GREATEST COMMON DIVISORS NEAR S-UNITS, APPLICATIONS, AND CONJECTURES ON ARITHMETIC ABELIAN SURFACES

By

Zheng Xiao

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Mathematics – Doctor of Philosophy

2022

ABSTRACT

We bound the greatest common divisor of two coprime multivariable polynomials evaluated at algebraic numbers, generalizing the work of Levin by thickening the group of S-units to allow for points that are merely “close" to S-units. Our inequalities make progress towards conjectured GCD inequalities of Silverman and towards Vojta’s conjecture for blowups. The proofs rely on Schmidt’s Subspace Theorem.

As an application, we prove results on the greatest common divisors of terms from two general linear recurrence sequences, extending the results of Levin, who considered the case where the linear recurrences are simple. In particular, we improve on recent results of Grieve and Wang for general linear recurrences, and bound the exceptional set to a logarithmic region. An example shows that the logarithmic region is necessary.

On abelian surfaces which come from the Jacobians of hyperelliptic curves, we establish a connection between GCD conjectures on the abelian surface and conjectures on the arithmetic discriminant for quadratic points on the associated hyperelliptic curve. It predicts, in particular situations, a stronger inequality than Vojta’s theorem on the arithmetic discriminant. We give some examples of extreme values of the arithmetic discriminant.

ACKNOWLEDGEMENTS

As the author of the thesis, I would like to thank Aaron Levin for many helpful comments on several proofs of the main theorems as well as helping polish the thesis. I would also thank Nathan Grieve and Joseph Silverman for advice on writing and making the reference list.

As a PhD student at Michigan State University, I thank all the staff, faculty and colleagues for creating such a good atmosphere of studying and researching. In particular, I would like to thank my academic committee members: Aaron Levin, George Pappas, Micheal Shapiro and Rajesh Kulkarni not only for offering great graduate courses but also for caring me on both academic and bureaucratic affairs throughout my PhD period.

In the end I would like to thank my parents for their unconditional trust and support. I would like to thank my girlfriend, Siqi Wang, for her timely encouragement, endless patience and love despite the long distance between us. I would like to thank my best friend, Zhihao Zhao, for his company during all these years. I would like to thank my supervisor, Aaron Levin, for not just teaching me math, but also teaching me the attitude towards research and starting me up in my early career. I also thank all my friends, Chuangtian (Armstrong) Guan, Yizhen Zhao, Chen Zhang, Keping Huang, and all other friends,for giving me a happy and unforgettable experience at Michigan State University.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Diophantine approximation

Upper bounds for the greatest common divisor of integers of the form $a^n - 1$ and $b^n - 1$ were first studied by Bugeaud, Corvaja, and Zannier in [3], where they proved the following inequality:

Theorem 1.1.1 (Bugeaud, Corvaja, Zannier [3])**.** *Let a, b be multiplicatively independent integers, and let $\epsilon > 0$. Then, provided n sufficiently large, we have*

$$\log \gcd(a^n - 1, b^n - 1) < \epsilon n.$$

Note that even though the statement is simple, the proof requires Schmidt's Subspace Theorem from Diophantine approximation. Actually, for most of the following works, it is the fundamental ingredient in their proofs.

Corvaja, Zannier [5] and Hernández, Luca [12] subsequently extended Theorem 1.1.1 to S-unit integers:

Theorem 1.1.2 (Corvaja, Zannier [5] and Hernández, Luca [12])**.** *Let $p_1, \ldots, p_t \in \mathbb{Z}$ be prime numbers and let $S = \{\infty, p_1, \ldots, p_t\}$. Then for every $\epsilon > 0$,*

$$\log \gcd(u - 1, v - 1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

for all but finitely many multiplicatively independent S-unit integers $u, v \in \mathbb{Z}_S^*$.

More generally, Corvaja and Zannier proved an inequality in the case of bivariate polynomials.

Theorem 1.1.3 (Corvaja, Zannier [6])**.** *Let $\Gamma \subset \mathbb{G}_m^2(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x, y), g(x, y) \in \bar{\mathbb{Q}}[x, y]$ be nonconstant coprime polynomials such that not both of them*

vanish at $(0,0)$. *For all* $\epsilon > 0$*, there exists a finite union* Z *of translates of proper algebraic subgroups of* $\mathbb{G}_m^2$ *such that*

$$\log \gcd(f(u,v), g(u,v)) < \epsilon \max\{h(u), h(v)\}$$

for all $(u,v) \in \Gamma \setminus Z$.

In recent work of Levin [14], the following result was proven, giving an inequality for greatest common divisors of polynomials evaluated at S-unit points, which is a higher-dimensional version of Corvaja-Zannier's theorem:

Theorem 1.1.4 (Levin [14])**.** *Let* n *be a positive integer. Let* $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ *be a finitely generated group. Let* $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n) \in \bar{\mathbb{Q}}[x_1, \ldots, x_n]$ *be non-constant coprime polynomials such that not both of them vanish at* $(0, \ldots, 0)$. *Let* $h(\alpha)$ *denote the (absolute logarithmic) height of an algebraic number* α. *For all* $\epsilon > 0$*, there exists a finite union* Z *of translates of proper algebraic subgroups of* $\mathbb{G}_m^n$ *such that*

$$\log \gcd(f(u_1, \ldots, u_n), g(u_1, \ldots, u_n)) < \epsilon \max\{h(u_1), \ldots, h(u_n)\}$$

for all $(u_1, \ldots, u_n) \in \Gamma \setminus Z$.

In particular, Γ in Theorem 1.1.4 can be taken as the full set of n-tuples of S-units in a number field k, where S is a finite set places of k containing the archimedean places. In the above statement, log gcd is the generalized logarithmic greatest common divisor, which is defined in Section 2.5.

In a slightly different direction, Luca [15] extended Theorem 1.1.2 to rational numbers u and v that are "close" to being an S-unit. Let u be a non-zero rational number, and S a fixed finite set of primes. We may write u uniquely, up to a sign, in the form $u = u_S \cdot u_{\bar{S}}$, where u_S is a rational number in reduced form having both its numerator and denominator composed of primes in S,

and $u_{\bar{S}}$ is a rational number in reduced form having both its numerator and denominator free of primes from S. Luca proved the following:

Theorem 1.1.5 (Luca [15])**.** *Let S be a finite set of places of $\mathbb{Q}$. For $\epsilon > 0$, there exist three positive constants K_1, K_2, K_3 depending on S and ϵ, such that for any rational numbers u and v satisfying*

$$\log \gcd(u-1, v-1) \geq \epsilon \max\{h(u), h(v)\},$$

one of the following three conditions holds:

(i) $\max\{h_{rat}(u), h_{rat}(v)\} < K_1$,

(ii) $u^i = v^j$ *with* $\max\{|i|, |j|\} < K_2$,

(iii) $\max\{h_{\bar{S}}(u), h_{\bar{S}}(v)\} > K_3 \dfrac{h}{\log h}$,

where $h_{\bar{S}}(u) = h(u_{\bar{S}})$, $h_{rat}\left(\dfrac{x}{y}\right) = \max\left\{\dfrac{h(x)}{h(y)}, \dfrac{h(y)}{h(x)}\right\}$ *and* $h = \max\{h(u), h(v)\}$.

This shows the GCD of two rational integers $u-1$ and $v-1$ cannot be large unless u and v are multiplicatively dependent or have large non-S height. One main theorem of this thesis (Corollary 7.0.4) can also be viewed as a generalization of Theorem 1.1.4 along the lines of Luca's theorem. It is studied as follows.

We want to generalize Theorem 1.1.4 beyond the setting of S-units points. To achieve this goal, we introduce the definition of almost S-units: Roughly speaking, an almost (S, δ)-unit for some set of places S in a number field k is an element $u \in k$ whose dominant part of its height is due to an S-unit.

Definition 1.1.6. For a fixed $\delta > 0$ and a fixed set of places S, if $u \in k^*$, then we say u is an almost (S, δ)-unit if

$$h_{\bar{S}}(u) := \sum_{v \notin S} \lambda_v(u) + \lambda_v\left(\frac{1}{u}\right) \leq \delta h(u)$$

(see Section 2.1 for the definition of λ_v). We denote the set of all almost (S,δ)-units by $k_{S,\delta}$. More generally, let

$$\mathbb{G}_m^n(k)_{S,\delta} := \{\mathbf{u} \in \mathbb{G}_m^n(k) | h_{\bar{S}}(\mathbf{u}) \leq \delta h(\mathbf{u})\},$$

where

$$h_{\bar{S}}(\mathbf{u}) = \sum_{v \notin S} \lambda_v(\mathbf{u}) + \lambda_v\left(\frac{1}{\mathbf{u}}\right).$$

With Definition 1.1.6, we prove the following generalization of Theorem 1.1.4, which shows that $\Gamma = (O_{k,S}^*)^n$ may be "thickened" to $\mathbb{G}_m^n(k)_{S,\delta}$ for some positive δ (depending on ϵ).

Theorem 1.1.7. *(Corollary 7.0.7) Let n be a positive integer and k a number field, $f(x_1,\ldots,x_n)$, $g(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$ be nonconstant coprime polynomials such that not both of them vanish at $(0,\ldots,0)$. For all $\epsilon > 0$, there exists $\delta > 0$ and a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that:*

$$\log \gcd(f(u_1,\ldots,u_n), g(u_1,\ldots,u_n)) < \epsilon \max\{h(u_1),\ldots,h(u_n)\}$$

for all $(u_1,\ldots,u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$.

By Theorem 5 of [8], we may further choose Z so that it is a (possibly infinite) union of positive-dimensional torus cosets.

In fact, we prove the following refinement of Theorem 1.1.7.

Theorem 1.1.8. *(Theorem 7.0.6) Let k be a number field and let S be a finite set of places of k containing the archimedean places. Let $f, g \in k[x_1,\ldots,x_n]$ be coprime polynomials that don't both vanish at the origin $(0,\ldots,0)$. For all $0 < \delta < 1$, there exists a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that*

$$\log \gcd(f(u_1,\ldots,u_n), g(u_1,\ldots,u_n)) < C\delta^{1/2} \sum_{i=1}^{n} h(u_i)$$

for all $\boldsymbol{u} = (u_1,\ldots,u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$ satisfying $h_{\bar{S}}(\boldsymbol{u}) < \delta h(\boldsymbol{u})$, where $C = 6(\deg f + \deg g)n^2$ is a constant.

Theorem 7.0.6 extends Levin's Theorem 1.1.4 from integral points to rational points, and may be viewed as progress towards Vojta's conjecture for certain blown-up varieties. This Theorem gives a GCD inequality of the form similar to what Vojta's Conjecture predicts. Assuming Vojta's Conjecture, Silverman obtained an upper bound for the polynomial GCD in [18]. By properly extending the notions from $\mathbb{Q}$ to a number field, we can compare Silverman's conjectural upper bound with our inequality. More precisely, in Remark 7.0.8 we discuss the relation of Theorem 7.0.6 with conjectured inequalities of Silverman based on Vojta's conjecture. We also note work of Grieve [10] in this direction.

1.2 Linear recurrence sequences

On the other hand, Levin [14] also gave a classification (Theorem 1.2.2) of large GCDs among terms from simple linear recurrence sequences (see also earlier work of Fuchs [9]). A primary goal of our work is to study the case of general linear recurrences (i.e., without the assumption that the linear recurrence is simple). In the case of binary linear recurrences, Luca [15] showed:

Theorem 1.2.1 (Luca [15])**.** *Let a and b be non-zero integers which are multiplicatively independent, and let f, g, f_1 and g_1 be non-zero polynomials with integer coefficients. For every positive integer n set*

$$u_n = f(n)a^n + g(n)$$

and

$$v_n = f_1(n)b^n + g_1(n).$$

Then, for every fixed $\epsilon > 0$ there exists a positive constant $C_\epsilon > 0$ depending on ϵ and on the given data a, b, f, f_1, g and g_1, such that

$$\log \gcd(u_n, v_m) < \epsilon \max\{m, n\}$$

holds for all pairs of positive integers (m, n) with $\max\{m, n\} > C_\epsilon$.

The essential assumption is that a and b are multiplicatively independent integers, which gives a contradiction to condition (ii) of Theorem 1.1.5. Note that Theorem 1.2.1 is proved without the assistance of Schmidt's Subspace Theorem, so one should expect that a stronger result can be proved with the Subspace Theorem applied to general linear recurrence sequences. In fact, a recent result due to Grieve and Wang [11] on general linear recurrences generalized Luca's binary case, and recovered Levin's result 1.2.2 at the same time. We will give an alternative proof of this theorem later.

Levin [14] applied Theorem 1.1.4 to terms from simple linear recurrence sequences, giving a classification of when two such terms may have a large GCD.

Theorem 1.2.2 (Levin [14])**.** *Let*

$$F(m) = \sum_{i=1}^{s} c_i \alpha_i^m,$$

$$G(n) = \sum_{j=1}^{t} d_j \beta_j^n,$$

define two algebraic simple linear recurrence sequences. Let k be a number field such that $c_i, \alpha_i, d_j, \beta_j \in k$ for $i = 1, \ldots, s$, $j = 1, \ldots, t$. Let M_k be the canonical set of places in k. Let

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v, \ldots, |\alpha_s|_v, |\beta_1|_v, \ldots, |\beta_t|_v\} < 1\}.$$

Let $\epsilon > 0$. All but finitely many solutions (m, n) of the inequality

$$\sum_{v \in M_k \setminus S_0} -\log^- \max\{|F(m)|_v, |G(n)|_v\} > \epsilon \max\{m, n\}$$

satisfy one of finitely many linear relations

$$(m, n) = (a_i t + b_i, c_i t + d_i),\ t \in \mathbb{Z},\ i = 1, \ldots, r,$$

where $a_i, b_i, c_i, d_i \in \mathbb{Z}$, $a_i c_i \neq 0$, and the linear recurrences $F(a_i \bullet + b_i)$ and $G(c_i \bullet + d_i)$ have a nontrivial common factor for $i = 1, \ldots, r$.

Grieve and Wang [11] have extended Theorem 1.2.2 to general linear recurrence sequences.

Theorem 1.2.3 (Grieve, Wang [11])**.** *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m)\alpha_i^m,$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n,$$

for $n \in \mathbb{N}$, be algebraic linear recurrence sequences, defined over a number field k, such that their roots generate together a torsion-free multiplicative subgroup Γ of $k^\times$. Suppose that

$$\max_{i,j}\{|\alpha_i|_v, |\beta_j|_v\} \geq 1,$$

for any $v \in M_k$. Let $\epsilon > 0$ and consider the inequality

$$\log \gcd(F(n), G(n)) < \epsilon \max\{m, n\} \qquad (\dagger)$$

for pairs of positive integers $(m, n) \in \mathbb{N}^2$. The following two assertions hold true.

1. *Consider the case that $m = n$. If the inequality $(\dagger)$ is valid for infinitely many positive integers $(n, n) \in \mathbb{N}^2$, then F and G have a non-trivial common factor.*

2. *Consider the case that $m \neq n$. If the inequality $(\dagger)$ is valid for infinitely many pairs of positive integers $(m, n) \in \mathbb{N}^2$, with $m \neq n$, then the roots of F and G are multiplicatively dependent (see Def 8.0.7). Further, in this case, there exist finitely many pairs of integers $(a, b) \in \mathbb{Z}^2$ such that*

$$|ma + nb| = o(\max\{m, n\}).$$

The proof of Theorem 1.2.3 in [11] is based on a “moving targets" version of Theorem 1.1.4. We will give an alternative proof of Theorem 1.2.3 and also give a quantitative improvement in which the error term $o(\max\{m, n\})$ can be controlled as a constant multiple of $\log \max\{m, n\}$.

As an application of the polynomial GCD inequality, we state our main result on linear recurrence sequences:

Theorem 1.2.4. *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m)\alpha_i^m,$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n,$$

define two algebraic linear recurrence sequences. Let k be a number field such that all coefficients of p_i and q_j and α_i, β_j are in k, for $i = 1, \ldots, s$, $j = 1, \ldots, t$. Let

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v, \ldots, |\alpha_s|_v, |\beta_1|_v, \ldots, |\beta_t|_v\} < 1\}.$$

Then all but finitely many solutions (m, n) of the inequality:

$$\sum_{v \in M_k \setminus S_0} -\log^- \max\{|F(m)|_v, |G(n)|_v\} < \epsilon \max\{m, n\}$$

are of the form:

$$(m, n) = (a_i t, b_i t) + (\mu_1, \mu_2), \quad \mu_1, \mu_2 \ll \log t,\ t \in \mathbb{N},\ i = 1, \ldots, r$$

with finitely many choices of nonzero integers (a_i, b_i) .

Moreover, if the roots of F and G are independent (see Def 8.0.7), then the solutions (m, n) satisfy one of the finitely many linear relations:

$$(m, n) = (a_i t + b_i, c_i t + d_i),\ t \in \mathbb{N}, i = 1, \ldots, r$$

where $a_i, b_i, c_i, d_i \in \mathbb{N}, a_i c_i \neq 0$, and the linear recurrences $F(a_i \bullet + b_i)$ and $G(c_i \bullet + d_i)$ have a nontrivial common factor for $i = 1, \ldots, r$.

