ABSTRACT

Title of dissertation: LINEAR FORMS IN LOGARITHMS AND INTEGER POINTS ON GENUS-TWO CURVES

John Vogler, Doctor of Philosophy, 2006

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

We consider a linear form with algebraic coefficients, evaluated at points on the analytic Jacobian of a genus-two curve whose projective coordinates are algebraic. Previous results on the existence of a lower bound of a particular shape are made explicit. We study various properties of Jacobians of genus-two curves, paying particular attention to their embeddings into projective space, and give a method which can be used to find provably all integer points on a genus-two curve. We apply this method to one particular curve by way of example.

LINEAR FORMS IN LOGARITHMS AND INTEGER POINTS ON GENUS-TWO CURVES

by

John Vogler

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2006

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor Niranjan Ramachandran
Professor Thomas Haines
Professor Harry Tamvakis
Professor William Gasarch

To my family.

Acknowledgments

I would like firstly to thank my advisor, Professor Washington, for the suggestions that prompted this paper, for mathematical advice, and for all of the time that he spent working with me to finish.

Next, I would like to thank Sinnou David, Victor Flynn, and Michel Waldschmidt for kindly taking the time to respond to my emails and questions about their papers.

None of this would have been possible without the immense support from my wife, Martha Vogler, who cared for and occupied our children countless hours in order to give me the space and time to work on my studies.

Lastly, I owe more than I know to God, who got me through it all even when it didn't seem possible.

Table of Contents

Chapter 1

Introduction and Terminology

1.1 History

In [1], Baker gave an explicit lower bound for a nonzero linear form in logarithms of algebraic numbers

$$|\beta_0 + \beta_1 \log \alpha_1 + ... + \beta_k \log \alpha_k| > Ce^{-(\log H)^\kappa}.$$

This H denotes an upper bound on the heights of the β's. The constant C depends on k, the α's, κ, and the degrees of the β's, but not on the β's themselves.

This theorem has since been improved in various ways, such as by tightening the bound. For example, in [2], we have

Theorem 1.1. *Let b_1, ..., b_n be integers, α_1, ..., α_n be algebraic numbers other than 0 or 1, and D be the degree of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}$. Let $B = \max\{|b_1|, \ldots, |b_n|, e^{1/D}\}$ and $A_i = \max\{\mathrm{h}(\alpha_i), |\log \alpha_i|/D, 1/D\}$. Let $L = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n$. If $L \neq 0$, then*

$$\log |L| \geq -CA_1 \ldots A_n \log B$$

where

$$C = 18(n+1)! n^{n+1} (32D)^{n+2} \log(2nD).$$

Another way in which Baker's theorem has been generalized is by allowing different kinds of logarithms in the linear form. For example, we can generalize to algebraic groups. The multiplicative group $\mathbb{G}_m$ has a tangent space $T_{\mathbb{G}_m}(\mathbb{C})$ which is isomorphic to $\mathbb{C}$, and its exponential map

$$\exp_{\mathbb{G}_m} : T_{\mathbb{G}_m}(\mathbb{C}) \to \mathbb{G}_m$$

is given by

$$\exp_{\mathbb{G}_m}(z) = e^z.$$

So we may consider our logarithms to be $u_i \in \mathbb{C}$, where $\exp_{\mathbb{G}_m}(u_i) = \alpha_i$ is an algebraic number for each i, or, in other words, $\exp_{\mathbb{G}_m}(u_i) \in \mathbb{G}_m(K)$ for some number field K.

In fact, the linear term β_0 may be considered a coefficient of $u_0 = 1$ in the tangent space of the additive group $\mathbb{G}_a$, $1 \in T_{\mathbb{G}_a}(\mathbb{C})$, where $\exp_{\mathbb{G}_a}(z) = z$. Then the linear form is

$$\beta_0 u_0 + \beta_1 u_1 + ... + \beta_k u_k,$$

where $u_i \in T_{G_i}(\mathbb{C})$ and satisfies $\exp_{G_i}(u_i) \in G_i(K)$ for certain algebraic groups, namely $G_0 = \mathbb{G}_a$ and $G_i = \mathbb{G}_m$ for $1 \leq i \leq k$.

In this context, it seems natural to ask if the theorem still holds in other algebraic groups. Except for the particular constants involved, the answer is yes. In [26], for example, Philippon and Waldschmidt gave the following lower bound.

Theorem 1.2. *Let G be an algebraic commutative group of dimension $d \geq 2$ defined over $\bar{\mathbb{Q}}$. Let*

$$\exp_G : T_G(\mathbb{C}) \to G(\mathbb{C})$$

denote the exponential map of G. Fix a basis of $T_G(\mathbb{C})$ defined over $\bar{\mathbb{Q}}$, and also an *embedding of G into projective space $\mathbb{P}^N$ defined over $\bar{\mathbb{Q}}$. Then there exists a positive real number C with the following property.*

Let K be any number field on which G, the embedding into projective space, and the basis for $T_G(\mathbb{C})$ are defined, and let D be its degree. Let

$$\mathcal{L}(\mathbf{z}) = \beta_1 z_1 + \beta_2 z_2 + ... + \beta_d z_d$$

be a nonzero linear form with coefficients in K (i.e. $\beta_i \in K$). Let $v \in T_G(\mathbb{C})$ such that $\gamma = \exp_G v \in G(K)$. Let $B \geq e$ and $V \geq e$ be real numbers with

$$\log B \geq \mathrm{h}(\beta_i) \text{ for } 1 \leq i \leq d,$$

$$\log V \geq \max(\mathrm{h}(\gamma), |v|^2)$$

If $\mathcal{L}(\mathbf{v}) \neq 0$, then

$$\log |L(v)| > -CD^{2d+2}(\log B + \log\log V)^{d+1}(\log V)^d.$$

They also had a more precise version of the theorem which, additionally, applies in the case where the logarithms could come from different algebraic groups. They did not, unfortunately, evaluate the constant C, or indicate how this might be done. Hirata-Kohno later improved this bound in [14] to

Theorem 1.3. *There exists a positive constant C with the following property. Let K be a number field on which the groups G_i, the bases of the tangent spaces of the G_i, and the embeddings of G_i in $\mathbb{P}^{N_i}$ are all defined. Let*

$$\mathcal{L}(\mathbf{z}) = \beta_0 z_0 + \beta_1 z_1 + ... + \beta_d z_d$$

be a nonzero linear form with coefficients in K (i.e. $\beta_i \in K$), on the tangent space $T_G(\mathbb{C})$. Let W be its kernel. For each $1 \leq i \leq k$, let $u_i \in T_{G_i}(\mathbb{C})$ with $u_i \neq 0$ such that $\gamma_i = \exp_{G_i}(u_i)$ belongs to $G_i(K)$. Write $\mathbf{v} = (1, u_1, \ldots, u_k) \in T_G(\mathbb{C})$ and $D = [K : \mathbb{Q}]$. Let B, E, V_1, ..., V_k be real numbers satisfying

$$\begin{aligned} D \log B &\geq \log V_i \\ \log B &\geq \max(e, \mathrm{h}(\beta_j), 0 \leq j \leq d) \\ \log V_i &\geq \max(\mathrm{h}(\gamma_i), |u_i|^{\rho_i} / D, 1/D) \\ e \leq E &\leq \min(e(D \log V_i)^{1/\rho_i} / |u_i|) \end{aligned}$$

One supposes additionally that for all algebraic subgroups G' of G with $T_{G'}(\mathbb{C}) \subset W$, one has $\mathbf{v} \notin T_{G'}(\mathbb{C})$. If $\mathcal{L}(\mathbf{v}) \neq 0$, then

$$\begin{aligned} \log |\mathcal{L}(v)| > &- C D^{2d+1} (\log B + \log DE) \times \\ & \left(\frac{\log \log B + \log D}{\log E} + 1 \right)^d \left(\prod_{i=1}^{k} (\log V_i)^{\delta_i} \right) (\log E)^{-d} \end{aligned}$$

Again, she did not indicate how to find the constant C.

Later, in [8], David evaluated the constant C in the particular case where G_i is an elliptic curve for $1 \leq i \leq k$. He proved

Theorem 1.4. *Let G_i ($1 \leq i \leq k$) be the elliptic curve given by*

$$y^2 = 4x^3 - g_{2,i}x - g_{3,i}$$

where $g_{2,i}$ and $g_{3,i}$ are elements of K. Let

$$\mathcal{L}(z) = \beta_0 z_0 + \beta_1 z_1 + \ldots + \beta_d z_d$$

be a nonzero linear form with coefficients in K (i.e. $\beta_i \in K$). For each $1 \leq i \leq k$, let u_i be a complex number such that $\gamma_i = (1, \wp_i(u_i), \wp_i'(u_i)) \in G_i(K) \subset \mathbb{P}^2(K)$ (or such that u_i is a pole of $\wp_i$, in which case $\gamma_i = (0,0,1)$). Write $\mathbf{v} = (1, u_1, \ldots, u_k) \in T_G(\mathbb{C})$ and $D = [K : \mathbb{Q}]$. Let B, E, V_1, ..., V_k be real numbers satisfying

$$D \log B \geq \log V_i$$

$$\log B \geq \max(eh, \mathrm{h}(\beta_j), 0 \leq j \leq k)$$

$$\log V_i \geq \max(\hat{\mathrm{h}}(\gamma_i), h, \frac{3\pi \left|u_i\right|^2}{D \left|\omega_{1,i} \operatorname{Im} \tau_i\right|})$$

$$e \leq E \leq \min(\frac{e(D \log V_i)^{1/2} \left|\omega_{1,i}\right| \sqrt{\operatorname{Im} \tau_i}}{\sqrt{3\pi} \left|u_i\right|}, 0 \leq i \leq k).$$

If $\mathcal{L}(\mathbf{v}) \neq 0$, then

$$\log|\mathcal{L}(\mathbf{v})| >$$

$$-CD^{2k+2}(\log B + \log DE)(\log E)^{-2k-1}(\log\log B + h + \log(DE))^{k+1} \prod_{i=1}^{k} (\log V_i),$$

where

$$C = 2.9(10^{6+6k})(4^{2k^2})(k+1)^{2k^2+9k+12.3}.$$

Using David's result, Gebel, Pethö, and Zimmer in [11] and Stroeker and Tzanakis in [36] independently showed how to find provably all integer points on an elliptic curve in Weierstrass form. This was shortly generalized in [37], [33], and [34] to quartics, to general nonsingular cubics, and to all genus-one plane curves, respectively.

Their technique could also apply to curves of higher genus if two obstacles could be overcome. Firstly, one would need to compute a set of Mordell-Weil generators for the Jacobian of the curve in question over $\mathbb{Q}$. Secondly, one would need to make the above theorems explicit, or, equivalently, generalize David's theorem to more algebraic groups, in particular, to Jacobians of dimension $g > 1$. This is much harder to do than simply prove that some constant exists that verifies the inequality.

Mordell-Weil generators are routinely computed on elliptic curves using descent, and this same method can also be used on higher-dimensional abelian varieties such as Jacobians, although it becomes computationally infeasible when the genus grows at all large, such as $g > 2$. But Flynn and others have recently computed a number of Mordell-Weil groups of Jacobians of genus-two curves (see, e.g., [10]).

It will be our purpose, therefore, to overcome the second obstacle for Jacobians of genus-two curves. In order to reduce the duplication of our work later by those wishing to extend to higher genus, we will do as much as we can for arbitrary abelian varieties and then we will come back and fill in the gaps for genus-two Jacobians. Finally, we will show how to use this result to find provably all integer points on a genus-two plane curve.

1.2 The Main Theorem

Let us suppose that G_i is an abelian variety, for $1 \leq i \leq k$, defined over a number field K of degree D over $\mathbb{Q}$, and $G_0 = \mathbb{G}_a$. Then G_i embeds into projective space, so we consider G_i to be an algebraic subset of $\mathbb{P}^{N_i}$. Let d_i be its dimension, and m_i its degree (under the aforementioned embedding). In particular, $N_0 = 1$, $d_0 = 1$, and $m_0 = 1$. Define $m = d! \prod_{i=0}^{k}(m_i/d_i!)$. Then the tangent space to G_i at the origin $T_{G_i}(\mathbb{C})$ is a vector space of dimension d_i. By fixing a basis of $T_{G_i}(\mathbb{C})$, we identify $T_{G_i}(\mathbb{C})$ with $\mathbb{C}^{d_i}$. We further suppose that the basis is defined over K.

Define the product group $\mathbb{G} = \mathbb{G}_a \times G_1 \times ... \times G_k$, which is a subset of $\bar{\mathbb{P}} = \mathbb{P}^1 \times \mathbb{P}^{N_1} \times ... \times \mathbb{P}^{N_k}$ and also an algebraic group of dimension d, where $d = 1 + d_1 + d_2 + ... + d_k$. Its tangent space is isomorphic to $T_{\mathbb{G}_a}(\mathbb{C}) \times T_{G_1}(\mathbb{C}) \times ... \times T_{G_k}(\mathbb{C})$ and therefore to $\mathbb{C}^d$.

We also have exponential maps on the G_i

$$\exp_{G_i} : T_{G_i}(\mathbb{C}) \to G_i$$

and an exponential map on the product group $\mathbb{G}$

$$\exp_{\mathbb{G}} : T_{\mathbb{G}}(\mathbb{C}) \to \mathbb{G}$$

$$\exp_{\mathbb{G}}(z_0, \mathbf{z}_1, \ldots, \mathbf{z}_k) = \exp_{G_0}(z_0) \times \exp_{G_1}(\mathbf{z}_1) \times \ldots \times \exp_{G_k}(\mathbf{z}_k).$$

The image of the exponential map is an element of multiprojective space. It will be convenient to look at particular coordinates. The exponential map can be given projectively by holomorphic functions

$$\Phi_{i,j} : \mathbb{C}^{d_i} \to \mathbb{C}.$$

We have, therefore,

$$\exp_{G_i}(\mathbf{z}_i) = \mathbf{\Phi}_i(\mathbf{z}_i) = (\Phi_{i,0}(\mathbf{z}_i), \ldots, \Phi_{i,N_i}(\mathbf{z}_i)) \in \mathbb{P}^{N_i}$$

and we will also denote

$$\mathbf{\Phi} = (\Phi_0, \ldots, \Phi_k).$$

As pointed out in [40], section 4(b), there are maps H_i^+ and $H_i^- : \mathbb{R}^+ \to \mathbb{R}$ such that for all $R \geq 0$ and all $\mathbf{z} \in \mathbb{C}^{d_i}$ with $|\mathbf{z}| \leq R$, one has

$$H_i^-(R) \leq \log \max\{|\Phi_{i,0}(\mathbf{z})|, \ldots, |\Phi_{i,N_i}(\mathbf{z})|\} \leq H_i^+(R).$$

Furthermore, H_i^+ and H_i^- may be chosen so that H_i^- is constant, and H_i^+ is quadratic,

$$H_i^+(R) = A_i^+R^2 + B_i^+R + C_i^+.$$

Multiplication by a scalar does not change the point in projective space, and so these functions $\Phi_{i,j}$ are not uniquely defined, which causes certain complications. It will, therefore, sometimes be more useful to look at the meromorphic functions

$$\mathbf{\Psi}_i : \mathbb{C}^{d_i} \to \mathbb{C}^{N_i}$$

given by the ratios

$$\Psi_{i,j} = \Phi_{i,j}/\Phi_{i,0}.$$

We will also denote

$$\mathbf{\Psi} = (\mathbf{\Psi}_0, \ldots, \mathbf{\Psi}_k).$$

Notice that the first coordinate in each embedding is given a special role by this definition of Ψ. The coordinates should be ordered so that this first coordinate (numbered 0) is nonzero at the identity of the group G_i.

Next, let $\mathbf{u}_i \in \mathbb{C}^{d_i}$ such that $\gamma_i = \exp_{G_i}(\mathbf{u}_i) \in G_i(K)$, and denote $\mathbf{u} = (u_0, \mathbf{u_1}, \ldots, \mathbf{u}_k)$. Notice that we use boldface to indicate a vector, and $\mathbf{u}_i \in \mathbb{C}^{d_i}$ for $i > 0$, but $d_0 = 1$ so u_0 is just a complex number.

In order to be able to apply the theorem to classes of abelian varieties G_i, we will allow a finite list of parameters $\vartheta_{i,1}, \ldots, \vartheta_{i,v_i}$, and we will denote $\mathrm{h}(G_i) = \mathrm{h}(1, \vartheta_{i,1}, \ldots, \vartheta_{i,v_i})$. These are assumed to be elements of K.

The fact that G_i is an algebraic group implies that the group law can be given in terms of polynomials in projective space. In particular, for every point (p, q) of

$G_i \times G_i$ there are polynomials $R_j^{(i)}(X_{i,0}, \ldots, X_{i,N_i}, X'_{i,0}, \ldots, X'_{i,N_i})$ homogeneous of degree c_i in the X variables, homogeneous of degree c_i in the X' variables, of degree (at most) c'_i in the parameters $\vartheta_{i,n}$, with integer coefficients, and with length (i.e. sum of the absolute values of the integer coefficients) at most r_i, such that, not all are zero at (p, q), and, projectively (i.e. up to a scalar multiple),

$$\Phi_{i,j}(\mathbf{z} + \mathbf{z}') = R_j^{(i)}(\mathbf{\Phi}_i(\mathbf{z}), \mathbf{\Phi}_i(\mathbf{z}')).$$

Let $c = \max\{c_i\}$. By the remark preceding Definition 4.1 of [24], one can choose the projective embedding of the G_i such that $c_i \leq 2$ for all i. While we will have $c = 2$ for genus-two curves (and for elliptic curves), our main theorem will not assume that $c = 2$ so that it may be applied to more general embeddings.

Fix an index i and thus a group G_i. By Lemma 4.1 (pg. 291) of [26], or Proposition 1.2.3 of [41], if one also fixes j and normalizes G_i variables by setting $X_{i,j} = 1$, then there exist homogeneous polynomials $Q_{k,l}^{(i,j)}(X_{i,0}, \ldots, X_{i,N_i})$, giving the k'th partial derivative of the variable $X_{i,l}$ in the group G_i. Said differently,

$$Q_{k,l}^{(i,j)}(X_{i,0}/X_{i,j}, X_{i,1}/X_{i,j}, \ldots, X_{i,N_i}/X_{i,j})$$

is the k'th partial derivative of the ratio $X_{i,l}/X_{i,j}$, and therefore

$$\frac{\partial}{\partial z_j} \frac{\Phi_{i,l}}{\Phi_{i,j}} = Q_{k,l}^{(i,j)}(\Phi_{i,0}, \ldots, \Phi_{i,N_i})/\Phi_{i,j}^{q_i},$$

where q_i is the degree of $Q_{k,l}^{(i,j)}$ in the X variables. When $j = l$, we clearly have $Q_{k,j}^{(i,j)} = 0$. Disregarding the case $j = l$, in practice q_i does not depend on j, k, or l. This is, however, not important, since the degree can be increased by multiplying $Q_{k,l}^{(i,j)}$ by $X_{i,j}$; so one might prefer to regard q_i as the maximum of the degrees of

$Q^{(i,j)}_{k,l}$ over $0 \leq j \leq N_i$, $1 \leq k \leq d_i$, $0 \leq l \leq N_i$. In fact, there is a positive integer κ_i such that $\kappa_i Q^{(i,j)}_{k,l}$ is a polynomial of degree q_i in the X variables., of degree q_i' in the parameters $\vartheta_{i,n}$, with integer coefficients and length at most r_i'.

Finally, let $\mathrm{h}(P)$ denote the height of the projective point P on the group G_i. (Height functions will be discussed in greater detail in Chapter 3.) Let $\hat{\mathrm{h}}(P)$ denote the canonical height

$$\hat{\mathrm{h}}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P).$$

Let $\hbar_i$ be a number such that

$$\mathrm{h}(P) \leq \hat{\mathrm{h}}(P) + \hbar_i$$

for all points P on G_i. (While $\hat{\mathrm{h}}$ depends on the group G_i, we will not subscript it since the group will always be clear from the point P.)

We wish to find an explicit lower bound for the linear form

$$\mathcal{L}(\mathbf{z}) = \beta_0 z_0 + \beta_1 z_1 + ... + \beta_{d-1} z_{d-1}$$

evaluated at

$$(z_0, z_1, ..., z_{d-1}) = (u_0, u_{1,1}, ..., u_{1,d_1}, ..., u_{k,1}, ..., u_{k,d_k}).$$

The bound will involve certain constants (i.e. depending only on the group $\mathbb{G}$) whose values will be determined in one case in the next section. The general result will only assume that C_1 is a constant satisfying the equations and inequalities given in Chapter 4.

First we define a parameter E such that

$$\log E \geq 1.$$

This parameter allows for better bounds when the numbers $|u_i|$ are small, but for many applications it is easiest simply to take $E = e$. Next we define parameters V_i, for each $1 \leq i \leq k$, which depend on the point $\mathbf{u}_i$. They need to satisfy

$$\log V_i \geq \max\left\{\hat{\mathrm{h}}(\gamma_i),\, (\log E)/D,\, A_i^+ \left|\mathbf{u}_i\right|^2 E^2/D\right\}.$$

The numbers B_i^+ and C_i^+ can also affect the result, but to a much lesser degree, so they only need to be considered if they are very large. About them, we will only assume that

$$\begin{aligned} D\log V_i \geq &(2A_i^+ + B_i^+)\left|\mathbf{u}_i\right| E/(50d!(2(k+1))^{d-1}) \\ D\log V_i \geq &(A_i^+ + B_i^+ + C_i^+)/(50d!(2(k+1))^{d-1})^2. \end{aligned}$$

Finally, we have the parameter B which depends on the coefficients β_i. We will assume that

$$\begin{aligned} \log B \geq &\max\{\mathrm{h}(\beta_j), 0 \leq j \leq d-1\} \\ \log\log B \geq &\max\{1,\, (\log E)/D,\, (\log\log V_i)/D,\, \mathrm{h}(G_i),\, \hbar_i\,/m,\, 1 \leq i \leq k\} \end{aligned}$$

Theorem 1.5. *With the notation from this section, if $\mathcal{L}(\mathbf{u}) \neq 0$, then*

$$\log|\mathcal{L}(\mathbf{u})| > -C_1 D^{2d}(\log B)(\log\log B)^d(\log E)^{-(2d-1)}\prod_{i=1}^{k}(\log V_i)^{d_i},$$

It will often be convenient to denote a d-tuple using subscripts from 0 to $d-1$, and it will often be convenient to denote it in $k+1$ groups of d_i elements, with double subscripts i,j where $0 \leq i \leq k$ and $1 \leq j \leq d_i$. We will use both notations. Therefore, if $\mathbf{z} \in \mathbb{C}^d$, then $z_i \in \mathbb{C}$ (where $0 \leq i \leq d$) and $z_{i,j} \in \mathbb{C}$ (where $0 \leq i \leq k$ and $1 \leq j \leq d_i$) but $\mathbf{z}_i \in \mathbb{C}^{d_i}$ (where $0 \leq i \leq k$).

1.3 Genus Two

In the case where G_i is the Jacobian of a genus-two curve

$$y^2 = f_{i,6}x^6 + f_{i,5}x^5 + f_{i,4}x^4 + f_{i,3}x^3 + f_{i,2}x^2 + f_{i,1}x + f_{i,0},$$

for each $i > 0$, we evaluate the constants in Chapter 7. Recall the definitions from the previous section. In particular, D is the degree of K over $\mathbb{Q}$, the numbers A_i^+, B_i^+, and C_i^+ come from the function H_i^+ which must be computed from the period matrices of each Jacobian. The result is the following:

Theorem 1.6. *If the parameters E, V_i, and B are chosen so that they satisfy*

$$\begin{aligned}
\log E \geq & 1 \\
\log V_i \geq & \max\left\{\hat{\mathrm{h}}(\gamma_i),\ (\log E)/D,\ A_i^+ \left|\mathbf{u}_i\right|^2 E^2/D\right\} \\
D \log V_i \geq & (2A_i^+ + B_i^+)\left|\mathbf{u}_i\right| E/(150(2k+3)!(2k+2)^{2k}) \\
D \log V_i \geq & (A_i^+ + B_i^+ + C_i^+)/(150(2k+3)!(2k+2)^{2k})^2 \\
\log B \geq & \max\{\mathrm{h}(\beta_j), 0 \leq j \leq 2k\} \\
\log\log B \geq & \max\{1,\ (\log E)/D,\ (\log\log V_i)/D,\ \mathrm{h}(G_i),\ \hbar_i\,/((2k+1)!2^{4k}),\ 1 \leq i \leq k\}
\end{aligned}$$

and if $\mathcal{L}(\mathbf{u}) \neq 0$, then

$$\log\left|\mathcal{L}(\mathbf{u})\right| > -C_1 D^{4k+2}(\log B)(\log\log B)^{2k+1}(\log E)^{-(4k+1)} \prod_{i=1}^{k}(\log V_i)^{d_i},$$

where an upper bound for C_1 is given by the following table.

k	C_1
1	2.1×10^{44}
2	6.8×10^{112}
3	6.6×10^{219}
4	2.5×10^{369}
5	4.9×10^{564}
6	1.9×10^{808}
7	2.1×10^{1102}
8	4.6×10^{1448}
$k \geq 9$	$(2k^2)^{16k^2+14k+3}2^{22k+8}$

Chapter 2

Overview of the Main Proof

2.1 Short Overview

Essentially all proofs in the field of Diophantine approximation come down to four general steps:

- Construct an auxiliary function.
- Show it is nonzero.
- Find an analytic upper bound.
- Find an arithmetic lower bound.

The first step generally uses some form of Siegel's lemma to get an auxiliary polynomial with the necessary properties and still have some control on its size (that is, the size of its coefficients). In our case, we will use Lemma 2.3 (which is Lemma 6.1 of [26]).

The next three steps refer to certain values of the auxiliary function. In our case, they refer to a large (but finite) set of points and the first several derivatives of the auxiliary function at those points.

For the second step, we will use a variant of Philippon's "Lemme de zéros" ([24]), which says that if the auxiliary polynomial has enough zeros of sufficiently high order, then there exists a subgroup with certain properties. But if the parameters defining the auxiliary polynomial are chosen correctly, then the existence of this subgroup can be ruled out from the beginning. The fact that these values of the auxiliary function are nonzero will be used to get the arithmetic lower bound.

The third step requires the bound on the size of the auxiliary polynomial given by Siegel's lemma, and it also generally uses some complex analysis, as well as the hypothesis that our linear form is especially small. That is, we construct the polynomial in such a way that, if linear form in logarithms is very small, then this gives us a way to get a very small upper bound on the values in question on our auxiliary function.

Finally, the lower bound comes from estimating (that is, bounding) the heights of the values in question, and using the Louiville inequality: A nonzero algebraic number of degree D and height h has absolute value $\geq \exp(-Dh)$. This is why it is important that we deal in algebraic numbers, and it is also why we needed to perform the second step in order to prove that the values in question are nonzero. In our case, bounding the height requires looking at the group law on our abelian variety (on our Jacobian embedded into projective space), describing what happens to the polynomial when one takes derivatives, examining heights of points, canonical heights, and so forth. This lower bound is called the "Inequality of the Tail" in the literature, and so we will use the same name.

