} |\mathbf{z}|_p^{(d-na'(G))/4a'(G)}} < |\mathbf{z}|_\infty^{-\frac{1}{4d}} \tag{5.3.8}$$

Write $\mathbf{z} = g\mathbf{z}'$ with $\mathbf{z}'$ primitive. Then $g \le m^{1/d}$ and $|\mathbf{z}'|_\infty = |\mathbf{z}|_\infty/g = (\prod_{p\in S} |\mathbf{z}|_p)/g \ge \mathcal{H}(G)$. It is clear that $\mathbf{z}'$ also satisfies (5.3.8). Hence we can apply a version of the quantitative Subspace Theorem such as [6, Corollary] which implies that the primitive integer solutions of the inequality (5.3.8) with $|\mathbf{z}'|_\infty \ge \mathcal{H}(G)$ lie in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$.

For $\mathbf{z} \in \mathbb{A}_{G,S}(m) \cap \mathbb{Z}^n$ with $(\frac{m}{m(G)})^{1/d} \le \prod_{p\in S} |T_p'^{-1}\mathbf{z}|_p \le (\frac{m}{m(G)})^{1/d} D^{l_1+1}$, we apply Proposition 5.3.2 to G and $\mathbf{T}'$, as $m(G_{\mathbf{T}'}) = \mathcal{H}(G_{\mathbf{T}'})$. Then

$$\left\{\mathbf{z} \in \mathbb{Z}^n : \begin{array}{l} \prod_{p\in S} |G(\mathbf{z})|_p \le m, |\mathbf{z}|_p = 1 \ (p \in S_0) \\ (\frac{m}{m(G)})^{1/d} B_0 \le \prod_{p\in S} |T_p^{-1}\mathbf{z}|_p \le (\frac{m}{m(G)})^{1/d} B_0 D^{l_1+1} \end{array}\right\}$$

can be covered by a finite set Ω with

$$|\Omega| \ll (\frac{m}{m(G)})^{n/d} D^{|S|\cdot(n-1)+2} (\sum_{l=0}^{l_1} (l+1)^{|S|(n-1)-1} e^{\frac{-l}{d}}) \ll (\frac{m}{m(G)})^{n/d} D^{|S|\cdot(n-1)+2},$$

and at most

$$\ll (l_1+1)^{|S|(n-1)} \ll (1+\log_D^* m + \log_D^* m(G))^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$.

At last, by Lemma 5.3.3, we know that the number of $\mathbf{z} \in \mathbb{A}_{G,S}(m) \cap \mathbb{Z}^n$ with $\prod_{p\in S} |T_p^{-1\prime}\mathbf{z}|_p \leq (\frac{m}{m(G)})^{1/d}$ and $|\mathbf{z}|_p = 1$ for $p \in S_0$ is at most $\ll (m/m(G))^{n/d}$. □

5.3.1 Theorems about the volume

In this section, we generalize some results from Thunder's paper [21] to the p-adic setting. Let $F \in \mathbb{Z}[X_1,\dots,X_n]$ be a decomposable form and for $p \in S$ write $F = \prod_{i=1}^d L_{pi}$ with $L_{p1},\dots,L_{pd}$ linear forms in $\overline{\mathbb{Q}}_p[X_1,\dots,X_n]$. Let $a_{p1},\dots,a_{pd} \in \overline{\mathbb{Q}}_p$ with $|a_{p1}\dots a_{pd}|_p = 1$ ($p \in S$). Let M_p be the $d \times n$ matrix with rows $a_{p1}\mathbf{L}_{p1},\dots,a_{pd}\mathbf{L}_{pd}$. Denote by $\mathbf{m}_{p1},\dots,\mathbf{m}_{pn}$ the columns of M_p.

Definition 5.3.5. *For each $p \in S$, define*

$$Q_p(F) = \min |\mathbf{m}_{p1} \wedge \cdots \wedge \mathbf{m}_{pn}|_p$$

where the minimum is taken over all $(a_{p1},\dots,a_{pd}) \in \overline{\mathbb{Q}}_p^d$ with $|a_{p1}\dots a_{pd}|_p = 1$. Define

$$Q(F) := \prod_{p\in S} Q_p(F).$$

Lemma 5.3.6. *Suppose that $\mu^n(\mathbb{A}_{F,S})$ is finite. Then*

$$\mu^n(\mathbb{A}_{F,S}) \gg Q(F)^{-1}.$$

Proof. By Lemma 5.2.5 , we have $\mu^n(\mathbb{A}_{F,S}) \gg m(F)^{-n/d}$. By Lemma 5.2.7, we have $m(F)^{n/d} \ll Q(F)$. □

Define

$$M(F) := \min \{\mathcal{H}(F_M) : M \in GL_n(\mathbb{Z}_S)\}.$$

Lemma 5.3.7. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose that $\mu^n(\mathbb{A}_{F,S})$ is finite and $F(\mathbf{z}) \neq 0$ for all $\mathbf{z} \in \mathbb{Q}^n \setminus \{0\}$. Then*

$$M(F)^{1/d} \ll Q(F) \ll M(F)^{n/d}.$$

Proof. By Lemma 5.2.7, we have $m(F)^{n/d} \ll Q(F)$. By Lemma 5.2.3, we have

$$m(F)^n \gg \mathcal{H}(F_m) \geq M(F).$$

Hence $Q(F) \gg M(F)^{1/d}$.

For $p \in S, i = 1, \ldots, d$, let $a_{pi} \in \overline{\mathbb{Q}}_p$ such that $|a_{pi}|_p = H_p(F)^{1/d}/|\mathbf{L}_{pi}|_p$. Then $|a_{p1} \ldots a_{pd}|_p = 1$ $(p \in S)$. By Hadamard's inequality, for each $p \in S$ we have

$$|\det(a_{p,i_1}\mathbf{L}_{p,i_1}, \ldots, a_{p,i_n}\mathbf{L}_{p,i_n})|_p \leq H_p(F)^{n/d}$$

for all $(\mathbf{L}_{p,i_1}, \ldots, \mathbf{L}_{p,i_n}) \in I_p(F)$. Hence $\mathcal{H}(F)^{n/d} \gg Q(F)$. Since it is clear that $Q(F) = Q(F_M)$ for every $M \in GL_n(\mathbb{Z}_S)$, we have $M(F)^{n/d} \gg Q(F)$. □

For $p \in S$, let $(a_{p1}, \ldots, a_{pd}) \in \overline{\mathbb{Q}}_p$ with $|a_{p,1} \ldots a_{p,d}|_p = 1$. Assume that $a(F) < d/n$. So F has n linearly independent linear factors. For each $p \in S$, choose $a_{p,i_1}, \ldots, a_{p,i_n}$ as follows:

Choose $i_1(p)$ such that $|a_{p,i_1(p)}|_p = \max\{|a_{p,1}|_p, \ldots, |a_{p,d}|_p\}$. Choose $i_{j+1}(p)$ such that $|a_{p,i_{j+1}(p)}|_p$ is maximal among those $|a_{p,l}|_p$'s where $L_{p,l}$ is linearly independent of $L_{p,i_1(p)}, \ldots, L_{p,i_j(p)}$. Let $c_{p,1}$ denote the number of $L_{p,i}$ in the $\overline{\mathbb{Q}}_p$-span of $L_{p,i_1(p)}$. For $2 \leq j \leq n$, let $c_{p,j}$ denote the number of $L_{p,i}$ in the $\overline{\mathbb{Q}}_p$-span $L_{p,i_1(p)}, \ldots, L_{p,i_j(p)}$ which are not in the $\overline{\mathbb{Q}}_p$-span of $L_{p,i_1(p)}, \ldots, L_{p,i_{j-1}(p)}$. Then for $1 \leq j \leq n$, $c_{p,1} + \cdots + c_{p,j}$ is the number of $L_{p,i}$ in the span of $L_{p,i_1(p)}, \ldots, L_{p,i_j(p)}$. By the definition of $a(F)$, we know $c_{p,1} + \cdots + c_{p,j} \leq j \cdot a(F)$ $(1 \leq j < n)$ and $c_{p,1} + \cdots + c_{p,n} = d$ for $p \in S$. So for each $p \in S$, we have

$$1 = \prod_{i=1}^{d} |a_{p,i}|_p \leq \prod_{j=1}^{n} |a_{p,i_j(p)}|_p^{c_{p,j}} = \left(\prod_{j=1}^{n-1} |a_{p,i_j(p)}|_p^{c_{p,j}} \right) \cdot |a_{p,i_n(p)}|_p^{na(F) - c_{p,1} + \cdots + c_{p,n-1}} \cdot |a_{p,i_n(p)}|_p^{d - na(F)}.$$