Example 1.2.5. Under the set up of Theorem 1.2.4, we give an example illustrating the necessity of (μ_1, μ_2) in the statement:

Define the two linear recurrence sequences as: $F(m) = mp^m + 1$, $G(n) = p^n + 1$, where p is a prime. In the notations of Theorem 1.2.4, $S_0 = \emptyset$. Let $\epsilon < \log 2$. It is easily seen that for $(m, n) = (p^k, p^k + k)$, $\forall k \in \mathbb{Z}_{>0}$, $F(m) = p^{p^k+k} + 1 = G(n)$, so the inequality

$$\log \gcd\{|F(m)|, |G(n)|\} = \log(p^{p^k+k} + 1) > \epsilon(p^k + k) = \epsilon \max\{m, n\}$$

holds for infinitely many k and hence infinitely many (m, n). It is easily seen that such pairs (m, n) do not lie on finitely many lines, but do lie in a logarithmic region around the line $x = y$, i.e., for such pairs we may write $(m, n) = (t, t) + (\mu_1, \mu_2)$ with $\mu_1, \mu_2 \ll \log t$ in agreement with Theorem 1.2.4.

1.3 Arithmetic discriminant

Vojta defined the arithmetic discriminant d_a in the proofs of [23] and [21], and an alternative definition is given in the other paper [22] under arithmetic geometry. In [23], he obtained a first estimate of d_a. Later, Vojta successfully proved the Vojta's conjecture [24] replacing $d(P)$, the usual logarithmic discriminant, by $d_a(P)$ in the curve case.

Theorem 1.3.1 (Theorem 4.2.4)**.** *Let C be a curve over a numerb field k and let $\pi : X \to B$ be a regular model, where B is the arithmetic curve corresponding to Spec$\mathbb{O}_k$. Fix an integer $\nu \geq 1$, a real number $\epsilon > 0$, an effective divisor D on X with no multiple components, and a divisor A on X which is ample on the generic fibre. Then for all points $P \in C(k) \setminus Supp(D)$ with $[k(P) : k] \leq \nu$,*

$$m(D, P) + h_K(P) \leq d_a(P) + \epsilon h_A(P) + O(1),$$

where the constant in $O(1)$ depends on X, D, ν, A and ϵ.

The proof gives a deep and extraordinary construction, which somehow has the similar flavor of the proof of Roth's theorem. However this result is not applied widely and needs more attention.

A follow up theorem, proven in [22], gives a finiteness statement for points of bounded degree on curves.

Theorem 1.3.2. *Let $f : C \to \mathbb{P}^1$ be a dominant morphism, let $s \in \mathbb{N}$, and let g be the genus of C. Assume also that*

$$g - 1 > (\deg f)(s - 1).$$

Then the set

$$\{P \in C(\bar{k}) | [k(P) : k] \leq s \text{ and } k(f(P)) = k(P)\}$$

is finite.

Using well-known upper bounds for the gonality of a curve, one immediately finds,

Corollary 1.3.3. *If $g \geq 6$ then there exists a dominant morphism $f : C \to \mathbb{P}^1$ such that the set*

$$\{P \in C(\bar{k}) | [k(P) : k] \leq 2 \text{ and } k(f(P)) = k(P)\}$$

is finite.

Song-Tucker [19] gave a general version of Theorem 1.3.2.

Proposition 1.3.4. *Let C and C' be curves of genus g and g', respectively, defined over a number field k, let ν be a positive integer, and let $f : C \to C'$ be a dominant k-morphism. Assume that*

$$g - 1 > (\nu + g' - 1) \deg f.$$

Then the set

$$\{P \in C(\bar{k}) | [k(P) : K] = \nu \text{ and } k(f(P)) = k(P)\}$$

is finite.

As an application, they obtained a stronger Castelnuovo's genus inequality under certain conditions.

In here, we continue study the connection between the arithmetic discriminant and the GCD conjecture, giving an equivalence of conjectures for quadratic points.

In later chapters, we will give the proofs of the main Diophantine approximation results and the application to linear recurrence sequences, respectively. We will also develope the connection between the GCD conjecture and the conjecture on arithmetic discriminant on quadratic points.

CHAPTER 2

ABSOLUTE VALUES AND HEIGHTS

2.1 Absolute values

Let k be a number field, M_k the set of places of k and O_k the ring of integers of k. For $v \in M_k$, let k_v denote the completion of k with respect to v. Throughout the thesis, we normalize the absolute value $|\cdot|_v$ corresponding to $v \in M_k$ as follows: If v is archimedean and σ is the corresponding embedding $\sigma : k \to \mathbb{C}$, then for $x \in k^*$, $|x|_v = |\sigma(x)|^{|k_v:\mathbb{R}|/|k:\mathbb{Q}|}$; if v is non-archimedean corresponding to a prime ideal $\mathcal{P}$ in O_k which lies above a rational prime p, then it is normalized so that $|p|_v = p^{-|k_v:\mathbb{Q}_p|/|k:\mathbb{Q}|}$. In this notation, we have the product formula:

$$\prod_{v \in M_k} |x|_v = 1$$

for all $x \in k^*$.

Let S be a finite set of places in M_k. The ring of S-integers and the group of S-units are denoted by $O_{k,S}$ and $O_{k,S}^*$ respectively.

2.2 Height functions on projective spaces

We will define height functions as in [13]. For a point $P = (\alpha_0 : \alpha_1 : \cdots : \alpha_n) \in \mathbb{P}^n(k)$, we define its height to be

$$h(P) = \sum_{v \in M_k} \log \max\{|\alpha_0|_v, \ldots, |\alpha_n|_v\}$$

and for any $x \in k$, its height $h(x)$ is defined to be the height of the point $(1 : x)$ in $\mathbb{P}^1(k)$.

Lemma 2.2.1. *We have the following properties of height functions:*

1. *The height $h(P)$ is independent of the choice of homogeneous coordinates for P.*

2. $h(P) \geq 0$ *for all* $P \in \mathbb{P}^n(k)$.

Proposition 2.2.2. *The action of the Galois group on* $\mathbb{P}^n(\bar{\mathbb{Q}})$ *leaves the height invariant.*

The following finiteness theorem is of fundamental importance for the application of height functions in Diophantine geometry.

Theorem 2.2.3 (Northcott property)**.** *For any numbers* $B, D \geq 0$*, the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) | h(P) \leq B, [\mathbb{Q}(P) : Q] \leq D\}$$

is finite. In particular, for any fixed number field k*, the set*

$$\{P \in \mathbb{P}^n(k) | h(P) \leq B\}$$

is finite.

2.3 Height functions on projective varieties

Weil's "Height Machine" constructs a height function associated to every divisor on a projective variety. These height functions satisfy the following properties.

Theorem 2.3.1. *Let* k *be a number field. For every smooth projective variety* V/k *there exists a map*

$$h_V : Div(V) \to \{functions\ V(\bar{k} \to \mathbb{R})\}$$

with the following properties:

1. *(Normalization) Let* $H \subset \mathbb{P}^n$ *be a hyperplane, and let* $h(P)$ *be the absolute logarithmic height on* $\mathbb{P}^n$*. Then*

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1)$$

for all $P \in \mathbb{P}^n(\bar{k})$.

2. *(Functoriality) Let $\phi : V \to W$ be a morphism and let $D \in Div(W)$. Then*

$$h_{V,\phi^* D}(P) = h_{W,D}(\phi(P)) + O(1),$$

for all $P \in V(\bar{k})$

3. *(Additivity) Let $D, E \in Div(V)$. Then*

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1)$$

for all $P \in V(\bar{k})$.

4. *(Linear Equivalence) Let $D, E \in Div(V)$ with D linearly equivalent to E. Then*

$$h_{V,D}(P) = h_{V,E}(P) + O(1)$$

for all $P \in V(\bar{k})$.

5. *(Positivity) Let $D \in Div(V)$ be an effective divisor, and let B be the base locus of the linear system $|D|$. Then*

$$h_{V,D}(P) \geq O(1)$$

for all $P \in (V \setminus B)(\bar{k})$.

6. *(Algebraic Equivalence) Let $D, E \in Div(V)$ with D ample and E algebraically equivalent to 0. Then*

$$\lim_{P \in V(\bar{k}), h_{V,D}(P) \to \infty} \frac{h_{V,E}(P)}{h_{V,D}(P)} = 0.$$

7. *(Finiteness) Let $D \in Div(V)$ be ample. Then for every finite extension k'/k and every constant B, the set*

$$\{P \in V(k') | h_{V,D}(P) \leq B\}$$

is finite.

8. *The height functions $h_{V,D}$ are determined, up to $O(1)$, by normalization, functoriality for embeddings $\phi : V \to \mathbb{P}^n$, and additivity.*

2.4 Local height functions

We now define local height functions. Let V be a projective variety over a number field k. Let D be a Cartier divisor on V and $v \in M_k$. First we define the support of a Cartier divisor $D = (U_\alpha, f_\alpha)_{\alpha \in I}$ to be

$$\mathrm{supp}(D) := \bigcup_\alpha \{x \in U_\alpha | f_\alpha \notin \mathcal{O}^*_{V,x}\},$$

where $\mathcal{O}^*_{V,x}$ is the group of units in the local ring $\mathcal{O}_{V,x}$. For notation convenience, we write

$$V_D = V \setminus \mathrm{supp}(D)$$

for the complement of the support of D. We would like to associate to each place $v \in M_k$ a function

$$\lambda_{D,v} : V_D(k_v) \to \mathbb{R}$$

so that the sum

$$\sum_{v \in M_k} \lambda_{D,v} = h_D$$

for all points in $V_D(k)$. Moreover, the local height functions should be additive in D. If D is a prime divisor, then $\lambda_{D,v}$ should be geometric in the following intuitive sense

$$\lambda_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

To make things precise, we need some definitions. We define an M_k-constant to be a map

$$\gamma : M_k \to \mathbb{R}$$

with the property that $\gamma(v) = 0$ for all but finitely many $v \in M_k$. We say that a real-valued function ϕ on a subset Y of $V(k) \times M_k$ is M_k-bounded if there is an M_k constant γ such that

$$|\phi(P, v)| \leq \gamma(v)$$

for all $(P, v) \in Y$. We will write $O_v(1)$ for an M_k-bounded function. We say a subset Y of $V(k) \times M_k$ is affine M_k-bounded if there is an affine open subset V_0 of V with affine coordinates

$x_1, \ldots, x_n$ such that $Y \subset V_0 \times M_k$ and such that the function

$$V_0(k) \times M_k \to \mathbb{R}, \quad P \mapsto \max_{1 \le i \le n} |x_i(P)|_v,$$

is M_k-bounded on Y. We say the set Y is M_k-bounded if it is a finite union of affine M_k-bounded sets. We are ready to state the local height machine. For $v \in M_k$, let $v(x) = -\log |x|_v$.

Theorem 2.4.1. *Let V/k be a smooth projective variety. For each $D \in Div(V)$ it is possible to assign a function*

$$\lambda_D : \coprod_{v \in M_k} V_D(k_v) \to \mathbb{R},$$

called the local height function with respect to D, such that the following properties hold:

1. *(Normalization) Let $f \in k(V)^*$ be a rational function on V, and let $D = div(f)$ be the divisor of f. Then the difference*

$$\lambda_{D,v}(P) - v(f(P))$$

is an M_k bounded function on every M_k bounded subset of $V_D(k) \times M_k$.

2. *(Additivity) For all $D_1, D_2 \in Div(V)$,*

$$\lambda_{D_1+D_2,v} = \lambda_{D_1,v} + \lambda_{D_2,v} + O_v(1).$$

3. *(Functoriality) Let $\phi : V \to W$ be a morphism of smooth varieties. Then*

$$\lambda_{\phi^* D,v} = \lambda_{D,v} \circ \phi + O_v(1).$$

4. *(Positivity) Let $D \ge 0$ be an effective divisor. Then*

$$\lambda_{D,v} \ge O_v(1).$$

5. *(Local/Global Property) Let $D \in Div(V)$, and let h_D be a Weil height attached to D. Then*

$$h_D(P) = \sum_{v \in M_k} \lambda_{D,v}(P) + O(1)$$

for all $P \in V_D(k)$.

In particular, if D is a hypersurface in $\mathbb{P}^n$ given by a homogeneous polynomial $F(x_0, \ldots, x_n) = 0$ of degree d, we have a choice of local height function

$$\lambda_{D,v}(P) = \log \max_{i=0,\ldots,n} \frac{|\alpha_i|_v^d}{|F(P)|_v} = \log \frac{|P|_v^d}{|F(P)|_v}$$

where P is written in coordinates $(\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n(k) \setminus \mathrm{Supp}(D)$ and $|P|_v = \max_i |\alpha_i|_v$. For any $x \in k$ and $v \in M_k$, we define the local height of x with respect to v to be $\lambda_v(x) = \log \max\{1, |x|_v\}$.

For a point $P = (\alpha_1, \cdots, \alpha_n) \in \mathbb{G}_m^n(k)$ and a place $v \in M_k$, we define its height and local height as $h(P) = \sum_{v \in M_k} \log \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}$ and $\lambda_v(P) = \log \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}$, respectively.

For a finite set of places S, we define the proximity function associated to D to be the

$$m(D, S, P) = \sum_{v \in S} \lambda_{D,v}(P).$$

2.5 Generalized greatest common divisors

One can extend the notion of $\log \gcd(a, b)$ to all algebraic numbers. Note that for a and b integers, we calculate their greatest common divisor as:

$$\begin{aligned}
\log \gcd(a, b) &= \sum_{p \text{ prime}} \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \log p \\
&= - \sum_{v \in M_{\mathbb{Q},\mathrm{fin}}} \log \max\{|a|_v, |b|_v\} \\
&= - \sum_{v \in M_{\mathbb{Q},\mathrm{fin}}} \log^- \max\{|a|_v, |b|_v\}
\end{aligned}$$

where $M_{\mathbb{Q},\mathrm{fin}}$ is the set of nonarchimedean places of $\mathbb{Q}$ and $\log^- z = \min\{0, \log z\}$. Similarly we define $\log^+ z = \max\{0, \log z\}$. With this observation, by adding contributions of archimedean places, the generalized greatest common divisor is defined as:

Definition 2.5.1. Let $a, b \in \bar{\mathbb{Q}}$ be two algebraic numbers, not both zero. We define the generalized logarithmic greatest common divisors of a and b by

$$\log \gcd(a, b) = -\sum_{v \in M_k} \log^- \max\{|a|_v, |b|_v\}$$

where k is any number field containing both a and b.

We will work with this generalized definition in the following chapters.

CHAPTER 3

DIOPHANTINE APPROXIMATION

3.1 Roth's theorem

The fundamental problem in Diophantine approximation is how closely an irrational number can be approximated by a rational number. Precisely, let $a \in \mathbb{R}$ be a given real number, and let $e > 0$ be a given exponent. We ask whether or not the inequality

$$\left| \frac{p}{q} - a \right| \leq \frac{1}{q^e}$$

can have infinitely many solutions in rational numbers $p/q \in \mathbb{Q}$.

Dirichlet, in 1842, showed that we can find rational numbers that are fairly close to a given real number.

Proposition 3.1.1 (Dirichlet)**.** *Let $a \in \mathbb{R}$ with $a \notin \mathbb{Q}$. Then there are infinitely many rational numbers $p/q \in \mathbb{Q}$ satisfying*

$$\left| \frac{p}{q} - a \right| \leq \frac{1}{q^2}.$$

Next result, due to Liouville in 1844, gives an estimate in the other direction.

Proposition 3.1.2 (Liouville)**.** *Let $a \in \bar{\mathbb{Q}}$ be an algebraic number of degree $d = [\mathbb{Q}(a) : \mathbb{Q}] \geq 2$. Fix a constant $\epsilon > 0$. Then there are only finitely many rational numbers $p/q \in \mathbb{Q}$ satisfying*

$$\left| \frac{p}{q} \right| \leq \frac{1}{q^{d+\epsilon}}.$$

Later, Thue (1909) improved d to $d/2 + 1$, Siegel (1921) improved to $2\sqrt{d}$, Gelfand, Dyson (1947) improved to $\sqrt{2d}$, and finally Roth (1955) improved to 2. In fact, the exponent $2 + \epsilon$ is essentially best possible since we already have Dirichlet's result.

Theorem 3.1.3 (Roth)**.** *For every algebraic number a and every $\epsilon > 0$, the inequality*

$$\left|\frac{p}{q} - a\right| \leq \frac{1}{q^{2+\epsilon}}$$

has only finitely many rational solutions $p/q \in \mathbb{Q}$.

A general formulation of Roth's theorem is the following.

Theorem 3.1.4. *Let k be a number field, let $S \subset M_k$ be a finite set of places on k, and assume that each place extends in some way to $\bar{k}$. Let $a \in \bar{k}$ and $\epsilon > 0$ be given. Then there are only finitely many $b \in k$ satisfying the inequality*

$$\prod_{v \in S} \min\{|b - a|_v, 1\} \leq \frac{1}{H_k(b)^{2+\epsilon}}.$$

As an application, we have Siegel's famous theorem on integral points on curves [16]. Let C be a geometrically irreducible affine curve over a number field k and let S be a finite set of places containing archimedean places. We assume that C is given as a closed subvariety of $\mathbb{A}^n_k$.