2.2 Long Overview

The main ideas used in this proof come from [8], although his lemmas and theorems were not appropriate for citing, since they used particular values for the constants which are only valid for elliptic curves. All of the constants had to be changed, as well as a few of the arguments, but this proof follows his method.

Define the number

$$U_0 = C_2 D^{2d} (\log B)(\log\log B)^d (\log E)^{-(2d-1)} \prod_{i=1}^{k} (\log V_i)^{d_i},$$

where C_2 is a constant (i.e. depending only on $\mathbb{G}$) to be determined later.

We begin by hypothesizing that

$$|\mathcal{L}(\mathbf{u})| \leq \exp(-C_3 U_0),$$

and we will use this to find a contradiction.

Our proof will follow the method of [26] and [14] and [8]. First of all, we may assume that $\beta_0 = -1$ as follows. In case $\beta_0 = 0$, we change β_0 to -1 and u_0 to 0. In case $\beta_0 \neq 0$, we change β_i to $-\beta_i/\beta_0$ for all i, and we relax the condition $\log B > \mathrm{h}(\beta_i)$ to $2\log B > \mathrm{h}(\beta_i)$. In what follows, we will be using the Hilbert function, which we will denote $\mathrm{Hf}(\mathbb{G}; \mathbf{L})$, and the leading term of the Hilbert function, which we will denote $\mathrm{H}(\mathbb{G}; \mathbf{L})$. Both are discussed in greater detail in the next chapter.

Ultimately, our proof will use P. Philippon's "Lemme de zéros" [24]. The following comes from [40] (Prop. 3.1 and the comment following) which is an application of the method of [9] to [25].

Lemma 2.1. *Let $\mathbb{G} = \mathbb{G}_a \times \mathbb{G}_1 \times ... \times \mathbb{G}_k$ embed in $\bar{\mathbb{P}} = \mathbb{P} \times \mathbb{P}^{N_1} \times ... \times \mathbb{P}^{N_k}$. Let W be a subspace of the tangent space to $\mathbb{G}$ at the origin. Let k be a nonnegative integer, and T, L_0, L_1, ... L_k be positive integers. Let Σ be a finite set of points of $\mathbb{G}(\mathbb{C})$ containing the identity element 0 of the algebraic group $\mathbb{G}$. Suppose that there is a polynomial P of $\mathbb{C}[\bar{\mathbb{P}}]$ of multidegree at most $(L_0, L_1, ...L_k)$, not identically zero on $\mathbb{G}$, but with a zero of order at least $(k+1)T+1$ along W at all points of $\Sigma^{(k+1)}$. Then there exists a connected algebraic subgroup $\mathbb{G}'$ of $\mathbb{G}$ ($\mathbb{G}' \neq \mathbb{G}$), such that the following inequality holds:*

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}') \operatorname{H}(\mathbb{G}'; L_0, ..., L_k) \leq \operatorname{H}(\mathbb{G}; L_0, ..., L_k)$$

where r is the codimension of $W \cap T_{\mathbb{G}'}(\mathbb{C})$ in W.

The notation $\Sigma^{(k+1)}$ is defined to be

$$\Sigma^{(k+1)} = \{\sigma_0 + \ldots + \sigma_k : \sigma_i \in \Sigma \text{ for all } i\}.$$

In our case, W will be the kernel of our linear form, which is a subspace of $T_{\mathbb{G}}(\mathbb{C})$ of dimension $d-1$ (hence codimension 1), and $\Sigma = \{s\mathbf{u} : s \in \mathbb{Z}, 0 \leq s < S\}$ for some integer S, so that $\Sigma^{(k+1)} \subset \{s\mathbf{u} : s \in \mathbb{Z}, 0 \leq s < (k+1)S\}$.

We will need to construct an auxiliary polynomial as in Lemma 2.1. But first we need to choose parameters so that the conclusion of the lemma cannot be true. We will define numbers S, T, S_1, T_1, U_0, $L_i^{\#}$ (for $1 \leq i \leq k$) and various c_i, and we will define $L_i = \lfloor L_i^{\#} \rfloor$ for $0 \leq i \leq k$, where $L_0^{\#}$ is given by the following lemma.

Lemma 2.2. *Let T be a positive integer, and let C_4, $L_1^{\#}$, ..., $L_k^{\#}$ be positive real numbers. Let Σ be a finite set of points of $\mathbb{G}(\mathbb{C})$. Then there exists a real number*

$L_0^{\#}$ *such that every connected algebraic subgroup* $\mathbb{G}'$ *of* $\mathbb{G}$ *with* $T_{\mathbb{G}'}(\mathbb{C}) \subset W$ *satisfies*

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0^{\#}, \ldots, L_k^{\#}) \geq (1 + C_4)\, \mathrm{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#}),$$

where $r+1$ *is the codimension of* $\mathbb{G}'$ *in* $\mathbb{G}$, *and there is (at least) one such subgroup* $\tilde{\mathbb{G}}$ *with equality. Additionally,* $C_5 \leq \lfloor L_0^{\#} \rfloor \leq L_0^{\#} \leq C_6 U_0/(D \log B)$.

Constructing this auxiliary polynomial is the hard part. It will have the form

$$P = \sum_{\boldsymbol{\lambda}, i} a_{\boldsymbol{\lambda},i} \xi_i \mathbf{X}^{\boldsymbol{\lambda}}$$

for certain rational numbers $a_{\boldsymbol{\lambda},i}$ (in fact, they will be integers in our construction) where the i runs from 1 to $D = [K : \mathbb{Q}]$ and the ξ_i form a basis for K as a vector space over $\mathbb{Q}$. We denote by $\mathbb{C}[\bar{\mathbb{P}}]$ the space of multihomogeneous polynomials with complex coefficients. It is generated by monomials of the form

$$\prod_{i,j} X_{i,j}^{\lambda_{i,j}},$$

and by multihomogeneous we mean that the sums $\sum_j \lambda_{i,j}$ (for all i) are the same in each term of the polynomial. We write $(\mathbb{C}[\bar{\mathbb{P}}]/I(\mathbb{G}))_{\mathbf{L}}$ to mean the vector subspace of those with multidegree $\mathbf{L}$, i.e. $\sum_j \lambda_{i,j} = L_i$ for each i. We write

$$\boldsymbol{\lambda} = (\lambda_{i,j})_{0 \leq i \leq k, 0 \leq j \leq N_i}$$

which satisfies, for all i,

$$\sum_{j=0}^{N_i} \lambda_{i,j} = L_i.$$

We write $\mathbf{X}^{\boldsymbol{\lambda}}$ to mean

$$\prod_{i,j} X_{i,j}^{\lambda_{i,j}}$$

We choose a set Λ such that $\{\mathbf{X}^{\boldsymbol{\lambda}}\}_{\boldsymbol{\lambda}\in\Lambda}$ is a set of representatives in $\mathbb{C}[\bar{\mathbb{P}}]$ of

$$(\mathbb{C}[\bar{\mathbb{P}}]/I(\mathbb{G}))_{\mathbf{L}}$$

and we let $\boldsymbol{\lambda}$ run over Λ in the sum defining P. It will be important later that

$$\begin{aligned}\operatorname{card}(\Lambda) &= \dim_{\mathbb{C}} \left(\mathbb{C}[\bar{\mathbb{P}}]/I(\mathbb{G})\right)_{\mathbf{L}} \\ &= \mathrm{Hf}(\mathbb{G};\mathbf{L}).\end{aligned}$$

Suppose that F is a meromorphic function on $\mathbb{C}^d$, and for each i, $\mathbf{x}_i = (x_{i,0},\ldots,x_{i,d-1}) \in \mathbb{C}^d$. Then we denote

$$\mathrm{D}_{\mathbf{x}_i} F = \sum_{j=0}^{d-1} x_{i,j} \frac{\partial F}{\partial z_j}.$$

If V is a vector subspace of $\mathbb{C}^d$, we say, as in Lemma 2.1, that P has a zero of order $\geq T$ along V at $\mathbf{z}$ if exists a basis $\{\mathbf{x}_1,\ldots,\mathbf{x}_h\}$ of V such that the function

$$F = P \circ \mathbf{\Phi} : \mathbb{C}^d \to \mathbb{C}$$

has

$$\mathrm{D}_{\mathbf{x}_1}^{t_1} \circ \ldots \circ \mathrm{D}_{\mathbf{x}_h}^{t_h} F(\mathbf{z}) = 0$$

for all h-tuples $\mathbf{t} = (t_1,\ldots,t_h) \in \mathbb{Z}^h$ with $t_i \geq 0$ for all i and $|\mathbf{t}| = t_1 + ... + t_h < T$. We will henceforth use the shorter notation

$$\mathrm{D}_{\mathbf{x}}^{\mathbf{t}} F(\mathbf{z}) = \mathrm{D}_{\mathbf{x}_1}^{t_1} \circ \ldots \circ \mathrm{D}_{\mathbf{x}_h}^{t_h} F(\mathbf{z}).$$

This definition does not depend on the choice of basis of V.

In our case, we want our function F to have a zero of large order along the kernel W of our linear form at many (but finitely many) points. Suppose that a basis for W is given by $\mathbf{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_{d-1}\}$. We will describe how this basis should be chosen later. (In fact, we will eventually have need to use a different basis. It will be denoted $\mathbf{e} = \{\mathbf{e}_1, \ldots, \mathbf{e}_{d-1}\}$ and will also be defined later.) Therefore, we want

$$\mathrm{D}_{\mathbf{f}}^{\mathbf{t}}\, F(s\mathbf{u}) = 0$$

for all $s \in \mathbb{Z}$ such that $0 \le s < S_1$ and all $\mathbf{t} \in \mathbb{Z}^{d-1}$ such that $0 \le t_i$ and $\sum_{i=1}^{d-1} t_i \le T_1$, i.e. $|\mathbf{t}| \le T_1$. (It will become apparent later why we won't be taking, as one might expect, $S_1 = (k+1)S$ and $T_1 = (k+1)T$.)

Well, since

$$F = P \circ \Phi = \sum_{\boldsymbol{\lambda}, i} a_{\boldsymbol{\lambda},i} \xi_i \Phi^{\boldsymbol{\lambda}}$$

and

$$\mathrm{D}_{\mathbf{f}}^{\mathbf{t}}\, F(s\mathbf{u}) = \sum_{\boldsymbol{\lambda}, i} a_{\boldsymbol{\lambda},i} \xi_i \, \mathrm{D}_{\mathbf{f}}^{\mathbf{t}}(\Phi^{\boldsymbol{\lambda}}(s\mathbf{u})),$$

we see that the system

$$\mathrm{D}_{\mathbf{f}}^{\mathbf{t}}\, F(s\mathbf{u})$$

is linear in the unknowns $a_{\boldsymbol{\lambda},i}$.

Therefore, we use a form of Siegel's Lemma to solve this linear system for the unknowns $a_{\boldsymbol{\lambda},i}$ and thereby find a polynomial P that satisfies our equations and has bounded height. We will be using

Lemma 2.3. *(Thue-Siegel) Let $(u_{i,j})_{1 \le i \le \nu, 1 \le j \le \mu}$ be a matrix of complex numbers, of rank at most ρ. Let δ, M, and p be positive real numbers such that*

$$\left[2\mu e^{\delta+M+p} + 1\right]^{2\rho} \le e^{\nu\delta},$$

and

$$\max_{1\le j\le \mu}\sum_{i=1}^{\nu}|u_{i,j}|\le e^{M}.$$

Then there exists $(a_1, ..., a_\nu)\in\mathbb{Z}^\nu$ *such that*

$$0<\max_{1\le i\le\nu}|a_i|\le e^{\delta}$$

and

$$\max_{1\le j\le\mu}\left|\sum_{i=1}^{\nu}u_{i,j}a_i\right|\le e^{-p}.$$

This is lemma 6.1 of [26] (pg 301) and is proved there using a Pigeonhole-Principle argument.

In order to use this lemma, we first need an upper bound on the rank of our system ρ, the number of equations μ, and the size of the coefficients

$$\xi_i\,\mathrm{D}_{\mathbf{f}}^{\mathbf{t}}\,\Phi^{\boldsymbol{\lambda}}(s\mathbf{u}),$$

and we also need a lower bound on the number of unknowns ν.

In order to satisfy the inequality in the lemma, it is necessary that $2\rho<\nu$, which is why using the upper bound ν for the rank ρ will not help. Another upper bound is μ, but we can't prove that the ratio μ/ν is bounded, so this is also too large for our purposes, and we need something a bit finer. We will prove

$$\nu\ge C_7D\rho$$

where C_7 is a small constant (less than $2/D$) to be given later. We will also prove

$$\log(2\mu)\le\frac{1}{2}U_0.$$

We will prove that the number

$$M = \log \max_{s,\mathbf{t}} \sum_{i,\boldsymbol{\lambda}} \left|\xi_i \, \mathrm{D}_{\mathbf{f}}^{\mathbf{t}} \, \Phi^{\lambda}(s\mathbf{u})\right|$$

satisfies

$$M \leq C_8 U_0.$$

Then we will take

$$p = C_9 U_0$$

and

$$\delta = C_{10} U_0 / D,$$

and after giving values for the constants $C_7, \ldots, C_{10}$, we will show that

$$C_8 + C_9 + C_{10} + 1 \leq \frac{1}{2} C_7 C_{10},$$

thereby establishing

$$\log(2\mu) + \delta + M + p + \frac{1}{2\mu} \exp(-\delta - m - p) \leq \nu\delta/2\rho,$$

and therefore

$$\left(2\mu e^{\delta+M+p} + 1\right)^{2\rho} \leq e^{\nu\delta}$$

(using the inequality $\log(1+x) \leq x$, which is valid for all real $x > -1$, and therefore $\log(1 + \frac{1}{2\mu}\exp(-\delta - M - p)) \leq \frac{1}{2\mu}\exp(-\delta - M - p) < \frac{1}{2} < \frac{1}{2}U_0$).

So we conclude that we have a polynomial P such that $F = P \circ \Phi$ has

$$\left|\mathrm{D}_{\mathbf{f}}^{\mathbf{t}} \, F(s\mathbf{u})\right| < e^{-p}$$

for all $|\mathbf{t}| \leq T_1$ and $0 \leq s \leq S_1$, and we also know that $|a_{\boldsymbol{\lambda},i}| \leq e^{\delta}$.

Computing the rank required us to use a special basis $\mathbf{f}$, but the remainder of the argument works better using a different basis $\mathbf{e}$, so we will convert between them using the following.

Lemma 2.4.

$$\left|\log\max\{\left|\mathrm{D}_{\mathbf{f}}^{\mathbf{t}}\,F(\mathbf{z})\right|, |\mathbf{t}| \le T'\} - \log\max\{\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(\mathbf{z})\right|, |\mathbf{t}| \le T'\}\right| \le T'\log(d-1).$$

In particular, we have

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(s\mathbf{u})\right| < \exp(-C_{11}U_0) \tag{2.1}$$

for all $|\mathbf{t}| \le T_1$ and $0 \le s \le S_1$, and we also know that

Even if we could show that $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(s\mathbf{u}) = 0$ for all such s and $\mathbf{t}$ (which we will do), we still have not used the hypothesis that

$$|\mathcal{L}(\mathbf{u})| < \exp(-C_3U_0),$$

and we can expect no useful results without using this hypothesis.

We will use the hypothesis as follows. Since $\mathcal{L}(\mathbf{u})$ is very small, $\mathbf{u}$ is very near a point w on the vector space $W = \ker\mathcal{L}$, and since w lies in the space along which we are taking derivatives, the function

$$f(z) = \mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(z\mathbf{u}),$$

of a single complex variable, has small derivatives as well, and we can apply to it the following lemma.

Lemma 2.5. *(Extrapolation) Let f be a function analytic in the disc $\{z : |z| \le R\} \subset \mathbb{C}$. Let S' and T' be two positive integers and r a real number such that $S' \ge 2$*

and $S' \le r \le \frac{1}{2}R$*. Then we have*

$$|f|_{2r} \le 2\,|f|_R \left(\frac{4r}{R}\right)^{T'S'} + 5\left(\frac{18r}{S'}\right)^{T'S'} \max\left\{\left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right|,\, 0 \le t < T',\, 0 \le s < S'\right\}$$

Proof. See Prop 7.5 of [8], or Lemme 2-3 of [39] (taking $\mathcal{E} = \{s \in \mathbb{Z} : 0 \le s < S'\}$, $l = S'$, $\delta = 1$), or Lemma 2 of [7]. □

This lemma allows us to get more small values than we started with (which, as we shall see, equates to more zeros). We will use it to prove the following:

Lemma 2.6. *For all* $|\mathbf{t}| \le (k+1)T$ *and* $0 \le s < (k+1)S$*,*

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u})\right| < \exp(-C_{12}U_0).$$

Making use of these lemmas requires relating the values of $F(s\mathbf{u})$ and $F(s\mathbf{w})$. We will prove that for all $|\mathbf{t}| \le T_1$ and $0 \le s < S_1$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u}) - \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{w})\right| < \exp(-C_{11}U_0)$$

and conclude therefore that for such s and $\mathbf{t}$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{w})\right| < 2\exp(-C_{11}U_0).$$

Next, we will fix some $\mathbf{t}$ with $|\mathbf{t}| \le (k+1)T$ and then apply Lemma 2.5 with

$$\begin{aligned} f(z) &= \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(z\mathbf{w}) \\ r &= \frac{1}{2}(k+1)S \\ R &= 2(k+1)SE \\ S' &= S_1 \\ T' &= (k+1)T. \end{aligned}$$

While $|f|_{2r}$ might be large, $(4r/R)^{T'S'} = E^{-T'S'}$ is small, and while $(18r/S')^{T'S'}$ might be large, the derivatives $f^{(t)}(s)$ are small. More precisely, we will prove that

$$2\,|f|_R \left(\frac{4r}{R}\right)^{T'S'} < \frac{1}{4}\exp(-C_{12}U_0)$$

and

$$5\left(\frac{18r}{S'}\right)^{T'S'} \max\left\{\left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right|,\, 0 \le t < T',\, 0 \le s < S'\right\} < \frac{1}{4}\exp(-C_{12}U_0)$$

so that we may conclude that for all $|\mathbf{t}| \le (k+1)T$ and $0 \le s \le (k+1)S$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{w})\right| < \frac{1}{2}\exp(-C_{12}U_0).$$

Then we will prove that for all such s and $\mathbf{t}$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{u}) - \mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{w})\right| < \frac{1}{2}\exp(-C_{12}U_0),$$

and therefore

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{u})\right| < \exp(-C_{12}U_0)$$

for all $|\mathbf{t}| \le (k+1)T$ and $0 \le s \le (k+1)S$,

Finally, all of the above tells us that F and many of its derivatives are small, but Lemma 2.1 needs them to vanish completely. So we will compute bounds on the heights of such values, with the intent to prove that any nonzero value must, in fact, be larger than the upper bounds that we already found.

Lemma 2.7. *(Inequality of the Tail) If* $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{u}) \neq 0$, *where* $|\mathbf{t}| \le (k+1)T$ *and* $0 \le s \le (k+1)S$, *and* $|\mathbf{t}|$ *is minimal with this property, then*

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{u})\right| > \exp(-C_{12}U_0).$$

Therefore, we may conclude that for all $|\mathbf{t}| \leq (k+1)T$ and $0 \leq s \leq (k+1)S$, $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\, F(s\mathbf{u}) = 0$, and consequently, the polynomial P has a zero of order $\geq (k+1)T+1$ along W at all points $s\mathbf{u}$ with $0 \leq s < (k+1)S$. By Lemma 2.1, there is an algebraic connected subgroup $\mathbb{G}'$ of $\mathbb{G}$ ($\mathbb{G}' \neq \mathbb{G}$) with

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0, ..., L_k) \leq \mathrm{H}(\mathbb{G}; L_0, ..., L_k).$$

In order to use Lemma 2.2, first we will prove

Lemma 2.8. *The subgroup $\mathbb{G}'$ in the Lemme de zéros has $T_{\mathbb{G}'}(\mathbb{C}) \subset W$.*

Finally, we will arrive at a contradiction by showing that the inequalities

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0, ..., L_k) \leq \mathrm{H}(\mathbb{G}; L_0, ..., L_k)$$

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0^{\#}, L_1^{\#}, \ldots, L_k^{\#}) \geq (1 + C_4)\, \mathrm{H}(\mathbb{G}; L_0^{\#}, L_1^{\#}, \ldots, L_k^{\#})$$

together imply that

$$\begin{aligned} T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0^{\#}, L_1^{\#}, \ldots, L_k^{\#}) & \\ &\geq (1 + C_4)\, \mathrm{H}(\mathbb{G}; L_0^{\#}, L_1^{\#}, \ldots, L_k^{\#}) \\ &\geq (1 + C_4)\, \mathrm{H}(\mathbb{G}; L_0, ..., L_k) \\ &\geq (1 + C_4) T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0, ..., L_k) \\ &> T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0^{\#}, L_1^{\#}, \ldots, L_k^{\#}), \end{aligned}$$

(see Equation 5.1 for the last inequality) which is a contradiction. Therefore, our hypothesis that

$$|\mathcal{L}(\mathbf{u})| < \exp(-C_3 U_0),$$

must be false.

Chapter 3

Background Material

3.1 Review of Heights

The height of an algebraic number α is given by

$$\mathrm{h}(\alpha) = \frac{1}{D} \log \left(C_D \prod_{i=1}^{D} \max\{1, \alpha_i\} \right)$$

where α_i, for $1 \leq i \leq D$, are the D Galois conjugates of α and C_D is the leading coefficient of the minimal polynomial

$$p(x) = C_D \prod_{i=1}^{D} (x - \alpha_i) \in \mathbb{Z}[x]$$

normalized so that the coefficients are integers that do not share a common prime factor. It can be shown that this height is also given in terms of valuations on a number field by

$$\mathrm{h}(\alpha) = \frac{1}{[K:\mathbb{Q}]} \log \prod_{\nu} \max\{1, |\alpha|_{\nu}^{n_\nu}\}$$

for any number field K which contains α. (Here, the number n_ν is the degree of the local field over $\mathbb{Q}_p$.)

We also define the height of a k-tuple of algebraic numbers by

$$\mathrm{h}(\alpha_1, \alpha_2, ..., \alpha_k) = \frac{1}{[K:\mathbb{Q}]} \log \prod_{\nu} \max\{|\alpha_1|_{\nu}^{n_\nu}, |\alpha_2|_{\nu}^{n_\nu}, ..., |\alpha_k|_{\nu}^{n_\nu}\}$$

This height is, in fact, defined on projective points, since the product formula

$$\prod_{\nu} |x|_{\nu}^{n_\nu} = 1,$$

implies that

$$\mathrm{h}(\beta\alpha_1, \beta\alpha_2, ..., \beta\alpha_k) = \mathrm{h}(\alpha_1, \alpha_2, ..., \alpha_k).$$

The height function has the properties

$$\mathrm{h}(p/q) = \log\max\{|p|\,, |q|\}$$

for a rational number p/q in lowest terms,

$$\mathrm{h}(\alpha^m) = |m|\,\mathrm{h}(\alpha)$$

for any integer m,

$$\mathrm{h}(\alpha\beta) \leq \mathrm{h}(\alpha) + \mathrm{h}(\beta)$$

$$\mathrm{h}(\alpha_1 + \alpha_2 + ... + \alpha_k) \leq \mathrm{h}(\alpha_1) + \mathrm{h}(\alpha_2) + ... + \mathrm{h}(\alpha_k) + \log(k)$$

and any positive integer k. Furthermore,

$$\mathrm{h}(1, \alpha) = \mathrm{h}(\alpha)$$

$$\mathrm{h}(\alpha_1 + \alpha_2 + ... + \alpha_k) \leq \mathrm{h}(1, \alpha_1, \alpha_2, ..., \alpha_k) + \log(k)$$

$$\mathrm{h}(1, \alpha_1, \alpha_2, ..., \alpha_k) \leq \mathrm{h}(\alpha_1) + \mathrm{h}(\alpha_2) + ... + \mathrm{h}(\alpha_k)$$

$$\mathrm{h}(1, \{\alpha_i\beta_j\}_{1\leq i\leq r, 1\leq j\leq s}) \leq \mathrm{h}(1, \{\alpha_i\}_{1\leq i\leq r}) + \mathrm{h}(1, \{\beta_j\}_{1\leq j\leq s})$$

$$\mathrm{h}(1, \{\sum_{i=1}^{k} \alpha_{ij}\}_{1\leq j\leq r}) \leq \mathrm{h}(1, \{\alpha_{ij}\}_{1\leq i\leq k, 1\leq j\leq r}) + \log(k).$$

It will also be important that the height of a collection of positive integers including 1 is equal to the logarithm of the greatest integer in the collection.

$$\mathrm{h}(1, n_1, n_2, ..., n_k) = \log\max\{1, n_1, n_2, ..., n_k\}.$$

We can prove most of these formulas easily by manipulating the product over valuations. We write $D = [K : \mathbb{Q}]$ for some number field K containing all of the algebraic numbers in the formula. First of all,

$$\mathrm{h}(1, \alpha) = \mathrm{h}(\alpha)$$

follows directly from the definition. For $m > 0$,

$$\begin{aligned}
\exp[D\,\mathrm{h}(\alpha^m)] &= \prod_\nu \max\{1, |\alpha^m|_\nu^{n_\nu}\} \\
&= \prod_\nu \max\{1, |\alpha|_\nu^{n_\nu}\}^m \\
&= \exp[D\,\mathrm{h}(\alpha)]^m \\
&= \exp[Dm\,\mathrm{h}(\alpha)].
\end{aligned}$$

Taking logs and dividing by D, we have the result for positive m. For $m < 0$,

$$\mathrm{h}(\alpha^m) = \mathrm{h}(1, \alpha^m) = \mathrm{h}(\alpha^{-m}, 1) = \mathrm{h}(\alpha^{-m}) = (-m)\,\mathrm{h}(\alpha).$$

Next,

$$\begin{aligned}
\exp[D\,\mathrm{h}(\alpha\beta)] &= \prod_\nu \max\{1, |\alpha\beta|_\nu^{n_\nu}\} \\
&= \prod_\nu \max\{1, |\alpha|_\nu^{n_\nu}\,|\beta|_\nu^{n_\nu}\} \\
&\le \prod_\nu \max\{1, |\alpha|_\nu^{n_\nu}\} \prod_\nu \max\{1, |\beta|_\nu^{n_\nu}\} \\
&= \exp[D\,\mathrm{h}(\alpha)]\exp[D\,\mathrm{h}(\beta)] \\
&= \exp[D\,\mathrm{h}(\alpha) + D\,\mathrm{h}(\beta)]
\end{aligned}$$

More generally,

$$
\begin{aligned}
&\exp[D\,\mathrm{h}(1,\{\alpha_i\beta_j\}_{1\le i\le r, 1\le j\le s})]\\
&\qquad\qquad = \prod_{\nu} \max\{1, \{|\alpha_i\beta_j|_{\nu}^{n_\nu}\}_{1\le i\le r, 1\le j\le s}\}\\
&\qquad\qquad \le \prod_{\nu} \max\{1, \{|\alpha_i|_{\nu}^{n_\nu}\}_{1\le i\le r}\} \prod_{\nu} \max\{1, \{|\beta_j|_{\nu}^{n_\nu}\}_{1\le j\le s}\}\\
&\qquad\qquad = \exp[D\,\mathrm{h}(1, \{\alpha_i\}_{1\le i\le r})] \exp[D\,\mathrm{h}(1, \{\beta_j\}_{1\le j\le s})]\\
&\qquad\qquad = \exp[D\,\mathrm{h}(1, \{\alpha_i\}_{1\le i\le r}) + D\,\mathrm{h}(1, \{\beta_j\}_{1\le j\le s})]
\end{aligned}
$$