Finally, by Lemma 2.2.3, we have

$$\left(\prod_{j=1}^{n} |a_{p,i_j(p)}|_p\right)^{a(F)} \cdot |a_{p,i_n(p)}|_p^{d-na(F)} \geq 1 \text{ for } p \in S. \tag{5.3.9}$$

For $p \in S$, we define the normalized semi-discriminant by

$$NS(F)_p := \prod_{(\mathbf{L}_{p,i_1},\ldots,\mathbf{L}_{p,i_n}) \in I_p(F)} \frac{|\det(\mathbf{L}_{p,i_1},\ldots,\mathbf{L}_{p,i_n})|_p}{\prod_{j=1}^{n} |\mathbf{L}_{i_j}|_p}$$

where $I_p(F)$ is the set of all ordered n-tuples $(\mathbf{L}_{p,i_1},\ldots,\mathbf{L}_{p,i_n})$ which are $\overline{\mathbb{Q}}_p$-linearly independent. Define

$$NS(F) := \prod_{p\in S} NS(F)_p.$$

Lemma 5.3.8. *Suppose that $a(F) < d/n$ is finite and let $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$ such that $\mathbf{x}_p \neq 0$ $(p \in S)$. Then there are linear independent linear forms $L_{p,i_1(p)},\ldots,L_{p,i_n(p)}$ for $p \in S$ such that*

$$\left(\prod_{p\in S} \frac{|L_{pi_1(p)}(\mathbf{x}_p)|_p \cdots |L_{pi_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)})|_p}\right)^{a(F)} \ll \frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p}{\prod_{p\in S}|\mathbf{x}_p|_p^{d-na(F)} \cdot \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}}.$$

Proof. Without loss of generality, we may assume that $|\mathbf{L}_{p1}|_p = \cdots = |\mathbf{L}_{pd}|_p = 1$ for each $p \in S$, so $H_p(F) = 1$ $(p \in S)$. Since both sides are homogeneous in $\mathbf{x}_p$ for each $p \in S$, we may also assume $|F(\mathbf{x}_p)|_p = 1$ $(p \in S)$. For each $p \in S, i = 1,\ldots,d$, let $a_{pi} \in \overline{\mathbb{Q}}_p^d$ such that $|a_{pi}|_p = |L_{pi}(\mathbf{x}_p)|_p^{-1}$.

By (5.3.9), we have

$$\left(\prod_{j=1}^{n} |L_{p,i_j(p)}(\mathbf{x}_p)|_p\right)^{a(F)} |L_{p,i_n(p)}(\mathbf{x}_p)|_p^{d-na(F)} \leq 1 \ (p \in S).$$

By Lemma 2.2.1, we have

$$|L_{p,i_n(p)}(\mathbf{x}_p)|_p = \max_{j=1,\ldots,n} |L_{p,i_j(p)}(\mathbf{x}_p)|_p \gg |\mathbf{x}_p|_p |\det(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)})|_p \ (p \in S).$$

Hence

$$\left(\prod_{p\in S}\prod_{j=1}^{n}|L_{p,i_j(p)}(\mathbf{x}_p)|_p\right)^{a(F)} \ll \prod_{p\in S}\frac{1}{|\mathbf{x}_p|_p^{d-na(F)}|\det(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)})|_p^{d-na(F)}}. \tag{5.3.10}$$

By Hadamard's inequality and $|\mathbf{L}_{pi}|_p = 1$ ($p \in S, i = 1,\ldots,d$), we know that each factor of $NS(F)$ is ≤ 1 and hence $NS(F) \leq \prod_{p\in S}|\det(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)})|_p)$. Inserting this into (5.3.10), we complete the proof. □

Lemma 5.3.9. *Suppose that $a(F) < d/n$ and let $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n$. Then there are linearly independent linear forms $L_{p,i_1(p)},\ldots,L_{p,i_n(p)}$ for $p \in S$ such that*

$$\prod_{p\in S}\frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p\cdots|L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)})|_p} \ll \frac{\prod_{p\in S}|F(\mathbf{x}_p)|_p^{n/d}}{Q(F)}.$$

Proof. For each $p \in S, i = 1,\ldots,d$, let $a_{pi} \in \overline{\mathbb{Q}}_p^d$ such that $|a_{pi}|_p = |F(\mathbf{x}_p)|_p^{1/d}|L_{pi}(\mathbf{x}_p)|^{-1}$. By definition of $Q(F)$, we have

$$Q(F) \ll \prod_{p\in S}|\det(a_{p,i_1(p)}\mathbf{L}_{p,i_1(p)},\ldots,a_{p,i_n(p)}\mathbf{L}_{p,i_n(p)})|_p$$

for some $(\mathbf{L}_{p,i_1(p)},\ldots,\mathbf{L}_{p,i_n(p)}) \in I_p(F)$ ($p \in S$). Lemma 5.3.9 follows from this. □

Let $B_0 = 0, A_0 = 1$. For $l \geq 1$, put

$$B_l = (NS(F))^{-(d-(n-1)a(F))/(d-na(F))}e^{l-1}, C_l = eB_l \text{ and } A_l = e^{\frac{-l(d-na(F))}{a(f)}}.$$

Define

$$\mathcal{M} := \left\{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l}\prod_{p\in S}|F(\mathbf{x}_p)|_p \leq m, |\mathbf{x}_p|_p = 1\ (p \in S_0),\\ m^{1/d}Q(F)^{-1/n}B_l \leq \prod_{p\in S}|\mathbf{x}_\infty|_\infty \leq m^{1/d}Q(F)^{-1/n}C_l\end{array}\right\}.$$

We consider how well the set $\mathcal{M}$ can be covered by sets of the form

$$\mathcal{C} = \{(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : |K_{pi}(\mathbf{x}_p)|_p \leq a_{pi}\ (p \in S, 1 \leq i \leq n)\} \tag{5.3.11}$$

where $K_{p1}, K_{p2}, \ldots, K_{pn}$ are linear forms in $\mathbb{Q}_p[X_1, \ldots, X_n]$ with

$$|\det(\mathbf{K}_{p1}, \mathbf{K}_{p2}, \ldots, \mathbf{K}_{pn})|_p = 1 \ , \ |\mathbf{K}_{p1}|_p = \cdots = |\mathbf{K}_{pn}|_p = 1$$

and a_{pi} are positive reals with

$$\prod_{p \in S} \prod_{i=1}^{n} a_{pi} \ll \frac{m^{n/d}}{Q(F)} A_l.$$

Lemma 5.3.10. *Assume $a(F) < d/n$. Let $1 \le B < C$, $D > 1$.*

(*a*) *If $l = 0$, $\mathcal{M}$ can be covered by at most $\ll (1 + |\log(NS(F))|)^{|S|n-1}$ convex sets $\mathcal{C}$ of the form* (5.3.11) *with*

$$\prod_{p \in S} \prod_{i=1}^{n} a_{pi} \ll \frac{m^{n/d}}{Q(F)} A_0.$$

(*b*) *If $l > 0$, $\mathcal{M}$ can be covered by at most $\ll (l + |\log(NS(F))|)^{|S|(n-1)-1}$ convex sets $\mathcal{C}$ of the form* (5.3.11) *with*

$$\prod_{p \in S} \prod_{i=1}^{n} a_{pi} \ll \frac{m^{n/d}}{Q(F)} A_l.$$

Proof. (*a*) Let $l = 0$ and $(\mathbf{x}_p)_{p \in S} \in \mathbb{A}_{F,S}(m)$. By Lemma 5.3.9, for each $p \in S$ there are linearly independent linear factors $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ such that

$$\prod_{p \in S} \frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \le c \frac{\prod_{p \in S} |F(\mathbf{x}_p)|_p^{n/d}}{Q(F)} \le \frac{cm^{n/d}}{Q(F)}. \tag{5.3.12}$$

Applying Lemma 2.2.13 with $A = \frac{cm^{n/d}}{Q(F)}, C = \frac{m^{1/d}}{Q(F)^{1/n}} C_0$, we know that the set of $(\mathbf{x}_p)_{p \in S} \in \mathbb{A}_{F,S}(m)$ with $|\mathbf{x}_\infty|_\infty \le \frac{m^{1/d}}{Q(F)^{1/n}} C_0$ satisfying(5.3.12) can be covered by at most $\ll (1 + |\log(NS(F))|)^{|S|n-1}$ convex sets $\mathcal{C}$ of the form (5.3.11) with

$$\prod_{p \in S} \prod_{i=1}^{n} a_{pi} \ll \frac{m^{n/d}}{Q(F)} A_0.$$

For the tuples $(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})$ $(p \in S)$, we have $\ll 1$ possibilities. Hence (*a*) follows.