Let $\pi : \tilde{C}_{\text{aff}} \to C$ be the normalization of C and we extend the affine curve $\tilde{C}_{\text{aff}}$ to a smooth projective curve $\tilde{C}$, which is unique up to isomorphism. The points in $\tilde{C} \setminus \tilde{C}_{\text{aff}}$ are called the points of C at ∞.

Then Siegel's theorem on integral points on curves states:

Theorem 3.1.5 (Siegel)**.** *If $\tilde{C}$ has genus $g > 0$ or C has at least three distinct points at ∞, then C has only finitely many S-integral points.*

3.2 Wirsing's theorem

Instead of taking the approximating elements from a fixed number field, another direction to generalize Roth's theorem is to consider approximation by algebraic numbers of bounded degree. Toward this end, Wirsing [25] proved a generalization of Roth's theorem, which we state in a general form.

Theorem 3.2.1 (Wirsing)**.** *Let S be a finite set of places of a number field k. Let $P_1, \ldots, P_q \in \mathbb{P}^1(k)$ be distinct points and let $D = \sum_{i=1}^{q} P_i$. Let $\epsilon > 0$ and let d be a positive integer. Then for all but finitely many points $P \in \mathbb{P}^1(\bar{k}) \setminus SuppD$ satisfying $[k(P) : k] \leq d$, we have*

$$m(D, S, P) < (2d + \epsilon)h(P).$$

Remark 3.2.2. When $d = 1$, Wirsing's theorem recovers Roth's theorem. It itself is also a special case of Vojta's inequality of arithmetic discriminant (Theorem 4.2.4), with $g = 0$ and ν arbitrary.

3.3 Schmidt's subspace theorem

A powerful tool in Diophantine Approximation is the famous Schmidt's Subspace Theorem, which will be the primary tool used in the proofs of this thesis.

Theorem 3.3.1 (Schmidt's Subspace Theorem)**.** *Let k be a number field and $S \subset M_k$ a finite set of places, $n \in \mathbb{N}$ and $\epsilon > 0$. For every $v \in S$, let $\{L_0^v, \ldots, L_n^v\}$ be a linearly independent set of linear forms in the variables $x_0, \ldots, x_n$ with coefficients in k. Then there are finitely many hyperplanes $T_1, \ldots, T_h$ of $\mathbb{P}_k^n$ such that the set of solutions $\boldsymbol{x} = (x_0 : \ldots : x_n) \in \mathbb{P}_k^n(k)$ of*

$$\sum_{v \in S} \log \prod_{i=0}^{n} \frac{|\boldsymbol{x}|_v}{|L_i^v(\boldsymbol{x})|_v} \geq (n + 1 + \epsilon)h(\boldsymbol{x}) + O(1)$$

is contained in $T_1 \cup \cdots \cup T_h$. If we take D_v to be the sum of divisors defined by L_i^v, $i = 0, \ldots, n$ and let $K_{\mathbb{P}^n}$ be the canonical divisor of $\mathbb{P}^n$, then this inequality can be written as

$$\sum_{v \in S} \lambda_{D_v, v}(\boldsymbol{x}) + h_{K_{\mathbb{P}^n}}(\boldsymbol{x}) \geq \epsilon h(\boldsymbol{x}) + O(1).$$

If H_i^v is the hyperplane defined by L_i^v, then the left-hand side of the inequality may be written as $\sum_{v \in M_k} \sum_{i=0}^{n} \lambda_{H_i^v, v}(x)$ up to $O(1)$.

Remark 3.3.2. A direct application of the Subspace Theorem is the unit equation. We will give a more general version of it later in 6.2.2.

CHAPTER 4

ARITHMETIC DISCRIMINANT

4.1 Arithmetic varieties

In this section, we will deal with arithmetic objects and we will follow Vojta's [22] notations under the general settings of Arakelov geometry.

Definition 4.1.1. An arithmetic variety $\mathcal{X}$ consists of the following:

1. The finite part is a reduced scheme $\mathcal{X}_{\text{fin}}$ which is projective and flat over $\text{Spec}\mathbb{Z}$ and whose generic fibre is smooth. Write $\mathcal{X}_\infty = \mathcal{X}_{\text{fin}} \times_{\text{Spec}\mathbb{Z}} \text{Spec}\mathbb{C}$.

2. The arithmetic part of $\mathcal{X}$ consists of a smooth function

$$\Lambda_{\mathcal{X}} = \Lambda : \mathcal{X}_\infty \times \mathcal{X}_\infty \to \mathbb{R}_{\geq 0},$$

such that $\Lambda(P_1, P_2) = 0$ if and only if $P_1 = P_2$,

$$\Lambda(P_1, P_2) = \Lambda(P_2, P_1),$$

and

$$\Lambda(P_1, P_2) \gg\ll |z_1(P_1) - z_1(P_2)|^2 + \cdots + |z_n(P_1) - z_n(P_2)|^2$$

in a neighborhood of the diagonal, where $z_1, \ldots, z_n$ are local coordinates on some open subset of $\mathcal{X}_\infty$. Thus Λ will be called a distance function. We also require that the form

$$\omega := d_1 d_1^c \Lambda(P, P)$$

be a Kähler form on $\mathcal{X}_\infty$ (where d_1 and d_1^c apply only to the first coordinate). Moreover, let

$$\lambda(P, Q) = -\log \Lambda(P, Q), P \neq Q.$$

A morphism f of arithmetic varieties is a morphism f_{fin} of their finite parts. Arithmetic curves and arithmetic surfaces are arithmetic varieties of relative dimension zero and one, respectively.

For a number field k, let R be its ring of integers, and let B be the arithmetic scheme with $B_{\text{fin}} = \text{Spec}R$ and $\Lambda_B(\sigma, \tau) = 0$ if $\sigma = \tau$ and 1 otherwise, with $\sigma, \tau \in B_\infty$. Note that $B_\infty = \{\sigma : k \hookrightarrow \mathbb{C}\}$. We define the arithmetic curve corresponding to R as the arithmetic curve obtained by using this choice of Λ. An arithmetic variety $\mathcal{X}$ over B is an arithmetic variety $\mathcal{X}$, together with a morphism $\pi : \mathcal{X} \to B$. For $\sigma : k \hookrightarrow \mathbb{C}$, let $\mathcal{X}_\sigma = \mathcal{X}_{\text{fin}} \times_\sigma \mathbb{C}$, so that $\mathcal{X}_\infty = \coprod_{\sigma \in B_\infty} \mathcal{X}_\sigma$. Also, we may refer to fibres of π_{fin} as (non-archimedean) fibres of π. More generally, one should view an arithmetic scheme as a scheme with an additional fibre over the archimedean absolute value of $\mathbb{Q}$. Therefore we inherit the notions of local rings and (non-archimedean and generic) fibres from $\mathcal{X}_{\text{fin}}$.

We also have the arithmetic version of divisors and sheaves.

Definition 4.1.2. An arithmetic divisor D on $\mathcal{X}$ is a divisor D_{fin} on $\mathcal{X}_{\text{fin}}$, together with a smooth function $g_D : \mathcal{X}_\infty \setminus |D_\infty| \to \mathbb{R}$, such that if for all open sets $U \subset \mathcal{X}_\infty$ on which $D_\infty := D_{\text{fin}}|_U$ is locally represented by a function f, the function

$$g_D(P) + \log |f(P)|^2, \ P \notin \text{Supp}(D_\infty)$$

extends to a continuous function of P on all of U.

Definition 4.1.3. An invertible sheaf $\mathcal{L}$ on $\mathcal{X}$ is an invertible sheaf $\mathcal{L}_{\text{fin}}$ on $\mathcal{X}_{\text{fin}}$, provided with a metric on $\mathcal{L}_\infty := \mathcal{L}_{\text{fin}}|_{\mathcal{X}_\infty}$ compatible with the action of complex conjugation.

4.2 Arithmetic discriminants

Let $P \in X(\bar{k})$ be an algebraic point on a regular arithmetic surface X. Let $F = k(P)$. Let B be the arithmetic curve corresponding to $\text{Spec}(\mathcal{O}_F)$, and let $i : B \to E_P$ be the prime horizontal divisor corresponding to P.

Definition 4.2.1. The arithmetic discriminant $d_a(P)$ of P on X is defined by the formula

$$d_a(P) = \frac{\deg i^*\Omega_{E_P/B}}{[F:\mathbb{Q}]}.$$

An alternative characterization of d_a is the following.

Definition 4.2.2. Let $K_{X/B}$ be a divisor corresponding to $\omega_{X/B}$. Then we define

$$d_a(P) := \frac{(E_P.E_P + K_{X/B})}{[F:\mathbb{Q}]}.$$

Note that under this sense, we could write height functions as

$$h_D(P) = \frac{(E_P.D)}{[F:\mathbb{Q}]}.$$

The arithmetic discriminant was initially defined in [23] or [21] using the alternative definition. It is clear that in the function field case, d_a is a function of the arithmetic genus $p_a(E_P)$:

$$d_a(P) = \frac{2p_a(E_P) - 2}{[F:k]} - (2g(B) - 2).$$

Compared to the discriminant defined in [20],

$$d(P) = \frac{\log|D_{F/\mathbb{Q}}|}{[F:\mathbb{Q}]} = \frac{\deg \Omega_{\mathrm{Nor}(E_P)/B}}{[F:\mathbb{Q}]},$$

where $\mathrm{Nor}(E_P)$ is the normalization of E_P. In the function field case, we have

$$d(P) = \frac{2g(\mathrm{Nor}(E_P)) - 2}{[F:k]} - (2g(B) - 2).$$

So the difference between $d_a(P)$ and $d(P)$ is related to the difference between the arithmetic and geometric genera. There are some elementary properties of d_a.

Lemma 4.2.3. *Let X, B, F defined as before. The following hold:*

1. *If X' is another model birational to X, and if P' denotes the point in $X'(\bar{k})$ corresponding to $P \in X(\bar{k})$, then*

$$d_a(P') = d_a(P) + O([F:\mathbb{Q}]).$$

2. *If X' is the model obtained from X by a base change and desingularizing, if P' is similarly defined, and if the base change is linearly disjoint from F, then*

$$d_a(P') = d_a(P) + O([F : \mathbb{Q}]).$$

3. *If $X = \mathbb{P}^1$, then*

$$d_a(P) = (2[F : k] - 2)h(P) + O(1).$$

4. *If $f : X \to Y$ is a morphism of arithmetic surfaces over B, and if $f|_{E_P}$ is generically injective, then*

$$d_S(P) \leq d_a(f(P)).$$

A celebrated result on the arithmetic discriminant by Vojta [24], which can be regarded as a proven weak version of Vojta's conjecture.

Theorem 4.2.4. *Fix an integer $\nu \geq 1$, a real number $\epsilon > 0$, an effective divisor D on X with no multiple components, and a divisor A on X which is ample on the generic fibre. Then for all points $P \in C(k) \setminus Supp(D)$ with $[k(P) : k] \leq \nu$,*

$$m(D, P) + h_K(P) \leq d_a(P) + \epsilon h_A(P) + O(1),$$

where the constant in $O(1)$ depends on X, D, ν, A and ϵ.

CHAPTER 5

TOOLS IN LINEAR RECURRENCE SEQUENCES

Here we give some basic definitions and results involving linear recurrence sequences.

Definition 5.0.1. A linear recurrence is a sequence $a = (a(i))$ of complex numbers satisfying a homogeneous linear recurrence relation

$$a(i+n) = s_1 a(i+n-1) + \cdots + s_{n-1} a(i+1) + s_n a(i),\ i \in \mathbb{N}$$

with constant coefficients $s_j \in \mathbb{C}$.

Definition 5.0.2. The polynomial

$$f(X) = X^n - s_1 X^{n-1} - \cdots - s_{n-1} X - s_n$$

associated to the relation in Definition 5.0.1 is called its characteristic polynomial and the roots of this polynomial are said to be its roots.

Definition 5.0.3. A generalized power sum is a finite polynomial-exponential sum

$$a(i) = \sum_{j=1}^{m} A_j(i) \alpha_j^i,\ i \in \mathbb{N}$$

with polynomial coefficients $A_j(z) \in \mathbb{C}[z]$. The α_j are the roots of the sequence $a(i)$.

It is a well-known fact that every linear recurrence sequence $a(x)$ can be written in the form of a generalized power sum and in fact these two forms are equivalent, see [7]. Throughout this thesis, linear recurrence sequences are presented in the form of a generalized power sum.

The linear recurrence sequence $a(i)$ is called degenerate if it has a pair of distinct roots whose ratio is a root of unity. Otherwise, it is called non-degenerate.

Fix a number field k. Let us define two linear recurrence sequences $F(n)$ and $G(n)$ by generalized power sums

$$F(n) = \sum_{i=1}^{m} A_i(n)\alpha_i^n$$

$$G(n) = \sum_{i=1}^{l} B_i(n)\beta_i^n$$

where $A(n), B(n)$ are polynomials over k and α_i and β_i are roots in k^*. Let Γ be the multiplicative group generated by all α_i and β_i with a set of generators $\{u_1, \ldots, u_r\}$. Then we can write $F(n)$ and $G(n)$ as

$$F(n) = f(n, u_1^n, \ldots, u_r^n)$$

$$G(n) = g(n, u_1^n, \ldots, u_r^n)$$

where f and g are rational functions in $x_0, \ldots, x_r$ of the form:

$$f(x_0, \ldots, x_r) = \frac{\tilde{f}(x_0, \ldots, x_r)}{x_1^{a_1} \cdots x_r^{a_r}}$$

$$g(x_0, \ldots, x_r) = \frac{\tilde{g}(x_0, \ldots, x_r)}{x_1^{b_1} \cdots x_r^{b_r}}$$

with $\tilde{f}, \tilde{g}$ polynomials, i.e., $f, g \in k[x_0, x_0^{-1}, \ldots, x_r, x_r^{-1}]$ are Laurent polynomials. In particular, the ring of such Laurent polynomials is a localization of $k[x_0, \ldots, x_r]$, so it is a UFD.

It is obvious that linear recurrence sequences are closed under term-wise sum and product from the generalized power sum point of view, hence we can talk about the sum and product of two recurrence sequences. Let $\mathcal{H}_\Gamma(k)$ be the ring of linear recurrence sequences whose coefficient polynomials are over k and roots belonging to a torsion-free multiplicative group $\Gamma \subset k^*$. We say $F(n), G(n) \in \mathcal{H}_\Gamma(k)$ are coprime if there does not exist a non-unit $H(n) \in \mathcal{H}_\Gamma(k)$ such that $F(n) = H(n)F_0(n)$ and $G(n) = H(n)G_0(n)$ with $F_0(n), G_0(n) \in \mathcal{H}_\Gamma(k)$. Recall that for $F(n), G(n) \in \mathcal{H}_\Gamma(k)$ and a choice of generators of the torsion-free group Γ, there are associated Laurent polynomials f and g respectively; if two such recurrence sequences are coprime then

the two associated Laurent polynomials are also coprime.

We also need a well-known theorem on the structure of the zeros of a linear recurrence:

Theorem 5.0.4 (Skolem-Mahler-Lech)**.** *The set of indices of the zeros of a linear recurrence sequence comprises a finite set together with a finite number of arithmetic progressions. If the linear recurrence sequence is nondegenerate, then there are only finitely many zeros.*

CHAPTER 6

ALMOST S-UNITS AND ALMOST S-UNIT EQUATIONS

6.1 Compatible definitions

The definition of almost S, δ-units was already given as in Definition 1.1.6. Here are some remarks about this definition and its properties.

Remark 6.1.1. Silverman has defined "quasi-S-integers" in [17]. For a number field k, a finite set of places S and $\epsilon > 0$, the set of quasi-S-integers are defined as

$$R_S(\epsilon) := \{x \in k : \sum_{v \in S} \max\{|x|_v, 0\} \geq \epsilon h(x)\}.$$

Silverman's notion of quasi-S-integers can be compared with our notion of almost (S, δ)-units as follows: if $x \in k_{S,1-\epsilon}$ then $x \in R_S(\epsilon)$, and if $x \in R_S(\epsilon)$ then $x \in k_{S,2-\epsilon}$.

Remark 6.1.2. We note that $k^n_{S,\delta} \subset \mathbb{G}^n_m(k)_{S,n\delta}$ and when $\delta = 0$ we recover n-tuples of S-units, $G^n_m(k)_{S,0} = (O^*_{k,S})^n$.