For sums, we need to distinguish between finite (non-Archimedean) and infinite (Archimedean) valuations, since the former satisfy the ultrametric inequality

$$|x+y|_{\nu} \le \max\{|x|_{\nu}, |y|_{\nu}\}$$

whereas the latter do not, but still satisfy the triangle inequality

$$|x+y|_{\nu} \le |x|_{\nu} + |y|_{\nu}.$$

We will distinguish these by writing $\nu \nmid \infty$ and $\nu \mid \infty$. Using this, and the fact that

$$\sum_{\nu|\infty} n_\nu = D,$$

we have

$$
\begin{aligned}
&\exp[D\,\mathrm{h}(\alpha_1+\alpha_2+...+\alpha_k)]\\
&\qquad=\prod_{\nu}\max\{1,|\alpha_1+\alpha_2+...+\alpha_k|_\nu^{n_\nu}\}\\
&\qquad=\prod_{\nu\nmid\infty}\max\{1,|\alpha_1+\alpha_2+...+\alpha_k|_\nu^{n_\nu}\}\prod_{\nu|\infty}\max\{1,|\alpha_1+\alpha_2+...+\alpha_k|_\nu^{n_\nu}\}\\
&\qquad\le\prod_{\nu\nmid\infty}\max\{1,|\alpha_1|_\nu^{n_\nu},|\alpha_2|_\nu^{n_\nu},...,|\alpha_k|_\nu^{n_\nu}\}\prod_{\nu|\infty}\max\{1,|\alpha_1|_\nu^{n_\nu}+|\alpha_2|_\nu^{n_\nu}+...+|\alpha_k|_\nu^{n_\nu}\}\\
&\qquad\le\prod_{\nu\nmid\infty}\max\{1,|\alpha_1|_\nu^{n_\nu},|\alpha_2|_\nu^{n_\nu},...,|\alpha_k|_\nu^{n_\nu}\}\prod_{\nu|\infty}k^{n_\nu}\max\{1,|\alpha_1|_\nu^{n_\nu},|\alpha_2|_\nu^{n_\nu},...,|\alpha_k|_\nu^{n_\nu}\}\\
&\qquad=\prod_{\nu}\max\{1,|\alpha_1|_\nu^{n_\nu},|\alpha_2|_\nu^{n_\nu},...,|\alpha_k|_\nu^{n_\nu}\}\prod_{\nu|\infty}k^{n_\nu}\\
&\qquad=k^D\prod_{\nu}\max\{1,|\alpha_1|_\nu^{n_\nu},|\alpha_2|_\nu^{n_\nu},...,|\alpha_k|_\nu^{n_\nu}\}\\
&\qquad=k^D\exp[D\,\mathrm{h}(1,\alpha_1,\alpha_2,...,\alpha_k)]\\
&\qquad=\exp[D(\mathrm{h}(1,\alpha_1,\alpha_2,...,\alpha_k)+\log(k))]
\end{aligned}
$$

More generally,

$$\begin{aligned}
&\exp[D\,\mathrm{h}(1,\{\sum_{i=1}^{k}\alpha_{ij}\}_{1\le j\le r})]\\
&\quad=\prod_{\nu}\max\{1,\{\left|\sum_{i=1}^{k}\alpha_{ij}\right|_{\nu}^{n_\nu}\}_{1\le j\le r}\}\\
&\quad=\prod_{\nu\nmid\infty}\max\{1,\{\left|\sum_{i=1}^{k}\alpha_{ij}\right|_{\nu}^{n_\nu}\}_{1\le j\le r}\}\prod_{\nu\mid\infty}\max\{1,\{\left|\sum_{i=1}^{k}\alpha_{ij}\right|_{\nu}^{n_\nu}\}_{1\le j\le r}\}\\
&\quad\le\prod_{\nu\nmid\infty}\max\{1,\{|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le i\le k,1\le j\le r}\}\prod_{\nu\mid\infty}\max\{1,\{\sum_{i=1}^{k}|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le j\le r}\}\\
&\quad\le\prod_{\nu\nmid\infty}\max\{1,\{|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le i\le k,1\le j\le r}\}\prod_{\nu\mid\infty}k^{n_\nu}\max\{1,\{|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le i\le k,1\le j\le r}\}\\
&\quad=\prod_{\nu}\max\{1,\{|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le i\le k,1\le j\le r}\}\prod_{\nu\mid\infty}k^{n_\nu}\\
&\quad=k^{D}\prod_{\nu}\max\{1,\{|\alpha_{ij}|_{\nu}^{n_\nu}\}_{1\le i\le k,1\le j\le r}\}\\
&\quad=k^{D}\exp[D\,\mathrm{h}(1,\{\alpha_{ij}\}_{1\le i\le k,1\le j\le r})]\\
&\quad=\exp[D\,\mathrm{h}(1,\{\alpha_{ij}\}_{1\le i\le k,1\le j\le r})+D\log(k)]
\end{aligned}$$

Finally, we define the height of a polynomial with algebraic coefficients to be the height of the projective point whose coordinates are 1 and the coefficients of the polynomial. When the polynomial has integer coefficients, we can get more precise bounds on sums, products, and values of such polynomials by considering, instead of the height of the polynomial, its length, which is defined to be the sum of the absolute values of its coefficients.

For example, if P has n terms, degree d, height $\mathrm{h}(P)$, and length L, then

$$\mathrm{h}(P(\beta))\le\log L+d\,\mathrm{h}(\beta)\le\mathrm{h}(P)+\log n+d\,\mathrm{h}(\beta).$$

Since $\mathrm{h}(P)$ is the log of the maximum of the coefficients of P, the length gives a better bound on $\mathrm{h}(P(\beta))$ unless all of the coefficients are equal. The easiest way to deal with lengths of polynomials is to consider the polynomial of length L to have L terms and all coefficients ± 1.

When $\mathbf{n}$ is a k-tuple of integers, we will also use the notation $|\mathbf{n}|$ to denote the length of $\mathbf{n}$.

$$|\mathbf{n}| = |n_1| + |n_2| + \ldots + |n_k|\,.$$

3.2 Review of Hilbert Functions

The ring of homogeneous polynomials in $N+1$ variables with complex coefficients is denoted $\mathbb{C}[X_0, X_1, \ldots, X_N]$ or (for brevity, and to emphasize that the polynomials must be homogeneous) $\mathbb{C}[\mathbb{P}^N]$ with those polynomials of degree n denoted $\{\mathbb{C}[\mathbb{P}^N]\}_n$.

An ideal $I \subset \mathbb{C}[\mathbb{P}^N]$ defines an algebraic variety V and an embedding into projective space $\mathbb{P}^N$. The quotient ring $\mathbb{C}[\mathbb{P}^N]/I$ is the coordinate ring of the variety and may be thought of as the ring of polynomials on the variety. The subset of polynomials of degree n is denoted $\{\mathbb{C}[\mathbb{P}^N]/I\}_n$.

The Hilbert function on I is the dimension of this vector space over $\mathbb{C}$,

$$\mathrm{Hf}(I; n) = \dim_{\mathbb{C}}\{\mathbb{C}[\mathbb{P}^N]/I\}_n.$$

We also write $\mathrm{Hf}(V; n)$ to mean $\mathrm{Hf}(I; n)$, but since Hf depends on the particular embedding of V into projective space, the notation $\mathrm{Hf}(V; n)$ only makes sense when a particular embedding of V is understood.

For every ideal I, there is a polynomial, $\mathrm{Hp}(I; x)$, called the Hilbert polynomial, such that

$$\mathrm{Hf}(I;x) = \mathrm{Hp}(I;x)$$

for all integers x that are sufficiently large. See [13] for a proof. Furthermore, the Hilbert polynomial has degree d, where d is the dimension of I (or of V), and the leading term is

$$(m/d!)x^d.$$

The number m is a positive integer called the degree of I (or of V). The degree is the maximum number of intersections of a linear space in $\mathbb{P}^N$ of codimension d. It turns out that this maximum is achieved generically, in the sense that the collection of linear spaces in $\mathbb{P}^N$ of codimension d which achieve the maximum is a Zariski open subset of all such linear spaces.

Since the Hilbert polynomial must take on values which are positive integers when the variable x is a sufficiently large integer, by considering finite differences of this polynomial, it is easy to see that all of the coefficients must be rational numbers, and, in fact, they must be integers divided by (some factor of) $d!$.

A lower bound is given by Nesterenko in [23] (see also [29])

$$\binom{x+d+1}{d+1} - \binom{x-m+d+1}{d+1} \leq \mathrm{Hf}(V;x). \tag{3.1}$$

He also gave an upper bound

$$\mathrm{Hf}(V;x) \leq m(4x)^d, \tag{3.2}$$

but tighter upper bounds were given by Chardin in [6]

$$\mathrm{Hf}(V;x) \leq m\binom{x+d}{d} \tag{3.3}$$

with a slightly more improved upper bound given by him in [5]

$$\mathrm{Hf}(V;x) \leq \binom{x+d}{d} + (m-1)\binom{x+d-1}{d}. \tag{3.4}$$

It is worth pointing out that the lower bound and both of Chardin's upper bounds are polynomials in x with the same leading term as the Hilbert polynomial. (This is a feature not shared with Nesterenko's upper bound.) In fact, those same three bounds are all equal when $m = 1$, which means that we have an exact value for the Hilbert function of a linear surface,

$$\mathrm{Hf}(L;x) = \binom{x+d}{d}.$$

When x is very large, we can compare the Hilbert function to the leading term as follows.

Lemma 3.1. *If $x \geq 1$ then*

$$\mathrm{Hf}(V;x) \geq \frac{m}{d!}x^d\left(1 - \frac{d!d(d+2)2^{d+1}m^d}{x}\right)$$

Proof. From 3.1 we have

$$\mathrm{Hf}(V;x) \geq \binom{x+d+1}{d+1} - \binom{x-m+d+1}{d+1}$$

If we expand the binomial coefficient as a polynomial, we get

$$\binom{x+d+1}{d+1} = \frac{1}{(d+1)!}\sum_{j=0}^{d+1} s_j x^j,$$

where s_j is the sum of all $\binom{d+1}{j}$ products of $d+1-j$ of the integers $1, 2, \ldots, d+1$. Evaluating the above at $x = 1$ gives

$$\sum_{j=0}^{d+1} s_j = (d+1)!\binom{d+2}{d+1} = (d+2)!.$$

Using the Binomial Theorem,

$$\begin{aligned}\binom{x+d+1}{d+1}-\binom{x-m+d+1}{d+1} =&\frac{1}{(d+1)!}\sum_{j=0}^{d+1} s_j\left(x^j-(x-m)^j\right)\\ =&\frac{1}{(d+1)!}\sum_{j=0}^{d+1}\sum_{i=0}^{j-1}(-1)^{j-i+1}\binom{j}{i}s_jm^{j-i}x^i\\ =&\frac{1}{(d+1)!}\sum_{i=0}^{d}\sum_{j=i+1}^{d+1}(-1)^{j-i+1}\binom{j}{i}s_jm^{j-i}x^i\\ =&\sum_{i=0}^{d} r_ix^i,\end{aligned}$$

where

$$r_i=\frac{1}{(d+1)!}\sum_{j=i+1}^{d+1}(-1)^{j-i+1}\binom{j}{i}s_jm^{j-i}.$$

In particular, $r_d = m/d!$, $r_{d-1} = m(d+2-m)/2(d-1)!$, and when $i < d$

$$\begin{aligned}|r_i| \leq&\frac{1}{(d+1)!}\binom{d+1}{i}m^{d+1-i}\sum_{j=0}^{d+1}s_j\\ \leq&\frac{1}{(d+1)!}\binom{d+1}{i}m^{d+1-i}(d+2)!\\ =&(d+2)\binom{d+1}{i}m^{d+1-i}\\ \leq&(d+2)2^{d+1}m^{d+1}.\end{aligned}$$

Therefore, we have

$$\begin{aligned}\left|\binom{x+d+1}{d+1}-\binom{x-m+d+1}{d+1}-\frac{m}{d!}x^d\right| =&\left|\sum_{i=0}^{d-1}r_ix^i\right|\\ \leq&\sum_{i=0}^{d-1}|r_i|\,x^i\\ \leq&d(d+2)2^{d+1}m^{d+1}x^{d-1}\end{aligned}$$

and so

$$\begin{aligned}\mathrm{Hf}(V;x) \geq & \binom{x+d+1}{d+1} - \binom{x-m+d+1}{d+1} \\ \geq & \frac{m}{d!}x^d - d(d+2)2^{d+1}m^{d+1}x^{d-1} \\ = & \frac{m}{d!}x^d\left(1 - \frac{d!d(d+2)2^{d+1}m^d}{x}\right)\end{aligned}$$

□

Since we will be dealing with products of algebraic varieties, We can generalize this notion to multihomogeneous ideals in multiprojective space $\bar{\mathbb{P}} = \mathbb{P}^{N_1} \times \mathbb{P}^{N_2} \times ... \times \mathbb{P}^{N_k}$

$$I \subset \mathbb{C}[X_{1,0}, ..., X_{1,N_1}, X_{2,0}, ..., X_{2,N_2}, ..., X_{k,0}, ..., X_{k,N_k}] = \mathbb{C}[\bar{\mathbb{P}}].$$

The Hilbert function on I (or on V) is defined by

$$\mathrm{Hf}(I; n_1, n_2, ..., n_k) = \dim_{\mathbb{C}}\{\mathbb{C}[\bar{\mathbb{P}}]/I\}_{n_1,n_2,...,n_k}.$$

As in the one-variable case, there is a polynomial, $\mathrm{Hp}(V; x_1, x_2, ..., x_k)$, of degree d, called the Hilbert polynomial, such that

$$\mathrm{Hf}(I; x_1, x_2, ..., x_k) = \mathrm{Hp}(I; x_1, x_2, ..., x_k)$$

whenever all of the x_i are sufficiently large integers. This is Theorem 7 (pg 757) of [38]. See also the appendix of [18].

Furthermore, in the special case when $V = V_1 \times V_2 \times ... \times V_k$ where V_i is a variety in $\mathbb{P}^{N_i}$, the vector space of polynomials on V is a tensor product of those on V_i,

$$\mathbb{C}[\bar{\mathbb{P}}]/I \;\cong \mathbb{C}[\mathbb{P}^{N_0}]/I_0 \otimes \ldots \otimes \mathbb{C}[\mathbb{P}^{N_k}]/I_k,$$

and therefore,

$$\mathrm{Hf}(V_1 \times V_2 \times ... \times V_k; x_1, x_2, ..., x_k) = \mathrm{Hf}(V_1; x_1)\,\mathrm{Hf}(V_2; x_2) ... \,\mathrm{Hf}(V_k; x_k), \qquad (3.5)$$

and therefore similarly for the Hilbert polynomial.

Using the notation of [24] we write

$$\mathrm{H}(V; x_1, x_2, ..., x_k)$$

to denote the homogeneous polynomial consisting of those terms of the Hilbert polynomial of maximum degree (that is, of degree d), multiplied by the integer $d!$. The extra factor is included so that the coefficients of H are all integers.

By Lemma 3.1 and the following paragraph in [24],

$$\mathrm{H}(I; x_1, x_2, ..., x_k) = \sum_{\alpha_1 + ... + \alpha_k = d} c_{\boldsymbol{\alpha}}(I) \frac{d!}{\alpha_1! \dots \alpha_k!} x_1^{\alpha_1} \dots x_k^{\alpha_k}$$

for $0 \leq \alpha_i \leq N_i$, $\alpha_1 + \ldots + \alpha_k = d$, and for all $\boldsymbol{\alpha}$, the coefficient $c_{\boldsymbol{\alpha}}(I)$ is a nonnegative integer, a generalization of the degree of I in the one-variable case. The numbers $c_{\boldsymbol{\alpha}}(I)$ are given by

$$c_{\boldsymbol{\alpha}}(I) = \deg_{\boldsymbol{\alpha}}(V) = H(V \cap L_1 \cap \ldots \cap L_k; 1, \ldots, 1)$$

where L_i is a general linear subvariety of $\mathbb{P}^{N_i}$ of codimension α_i. The reader will notice the similarity between this formula and the formula for the leading term of the one-variable Hilbert function.

Chapter 4

Some Lemmas

Lemma 4.1. *Let $a_{i,j}$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$ be complex numbers, $\mathbf{f}_1, \ldots, \mathbf{f}_m$ elements of $\mathbb{C}^d$, and $f : \mathbb{C}^d \to \mathbb{C}$ a complex-valued function analytic in a neighborhood of $\mathbf{z} \in \mathbb{C}^{\mathbf{d}}$. Let*

$$\mathbf{u}_i = \sum_{j=1}^{m} a_{i,j} \mathbf{f}_j$$

and

$$A = \max_{1 \leq i \leq n} \left\{ \sum_{j=1}^{m} |a_{i,j}| \right\}.$$

Then for any positive integer T,

$$\max_{|\mathbf{t}|=T} \left\{ \left| \mathrm{D}_{\mathbf{u}_1}^{t_1} \circ \ldots \circ \mathrm{D}_{\mathbf{u}_n}^{t_n} f(\mathbf{z}) \right| \right\} \leq A^T \max_{|\tau|=T} \left\{ \left| \mathrm{D}_{\mathbf{f}_1}^{\tau_1} \circ \ldots \circ \mathrm{D}_{\mathbf{f}_m}^{\tau_m} f(\mathbf{z}) \right| \right\}$$

Proof. This is lemma 3.1 of [26], but we will reproduce the proof here since it is short, and we will need a variant for the next lemma. For $1 \leq i \leq n$, we have

$$\mathrm{D}_{\mathbf{u}_i} = \sum_{j=1}^{m} a_{i,j} \, \mathrm{D}_{\mathbf{f}_j},$$

and therefore

$$\prod_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j} \, \mathrm{D}_{\mathbf{f}_j} \right)^{t_i} = \sum_{j_1=1}^{m} \ldots \sum_{j_T=1}^{m} a_{i_1,j_1} \ldots a_{i_T,j_T} \, \mathrm{D}_{\mathbf{f}_{j_1}} \ldots \mathrm{D}_{\mathbf{f}_{j_T}}, \tag{4.1}$$

where $(i_1, \ldots, i_T) = (1, \ldots, 1, 2, \ldots, 2, \ldots, n, \ldots, n)$ with each number i repeated t_i times, for $1 \leq i \leq n$, and the result follows from

$$\left| \sum_{j_1=1}^{m} \ldots \sum_{j_T=1}^{m} a_{i_1,j_1} \ldots a_{i_T,j_T} \right| \leq A^T.$$

□

For our purposes, we need the following variant of the above lemma.

Lemma 4.2. *Let $a_{i,j}$ $(1 \le i \le n,\ 1 \le j \le m)$ be complex numbers, $\mathbf{f}_1, \ldots, \mathbf{f}_m$ elements of $\mathbb{C}^d$, and $f : \mathbb{C}^d \to \mathbb{C}$ a complex-valued function analytic in a neighborhood of $\mathbf{z}$, with $\mathrm{D}^t_{\mathbf{f}_1} f(\mathbf{z}) = 0$ for all $\mathbf{z}$ when $t > L$. Let*

$$\mathbf{u}_i = \sum_{j=1}^{m} a_{i,j}\mathbf{f}_j$$

and

$$\begin{aligned} A_0 =& \max\left\{1,\ |a_{i,1}|\,,\ 1 \le i \le n\right\}, \\ A_1 =& \max\left\{1,\ |a_{i,j}|\,,\ 1 \le i \le n, 2 \le j \le m\right\}. \end{aligned}$$

Then for any positive integer T,

$$\max_{|\mathbf{t}|=T} \left\{\left|\mathrm{D}^{t_1}_{\mathbf{u}_1} \circ \ldots \circ \mathrm{D}^{t_n}_{\mathbf{u}_n} f(\mathbf{z})\right|\right\} \le m^T A_0^L A_1^T \max_{|\tau|=T} \left\{\left|\mathrm{D}^{\tau_1}_{\mathbf{f}_1} \circ \ldots \circ \mathrm{D}^{\tau_m}_{\mathbf{f}_m} f(\mathbf{z})\right|\right\}$$

Proof. Since $\mathrm{D}^t_{\mathbf{f}_0} f(\mathbf{z}) = 0$ when $t > L_0$, we can remove from Equation 4.1 all summands where $j_t = 1$ for more than L values of t, and the sum of the remaining coefficients is bounded by

$$\left|\sum a_{i_1,j_1} \ldots a_{i_T,j_T}\right| \le m^T A_0^L A_1^T,$$

since there are at most m^T terms, each of which has at most L terms $a_{i,1}$ and at most T terms $a_{i,j}$ with $j \ge 2$. □

Lemma 4.3. *Let P be a polynomial in $\mathbb{C}[\bar{\mathbb{P}}]$ of multidegree $\le (L_0, \ldots, L_k)$. Let $\Phi_{i,j} : \mathbb{C}^{d_i} \to \mathbb{C}$ be holomorphic functions, and H_i^+ nondecreasing real-valued functions* *satisfying*

$$\log \max_{0\le j\le N_i} |\Phi_{i,j}(z)| \le H_i^+(|z|).$$

Suppose P has K terms, and all coefficients of absolute value $\le H$. Suppose $\mathbf{t} \in \mathbb{Z}^l$ and $T = |\mathbf{t}| = \sum_{i=1}^l t_i$. Suppose $\mathbf{x}_i \in \mathbb{C}^d$ for $1 \le i \le l$, and $\mathbf{v} = (v_0, \ldots, v_{d-1}) \in \mathbb{C}^d$. Then $F = P \circ \mathbf{\Phi}$ satisfies

$$\begin{aligned}\log \left|\mathrm{D}^{\mathbf{t}}_{\mathbf{x}} F(\mathbf{v})\right| \le & T\log d + L_0 \log \max_i \{1, |x_{i,0}|\} + T \log \max_{i,j>0}\{1, |x_{i,j}|\} \\ & + T\log T + \log K + \log H + \sum_{i=0}^k L_i H_i^+(|\mathbf{v}|+1).\end{aligned}$$

Proof. By Lemma 4.2, we have

$$\begin{aligned}\left|\mathrm{D}^{\mathbf{t}}_{\mathbf{x}} F(\mathbf{v})\right| \le & d^T \max_i \{1, |x_{i,0}|\}^{L_0} \max_{i,j>0}\{1, |x_{i,j}|\}^T \times \\ & \max\left\{\left|\left(\frac{\partial}{\partial z_0}\right)^{\tau_1} \circ \ldots \circ \left(\frac{\partial}{\partial z_{d-1}}\right)^{\tau_{d-1}} F(\mathbf{v})\right|, |\boldsymbol{\tau}| = T\right\}\end{aligned}$$

By Cauchy's Theorem,

$$\begin{aligned}&\left\{\left|\left(\frac{\partial}{\partial z_0}\right)^{\tau_1} \circ \ldots \circ \left(\frac{\partial}{\partial z_{d-1}}\right)^{\tau_{d-1}} F(\mathbf{v})\right|, |\boldsymbol{\tau}| = T\right\} \\ &\le T! \sup\{|F(\mathbf{z})| : |\mathbf{z}_i - \mathbf{v}_i| \le 1, 0 \le i \le k\} \\ &\le \exp\left(T\log T + \log K + \log H + \sum_{i=0}^k L_i H_i^+(|\mathbf{v}|+1)\right).\end{aligned}$$

□

Recall that we defined W to be the kernel of our linear form

$$\mathcal{L}(\mathbf{z}) = -z_0 + \beta_1 z_1 + \beta_2 z_2 + ... + \beta_{d-1} z_{d-1}.$$

For $1 \le i \le d-1$, let

$$\mathbf{e}_i = (\beta_i, 0, \ldots, 0, 1, 0, \ldots, 0),$$

where the 1 is in the $(i+1)$'st position. Then the $\mathbf{e}_i$ form a basis for W. Let

$$\begin{aligned}\mathbf{w} =&(\beta_1 u_1 + ... + \beta_{d-1} u_{d-1}, u_1, \ldots, u_{d-1})\\ =&\beta_1 \mathbf{e}_1 + ... + \beta_{d-1}\mathbf{e}_{d-1} \in W,\end{aligned}$$

which has

$$\mathbf{w} - \mathbf{u} = (\mathcal{L}(\mathbf{u}), 0, \ldots, 0).$$

There is an isomorphism between W and $\mathbb{C}^{d-1}$ given by

$$a_1\mathbf{e}_1 + \ldots + a_{d-1}\mathbf{e}_{d-1} \to (a_1, \ldots, a_{d-1}),$$

and the usual metric on $\mathbb{C}^{d-1}$ may be pulled back to a metric on W, with respect to which the basis $(\mathbf{e}_1, \ldots, \mathbf{e}_{d-1})$ is orthonormal. Recall the subgroup $\tilde{\mathbb{G}}$ defined in Lemma 2.2. Let $\tilde{d}$ denote its dimension, and $\tilde{r} = d - 1 - \tilde{d}$. Since $T_{\tilde{\mathbb{G}}}(\mathbb{C}) \subset W$, we may also choose a basis $(\mathbf{f}_1, \ldots, \mathbf{f}_{\tilde{d}})$ of $T_{\tilde{\mathbb{G}}}(\mathbb{C})$ orthonormal with respect to our derived metric on W, and extend it to an orthonormal basis $(\mathbf{f}_1, \ldots, \mathbf{f}_{d-1})$ of W. Then the change-of-basis matrices between $(\mathbf{e}_1, \ldots, \mathbf{e}_{d-1})$ and $(\mathbf{f}_1, \ldots, \mathbf{f}_{d-1})$ are unitary, so all entries of those matrices have absolute value ≤ 1. Applying Lemma 4.1 to both of these matrices (inverses of one another), proves

Lemma 4.4.

$$\log\max\{\left|\mathrm{D}^{\mathbf{t}}_{\mathbf{f}} F(\mathbf{z})\right|, |\mathbf{t}| \leq T'\} \leq \log\max\{\left|\mathrm{D}^{\mathbf{t}}_{\mathbf{e}} F(\mathbf{z})\right|, |\mathbf{t}| \leq T'\} + T'\log(d-1),$$

$$\log\max\{\left|\mathrm{D}^{\mathbf{t}}_{\mathbf{e}} F(\mathbf{z})\right|, |\mathbf{t}| \leq T'\} \leq \log\max\{\left|\mathrm{D}^{\mathbf{t}}_{\mathbf{f}} F(\mathbf{z})\right|, |\mathbf{t}| \leq T'\} + T'\log(d-1).$$