(*b*) Let $l > 0$ and $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_{F,S}(m)$ with $\frac{m^{1/d}}{Q(F)^{1/n}} B_l \leq |\mathbf{x}_\infty|_\infty \leq \frac{m^{1/d}}{Q(F)^{1/n}} C_l$. By Lemma 5.3.8, there are linear independent linear forms $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ for $p \in S$ such that

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \ll \left(\frac{\prod_{p\in S} |F(\mathbf{x}_p)|_p}{\prod_{p\in S} |\mathbf{x}_p|_p^{d-na(F)} \cdot M(F)(NS(F))^{d-(n-1)a(F)}} \right)^{1/a(F)}.$$

By Lemma 5.3.7, we have $M(F) \gg Q(F)^{d/n}$ and hence

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}_p)|_p \cdots |L_{p,i_n(p)}(\mathbf{x}_p)|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \leq c' A_l \frac{m^{n/d}}{Q(F)} \tag{5.3.13}$$

where c' is a constant depending only on n, d, S.

Apply Lemma 2.2.12 with $A = c' A_l \frac{m^{n/d}}{Q(F)}$, $B = \frac{m^{1/d}}{Q(F)^{1/n}} B_l, C = \frac{m^{1/d}}{Q(F)^{1/n}} C_l$ and $D = e$. Then the set of $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_{F,S}(m)$ with $\frac{m^{1/d}}{Q(F)^{1/n}} B_l \leq |\mathbf{x}_\infty|_\infty \leq \frac{m^{1/d}}{Q(F)^{1/n}} C_l$ satisfying (5.3.13) can be covered by $\ll (\log \frac{BC^{n-1}}{A})^{|S|(n-1)-1} \ll (l + |\log(NS(F))|)^{|S|(n-1)-1}$ convex sets $\mathcal{C}$ of the form (5.3.11) with

$$\prod_{p\in S} \prod_{i=1}^{n} a_{pi} \ll \frac{CA}{B} \ll \frac{m^{n/d}}{Q(F)} A_l.$$

□

Theorem 5.3.11. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Assume $a(F) < d/n$ and $F(\mathbf{z}) \neq 0$ for all $\mathbf{z} \in \mathbb{Q}^n \setminus \{0\}$. Then we have*

(a) $Q(F)^{-1} \ll \mu^n(\mathbb{A}_{F,S}) \ll Q(F)^{-1}(1 + |\log(NS(F))|)^{|S|n-1}$,

(b) $M(F)^{1/d} \ll Q(F) \ll M(F)^{n/d}$,

(c) $M(F)^{-n/d} \ll \mu^n(\mathbb{A}_{F,S}) \ll M(F)^{-1/d}(1 + |\log M(F)|)^{|S|n-1}$.

Proof. (a) By Lemma 1.2.5, for convex set $\mathcal{C}$ of the form (5.3.11) we have $\mu^n(\mathcal{C}) \ll \prod_{p\in S}\prod_{i=1}^{n} a_{pi}$. Applying Lemma 5.3.6 and 5.3.10, we have

$$\begin{aligned}
\frac{m^{n/d}}{Q(F)} &\ll m^{n/d}\mu^n(\mathbb{A}_{F,S}) \\
&\ll \frac{m^{n/d}}{Q(F)}A_0(1+|\log(NS(F))|)^{|S|n-1} + \frac{m^{n/d}}{Q(F)}\left(\sum_{l\geq 1} A_l(l+|\log(NS(F))|)^{|S|(n-1)-1}\right) \\
&\ll \frac{m^{n/d}}{Q(F)}(1+|\log(NS(F))|)^{|S|n-1}\left(\sum_{l\geq 1} l^{|S|(n-1)-1}e^{\frac{-l(d-na(F))}{a(F)}}\right) \\
&\ll \frac{m^{n/d}}{Q(F)}(1+|\log(NS(F))|)^{|S|n-1}.
\end{aligned}$$

(b) This is Lemma 5.3.7.

(c) By Lemma 1.1.8, we have $|\log NF(S)| \ll \log \mathcal{H}(F)$. Then ($a$) and Lemma 5.3.7 imply that

$$\begin{aligned}
M(F)^{-n/d} \ll Q(F)^{-1} \ll \mu^n(\mathbb{A}_{F,S}) &\ll Q(F)^{-1}(1+|\log(NS(F))|)^{|S|n-1} \\
&\ll M(F)^{-1/d}(1+\log M(F))^{|S|n-1}.
\end{aligned}$$

□

Theorem 5.3.12. *Let $F \in \mathbb{Z}[X_1,\dots,X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then we have*

(a) $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ is contained in the union of a set Ω with

$$|\Omega| \ll \frac{m^{n/d}}{Q(F)}(1+\log \mathcal{H}(F))^{|S|n-1}$$

and at most

$$\ll (1+\log m)^{|S|(n-1)} + (\log \mathcal{H}(F))^{|S|n-1}$$

proper linear subspaces of $\mathbb{Q}^n$, and

$$N_{F,S}(m) \ll \frac{m^{n/d}}{\mathcal{H}(F)^{1/d}}(1+\log \mathcal{H}(F))^{|S|n-1} + m^{\frac{n-1}{d}}(1+\log m^{|S|(n-1)} + (\log \mathcal{H}(F))^{|S|n-1}).$$

(b) *Let $\epsilon > 0$ and assume $\mathcal{H}(F)^{1-\epsilon} \geq m^n$. Then $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ is contained in at most $\ll (1+\epsilon^{-1})^{|S|n-1}$ proper linear subspaces of $\mathbb{Q}^n$, and*

$$N_{F,S}(m) \ll m^{\frac{n-1}{d}}(1+\epsilon^{-1})^{|S|n-1}.$$

Proof. (a) Let Ω be the set consisting of solutions of (5.0.1) lying in the convex sets $\mathcal{C}$ of the form (5.3.11) that contain n linearly independent points. Similarly as the estimation of $\mu^n(\mathbb{A}_{F,S}(m))$ in Theorem 5.3.11, we have

$$\Omega \ll \frac{m^{n/d}}{Q(F)} A_0(1+|\log(NS(F))|)^{|S|n-1} + \frac{m^{n/d}}{Q(F)}\left(\sum_{l\geq 1} A_l(l+|\log(NS(F))|)^{|S|(n-1)-1}\right)$$
$$\ll \frac{m^{n/d}}{Q(F)}(l+|\log(NS(F))|)^{|S|n-1}.$$

Let $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \geq \frac{m^{1/d}}{Q(F)^{1/n}} B_l$. Write $\mathbf{x} = g\mathbf{x}'$ with $\mathbf{x}'$ primitive. As usual, we have $g \leq m^{1/d}$ and hence $|\mathbf{x}'|_\infty = \frac{1}{g}|\mathbf{x}|_\infty \geq \frac{B_l}{Q(F)}$. Applying Lemma 5.3.8 to $\mathbf{x}'$, there are linearly independent linear factors $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ ($p \in S$) of F such that

$$\left(\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}')|_p \cdots |L_{p,i_n(p)}(\mathbf{x}')|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p}\right)^{a(F)} \leq \frac{c\prod_{p\in S}|F(\mathbf{x}')|_p}{|\mathbf{x}'|_\infty^{d-na(F)} \cdot \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}}$$
$$\leq \frac{c\cdot m}{|\mathbf{x}'|_\infty^{(d-na(F))/2}\left(\frac{B_l}{Q(F)}\right)^{(d-a(F))/2} \cdot \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}}.$$

Let l_0 be minimal such that

$$\frac{c\cdot m}{\left(\frac{B_{l_0}}{Q(F)}\right)^{(d-a(F))/2} \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}} < 1 \text{ and } |\mathbf{x}'|_\infty \geq \frac{B_{l_0}}{Q(F)} \geq \mathcal{H}(F).$$

Then $l_0 \ll 1 + \log m + |\log(NS(F))| + \log \mathcal{H}(F)$.

Now every $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \geq \frac{m^{1/d}}{Q(F)^{1/n}} B_l$ is proportional to a primitive $\mathbf{x}'$ with $|\mathbf{x}'|_\infty \geq \mathcal{H}(F)$ which satisfies

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}')|_p \cdots |L_{p,i_n(p)}(\mathbf{x}')|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} < |\mathbf{x}'|_\infty^{-\frac{d-na(F)}{a(F)}}. \tag{5.3.14}$$

Now we apply a version of the quantitative Subspace Theorem such as [6, Corollary] which implies that the primitive solutions $\mathbf{x}'$ of (5.3.14) with $|\mathbf{x}'|_\infty \geq \mathcal{H}(F)$ lie in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$.