Remark 6.1.3. We use projective height to define almost S-units in $\mathbb{G}^n_m(k)_{S,\delta}$. In other references standard height is frequently used, where for a point $P = (x_1, \ldots, x_n) \in \mathbb{G}^n_m(k)_{S,\delta}$,

$$h_{stand}(P) := \sum_{i=1}^{n} h(x_n).$$

Local heights are defined similarly as

$$\lambda_{stand,v}(P) := \sum_{i=1}^{n} \lambda_v(x_n).$$

One can verify that if $P \in \mathbb{G}^n_m(k)$ is an (S, δ)-unit under the projective height, then it is an

$(S, n\delta)$-unit under the standard height. Indeed, in this case we have

$$\begin{aligned}\sum_{v\notin S}\lambda_{stand,v}(P)+\lambda_{stand,v}(1/P) &= \sum_{v\notin S}(\sum_{i=1}^{n}\lambda_v(x_i)+\lambda_v(1/x_i))\\ &\le n\sum_{v\notin S}\lambda_v(P)+\lambda_v(1/P)\\ &\le n\delta h(P)\le n\delta h_{stand}(P).\end{aligned}$$

6.2 Almost S-unit equation theorem

Before the main proof, we need a generalized version of the unit equation.

Lemma 6.2.1. *Let k be a number field and let S be a finite set of places of k containing all archimedean places. Let $0<\delta<1/((n+1)(n+2))$. Let χ be the set of solutions of*

$$x_0+\cdots+x_n=1,\ (x_0,\ldots,x_n)\in k_{S,\delta}^{n+1},$$

such that no proper subsum of $x_0+\cdots+x_n$ vanishes. Then χ is a finite set.

Proof. Let $(a_0,\ldots,a_n)$ be a solution in $k_{S,\delta}^{n+1}$ and $P=(a_0:\ldots:a_n)\in\mathbb{P}^n$. Let H_i, $i=0,\ldots,n$ be hyperplanes defined by $x_i=0$, H_{n+1} be the hyperplane defined by $x_0+\cdots+x_n=0$. Let $P'=(a_0,\ldots,a_n)$. Note that every coordinate of P' is in $k_{S,\delta}$, and by easy calculations and Remark 6.1.2, we know $P'\in\mathbb{G}_m^{n+1}(k)_{S,(n+1)\delta}$. By triangle inequalities, for any $v\in M_{k,\infty}$,

$$|1|_v=|a_0+\cdots+a_n|_v\le(n+1)\max_i|a_i|_v,$$

and for $v\notin M_{k,\infty}$

$$|1|_v=|a_0+\cdots+a_n|_v\le\max_i|a_i|_v.$$

It follows that for all $v\in M_k$

$$h(P')=h(P)+O(1)\text{ and }\lambda_v(P')=\lambda_v(P)+O(1).$$

Hence we get

$$\sum_{i=0}^{n+1} \sum_{v \in S} \lambda_{H_i,v}(P) \geq (n+2-(n+1)(n+2)\delta)h(P) + O(1).$$

Applying the Subspace theorem, we have

$$(n+2-(n+1)(n+2)\delta)h(P) \leq (n+1+\epsilon)h(P) + O(1)$$

unless P lies in some certain proper linear subspaces of $\mathbb{P}^n$. For a fixed $\delta < 1/((n+1)(n+2))$, taking ϵ sufficiently small, the above implies such P is contained in a finite union of hyperplanes in $\mathbb{P}^n$. If $n = 1$, we are done. Otherwise, we proceed by induction as in the proof of the standard unit equation [2, Theorem 7.4.2]. □

Corollary 6.2.2. *Let $0 < \delta < 1/((n+1)(n+2))$. Let χ be the set of solutions of*

$$x_0 + \cdots + x_n = 1$$

such that $(x_0, \ldots, x_n) \in k_{S,\delta}^{n+1}$. Then there is a finite set $\mathcal{F} \subset k^*$ such that every $\boldsymbol{x} \in \chi$ has at least one coordinate in $\mathcal{F}$.

Proof. The proof follows from Lemma 6.2.1 and induction.

□

Lemma 6.2.1 and Corollary 6.2.2 together give the generalized unit equation for $k_{S,\delta}^n$, which allows us to obtain finiteness of solutions in several of the following theorems.

CHAPTER 7

PROOFS OF DIOPHANTINE APPROXIMATION THEOREMS

In this section, our main goal is to give the proof of Theorem 1.1.7.

In the following we will use the notation $\mathbf{u}$ and $\mathbf{i}$ for n-tuples $(u_1, \ldots, u_n)$ and $(i_1, \ldots, i_n)$, respectively, with $|\mathbf{i}| = i_1 + \cdots + i_n$ and denote by $\mathbf{u}^{\mathbf{i}}$ the multi-variable monomial $u_1^{i_1} \cdots u_n^{i_n}$. Let m be a positive integer. For a subset $T \subset k[x_1, \ldots, x_n]$, we let

$$T_m = \{p \in T | \deg p \leq m\},$$

and

$$T_{[m]} = \{p \in T | p \text{ is homogeneous of degree } m\}.$$

For $f, g \in k[x_1, \ldots, x_n]$, we let

$$(f, g)_{(m)} = \{fp + gq | \deg fp, \deg gq \leq m\},$$

where deg denotes the (total) degrees of the polynomials.

Before the proof, we need a combinatorial lemma.

Lemma 7.0.1. *Let m be a positive integer. Let $I = \{\mathbf{i} = (i_0, \ldots, i_n)\}$ be the set of $(n+1)$-tuples in $\mathbb{N}^{n+1}$ with $i_0 + \cdots + i_n = m$. Then*

$$\sum_{\mathbf{i} \in I} \mathbf{i} = \frac{m\binom{n+m}{n}}{n+1}(1, \ldots, 1)$$

where addition and scalar multiplication are coordinate-wise.

We also need Lemma 2.1 from [Corvaja et al.].

Lemma 7.0.2. *Let $F_1, F_2 \in k[x_0, \ldots, x_n]$ be coprime homogeneous polynomials of degrees d_1 and d_2, respectively. Let $B \subset k[x_0, \ldots, x_n]_{[m]}$ be a set of monomials of degree m whose images are linearly independent in $k[x_0, \ldots, x_n]_{[m]}/(F_1, F_2)_{[m]}$. Then*

$$\begin{aligned}\sum_{\mathbf{x}^\mathbf{j} \in B} ord_{x_i} \mathbf{x}^\mathbf{j} &\leq \binom{m+n}{n+1} - \binom{m+n-d_1}{n+1} - \binom{m+n-d_2}{n+1} + \binom{m+n-d_1-d_2}{n+1} \\ &\leq d_1 d_2 \binom{m+n-2}{n-1}\end{aligned}$$

for $i = 0, \ldots, n$.

Proof. Let $S = k[x_0, \ldots, x_n]$. For an $l \in \mathbb{N}$ and a graded module M over S, let $d_M(l) = \dim_k M_{[l]}$. Let I be an ideal generated by a homogeneous polynomial of degree i. By the well-known theory of Hilbert polynomials, $d_{S/I}(l) = d_S(l) - d_S(l-i)$. In this case,

$$\begin{aligned}\dim(S_{[l]}/(F_1, F_2)_{[l]}) &= d_{S/(F_1)}(l) - d_{S/(F_1)}(l - d_2) \\ &= d_S(l) - d_S(l-d_1) - (d_S(l-d_2) - d_S(l-d_1-d_2)) \\ &= \binom{l+n}{n} - \binom{l+n-d_1}{n} - \binom{l+n-d_2}{n} + \binom{l+n-d_1-d_2}{n}.\end{aligned}$$

Let $i \in \{0, \ldots, n\}$, let $S'_{[l]}$ be the image of $x_i^l k[x_0, \ldots, x_n]_{[m-l]}$ in $S_{[m]}/(F_1, F_2)_{[m]}$. Notice that

$$\sum_{\mathbf{x}^\mathbf{j} \in B} \operatorname{ord}_{x_i} \mathbf{x}^\mathbf{j} \leq \sum_{j=1}^{m} j(\dim S'_{[j]} - \dim S'_{[j+1]}) = \sum_{j=1}^{m} \dim S'_{[j]},$$

and that $\dim S'_{[l]} \leq \dim S_{[m-l]}/(F_1, F_2)_{[m-l]}$, hence we have

$$\sum_{\mathbf{x}^\mathbf{j} \in B} \operatorname{ord}_{x_i} \mathbf{x}^\mathbf{j} \leq \sum_{j=0}^{m-1} \dim S_{[j]}/(F_1, F_2)_{[j]}.$$

Using Pascal's identity for binomial coefficients,

$$\begin{aligned}\sum_{\mathbf{x}^\mathbf{j} \in B} \operatorname{ord}_{x_i} \mathbf{x}^\mathbf{j} &\leq \binom{m+n}{n+1} - \binom{m+n-d_1}{n+1} - \binom{m+n-d_2}{n+1} + \binom{m+n-d_1-d_2}{n+1} \\ &\leq d_1 d_2 \binom{m+n-2}{n-1}.\end{aligned}$$

□

Theorem 7.0.3. *Let k be a number field and let S be a finite set of places of k containing the archimedean places. Let $f, g \in k[x_1, \ldots, x_n]$ be coprime polynomials. For all $0 < \delta < 1$, there exists a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that*

$$-\sum_{v \in M_k \setminus S} \log^- \max\{|f(u_1, \ldots, u_n)|_v, |g(u_1, \ldots, u_n)|_v\} < C\delta^{1/2} \sum_{1 \le i \le n} h(u_i)$$

for all $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$, where $C = 2(n^2 \deg f + n \deg g)$ is a constant.

Proof. This proof is modeled on the proof of Theorem 3.2 of [14].

Consider the ideal $(f, g) \subset k[x_1, \ldots, x_n]$. We first assume that $(f, g)_{(m)} \neq k[x_1, \ldots, x_n]_m$. It follows that the k-vector space $V_m = k[x_1, \ldots, x_n]_m/(f, g)_{(m)}$ is not trivial. Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta}$. For $v \in S$, we construct a basis B_v for V_m as follows. Choose a monomial $\mathbf{x}^{\mathbf{i}_1} \in k[x_1, \ldots, x_n]_m$ so that $|\mathbf{u}^{\mathbf{i}_1}|_v$ is minimal subject to the condition $\mathbf{x}^{\mathbf{i}_1} \notin (f, g)_{(m)}$. Suppose now that $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_j}$ have been constructed and are linearly independent modulo $(f, g)_{(m)}$, but don't span $k[x_1, \ldots, x_n]_m$ modulo $(f, g)_{(m)}$. Then we let $\mathbf{x}^{\mathbf{i}_{j+1}} \in k[x_1, \ldots, x_n]_m$ be a monomial such that $|\mathbf{u}^{\mathbf{i}_{j+1}}|_v$ is minimal subject to the condition that $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_{j+1}}$ are linearly independent modulo $(f, g)_{(m)}$. In this way, we construct a basis of V_m with monomial representatives $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_{N'}}$, where $N' = N'_m = \dim V_m$. Let $I_v = \{\mathbf{i}_1, \ldots, \mathbf{i}_{N'}\}$. We also choose a basis $\phi_1, \ldots, \phi_N$ of the vector space $(f, g)_{(m)}$, where $N = N_m = \dim(f, g)_{(m)}$. Now for $\mathbf{i}$, $|\mathbf{i}| \le m$, we have that

$$\mathbf{x}^{\mathbf{i}} + \sum_{j=1}^{N'} c_{\mathbf{i},j} \mathbf{x}^{\mathbf{i}_j} \in (f, g)_{(m)}$$

for some choice of coefficients $c_{\mathbf{i},j} \in k$. Then for each such $\mathbf{i}$ there is a linear form $L_{\mathbf{i}}^v$ over k such that

$$L_{\mathbf{i}}^v(\phi_1, \ldots, \phi_N) = \mathbf{x}^{\mathbf{i}} + \sum_{j=1}^{N'} c_{\mathbf{i},j} \mathbf{x}^{\mathbf{i}_j}.$$

Note that $\{L^v_{\mathbf{i}}(\phi_1, \ldots, \phi_N) : |\mathbf{i}| \leq m, \mathbf{i} \notin I_v\}$ is a basis for $(f, g)_{(m)}$, and $\{L^v_{\mathbf{i}} : |\mathbf{i}| \leq m, \mathbf{i} \notin I_v\}$ is a set of N linearly independent forms in N variables. Let

$$P = \phi(\mathbf{u}) := (\phi_1(\mathbf{u}), \ldots, \phi_N(\mathbf{u})) \in k^N.$$

We may additionally assume that $\phi(\mathbf{u}) \neq 0$ (by enlarging the set Z). From the triangle inequality and the definition of $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_{N'}}$, for any $\mathbf{i}$ with $|\mathbf{i}| \leq m$, $\mathbf{i} \notin I_v$, we have the key inequality

$$\log |L^v_{\mathbf{i}}(P)|_v \leq \log |\mathbf{u}^{\mathbf{i}}|_v + C_v$$

where the constant C_v depends only on $v \in S$ and the set $\{\mathbf{i}_1, \ldots, \mathbf{i}_{N'}\}$ (and not on $\mathbf{u}$).

We will apply the Subspace Theorem with the choice of linear forms $L^v_{\mathbf{i}}$, $|\mathbf{i}| \leq m$, $\mathbf{i} \notin I_v$, for each $v \in S$. We want to estimate the sum

$$\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin I_v} \log \frac{|P|_v}{|L^v_{\mathbf{i}}(P)|_v}.$$

Towards this end, we estimate the sums

$$-\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin I_v} \log |L^v_{\mathbf{i}}(P)|_v \text{ and } \sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin I_v} \log |P|_v$$

separately.

We have

$$-\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin \mathbf{I}_v} \log |L^v_{\mathbf{i}}(P)|_v \geq -\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin \mathbf{I}_v} \log |\mathbf{u}^{\mathbf{i}}|_v - CN$$

where $C = \sum_{v \in S} C_v$. By the product formula,

$$\sum_{v \in S} \log |\mathbf{u}^{\mathbf{i}}|_v + \sum_{v \in M_k \setminus S} \log |\mathbf{u}^{\mathbf{i}}|_v = \sum_{v \in M_k} \log |\mathbf{u}^{\mathbf{i}}|_v = 0.$$

It follows that,

$$\begin{aligned} -\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin \mathbf{I}_v} \log |\mathbf{u}^{\mathbf{i}}|_v &= -\sum_{v \in S} \sum_{|\mathbf{i}| \leq m} \log |\mathbf{u}^{\mathbf{i}}|_v + \sum_{v \in S} \sum_{\mathbf{i} \in \mathbf{I}_v} \log |\mathbf{u}^{\mathbf{i}}|_v \\ &= \sum_{v \in S} \sum_{\mathbf{i} \in \mathbf{I}_v} \log |\mathbf{u}^{\mathbf{i}}|_v + \sum_{v \in M_k \setminus S} \sum_{|\mathbf{i}| \leq m} \log |\mathbf{u}^{\mathbf{i}}|_v. \end{aligned}$$

Let $d_1 = \deg f$ and $d_2 = \deg g$. By Lemma 7.0.2, we have

$$-\sum_{v\in S}\sum_{\mathbf{i}\in\mathbf{I}_v}\log|\mathbf{u}^{\mathbf{i}}|_v \le d_1d_2\binom{m+n-2}{n-1}\sum_{1\le i\le n}h(u_i),$$

we find that,

$$\begin{aligned}-\sum_{v\in S}\sum_{|\mathbf{i}|\le m,\mathbf{i}\notin\mathbf{I}_v}\log|L^v_{\mathbf{i}}(P)|_v \ge &- d_1d_2\binom{m+n-2}{n-1}\sum_{1\le i\le n}h(u_i) - CN\\ &+\sum_{v\in M_k\setminus S}\sum_{|\mathbf{i}|\le m}\log|\mathbf{u}^{\mathbf{i}}|_v.\end{aligned}$$

By Lemma 7.0.1,

$$\begin{aligned}\sum_{v\in M_k\setminus S}\sum_{|\mathbf{i}|\le m}\log|\mathbf{u}^{\mathbf{i}}|_v &= \sum_{|\mathbf{i}|\le m}\sum_{v\in M_k\setminus S}\log|\mathbf{u}^{\mathbf{i}}|_v\\ &= \frac{m\binom{n+m}{n}}{n+1}\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\log|u_i|_v\\ &\ge -\frac{m\binom{n+m}{n}}{n+1}\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v\left(\frac{1}{u_i}\right).\end{aligned}$$

So we estimate,

$$\begin{aligned}-\sum_{v\in S}\sum_{|\mathbf{i}|\le m,\mathbf{i}\notin\mathbf{I}_v}\log|L^v_{\mathbf{i}}(P)|_v \ge &-d_1d_2\binom{m+n-2}{n-1}\sum_{1\le i\le n}h(u_i) - \frac{m\binom{n+m}{n}}{n+1}\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v\left(\frac{1}{u_i}\right)\\ &- CN.\end{aligned}$$

On the other hand,

$$\sum_{v\in S}\sum_{|\mathbf{i}|\le m,\mathbf{i}\notin\mathbf{I}_v}\log|P|_v = N\sum_{v\in S}\log|P|_v = N(h(P) - \sum_{v\in M_k\setminus S}\log|P|_v).$$

Now since $\phi_i = fp_i + gq_i$, $\deg fp_i, \deg gq_i \le m$, we have for $v \in M_k \setminus S$,

$$\begin{aligned}\log|\phi_i(\mathbf{u})|_v &= \log|fp_i(\mathrm{u}) + gq_i(\mathbf{u})|_v\\ &\le \log\max\{|fp_i(\mathbf{u})|_v, |gq_i(\mathbf{u})|_v\} + O_v(1)\\ &\le \log^-\max\{|fp_i(\mathbf{u})|_v, |gq_i(\mathbf{u})|_v\} + m\lambda_v(\mathbf{u}) + O_v(1)\\ &\le \log^-\max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} + m\lambda_v(\mathbf{u}) + O_v(1),\end{aligned}$$

where $O_v(1) = 0$ for all but finitely many v.