Now we will give values to the parameters mentioned in Chapter 2. Recall the definitions of D, B, E, and V_i from Chapter 1. Define

$$\begin{aligned}
S &= \lfloor C_{13} D \log\log B / \log E \rfloor \\
U_0 &= C_2 D^{2d} (\log B)(\log\log B)^d (\log E)^{-(2d-1)} \prod_{i=1}^{k} (\log V_i)^{d_i} \\
T &= \lfloor U_0 / D \log\log B \rfloor \\
L_i^{\#} &= U_0 (\log E)^2 / C_{15} D^3 (\log V_i)(\log\log B)^2, \text{ for } 1 \leq i \leq k \\
L_i &= \lfloor L_i^{\#} \rfloor, \text{ for } 1 \leq i \leq k \\
T_1 &= 2(k+1)T \\
S_1 &= \lfloor S / C_{14} \rfloor
\end{aligned}$$

The constants C_i are positive real numbers (with the exception that C_{19} can equal zero, and C_5 is required to be an integer) that only depend on the characteristics of the group $\mathbb{G}$ (including k, d, m, c_j, r_j, etc.) and not, for example, on $\mathbf{u}$, β_i, V_i, K, D, B, or E. We will give values for them later, but for now we will assume that they satisfy the following equations and inequalities.

$$\begin{aligned}
C_1 =& C_3 C_2 & C_{15} =& C_{13}^2 / C_{17} \\
C_{13} =& C_{14} C_{16} & 0 \leq& C_{19} < 1 \\
1 \leq& C_{16} & 1 \leq& C_{14} \\
C_7 C_{18} \leq& C_{14} & 2/d \leq& C_6 \\
C_{17} \leq& C_{14}^2 & (1 + C_4) m C_5 \leq& C_{15} \\
C_{22} + C_{12} \leq& C_{11} & C_{10} + C_{23} \leq& C_{12}
\end{aligned}$$

$$C_{11} + \log(d-1) \le C_9$$

$$(9k+10)C_{14} + 1 \le C_{13}$$

$$d!(2(k+1))^{d-1}\binom{c+d-1}{c}(1+C_4)^3/(1-C_{19}) \le C_{18}$$

$$2 + 8\left(1 + \log(9k+10) + \log C_{14}\right) \le C_7$$

$$2C_{13}^{2d-1} \le m C_{17}^{d-1} C_6 C_2$$

$$C_{10} + C_{21} + C_{12} \le (k+1)C_{16}$$

$$C_8 + C_9 + 1 \le (\frac{1}{2}C_7 - 1)C_{10}$$

$$2(k+1)\left(\log(2(k+1)) + \log C_2 + d\right) \le C_{20}$$

$$C_{20} + (k+1)(4\log d + 3) + (\log C_{16})/d \le C_8$$

$$(k+1)C_{16}\log((9k+10)C_{14}) + 1 \le C_{22}$$

$$2(d\log 2 + \log C_{13} + (d-1)\log C_2 + d - 1) \le C_2$$

$$2(1 + \log m + d\log 2 + d\log C_2 + d) \le C_2$$

$$\max\{\exp(3d),\ 4((k+1)C_{16} + \log 8),\ 4(\log(k+1) + C_{13})\} \le C_2$$

$$C_{11} + 2(k+1)\log d + C_{20} + C_{10} + \frac{1}{d}(\log C_{16}) + 3k + 3 \le C_3$$

$$\begin{aligned}(k+1)\log d + \frac{1}{2}C_{20} + \frac{1}{d}(\log(2(k+1)C_{16}))&\\ +k(4k^2 + 10k + 7)C_{17} + k + 3 &\le C_{21}\end{aligned}$$

$$\begin{aligned}C_{11} + (k+1)\log d + \frac{1}{2}C_{20} + 3 + C_{10} + \frac{1}{d}\log((k+1)C_{13})&\\ +k((k+1)^2 C_{17} + k + 2) &\le C_3\end{aligned}$$

$$(1/d)\log C_2 + 4 + (1/d)\log((k+1)C_{13}) + (2/C_{15})\sum_{i=1}^{k}\log r_i + \frac{1}{2}C_{20}$$
$$+ (k+1)\left[\log 2 + \log\max_i r_i' + \log\max_i(q_i - 1) + \log\max_i \kappa_i + \max_i q_i'\right]$$
$$+ \sum_{i=1}^{k}\left[2(k+1)^2 c_i C_{17} + 2c_i + 2c_i' + (2c_i + (k+1)(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0)\right] \leq C_{23}$$

$$\begin{aligned} D\log V_i \geq& (2A_i^+ + B_i^+)\,|\mathbf{u}_i|\,E/C_{14} \text{ for } 1 \leq i \leq k \\ D\log V_i \geq& (A_i^+ + B_i^+ + C_i^+)/C_{14}^2 \text{ for } 1 \leq i \leq k \\ \max_{1\leq i\leq k} D\log V_i \geq& \max_{0\leq i\leq d-1} |u_i|\,/(C_2/2d) \\ c_i L_i \leq& (k+1)T(q_i-1) \\ (1-C_{19})\frac{1}{d!}\,\mathrm{H}(\mathbb{G};\mathbf{L}) \leq& \mathrm{Hf}(\mathbb{G};\mathbf{L}) \end{aligned}$$

In the general case, one can use 3.1 and a lower bound on L_i to get the last inequality, but in our case, we will know $\mathrm{Hf}(\mathbb{G};\mathbf{L})$ explicitly, so a more precise estimate will be available to us.

We will also assume that there is a basis for K over $\mathbb{Q}$ of elements of height $\leq D\log B$.

From these equations, it is easy to prove the following relations:

$$\begin{aligned}
T/L_i^{\#} &\geq (1+C_4)mC_5, \ \ \text{for } i>0 \\
T/L_i &\geq m, \ \ \text{for } i>0 \\
T/L_0 &\geq d \geq 1 \\
L_i S^2 D \log V_i &\leq C_{17} U_0, \ \ \text{for } i>0 \\
L_i &\geq d/\log(1+C_4), \ \ \text{for } i \geq 0 \\
U_0 \geq U_0/\log B &\geq C_2
\end{aligned}$$

Now we can prove the lemmas used in Chapter 2.

Lemma 4.5. *Every connected algebraic subgroup $\mathbb{G}'$ of $\mathbb{G} = \mathbb{G}_a \times G_1 \times ... \times G_k$ has the form $\mathbb{G}' = B_1 \times B_2$ where B_1 is a connected algebraic subgroup of $\mathbb{G}_a$ and B_2 is a connected algebraic subgroup of $G_1 \times ... \times G_k$. Furthermore, either $B_1 = 0$ or $B_1 = \mathbb{G}_a$.*

Proof. The Chevalley-Rosenlicht theorem says that $\mathbb{G}'$ sits in a canonical exact sequence of group varieties

$$1 \to B_1 \to \mathbb{G}' \to B_2' \to 1,$$

where B_1 is a connected linear algebraic group, and B_2' is an abelian variety.

Since B_1 is connected and commutative, it is a product of $\mathbb{G}_a$'s and $\mathbb{G}_m$'s, and none of these has a non-trivial map to $G_1 \times ... \times G_k$, so that B_1 must embed into the $\mathbb{G}_a$ factor, hence must be 1 or $\mathbb{G}_a$.

If $B_1 = 1$, then $\mathbb{G}'$ is an abelian variety, so maps trivially to the $\mathbb{G}_a$ factor. Hence $\mathbb{G}' = 1 \times B_2$, where B_2 is a connected subgroup of $G_1 \times ... \times G_k$ isomorphic to B_2'.

If $B_1 = \mathbb{G}_a$, then the composition of the inclusion $B_1 \to \mathbb{G}'$ with the projection

$$\mathbb{G}_a \times G_1 \times ... \times G_k \to G_1 \times ... \times G_k$$

is trivial, hence B_1 injects into $\mathbb{G}_a \times 1$. In fact B_1 maps onto $\mathbb{G}_a \times 1$, since both are 1-dimensional, and so $\mathbb{G}'$ contains $\mathbb{G}_a \times 1$ as a subgroup, and this is B_1. Then the projection onto the first factor gives a splitting of the above exact sequence.

It follows that $\mathbb{G}' = \mathbb{G}_a \times B_2$, where B_2 is a connected subgroup of $G_1 \times ... \times G_k$ isomorphic to B_2'. □

Lemma 4.6. *Let T be a positive integer, and let $L_1^{\#}$, ... $L_k^{\#}$ be positive real numbers. Let Σ be a finite set of points of $\mathbb{G}(\mathbb{C})$. Then there exists a real number $L_0^{\#}$ such that every connected algebraic subgroup $\mathbb{G}'$ of $\mathbb{G}$ with $T_{\mathbb{G}'}(\mathbb{C}) \subset W$ satisfies*

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}') \operatorname{H}(\mathbb{G}'; L_0^{\#}, \ldots, L_k^{\#}) \geq (1 + C_4) \operatorname{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#}),$$

where $r+1$ is the codimension of $\mathbb{G}'$ in $\mathbb{G}$, and there is (at least) one such subgroup $\tilde{\mathbb{G}}$ with equality. Additionally, $C_5 \leq \lfloor L_0^{\#} \rfloor \leq L_0^{\#} \leq C_6 U_0/(2D \log B)$.

Proof. If $\mathbb{G}'$ is a connected algebraic subgroup of $\mathbb{G}$, with $T_{\mathbb{G}'}(\mathbb{C}) \subset W$, then by Lemma 4.5, $\mathbb{G}' = L \times H$ where L is a connected algebraic subgroup of $\mathbb{G}_a$, H is a connected algebraic subgroup of $G_1 \times ... \times G_k$, and $T_{\mathbb{G}'}(\mathbb{C}) = T_L(\mathbb{C}) \times T_H(\mathbb{C})$. But if $T_L(\mathbb{C}) \neq 0$, then $(1, 0, \ldots, 0) \in T_{\mathbb{G}'}(\mathbb{C})$, contradicting $T_{\mathbb{G}'}(\mathbb{C}) \subset W$. Therefore, $\mathbb{G}'$ is a subgroup of $G_1 \times ... \times G_k$. Consequently, $\operatorname{H}(\mathbb{G}'; L_0^{\#}, \ldots, L_k^{\#})$ is independent of

$L_0^{\#}$. On the other hand, by Equation 3.5,

$$\mathrm{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#}) = d! \prod_{i=0}^{k} \frac{m_i}{d_i!} (L_i^{\#})^{d_i} = m L_0^{\#} \prod_{i=1}^{k} (L_i^{\#})^{d_i}$$

is linear in $L_0^{\#}$. Thus

$$\mathrm{H}(\mathbb{G}'; L_0^{\#}, \ldots, L_k^{\#}) = \mathrm{H}(\mathbb{G}'; 1, L_1^{\#}, \ldots, L_k^{\#})$$
$$\mathrm{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#}) = L_0^{\#}\, \mathrm{H}(\mathbb{G}; 1, L_1^{\#}, \ldots, L_k^{\#}).$$

Define

$$A(\mathbb{G}') = \frac{T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; 1, L_1^{\#}, \ldots, L_k^{\#})}{(1 + C_4)\, \mathrm{H}(\mathbb{G}; 1, L_1^{\#}, \ldots, L_k^{\#})}$$

on the space of all connected algebraic subgroups $\mathbb{G}'$ of $\mathbb{G}$ satisfying $T_{\mathbb{G}'}(\mathbb{C}) \subset W$. This function is clearly everywhere positive, and we will show that it achieves its minimum value. There are only finitely many possibilities for r $(0 \leq r \leq d)$ and only finitely many possibilities for $\operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')$ (it is also a positive integer and $\leq \operatorname{card}(\Sigma)$). Furthermore, for each such choice, there are only finitely many polynomials whose coefficients are positive integers not bigger than

$$A(0) \frac{(1 + C_4)\, \mathrm{H}(\mathbb{G}; 1, L_1^{\#}, \ldots, L_k^{\#})}{T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')}.$$

Therefore, there are only finitely many values $A(\mathbb{G}') \leq A(0)$. Let $\tilde{\mathbb{G}}$ be one such subgroup with A minimal, and let $L_0^{\#} = A(\tilde{\mathbb{G}})$.

It remains to show that $C_5 \leq \lfloor L_0^{\#} \rfloor \leq L_0^{\#} \leq C_6 U_0 / (2D \log B)$. Since $C_5 \in \mathbb{Z}$, it suffices to show $C_5 \leq L_0^{\#} \leq C_6 U_0 / (2D \log B)$. We will start with the right inequality:

$$\begin{aligned}
L_0^{\#} \leq & A(0) \\
= & \frac{T^{d-1} S}{(1+C_4) m \prod_{i=1}^{k} (L_i^{\#})^{d_i}} \\
\leq & \left(\frac{U_0}{D \log\log B} \right)^{d-1} S \left(\frac{1}{1+C_4} \right) \left(\frac{1}{m} \right) \prod_{i=1}^{k} \left(\frac{D S^2 \log V_i}{C_{17} U_0} \right)^{d_i} \\
= & \left(\frac{U_0}{D \log\log B} \right)^{d-1} S \left(\frac{1}{1+C_4} \right) \left(\frac{1}{m} \right) \left(\frac{D S^2}{C_{17} U_0} \right)^{d-1} \prod_{i=1}^{k} (\log V_i)^{d_i} \\
= & \left(\frac{C_{13}^{2d-1}}{(1+C_4) m C_{17}^{d-1}} \right) D^{2d-1} (\log\log B)^{d} (\log E)^{-(2d-1)} \prod_{i=1}^{k} (\log V_i)^{d_i} \\
= & \left(\frac{2 C_{13}^{2d-1}}{(1+C_4) m C_{17}^{d-1} C_2} \right) \frac{U_0}{2D \log B} \\
\leq & C_6 \frac{U_0}{2D \log B}.
\end{aligned}$$

For the lower bound, we have

$$\begin{aligned}
L_0^{\#} = & A(\tilde{\mathbb{G}}) \\
= & \frac{T^{\tilde{r}} \operatorname{card}(\Sigma + \tilde{\mathbb{G}}/\tilde{\mathbb{G}}) \, \mathrm{H}(\tilde{\mathbb{G}}; 1, L_1^{\#}, \ldots, L_k^{\#})}{(1+C_4) \, \mathrm{H}(\mathbb{G}; 1, L_1^{\#}, \ldots, L_k^{\#})} \\
\geq & \frac{T^{\tilde{r}} \, \mathrm{H}(\tilde{\mathbb{G}}; 1, L_1^{\#}, \ldots, L_k^{\#})}{(1+C_4) m \prod_{i=1}^{k} (L_i^{\#})^{d_i}}.
\end{aligned}$$

Since $\mathrm{H}(\tilde{\mathbb{G}})$ is a homogeneous polynomial of degree $d-1-\tilde{r}$, with coefficients that are positive integers, the last numerator is $\geq T^{\tilde{r}}$ times the product of the smallest $d-1-\tilde{r}$ numbers from the multiset $L_1^{\#}, \ldots, L_1^{\#}, \ldots, L_k^{\#}, \ldots, L_k^{\#}$ where each $L_i^{\#}$ appears d_i times. Therefore

$$L_0^{\#} \geq \frac{1}{(1+C_4) m} \left(\min_{1 \leq i \leq k} \frac{T}{L_i^{\#}} \right)^{\tilde{r}} \geq \frac{1}{(1+C_4) m} \left((1+C_4) m C_5 \right)^{\tilde{r}}.$$

Now, $\tilde{r}+1$ is the codimension of $\tilde{\mathbb{G}}$ in $\mathbb{G}$. We already showed that $\tilde{\mathbb{G}}$ is a subgroup of $G_1 \times \ldots \times G_k$, so the codimension must be at least 1. If the codimension were exactly 1, however, then we would have $\tilde{\mathbb{G}} = G_1 \times ... \times G_k$, and therefore $T_{\tilde{\mathbb{G}}}(\mathbb{C}) = \{\mathbf{w} \in \mathbb{C}^d : w_0 = 0\}$, contradicting $T_{\tilde{\mathbb{G}}}(\mathbb{C}) \subset W$. Therefore, the codimension must be at least 2, and so $\tilde{r} \geq 1$. This, together with $C_5 \geq 1$, gives the result. □

Lemma 4.7.

$$\log(2\mu) < \frac{1}{2}U_0.$$

Proof. We have the exact value

$$\begin{aligned}\mu =& \operatorname{card}\{s \in \mathbb{Z} : 0 \leq s < S_1\} \times \operatorname{card}\{\mathbf{t} \in \mathbb{Z}^{d-1} : |t| \leq T_1\} \\ =& S_1 \binom{T_1 + d - 1}{d - 1}.\end{aligned}$$

Since $\log(2\mu)$ is actually very small, we will use the crude upper bound

$$\mu < S_1(T_1 + d - 1)^{d-1} < S_1(2T_1)^{d-1}.$$

Then we compute

$$\begin{aligned}\log(2\mu) \leq& d\log 2 + \log S_1 + (d-1)\log T_1 \\ \leq& d\log 2 + \log C_{13} + \log(D\log\log B/\log E) + (d-1)\log(U_0/D\log\log B) \\ \leq& d\log 2 + \log C_{13} + (d-1)\log(D\log\log B) + (d-1)\log(U_0/D\log\log B) \\ =& d\log 2 + \log C_{13} + (d-1)\log(U_0) \\ =& d\log 2 + \log C_{13} + (d-1)\log C_2 + (d-1)\log(U_0/C_2) \\ \leq& (d\log 2 + \log C_{13} + (d-1)\log C_2)(U_0/C_2) + (d-1)(U_0/C_2) \\ =& ((d\log 2 + \log C_{13} + (d-1)\log C_2 + d - 1)/C_2)U_0 \\ \leq& \frac{1}{2}U_0.\end{aligned}$$

□

Lemma 4.8. *The number of unknowns ν satisfies*

$$\log \nu \leq \frac{1}{2} U_0.$$

Proof. The number of unknowns ν is equal to the number of i values times the number of λ values. The former is also the number of ξ_i values, which is $D = [K : \mathbb{Q}]$. The latter is the dimension of the space of multihomogeneous polynomials on $\mathbb{G}$, that is,

$$\begin{aligned} \operatorname{card}(\Lambda) &= \dim_{\mathbb{C}} \left(\mathbb{C}[\bar{\mathbb{P}}]/I(\mathbb{G})\right)_{\mathbf{L}} \\ &= \operatorname{Hf}(\mathbb{G}; \mathbf{L}) \\ &= \prod_{i=0}^{k} \operatorname{Hf}(G_i; L_i). \end{aligned}$$

the Hilbert function evaluated at L. We will use 3.1 to bound $\operatorname{Hf}(\mathbb{G}; \mathbf{L})$ from below, and 3.3 to bound it from above. For the upper bound, we have

$$\begin{aligned}
\log \nu =& \log \left(D \prod_{i=0}^{k} \mathrm{Hf}(G_i; L_i) \right) \\
\leq & \log D + \log \mathrm{Hf}(\mathbb{G}_a; L_0) + \log \prod_{i=1}^{k} m_i \binom{L_i + d_i}{d_i} \\
\leq & D + \log(L_0 + 1) + \log \prod_{i=1}^{k} \frac{m_i}{d_i!} (L_i + d_i)^{d_i} \\
\leq & D + \log(2L_0) + \log m + \sum_{i=1}^{k} d_i \log(L_i + d_i) \\
\leq & D + \log(2U_0) + \log m + \sum_{i=1}^{k} d_i \log(2U_0) \\
=& D + \log(2U_0) + \log m + (d-1)\log(2U_0) \\
=& D + \log m + d\log(2U_0) \\
\leq & D + \log m + d\log(2C_2) + d\log(U_0/C_2) \\
\leq & U_0/C_2 + (\log m + d\log(2C_2))U_0/C_2 + d(U_0/C_2) \\
=& (1 + \log m + d\log 2 + d\log C_2 + d)U_0/C_2 \\
\leq & \frac{1}{2} U_0.
\end{aligned}$$

□

Lemma 4.9.

$$T_1 \log T_1 \leq C_{20} U_0$$

Proof.

$$\begin{aligned}
(T_1 \log T_1)/U_0 =& 2(k+1)(\log(2(k+1)) + \log T)(T/U_0) \\
\leq& 2(k+1)(\log(2(k+1)) + \log(U_0/D \log\log B))(T/U_0) \\
\leq& 2(k+1)(\log(2(k+1)) + \log C_2 + (2d-1)\log D + \log\log B + \\
& (d-1)\log\log\log B + \sum_{i=1}^{k} d_i \log\log V_i - (2d-1)\log\log E)(T/U_0) \\
\leq& 2(k+1)(\log(2(k+1)) + \log C_2 + (2d-1)(D-1) + \log\log B + \\
& (d-1)(\log\log B - 1) + (d-1)D\log\log B)/(D\log\log B) \\
\leq& 2(k+1)((\log(2(k+1)) + \log C_2 - 3d + 2) + (2d-1)D + \\
& d\log\log B + (d-1)D\log\log B)/(D\log\log B) \\
\leq& 2(k+1)(\log(2(k+1)) + \log C_2 + 2 - 3d + 2d - 1 + d + d - 1) \\
\leq& C_{20}.
\end{aligned}$$

□

Lemma 4.10.

$$M \leq C_8 U_0.$$

Proof. We defined

$$M = \log \max_{s,\mathbf{t}} \sum_{i,\boldsymbol{\lambda}} \left| \xi_i \, \mathrm{D}_{\mathbf{f}}^{\mathbf{t}} \, \Phi^{\lambda}(s\mathbf{u}) \right| .$$

Since ν is the number of pairs $(i, \boldsymbol{\lambda})$ in the summation,

$$M \leq \log \nu + \log \max |\xi_i| + \log \max\{ \left| \mathrm{D}_{\mathbf{f}}^{\mathbf{t}} \, \Phi^{\lambda}(s\mathbf{u}) \right| : |\mathbf{t}| \leq T_1, 0 \leq s < S_1 \}.$$

By lemma 4.4,

$$M \leq \log \nu + \log \max |\xi_i| + T_1 \log(d-1) + \log \max\{ \left| \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} \, \Phi^{\lambda}(s\mathbf{u}) \right| : |\mathbf{t}| \leq T_1, 0 \leq s < S_1 \}.$$

We use 4.3 to get a bound on the last expression, taking $A_0 = 2D\log B$ and $A_1 = 1$.

$$\begin{aligned}
&\log\max\{\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,\Phi^{\lambda}(s\mathbf{u})\right| : |\mathbf{t}| \leq T_1, 0 \leq s < S_1\} \\
&\quad\leq T_1\log d + L_0(2D\log B) + T_1\log T_1 + L_0\log(|su_0|+1) + \sum_{i=1}^{k} L_i H_i^{+}(|s\mathbf{u}_i|+1).
\end{aligned}$$

Now we will bound each piece separately. By Lemma 4.8,

$$\log\nu \leq \frac{1}{2}U_0.$$

Since each ξ_i has height $\leq D\log B$, we have

$$\log\max|\xi_i| \leq D^2\log B \leq (1/C_2)U_0 \leq \frac{1}{4}U_0.$$

By Lemma 2.2,

$$2L_0 D\log B \leq C_6 U_0 \leq 2U_0.$$

Using $H_i^{+}(R) = A_i^{+}R^2 + B_i^{+}R + C_i^{+}$, we have

$$\begin{aligned}
L_i H_i^{+}(|s\mathbf{u}_i|+1) =& L_i(A_i^{+}(|s\mathbf{u}_i|+1)^2 + B_i^{+}(|s\mathbf{u}_i|+1) + C_i^{+}) \\
=& L_i(A_i^{+}\,|s|^2\,|\mathbf{u}_i|^2 + (2A_i^{+} + B_i^{+})\,|s|\,|\mathbf{u}_i| + A_i^{+} + B_i^{+} + C_i^{+}) \\
\leq& L_i(A_i^{+}S_1^2\,|\mathbf{u}_i|^2 + (2A_i^{+} + B_i^{+})S_1\,|\mathbf{u}_i| + A_i^{+} + B_i^{+} + C_i^{+}) \\
\leq& L_i S_1^2 D\log V_i + L_i S_1 C_{14} D\log V_i + L_i C_{14}^2 D\log V_i \\
\leq& (C_{17}/C_{14}^2)U_0 + (1/C_{13})U_0 + (C_{14}/C_{13})^2 U_0 \\
\leq& 3U_0.
\end{aligned}$$

From the definitions of T_1 and T, we have

$$\begin{aligned}
T_1\log(d-1) \leq& (2(k+1)\log(d-1)/\log\log B_0)U_0 \leq (2(k+1)\log(d-1))U_0 \\
T_1\log d \leq& (2(k+1)\log d/\log\log B_0)U_0 \leq (2(k+1)\log d)U_0
\end{aligned}$$

From the Mean Value Theorem, when $x \geq 1$,

$$1/(x+1) \leq \log(x+1) - \log x \leq 1/x \leq 1.$$

Using this, and the fact that $u_0 = 0$ or $u_0 = 1$,

$$\begin{aligned}
L_0 \log(|su_0| + 1) \leq & L_0 \log(S_1 + 1) \\
\leq & L_0(1 + \log C_{16} + \log D + \log\log\log B) \\
\leq & L_0(\log C_{16} + \log D + \log\log B) \\
= & L_0(\log C_{16} + \log(D \log B)) \\
\leq & L_0(\log C_{16} - 1 + D \log B) \\
\leq & L_0(\log C_{16} - 1 + 1) D \log B \\
\leq & \frac{1}{2}(\log C_{16}) C_6 U_0 \\
\leq & \frac{1}{d}(\log C_{16}) U_0.
\end{aligned}$$

Putting all of these together, we get

$$\begin{aligned}
M/U_0 \leq & \frac{1}{2} + \frac{1}{4} + 2(k+1)\log(d-1) + 2(k+1)\log d + 2 + C_{20} + \frac{1}{d}\log C_{16} + 3k \\
\leq & 3k + 3 + 2(k+1)\log d + 2(k+1)\log d + C_{20} + \frac{1}{d}\log C_{16} \\
= & (k+1)(4\log d + 3) + C_{20} + \frac{1}{d}\log C_{16} \\
\leq & C_8
\end{aligned}$$

□

Lemma 4.11. *Fixing some* $\mathbf{t}$ *and* s *with* $|\mathbf{t}| \leq (k+1)T$*, if we take*

$$\begin{aligned} f(z) =& \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(z\mathbf{w}) \\ r =& \frac{1}{2}(k+1)S \\ R =& 2(k+1)SE \\ S' =& S_1 \\ T' =& (k+1)T. \end{aligned}$$

then we have

$$2\,|f|_R \left(\frac{4r}{R}\right)^{T'S'} < \frac{1}{4}\exp(-C_{12}U_0)$$

and

$$5\left(\frac{18r}{S'}\right)^{T'S'} \max\left\{\left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right|,\ 0 \leq t < T',\ 0 \leq s < S'\right\} < \frac{1}{4}\exp(-C_{12}U_0).$$