Now we deal with $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \leq \frac{m^{1/d}}{Q(F)^{1/n}} B_l$. Lemma 5.3.10 implies that these solutions outside of Ω can be covered by at most

$$\begin{aligned}&\ll (1 + |\log(NS(F))|)^{|S|n-1} + \left(\sum_{l=1}^{l_0} (l + |\log(NS(F))|)^{|S|(n-1)-1}\right)\\&\ll 1 + \log m^{|S|(n-1)} + (\log \mathcal{H}(F))^{|S|n-1}\end{aligned}$$

proper subspaces of $\mathbb{Q}^n$.

Applying Theorem 2.1.3, we know

$$\begin{aligned}N_{F,S}(m) &\ll |\Omega| + m^{\frac{n-1}{d}}(1 + \log m^{|S|(n-1)} + (\log \mathcal{H}(F))^{|S|n-1})\\&\ll \frac{m^{n/d}}{\mathcal{H}(F)^{1/d}}(l + \log \mathcal{H}(F))^{|S|n-1} + m^{\frac{n-1}{d}}(1 + \log m^{|S|(n-1)} + (\log \mathcal{H}(F))^{|S|n-1}).\end{aligned}$$

(b) Let $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$. Using Lemma 5.3.7 and 5.3.9, there are linearly independent linear forms $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ for $p \in S$ such that

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}')|_p \cdots |L_{p,i_n(p)}(\mathbf{x}')|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \ll \frac{\prod_{p\in S} |F(\mathbf{x}')|_p^{n/d}}{Q(F)} \ll \frac{m^{n/d}}{\mathcal{H}(F)^{1/d}} \leq c'\mathcal{H}(F)^{-\epsilon/d}.$$

Apply Lemma 2.2.13 with $A = c'\mathcal{H}(F)^{-\epsilon/d}$ and $D = \mathcal{H}(F)^{\frac{\epsilon}{d(|S|n+1)}}$. Then $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \leq C$, where C is chosen later, can be covered by at most $\ll \log_D^*(\frac{C^n}{A})^{|S|n-1}$ sets of the form $\mathcal{C}$ with

$$\prod_{p\in S}\prod_{i=1}^{d} a_{pi} \ll AD^{|S|n+1} \ll 1.$$

Let $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \geq C$. Applying Lemma 5.3.8 to $\mathbf{x}$, there are linearly independent linear forms $L_{p,i_1(p)}, \ldots, L_{p,i_n(p)}$ $(p \in S)$ such that

$$\left(\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x})|_p \cdots |L_{p,i_n(p)}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p}\right)^{a(F)} < \frac{c \cdot \prod_{p\in S} |F(\mathbf{x})|_p}{|\mathbf{x}|_\infty^{d-na(F)} \cdot \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}}$$
$$\leq \frac{c \cdot m}{|\mathbf{x}|_\infty^{(d-na(F))/2} C^{(d-a(F))/2} \cdot \mathcal{H}(F)(NS(F))^{d-(n-1)a(F)}}.$$

Let

$$C = \max\{m^{1/d}\mathcal{H}(F), (c(NS(F))^{(n-1)a(F)-d})^{2/(d-na(F))}\}.$$

First, we have $\log_D^*(\frac{C^n}{A})^{|S|n-1} \ll (1+\epsilon^{-1})^{|S|n-1}$. Hence by Lemma 2.2.13 the set of $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \leq C$ lie in at most $(1+\epsilon^{-1})^{|S|n-1}$ convex sets of the form $\mathcal{C}$ (defined in (5.3.11)) with $\prod_{p\in S}\prod_{i=1}^d a_{pi} \ll 1$. By Lemma 1.2.5, we know that if $\mathcal{C}$ contains n linearly independent points then $\mathcal{C} \cap \mathbb{Z}^n \ll \prod_{p\in S}\prod_{i=1}^n a_{pi} \ll 1$. Thus the set of $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \leq C$ is contained in at most $(1+\epsilon^{-1})^{|S|n-1}$ proper linear subspaces of $\mathbb{Q}^n$.

Second, for $\mathbf{x} \in \mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ with $|\mathbf{x}|_\infty \geq C$ we have

$$\prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x})|_p \cdots |L_{p,i_n(p)}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} < \left(\frac{m}{|\mathbf{x}|_\infty^{(d-na(F))/2}\mathcal{H}(F)}\right)^{1/a(F)} \leq |\mathbf{x}|_\infty^{\frac{-(d-na(F))}{2a(F)}}$$

Write $\mathbf{x} = g\mathbf{x}'$ with $\mathbf{x}'$ primitive. As usual, we have $g \leq m^{1/d}$ and $|\mathbf{x}'|_\infty = \frac{1}{g}|\mathbf{x}|_\infty \geq \mathcal{H}(F)$. Also

$$|\mathbf{x}'|_\infty^{\frac{-(d-na(F))}{2a(F)}} \geq |\mathbf{x}|_\infty^{\frac{-(d-na(F))}{2a(F)}} > \prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x})|_p \cdots |L_{p,i_n(p)}(\mathbf{x})|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p}$$
$$\geq \prod_{p\in S} \frac{|L_{p,i_1(p)}(\mathbf{x}')|_p \cdots |L_{p,i_n(p)}(\mathbf{x}')|_p}{|\det(\mathbf{L}_{p,i_1(p)}, \ldots, \mathbf{L}_{p,i_n(p)})|_p} \quad (5.3.15)$$

Now we apply a version of the quantitative Subspace Theorem such as [6, Corollary] which implies that the primitive solutions of (5.3.15) with $|\mathbf{x}'|_\infty \geq \mathcal{H}(F)$ lie in the union of $\ll 1$ proper subspace of $\mathbb{Q}^n$

Now Theorem 2.1.3 allows us to complete the proof. □

5.3.2 Solutions in subspaces

Proposition 5.3.13. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Let W be a linear subspace of $\mathbb{Q}^n$. There are effectively computable positive constants c_8, c_{10}, c_{11} depending on n, d, S and $0 < c_9 < 1$ depending on n, d such that the following holds:*

(*a*) $N_{F|_W,S}(m) \leq c_8 m^{\frac{\dim W}{d}}$,

(*b*) *if* $\dim W = n-1$ *and* $M(F|_W) \leq m^{c_9}$, *then*

$$c_{10} m^{(n-1)/d} \mu^{n-1}(\mathbb{A}_{F|_W,S}) \leq N_{F|_W,S}(m) \leq c_{11} m^{(n-1)/d} \mu^{n-1}(\mathbb{A}_{F|_W,S}).$$

Proof. (*a*) This follows directly from Theorem 2.1.3.

(*b*) Let for the moment c_9 be any constant with $0 < c_9 < 1$. If $M(F|_W) \leq m^{c_9}$, applying Theorem 2.1.4 (see formula (2.5.1)) to $F|_W$, we obtain

$$\left|N_{F|_W,S}(m) - m^{(n-1)/d} \mu^{n-1}(\mathbb{A}_{F|_W,S})\right| \ll m^{\frac{(1-\epsilon)(n-1)}{d}} (m^{c_9})^{c(F|_W)}$$

for some $0 < \epsilon < 1$. By Theorem 5.3.11, we know

$$m^{(n-1)/d} \mu^{n-1}(\mathbb{A}_{F|_W,S}) \gg m^{(n-1)/d} M(F|_W)^{-(n-1)/d} \gg m^{(n-1)(1-c_9)/d}.$$

Choose c_9 such that $0 < c_9 < \frac{\epsilon(n-1)}{d \cdot c(F|_W)+n-1}$. Then (*b*) follows. □

Corollary 5.3.14. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Assume $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also assume $a'(F) < d/n$ and $a(F_T) < d/\dim T$ for every proper linear subspace of dimension at least 2 of $\mathbb{Q}^n$. If $m(F) \geq m^{2/n}$, then $N_{F,S}(m) \ll m^{(n-1)/d}$.*

Proof. Let $D = m(F)^{\frac{n}{2d(|S|(n-1)+2)}}$. Then $m(F) \geq m^{2/n}$ implies $D \geq m^{\frac{1}{d(|S|(n-1)+2)}}$. By Proposition 5.3.4, the set $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ is contained in the union of a set $\mathcal{Z}$ with

$$|\mathcal{Z}| \ll (\frac{m}{m(F)})^{n/d} D^{|S| \cdot (n-1)+2} = \frac{m^{n/d}}{m(F)^{n/(2d)}} \leq m^{(n-1)/d}$$

and at most

$$\ll (1 + \log_D^* m + \log_D^* m(F))^{|S|(n-1)} \ll 1$$

proper linear subspaces of $\mathbb{Q}^n$. Then Theorem 2.1.3 implies Corollary 5.3.14. $\square$