Then for $v \in M_k \setminus S$,

$$\log |P|_v \leq \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} + m\lambda_v(\mathbf{u}) + C_v.$$

Now we sum over $v \in M_k \setminus S$ to get:

$$\sum_{v \in M_k \setminus S} \log |P|_v \leq \sum_{v \in M_k \setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} + m \sum_{v \in M_k \setminus S} \lambda_v(\mathbf{u}) + O(1).$$

Then we find the estimate:

$$\begin{aligned}\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin \mathbf{I}_v} \log |P|_v \geq & N(h(P) - \sum_{v \in M_k \setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \\ & - m \sum_{v \in M_k \setminus S} \sum_{1 \leq i \leq n} \lambda_v(u_i)) + O(1).\end{aligned}$$

One also has the easy estimate

$$h(P) \leq mh(\mathbf{u}) + O(1).$$

Schmidt's Subspace Theorem implies that there exists a finite union Z of proper subspaces of k^N such that

$$\sum_{v \in S} \sum_{|\mathbf{i}| \leq m, \mathbf{i} \notin \mathbf{I}_v} \log \frac{|Q|_v}{|L^v_{\mathbf{i}}(Q)|_v} \leq (N+1)h(Q)$$

for all $Q \in k^N \setminus Z$.

Using the above estimates, if $P = \phi(\mathbf{u}) \notin Z$, we find that up to an $O(1)$,

$$\begin{aligned}& N\left(h(P) - \sum_{v \in M_k \setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} - m \sum_{v \in M_k \setminus S} \sum_{1 \leq i \leq n} \lambda_v(u_i)\right) \\ & - d_1 d_2 \binom{m+n-2}{n-1} \sum_{1 \leq i \leq n} h(u_i) - \frac{m\binom{n+m}{n}}{n+1} \sum_{v \in M_k \setminus S} \sum_{1 \leq i \leq n} \lambda_v\left(\frac{1}{u_i}\right) \leq (N+1)h(P) + CN.\end{aligned}$$

Applying the estimate for $h(P)$, combining terms, and dividing by N, we obtain up to an $O(1)$,

$$-\sum_{v\in M_k\setminus S}\log^-\max\{|f(\mathbf{u})|_v,|g(\mathbf{u})|_v\}-m\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v(u_i)-\frac{m\binom{n+m}{n}}{N(n+1)}\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v\left(\frac{1}{u_i}\right)$$
$$\le\frac{m+d_1d_2\binom{m+n-2}{n-1}}{N}\sum_{1\le i\le n}h(u_i).$$

Since f and g are coprime, the ideal (f,g) defines a closed subset of $\mathbb{A}^n$ of codimension at least 2. Without loss of generality, assume $d_1\ge d_2$. By Lemma 7.0.2, we find that $N'=\binom{m+n}{n}-\binom{m+n-d_1}{n}-\left(\binom{m+n-d_2}{n}-\binom{m+n-d_1-d_2}{n}\right)\le d_1d_2\binom{m+n-2}{n-2}$ and that $N=\binom{m+n}{n}-N'\ge\binom{m+n}{n}-d_1d_2\binom{m+n-2}{n-2}$. We assume now $m\ge d_1n$. Then we have the estimate

$$\left(\binom{m+n}{n}-d_1d_2\binom{m+n-2}{n-2}\right)\Big/\binom{m+n}{n}=1-\frac{d_1d_2n(n-1)}{(m+n)(m+n-1)}$$
$$\ge 1-\frac{d_1d_2n(n-1)}{d_1^2n^2}$$
$$\ge 1-\frac{n-1}{n}=\frac{1}{n}.$$

Therefore we have

$$-\sum_{v\in M_k\setminus S}\log^-\max\{|f(\mathbf{u})|_v,|g(\mathbf{u})|_v\}\le\frac{m+d_1d_2\binom{m+n-2}{n-1}}{1/n\binom{m+n}{n}}\sum_{1\le i\le n}h(u_i)$$
$$+m\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v(u_i)$$
$$+\frac{m\binom{m+n}{n}/(n+1)}{1/n\binom{m+n}{n}}\sum_{v\in M_k\setminus S}\sum_{1\le i\le n}\lambda_v\left(\frac{1}{u_i}\right).$$

One shall notice that

$$\frac{m+d_1d_2\binom{m+n-2}{n-1}}{1/n\binom{m+n}{n}}\le\frac{2d_1d_2n^2}{m+1},$$

and that

$$\frac{\frac{m\binom{m+n}{n}}{n+1}}{1/n\binom{m+n}{n}}\le m.$$

By Remark 6.1.3, hence the condition $\sum_{1\le i\le n}h_{\bar{S}}(u_i)\le n\delta\sum_{1\le i\le n}h(u_i)$ is satisfied, we get

$$-\sum_{v\in M_k\setminus S}\log^-\max\{|f(\mathbf{u})|_v,|g(\mathbf{u})|_v\}\le\left(\frac{2d_1d_2n^2}{m+1}+mn\delta\right)\sum_{1\le i\le n}h(u_i).$$

Now letting $m = \left\lfloor \frac{2d_1 n}{\delta^{1/2}} \right\rfloor$, it follows that

$$-\sum_{v \in M_k \setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \leq 2(d_1 n^2 + d_2 n)\delta^{1/2} \sum_{1 \leq i \leq n} h(u_i).$$

We can see this choice of m satisfies the conditions $m \geq d_1 n$ and $m \geq \max\{d_1, d_2\}$. Now letting $C(n, d_1, d_2) = 2(d_1 n^2 + d_2 n)$, we have

$$-\sum_{v \in M_k \setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \leq C(n, d_1, d_2)\delta^{1/2} \sum_{1 \leq i \leq n} h(u_i)$$

as long as $\mathbf{u}$ does not lie in the proper closed subset coming from the exceptional set in the application of the Subspace Theorem.

Finally, we note that the choice of linear forms in the application of Schmidt's Subspace Theorem depends not on $\mathbf{u}$, but on the choice of the monomial bases B_v, $v \in S$. Since for fixed m there are only finitely many monomials of degree at most m, and hence only finitely many choices for these bases, we see that for fixed m the given argument leads to only finitely many applications of Schmidt's Subspace Theorem (over all choices of $\mathbf{u}$). Therefore there exists a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that the inequality is valid for all $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$.

Now consider the case when $(f, g)_{(m)} = k[x_1, \ldots, x_n]_m$. We can find polynomials $\tilde{f}, \tilde{g} \in k[x_1, \ldots, x_n]$ such that

$$f\tilde{f} + g\tilde{g} = 1$$

with $\deg \tilde{f}, \deg \tilde{g} \leq m$. Hence for any $v \in M_k$ and $\mathbf{u} \in \mathbb{G}_m^n(s)_{S,\delta}$, we have

$$\begin{aligned} 1 = |(f\tilde{f} + g\tilde{g})(\mathbf{u})|_v &\leq \max\{|f(\mathbf{u})|_v |\tilde{f}(\mathbf{u})|_v, |g(\mathbf{u})|_v |\tilde{g}(\mathbf{u})|_v\} \\ &\leq \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \max\{|\tilde{f}(\mathbf{u})|_v, |\tilde{g}(\mathbf{u})|_v\}. \end{aligned}$$

Then we have

$$\max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \geq \min\{|1/\tilde{f}(\mathbf{u})|_v, |1/\tilde{g}(\mathbf{u})|_v\}.$$

Applying $-\log^-$ on both sides and summing over $v \in M_k \setminus S$, it follows that

$$\begin{aligned} -\sum_{v\in M_k\setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} &\leq -\sum_{v\in M_k\setminus S} \log^- \min\{|1/\tilde{f}(\mathbf{u})|_v, |1/\tilde{g}(\mathbf{u})|_v\} \\ &= -\sum_{v\in M_k\setminus S} \min\{\log|1/\tilde{f}(\mathbf{u})|_v, \log|1/\tilde{g}(\mathbf{u})|_v, 0\} \\ &= \sum_{v\in M_k\setminus S} \max\{\log|\tilde{f}(\mathbf{u})|_v, \log|\tilde{g}(\mathbf{u})|_v, 0\}. \end{aligned}$$

Now since $\deg \tilde{f}, \deg \tilde{g} \leq m$, together with $\sum_{1\leq i\leq n} h_{\bar{S}}(u_i) \leq \delta \sum_{1\leq i\leq n} h(u_i)$ (by Remark 6.1.3), we obtain

$$-\sum_{v\in M_k\setminus S} \log^- \max\{|f(\mathbf{u})|_v, |g(\mathbf{u})|_v\} \leq mn\delta \sum_{1\leq i\leq n} h(u_i),$$

which is an even better estimate according to the proof of the first case. □

By letting $\delta = \dfrac{\epsilon^2}{4n^2(n^2 \deg f + n \deg g)^2}$, we obtain an immediate result:

Corollary 7.0.4. *Let k be a number field and let S be a finite set of places of k containing the archimedean places. Let $f, g \in k[x_1, \ldots, x_n]$ be coprime polynomials. For all $\epsilon > 0$, there exist $\delta > 0$ and a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that*

$$-\sum_{v\in M_k\setminus S} \log^- \max\{|f(u_1, \ldots, u_n)|_v, |g(u_1, \ldots, u_n)|_v\} < \epsilon \max\{h(u_1), \ldots, h(u_n)\}$$

for all $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$.

The next theorem allows us to control the S-part of the greatest common divisor in Theorem 1.1.7.

Theorem 7.0.5. *Let k be a number field and let S be a finite set of places of k containing the archimedean places. Let $f \in k[x_1, \ldots, x_n]$ be a polynomial of degree d that doesn't vanish at the origin $(0, \ldots, 0)$. For all $0 < \delta < 1$, there exists a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that*

$$-\sum_{v\in S} \log^- |f(u_1, \ldots, u_n)|_v < 4nd\delta \sum_{1\leq i\leq n} h(u_i)$$

for all $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$.

Proof. In the following proof we will not consider the points $\{(u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} : f(u_1, \ldots, u_n) = 0\}$. Since this set can be covered by a proper Zariski closed subset, by taking it into the exceptional set, we can ignore such points.

For a subset S' of S, let $R_{S'}$ consist of the set of points $(u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta}$ such that

$$S' = \{v \in S : \log |f(u_1, \ldots, u_n)|_v < 0\}.$$

Then for $(u_1, \ldots, u_n) \in R_{S'}$,

$$\log^- |f(u_1, \ldots, u_n)|_v = \begin{cases} \log |f(u_1, \ldots, u_n)|_v, & v \in S', \\ 0, & v \in S \setminus S'. \end{cases}$$

Let $d = \deg f$, $m \in \mathbb{N}$ and $\phi : \mathbb{P}^n \to \mathbb{P}^N$, $\phi = (\phi_0, \ldots, \phi_N)$, $N = \binom{n+md}{n} - 1$, be the md-uple embedding of $\mathbb{P}^n$ given by the set of monomials of degree md in $k[x_0, \ldots, x_n]$. Let $F = x_0^d f(x_1/x_0, \ldots, x_n/x_0)$ be the homogenization of f in $k[x_0, \ldots, x_n]$. Let V_{md} be the vector space of homogeneous polynomials of degree md, and let Mon_{md} consist of the set of all monomials in $k[x_0, \ldots, x_n]$ of degree md.

If $v \in S'$, we construct a basis for V_{md} as follows. Let $k_{\mathbf{i}} = \left\lfloor \dfrac{\mathrm{ord}_{x_0} \mathbf{x}^{\mathbf{i}}}{d} \right\rfloor$ and define $B_v^{\mathbf{i}} = \dfrac{\mathbf{x}^{\mathbf{i}}}{x_0^{k_{\mathbf{i}} d}} F^{k_{\mathbf{i}}}$. Let B_v be the set of all $B_v^{\mathbf{i}}$. Since f doesn't vanish at the origin, x_0^d appears with a nonzero coefficient in F, and thus it's clear that B_v is a basis for V_{md}.

If $v \in S \setminus S'$, then we let $B_v = \mathrm{Mon}_{md}$. Applying the Subspace Theorem on $\mathbb{P}^N$ with appropriate linear forms, we find that for a fixed $\epsilon > 0$

$$\sum_{v \in S} \sum_{Q \in B_v} \log \frac{|\phi(P)|_v}{|Q(P)|_v} \leq (N + 1 + \epsilon) h(\phi(P))$$

for all $P \in \mathbb{P}^n(k) \setminus Z$, where $Z = \phi^{-1}(Z')$ and Z' is a finite union of hyperplanes in $\mathbb{P}^N$. From the definition of B_v, we can rewrite the left-hand side of above as

$$\sum_{v\in S}\sum_{Q\in \mathrm{Mon}_{md}} \log \frac{|\phi(P)|_v}{|Q(P)|_v} - \sum_{\mathbf{i}}\sum_{v\in S'} \log \frac{|B_v^{\mathbf{i}}(P)|_v}{|\mathbf{x}^{\mathbf{i}}(P)|_v} \leq (N+1+\epsilon)h(\phi(P)).$$

Suppose now that $(u_1,\dots,u_n) \in R_{S'}$ and let $P = [1 : u_1 : \dots : u_n] \in \mathbb{P}^n(k)$. It follows immediately that for $B_v^{\mathbf{i}}$ with $k_{\mathbf{i}}d \leq \mathrm{ord}_{x_0}\mathbf{x}^{\mathbf{i}} < (k_{\mathbf{i}}+1)d$,

$$-\sum_{v\in S'} \log \frac{|B_v^{\mathbf{i}}(P)|_v}{|\mathbf{x}^{\mathbf{i}}(P)|_v} = -k_{\mathbf{i}} \sum_{v\in S'} \log |f(u_1,\dots,u_n)|_v.$$

Letting $I = \sum_{\mathbf{i}} k_{\mathbf{i}}$,

$$\begin{aligned} -\sum_{\mathbf{i}}\sum_{v\in S'} \log \frac{|B_v^{\mathbf{i}}(P)|_v}{|\mathbf{x}^{\mathbf{i}}(P)|_v} &= -I \sum_{v\in S'} \log |f(u_1,\dots,u_n)|_v \\ &= -I \sum_{v\in S} \log^- |f(u_1,\dots,u_n)|_v. \end{aligned}$$

By an easy calculation, we find that

$$\begin{aligned} I &= 1\cdot m + \left(\binom{n+d}{n} - 1\right)(m-1) + \cdots + \left(\binom{n+(m-1)d}{n} - \binom{n+(m-2)d}{n}\right)\cdot 1 \\ &= 1 + \binom{n+d}{n} + \cdots + \binom{n+(m-1)d}{n} \\ &\geq \binom{n+(m-1)d}{n}. \end{aligned}$$

Note that ϕ induces a natural map $\mathbb{G}_m^n \to \mathbb{G}_m^N$ and $\phi(\mathbb{G}_m^n(k)_{S,\delta}) \subset \mathbb{G}_m^N(k)_{S,\delta}$. Indeed,

$$\sum_{v\in M_k\setminus S} \log |\phi(P)|_v = \sum_{v\in M_k\setminus S} \log \max_{Q\in \mathrm{Mon}_{md}} \{|Q(P)|_v\} \leq md \sum_{v\in M_k\setminus S} \log \max_i |u_i|_v.$$

Similarly, we have

$$\sum_{v\in M_k\setminus S} \log \left|\frac{1}{\phi(P)}\right|_v \leq md \sum_{v\in M_k\setminus S} \log \max_i \left|\frac{1}{u_i}\right|_v.$$

Thus we have

$$\sum_{v\in M_k\setminus S} \lambda_v(\phi(P)) + \lambda_v\left(\frac{1}{\phi(P)}\right) \leq \sum_{v\in M_k\setminus S} md\left(\lambda_v(P) + \lambda_v\left(\frac{1}{P}\right)\right) \leq md\delta h(P) \leq \delta h(\phi(P)).$$

Now since $\phi(P) \in \mathbb{G}_m^N(k)_{S,\delta}$ and $\min_i |\phi_i(P)|_v \leq |Q(P)|_v$ for all $Q \in \mathrm{Mon}_{md}$, then

$$\begin{aligned}
&\sum_{v\in S}\sum_{Q\in Mon_{md}} \log\frac{|\phi(P)|_v}{|Q(P)|_v}\\
&= \sum_{v\in M_k}\sum_{Q\in Mon_{md}} \log\frac{|\phi(P)|_v}{|Q(P)|_v} - \sum_{v\in M_k\setminus S}\sum_{Q\in Mon_{md}} \log\frac{|\phi(P)|_v}{|Q(P)|_v}\\
&= (N+1)h(\phi(P)) - \sum_{v\in M_k\setminus S}\sum_{Q\in Mon_{md}} \log\frac{|\phi(P)|_v}{|Q(P)|_v}\\
&\geq (N+1)h(\phi(P)) - (N+1)\left(\sum_{v\in M_k\setminus S}\log|\phi(P)|_v + \sum_{v\in M_k\setminus S}\log\left|\frac{1}{\phi(P)}\right|_v\right)\\
&\geq (N+1)(1-\delta)h(\phi(P)).
\end{aligned}$$

Therefore, we have

$$(N+1)(1-\delta)h(\phi(P)) - I\sum_{v\in S}\log^-|f(u_1,\ldots,u_n)|_v \leq (N+1+\epsilon)h(\phi(P))$$

for all $(u_1,\ldots,u_n) \in R_{S'}$ outside of some proper Zariski closed subset Z. It follows that for a sufficiently small ϵ

$$\begin{aligned}
-\sum_{v\in S}\log^-|f(u_1,\ldots,u_n)|_v &< \frac{(N+1+\epsilon/\delta)}{I}\delta h(\phi(P))\\
&< \frac{\binom{n+md}{n}}{\binom{n+(m-1)d}{n}}\delta mdh(P)\\
&= \frac{(n+(m-1)d+1)\cdots(n+md)}{((m-1)d+1)\cdots(md)}\delta mdh(P)
\end{aligned}$$

for all $(u_1,\ldots,u_n) \in R_{S'}$ outside of some proper Zariski closed subset Z. Choose $m = \left\lceil \frac{n-2^{1/d}+1}{d(2^{1/d}-1)} + 1 \right\rceil$, we have

$$\frac{n+(m-1)d+1}{(m-1)d+1} \leq 2^{1/d},$$

hence $\frac{(n+(m-1)d+1)\cdots(n+md)}{((m-1)d+1)\cdots(md)} \leq 2$. Also notice that $m \leq 2n$, we obtain

$$-\sum_{v\in S}\log^-|f(u_1,\ldots,u_n)|_v < 2\delta mdh(P) < 4nd\delta h(P) < 4nd\delta\sum_{1\leq i\leq n}h(u_i)$$

for all $(u_1, \ldots, u_n) \in R_{S'}$ outside of some proper Zariski closed subset Z. In fact, since there are only finitely many choices of the subset $S' \subset S$, we find that the inequality holds for all $P \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$, for some proper closed subset Z.