Proof. By Lemma 4.3, we have

$$\begin{aligned} \log|f|_R =& \log\max\{\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(z\mathbf{w}) : |z| = R\} \\ \leq& T'\log d + L_0(2D\log B) + T'\log T' + \log\nu \\ & + \log(|\xi_i|\, e^{\delta}) + L_0\log(R\,|w_0| + 1) + \sum_{i=1}^{k} L_i H_i^{+}(R\,|w_i| + 1) \\ \leq& (k+1)T\log d + C_6U_0 + \frac{1}{2}T_1\log T_1 + \log\nu \\ & + \log|\xi_i| + \delta + L_0\log(R\,|w_0| + 1) + \sum_{i=1}^{k} L_i H_i^{+}(R\,|w_i| + 1) \\ \leq& ((k+1)\log d)U_0 + U_0 + \frac{1}{2}C_{20}U_0 + \frac{1}{2}U_0 \\ & + \frac{1}{2}U_0 + C_{10}U_0 + L_0\log(R\,|w_0| + 1) + \sum_{i=1}^{k} L_i H_i^{+}(R\,|w_i| + 1). \end{aligned}$$

We bound the last two terms as we did in the previous theorem.

$$\begin{aligned}
L_i H_i^+(R\left|\mathbf{w}_i\right|+1) =& L_i H_i^+(R\left|\mathbf{u}_i\right|+1) \\
=& L_i(A_i^+(R\left|\mathbf{u}_i\right|+1)^2 + B_i^+(R\left|s\mathbf{u}_i\right|+1) + C_i^+) \\
=& L_i(A_i^+ R^2\left|\mathbf{u}_i\right|^2 + (2A_i^+ + B_i^+)R\left|\mathbf{u}_i\right| + A_i^+ + B_i^+ + C_i^+) \\
=& L_i(4(k+1)^2 A_i^+ S^2 E^2\left|\mathbf{u}_i\right|^2 + 2(k+1)(2A_i^+ + B_i^+)SE\left|\mathbf{u}_i\right| + \\
& A_i^+ + B_i^+ + C_i^+) \\
\leq& L_i(4(k+1)^2 S^2 D\log V_i + 2(k+1)C_{14}SD\log V_i + C_{14}^2 D\log V_i) \\
\leq& 4(k+1)^2 C_{17}U_0 + 2(k+1)C_{17}U_0 + C_{17}U_0 \\
=& (4k^2+10k+7)C_{17}U_0.
\end{aligned}$$

$$\begin{aligned}
L_0\log(R\left|w_0\right|+1) =& L_0\log(R\left|u_0+\mathcal{L}(\mathbf{u})\right|+1) \\
\leq& L_0\log(R+2) \\
\leq& L_0(1+\log(2(k+1)) + \log S + \log E) \\
\leq& L_0(1+\log(2(k+1)) + \log E + \log C_{16} + \log D + \log\log\log B) \\
\leq& L_0(\log(2(k+1)) + D\log\log B + \log C_{16} + \log D + \log\log B) \\
=& L_0(\log(2(k+1)) + D\log\log B + \log C_{16} + \log(D\log B)) \\
\leq& L_0(\log(2(k+1)) + D(\log B - 1) + \log C_{16} - 1 + D\log B) \\
\leq& L_0(\log(2(k+1)) + \log C_{16} - 2 + 2D\log B) \\
\leq& L_0(\log(2(k+1)) + \log C_{16} - 2 + 2)D\log B \\
\leq& \frac{1}{2}(\log(2(k+1)) + \log C_{16})C_6U_0 \\
\leq& \frac{1}{d}(\log(2(k+1)) + \log C_{16})U_0.
\end{aligned}$$

We also have

$$\begin{aligned}\log\left(\frac{4r}{R}\right)^{T'S'} =& -T'S'\log E\\ \leq& -(k+1)T(\frac{S}{C_{14}}-1)\log E\\ \leq& -(k+1)T(C_{16}D\log\log B-\log E)\\ \leq& -(k+1)(\frac{U_0}{D\log\log B}-1)(C_{16}D\log\log B-\log E)\\ \leq& -(k+1)C_{16}U_0+(k+1)C_{16}D\log\log B+(k+1)T\log E\\ \leq& -(k+1)C_{16}U_0+(k+1)C_{16}D\log\log B+(k+1)U_0\frac{\log E}{D\log\log B}\\ \leq& -(k+1)C_{16}U_0+(k+1)C_{16}D\log\log B+(k+1)U_0.\end{aligned}$$

which, together, give

$$\begin{aligned}\log\left(8\,|f|_R\left(\frac{4r}{R}\right)^{T'S'}\right) \leq& \log 8+((k+1)\log d)U_0+U_0+\frac{1}{2}C_{20}U_0+\frac{3}{4}U_0+C_{10}U_0+\\ &\frac{1}{d}(\log(2(k+1)C_{16})U_0+k(4k^2+10k+7)C_{17}U_0\\ &-(k+1)C_{16}U_0+(k+1)C_{16}D\log\log B+(k+1)U_0\\ \leq&((k+1)\log d+\frac{1}{2}C_{20}+C_{10}+\frac{1}{d}(\log(2(k+1)C_{16}))+\\ &k(4k^2+10k+7)C_{17}-(k+1)C_{16}+k+3)U_0\\ \leq&(-(k+1)C_{16}+C_{10}+C_{21})U_0\\ \leq& -C_{12}U_0.\end{aligned}$$

Next, we set $C_{24} = (9k+10)C_{14}$ and

$$\begin{aligned} S \geq C_{13} - 1 \geq & C_{24} = \frac{C_{14}C_{24}}{C_{24} - 9(k+1)C_{14}} \\ (C_{24} - 9(k+1)C_{14})S \geq & C_{14}C_{24} \\ C_{24}(S - C_{14}) \geq & 9(k+1)C_{14}S \end{aligned}$$

which we use in

$$\begin{aligned} \log\left(\frac{18r}{S'}\right)^{T'S'} =& (k+1)TS_0 \log\left(\frac{9(k+1)S}{S_0}\right) \\ \leq & (k+1)TS_0 \log\left(\frac{9(k+1)C_{14}S}{S - C_{14}}\right) \\ \leq & (k+1)\frac{U_0}{D \log\log B}\frac{C_{16}D\log\log B}{\log E}\log C_{24} \\ \leq & (k+1)C_{16}(\log C_{24})U_0 \end{aligned}$$

Next, we need to bound

$$\max\left\{\left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right|,\, 0 \leq t < T',\, 0 \leq s < S'\right\}$$

using inequality 2.1. We know that

$$\begin{aligned} \frac{d^t}{dz^t}f(z) =& D^t_{\mathbf{w}}\,\mathrm{D}^{\mathbf{t}}_{\mathbf{e}}\,F(z\mathbf{u}) \\ =& (\sum_{i=1}^{d-1} u_i D_{\mathbf{e}^{\mathbf{i}}})^t\,\mathrm{D}^{\mathbf{t}}_{\mathbf{e}}\,F(z\mathbf{u}) \end{aligned}$$

Applying 2.1 and using the Taylor series for the exponential function, we have for $0 \leq s < S_1$,

$$\begin{aligned} \left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right| \leq & \frac{(\sum_{i=1}^{d-1}|u_i|)^t}{t!}\max\{|\mathrm{D}^{\boldsymbol{\tau}}_{\mathbf{e}}\,F(s\mathbf{u})| : |\boldsymbol{\tau}| \leq 2(k+1)T\} \\ \leq & \exp(\sum_{i=1}^{d-1}|u_i|)\exp(-C_{11}U_0). \end{aligned}$$

Therefore, we conclude that

$$\begin{aligned}
&\log\left(20\left(\frac{18r}{S'}\right)^{T'S'}\max\left\{\left|\frac{1}{t!}\frac{d^t}{dz^t}f(s)\right|,\, 0\le t<T',\, 0\le s<S'\right\}\right)\\
&\le \log 20+(k+1)C_{16}(\log C_{24})U_0+\sum_{i=1}^{d-1}|u_i|-C_{11}U_0\\
&\le \log 20+(k+1)C_{16}(\log C_{24})U_0+d\frac{1}{2d}C_2D\log V_i-C_{11}U_0\\
&\le((k+1)C_{16}\log C_{24}+1-C_{11})U_0\\
&\le(C_{22}-C_{11})U_0\\
&\le -C_{12}U_0.
\end{aligned}$$

□

Lemma 4.12. *For all* $|\mathbf{t}|\le T_1$ *and* $0\le s\le S_1$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{u})-\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{w})\right|<\exp(-C_{11}U_0),$$

and for all $|\mathbf{t}|\le(k+1)T$ *and* $0\le s\le(k+1)S$,

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{u})-\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{w})\right|<\frac{1}{2}\exp(-C_{12}U_0).$$

Proof. Fix some $|\mathbf{t}|\le T'$ and $0\le s\le S'$ (where T' is either T_1 or $(k+1)T$, and similarly for S'). Define a holomorphic function $f:\mathbb{C}\to\mathbb{C}$ by

$$f(z)=\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{u}+sz(\mathbf{w}-\mathbf{u})).$$

The Mean Value Theorem gives

$$|f(0)-f(1)|\le\max\{|f'(x)|:0\le x\le 1\}.$$

By the Chain Rule,

$$f'(x)=\sum_{i=0}^{d-1}s(w_i-u_i)\frac{\partial}{\partial z_i}\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}F(s\mathbf{u}+sx(\mathbf{w}-\mathbf{u})),$$

but since $w_i - u_i = 0$ whenever $i\neg 0$, and $w_0 - u_0 = \mathcal{L}(\mathbf{u})$, this is

$$f'(x) = s\,\mathcal{L}(\mathbf{u})\frac{\partial}{\partial z_0}\,\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(s\mathbf{u} + sx(\mathbf{w} - \mathbf{u})).$$

Applying lemma 4.3 with $\mathbf{x}_1 = (1, 0, \ldots, 0)$ and $\mathbf{x}_{i+1} = \mathbf{e}_i$, we have

$$\begin{aligned}\log \max_{0\leq x\leq 1} |f'(x)| \leq{}& \log S' + \log |\mathcal{L}(\mathbf{u})| + T' \log d + 2L_0 D \log B \\ &+ T' \log T' + \log \nu + \log(|\xi_i|\, e^{\delta}) + L_0 \log(|su_0 + sx\,\mathcal{L}(\mathbf{u})| + 1) \\ &+ \sum_{i=1}^{k} L_i H_i^+(|s\mathbf{u}_i| + 1).\end{aligned}$$

Now we have

$$\log(|su_0 + sx\,\mathcal{L}(\mathbf{u})| + 1) \leq \log(S' + 2) \leq \log S' + \frac{2}{S'} \leq 1 + \log S'.$$

As shown in Lemma 4.10, when $S' = S_1$ we have

$$\begin{aligned}L_i H_i^+(|s\mathbf{u}_i| + 1) \leq{}& 3U_0 \\ L_0(1 + \log S_1) \leq{}& \frac{1}{d}(\log C_{16})U_0.\end{aligned}$$

and even when $S' = (k + 1)S$, the same arguments give

$$\begin{aligned}L_i H_i^+(|s\mathbf{u}_i| + 1) \leq{}& L_i(A_i^+(S')^2\,|\mathbf{u}_i|^2 + (2A_i^+ + B_i^+)S'\,|\mathbf{u}_i| + A_i^+ + B_i^+ + C_i^+) \\ \leq{}& L_i(k + 1)^2 S^2 D \log V_i + L_i(k + 1)SC_{14} D \log V_i + L_i C_{14}^2 D \log V_i \\ \leq{}& ((k + 1)^2 C_{17})U_0 + (k + 1)(C_{14}/C_{13})U_0 + (C_{14}/C_{13})^2 U_0 \\ \leq{}& ((k + 1)^2 C_{17} + k + 2)U_0.\end{aligned}$$

and

$$\begin{aligned}
&L_0 \log((k+1)S+1)\\
&\qquad\qquad \le L_0(1+\log((k+1)C_{13})+\log D+\log\log\log B)\\
&\qquad\qquad \le \frac{1}{d}(\log((k+1)C_{13}))U_0.
\end{aligned}$$

Putting these together, we have in the case $T' = T_1$ and $S' = S_1$,

$$\begin{aligned}
&\log\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u}) - \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{w})\right|\\
&\le \log S_1 - C_3U_0 + 2(k+1)(\log d)U_0 + C_6U_0 + C_{20}U_0 +\\
&\quad \frac{1}{2}U_0 + \frac{1}{4}U_0 + \delta + \frac{1}{d}(\log C_{16})U_0 + 3kU_0\\
&\le (-C_3 + 2(k+1)\log d + C_{20} + C_{10} + \frac{1}{d}(\log C_{16}) + 3k + 3)U_0\\
&\le -C_{11}U_0.
\end{aligned}$$

In the case $T' = (k+1)T$ and $S' = (k+1)S$, we have

$$\begin{aligned}
&\log\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u}) - \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{w})\right|\\
&\le \log((k+1)S) - C_3U_0 + (k+1)(\log d)U_0 + C_6U_0 + \frac{1}{2}C_{20}U_0 +\\
&\quad \frac{1}{2}U_0 + \frac{1}{4}U_0 + \delta + \frac{1}{d}(\log((k+1)C_{13}))U_0 + k((k+1)^2C_{17} + k + 2)U_0\\
&\le (-C_3 + (k+1)\log d + \frac{1}{2}C_{20} + 3 + C_{10} +\\
&\quad \frac{1}{d}\log((k+1)C_{13}) + k((k+1)^2C_{17} + k + 2))U_0\\
&\le -C_{11}U_0.
\end{aligned}$$

□

Lemma 4.13. *The subgroup $\mathbb{G}'$ in the Lemme de zéros has $T_{\mathbb{G}'}(\mathbb{C}) \subset W$.*

Proof. Suppose, to the contrary, that $T_{\mathbb{G}'}(\mathbb{C}) \not\subseteq W$. Then $W \cap T_{\mathbb{G}'}(\mathbb{C})$ has dimension one less than $\mathbb{G}'$. So if $\mathbb{G}'$ has dimension d', then (since $\mathbb{G}$ has dimension d and W has dimension $d-1$) we have $r = d - d'$. Since $\mathbb{G}'$ is a subgroup of $\mathbb{G}_a \times G_1 \times ... \times G_k$, Lemma 4.5 tells us that $\mathbb{G}' = B_1 \times B_2$ where B_1 is a connected algebraic subgroup of $\mathbb{G}_a$, B_2 is a connected algebraic subgroup of $G_1 \times ... \times G_k$, and $T_{\mathbb{G}'}(\mathbb{C}) = T_{B_1}(\mathbb{C}) \times T_{B_2}(\mathbb{C})$, and $\mathrm{H}(\mathbb{G}'; L_0, ..., L_k) = \mathrm{H}(B_1; L_0)\,\mathrm{H}(B_2; L_1, ..., L_k)$. Now the Lemme de zéros tells us

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\,\mathrm{H}(\mathbb{G}'; L_0, ..., L_k) \leq \mathrm{H}(\mathbb{G}; L_0, ..., L_k)$$

and we know that

$$\mathrm{H}(\mathbb{G}; L_0, \ldots, L_k) = d! \prod_{i=0}^{k} \frac{m_i}{d_i!}(L_i)^{d_i} = mL_0 \prod_{i=1}^{k} (L_i)^{d_i}.$$

Since $\mathrm{H}(B_2)$ is a homogeneous polynomial of degree $d_2' = \dim B_2$, with coefficients that are positive integers, $\mathrm{H}(B_2; L_1, ..., L_k)$ is greater than or equal to the product of the smallest d_2' numbers from the multiset $L_1, \ldots, L_1, \ldots, L_k, \ldots, L_k$ where each L_i appears d_i times. Therefore

$$\frac{\mathrm{H}(B_2; L_1, ..., L_k)}{\mathrm{H}(\mathbb{G}; L_0, \ldots, L_k)} \geq \frac{1}{mL_0} \left(\min_{1 \leq i \leq k} \frac{1}{L_i} \right)^{d-1-d_2'}.$$

Now we have three cases:

Case 1: $B_1 = 0$ and $d' = d - 1$, so $\mathbb{G}' = G_1 \times ... \times G_k$. In this case, $r = 1$ and

$$\mathrm{H}(\mathbb{G}'; L_0, \ldots, L_k) = m \prod_{i=1}^{k} (L_i)^{d_i} (d')! \prod_{i=1}^{k} \frac{m_i}{d_i!}(L_i)^{d_i} = \frac{m}{d} \prod_{i=1}^{k} (L_i)^{d_i},$$

and since $T > dL_0$, we have

$$T \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\,\mathrm{H}(\mathbb{G}'; L_0, ..., L_k) > dL_0\,\mathrm{H}(\mathbb{G}'; L_0, ..., L_k) = \mathrm{H}(\mathbb{G}; L_0, ..., L_k),$$

contradicting the Lemme de zéros.

Case 2: $B_1 \neq 0$ and $d' \leq d-1$. In this case, $r \geq 1$, $B_1 = \mathbb{G}_a$, $\mathrm{H}(B_1; L_0) = L_0$, $d'_2 = d' - 1 \leq d-2$, so $d - 1 - d'_2 = r$ and

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0, ..., L_k)/\, \mathrm{H}(\mathbb{G}; L_0, ..., L_k)$$

$$\begin{aligned}
&\geq T^r\, \mathrm{H}(B_1; L_0)\, \mathrm{H}(B_2; L_1, ..., L_k)/\, \mathrm{H}(\mathbb{G}; L_0, ..., L_k) \\
&\geq \frac{1}{m} \left(\min_{1 \leq i \leq k} \frac{T}{L_i} \right)^r,
\end{aligned}$$

which is bigger than 1, since $T/L_i > m$ for all $i \geq 1$.

Case 3: $B_1 = 0$ and $d' \leq d-2$. In this case, $r \geq 2$, $d'_2 = d'$, so $d-1-d'_2 = r-1$ and

$$T^r \operatorname{card}(\Sigma + \mathbb{G}'/\mathbb{G}')\, \mathrm{H}(\mathbb{G}'; L_0, ..., L_k)/\, \mathrm{H}(\mathbb{G}; L_0, ..., L_k)$$

$$\begin{aligned}
&\geq T^r\, \mathrm{H}(B_2; L_1, ..., L_k)/\, \mathrm{H}(\mathbb{G}; L_0, ..., L_k) \\
&\geq \frac{T^r}{mL_0} \left(\min_{1 \leq i \leq k} \frac{1}{L_i} \right)^{r-1} \\
&= \frac{T}{mL_0} \left(\min_{1 \leq i \leq k} \frac{T}{L_i} \right)^{r-1}
\end{aligned}$$

which is bigger than 1, since $T > L_0$ and $T/L_i > m$ for all $i \geq 1$. □

Chapter 5

The Rank Theorem

As in [24], if we fix an element of our group g, then the map

$$T : \mathbb{G} \times \mathbb{C}^d \to \mathbb{G}$$

given by the group operation

$$T(h, \mathbf{z}) = h + g + \mathbf{\Phi}(\mathbf{z})$$

can be defined by functions $T_{i,j}$ which have degree c_i in h and are analytic in $\mathbf{z}$. In fact, we can take

$$T_{i,j}(h, \mathbf{z}) = R_{i,j}(h, R_i(g, \mathbf{\Phi}(\mathbf{z})))$$

where $R_i = (R_{i,0}, \ldots, R_{i,N_i})$ are the bihomogeneous polynomials of degree (c_i, c_i) defining the group law, which were introduced in the first chapter.

For a polynomial P and $t \in \mathbb{N}^k$ write $\partial_g^t P$ to mean

$$\frac{\partial^t}{\partial z^t} P(T_{1,0}(X_1, z), \ldots, T_{k,N_k}(X_k, z))|_{z=0}$$

Let $\tilde{\mathbb{G}}$ be the subgroup of $\mathbb{G}$ indicated in 2.2. Let $\tilde{d}$ denote its dimension and $\tilde{r}+1$ its codimension (or $\tilde{r}$ the codimension of $\mathrm{T}_{\tilde{\mathbb{G}}}(\mathbb{C})$ in W), so

$$\tilde{d} + \tilde{r} + 1 = d.$$

Recall that we defined a basis $\mathbf{f}_1, ..., \mathbf{f}_d$ for $\mathrm{T}_{\mathbb{G}}(\mathbb{C})$, such that $\mathbf{f}_1, ..., \mathbf{f}_{\tilde{d}-1}$ is a basis for $\mathrm{T}_{\tilde{\mathbb{G}}}(\mathbb{C})$. We use the argument from [26] that the rank of the linear system

$$\mathrm{D}_{\mathbf{f}}^{\mathbf{t}} F(s\mathbf{u}) = 0,$$

for all $0 \leq s < S_1$ and $|\mathbf{t}| \leq T_1$, is less than or equal to

$$\binom{T_1 + \tilde{r}}{\tilde{r}} \times S_1 \times \dim_{\mathbb{C}} \{\mathbb{C}[\bar{\mathbb{P}}]/I(\tilde{\mathbb{G}})\}_{c_0 L_0, \ldots, c_k L_k}.$$

To get an upper bound on the last factor, we will use inequality 3.3 (or [6]). This, however, only applies to groups embedded in normal projective space $\mathbb{P}^N$ (instead of multiprojective space $\bar{\mathbb{P}}$), so first, as in [27], we use the embedding

$$\bar{\mathbb{P}} \to \mathbb{P}^N$$
$$(X_{i,j})_{0 \leq i \leq k, 0 \leq j \leq N_i} \to \left(\prod_{i,j} X_{i,j}^{\alpha_{i,j}} \right)_{\sum_{j=0}^{N_i} \alpha_{i,j} = L_i, 0 \leq i \leq k}$$

(We won't need to make use of the fact that $N = \sum_{i=0}^{k} \binom{L_i + N_i}{L_i}$.) Let I be the ideal of polynomials in $\mathbb{P}^N$ that are zero on the image of $\tilde{\mathbb{G}}$ under this embedding. Then we have the following two lemmas.

Lemma 5.1.

$$\{\mathbb{C}[\bar{\mathbb{P}}]/I(\tilde{\mathbb{G}})\}_{cL_0, \ldots, cL_k} \cong \{\mathbb{C}[\mathbb{P}^N]/I\}_c$$

Proof. We will describe the isomorphism and its inverse explicitly. A term X_α on the right maps to the monomial $\prod_{i,j} X_{i,j}^{\alpha_{i,j}}$ on the left. Conversely, each monomial in any polynomial on the left will have multidegree $(cL_0, ..., cL_k)$. If the multidegree is partitioned into c $(k+1)$-tuples $\alpha^{(\mathbf{i})}$ which sum to $\sum \alpha^{(\mathbf{i})} = (cL_0, ..., cL_k)$, then the monomial maps to $X_{\alpha^{(\mathbf{1})}} ... X_{\alpha^{(\mathbf{c})}}$. There are, in general, many ways to choose the $\alpha^{(\mathbf{i})}$, but the difference of two polynomials created in this way is zero at every point in the image of $\bar{\mathbb{P}}$ (and therefore at every point in the image of $\tilde{\mathbb{G}}$), and consequently the difference is in I. Extending both maps linearly, it is easy to see that they are inverses of one another, hence bijective. □

Lemma 5.2.

$$\deg I = \mathrm{H}(\tilde{\mathbb{G}}; L_0, \ldots, L_k)$$

Proof. Consider the Hilbert function for I. It has the form

$$\mathrm{Hf}(I; x) = \frac{1}{\tilde{d}!}(\deg I)x^{\tilde{d}} + \mathrm{O}(x^{\tilde{d}-1})$$

for large values of x, but also equals

$$\begin{aligned}\mathrm{Hf}(I; x) &= \dim_{\mathbb{C}}\{\mathbb{C}[\mathbb{P}^N]/I\}_x \\ &= \dim_{\mathbb{C}}\{\mathbb{C}[\bar{\mathbb{P}}]/I(\tilde{\mathbb{G}})\}_{xL_0,\ldots,xL_k} \\ &= \mathrm{Hf}(\tilde{\mathbb{G}}; xL_0, \ldots, xL_k).\end{aligned}$$

Since this equality holds for all x, and the two functions are polynomials when x is sufficiently large, the polynomials must also be the same,

$$\mathrm{Hp}(I; x) = \mathrm{Hp}(\tilde{\mathbb{G}}; xL_0, \ldots, xL_k).$$

Treating the right side as a polynomial in x with the L_i constant, the leading terms must be the same. The leading term on the left is

$$\frac{1}{\tilde{d}!}(\deg I)x^{\tilde{d}}.$$

The leading term on the right is the homogeneous part of highest total degree in the L_i, that is, of degree $\tilde{d}$ in x, and this is exactly

$$\frac{1}{\tilde{d}!}\,\mathrm{H}(\tilde{\mathbb{G}}; L_0, \ldots, L_k)x^{\tilde{d}}.$$

□

Therefore,

$$\begin{aligned}\dim_{\mathbb{C}}\{\mathbb{C}[\bar{\mathbb{P}}]/I(\tilde{\mathbb{G}})\}_{c_0L_0,\ldots,c_kL_k} \leq & \dim_{\mathbb{C}}\{\mathbb{C}[\bar{\mathbb{P}}]/I(\tilde{\mathbb{G}})\}_{c\mathbf{L}} \\ = & \dim_{\mathbb{C}}\{\mathbb{C}[\mathbb{P}^N]/I\}_c \\ \leq & (\deg I)\binom{c+\tilde{d}}{\tilde{d}} \\ = & \binom{c+\tilde{d}}{\tilde{d}}\mathrm{H}(\tilde{\mathbb{G}};L_0,\ldots,L_k).\end{aligned}$$

But we have, by the definition of $\tilde{\mathbb{G}}$ (see 2.2),

$$\mathrm{H}(\tilde{\mathbb{G}};L_0^{\#},\ldots,L_k^{\#}) = \frac{(1+C_4)}{T^{\tilde{r}}\operatorname{card}(\Sigma+\tilde{\mathbb{G}}/\tilde{\mathbb{G}})}\mathrm{H}(\mathbb{G};L_0^{\#},\ldots,L_k^{\#})$$

Since the coefficients of $\mathrm{H}(\tilde{\mathbb{G}})$ are nonnegative, and $L_i \leq L_i^{\#}$ for all i

$$\mathrm{H}(\tilde{\mathbb{G}};L_0,\ldots,L_k) \leq \mathrm{H}(\tilde{\mathbb{G}};L_0^{\#},\ldots,L_k^{\#})$$

On the other hand, recall that

$$\mathrm{H}(\mathbb{G};L_0,\ldots,L_k) = d!\prod_{i=0}^{k}\frac{m_i}{d_i!}(L_i)^{d_i} = mL_0\prod_{i=1}^{k}(L_i)^{d_i},$$

so

$$\begin{aligned}
\frac{\mathrm{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#})}{\mathrm{H}(\mathbb{G}; L_0, \ldots, L_k)} &= \prod_{i=0}^{k} \left(\frac{L_i^{\#}}{L_i} \right)^{d_i} \\
&\leq \prod_{i=0}^{k} \left(\frac{L_i + 1}{L_i} \right)^{d_i} \\
&\leq \left(\max_i \frac{L_i + 1}{L_i} \right)^{d} \\
&= \left(\max_i 1 + \frac{1}{L_i} \right)^{d} \\
&\leq \left(1 + \frac{\log(1 + C_4)}{d} \right)^{d} \\
&< \exp\left(\frac{\log(1 + C_4)}{d} \right)^{d} \\
&= 1 + C_4.
\end{aligned}$$

In fact, for any subgroup B of $\mathbb{G}$, each term of $\mathrm{H}(B; L_0^{\#}, \ldots, L_k^{\#})$ is no more than $\prod_{i=0}^{k} (L_i^{\#}/L_i)^{d_i}$ times the corresponding term of $\mathrm{H}(B; L_0, \ldots, L_k)$, and so we get the same upper bound for B:

$$\frac{\mathrm{H}(B; L_0^{\#}, \ldots, L_k^{\#})}{\mathrm{H}(B; L_0, \ldots, L_k)} < 1 + C_4. \tag{5.1}$$

Therefore, we have

$$\begin{aligned}
\rho \leq & \binom{T_1+\tilde{r}}{\tilde{r}} S_1 \binom{c+\tilde{d}}{\tilde{d}} \mathrm{H}(\tilde{\mathbb{G}}; L_0, \ldots, L_k) \\
\leq & \binom{T_1+\tilde{r}}{\tilde{r}} S_1 \binom{c+\tilde{d}}{c} \mathrm{H}(\tilde{\mathbb{G}}; L_0^{\#}, \ldots, L_k^{\#}) \\
= & \binom{T_1+\tilde{r}}{\tilde{r}} S_1 \binom{c+\tilde{d}}{c} \frac{(1+C_4)}{T^{\tilde{r}}S} \mathrm{H}(\mathbb{G}; L_0^{\#}, \ldots, L_k^{\#}) \\
= & \frac{1}{T^{\tilde{r}}} \binom{T_1+\tilde{r}}{\tilde{r}} \frac{S_1}{S} \binom{c+\tilde{d}}{c} (1+C_4)^2 \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k) \\
\leq & \frac{1}{T^{\tilde{r}}} \frac{(T_1+\tilde{r})^{\tilde{r}}}{\tilde{r}!} \frac{1}{C_{14}} \binom{c+\tilde{d}}{c} (1+C_4)^2 \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k) \\
\leq & (2(k+1))^{\tilde{r}} \frac{1}{\tilde{r}!} (1+\frac{\tilde{r}}{T_1})^{\tilde{r}} \frac{1}{C_{14}} \binom{c+\tilde{d}}{c} (1+C_4)^2 \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k) \\
\leq & (2(k+1))^{d-1} (1+\frac{d}{T_1})^{d} \frac{1}{C_{14}} \binom{c+\tilde{d}}{c} (1+C_4)^2 \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k) \\
\leq & (2(k+1))^{d-1} \frac{1}{C_{14}} \binom{c+\tilde{d}}{c} (1+C_4)^3 \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k),
\end{aligned}$$

where the last inequality is true because $T_1 > T > dL_0 > d^2/\log(1+C_4)$.