Proposition 5.3.15. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Let $m \geq 1$ and $1 \leq B \leq m^{c_9}$. Let $W_1, \ldots, W_N$ be distinct subspaces of $\mathbb{Q}^n$ of dimension $n-1$ with $M(F|_{W_i}) \leq B$ $(i = 1, \ldots, N)$ and $\left(\frac{m}{B^{n-1}}\right)^{1/d} \geq c_{12}(N-1)$ where $c_{12} = \frac{2c_8}{c_{11}}$. Then the number of integer solutions $\mathbf{x}$ to (5.0.1) with $\mathbf{x} \in \bigcup_{i=1}^N W_i$ is at least $\frac{1}{2}\sum_{i=1}^N N_{F|_{W_i},S}(m)$. In particular,*

$$N_{F,S}(m) \geq \frac{1}{2}\sum_{i=1}^N N_{F|_{W_i},S}(m).$$

Proof. It is easy to see that the number of integer solutions $\mathbf{x}$ to (5.0.1) with $\mathbf{x} \in \bigcup_{i=1}^N W_i$ is at least

$$\sum_{i=1}^N N_{F|_{W_i},S}(m) - \sum_{i=1}^{N-1}\left(\sum_{j=i+1}^N N_{F|_{W_i \cap W_j},S}(m)\right).$$

By Proposition 5.3.13, we have

$$\sum_{j=i+1}^N N_{F|_{W_i \cap W_j},S}(m) \leq c_8(N-1)m^{(n-2)/d} \text{ for } i = 1, \ldots, N-1.$$

Hence the number of integer solutions that we are considering is at least

$$\sum_{i=1}^N (N_{F|_{W_i},S}(m) - c_8 m^{(n-2)/d}). \tag{5.3.16}$$

On the other hand, by Proposition 5.3.13 and Lemma 5.2.5 we have

$$\begin{aligned}
N_{F|_{W_i},S}(m) &\geq c_{10} m^{\frac{n-1}{d}} \mu^n(\mathbb{A}_{F|_{W_i},S}) \geq c_{11} m^{\frac{n-1}{d}} m(F)^{-\frac{(n-1)}{d}} \\
&\geq c_{11} m^{\frac{n-1}{d}} M(F)^{-\frac{(n-1)}{d}} \geq c_{11} m^{\frac{n-2}{d}} (\frac{m}{B^{n-1}})^{1/d} \\
&\geq 2c_8 m^{\frac{n-1}{d}} \quad \text{for all } i.
\end{aligned}$$

This together with (5.3.16) completes the proof. $\square$

Proposition 5.3.16. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Let $\mathcal{W}$ be a collection of subspaces of $\mathbb{Q}^n$ of dimension $n-1$ with $|\mathcal{W}| = N$. Suppose that $m^{\frac{1}{2d}} \geq M(F)^{\frac{1}{4nd}} \geq c_{12}(N-1)$. Then there is a constant c_{13} depending on n, d such that*

$$\sum_{W \in \mathcal{W}} N_{F|_W,S}(m) \ll m^{\frac{n-1}{d}} + N(m^{\frac{n-1}{d}} M(F)^{-c_{13}} + m^{\frac{n-2}{d}}(1 + \log m)^{|S|n-1}).$$

Proof. Let $B = M(F)^{c_9'}$ where $c_9' = \min\{\frac{c_9}{2n}, \frac{1}{4n(n-1)}\}$. Define

$$\mathcal{W}_1 := \{W \in \mathcal{W} : M(F|_W) \leq B\},$$
$$\mathcal{W}_2 := \{W \in \mathcal{W} : B < M(F|_W) \leq m^{2n}\},$$
$$\mathcal{W}_3 := \{W \in \mathcal{W} : M(F|_W) \geq m^{2n}\}.$$

First, let $m = M(F)^{\frac{1}{2n}}$. Then since $B \leq M(F)^{\frac{1}{4n(n-1)}}$, we have $\left(\frac{m}{B^{n-1}}\right)^{1/d} \geq M(F)^{\frac{1}{4nd}} \geq c_{12}(N-1)$. Also, since $B \leq M(F)^{\frac{c_9}{2n}} \leq m^{c_9}$, Propositions 5.3.13 and 5.3.15 imply that

$$c_{10} m^{\frac{n-1}{d}} \sum_{W \in \mathcal{W}_1} \mu^n(\mathbb{A}_{F|_W,S}) \leq \sum_{W \in \mathcal{W}_1} N_{F|_W,S}(m) \leq 2N_{F,S}(m).$$

Then by Theorem 5.3.12 (b) (take $\epsilon = 1/2$), $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ lies in the union of at most

$$c_{14} \ll 1$$

proper linear subspaces of $\mathbb{Q}^n$, while Proposition 5.3.13 tells us that in each proper linear subspace there are at most $\leq c_8 m^{\frac{n-1}{d}}$ solutions. Therefore, again by Proposition 5.3.13,

$$c_{10} m^{\frac{n-1}{d}} \sum_{W \in \mathcal{W}_1} \mu^{n-1}(\mathbb{A}_{F|_W,S}) \leq \sum_{W \in \mathcal{W}_1} N_{F|_W,S}(m) \leq 2N_{F,S}(m) \leq c_{14} \cdot c_8 m^{\frac{n-1}{d}}$$

and hence

$$\sum_{W \in \mathcal{W}_1} \mu^{n-1}(\mathbb{A}_{F|_W,S}) \ll 1. \tag{5.3.17}$$

Now, let $m \geq M(F)^{\frac{1}{2n}}$. By Proposition 5.3.13 and (5.3.17), we have

$$\sum_{W \in \mathcal{W}_1} N_{F|_W,S}(m) \ll c_{11} m^{(n-1)/d} \sum_{W \in \mathcal{W}_1} \mu^{n-1}(\mathbb{A}_{F|_W,S}) \ll m^{(n-1)/d}. \tag{5.3.18}$$

For $W \in \mathcal{W}_2$, by Theorem 5.3.12 (a) we have

$$\begin{aligned} N_{F|_W,S}(m) \ll & \frac{m^{(n-1)/d}}{M(F|_W)^{1/d}} (1 + \log M(F|_W))^{|S|(n-1)-1} + \\ & m^{\frac{n-2}{d}} \left(1 + \log m^{|S|(n-2)} + (\log M(F|_W))^{|S|(n-1)-1}\right) \\ \ll & \frac{m^{(n-1)/d}}{B^{1/2d}} + m^{\frac{n-2}{d}} \left(1 + \log m^{|S|(n-1)-1}\right). \end{aligned}$$

Thus,

$$\sum_{W \in \mathcal{W}_2} N_{F|_W,S}(m) \leq N \cdot \left(\frac{m^{(n-1)/d}}{B^{1/2d}} + m^{\frac{n-2}{d}} \left(1 + \log m^{|S|(n-1)-1}\right)\right). \tag{5.3.19}$$

For $W \in \mathcal{W}_3$, by Theorem 5.3.12 (b) we have $N_{F|_W,S}(m) \ll m^{\frac{n-2}{d}}$. Hence

$$\sum_{W \in \mathcal{W}_3} N_{F|_W,S}(m) \ll N \cdot m^{\frac{n-2}{d}}. \tag{5.3.20}$$

Proposition 5.3.16 follows from (5.3.18), (5.3.19) and (5.3.20) with $c_{13} = \frac{c_9'}{2d}$. □

5.4 Proof of Theorem 5.0.3

Theorem 5.4.1. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. Then we have*

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll \left(\frac{m}{m(F)^{\frac{na'(F)}{d}}} \right)^{\frac{n-1}{d-a'(F)}} (1 + \log m)^{2d|S|}.$$

Proof. Similarly as in the proof of Proposition 5.3.4, there is $\mathbf{T} \in \mathrm{GL}_n(\mathbb{A}_S)$ with $|\det \mathbf{T}|_S = 1$ such that

$$m(F) = m(F_{\mathbf{T}}) = \mathcal{H}(F_{\mathbf{T}}), \mathcal{H}(F) \ll m(F)^n$$
$$c_6 m(F)^{-1/d} \prod_{p\in S} |\mathbf{x}_p|_p \le \prod_{p\in S} |T_p^{-1}(\mathbf{x}_p)|_p \le c_7 m(F)^{(n-1)/d} \prod_{p\in S} |\mathbf{x}_p|_p \text{ for } (\mathbf{x}_p)_{p\in s} \in \mathbb{A}_S^n.$$