□

From Theorem 7.0.5, the immediate result combined with Theorem 7.0.3 is

Theorem 7.0.6. *Let k be a number field and let S be a finite set of places of k containing the archimedean places. Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials that don't both vanish at the origin $(0, \ldots, 0)$. For all $0 < \delta < 1$, there exists a proper Zariski closed subset Z of $\mathbb{G}_m^n$ such that*

$$-\sum_{v \in M_k} \log^- \max\{|f(u_1, \ldots, u_n)|_v, |g(u_1, \ldots, u_n)|_v\} < C\delta^{1/2} \sum_{1 \le i \le n} h(u_i)$$

for all $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$, where $C = 6(\deg f + \deg g)n^2$ is a constant.

Proof. With not loss of generality, assume $\deg f \le \deg g$ and g doesn't vanish at the origin. Then applying Theorem 7.0.5 to g, on the right hand side we obtain

$$4n\delta \deg g \sum_{1 \le i \le n} h(u_i) < 4n(\deg g + \deg f)\delta \sum_{1 \le i \le n} h(u_i).$$

Combining with the inequality from Theorem 7.0.3 finishes the proof. □

Now we are ready to show the desired result (Theorem 1.1.7):

Corollary 7.0.7. *Let k be a number field and S a finite set of places of k containing the archimedean places. Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials that don't both vanish at the origin $(0, \ldots, 0)$. For all $\epsilon > 0$, there exist a $\delta > 0$ and a proper Zariski closed subset $Z \subset \mathbb{G}_m^n$ such that:*

$$-\sum_{v \in M_k} \log^- \max\{|f(u_1, \ldots, u_n)|_v, |g(u_1, \ldots, u_n)|_v\} < \epsilon \max_i h(u_i)$$

for all $(u_1, \ldots, u_n) \in \mathbb{G}_m^n(k)_{S,\delta} \setminus Z$.

Proof. By letting $\delta = \left(\frac{\epsilon}{6n^3(\deg f + \deg g)}\right)^2$, we obtain the inequality from Theorem 7.0.6. □

As discussed in the following remark, under a normal crossings assumption, a result of Silverman shows that Vojta's conjecture predicts an improvement to Theorem 7.0.6.

Remark 7.0.8. From Theorem 2 in [18, Silverman], if we assume Vojta's Conjecture is true, there is an improvement of the inequality as in Theorem 7.0.3. Let k be a number field. Fix $\epsilon > 0$. For f and g homogeneous coprime polynomials in $k[x_0, \ldots, x_n]$ and $Y = \{f = g = 0\}$ that intersects the coordinate hyperplanes transversally, there is a proper closed subset Z such that we have for all $\mathbf{x} \in \mathbb{P}^n(k) \setminus Z$,

$$\log \gcd(f(\mathbf{x}), g(\mathbf{x})) \leq \epsilon \max\{h(x_0), \ldots, h(x_n)\} + \frac{1}{1+\gamma\epsilon} \sum_{1 \leq i \leq n} h_{\bar{S}}(x_i)$$

where γ is a positive constant.

Suppose $h_{\bar{S}}(\mathbf{x}) \leq \delta h(\mathbf{x})$. Using the estimate

$$\sum_{1 \leq i \leq n} h_{\bar{S}}(x_i) \leq n h_{\bar{S}}(\mathbf{x}),$$

we get

$$\log \gcd(f(\mathbf{x}), g(\mathbf{x})) \leq \left(\epsilon + \frac{n\delta}{1+\gamma\epsilon}\right) \sum_{1 \leq i \leq n} h(x_i) \leq \left(\epsilon + \frac{\delta}{1+\gamma\epsilon}\right) n \sum_{1 \leq i \leq n} h(x_i).$$

Let $\epsilon = \dfrac{-1+\sqrt{1+4\gamma\delta}}{2\gamma}$, we obtain a similar inequality as in Theorem 7.0.3,

$$\begin{aligned}
\log \gcd(f(\mathbf{x}), g(\mathbf{x})) &\leq \left(\frac{-1+\sqrt{1+4\gamma\delta}}{2\gamma} + \frac{\delta}{1+\dfrac{-1+\sqrt{1+4\gamma\delta}}{2}} \right) n \sum_{1\leq i\leq n} h(x_i) \\
&= (-1+\sqrt{1+4\gamma\delta}) \left(\frac{1}{2\gamma} + \frac{2\delta}{4\gamma\delta} \right) n \sum_{1\leq i\leq n} h(x_i) \\
&\leq \left(-1+1+\frac{4\gamma\delta}{2} \right) \frac{1}{\gamma} n \sum_{1\leq i\leq n} h(x_i) \\
&= 2\delta n \sum_{1\leq i\leq n} h(x_i).
\end{aligned}$$

Thus, under a normal crossings assumption, Vojta's conjecture predicts a linear dependence on δ in place of the square root dependence in Theorem 7.0.6 (note, however, that without a normal crossings assumption, the dependence on the degree of f and g in Theorem 7.0.6 is necessary, as can be seen by taking high powers of appropriate polynomials).

Example 7.0.9. In this example we show that the predicted linear dependence on δ is sharp (if true). Let $\mathbb{Q}$ be the field of rationals and $S = \{p, \infty\}$ be a finite set of places in $M_{\mathbb{Q}}$. Let $0 < \delta < 1$. Let $x = p^m, u = p^n$ for positive integers m and n such that $P := (x, u(x+1))$ satisfies $1/2\delta h(P) \leq h_{\bar{S}}(P) \leq \delta h(P)$. Let x_1, x_2 be the coordinates in $\mathbb{G}_m^2$, then we take $f = x_1 + 1$, $g = x_2$. We make the estimate

$$\begin{aligned}
\log \gcd(f(P), g(P)) &= -\sum_{v\notin S} \log^- \max\{|x+1|_v, |u(x+1)|_v\} - \sum_{v\in S} \log^- \max\{|x+1|_v, |u(x+1)|_v\} \\
&\geq \sum_{v\notin S} \lambda_v \left(\frac{1}{x+1} \right) = h(x+1).
\end{aligned}$$

One shall also notice that for $x \in O_{S,\mathbb{Q}}^*$, we have $h_{\bar{S}}(P) = h_{\bar{S}}(x+1) = h(x+1)$. Then it follows that

$$\log \gcd(f(P), g(P)) \geq 1/2\delta h(P).$$

It's easily seen that one may choose infinitely many appropriate x and u such that the set of resulting points P forms a Zariski dense set in $\mathbb{G}_m^2$. Therefore the dependence on δ has to be at least linear.

CHAPTER 8

PROOFS OF LINEAR RECURRENCE SEQUENCES THEOREMS

In this section our main goal is to give the proof of Theorem 1.2.4, which requires Corollary 7.0.4 from the previous section.

Lemma 8.0.1. *Let*

$$F(n) = \sum_{i=0}^{s} p_i(n)\alpha_i^n$$

define a nondegenerate algebraic linear recurrence sequence. Let $|\cdot|$ *be an absolute value on* $\bar{\mathbb{Q}}$ *such that* $|\alpha_i| \geq 1$ *for some* i. *Let* $0 < \epsilon < 1$. *Then*

$$-\log|F(n)| < \epsilon n$$

for all but finitely many $n \in \mathbb{N}$.

Proof. Let k be a number field and S a finite set of places of k such that $p_i(x) \in k[x]$, $\alpha_i \in \mathcal{O}_{k,S}^*$, $i = 0, \ldots, s$, and $|\cdot|$ restricted to k is equivalent to $|\cdot|_v$ for some $v \in S$ (note that if $|\cdot|$ is trivial, the lemma is obvious). The $s = 0$ case is trivial and so we may assume that $s > 0$. By taking sufficiently large n, we can always assume that $p_i(n)$ don't vanish simultaneously. It suffices to prove that

$$-\log|F(n)|_v < \epsilon n$$

for all but finitely many $n \in \mathbb{N}$.

Let H_i be the coordinate hyperplane in $\mathbb{P}^s$ defined by $x_i = 0$, $i = 0, \ldots, s$. Let H_{s+1} be the hyperplane in $\mathbb{P}^s$ defined by $x_0 + x_1 + \cdots + x_s = 0$. Note that the $s + 2$ hyperplanes $H_0, \ldots, H_{s+1}$

are in general position. Let

$$P = [\alpha_0 : \cdots : \alpha_s] \in \mathbb{P}^s(k)$$

$$P_n = [p_0(n)\alpha_0^n : \cdots : p_s(n)\alpha_s^n] \in \mathbb{P}^s(k),\ n \in \mathbb{N}$$

$$Q_n = [p_0(n) : \cdots : p_s(n)] \in \mathbb{P}^s(k),\ n \in \mathbb{N}.$$

Let $h = \max\{1, h(P)\}$. Then the Schmidt Subspace Theorem gives that for some finite union of hyperplanes Z in $\mathbb{P}^s$,

$$\sum_{i=0}^{s+1} m_{H_i,S}(P_n) < (s + 1 + \epsilon/(4h))h(P_n) \qquad (*)$$

for all points $P_n \in \mathbb{P}^s(k) \setminus Z$. In fact, since F is nondegenerate, by the Skolem-Mahler-Lech theorem, only finitely many points P_n belong to the given hyperplanes in $\mathbb{P}^s$, and thus the inequality holds for all but finitely many n. By taking n to be sufficiently large, we can assume that $h(Q_n) \leq \delta h(P_n)$ with $\delta \leq \dfrac{\epsilon}{4(s+1)h}$, so that we assume $P_n \in \mathbb{G}_m^n(k)_{S,\delta}$. Since $\alpha_i \in O_{k,S}^*$ for all i, $m_{H_i,S}(P_n) \geq (1-\delta)h(P_n)$, $i = 0, \ldots, s$. Note also that

$$h(P_n) \leq nh(P) + h(Q_n) \leq \frac{n}{1-\delta}h(P)$$

for all n sufficiently large. Substituting in $(*)$, we have

$$m_{H_{s+1},S}(P_n) < (\epsilon/(4h) + (s+1)\delta)\frac{n}{1-\delta}h(P) \leq \frac{n\epsilon}{2(1-\delta)}.$$

Note that $\delta = \dfrac{\epsilon}{4(s+1)h} \leq \dfrac{1}{4(s+1)} \leq 1/2$, so we have $1 - \delta > 1/2$ and then

$$m_{H_{s+1}}(P_n) < \epsilon n.$$

Pick α_j with $|\alpha_j|_v \geq 1$. Then

$$\max_i \log |p_i(n)\alpha_i^n|_v \geq \log |p_j(n)|_v |\alpha_j|_v^n \geq \log |p_j(n)|_v.$$

To give $p_j(n)$ an estimate, we can take the inequality

$$\log |p_j(n)|_v \geq -h(p_j(n)).$$

Then it follows that

$$\log |p_j(n)|_v \geq -\deg p_j \log n + O(1).$$

It follows that

$$\lambda_{H_{s+1},v}(P_n) = \log \frac{\max_i |p_i(n)\alpha_i^n|_v}{|\sum_{i=0}^{s} p_i(n)\alpha_i^n|_v} \geq -\log |F(n)|_v - C' \log n$$

for some constant C'. Together with $m_{H_{s+1},S}(P_n) \geq \lambda_{H_{s+1},v}(P_n) + O(1)$, we have for all $\epsilon > 0$,

$$-\log |F(n)|_v < \epsilon n + C' \log n + O(1).$$

It follows that for all sufficiently large n,

$$-\log |F(n)|_v < \epsilon n.$$

□

Now we can state Theorem 1.8 (i) of Grieve-Wang [11] on the greatest common divisor between the terms of two linear recurrence sequences with the same index and give an alternative proof:

Theorem 8.0.2. *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m)\alpha_i^m$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n$$

define two algebraic linear recurrence sequences, where p_i and q_j are polynomials. Let k be a number field such that all coefficients of p_i and q_j and α_i, β_j are in k, for $i = 1, \ldots, s$, $j = 1, \ldots, t$. Let

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v, \ldots, |\alpha_s|_v, |\beta_1|_v, \ldots, |\beta_t|_v\} < 1\}.$$

Let $\epsilon > 0$. Then all but finitely many solutions $l \in \mathbb{N}$ of the inequality

$$\sum_{v \in M_k \setminus S_0} -\log^- \max\{|F(l)|_v, |G(l)|_v\} > \epsilon l$$

lie in one of finitely many nontrivial arithmetic subprogressions:

$$a_i t + b_i, \quad t \in \mathbb{N}, i = 1, \ldots, r$$

where $a_i, b_i \in \mathbb{N}, a_i \neq 0$, and the linear recurrences $F(a_i \bullet + b_i)$ and $G(a_i \bullet + b_i)$ have a nontrivial common factor for $i = 1, \ldots, r$. Furthermore, if F and G are coprime and their roots generate a torsion-free group, then there are only finitely many solutions to the inequality above.

Proof. We begin with a couple of convenient reductions. First, by considering finitely many arithmetic progressions in l, we may reduce to the case where the combined roots of F and G generate a torsion-free group Γ of rank r (in particular, both F and G are nondegenerate). Let $S \supset S_0$ be a finite set of places of k, containing the archimedean places, such that all coefficients of p_i and q_j and α_i, β_j are in $O_{k,S}^*$ for all i and j.

By Lemma 8.0.1,

$$\sum_{v \in S \setminus S_0} -\log^- \max\{|F(l)|_v, |G(l)|_v\} \leq \frac{\epsilon}{2} l$$

for all but finitely many $l \in \mathbb{N}$. Thus it suffices to prove the statement of the theorem with the inequality:

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(l)|_v, |G(l)|_v\} < \epsilon l.$$

Let $u_1, \ldots, u_r$ be generators for Γ. Let $f, g \in k[l, x_1, \ldots, x_r, x_1^{-1}, \ldots, x_r^{-1}]$ be the Laurent polynomials corresponding to F and G. We may write

$$f(l, x_1, \ldots, x_r) = x_1^{i_1} \cdots x_r^{i_r} f_0(l, x_1, \ldots, x_r),$$

$$g(l, x_1, \ldots, x_r) = x_1^{j_1} \cdots x_r^{j_r} g_0(l, x_1, \ldots, x_r)$$

where $i_1, \ldots, i_r, j_1, \ldots, j_r \in \mathbb{Z}$ and $f_0 \in k[l, x_1, \ldots, x_r]$, $g_0 \in k[l, x_1, \ldots, x_r]$ with $x_i \nmid f_0 g_0$, $i = 1, \ldots, r$. Let F_0 and G_0 be the linear recurrence sequences corresponding to f_0 and g_0, respectively. Since $u_1, \ldots, u_r \in O_{k,S}^*$, it follows that

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(l)|_v, |G(l)|_v\} = \sum_{v \in M_k \setminus S} -\log^- \max\{|F_0(l)|_v, |G_0(l)|_v\}.$$

Then it suffices to prove the statement of the theorem with F and G replaced by F_0 and G_0, respectively. Note that since $x_1, \ldots, x_r$ are units in $k[x_1, \ldots, x_r, x_1^{-1}, \ldots, x_r^{-1}]$, replacing F and G by F_0 and G_0 has no effect on coprimality statements. Thus, we now assume that F and G correspond to polynomials f and g in $k[l, x_1, \ldots, x_r]$.