On the other hand, we have

$$\begin{aligned}
\nu = & D \, \mathrm{Hf}(\mathbb{G}; L_0, \ldots, L_k) \\
\geq & (1-C_{19}) D \frac{1}{d!} \mathrm{H}(\mathbb{G}; L_0, \ldots, L_k).
\end{aligned}$$

Putting these two together, we conclude that

$$\begin{aligned}
\frac{D\rho}{\nu} \leq & d!(2(k+1))^{d-1} \frac{1}{C_{14}} \binom{c+\tilde{d}}{c} (1+C_4)^3/(1-C_{19}) \\
\leq & \frac{C_{18}}{C_{14}} \\
\leq & \frac{1}{C_7}.
\end{aligned}$$

Chapter 6

The Inequality of the Tail

Before we get to the main lemma of this section, we need to prove a lemma about derivatives of polynomials on our algebraic group.

Lemma 6.1. *Suppose that $P^{(0)}$ is a polynomial in the coordinates of $\boldsymbol{\Psi}(\mathbf{z})$, in the parameters $\boldsymbol{\vartheta}$, and in the coordinates of γ'. Suppose also that $D^{(0)}$ is an integer such that $D^{(0)}P^{(0)}$ has integer coefficients. Recursively define*

$$P^{(n+1)} = \frac{\partial}{\partial z_{t_n}} \left[P^{(n)}\right].$$

Suppose further that there are polynomials $Q_{t,s}$ with

$$\frac{\partial}{\partial z_t}\Psi_s = Q_{t,s}(1, \Psi_1, \ldots, \Psi_N),$$

and a positive integer κ such that $\kappa Q_{t,s}$ is a polynomial of degree q in $\boldsymbol{\Psi}(\mathbf{z})$, of degree q' in the parameters $\boldsymbol{\vartheta}$, with integer coefficients and length at most r'. Suppose that each polynomial $P^{(n)}$ has degree $A^{(n)}$ in $\boldsymbol{\Psi}(\mathbf{z})$, degree $B^{(n)}$ in the parameters $\boldsymbol{\vartheta}$, and degree $C^{(n)}$ in γ'. Then $\kappa^n D^{(0)}P^{(n)}$ has integer coefficients. Suppose that its length *is $E^{(n)}$. Then we have*

$$\begin{aligned}
A^{(n)} \leq& A^{(0)} + n(q-1) \\
B^{(n)} \leq& B^{(0)} + nq' \\
C^{(n)} =& C^{(0)} \\
D^{(n)} =& \kappa^n D^{(0)} \\
\log E^{(n)} \leq& \log E^{(0)} + n \log r' + n \log(A^{(0)} + n(q-1)).
\end{aligned}$$

Proof. The proof is by induction on n, with the case $n = 0$ being clearly true. Let us write

$$P^{(n)} = \sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \mathbf{\Psi}^{\boldsymbol{\lambda}_e} = \sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \prod_{s=1}^{N} \Psi_s^{\lambda_{e,s}},$$

where each p_e is either 0 or ± 1 times a product of at most $B^{(n)}$ ϑ_j's and at most $C^{(n)}$ γ_j''s, and $\sum_{s=1}^{N} \lambda_{e,s} = A^{(n)}$. (This is done by expanding a term with coefficient $\pm i$ into i different terms. Perhaps surprisingly, this method gives better bounds on heights than taking heights of coefficients.) Similarly, we write

$$Q_{t,s} = \sum_{\mu=1}^{r'} \frac{\varrho_\mu}{\kappa} \mathbf{\Psi}^{\boldsymbol{\lambda}'_\mu}.$$

We also write ι_s for the vector with a 1 in the s'th position and zeros elsewhere, and we compute

$$\begin{aligned}
P^{(n+1)} =&\frac{\partial}{\partial z_t}\left[P^{(n)}\right] \\
=&\sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \frac{\partial}{\partial z_t} \prod_{s=1}^{N} \Psi_s^{\lambda_{e,s}} \\
=&\sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \sum_{s=1}^{N} \lambda_{e,s} \boldsymbol{\Psi}^{\boldsymbol{\lambda}_e-\iota_s} \frac{\partial}{\partial z_t} \Psi_s \\
=&\sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \sum_{s=1}^{N} \lambda_{e,s} \boldsymbol{\Psi}^{\boldsymbol{\lambda}_e-\iota_s} Q_{t,s} \\
=&\sum_{e=1}^{E^{(n)}} \frac{p_e}{D^{(n)}} \sum_{s=1}^{N} \lambda_{e,s} \boldsymbol{\Psi}^{\boldsymbol{\lambda}_e-\iota_s} \sum_{\mu=1}^{r'} \frac{\varrho_\mu}{\kappa} \boldsymbol{\Psi}^{\boldsymbol{\lambda}'_\mu} \\
=&\sum_{e=1}^{E^{(n)}} \sum_{s=1}^{N} \sum_{\mu=1}^{r'} \frac{\lambda_{e,s} p_e \varrho_\mu}{D^{(n)}\kappa} \boldsymbol{\Psi}^{\boldsymbol{\lambda}_e-\iota_s+\boldsymbol{\lambda}'_\mu}
\end{aligned}$$

and from this we conclude that $P^{(n+1)}$ has

$$\begin{aligned}
A^{(n+1)} \leq& A^{(n)} - 1 + q \\
B^{(n+1)} \leq& B^{(n)} + q' \\
C^{(n+1)} =& C^{(n)} \\
D^{(n+1)} =& \kappa D^{(n)}
\end{aligned}$$

and since

$$\sum_{e=1}^{E^{(n)}} \sum_{s=1}^{N} \sum_{\mu=1}^{r'} \lambda_{e,s} = \sum_{e=1}^{E^{(n)}} \sum_{\mu=1}^{r'} \left(\sum_{s=1}^{N} \lambda_{e,s} \right) = E^{(n)} r' A^{(n)},$$

we also have

$$\log E^{(n+1)} \leq \log E^{(n)} + \log r' + \log A^{(n)}.$$

These recurrences easily give the bounds stated in the lemma. A slightly more precise value for $E^{(n)}$ could be given by estimating

$$\sum_{i=0}^{n-1} \log(A^{(0)} + i(q-1)).$$

with an associated integral, but when n is large, this changes very little, so we will have no need for this more precise bound. $\square$

In order to give a lower bound on nonzero values of our polynomial, we need to compute an upper bound on its height. Recall that we have a polynomial

$$P = \sum_{\boldsymbol{\lambda},i} a_{\lambda,i}\xi_i \mathbf{X}^{\boldsymbol{\lambda}}$$

which we can also write as

$$P = \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \mathbf{X}^{\boldsymbol{\lambda}}$$

where

$$p_{\boldsymbol{\lambda}} = \sum_{i=1}^{D} a_{\boldsymbol{\lambda},i}\xi_i.$$

We also define

$$F = P \circ \Phi = \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \boldsymbol{\Phi}^{\boldsymbol{\lambda}}.$$

Then we need to compute a lower bound for

$$\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u}) = \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \, \mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(\boldsymbol{\Phi}^{\boldsymbol{\lambda}}(s\mathbf{u})).$$

Lemma 6.2. *(Inequality of the Tail) If* $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u}) \neq 0$*, where* $|\mathbf{t}| \leq (k+1)T$ *and* $0 \leq s \leq (k+1)S$*, and* $\mathbf{t}$ *is minimal with this property, then*

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u})\right| > \exp(-C_{12}U_0).$$

Proof. We would like to compute the height of $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(s\mathbf{u})$, but $\boldsymbol{\Phi}^{\boldsymbol{\lambda}}(s\mathbf{u})$ is not necessarily even algebraic, so for each i we let ν_i be such that

$$|\Phi_{i,\nu_i}(s\mathbf{u})| = \max_j |\Phi_{i,j}(s\mathbf{u})| .$$

Then we define

$$\Psi_{i,j} = \Phi_{i,j}/\Phi_{i,0}.$$

Now if we change Φ to Ψ, we can compute its height, but if we take T derivatives and then evaluate the derivative at the point $s\mathbf{u}$, it is very difficult to get good estimates on the height. Instead, we need to translate first. (In some sense, this could be thought of as taking a Taylor series around the point in question, instead of around zero, in order to get a better approximation to the function.) That is,

$$\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(\mathbf{z})\big|_{\mathbf{z}=s\mathbf{u}} = \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} F(\mathbf{z}+s\mathbf{u})\big|_{\mathbf{z}=0} .$$

For each $1 \le i \le k$, let $R_0^{(i)}, \ldots, R_{N_i}^{(i)}$ be $N_i + 1$ polynomials in the variables $z_0, \ldots, z_{N_i}, w_0, \ldots, w_{N_i}$ which give, projectively, the sum of $\mathbf{z}$ and $\mathbf{w}$, and are defined at (hence in a neighborhood of) $(\boldsymbol{\Phi}_i(0), \boldsymbol{\Phi}_i(s\mathbf{u}))$. By assumption, we can choose such $R_j^{(i)}$ to be homogeneous of degree c_i in the $\mathbf{z}$ variables, homogeneous of degree c_i in the $\mathbf{w}$ variables, of degree at most d_i in parameters $\boldsymbol{\vartheta}$ defining G_i, and of length at most r_i.

Now, since we only have

$$\Phi_{i,j}(\mathbf{z}+\mathbf{z}') = R_j^{(i)}(\boldsymbol{\Phi}_i(\mathbf{z}), \boldsymbol{\Phi}_i(\mathbf{z}'))$$

up to a scalar multiple, we will deal in ratios

$$\frac{\Phi_{i,j}(\mathbf{z}+s\mathbf{u})}{\Phi_{i,\nu_i}(\mathbf{z}+s\mathbf{u})} = \frac{R_j^{(i)}(\boldsymbol{\Phi}_i(\mathbf{z}), \boldsymbol{\Phi}_i(s\mathbf{u}))}{R_{\nu_i}^{(i)}(\boldsymbol{\Phi}_i(\mathbf{z}), \boldsymbol{\Phi}_i(s\mathbf{u}))} = \frac{R_j^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}), \gamma_i')}{R_{\nu_i}^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}), \gamma_i')}$$

where γ_i' is projective coordinates for $s\gamma$. This is not necessary for $i = 0$, since $\Phi_0(\mathbf{z}) = z_0$. In particular, we have

$$\begin{aligned}
F(\mathbf{z}+s\mathbf{u}) =& \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \boldsymbol{\Phi}^{\boldsymbol{\lambda}}(\mathbf{z}+s\mathbf{u}) \\
=& \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \Phi_0(\mathbf{z}+s\mathbf{u})^{\lambda_0} \prod_{i=1}^{k} \Phi_{i,\nu_i}(\mathbf{z}+s\mathbf{u})^{L_i} \prod_{i=1}^{k}\prod_{j=0}^{N_i} \left(\frac{\Phi_{i,j}(\mathbf{z}+s\mathbf{u})}{\Phi_{i,\nu_i}(\mathbf{z}+s\mathbf{u})} \right)^{\lambda_{i,j}} \\
=& \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \Phi_0(\mathbf{z}+s\mathbf{u})^{\lambda_0} \prod_{i=1}^{k} \Phi_{i,\nu_i}(\mathbf{z}+s\mathbf{u})^{L_i} \prod_{i=1}^{k}\prod_{j=0}^{N_i} \left(\frac{R_j^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}),\gamma_i')}{R_{\nu_i}^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}),\gamma_i')} \right)^{\lambda_{i,j}} \\
=& f \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \Phi_0(\mathbf{z}+s\mathbf{u})^{\lambda_0} \prod_{i=1}^{k}\prod_{j=0}^{N_i} \left(R_j^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}),\gamma_i') \right)^{\lambda_{i,j}},
\end{aligned}$$

where

$$f = \prod_{i=1}^{k} \left(\frac{\Phi_{i,\nu_i}(\mathbf{z}+s\mathbf{u})}{R_{\nu_i}^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}),\gamma_i')} \right)^{L_i}.$$

By Leibniz' Rule,

$$\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f) = \mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F)/f$$

plus derivatives of F of lower order than $|\mathbf{t}|$, but since $|\mathbf{t}|$ is minimal with $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F) \neq 0$, all such derivatives are zero.

A lower bound on the numerator of f is given by the inequality

$$\log \max_j |\boldsymbol{\Phi}_{i,j}(s\mathbf{u})| \geq H_i^-(|s\mathbf{u}|).$$

An upper bound on the denominator of f will result from an upper bound on its height. We can also get a lower bound on the factor $\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f)$ from an upper bound on its height.

Since $\mathbf{e}$ is the basis $(e_1, e_2, ..., e_k)$, where e_i has β_i in position 0, 1 in position i, and 0 in all other positions, then

$$\mathrm{D}_{\mathbf{e}}^{\mathbf{t}} = \left(\beta_1 \frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_1} \right)^{t_1} \circ ... \circ \left(\beta_{d-1} \frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_{d-1}} \right)^{t_{d-1}}.$$

Since

$$\left(\beta_j \frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_j}\right)^{t_j} = \sum_{n=0}^{t_j} \binom{t_j}{n} \beta_j^{t_j - n} \left(\frac{\partial}{\partial z_0}\right)^{t_j - n} \left(\frac{\partial}{\partial z_j}\right)^{n},$$

and

$$\left(\frac{\partial}{\partial z_0}\right)^{|\mathbf{t}|-|\mathbf{n}|} (z_0 + su_0)^{\lambda_0} = \frac{\lambda_0!}{(\lambda_0 - |\mathbf{t}| + |\mathbf{n}|)!} (z_0 + su_0)^{\lambda_0 - |\mathbf{t}| + |\mathbf{n}|}$$

when $\lambda_0 - |\mathbf{t}| + |\mathbf{n}| = \lambda_0 - (t_1 + ... + t_{d-1}) + (n_1 + ... + n_{d-1}) \geq 0$, and zero otherwise, we have

$$\begin{aligned}
\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f) &= \sum_{\lambda} p_{\boldsymbol{\lambda}} \, \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} \left[\Phi_0(\mathbf{z} + s\mathbf{u})^{\lambda_0} \prod_{i=1}^{k} \prod_{j=0}^{N_i} \left(R_j^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}), \gamma_i') \right)^{\lambda_{i,j}} \right] \\
&= \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \, \mathrm{D}_{\mathbf{e}}^{\mathbf{t}} \left((z_0 + su_0)^{\lambda_0} Q_{\boldsymbol{\lambda}} \right) \\
&= \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \sum_{\mathbf{n}} \binom{t_1}{n_1} \cdots \binom{t_{d-1}}{n_{d-1}} \times \frac{\lambda_0!}{(\lambda_0 - |\mathbf{t}| + |\mathbf{n}|)!} \times \beta_1^{t_1 - n_1} ... \beta_{d-1}^{t_{d-1} - n_{d-1}} \\
&\quad \times (z_0 + su_0)^{\lambda_0 - |\mathbf{t}| + |\mathbf{n}|} \times \left(\frac{\partial}{\partial z_1}\right)^{n_1} \circ \ldots \circ \left(\frac{\partial}{\partial z_{d-1}}\right)^{n_{d-1}} Q_{\boldsymbol{\lambda}}
\end{aligned}$$

where the second sum is over all $d-1$-tuples of integers $\mathbf{n} = (n_1, ..., n_{d-1})$ with $0 \leq n_j \leq t_j$ and $\lambda_0 - |\mathbf{t}| + |\mathbf{n}| \geq 0$.

Taking the height of this formula, we get

$$\begin{aligned}
\mathrm{h}\left(\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f)\big|_0 \right) \leq{}& \mathrm{h}\left(\{p_{\boldsymbol{\lambda}}\}_{\boldsymbol{\lambda}}\right) + \mathrm{h}\left(\left\{ \binom{t_1}{n_1} \cdots \binom{t_{d-1}}{n_{d-1}} \right\}_{\mathbf{n}} \right) + \\
& \mathrm{h}\left(\left\{ \frac{\lambda_0!}{(\lambda_0 - |\mathbf{t}| + |\mathbf{n}|)!} \right\}_{\boldsymbol{\lambda},\mathbf{n}} \right) + \\
& \mathrm{h}\left(\left\{ \beta_1^{t_1 - n_1} ... \beta_{d-1}^{t_{d-1} - n_{d-1}} \right\}_{\mathbf{n}} \right) + \mathrm{h}\left(\left\{ (su_0)^{\lambda_0 - |\mathbf{t}| + |\mathbf{n}|} \right\}_{\boldsymbol{\lambda},\mathbf{n}} \right) + \\
& \mathrm{h}\left(\left\{ \left(\frac{\partial}{\partial z_1}\right)^{n_1} \circ \ldots \circ \left(\frac{\partial}{\partial z_{d-1}}\right)^{n_{d-1}} Q_{\boldsymbol{\lambda}} \Big|_0 \right\}_{\boldsymbol{\lambda},\mathbf{n}} \right)
\end{aligned}$$

We can bound each of these as follows:

$$\begin{aligned}\mathrm{h}\left(\{p_{\boldsymbol{\lambda}}\}_{\boldsymbol{\lambda}}\right) =&\,\mathrm{h}\left(\left\{\sum_{i=1}^{D} a_{\boldsymbol{\lambda},i}\xi_i\right\}_{\boldsymbol{\lambda}}\right) \leq \log D + \mathrm{h}\left(\{\xi_i\}_i\right) + \mathrm{h}\left(\{a_{\boldsymbol{\lambda},i}\}_{\boldsymbol{\lambda},i}\right)\\ &\leq \log D + D\log B + \delta\end{aligned}$$

Using the fact that the height of a collection of positive integers is the log of the largest one, we have

$$\begin{aligned}\mathrm{h}\left(\left\{\binom{t_1}{n_1}\dots\binom{t_{d-1}}{n_{d-1}}\right\}_{\mathbf{n}}\right) &\leq \log(2^{t_1}\dots 2^{t_{d-1}}) = \log(2^{|\mathbf{t}|}) \leq (k+1)T\log 2\\ \mathrm{h}\left(\left\{\frac{\lambda_0!}{(\lambda_0-|\mathbf{t}|+|\mathbf{n}|)!}\right\}_{\boldsymbol{\lambda},\mathbf{n}}\right) &\leq \log(\lambda_0!) \leq L_0\log L_0\\ \mathrm{h}\left(\left\{\beta_1^{t_1-n_1}\dots\beta_{d-1}^{t_{d-1}-n_{d-1}}\right\}_{\mathbf{n}}\right) &\leq (|\mathbf{t}|-|\mathbf{n}|)\,\mathrm{h}\left(\{\beta_i\}_i\right) \leq (L_0)(k)(2\log B)\end{aligned}$$

Since u_0 is either 0 or 1, we have

$$\mathrm{h}\left(\left\{(su_0)^{\lambda_0-|\mathbf{t}|+|\mathbf{n}|}\right\}_{\boldsymbol{\lambda},\mathbf{n}}\right) \leq \lambda_0\log s \leq L_0\log((k+1)S).$$

Since $Q_{\boldsymbol{\lambda}} = \prod_{i=1}^{k} Q_{\boldsymbol{\lambda},i}$, we have

$$\frac{\partial^{n_1}}{\partial z_1^{n_1}}\circ\dots\circ\frac{\partial^{n_{d-1}}}{\partial z_{d-1}^{n_{d-1}}}Q_{\boldsymbol{\lambda}} = \prod_{i=1}^{k}\frac{\partial^{n_{i,1}}}{\partial z_{i,1}^{n_{i,1}}}\circ\dots\circ\frac{\partial^{n_{i,d_i}}}{\partial z_{i,d_i}^{n_{i,d_i}}}Q_{\boldsymbol{\lambda},i}$$

The polynomial

$$Q_{\boldsymbol{\lambda},i} = \prod_{j=0}^{N_i}\left(R_j^{(i)}(\boldsymbol{\Psi}_i(\mathbf{z}),\gamma_i')\right)^{\lambda_{i,j}}$$

has degree c_iL_i in the $\boldsymbol{\Psi}_i(\mathbf{z})$ variables, degree c_iL_i in the coordinates of γ_i', degree $c_i'L_i$ in parameters ϑ defining G_i, and length at most $r_i^{L_i}$.

Therefore, by Lemma 6.1,

$$\frac{\partial^{n_{i,1}}}{\partial z_{i,1}^{n_{i,1}}}\circ\dots\circ\frac{\partial^{n_{i,d_i}}}{\partial z_{i,d_i}^{n_{i,d_i}}}Q_{\boldsymbol{\lambda},i}$$

is a polynomial of degree $c_iL_i+|\mathbf{n}_i|\,(q_i-1)$ in the $\mathbf{\Psi}_i(\mathbf{z})$ variables, degree c_iL_i in the coordinates of γ_i', degree at most $c_i'L_i+|\mathbf{n}_i|\,q_i'$ in parameters ϑ defining G_i, and, after multiplying by $\kappa_i^{|\mathbf{n}_i|}$, length at most $r_i^{L_i}(r_i')^{|\mathbf{n}_i|}(c_iL_i+|\mathbf{n}_i|\,(q_i-1))^{|\mathbf{n}_i|}$. Evaluating at $\mathbf{z}=0$ and taking the height, we get the upper bound

$$\begin{gathered}L_i\log r_i+|\mathbf{n}_i|\log r_i'+|\mathbf{n}_i|\log(c_iL_i+|\mathbf{n}_i|\,(q_i-1))+|\mathbf{n}_i|\log\kappa_i+c_iL_i\,\mathrm{h}(\gamma_i')\\ +(c_i'L_i+|\mathbf{n}_i|\,q_i')\,\mathrm{h}(G_i)+(c_iL_i+|\mathbf{n}_i|\,(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0)).\end{gathered}$$

Summing over $1\le i\le k$, we get

$$\begin{aligned}&\mathrm{h}\left(\left\{\left(\frac{\partial}{\partial z_1}\right)^{n_1}\circ\ldots\circ\left(\frac{\partial}{\partial z_{d-1}}\right)^{n_{d-1}}Q_{\boldsymbol{\lambda}}\bigg|_0\right\}_{\boldsymbol{\lambda},\mathbf{n}}\right)\\ &\quad\le\sum_{i=1}^{k}[L_i\log r_i+|\mathbf{n}_i|\log r_i'+|\mathbf{n}_i|\log(c_iL_i+|\mathbf{n}_i|\,(q_i-1))+|\mathbf{n}_i|\log\kappa_i\\ &\quad+c_iL_i\,\mathrm{h}(\gamma_i')+(c_i'L_i+|\mathbf{n}_i|\,q_i')\,\mathrm{h}(G_i)+(c_iL_i+|\mathbf{n}_i|\,(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))]\end{aligned}$$

The denominator of f (evaluated at $\mathbf{z}=0$) is

$$\prod_{i=1}^{k}\left(R_{\nu_i}^{(i)}(\mathbf{\Psi}_i(0),\gamma_i')\right)^{L_i}.$$

Since $R_{\nu_i}^{(i)}$ is a polynomial of degree c_i in the coordinates of $\mathbf{\Psi}_i(0)$, degree c_i in the coordinates of γ_i', degree c_i' in parameters ϑ defining G_i, and length at most r_i, we have

$$\begin{aligned}&\mathrm{h}\left(\prod_{i=1}^{k}\left(R_{\nu_i}^{(i)}(\mathbf{\Psi}_i(0),\gamma_i')\right)^{L_i}\right)\\ &\quad\le\sum_{i=1}^{k}\left[L_i\log r_i+c_iL_i\,\mathrm{h}(\mathbf{\Psi}_i(0))+c_iL_i\,\mathrm{h}(\gamma_i')+c_i'L_i\,\mathrm{h}(G_i)\right].\end{aligned}$$

Combining all of the above, we have

$$\mathrm{h}\left(\frac{\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f)\big|_0}{\prod_{i=1}^{k}\left(R_{\nu_i}^{(i)}(\mathbf{\Psi}_i(0),\gamma_i')\right)^{L_i}}\right) \leq \log D + D\log B + \delta$$

$$+ (k+1)T\log 2 + L_0\log L_0 + 2kL_0\log B + L_0\log((k+1)S)$$

$$+ \sum_{i=1}^{k}[2L_i\log r_i + |\mathbf{n}_i|\log r_i' + |\mathbf{n}_i|\log(c_iL_i + |\mathbf{n}_i|(q_i-1)) + |\mathbf{n}_i|\log\kappa_i$$

$$+ 2c_iL_i\,\mathrm{h}(\gamma_i') + (2c_i'L_i + |\mathbf{n}_i|\,q_i')\,\mathrm{h}(G_i) + (2c_iL_i + |\mathbf{n}_i|(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))].$$