Fix $B_0 \ge 1$ for now. We choose B_0 optimally later in (5.4.1). By Proposition 1.4.6, we have

$$\begin{aligned}
&\left| \left|(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0) \cap \mathbb{Z}^n)\right| - \mu^n(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0))\right| \\
&\ll (m^{1/d}B_0)^{n-1}(1 + \log(\mathcal{H}(F) m^{1/d} B_0))^{dr} \ll (m^{1/d}B_0)^{n-1}(1 + \log(m(F)^n m^{1/d} B_0))^{dr} \\
&\ll (m^{1/d}B_0)^{n-1}(1 + \log m + \log B_0))^{dr}.
\end{aligned}$$

If $(\mathbf{x}_p)_{p\in S} \in \mathbb{A}_{F,S}(m)$ with $|\mathbf{x}_\infty|_\infty \ge c_6^{-1} m^{1/d} B_0$, we have $\prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p \gg (\frac{m}{m(F)})^{1/d} B_0$. Hence we have

$$\begin{aligned}
&\mu^n\left(\left\{ (\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m, |\mathbf{x}_p|_p = 1 \ (p \in S_0), \\ |\mathbf{x}_\infty|_\infty \ge c_6^{-1} m^{1/d} B_0 \end{array} \right\}\right) \\
&\le \mu^n\left(\left\{ (\mathbf{x}_p)_{p\in S} \in \mathbb{A}_S^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{x}_p)|_p \le m, |\mathbf{x}_p|_p = 1 \ (p \in S_0), \\ \prod_{p\in S} |T_p^{-1}\mathbf{x}_p|_p \ge \left(\frac{m}{m(F)}\right)^{1/d} B_0 \end{array} \right\}\right) \\
&\ll (\frac{m}{m(F)})^{n/d}(1 + \log B_0)^{|S|(n-1)-1} B_0^{\frac{-d+na'(F)}{a'(F)}} \ (\text{ by Proposition 5.3.2 with } D = e).
\end{aligned}$$

Therefore,

$$\left|\mu^n(\mathbb{A}_{F,S}(m)) - \mu^n(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0))\right| \ll \left(\frac{m}{m(F)}\right)^{n/d} (1 + \log B_0)^{|S|(n-1)-1} B_0^{\frac{-d+na'(F)}{a'(F)}}.$$

Let l_1 be the same as in (5.3.6). Then we have

$$l_1 \ll 1 + \log m + \log m(F) \ll 1 + \log m.$$

Similar to the proof of Proposition 5.3.4, using the p-adic Subspace Theorem, we know that these $\mathbf{z} \in \mathbb{A}_{G,S}(m) \cap \mathbb{Z}^n$ with $\prod_{p\in S} |T_p^{-1}\mathbf{z}|_p \ge B_0 e^{l_1+1}(\frac{m}{m(H)})^{1/d}$ are contained in the union of $\ll 1$ proper linear subspaces of $\mathbb{Q}^n$.

By Proposition 5.3.2, the set

$$\left\{ \mathbf{z} \in \mathbb{Z}^n : \begin{array}{l} \prod_{p\in S} |F(\mathbf{z})|_p \le m, |\mathbf{z}|_p = 1 \ (p \in S_0), \\ (\frac{m}{m(F)})^{1/d} B_0 \le \prod_{p\in S} |T_p^{-1}\mathbf{z}|_p \le (\frac{m}{m(F)})^{1/d} B_0 e^{l_1+1} \end{array} \right\}$$

can be covered by a finite set Ω with

$$|\Omega| \ll (\frac{m}{m(F)})^{n/d} (1+\log B_0)^{|S|(n-1)-1} B_0^{\frac{-d+na'(F)}{a'(F)}}$$

and

$$\ll (1+\log B_0)^{|S|(n-1)-1} (l_1+1)^{|S|(n-1)} \ll (1+\log B_0)^{|S|(n-1)-1} (1+\log m)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$. Let $\mathcal{W}$ be the collection of these proper subspaces and $N = |\mathcal{W}|$.

Choose B_0 such that

$$(B_0 m^{1/d}) = \left(\frac{m}{m(F)}\right)^{n/d} B_0^{\frac{-d+na'(F)}{a'(F)}}. \tag{5.4.1}$$

Then

$$B_0 = \left(\frac{m}{m(F)^n}\right)^{\frac{a'(F)}{d(d-a'(F))}}, \ (B_0 m^{1/d})^{n-1} = \frac{m^{\frac{n-1}{d-a'(F)}}}{m(F)^{\frac{n(n-1)a'(F)}{d(d-a'(F))}}}.$$

Since $m(F) \le m^{1/n}$, we have $B_0 \ge 1$.

Suppose that $M(F) \ge m^{\frac{1}{4n}}$. If $m^{1/2d} \ge M(F)^{\frac{1}{4nd}} \ge c_{12}(N-1)$, then by Proposition 5.3.16, we have

$$\sum_{W\in\mathcal{W}} N_{F|_W,S}(m) \ll m^{\frac{n-1}{d}} + N(m^{\frac{n-1}{d}} M(F)^{-c_{13}} + m^{\frac{n-2}{d}}(1+\log m)^{|S|n-1}) \ll m^{\frac{n-1}{d}}.$$

If $M(F)^{\frac{1}{4nd}} \ge m^{1/2d}$, then $m \le M(F)^{\frac{1}{2n}} \ll m(F)^{1/2} \le m^{\frac{1}{2n}}$ and hence $m \ll 1$. If $M(F)^{\frac{1}{4nd}} \le c_{12}(N-1)$, then $m^{\frac{1}{16n^2d}} \le M(F)^{\frac{1}{4nd}} \le c_{12}(N-1) \le (1+\log m)^{2|S|(n-1)-1}$, hence also $m \ll 1$. Moreover, since $m \ll 1$ implies $N \ll 1$, we have

$$\sum_{W\in\mathcal{W}} N_{F|_W,S}(m) \ll N \cdot m^{\frac{n-1}{d}} \ll m^{\frac{n-1}{d}}. \tag{5.4.2}$$

Suppose that $M(F) < m^{\frac{1}{4n}}$. Then $m(F) < m^{\frac{1}{4n}}$ and hence

$$(B_0 m^{1/d})^{n-1} = \frac{m^{\frac{n-1}{d-a'(F)}}}{m(F)^{\frac{n(n-1)a'(F)}{d(d-a'(F))}}} > m^{\frac{n-1}{d}} m^{\frac{3a'(F)(n-1)}{4d(d-a'(F))}} \gg m^{\frac{n-1}{d}}(1+\log m)^{2|S|(n-1)-1}.$$

Therefore

$$\sum_{W \in \mathcal{W}} N_{F|_W,S}(m) \ll N m^{\frac{n-1}{d}} \ll m^{\frac{n-1}{d}}(1+\log m)^{2|S|(n-1)-1} \ll (B_0 m^{1/d})^{n-1}.$$

Finally, we have

$$\begin{aligned}&\left|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))\right| \le \left|\mu^n(\mathbb{A}_{F,S}(m)) - \mu^n(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0))\right| + \\ &\left|\,\left|(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0) \cap \mathbb{Z}^n)\right| - \mu^n(\mathbb{A}_{F,S}(m, c_6^{-1} m^{1/d} B_0))\right| + |\Omega| + \sum_{W \in \mathcal{W}} N_{F|_W,S}(m) \\ &\ll \left(\frac{m}{m(F)^{\frac{na'(F)}{d)}}}\right)^{\frac{n-1}{d-a'(F)}} (1+\log m)^{2d|S|}.\end{aligned}$$

□

Theorem 5.4.2. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree d. Suppose $F(\mathbf{x}) \neq 0$ for every non-zero $\mathbf{x} \in \mathbb{Z}^n$. Also suppose $a(F|_T) < \frac{d}{\dim T}$ for every linear subspace T of dimension at least 2 of $\mathbb{Q}^n$. If $a'(F) < d/n$, we have*

$$N_{F,S}(m) \ll \left(\frac{m}{m(F)}\right)^{\frac{n}{d}} + m^{\frac{n-1}{d}}.$$

Proof. If $m(F) \ge m^{2/n}$, then Corollary 5.3.14 implies Theorem 5.4.2.