Suppose now that F and G are coprime (equivalently, f and g are coprime). Let

$$P_n = (n, u_1^n, \ldots, u_r^n).$$

Now for a fixed sufficiently small positive δ (coming from the proof of Corollary 7.0.4), take n to be sufficiently large such that $h(n) \leq \delta n \min_i h(u_i)$, and so $P_n \in \mathbb{G}_m^{r+1}(k)_{S,\delta}$.
By Corollary 7.0.4,

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|f(P_n)|_v, |g(P_n)|_v\} < \epsilon \max\{h(u_1^n), \ldots, h(u_r^n)\}$$

for all $P_n \in \mathbb{G}_m^{r+1}(k)_{S,\delta}$ outside a proper Zariski closed set Z. Noting that $f(P_n) = F(n)$ and $g(P_n) = G(n)$, and also that $\max\{h(u_1^n), \ldots, h(u_r^n)\} = n \max\{h(u_1), \ldots, h(u_r)\}$, after possibly shrinking ϵ,we can write the above inequality as

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(n)|_v, |G(n)|_v\} < \epsilon n.$$

Cover the exceptional set Z by a hypersurface defined by a polynomial $Exc(x_1, \ldots, x_{r+1})$ in $k[x_1, \ldots, x_{r+1}]$ such that if $P_n \in Z$ then $Exc(P_n) = 0$. We can view $Exc(P_n)$ as terms of a linear recurrence sequence $E(n)$ with E non-degenerate. By the Skolem-Mahler-Lech theorem, there are only finitely many zeros for E, which completes the proof.

□

Here we deal with a special case when m and n are algebraically related:

Lemma 8.0.3. *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m) \alpha_i^m$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n$$

be two linear recurrence sequences over a number field k and S be a finite set of places in M_k containing archimedean places and S_0, where S_0 is defined as

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v, \ldots, |\alpha_s|_v, |\beta_1|_v, \ldots, |\beta_t|_v\} < 1\}.$$

Let $C \subset \mathbb{A}^2$ be an affine irreducible plane curve over k. If there are infinitely many $(m, n) \in C(\mathbb{Z})$ satisfying the inequality

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(m)|_v, |G(n)|_v\} > \epsilon \max\{m, n\}$$

then C is a line over k. In particular, if $m(t), n(t) \in \mathbb{Z}[t]$ are polynomials that are not linearly related, then the inequality

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(m(t))|_v, |G(n(t))|_v\} > \epsilon \max\{m(t), n(t)\}$$

has only finitely many solutions $t \in \mathbb{Z}$.

Remark 8.0.4. Note that if C is a line, the solutions are easily classified using Theorem 8.0.2

The following lemma is a basic fact from linear algebra, we state it without a proof.

Lemma 8.0.5. *Let $\{v_1, \ldots, v_n\}$ be a linearly independent subset of a normed vector space X. Then there exists a constant $c > 0$ such that for every set of scalars $\{\alpha_1, \ldots, \alpha_n\}$:*

$$|\alpha_1 v_1 + \cdots + \alpha_n v_n| \geq c(|\alpha_1| + \cdots + |\alpha_n|).$$

Let $Tor(\overline{\mathbb{Q}}^*)$ denote the torsion subgroup of $\overline{\mathbb{Q}}^*$. Since the height h gives $\overline{\mathbb{Q}}^*/Tor(\overline{\mathbb{Q}}^*)$ the structure of a normed vector space over $\mathbb{Q}$ as in Allcock and Vaaler [1], we immediately find:

Lemma 8.0.6. *Let $u_1, \ldots, u_n$ be multiplicatively independent elements of $\overline{\mathbb{Q}}^*$. Then there exists a constant $c > 0$ such that for all $i_1, \ldots, i_n \in \mathbb{Z}$,*

$$h(u_1^{i_1} \cdots u_n^{i_n}) \geq c \max_j |i_j|.$$

We now prove Lemma 8.0.3.

Proof. Using the same reduction as in the proof of Theorem 8.0.2, we can assume that the roots of F and G are S-units, and by considering finitely many congruence classes, we can assume that the roots of F and G generate a torsion free group. Let C be the affine curve defined by the algebraic relation $R(x_1, x_2) = 0$, with $R(x_1, x_2) \in k[x_1, x_2]$ irreducible. If C is not geometrically irreducible then $C(k)$ (and hence $C(\mathbb{Z})$) is finite, and so we further assume C is geometrically irreducible. By Siegel's Theorem, $C(\mathbb{Z})$ is finite unless C has genus 0 and C has two or fewer distinct points at infinity, which we now assume. After replacing k by a suitable finite extension, we can parametrize C by Laurent polynomials $m(t), n(t) \in k[t, 1/t]$. Assume that C is not a line, or equivalently, that $m(t)$ and $n(t)$ do not satisfy a linear relation.

Let Γ be the torsion free group generated by the roots of F and G and let $\{u_1, \dots, u_r\}$ be generators of Γ. Consider the points

$$P_t = (t, u_1^{m(t)}, \dots, u_r^{m(t)}, u_1^{n(t)}, \dots, u_r^{n(t)}),$$

for $t \in k$ where, as we implicitly assume from now on, we have $m(t), n(t) \in \mathbb{Z}$. Then for some Laurent polynomials

$$f(x_1, \dots, x_{r+1}), g(x_1, x_{r+2}, \dots, x_{2r+1}) \in k[x_1, \dots, x_{2r+1}, x_1^{-1}, \dots, x_{2r+1}^{-1}],$$

we have $F(m(t)) = f(P_t)$ and $G(n(t)) = g(P_t)$. From the form of f and g, we may write

$$f(x_1, \dots, x_{r+1}) = x_2^{i_1} \cdots x_{r+1}^{i_r} c(x_1) \bar{f}(x_1, \dots, x_{r+1}),$$
$$g(x_1, x_{r+2}, \dots, x_{2r+1}) = x_{r+2}^{j_1} \cdots x_{2r+1}^{j_r} c(x_1) \bar{g}(x_1, x_{r+2}, \dots, x_{2r+1})$$

where $i_1, \dots, i_r, j_1, \dots, j_r \in \mathbb{Z}$, $\bar{f}$ and $\bar{g}$ are coprime polynomials in $k[x_1, \dots, x_{2r+1}]$, and $c(x_1)$ is a Laurent polynomial in x_1.

By elementary properties of heights, if $m(t), n(t) \in \mathbb{Z}$, then $h(t) \ll \log \max\{|m(t)|, |n(t)|\}$ and $h(P_t) \gg \max\{|m(t)|, |n(t)|\}$. It follows that for any $\delta > 0$, we have $P_t \in \mathbb{G}_m^{2r+1}(k)_{S,\delta}$ for all

but finitely many $t \in k$ (with $m(t), n(t) \in \mathbb{Z}$). Then Corollary 7.0.4 applies to $\bar{f}$ and $\bar{g}$ and we obtain that for any $\epsilon > 0$ there exists a proper Zariski closed subset $Z \subset \mathbb{G}_m^{2r+1}$ such that

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|\bar{f}(P_t)|_v, |\bar{g}(P_t)|_v\} < \epsilon \max_{i=1,\dots,r} \{h(u_i^{m(t)}), h(u_i^{n(t)})\}$$

for all points P_t outside Z. By elementary estimates, for all but finitely many $t \in k$,

$$\sum_{v \in M_k \setminus S} -\log^- |c(t)|_v \leq h(c(t)) < \epsilon \max_{i=1,\dots,r} \{h(u_i^{m(t)}), h(u_i^{n(t)})\}.$$

Using this inequality and that $u_1, \dots, u_r \in O_{k,S}^*$, the inequality for $\bar{f}$ and $\bar{g}$ implies the inequality for f and g:

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|f(P_t)|_v, |g(P_t)|_v\} < \epsilon \max_{i=1,\dots,r} \{h(u_i^{m(t)}), h(u_i^{n(t)})\}$$

for all points P_t outside a proper Zariski closed subset $Z \subset \mathbb{G}_m^{2r+1}$. Setting $(m, n) = (m(t), n(t)) \in C(\mathbb{Z})$, note that $f(P_t) = F(m)$, $g(P_t) = G(n)$, and

$$\max\{h(u_1^m), \dots, h(u_r^m), h(u_1^n), \dots, h(u_r^n)\} \leq \max\{m, n\} \max\{h(u_1), \dots, h(u_r)\}.$$

Then we can write the above inequality as

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(m)|_v, |G(n)|_v\} < \epsilon \max\{m, n\}.$$

It remains to show that there are only finitely many $t \in k$ with $m(t), n(t) \in \mathbb{Z}$ and $P_t \in Z$. Now we cover Z by a hypersurface defined by an equation $z(x_1, \dots, x_{2r+1}) = 0$. Then every P_t in Z satisfies an equation

$$z(P_t) = \sum_{w=1}^{K} P_w(t) u_1^{m(t)s_{1,w}} \cdots u_r^{m(t)s_{r,w}} u_1^{n(t)t_{1,w}} \cdots u_r^{n(t)t_{r,w}} = 0,$$

where $P_w \in k[t]$, $w = 1, \dots, K$ are nonzero polynomials and the integer tuples $(s_{1,w}, \dots, s_{r,w}, t_{1,w}, \dots, t_{r,w})$, $w = 1, \dots, K$, are distinct. If $K = 1$ then t must be one of the finitely many roots of the polynomial $P_1(t)$. Otherwise, dividing by the first term we find

$$\sum_{w=2}^{K} Q_w(t) u_1^{m(t)s'_{1,w} + n(t)t'_{1,w}} \cdots u_r^{m(t)s'_{r,w} + n(t)t'_{r,w}} = 1, \tag{8.1}$$

where $Q_w(t), i = 2, \ldots, K$, are rational functions in t and $s'_{i,w} = s_{i,w} - s_{i,1}$, $t'_{i,w} = t_{i,w} - t_{i,1}$.

Note that

$$h(Q_w(t)) = (\deg Q_w)h(t) + O(1)$$

and by Lemma 8.0.6 (assuming $m(t), n(t) \in \mathbb{Z}$ as usual)

$$\begin{aligned} h\left(u_1^{m(t)s'_{1,w}+n(t)t'_{1,w}} \cdots u_r^{m(t)s'_{r,w}+n(t)t'_{r,w}}\right) &\gg \max_i\{|m(t)s'_{i,w} + n(t)t'_{i,w}|\} \\ &= e^{\max_i h(m(t)s'_{i,w}+n(t)t'_{i,w})} \\ &\gg e^{h(t)\max_i \deg(ms'_{i,w}+nt'_{i,w})} \\ &\gg e^{h(t)} \end{aligned}$$

since $(s'_{i,w}, t'_{i,w}) \neq (0,0)$ for some i, and in this case $ms'_{i,w} + nt'_{i,w}$ must be nonconstant by our assumption that m and n aren't linearly related.

Since the terms in the sum in (8.1) are S-units outside the factors $Q_w(t)$, it follows from the height estimates above and the almost S-unit equation (Corollary 6.2.2) that there exists a finite set $\mathcal{F} \subset k$ such that every solution $t \in k$ to (8.1) (with $m(t), n(t) \in \mathbb{Z}$) satisfies

$$Q_w(t)u_1^{m(t)s'_{1,w}+n(t)t'_{1,w}} \cdots u_r^{m(t)s'_{r,w}+n(t)t'_{r,w}} \in \mathcal{F}$$

for some w. By the height estimates above,

$$h(Q_w(t)u_1^{m(t)s'_{1,w}+n(t)t'_{1,w}} \cdots u_r^{m(t)s'_{r,w}+n(t)t'_{r,w}}) \gg e^{h(t)},$$

and Northcott's Theorem implies that there are only finitely many solutions $t \in k$ with $m(t), n(t) \in \mathbb{Z}$ satisfying (8.1). It follows that there are only finitely many pairs $(m,n) \in C(\mathbb{Z})$ satisfying the inequality of the theorem.

□

Definition 8.0.7. Let F and G be two linear recurrence sequences. Suppose that the roots of F and G generate multiplicative torsion-free groups of rank r and s, respectively. We say that the roots of F and G are multiplicatively independent if the combined roots generate a group of rank $r + s$. Otherwise, we say they are multiplicatively dependent.

The following result is a generalization of Theorem 8.0.2 under a multiplicative independence assumption, which was proved by Grieve-Wang [11]. Here we give an alternative proof:

Theorem 8.0.8. *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m)\alpha_i^m$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n$$

define two algebraic linear recurrence sequences, where p_i and q_j are polynomials. Let k be a number field such that all coefficients of p_i and q_j and α_i, β_j are in k, for $i = 1, \ldots, s$, $j = 1, \ldots, t$. Let

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v, \ldots, |\alpha_s|_v, |\beta_1|_v, \ldots, |\beta_t|_v\} < 1\}.$$

Let $\epsilon > 0$. If we assume further the roots of F and G are independent, then all but finitely many $(m, n) \in \mathbb{N}^2$ satisfy the inequality

$$\sum_{v \in M_k \setminus S_0} -\log^- \max\{|F(m)|_v, |G(n)|_v\} < \epsilon \max\{m, n\}.$$

In particular, if $S_0 = \emptyset$, then all but finitely many (m, n) satisfy the inequality

$$\log \gcd(F(m), G(n)) < \epsilon \max\{m, n\}$$

Proof. Notice that

$$\begin{aligned}\sum_{v \in M_k \setminus S} -\log^- \max\{|F(m)|_v, |G(n)|_v\} &\leq \min\{h(F(m)), h(G(n))\} \\ &\leq \mathcal{K} \min\{m, n\}\end{aligned}$$

for some constant $\mathcal{K}$. Hence for the inequality in the statement to be true, for a fixed $\epsilon > 0$,

$$\mathcal{K} \min\{m, n\} \geq \epsilon \max\{m, n\}.$$

The combined roots of F and G generate a torsion-free group Γ of rank $r+s$ whose generators are $\{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ where $u_1, \ldots, u_r$ generate the roots α_i and $v_1, \ldots, v_s$ generate the

roots β_j. By the same reduction step in the previous proof, assume all the coefficients of the polynomials p_i and q_j and all of the roots of F and G are S-units. We can also assume the Laurent polynomials f and g corresponding to F and G with respect to the roots $u_1, \ldots, u_r$ and $v_1, \ldots, v_s$, respectively, are polynomials.

Let $\hat{f}, \hat{g} \in k[x_1, \ldots, x_{r+s+2}]$ be polynomials such that

$$\hat{f}(x_1, \ldots, x_{r+s+2}) = f(x_1, \ldots, x_{r+1})$$

$$\hat{g}(x_1, \ldots, x_{r+s+2}) = g(x_{r+2}, \ldots, x_{r+s+2}).$$

Note that $\hat{f}$ and $\hat{g}$ are coprime since they involve disjoint sets of variables.

For $m, n \in \mathbb{N}$, let

$$P_{m,n} = (m, u_1^m, \ldots, u_r^m, n, v_1^n, \ldots, v_s^n).$$

Let $\epsilon > 0$ and let $\delta > 0$ be the quantity from Corollary 7.0.4 for $\hat{f}, \hat{g}$, and ϵ. After excluding finitely many pairs (m, n), we can always assume that

$$h(m) + h(n) < \delta(r + s + 2) \max_{i,j}\{h(u_i^m), h(v_j^n)\}.$$

Therefore $P_{m,n} \in \mathbb{G}_m^{r+s+2}(k)_{S,\delta}$. Applying Corollary 7.0.4,

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|\hat{f}(P_{m,n})|_v, |\hat{g}(P_{m,n})|_v\} < \epsilon \max\{h(u_1^m), \ldots, h(u_r^m), h(v_1^n), \ldots, h(v_s^n)\}$$

for all $P_{m,n} \in \mathbb{G}_m^{r+s+2}(k)_{S,\delta}$ outside a proper Zariski closed set $Z \subset \mathbb{G}_m^{r+s+2}$. Noting that $\hat{f}(P_{m,n}) = F(m)$, $\hat{g}(P_{m,n}) = G(n)$, and

$$\max_{1 \le i \le r, 1 \le j \le s}\{h(u_i^m), h(v_j^n)\} \le \max\{n, m\} \max_{1 \le i \le r, 1 \le j \le s}\{h(u_i), h(v_j)\},$$

we can write the above inequality as

$$\sum_{v \in M_k \setminus S} -\log^- \max\{|F(m)|_v, |G(n)|_v\} < \epsilon \max\{n, m\}.$$

As in the $m = n$ case, we cover Z by a hypersurface defined by a polynomial equation:

$$Exc(x_1, \ldots, x_{r+s+2}) = 0.$$

Hence all the points $P_{m,n}$ in Z must satisfy the above equation. Therefore, if $P_{m,n} \in Z$, after combining the terms with the same exponents on $u_1, \ldots, u_r, v_1, \ldots, v_s$, we obtain an equation in terms of $m, n, u_1, \ldots, u_r, v_1, \ldots, v_s$:

$$Exc(m, u_1^m, \ldots, u_r^m, n, v_1^n, \ldots, v_s^n) = \sum_{w=1}^{W} P_w(m,n) u_1^{ms_{1,w}} \cdots u_r^{ms_{r,w}} v_1^{nt_{1,w}} \cdots v_s^{nt_{s,w}} = 0,$$

where $P_w(m,n)$ is a non-zero polynomial in m and n. It follows from Theorem 8.0.2 and Lemma 8.0.3 that after excluding finitely many pairs (m,n) we can assume that (m,n) is not a zero of any of the polynomials P_w.