We can bound these as follows:

$$\log D + D\log B + \delta + (k+1)T\log 2 \leq (1 + C_{10} + (k+1)\log 2)(U_0/D)$$

$$\begin{aligned} &L_0\log L_0 + 2kL_0\log B + L_0\log((k+1)S) \\ &\qquad \leq ((1/2)(C_6)\log C_2 + kC_6 + (1/2)(C_6)\log((k+1)C_{13}))(U_0/D) \\ &\qquad \leq ((1/d)\log C_2 + 2k/d + (1/d)\log((k+1)C_{13}))(U_0/D) \\ &\qquad \leq ((1/d)\log C_2 + 2 + (1/d)\log((k+1)C_{13}))(U_0/D) \end{aligned}$$

$$\sum_{i=1}^{k} 2L_i\log r_i \leq (2/C_{15})\left(\sum_{i=1}^{k}\log r_i\right)(U_0/D)$$

$$\begin{aligned} \sum_{i=1}^{k}|\mathbf{n}_i|\log r_i' &\leq |\mathbf{n}|\log\max_i r_i' \\ &\leq (k+1)T\log\max_i r_i' \\ &\leq (k+1)(\log\max_i r_i')(U_0/D) \end{aligned}$$

$$\begin{aligned}\sum_{i=1}^{k} |\mathbf{n}_i| \log(c_i L_i + |\mathbf{n}_i|\,(q_i - 1)) \le& |\mathbf{n}| \log \max_i (2(k+1)T(q_i - 1)) \\ \le& (k+1)T \log \max_i (2(k+1)T(q_i - 1)) \\ =& (k+1)T(\log(2(k+1)T) + \log \max_i (q_i - 1)) \\ \le& (\frac{1}{2} C_{20} + (k+1) \log \max_i (q_i - 1))(U_0/D)\end{aligned}$$

$$\begin{aligned}\sum_{i=1}^{k} |\mathbf{n}_i| \log \kappa_i \le& |\mathbf{n}| \log \max_i \kappa_i \\ \le& (k+1)T \log \max_i \kappa_i \\ \le& (k+1)(\log \max_i \kappa_i)(U_0/D)\end{aligned}$$

$$\begin{aligned}&\sum_{i=1}^{k} 2c_i L_i \,\mathrm{h}(\gamma_i') \\ \le& \sum_{i=1}^{k} 2c_i L_i (\hat{\mathrm{h}}(\gamma_i') + \hbar_i) \\ \le& \sum_{i=1}^{k} 2c_i L_i (k+1)^2 S^2 \,\hat{\mathrm{h}}(\gamma_i) + \sum_{i=1}^{k} 2c_i T/m \,\hbar_i \\ \le& \left(\sum_{i=1}^{k} 2(k+1)^2 c_i C_{17} + \sum_{i=1}^{k} 2c_i \right) (U_0/D)\end{aligned}$$

$$\begin{aligned}\sum_{i=1}^{k}(2c_i'L_i + |\mathbf{n}_i|\, q_i')\,\mathrm{h}(G_i) &\leq \sum_{i=1}^{k} 2c_i'T\,\mathrm{h}(G_i) + |\mathbf{n}|\max_i q_i'\,\mathrm{h}(G_i)\\ &\leq \sum_{i=1}^{k} 2c_i'(U_0/D) + (k+1)T\max_i q_i'\,\mathrm{h}(G_i)\\ &\leq \left(\sum_{i=1}^{k} 2c_i' + (k+1)\max_i q_i'\right)(U_0/D)\end{aligned}$$

$$\begin{aligned}&\sum_{i=1}^{k}(2c_iL_i + |\mathbf{n}_i|\,(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))\\ \leq&\sum_{i=1}^{k}(2c_iT + (k+1)T(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))\\ \leq&\sum_{i=1}^{k}(2c_i + (k+1)(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))(U_0/D)\end{aligned}$$

Putting all of this together, we get

$$\begin{aligned}&\mathrm{h}\left(\frac{\mathrm{D}^{\mathbf{t}}_{\mathbf{e}}(F/f)\big|_0}{\prod_{i=1}^{k}\left(R^{(i)}_{\nu_i}(\mathbf{\Psi}_i(0),\gamma_i')\right)^{L_i}}\right)\\ \leq&(C_{10} + 1 + (k+1)\log 2 + (1/d)\log C_2 + 2 + (1/d)\log((k+1)C_{13})\\ &+ (2/C_{15})\sum_{i=1}^{k}\log r_i + (k+1)\log\max_i r_i'\\ &+ \frac{1}{2}C_{20} + (k+1)\log\max_i(q_i-1) + (k+1)\log\max_i\kappa_i\\ &+ \sum_{i=1}^{k}2(k+1)^2c_iC_{17} + \sum_{i=1}^{k}2c_i + \sum_{i=1}^{k}2c_i' + (k+1)\max_i q_i'\\ &+ \sum_{i=1}^{k}(2c_i + (k+1)(q_i-1))\,\mathrm{h}(\mathbf{\Psi}_i(0))(U_0/D)\\ \leq&(C_{10} + C_{23} - 1)U_0/D\\ \leq&(C_{12} - 1)U_0/D\end{aligned}$$

By Louiville's Theorem, therefore, we have

$$\log\left|\frac{\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f)\big|_0}{\prod_{i=1}^{k}\left(R_{\nu_i}^{(i)}(\mathbf{\Psi}_i(0),\gamma_i')\right)^{L_i}}\right| > -(C_{12}-1)U_0.$$

Finally, since

$$\log|\Phi_{i,\nu_i}(s\mathbf{u})| \geq H_i^-(|s\mathbf{u}_i|) \geq -(1/k)U_0,$$

we conclude that

$$\left|\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}\,F(s\mathbf{u})\right| = \left|f\,\mathrm{D}_{\mathbf{e}}^{\mathbf{t}}(F/f)\right| > \exp(-C_{12}U_0).$$

□

Chapter 7

Evaluating the Constants

In this chapter, we assume that for each $1 \leq i \leq k$, the group G_i is the Jacobian of the genus-two curve

$$y^2 = f_{i,6}x^6 + f_{i,5}x^5 + f_{i,4}x^4 + f_{i,3}x^3 + f_{i,2}x^2 + f_{i,1}x + f_{i,0}.$$

The parameters defining the group are $\boldsymbol{\vartheta}_i = (f_{i,0}, f_{i,1}, f_{i,2}, f_{i,3}, f_{i,4}, f_{i,5}, f_{i,6})$, and so we define

$$\mathrm{h}(G_i) = (1, f_{i,0}, f_{i,1}, f_{i,2}, f_{i,3}, f_{i,4}, f_{i,5}, f_{i,6}).$$

In the next chapter, we will see how to compute the polynomials $R_j^{(i)}$ and $Q_{k,l}^{(i,j)}$. The result is the following: The polynomials $Q_{k,l}^{(i,j)}$ have degree $q_i = 2$ in the variables and degree at most $q_i' = 4$ in the parameters $f_{i,0}, \ldots, f_{i,6}$. The polynomials $2Q_{k,l}^{(i,j)}$ have integer coefficients (so $\kappa_i = 2$) and length at most $r_i' = 2234$. The polynomials $R_j^{(i)}$ have degree $c_i = 2$ in each set of variables, and degree at most $c_i' = 8$ in the parameters $f_{i,0}, \ldots, f_{i,6}$, and length at most $r_i = 32920512$. Therefore, $c = 2$ as well.

Since the Jacobian has dimension $d_i = 2$, and $d_0 = 1$, we have $d = 2k + 1$. By Equations 3.5 and 8.1,

$$\mathrm{Hf}(\mathbb{G}; L_0, \ldots, L_k) = (L_0 + 1) \prod_{i=1}^{k} (16L_i)^2$$

and therefore we have

$$m = d!16^k = (2k + 1)!2^{4k}.$$

Furthermore, this simple form of the Hilbert function allows us to guarantee

$$\frac{1}{d!}\,\mathrm{H}(\mathbb{G};\mathbf{L}) \leq \mathrm{Hf}(\mathbb{G};\mathbf{L}),$$

allowing us to take $C_{19} = 0$.

Now we choose the constants as follows: First we define

$$\begin{aligned} C_4 =& 1/5 \\ C_{19} =& 0 \\ C_5 =& 6d \\ C_{17} =& 1 \\ C_6 =& 2/d = 2/(2k+1) \\ C_{18} =& (2k+3)!(2k+2)^{2k}. \end{aligned}$$

Then we guess an upper bound for C_{14} and use it to define C_7. One choice is the following:

$$\begin{aligned} C_7 =& 28 + 16(2k+3)\log(2k+3) \\ C_{14} =& C_7 C_{18} \end{aligned}$$

Next, we guess an upper bound for C_{16} and use this to guess an upper bound for C_2, which we use to define C_{20}. Then we can use these to define the remaining constants. The result is the following:

$$\begin{aligned}
\log C_2 <&16k+4+(16k^2+34k+8)\log(2k+3)\\
C_{20} =&2(k+1)(18k+5+(16k^2+34k+9)\log(2k+3))\\
=&36k^2+46k+10+(32k^3+100k^2+86k+18)\log(2k+3)\\
C_{23} =&4k^3+26k^2+61k+39+(16k^3+50k^2+51k+24)\log(2k+3)\\
C_{21} =&4k^3+28k^2+31k+11+(16k^3+50k^2+44k+10)\log(2k+3)\\
C_{16} =&4(4k^2+23k+27)+4(16k^2+34k+14)\log(2k+3)\\
C_{13} =&C_{14}C_{16}\\
C_2 =&2C_{13}^{2d-1}/mC_{17}^{d-1}C_6\\
C_{10} =&\frac{1}{4}(k+1)C_{16}\\
=&4k^3+27k^2+50k+27+(16k^3+50k^2+48k+14)\log(2k+3)\\
C_{12} =&C_{10}+C_{23}\\
=&8k^3+53k^2+111k+66+(32k^3+100k^2+99k+38)\log(2k+3)\\
C_{22} =&(k+1)(7/4+2(2k+3)\log(2k+3))C_{16}+1\\
C_{11} =&(k+1)(11/4+2(2k+3)\log(2k+3))C_{16}+1\\
C_9 =&(k+1)(11/4+2(2k+3)\log(2k+3))C_{16}+1+\log(d-1)\\
C_8 =&36k^2+49k+16+(32k^3+100k^2+90k+22)\log(2k+3)\\
C_3 =&C_{11}+2(k+1)\log d+C_{20}+C_{10}+3k+6\\
<&C_{11}+4k^3+63k^2+99k+43+(48k^3+150k^2+136k+34)\log(2k+3)
\end{aligned}$$

It is readily checked that these formulas satisfy all of the inequalities from chapter 4.

Computing the values of $C_1 = C_3C_2$ from the above formulas, we get the first 8 rows of the table given in section 1.3, reproduced here:

k	C_1
1	2.1×10^{44}
2	6.8×10^{112}
3	6.6×10^{219}
4	2.5×10^{369}
5	4.9×10^{564}
6	1.9×10^{808}
7	2.1×10^{1102}
8	4.6×10^{1448}
$k \geq 9$	$(2k^2)^{16k^2+14k+3}2^{22k+8}$

The last row is computed by assuming $k \geq 9$ and computing upper bounds on C_7, C_{14}, C_{16}, C_{13}, C_2, C_3, and finally C_1.

Chapter 8

Jacobians of Genus 2 Curves

8.1 Classes of Divisors

As stated in [4] (chapter one), every curve of genus 2, over a number field K, is birationally equivalent to a plane curve of the form

$$y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where the polynomial $f(x)$ has degree 5 or 6 (i.e. not both f_5 and f_6 are zero) and has no multiple factors. (Indeed, the degree being at least 5 can be thought of as ∞ not being a double root.) This form is unique up to a fractional linear transformation of x and an associated transformation of y, of the form

$$x \rightarrow (ax + b)/(cx + d),\, y \rightarrow ey/(cx + d)^3$$

where a, b, c, d, and e are elements of K, with e and $ad - bc$ nonzero. If the polynomial on the right has a root in K (e.g. if K is algebraically closed), then one such transformation will make $f_6 = 0$ and $f_5 = 1$. This is often assumed in the classical theory, but since number fields are not algebraically closed, and we will not, in general, have a root in the field, we will not assume that $f_6 = 0$.

This curve is nonsingular at all finite points (x, y) but has a singular point at infinity. In the case where $f_6 \neq 0$, there are two distinct places at infinity, whose power series are given by

$$(t^{-1},\, st^{-3}+O(t^{-4}))$$

for each of the two square roots s of f_6. Using the notation of [4], we denote them by ∞^+ and ∞^-. (If f_6 is real, then we can interpret the $+$ and $-$ as the sign of the square root. In most cases, however, it won't matter which is which.) In the case where $f_6 = 0$, there is a single place at infinity, whose power series is given by

$$(t^{-2},\, \sqrt{f_5}t^{-5}+O(t^{-6}))$$

where the choice of the square root does not matter, since the change-of-variables

$$t \to -t$$

changes one into the other. In this case, we will say that $\infty^+ = \infty^-$.

The Jacobian J is the group of divisors of degree zero modulo principal divisors.

Theorem 8.1. *Every divisor class of degree zero contains exactly one divisor of the form*

$$P+Q-\infty^+-\infty^-$$

(for some points P and Q on the curve) except for the zero (i.e. identity or principal) divisor class, which contains all divisors of the form

$$P+\bar{P}-\infty^+-\infty^-$$

where $\bar{P}$ denotes the conjugate of P (under the $Y \to -Y$ involution).

Proof. For the second part, if $P = (a, b)$ is a finite point, then the line $x = a$ intersects the curve in the divisor

$$P+\bar{P}-\infty^+-\infty^-.$$

Similarly, if P is a point at infinity, then

$$P + \bar{P} = \infty^+ + \infty^-$$

and a nonzero constant function has the required divisor.

For the first part, let D be a divisor of degree zero, and let C be the canonical divisor

$$C = \infty^+ + \infty^-.$$

Let $L(C+D)$ and $L(-D)$ be the vector spaces of functions with divisor greater than or equal to $-(C+D)$ and D, respectively. The Riemann-Roch Theorem says that

$$\dim L(C+D) = \deg(C+D) + 1 - g + \dim L(-D).$$

The genus $g = 2$, and the degree of $C+D$ is also 2. The question that remains is the dimension of $L(-D)$. The degree of $-D$ is zero. Since the divisor of a function always has degree zero, any function in $L(-D)$ must have a divisor equal to $-D$. Therefore, $L(-D)$ has dimension zero unless $-D$ (and therefore D) is in the principal divisor class. So if D is not principal, then the dimension of $L(C+D)$ is one, which means that there is a nonzero function f in $L(C+D)$, which must have

$$\operatorname{div}(f) = P + Q - C - D = P + Q - \infty^+ - \infty^- - D.$$

Therefore

$$D + \operatorname{div}(f) = P + Q - \infty^+ - \infty^-$$

is in the same class as D. Furthermore, every other function in $L(C+D)$ is a constant multiple of f and therefore has the same divisor, so the pair $\{P, Q\}$ is unique (up to exchanging P with Q). □

We shall, therefore, represent points on the Jacobian by pairs of points on the curve, $\{P, Q\}$. Every point of the Jacobian can be represented in this way, and the representation is unique (up to order) unless it represents the zero point of the Jacobian, in which case we will usually simply write 0.

If the coordinates of P and Q belong to a field $\bar{K}$, then elements of the Galois group of $\bar{K}$ over K act on the divisor $P + Q - \infty^+ - \infty^-$ and the pair $\{P, Q\}$. The divisor (or point on the Jacobian) is rational when it is fixed by the Galois group. Therefore, it is rational if and only if P and Q are both rational points on the curve or are defined over a quadratic extension of K and their x (resp. y) coordinates are conjugate to one another. In particular, ∞^+ and ∞^- are both rational points if and only if f_6 is a square (possibly zero), and otherwise they are defined over a quadratic extension (namely $K(\sqrt{f_6})$) and conjugate. For example, the pair $\{(\sqrt{2}, 1 + \sqrt{2}), (-\sqrt{2}, 1 - \sqrt{2})\}$ gives a rational point on the Jacobian of the curve $y^2 = x^5 - x^3 + 3$.

Addition in the Jacobian corresponds to addition of divisors, but there is some work involved in putting the sum in the same form as the summands. In particular, the sum of the divisor

$$P_1 + Q_1 - \infty^+ - \infty^-$$

and the divisor

$$P_2 + Q_2 - \infty^+ - \infty^-$$

can be written as

$$P_1 + Q_1 - \infty^+ - \infty^- + P_2 + Q_2 - \infty^+ - \infty^- = P_3 + Q_3 - \infty^+ - \infty^-$$

for some points P_3 and Q_3. One way to find these points, in the general case, is to compute the unique polynomial $g(x)$ of degree less than 4 such that $y = g(x)$ passes through all four points P_1, Q_1, P_2, and Q_2. Then the divisor of $y - g(x)$ is $-3(\infty^+ + \infty^-)$ plus six points whose x coordinates are the roots of the polynomial

$$g(x)^2 - f(x)$$

and whose y coordinates are given by $y = g(x)$. It is easily checked that four of these six points must be P_1, Q_1, P_2, and Q_2, and the remaining two are $\bar{P}_3$ and $\bar{Q}_3$.

8.2 Projective Coordinates

The Jacobian is also a complete algebraic variety, and therefore it can be embedded into projective space and the group law given as polynomials in the projective coordinates. This is proved in [20] by embedding Zariski-open subsets of the Jacobian into affine 4-space. For example, when $P = (a, b)$ and $Q = (c, d)$ are distinct finite points and not conjugates of one another, then we may map the point $\{P, Q\}$ to

$$(a + c,\ ac,\ (b - d)/(a - c),\ (bc - ad)/(a - c)).$$

Notice that this is rational if and only if $\{P, Q\}$ is a rational point of the Jacobian.

It is customary to describe this mapping in terms of polynomials. That is, the point on the Jacobian given by the two points P and Q is represented by the pair of polynomials

$$
\begin{aligned}
U(T) =&(T-a)(T-c) = T^2 - (a+c)T + ac \\
V(T) =&T(b-d)/(a-c) - (bc-ad)/(a-c).
\end{aligned}
$$

These are the (unique) polynomials such that $U(T)$ is a monic quadratic whose roots are the x coordinates of the points P and Q, and $V(T)$ is a polynomial of degree less than 2 such that both P and Q lie on the line given by $y = V(x)$. Notice that these polynomials have the property that $U(T)$ divides the polynomial $f(T) - V(T)^2$. Sometimes a third polynomial $W(T)$ is also used, where

$$U(T)W(T) = f(T) - V(T)^2.$$

The group law may be described in terms of these polynomials using an algorithm reminiscent of the method of reduction of quadratic forms. (This is known as "Cantor's Algorithm" in some sources.) We shall not have need to use this algorithm, but details may be found in [3]. (See also [15].)

The map from the Jacobian J into affine four-space given by the coefficients of $U(T)$ and $V(T)$ is, unfortunately, singular along the so-called "theta divisor" of the Jacobian, where P or Q is infinite, or where they are conjugates of one another. (This is a divisor, or codimension-one subvariety, of the Jacobian, and not of the curve.) This map can, however, be extended to the case where $P = Q$. When doing group law computations, this problem may be avoided by using polynomials of different degrees on the theta divisor, and this technique works very nicely with the algorithm for adding points. It does not, unfortunately, lend itself well to defining a nonsingular embedding of J.

A different embedding is given in [4] which is not singular. Its image lies in projective 15-space. For P and Q as above (with $a \neq c$), we set

$$\begin{aligned}
X_{15} &= (a-c)^2 \\
X_{14} &= 1 \\
X_{13} &= a+c \\
X_{12} &= ac \\
X_{11} &= ac(a+c) \\
X_{10} &= a^2c^2 \\
X_9 &= (b-d)/(a-c) \\
X_8 &= (bc-ad)/(a-c) \\
X_7 &= (bc^2-a^2d)/(a-c) \\
X_6 &= (bc^3-a^3d)/(a-c) \\
X_5 &= (F_0(a,c)-2bd)/(a-c)^2 \\
X_4 &= (F_1(a,c)-(a+c)bd)/(a-c)^2 \\
X_3 &= acX_5 \\
X_2 &= (G(a,c)b-G(c,a)d)/(a-c)^3 \\
X_1 &= (H(a,c)b-H(c,a)d)/(a-c)^3 \\
X_0 &= X_5^2
\end{aligned}$$

where

$$\begin{aligned}
F_0(a,c) =& 2f_0 + f_1(a+c) + 2f_2(ac) + f_3(a+c)(ac) \\
& + 2f_4(ac)^2 + f_5(a+c)(ac)^2 + 2f_6(ac)^3 \\
F_1(a,c) =& f_0(a+c) + 2f_1(ac) + f_2(a+c)(ac) + 2f_3(ac)^2 \\
& + f_4(a+c)(ac)^2 + 2f_5(ac)^3 + f_6(a+c)(ac)^3 \\
G(a,c) =& 4f_0 + f_1(a+3c) + f_2(2ac+2c^2) + f_3(3ac^2+c^3) \\
& + f_4(4ac^3) + f_5a(ac^3+3c^4) + f_6(2a)(ac^4+c^5) \\
H(a,c) =& 2f_0(a+c) + f_1c(3a+c) + f_2(4ac^2) + f_3ac^2(a+3c) \\
& + f_42ac^3(a+c) + f_5ac^4(3a+c) + f_6(4a^2c^5)
\end{aligned}$$

Ten of these variables are even in the sense that they are unchanged by the transformation

$$b \to -b, \, d \to -d.$$

The remaining six variables are odd, for they change change sign under this transformation. The even variables are X_0, X_3, X_4, X_5, X_{10}, X_{11}, X_{12}, X_{13}, X_{14}, and X_{15}. The odd variables are X_1, X_2, X_6, X_7, X_8, and X_9.

Some of the quadratic equations that are satisfied everywhere on the Jacobian include the following:

$$
\begin{aligned}
X_{15}X_{14} =& X_{13}^2 - 4X_{12}X_{14} \\
X_{11}X_{14} =& X_{12}X_{13} \\
X_{10}X_{14} =& X_{12}^2 \\
X_7X_{14} =& X_8X_{13} - X_9X_{12} \\
X_6X_{14} =& X_7X_{13} - X_8X_{12} \\
X_5X_{14} =& - f_2X_{14}^2 - f_3X_{14}X_{13} - f_4X_{13}^2 - 3f_5X_{13}X_{12} - f_5X_{13}X_{15} \\
& - f_6X_{14}X_{10} - 6f_6X_{12}X_{15} - 8f_6X_{12}^2 - f_6X_{15}^2 + X_9^2 \\
X_4X_{14} =& X_9X_8 - f_3X_{14}X_{12} - f_4X_{14}X_{11} - f_5X_{12}X_{15} - 4f_5X_{12}^2 \\
& - f_6X_{11}X_{15} - 2f_6X_{11}X_{12} - f_6X_{13}X_{10} \\
X_3X_{14} =& X_{12}X_5 \\
X_2X_{14} =& X_9X_5 - f_3X_{14}X_8 - 2f_4X_{14}X_7 - 2f_5X_{14}X_6 - 2f_6X_{13}X_6 - f_5X_8X_{12} \\
X_1X_{14} =& X_5X_8 - 2f_6X_{12}X_6 - f_5X_7X_{12} \\
X_0X_{14} =& X_5^2
\end{aligned}
$$

These equations are significant in that, when the variables are normalized by setting $X_{14} = 1$, we can define the other variables as polynomials in only the four X_8, X_9, X_{12}, X_{13} (which are the coefficients of $U(T)$ and $V(T)$). In fact, the Jacobian is defined, as an algebraic variety in $\mathbb{P}^15$, by the above polynomials together with the following two:

$$0 = -f_1X_{14}^2 - f_3X_{14}X_{12} + 2f_4X_{13}X_{12} - f_5X_{12}^2 - 2X_4X_{14} - 2f_4X_{14}X_{11} + X_5X_{13}$$

$$0 = X_8^2 - X_5X_{12} - f_0X_{14}^2 - f_4X_{12}^2 - f_5X_{12}X_{11} - f_6X_{15}X_{10} - 4f_6X_{10}X_{12}$$

We can take limits as P approaches Q or $\bar{Q}$, and as one or both points grows to infinity. The result are as follows: The identity (when $P = \bar{Q}$) is

$$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

When $P = Q = (a, b)$ (and $b \neq 0$ so that $P \neq \bar{Q}$), the image is

$$\begin{aligned} X_{15} =& 0 & X_{10} =& a^4 \\ X_{14} =& 1 & X_9 =& f'(a)/(2b) \\ X_{13} =& 2a & X_8 =& -b + af'(a)/(2b) \\ X_{12} =& a^2 & X_7 =& -2ab + a^2f'(a)/(2b) \\ X_{11} =& 2a^3 & X_6 =& -3a^2b + a^3f'(a)/(2b) \end{aligned}$$

Then X_0 through X_5 are defined from the equations above. Of course, since $X_{14} = 1$, it suffices to define X_8, X_9, X_{12}, and X_{13}, and then the others follow from the equations above.

When $P = (a, b)$ and Q is the point at infinity with $y/x^3 = s$ for one of the square roots s of f_6 (note that this only gives a rational divisor, hence a rational point on the Jacobian, when f_6 is a square, and also note that $f_6 = 0$ implies $s = 0$), then the image is

$$
\begin{array}{ll}
X_{15} = 1 & X_7 = sa^2 \\
X_{14} = 0 & X_6 = sa^3 - b \\
X_{13} = 0 & X_5 = 0 \\
X_{12} = 0 & X_4 = s^2a^3 - sb = sX_6 \\
X_{11} = a & X_3 = 2s^2a^4 + f_5a^3 - 2sab \\
X_{10} = a^2 & X_2 = 2s^3a^4 + f_5sa^3 - 2s^2ab = sX_3 \\
X_9 = s & X_1 = 4s^3a^5 + 3f_5sa^4 + 2f_4sa^3 + f_3sa^2 - 4s^2a^2b - f_5ab \\
X_8 = sa & X_0 = (2s^2a^3 + f_5a^2 - 2sb)^2 = (X_3/a)^2.
\end{array}
$$

These formulas can be obtained by substituting into the above equations $c = t$, writing $d = \sqrt{f(t)}$ as a power series in t^{-1}, and taking the leading coefficient in each expansion. The same formulas are obtained in the case where $f_6 = 0$ by substituting $c = t^2$ and $d = \sqrt{f(t^2)}$.

When $P = Q$ is the point at infinity with $y/x^3 = s$ for one of the square roots

s of f_6, then the image is

$$\begin{aligned}
X_{15} &= 0 & X_7 &= 16s^5 \\
X_{14} &= 0 & X_6 &= -8f_5s^3 \\
X_{13} &= 0 & X_5 &= 0 \\
X_{12} &= 0 & X_4 &= -8f_4s^4 \\
X_{11} &= 0 & X_3 &= 4s^2(f_5^2 - 4f_4s^2) \\
X_{10} &= 16s^4 & X_2 &= 4s^3(f_5^2 - 4f_4s^2) = sX_3 \\
X_9 &= 0 & X_1 &= 2s(4f_4f_5s^2 - 3f_5^3 - 8f_3s^4) \\
X_8 &= 0 & X_0 &= (f_5^2 - 4f_4s^2)^2.
\end{aligned}$$

These formulas can be obtained by using either the formulas for $Q = \infty$ or the formulas for $P = Q$ and substituting the power series obtained from $b = \sqrt{f(a)}$. Notice, in particular, that this formula also applies when $s = 0$, in which case

$$P + Q - \infty^+ - \infty^- = \infty + \infty - \infty - \infty = 0,$$

and so we have the zero point

$$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

As pointed out in [4] (at the end of section 2.3), these projective variables generate the same line bundle as Mumford's theta functions (see [22]). Therefore, the Hilbert function for the Jacobian is

$$\mathrm{Hf}(J; x) = (4x)^2, \tag{8.1}$$

and therefore this embedding of the Jacobian into projective 15-space maps the Jacobian onto a 2-dimensional surface of degree 32.