If $m(F) \le m^{2/n}$, then Proposition 5.3.4 (with $D = e$) implies that $\mathbb{A}_{F,S}(m) \cap \mathbb{Z}^n$ lies in the union of a set $\mathcal{Z}$ with

$$|\mathcal{Z}| \ll \left(\frac{m}{m(F)}\right)^{n/d}$$

and at most

$$\ll (1 + \log^* m + \log^* m(F))^{|S|(n-1)} \ll (1 + \log^* m)^{|S|(n-1)}$$

proper linear subspaces of $\mathbb{Q}^n$. Let $\mathcal{W}$ be the collection of these proper subspaces. Without loss of generality, we assume all these proper subspaces are of dimension $n-1$. If $M(F) \geq m^{1/4n}$, by (5.4.2), we have

$$\sum_{W \in \mathcal{W}} N_{F|_W,S}(m) \ll m^{\frac{n-1}{d}}.$$

If $M(F) < m^{1/4n}$, by Theorem 2.1.3 we have

$$\sum_{W \in \mathcal{W}} N_{F|_W,S}(m) \ll m^{\frac{n-1}{d}} \cdot (1+\log^* m)^{|S|(n-1)} \ll \frac{m^{n/d}}{m^{1/(4d)}} \leq \left(\frac{m}{M(F)}\right)^{n/d} \leq \left(\frac{m}{m(F)}\right)^{n/d}.$$

□

Proof of Theorem 5.0.3. Note that if $\gcd(n,d) = 1$ then $a'(F) < d/n$. If $m(F) \leq m^{1/n}$, Theorem 5.4.1 implies Theorem 5.0.3. If $m(F) \geq m^{1/n}$, Lemma 5.2.5 implies that

$$\mu^n(\mathbb{A}_{F,S}(m)) = m^{n/d} \mu^n(\mathbb{A}_{F,S}) \ll \frac{m^{n/d}}{m(F)^{n/d}} \ll m^{\frac{n-1}{d}}.$$

Theorem 5.4.2 implies that $N_{F,S}(m) \ll m^{(n-1)/d}$. Thus

$$|N_{F,S}(m) - \mu^n(\mathbb{A}_{F,S}(m))| \ll m^{(n-1)/d}.$$

□

Bibliography

[1] M.A. Bean and J.L. Thunder. Isoperimetric inequalities for volumes associated with decomposable forms. *J. London Math. Soc. (2)*, 54(1):39–49, 1996.

[2] S.K. Berberian. *Measure and integration.* AMS Chelsea Publishing, Providence, RI, 2011. Reprint of the 1965 original.

[3] Z.I. Borevich and I.R. Shafarevich. *Théorie des nombres.* 1993.

[4] J.-H. Evertse. The Subspace Theorem of W. M. Schmidt. In *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, volume 1566 of *Lecture Notes in Math.*, pages 31–50. Springer, Berlin, 1993.

[5] J.-H. Evertse. The number of solutions of decomposable form equations. *Invent. Math.*, 122(3):559–601, 1995.

[6] J.-H. Evertse. An improvement of the quantitative Subspace Theorem. *Compositio Math.*, 101(3):225–311, 1996.

[7] J.-H. Evertse. On the norm form inequality $|F(x)| \leq h$. *Publ. Math. Debrecen*, 56(3-4):337–374, 2000.

[8] J.-H. Evertse and K. Győry. The number of families of solutions of decomposable form equations. *Acta Arith.*, 80(4):367–394, 1997.

[9] R.S. de Jong. On p-adic norm form inequalities. *Master Thesis, Leiden*, 1999.

[10] K. Mahler. Zur Approximation algebraischer Zahlen. III. *Acta Math.*, 62(1):91–166, 1933. Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen.

[11] K. Mahler. On Minkowski's theory of reduction of positive definite quadratic forms. *The Quarterly Journal of Mathematics*, os-9(1):259–262, 1938.

[12] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[13] H.P. Schlickewei. Lower bounds for heights on finitely generated groups. *Monatsh. Math.*, 123(2):171–178, 1997.

[14] W.M. Schmidt. Norm form equations. *Ann. of Math. (2)*, 96:526–551, 1972.

[15] W.M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[16] W.M. Schmidt. The number of solutions of norm form equations. *Trans. Amer. Math. Soc.*, 317(1):197–227, 1990.

[17] A. Thue. Über Annherungswerte algebraischer Zahlen. *Journal fr die reine und angewandte Mathematik*, 135:284–305, 1909.

[18] J.L. Thunder. On cubic Thue inequalities and a result of Mahler. *Acta Arith.*, 83(1):31–44, 1998.

[19] J.L. Thunder. Decomposable form inequalities. *Ann. of Math. (2)*, 153(3):767–804, 2001.

[20] J.L. Thunder. Inequalities for decomposable forms of degree $n + 1$ in n variables. *Trans. Amer. Math. Soc.*, 354(10):3855–3868 (electronic), 2002.

[21] J.L. Thunder. Volumes and Diophantine inequalities associated with decomposable forms. *J. Number Theory*, 101(2):294–309, 2003.

[22] J.L. Thunder. Asymptotic estimates for the number of integer solutions to decomposable form inequalities. *Compos. Math.*, 141(2):271–292, 2005.

Abstract

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a *decomposable form*, that is, a homogeneous polynomial of degree d which can be factored into linear forms over $\mathbb{C}$. Denote by $N_F(m)$ the number of integer solutions to the inequality $|F(\mathbf{x})| \leq m$ and by $V_F(m)$ the volume of the set $\{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\}$. In 2001, Thunder [19] proved a conjecture of W.M. Schmidt, stating that, under suitable finiteness conditions, one has

$$N_F(m) \ll m^{n/d}$$

where the implicit constant depends only on n and d. Further, he showed an asymptotic formula

$$N_F(m) = m^{n/d}V(F) + O_F(m^{n/(d+n^{-2})})$$

where, however, the implicit constant depends on F. In subsequent papers, Thunder's concern was to obtain a similar asymptotic formula, but with the upper bound of the error term $|N_F(m) - m^{n/d}V(F)|$ depending only on n and d. In [20] and [22], he managed to prove that if $\gcd(n, d) = 1$, the implicit constant in the error term can indeed be made depending only on n and d.

The main objective of this thesis is to extend Thunder's results to the p-adic setting. Namely, we are interested in solutions to the inequality

$$\begin{gathered} |F(\mathbf{x})| \cdot |F(\mathbf{x})|_{p_1} \ldots |F(\mathbf{x})|_{p_r} \leq m \quad \text{in} \quad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ \text{with} \quad \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \end{gathered} \tag{5.4.3}$$

where $p_1, \ldots, p_r$ are distinct primes and $|\cdot|_p$ denotes the usual p-adic absolute value. Chapter 1 is devoted to the p-adic set-up of this problem and to the proofs of the auxiliary lemmas. Chapter 2 is devoted to extending Thunder's results from [19]. In chapter 3, we show the effectivity of the condition under which the number of solutions of (5.4.3) is finite. Chapter 4 and chapter 5 generalize Thunder's results from [20], [21] and [22].

Samenvatting

De resultaten in dit proefschrift bouwen voort op eerder werk over de zogenaamde *Thue-ongelijkheid*

$$|F(x,y)| \leq m \text{ in } x, y \in \mathbb{Z} \tag{5.4.4}$$

waarbij $F \in \mathbb{Z}[X,Y]$ een homogeen polynoom is dat irreducibel is over $\mathbb{Q}$. Als F van graad 1 is of van graad 2 en van positieve discriminant, dan heeft (5.4.4) voor alle voldoend grote m oneindig veel oplossingen. Als F van graad 2 is en van negatieve discriminant, dan geeft (5.4.4) het binnengebied van een ellips aan, en heeft (5.4.4) dus maar eindig veel oplossingen. Uit een beroemd resultaat van de Noorse wiskundige A. Thue [17], naar wie ongelijkheid (5.4.4) is genoemd, volgt dat (5.4.4) maar eindig veel oplossingen heeft als F graad $d \geq 3$ heeft. In 1933 bewees de Duitse wiskundige K. Mahler [10] een asymptotische fomule voor het aantal oplossingen van (5.4.4), waarin het aantal oplossingen van (5.4.4) wordt vergeleken met de oppervlakte van het gebied in $\mathbb{R}^2$ gegeven door $|F(x,y)| \leq m$. Preciezer gezegd, bewees hij voor het aantal oplossingen $N_F(m)$ van (5.4.4) dat

$$N_F(m) = m^{2/d} V_F + O_F(m^{1/(d-1)}) \text{ als } m \to \infty$$

waarbij V_F de (onder de aannamen eindige) oppervlakte is van het gebied

$$\{\mathbf{x} \in \mathbb{R}^2 : |F(x,y)| \leq 1\}.$$

Hierbij hangt de constante in het O-symbool af van F.

We bekijken nu een generalisatie van (5.4.4) waarbij F een *normvorm* is in $n \geq 3$ variabelen, dat wil zeggen een homogeen polynoom van het type

$$F = cN_{\mathbb{L}/\mathbb{Q}}(\lambda_1 X_1 + \lambda_2 X_2 + \cdots + \lambda_n X_n)$$

waarbij $\lambda_1, \lambda_2, \ldots, \lambda_n$ algebraïsche getallen zijn, $\mathbb{L}$ het door deze getallen voorgebrachte getallenlichaam, en c een rationaal getal ongelijk aan 0 zodat F gehele coëfficiënten heeft.