Dividing both sides by the negative of the first term,

$$\sum_{w=2}^{W} \frac{P_w(m,n) u_1^{ms_{1,w}} \cdots u_r^{ms_{r,w}} v_1^{nt_{1,w}} \cdots v_s^{nt_{s,w}}}{-P_1(m,n) u_1^{ms_{1,1}} \cdots u_r^{ms_{r,1}} v_1^{nt_{1,1}} \cdots v_s^{nt_{s,1}}} = 1.$$

Let $Q_w(m,n) = \dfrac{P_w(m,n)}{-P_1(m,n)}$ $(w = 2, \ldots, W)$, then

$$\sum_{w=2}^{W} Q_w(m,n) u_1^{m(s_{1,w}-s_{1,1})} \cdots u_r^{m(s_{r,w}-s_{r,1})} v_1^{n(t_{1,w}-t_{1,1})} \cdots v_s^{n(t_{s,w}-t_{s,1})} = 1.$$

Letting $s'_{i,w} = s_{i,w} - s_{i,1}$, $t'_{i,w} = t_{i,w} - t_{i,1}$, we have

$$\sum_{w=2}^{W} Q_w(m,n) u_1^{ms'_{1,w}} \cdots u_r^{ms'_{r,w}} v_1^{nt'_{1,w}} \cdots v_s^{nt'_{s,w}} = 1$$

with $s'_{i,w}$, $t'_{i,w}$ fixed and only depending on Exc.

As in the proof of Lemma 8.0.3, it follows from Lemma 8.0.6 that if $\min\{m,n\}$ is sufficiently large, then Corollary 6.2.2 applies to the equation

$$\sum_{w=2}^{W} Q_w(m,n) u_1^{ms'_{1,w}} \cdots u_r^{ms'_{r,w}} v_1^{nt'_{1,w}} \cdots v_s^{nt'_{s,w}} = 1,$$

and we conclude that one of the summands on the left-hand side belongs to a finite set $\mathcal{F}$. But since

$$h(Q_w(m,n)u_1^{ms'_{1,w}}\cdots u_r^{ms'_{r,w}}v_1^{nt'_{1,w}}\cdots v_s^{nt'_{s,w}}) \to \infty \text{ as } \min\{m,n\} \to \infty,$$

and $\min\{m,n\} \to \infty$ also means $max\{m,n\} \to \infty$ by the remarks at the beginning of the proof, this implies that there are only finitely many possibilities for the pair (m,n). □

We now prove a result in the general case where the roots of F and G are not necessarily independent. The following theorem gives an improvement to Theorem 1.8 (ii) of Grieve-Wang [11], who proved a similar result but with $\log\max\{m,n\}$ replaced by the weaker expression $o(\max\{m,n\})$.

Theorem 8.0.9. *Let*

$$F(m) = \sum_{i=1}^{s} p_i(m)\alpha_i^m$$

$$G(n) = \sum_{j=1}^{t} q_j(n)\beta_j^n$$

define two distinct algebraic linear recurrence sequences, where p_i and q_j are polynomials. Let k be a number field such that all coefficients of p_i and q_j and α_i, β_j are in k, for $i = 1,\ldots,s$, $j = 1,\ldots,t$. Let

$$S_0 = \{v \in M_k : \max\{|\alpha_1|_v,\ldots,|\alpha_s|_v,|\beta_1|_v,\ldots,|\beta_t|_v\} < 1\}.$$

Then there are finitely many choices of nonzero integers (a_i,b_i,c_i,d_i), $a_ic_i \neq 0$ such that all solutions $(m,n) \in \mathbb{N}^2$ of the inequality

$$\sum_{v\in M_k\setminus S_0} -\log^- \max\{|F(m)|_v,|G(n)|_v\} > \epsilon\max\{m,n\} \qquad (\triangle)$$

are of the form:

$$(m,n) = (a_it+b_i, c_it+d_i) + (\mu_1,\mu_2),\ |\mu_1|,|\mu_2| \ll \log t,\ t \in \mathbb{N},\ i = 1,\ldots,r.$$

Proof. Now let $\{u_1, \ldots, u_r\}$ be a set of generators which generates the roots of F and G and assume that the u_i's are multiplicatively independent (as in the proof of Theorem 8.0.2). It follows from the first part of the proof of Theorem 8.0.8 (using the points $P_{m,n} = (m, u_1^m, ..., u_r^m, n, u_1^n, ..., u_r^n)$) that all but finitely many pairs (m, n) that fail the above inequality either satisfy finitely many linear relations $(m, n) = (a_i t + b_i, c_i t + d_i)$ or satisfy an exponential-polynomial equation coming from Schmidt's Subspace Theorem:

$$\sum_{w=1}^{W} P_w(m,n) u_1^{ms_{1,w}+nt_{1,w}} \cdots u_r^{ms_{r,w}+nt_{r,w}} = 0,$$

where $P_w(m, n)$ are non-zero polynomials in m and n. After ignoring finitely many arithmetic progressions, we can assume that (m, n) is not a zero of any P_w by Lemma 8.0.3.

Dividing by the first term, we need to study the solutions (m, n) to the equation

$$\sum_{w=2}^{W} Q_w(m,n) u_1^{ms'_{1,w}+nt'_{1,w}} \cdots u_r^{ms'_{r,w}+nt'_{r,w}} = 1 \qquad (\blacktriangle)$$

where $Q_w = -P_w(m, n)/P_1(m, n)$.

As in Theorem 8.0.8, we can estimate the non-S contribution to the height of each term in $(\blacktriangle)$ by

$$h(Q_w(m,n)) \leq R_w \max\{\log m, \log n\} + O(1)$$

for some constant R_w. On the other hand, we have the estimate

$$h(Q_w(m,n) u_1^{ms'_{1,w}+nt'_{1,w}} \cdots u_r^{ms'_{r,w}+nt'_{r,w}}) \geq c_w \max_i\{|ms'_{i,w} + nt'_{i,w}|\} - R_w \log \max\{m, n\} + O(1)$$

for some constant c_w.

In order to apply Corollary 6.2.2, we need each summand to be in $k_{S,\delta}$ for some $\delta < \frac{1}{W(W+1)}$. So it suffices to require, for every w,

$$C_w \max\{\log m, \log n\} \leq \max_i\{|ms'_{i,w} + nt'_{i,w}|\} \qquad (\bigstar)$$

where $C_w = \dfrac{4R_wW(W+1)}{c_w}$. For those (m,n) satisfying ($\bigstar$), we can apply Corollary 6.2.2 to ($\blacktriangle$). But since

$$h(Q_w(m,n)u_1^{ms'_{1,w}+nt'_{1,w}}\cdots u_r^{ms'_{r,w}+nt'_{r,w}}) \to \infty \text{ as } \max\{m,n\} \to \infty,$$

this implies that there are only finitely many solutions (m,n) of

$$\sum_{v\in M_k\setminus S_0} -\log^- \max\{|F(m)|_v, |G(n)|_v\} > \epsilon \max\{m,n\}$$

satisfying ($\bigstar$).

For pairs (m,n) not satisfying ($\bigstar$), there exists some w_0 and i_0 such that $(s'_{i_0,w_0}, t'_{i_0,w_0}) \neq (0,0)$ and

$$C_{w_0}\max\{\log m, \log n\} \geq |ms'_{i_0,w_0} + nt'_{i_0,w_0}|.$$

In fact, since as previously observed, $\min\{m,n\} \gg \max\{m,n\}$ for solutions (m,n) to ($\triangle$), we may assume $s'_{i_0,w_0}t'_{i_0,w_0} \neq 0$.

Fix such a pair (m,n) and corresponding w_0 and i_0. Let $a = s'_{i_0,w_0}, b = t'_{i_0,w_0}$, and $t = \max\left\{\left\lfloor \frac{m}{b}\right\rfloor, \left\lfloor -\frac{n}{a}\right\rfloor\right\}$. Replacing (a,b) by $(-a,-b)$ if necessary, we may assume that $a<0$ and $b>0$. We set $\mu_1 = m - bt$ and $\mu_2 = n + at$, so that $(m,n) = (bt,-at) + (\mu_1,\mu_2)$. Then clearly $\min\{|\mu_1|,|\mu_2|\} \leq \max\{|a|,|b|\}$ and so

$$\max\{|\mu_1|,|\mu_2|\} \ll |a\mu_1 + b\mu_2| = |am+bn| \ll \max\{\log m, \log n\} \ll \log t$$

as desired. □

CHAPTER 9

QUADRATIC POINTS ON ABELIAN SURFACES

Let C be a curve of genus 2 over a number field k, it is necessarily a hyperelliptic curve and we denote its hyperelliptic involution by σ. Let P_0 be a rational point on C, after possibly enlarging the number field k, and consider the embedding $j : C \to J(C), P \mapsto [P - P_0]$, where $[P - P_0]$ denote the divisor class of $P - P_0$ on C.

By Song-Tucker [19],

Theorem 9.0.1. *For any $\epsilon > 0$, there exists a constant $O_\epsilon(1)$ such that for all $P \in C(\bar{k})$ of degree d over k with $h^0(C, P^{[1]} + \cdots + P^{[d]}) = 1$, we have*

$$d_a(P) \leq h_K(P) + (2d - 2 + \epsilon)h(P) + O_\epsilon(1),$$

where P^i are the conjugates of P.

Let P be a quadratic point over k on C with τ the nontrivial element of the Galois group of $k(P)$ over k, suppose that $(P, \tau P) \neq (P, \sigma P)$. Then $P + \tau P \nsim 2P_0$, hence $\dim |P + \tau P| = 0$. The above theorem tells us

$$d_a(P) \leq h_K(P) + (2 + \epsilon)h(P) + O_\epsilon(1) \leq (4 + \epsilon)h(P).$$

On the other hand, we have

$$\phi : C^2 \to C^{(2)} \to J(C)$$

with the first map being the quotient by S_2 and the second map being the blow up along the point 0. In Silverman's definition of generalized GCD [18], let X be a variety and Y a subvariety of codimension at least 2, then let $\tilde{X}$ be the blow up of X along Y and $\tilde{Y}$ be the exceptional divisor. Let $\tilde{P}$ be the preimage of P in $\tilde{X}$. Then the generalized GCD of a point $P \in (X \setminus Y)$ with respect to Y is

$$h_{gcd}(P; Y) = h_{\tilde{X},\tilde{Y}}(\tilde{P}).$$

Followed by this definition, we can conjecture the GCD inequality on abelian surfaces, which is a consequence of Vojta's conjecture.

Conjecture 9.0.2. Let X be an abelian surface and A an ample divisor on X, then for $P \in X$ we have

$$h_{gcd}(P) \leq \epsilon h_A(P) + O(1)$$

for all points outside a Zariski closed proper subset Z of X.

It is well-known that all abelian varieties are quotients of Jacobian varieties, in particular, almost all abelian surfaces come from $J(C)$ of a curve C of genus 2. Then the question turns to whether the above inequality holds on $J(C)$. If we consider the rational points on $J(C)$, and they pull back to rational points on $C^{(2)}$ and all but finitely many pull back to quadratic points on C^2. By pulling everything back to C^2, the conjecture is equivalent to the following inequality on C, for $\{P \in C | [k(P) : k] = 2, \sigma P \neq \tau P\}$,

$$h_{\Delta_\alpha}(P) \leq \epsilon h_A(P) + O(1)$$

where $\Delta_\alpha = \{(P, \sigma P) | P \in C\}$. Note that we have the relation between arithmetic discriminant and heights:

$$d_a(P) = h_K(P) + 4h(P) - h_{\phi^*\Theta}(P^{[1]}, P^{[2]}) + O(1) \tag{9.1}$$

where Θ is the theta divisor defined by $\Theta = j(C)$ with j the map $j : C \to J(C)$ via $P \mapsto [P - P_0]$. Since

$$\phi^*\Theta = \Delta_\alpha + \{P_0\} \times C + C \times \{P_0\}$$

then if one assumes Conjecture 9.0.2 is true, then

$$\begin{aligned} d_a(P) &= 4h(P) - h_{\Delta_\alpha}(P^{[1]}, P^{[2]}) + O(1) \\ &\geq 4h(P) - \epsilon h(P) + O(1) \\ &\geq (4 - \epsilon)h(P). \end{aligned}$$

Hence in this case one should expect the conjecture

Conjecture 9.0.3. Notations are as before. For all but finitely many quadratic points P with $(P, \tau P) \neq (P, \sigma P)$, then if the GCD conjecture is true, we have

$$(4 - \epsilon)h(P) \leq d_a(P) \leq (4 + \epsilon)h(P).$$

Conjecture 9.0.3 is equivalent to Conjecture 9.0.2 in the case of Jacobians of genus two curves.

Remark 9.0.4. For the quadratic points P with $(P, \sigma P) = (P, \tau P)$ (the quadratic points coming from pulling back k-rational points via the hyperelliptic map $\psi : C \to \mathbb{P}^1$), the inequality of Conjecture 9.0.3 does not hold. In fact, we can show that for such points

$$(6 - \epsilon)h(P) \leq d_a(P) \leq (6 + \epsilon)h(P).$$

Consider $\psi \times \psi : C \times C \to \mathbb{P}^1 \times \mathbb{P}^1$. Let F_1 and F_2 be fibers of the two natural projections on $\mathbb{P}^1 \times \mathbb{P}^1$. Indeed, since $h_{\phi^*\Theta}(P, \sigma P) = h_\Theta(0)$ is constant for such points, this follows immediately from (9.1).

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Allcock, D. and Vaaler, J. D. (2009). A Banach space determined by the Weil height. *Acta Arith.*, 136(3):279–298.

[2] Bombieri, E. and Gubler, W. (2006). *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge.

[3] Bugeaud, Y., Corvaja, P., and Zannier, U. (2003). An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.*, 243(1):79–84.

[Corvaja et al.] Corvaja, P., Levin, A., and Zannier, U. Greatest common divisors over characteristic zero function fields. *preprint*.

[5] Corvaja, P. and Zannier, U. (2003). On the greatest prime factor of $(ab + 1)(ac + 1)$. *Proc. Amer. Math. Soc.*, 131(6):1705–1709.

[6] Corvaja, P. and Zannier, U. (2005). A lower bound for the height of a rational function at S-unit points. *Monatsh. Math.*, 144(3):203–224.

[7] Everest, G., van der Poorten, A., Shparlinski, I., and Ward, T. (2003). *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI.

[8] Evertse, J.-H. (2002). Points on subvarieties of tori. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 214–230. Cambridge Univ. Press, Cambridge.

[9] Fuchs, C. (2003). An upper bound for the G.C.D. of two linear recurring sequences. *Math. Slovaca*, 53(1):21–42.

[10] Grieve, N. (2020). Generalized GCD for toric Fano varieties. *Acta Arith.*, 195(4):415–428.

[11] Grieve, N. and Wang, J. T.-Y. (2020). Greatest common divisors with moving targets and consequences for linear recurrence sequences. *Trans. Amer. Math. Soc.*, 373(11):8095–8126.

[12] Hernández, S. and Luca, F. (2003). On the largest prime factor of $(ab+1)(ac+1)(bc+1)$. *Bol. Soc. Mat. Mexicana (3)*, 9(2):235–244.

[13] Hindry, M. and Silverman, J. H. (2000). *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York. An introduction.

[14] Levin, A. (2019). Greatest common divisors and Vojta's conjecture for blowups of algebraic tori. *Invent. Math.*, 215(2):493–533.

[15] Luca, F. (2005). On the greatest common divisor of $u - 1$ and $v - 1$ with u and v near $\mathcal{S}$-units. *Monatsh. Math.*, 146(3):239–256.

[16] Serre, J.-P. (1997). *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[17] Silverman, J. H. (1987). A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves. *J. Reine Angew. Math.*, 378:60–100.

[18] Silverman, J. H. (2005). Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. *Monatsh. Math.*, 145(4):333–350.

[19] Song, X. and Tucker, T. J. (2001). Arithmetic discriminants and morphisms of curves. *Trans. Amer. Math. Soc.*, 353(5):1921–1936.

[20] Vojta, P. (1987). *Diophantine approximations and value distribution theory*, volume 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin.

[21] Vojta, P. (1989). Mordell's conjecture over function fields. *Invent. Math.*, 98(1):115–138.

[22] Vojta, P. (1991a). Arithmetic discriminants and quadratic points on curves. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 359–376. Birkhäuser Boston, Boston, MA.

[23] Vojta, P. (1991b). Siegel's theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548.

[24] Vojta, P. (1992). A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing. *J. Amer. Math. Soc.*, 5(4):763–804.

[25] Wirsing, E. A. (1971). On approximations of algebraic numbers by algebraic numbers of bounded degree. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 213–247.