In 1971 bewees de Oostenrijkse wiskundige W.M. Schmidt [14] dat voor normvormen F die aan een natuurlijke niet-gedegenereerdheidsvoorwaarde voldoen, de *normvorm-ongelijkheid*

$$|F(\mathbf{x})| \leq m \text{ in } \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \tag{5.4.5}$$

maar eindig veel oplossingen heeft. Bijvoorbeeld homogene polynomen in twee variabelen met gehele coëfficiënten die irreducibel zijn over $\mathbb{Q}$ van graad minstens 3 of van graad 2 en met negatieve discriminant zijn normvormen die voldoen aan Schmidt's niet-gedegenereerdheidsvoorwaarde. Evertse gaf in [7] een expliciete bovengrens voor het aantal oplossingen $N_F(m)$ van (5.4.5), namelijk

$$N_F(m) \leq (16d)^{\frac{(n+7)^3}{3}} m^{\frac{n+\sum_{i=2}^{n-1} i^{-1}}{d}} (1+\log m)^{\frac{n(n+1)}{2}},$$

waarbij d de graad is van F.

We bekijken nu meer algemeen ongelijkheden van het type (5.4.5) waarbij F een zogenaamde *ontbindbare vorm* is, dat wil zeggen dat F een homogeen polynoom met gehele coëfficiënten is dat kan worden ontbonden als product van lineaire vormen met coëfficiënten in de algebraïsche afsluiting van $\mathbb{Q}$. Normvormen zijn speciale gevallen hiervan, alsmede alle homogene polynomen in twee variabelen met gehele coëfficiënten, al of niet irreducibel over $\mathbb{Q}$. We geven weer met $N_F(m)$ het aantal oplossingen van (5.4.5) aan, en met V_F het n-dimensionale volume van het gebied

$$\{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\}.$$

In 2001, bewees Thunder [19] een vermoeden van Schmidt dat zegt dat onder de noodzakelijke eindigheidsvoorwaarden

$$\begin{aligned} N_F(m) &\ll_{n,d} m^{n/d}, \\ V_F &\ll_{n,d} 1, \end{aligned} \tag{5.4.6}$$

waarbij d de graad is van F en waarbij de constanten in de Vinogradov-symbolen alleen afhangen van n en d en niet van de coëfficiënten van F. Verder bewees Thunder een asymptotische formule

$$N_F(m) = V_F \cdot m^{n/d} + O_F(m^{n/(d+n^{-2})}) \text{ als } m \to \infty, \tag{5.4.7}$$

waarbij de constante in het O-symbool wel van de coëfficiënten van F afhangt. In latere artikelen bekeek Thunder het probleem om een dergelijke formule af te leiden met een foutterm onafhankelijk van de coëfficiënten van F. In [20] en [22], slaagde hij hier in, in het speciale geval dat n en d relatief priem zijn. Het geval dat n en d niet relatief priem zijn is nog steeds open.

Het doel van dit proefschrift is om de resultaten van Thunder uit te breiden naar p-adische absolute waarden. Preciezer gezegd zijn we geïnteresseerd in afschattingen voor het aantal oplossingen van de ongelijkheid

$$\begin{aligned} |F(\mathbf{x})| \cdot |F(\mathbf{x})|_{p_1} \dots |F(\mathbf{x})|_{p_r} \leq m \quad \text{in} \quad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \\ \text{met} \quad \gcd(x_1, x_2, \dots, x_n, p_1 \cdots p_r) = 1 \end{aligned} \tag{5.4.8}$$

waarbij $p_1, \dots, p_r$ verschillende priemgetallen zijn en $| \cdot |_p$ de gebruikelijke p-adische absolute waarde aangeeft. In hoofdstuk 1 geven we de benodigde definities en bewijzen we enkele hulpresultaten. Hoofdstuk 2 is gewijd aan de generalisaties van (5.4.6) en (5.4.7). In hoofdstuk 3 laten we zien dat de voorwaarden onder welke het aantal oplossingen van (5.4.8) eindig is effectief beslisbaar zijn. In hoofdstuk 4 en hoofdstuk 5 veralgemenen we de resultaten van Thunder uit [20], [21] en [22] en leiden we, in het geval dat n en d relatief priem zijn, asymptotische fomules van het tpye (5.4.7) af waarbij de foutterm onafhankelijk is van de coëfficiënten van F.

Résumé

Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ une *forme décomposable*, c'est-à-dire un polynôme homogène de degré d qui peut être factorisé en formes linéaires sur $\mathbb{C}$. Notons $N_F(m)$ le nombre de solutions entières à l'inégalité $|F(\mathbf{x})| \leq m$ et $V_F(m)$ le volume de l'ensemble $\{\mathbf{x} \in \mathbb{R}^n : |F(\mathbf{x})| \leq m\}$. En 2001, Thunder [19] a prouvé une conjecture de W.M. Schmidt, énonçant que, sous des conditions de finitude appropriées, on a

$$N_F(m) \ll m^{n/d}$$

où la constante implicite ne dépend que de n et d. En outre, il a montré une formule asymptotique

$$N_F(m) = m^{n/d} V(F) + O_F(m^{n/(d+n^{-2})})$$

où, cependant, la constante implicite dépend de F. Dans des articles ultérieurs, la préoccupation de Thunder était d'obtenir une formule asymptotique similaire, mais avec la borne supérieure du terme d'erreur $|N_F(m) - m^{n/d}V(F)|$ ne dépendant que de n et d. Dans [20] et [22], il a réussi à prouver que si $\gcd(n, d) = 1$, la constante implicite dans le terme d'erreur peut en effet être fonction uniquement de n et d.

L'objectif principal de cette thèse est d'étendre les résultats de Thunder au cadre p-adique. À savoir, nous sommes intéressés par les solutions à l'inégalité

$$\begin{aligned} &|F(\mathbf{x})| \cdot |F(\mathbf{x})|_{p_1} \ldots |F(\mathbf{x})|_{p_r} \leq m \quad \text{en} \quad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \\ &\text{avec} \quad \gcd(x_1, x_2, \ldots, x_n, p_1 \cdots p_r) = 1. \end{aligned} \tag{5.4.9}$$

où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $|\cdot|_p$ désigne la valeur absolue p-adique habituelle. Le chapitre 1 est consacré au cadre p-adique de ce problème et aux preuves des lemmes auxiliaires. Le chapitre 2 est consacré à l'extension des résultats de Thunder de [19]. Dans le chapitre 3, nous montrons l'effectivité de la condition sous laquelle le nombre de solutions de (5.4.9) est fini. Le chapitre 4 et le chapitre 5 généralisent les résultats de Thunder dans [20], [21] et [22].

Acknowledgments

First of all, I want to express my greatest gratitude to my advisors Jan-Hendrik and Pascal for proposing me such an interesting subject, guiding me and teaching me from my Master thesis to Ph.D thesis. Without them, this thesis won't exist and I won't be here. I also would like to express my thanks to Peter for being my promotor and helping me out whenever he can.

I am grateful to the promotiecommissie for the time and effort they spent on carefully reading my thesis draft and typing down their helpful comments and corrections.

Taking this opportunity, I want to thank the ALGANT consortium for funding. I am also indebted to all the people in Algant program who ever helped me.

Many thanks goes to the number theory, algebra and geometry group in Leiden and the number theory group in Bordeaux. Especially to Yuri Bilu, Bas Edixhoven, Robin de Jong, Qing Liu, Lenny Taelman and Robert Tijdeman for the nice courses and seminars they teach and their help throughout these years.

I also thank my friends in Algant program for the happy experience and memory we shared during last five years. Especially to Alberto, Andrea, Angela, Chao, Duong, Samuele, Valerio, Novi, Weidong, Jinbi, Albert, Dino, Martin, Pinar, Ziyang, Abtien, Djordjo, Mima, Giulio, Carlo...and all the others.

Last but not least, I thank my parents and my wife for their love and trust. Especially to Bo for the accompanying and supporting of all these years.

Curriculum Vitae

Junjiang Liu was born on 26th October 1988 in Henan, China. In 2005, he started his bachelor in mathematics in Wuhan University. In 2009, he obtained his bachelor diploma and started the Erasmus-Mundus Algant-master program. He studied in Leiden for the first year and spent his second year in Bordeaux where he wrote his master thesis entitled ”On Bilu’s Theorem” under the supervision of Pascal Autissier. At the Algant graduation ceremony in Milan in 2011, he received his master degree from Université Bordeaux I. He was admitted into the Algant-Doc joint Ph.D program in 2011, studying Diophantine Approximation under the supervision of Jan-Hendrik Evertse from Leiden and Pascal Autissier from Bordeaux.