8.3 Local Series

It is useful to consider, as described in [4] (section 2.3), the behavior of basis elements near the zero of the Jacobian. To do this, one normalizes to $X_0 = 1$ and writes the other coordinates as power series in X_1 and X_2. The leading terms are

$$\begin{aligned} X_3 =& X_1^2 + \dots & X_9 =& X_2^3 + \dots \\ X_4 =& X_1X_2 + \dots & X_{10} =& X_1^4 + \dots \\ X_5 =& X_2^2 + \dots & X_{11} =& 2X_1^3X_2 + \dots \\ X_6 =& X_1^3 + \dots & X_{12} =& X_1^2X_2^2 + \dots \\ X_7 =& X_1^2X_2 + \dots & X_{13} =& 2X_1X_2^3 + \dots \\ X_8 =& X_1X_2^2 + \dots & X_{14} =& X_2^4 + \dots \end{aligned}$$

$$X_{15} = 4\sum_{j=0}^{6} f_j X_1^j X_2^{6-j} + \dots .$$

Cassels and Flynn point out in [4] that the local series are useful for finding relations between the basis elements. Other uses stem from the fact that a function given by local series has a unique form, whereas the same function can be described in many different ways using projective coordinates. For example, it is easy to take the square root of a square function described as a local series, but it is much more difficult to do the same thing directly with projective coordinates.

Furthermore, even when dealing with projective coordinates directly, or when dealing in the x and y coordinates of the points P and Q, it is useful to speak of the “order” of coordinates or functions, where this order is defined as the order of the local series (or as the order of vanishing of the function at the origin). For example, X_0 has order 0, X_1 and X_2 have order 1, X_3, X_4, and X_5 have order 2, X_6 through X_9 have order 3, X_{10} through X_{14} have order 4, and X_{15} has order 6.

We describe how to compute the local series for the basis elements. Recall that the zero of the Jacobian is the represented by the pair $\{(a, b), (c, d)\}$ with $a = c$ and $b = -d$. Therefore, we first write $c = a - h$ ([4] says $c = a + h$, but this is a typo, as it gives different signs on many of the other formulas in [4]) and then we write $d = \sqrt{f(a-h)}$ as a power series in h with first term $-b$,

$$d = -b + \frac{f'(a)}{2b}h + \frac{f'(a)^2 - 2b^2 f''(a)}{(2b)^3}h^2 + O(h^3).$$

Then all of the basis elements can be written as power series in h by substitution. For example,

$$X_1 = \frac{H(a,c)b - H(c,a)d}{(F_0(a,c) - 2bd)^2(a-c)} = \frac{a}{2b}h + \frac{af'(a) - 2f(a)}{(2b)^3}h^3 + O(h^5).$$

Since the leading terms of X_1 and X_2 are, respectively, $ah/2b$ and $h/2b$, one can read off the first terms of a local series from the coefficients of a. That is, take the coefficient of the leading term h^n, multiply by $(2b)^n$, and the result will be expressible (possibly by changing b^2 to $f(a)$) as a polynomial in a, of degree at most n. The coefficient of a^j in this polynomial is the coefficient of $X_1^j X_2^{n-j}$ in the local series. For example,

$$X_3 = \frac{ac(a-c)^2}{F_0(a,c) - 2bd} = \frac{a^2}{(2b)^2}h^2 + \frac{2a(af'(a) - 2f(a))}{(2b)^4}h^3 + O(h^4)$$

has leading coefficient $a^2/(2b)^2$ of h^2. Multiplying by $(2b)^2$, we get the polynomial a^2. Therefore, the first-order terms of the local series for X_3 are X_1^2. By substituting $X_1^j X_2^{n-j}$ (as a series in h) for a^j and subtracting the resulting series, one may expose the terms of next degree and repeat the process. For example,

$$X_3 - X_1^2 = -\frac{f_0 + f_4 a^4}{(2b)^4} h^4 + O(h^5),$$

and so the second-order terms of the local series for X_3 are $-f_4 X_1^4 - f_0 X_2^4$.

The power series that are computed in this process have rational functions for coefficients that tend to grow large very quickly and become difficult to compute, so certain optimizations help considerably. One can avoid the need for rational functions and use only polynomials if one writes everything as power series in $k = h/(2b)^2$ instead of h. For example,

$$X_3 = a^2(2b)^2k^2 + 2a(af'(a) - 2f(a))(2b)^2k^3 + O(k^4).$$

Of course, this necessitates dividing the coefficient of k^n by $(2b)^n$ instead of multiplying.

Furthermore, doing these computations requires some changing back and forth between a and b (that is, between $f(a)$ and b^2), which is easy to do manually but harder to automate. It turns out, however, that one can avoids all use of the variable b, which makes the computations run significantly faster. It turns out that d/b can be written easily as a power series in k whose coefficients are polynomials in a,

$$d/b = -1 + 2f'(a)k + 2(f'(a)^2 - 2b^2 f''(a))k^2 + O(k^3).$$

Furthermore, if we let n be the order of X_i, then $X_i/(2b)^n$ can be written in terms of a, c, and d/b (by changing b^2 to $f(a)$). The first term in the resulting series is k^n times a polynomial in a of degree at most n, and the coefficient of a^j is the coefficient in the local series of $X_1^j X_2^{n-j}$. Those terms of the local series should be subtracted off in order to get the next term. Since each of the basis elements is either even or odd, there is no k^{n+1} term, and the higher terms will now all be divisible by $(2b)^2 = 4f(a)$. After dividing, the coefficient of k^{n+2} is a polynomial in a whose coefficients give the next terms of the local series, and so on.

Repeating our previous example with this new method, we have

$$\frac{X_3}{(2b)^2} = a^2k^2 + 2a(af'(a) - 2f(a))k^3 + O(k^4),$$

and we pull off the first-order terms X_1^2 from the leading coefficient. Then we subtract the first-order terms. Notice that since we have stored $X_1/2b$ and $X_2/2b$, we can simply use the squares of these series, and the denominators match. Subtracting the first-order terms also eliminates the k^3 term, and the result is divisible by $(2b)^2$, so we divide each term of the series by 4f(a), and get

$$\left(\frac{X_3}{(2b)^2} - \left(\frac{X_1}{2b}\right)^2\right) = (-f_0 - f_4x^4)k^4 + O(k^5).$$

Mathematica© code for generating the local series can be found in Appendix B.

8.4 Quadratic Forms

The group law on the Jacobian, as will as derivatives of the coordinate functions, can be given by quadratic forms in the 16 basis elements. The quadratic forms that are zero on the Jacobian give a set of defining equations for the Jacobian as a projective variety. For these reasons and others, it is worthwhile to understand the space of quadratic forms on the Jacobian.

By 8.1, the vector space of quadratic functions on the Jacobian has dimension 64. Since there are $16 \times 17/2 = 136$ ways to multiply 2 of the 16 basis elements together, the vector space of quadratic forms that are zero on the Jacobian has dimension 72. A basis for this vector space can be downloaded from Flynn's ftp site, as stated in [4].

It is useful to categorize these functions by their orders, as introduced in the previous section, and we will give an explicit basis for the vector space of quadratic functions on the Jacobian.

Consider the vector space of all local series of order n modulo those of order $n+1$. Since this vector space is generated by the basis

$$X_1^n,\, X_1^{n-1}X_2,\, \ldots, X_1X_2^{n-1}, X_2^n,$$

it has dimension $n+1$. Consequently, the subspace (which we will denote V_n for the moment) of quadratic functions of order n modulo those of order $n+1$ has dimension at most $n+1$. It turns out that we get equality when $n \leq 9$. In fact, when $n \leq 8$, it is easy to find a basis for V_n by looking at the leading terms of the local series. For $n = 9$, one has to look at second-order terms in the local series to find ten generators.

n	Basis for V_n
0	$\{X_0^2\}$
1	$\{X_0X_1,\ X_0X_2\}$
2	$\{X_0X_3,\ X_0X_4,\ X_0X_5\}$
3	$\{X_0X_6,\ X_0X_7,\ X_0X_8,\ X_0X_9\}$
4	$\{X_0X_{10},\ X_0X_{11},\ X_0X_{12},\ X_0X_{13},\ X_0X_{14}\}$
5	$\{X_3X_6,\ X_4X_6,\ X_5X_6,\ X_5X_7,\ X_5X_8,\ X_5X_9\}$
6	$\{X_3X_{10},\ X_4X_{10},\ X_5X_{10},\ X_4X_{12},\ X_5X_{12},\ X_4X_{14},\ X_5X_{14}\}$
7	$\{X_6X_{10},\ X_7X_{10},\ X_8X_{10},\ X_9X_{10},\ X_8X_{12},\ X_9X_{12},\ X_8X_{14},\ X_9X_{14}\}$
8	$\{X_{10}X_{10},\ X_{10}X_{11},\ X_{10}X_{12},\ X_{10}X_{13},\ X_{10}X_{14},$ $X_{11}X_{14},\ X_{12}X_{14},\ X_{13}X_{14},\ X_{14}X_{14}\}$
9	$\{X_6X_{15},\ X_7X_{15},\ X_8X_{15},\ X_9X_{15},\ 2X_7X_{10}-X_6X_{11},\ X_8X_{10}-X_6X_{12},$ $X_9X_{10}-X_7X_{12},\ X_8X_{12}-X_6X_{14},\ X_9X_{12}-X_7X_{14},\ X_9X_{13}-2X_8X_{14}\}$

We have given 55 linearly independent quadratic forms in the above table, which means that there are still 9 dimensions left undescribed. It turns out that 8 of them have order 10, and the remaining 1 has order 12. A basis for the 8-dimensional space V_{10} is given by

$$X_{15}X_{10} = (a-c)^2a^2c^2$$

$$X_{15}X_{11} = (a-c)^2(a+c)ac$$

$$X_{15}X_{12} = (a-c)^2ac$$

$$X_{15}X_{13} = (a-c)^2(a+c)$$

$$X_{15}X_{14} = (a-c)^2$$

$$-X_{15}X_5 + 4f_6X_{10}X_{12} + 2f_5X_{10}X_{13} + 4f_4X_{10}X_{14}$$

$$+2f_3X_{11}X_{14} + 4f_2X_{12}X_{14} + 2f_1X_{13}X_{14} + 4f_0X_{14}X_{14} = F_0(a,c) + 2bd$$

$$-X_{15}X_4 + 2f_6X_{10}X_{11} + 4f_5X_{10}X_{12} + 2f_4X_{10}X_{13}$$

$$+4f_3X_{10}X_{14} + 2f_2X_{11}X_{14} + 4f_1X_{12}X_{14} + 2f_0X_{13}X_{14} = F_1(a,c) + (a+c)bd$$

$$-X_{15}X_3 + 4f_6X_{10}X_{10} + 2f_5X_{10}X_{11} + 4f_4X_{10}X_{12}$$

$$+2f_3X_{10}X_{13} + 4f_2X_{10}X_{14} + 2f_1X_{11}X_{14} + 4f_0X_{12}X_{14} = ac(F_0(a,c) + 2bd)$$

The 1-dimensional space V_{12} is, of course, generated by

$$X_{15}^2 = (a-c)^4.$$

8.5 The Kummer Variety

Associated with the Jacobian of our genus-2 curve is another variety known as the Kummer variety. It is a 2-dimensional surface embedded into projective 3-space, and it is defined by $(\xi_1, \xi_2, \xi_3, \xi_4) \in \mathbb{P}^3$ satisfying a certain fourth-degree polynomial which can be found in [4], chapter 3. There is a surjective map from the Jacobian to the Kummer variety given by

$$(\xi_1, \xi_2, \xi_3, \xi_4) = (X_{14}, X_{13}, X_{12}, X_5),$$

which is two-to-one except at the 16 (complex) points of order 2 on the Jacobian, where the Jacobian points P and $-P$ map to the same point on the Kummer variety. The above map is not properly defined at certain points where

$$X_{14} = X_{13} = X_{12} = X_5 = 0,$$

namely, at points corresponding to the divisors $P + Q - \infty^+ - \infty^-$ where P or Q is itself a point at infinity. The map does, however, extend continuously to such points, and the map becomes as follows. When $P = (a, b)$ and Q is the point at infinity with $y/x^3 = s$ for one of the square roots s of f_6, the image is

$$(\xi_1, \xi_2, \xi_3, \xi_4) = (0, 1, a, 2s^2a^3 + f_5a^2 - 2sb),$$

and when $P = Q$ is a point at infinity, the image is

$$(\xi_1, \xi_2, \xi_3, \xi_4) = (0, 0, 4f_6, f_5^2 - 4f_4f_6),$$

The identity maps to $(0, 0, 0, 1)$.

The Kummer variety plays two important roles for us. One is an aid related to the projective heights of points of the Jacobian, as the Kummer variety plays the role that the x coordinate plays in heights of points on an elliptic curve. The other is an aid related to the group law on the Jacobian. While the Kummer variety is not itself an abelian variety (or an algebraic group), some elements of the group law on the Jacobian remain, and they are simpler and easier to compute than the group law on the Jacobian, and they are useful in computing the full group law.

8.6 Heights

We defined the Kummer variety by the map

$$(\xi_1, \xi_2, \xi_3, \xi_4) = (X_{14}, X_{13}, X_{12}, X_5).$$

Projectively, we also have

$$(\xi_1^2, \xi_1\xi_2, \xi_1\xi_3, \xi_1\xi_4) = (X_{14}, X_{13}, X_{12}, X_5),$$

and under this normalization, the space of linear forms in the ten even variables on the Jacobian is the same as the space of quadratic forms on the Kummer variety. We have the relations

$$\begin{aligned}
\xi_1\xi_1 &= X_{14} & \xi_2\xi_3 &= X_{11}\\
\xi_1\xi_2 &= X_{13} & \xi_2\xi_4 &= 2X_4 + f_1X_{14} + f_3X_{12} + f_5X_{10}\\
\xi_1\xi_3 &= X_{12} & \xi_3\xi_3 &= X_{10}\\
\xi_1\xi_4 &= X_5 & \xi_3\xi_4 &= X_3\\
\xi_2\xi_2 &= X_{15} + 4X_{12} & \xi_4\xi_4 &= X_0.
\end{aligned}$$

This provides us with the very useful relation between projective heights on the Jacobian and projective heights on the Kummer variety

Lemma 8.2.

$$2\,\mathrm{h}(\xi_1, \xi_2, \xi_3, \xi_4) \leq \mathrm{h}(X_0, X_1, \ldots, X_{15}) + \log 5.$$

Proof. This follows from the above equations and the equality

$$2\,\mathrm{h}(\xi_1, \xi_2, \xi_3, \xi_4) = \mathrm{h}(\xi_1^2, \xi_2^2, \xi_3^2, \xi_4^2).$$

□

Reversing the above equations, we get

$$\begin{aligned}
X_0 &= \xi_4^2 & X_{11} &= \xi_2\xi_3 \\
X_3 &= \xi_3\xi_4 & X_{12} &= \xi_1\xi_3 \\
X_4 &= \frac{1}{2}(\xi_2\xi_4 - f_1\xi_1^2 - f_3\xi_1\xi_3 - f_5\xi_3^2) & X_{13} &= \xi_1\xi_2 \\
X_5 &= \xi_1\xi_4 & X_{14} &= \xi_1^2 \\
X_{10} &= \xi_3^2 & X_{15} &= \xi_2^2 - 4\xi_1\xi_3.
\end{aligned}$$

Unfortunately, since the ξ_i variables are unchanged by negating the point on the Jacobian, we cannot express the six odd variables as polynomials in the ξ_i's. We can, however, write their squares as quadratic polynomials in the ten even variables.

$$\begin{aligned}
X_1^2 = & f_4X_0X_{10} + f_2f_5^2X_{10}^2 + f_3^2f_6X_{10}^2 - 4f_2f_4f_6X_{10}^2 - 4f_1f_5f_6X_{10}^2 + \\
& f_1f_5^2X_{10}X_{11} - 4f_1f_4f_6X_{10}X_{11} + 2f_0f_5^2X_{10}X_{12} - 6f_1f_3f_6X_{10}X_{12} - \\
& 16f_0f_4f_6X_{10}X_{12} + 8f_0f_3f_6X_{11}X_{12} + 16f_0f_2f_6X_{12}^2 - 12f_0f_3f_6X_{10}X_{13} + \\
& 8f_0f_1f_6X_{12}X_{13} + f_0X_0X_{14} - 2f_0f_3f_5X_{10}X_{14} - 3f_1^2f_6X_{10}X_{14} - \\
& 20f_0f_2f_6X_{10}X_{14} - 8f_0f_1f_6X_{11}X_{14} - 2f_0f_1f_5X_{12}X_{14} + \\
& (f_0f_5^2 - 4f_0f_4f_6)X_{10}X_{15} + X_0X_3 + f_3f_5X_{10}X_3 - 4f_2f_6X_{10}X_3 - \\
& 4f_0f_6X_{15}X_3 - 8f_1f_6X_{10}X_4 - 4f_0f_5X_{12}X_4 - f_1f_5X_{10}X_5 - 16f_0f_6X_{10}X_5,
\end{aligned}$$

$$\begin{aligned}
X_2^2 =& f_6X_0X_{10} - 2f_1f_5f_6X_{10}X_{12} + 8f_0f_5f_6X_{11}X_{12} + 16f_0f_4f_6X_{12}^2 - \\
& 8f_0f_5f_6X_{10}X_{13} + 8f_0f_3f_6X_{12}X_{13} + f_2X_0X_{14} - 3f_0f_5^2X_{10}X_{14} - \\
& 2f_1f_3f_6X_{10}X_{14} - 20f_0f_4f_6X_{10}X_{14} - 12f_0f_3f_6X_{11}X_{14} - 6f_0f_3f_5X_{12}X_{14} + \\
& 2f_1^2f_6X_{12}X_{14} - 16f_0f_2f_6X_{12}X_{14} + f_1^2f_5X_{13}X_{14} - 4f_0f_2f_5X_{13}X_{14} + \\
& f_0f_3^2X_{14}^2 + f_1^2f_4X_{14}^2 - 4f_0f_2f_4X_{14}^2 - 4f_0f_1f_5X_{14}^2 + \\
& (f_1^2f_6 - 4f_0f_2f_6)X_{14}X_{15} - 4f_1f_6X_{12}X_4 - 8f_0f_5X_{14}X_4 + X_0X_5 - \\
& f_1f_5X_{12}X_5 - 16f_0f_6X_{12}X_5 + f_1f_3X_{14}X_5 - 4f_0f_4X_{14}X_5 - 4f_0f_6X_{15}X_5, \\
X_6^2 =& f_4X_{10}^2 + f_3X_{10}X_{11} + 4f_2X_{10}X_{12} + 3f_1X_{10}X_{13} + 9f_0X_{10}X_{14} + \\
& f_2X_{10}X_{15} + f_1X_{11}X_{15} + 6f_0X_{12}X_{15} + f_0X_{15}^2 + X_{10}X_3, \\
X_7^2 =& f_6X_{10}^2 + f_2X_{10}X_{14} + f_1X_{11}X_{14} + 4f_0X_{12}X_{14} + f_0X_{14}X_{15} + X_{10}X_5, \\
X_8^2 =& 4f_6X_{10}X_{12} + f_5X_{10}X_{13} + f_4X_{10}X_{14} + f_0X_{14}^2 + f_6X_{10}X_{15} + X_{12}X_5, \\
X_9^2 =& 9f_6X_{10}X_{14} + 3f_5X_{11}X_{14} + 4f_4X_{12}X_{14} + f_3X_{13}X_{14} + f_2X_{14}^2 + \\
& 6f_6X_{12}X_{15} + f_5X_{13}X_{15} + f_4X_{14}X_{15} + f_6X_{15}^2 + X_{14}X_5,
\end{aligned}$$

This allows us to prove a counterpart to the previous lemma.

Lemma 8.3.

$$\mathrm{h}(X_0, X_1, \ldots, X_{15}) \leq 2\,\mathrm{h}(\xi_1, \xi_2, \xi_3, \xi_4) + \frac{3}{2}\,\mathrm{h}(J) + \frac{1}{2}\log 184,$$

where $h(J)$ is defined as

$$\mathrm{h}(J) = \mathrm{h}(1, f_0, f_1, f_2, f_3, f_4, f_5, f_6).$$

Proof. We have

$$2\,\mathrm{h}(X_0, X_1, \ldots, X_{15}) = \mathrm{h}(X_0^2, X_1^2, \ldots, X_{15}^2).$$

Then we can substitute the above formulas for the squares of odd variables as homogeneous quadratic polynomials in the ten even variables. Next, we substitute the formulas for the ten even variables as homogeneous quadratic polynomials in the four ξ_i variables. Then result is sixteen homogeneous polynomials of degree 4 in the ξ_i, of degree at most 3 in the f_i coefficients, with lengths at most 184. □

One useful property of heights (shared with any positive definite quadratic form) is

$$\hat{\mathrm{h}}(P_1 + \ldots + P_n) \le n \left(\hat{\mathrm{h}}(P_1) + \ldots + \hat{\mathrm{h}}(P_n) \right).$$

This is a corollary of the following theorem, since $\hat{\mathrm{h}}$ is a quadratic form and also satisfies $0 \le \hat{\mathrm{h}}(P)$ for all P (i.e. $\hat{\mathrm{h}}$ is a positive definite quadratic form).

Theorem 8.4. *If* $\hat{\mathrm{h}}$ *is any quadratic form, then*

$$\hat{\mathrm{h}}\left(\sum_{j=1}^{n} P_j\right) + \sum_{i=1}^{n} \frac{n}{i(i+1)} \hat{\mathrm{h}}\left(\sum_{j=1}^{i} P_j - iP_i\right) = n \sum_{i=1}^{n} \hat{\mathrm{h}}(P_i).$$

For example, when $n = 2$, $\hat{\mathrm{h}}(P+Q) + \hat{\mathrm{h}}(P-Q) = 2(\hat{\mathrm{h}}(P) + \hat{\mathrm{h}}(Q))$, and when $n = 3$, $\hat{\mathrm{h}}(P+Q+R) + \frac{1}{2}\hat{\mathrm{h}}(P+Q-2R) + \frac{3}{2}\hat{\mathrm{h}}(P-Q) = 3(\hat{\mathrm{h}}(P) + \hat{\mathrm{h}}(Q) + \hat{\mathrm{h}}(R))$.

Proof. To say that $\hat{\mathrm{h}}$ is a quadratic form is to say that the pairing

$$\langle P, Q \rangle = \frac{1}{2} \left[\hat{\mathrm{h}}(P+Q) - \hat{\mathrm{h}}(P) - \hat{\mathrm{h}}(Q) \right]$$

is a bilinear form. Therefore, we have

$$\begin{aligned}\hat{\mathrm{h}}\left(\sum_{j=1}^{n} P_j\right) + \sum_{i=1}^{n} \frac{n}{i(i+1)}\, \hat{\mathrm{h}}\left(\sum_{j=1}^{i} P_j - iP_i\right) \\ &= \left\langle \sum_{j=1}^{n} P_j, \sum_{k=1}^{n} P_k \right\rangle + \sum_{i=1}^{n} \frac{n}{i(i+1)} \left\langle \sum_{j=1}^{i} P_j - iP_i, \sum_{k=1}^{i} P_k - iP_i \right\rangle \\ &= \sum_{j=1}^{n}\sum_{k=1}^{n} a_{j,k} \left\langle P_j, P_k \right\rangle\end{aligned}$$

where for $j = k$ we have

$$a_{k,k} = 1 + \sum_{i=k}^{n} \frac{n}{i(i+1)} - (k-1)^2 \frac{n}{k(k-1)} = n$$

(notice that the middle term is a telescoping series), and for $j < k$,

$$a_{j,k} = 1 + \sum_{i=k}^{n} \frac{n}{i(i+1)} - (k-1) \frac{n}{k(k-1)} = 0.$$

Similarly for $k < j$. □

8.7 Projective Group Law

We already described the group law in terms of divisors at the end of section 8.1, as did Cassels and Flynn in [4]. We also mentioned Cantor's algorithm for adding points in the form of pairs of polynomials in section 8.3, as described in [3]. The article [15] shows that these two are equivalent.

Since the Jacobian is an abelian variety, however, the group law must be expressible as rational functions. Either of the above methods can be implemented generically to get such rational functions, but the degrees become quite large.

Cassels and Flynn show in [4] that the group law can be expressed in biquadratic forms in the following sense. Writing $X_i(P)$ for the i'th projective coordinate of the Jacobian point P, there are 256 biquadratic forms $\Psi_{i,j}(\mathbf{X}(P), \mathbf{X}(Q))$ such that the 16-by-16 matrix

$$(\Psi_{i,j}(\mathbf{X}(P), \mathbf{X}(Q)))_{i,j}$$

is projectively (i.e. up to a scalar multiple) the same as

$$(X_i(P-Q)X_j(P+Q))_{i,j}\,.$$

This gives 16 different group laws, none of which is defined everywhere, since any row is all zeros whenever $X_j(P-Q) = 0$. For every P and Q, however, one of the 16 group laws is defined, since at least one of the coordinates of $X_j(P-Q)$ must be nonzero.

Cassels and Flynn indicated how these polynomials could be computed, but they did not compute them. They did, however, compute sixteen bilinear polynomials $\Phi_{i,j}(\mathbf{X}(P), \mathbf{X}(Q))$ such that the 4-by-4 matrix

$$(\Phi_{i,j}(\mathbf{X}(P), \mathbf{X}(Q)))_{i,j}$$

is projectively the same as

$$(\xi_i(P-Q)\xi_j(P+Q))_{i,j}\,.$$

As we saw, the even projective variables can be written as quadratic polynomials in the ξ_i variables. Therefore, the even-even polynomials $\Psi_{i,j}$ (that is, when X_i and X_j are even variables) are straight-forward to compute using the following method:

First, write $X_i(P-Q)$ and $X_j(P+Q)$ as quadratic polynomials in the variables $\xi_1(P-Q)$ through $\xi_4(P-Q)$ and $\xi_1(P+Q)$ through $\xi_4(P+Q)$, respectively. Multiply the two polynomials together. Then each term is a product of two of the $\xi(P-Q)$ variables and two of the $\xi(P+Q)$ variables. Pairing up one of each in two pairs, replace $\xi_a(P-Q)\xi_b(P-Q)$ with the polynomial $\Phi_{a,b}(\mathbf{X}(P),\mathbf{X}(Q))$. The result is the polynomial $\Psi_{i,j}(\mathbf{X}(P),\mathbf{X}(Q))$.

The even-odd and the odd-odd polynomials are much harder to compute. Cassels and Flynn suggested the following method: First, take the square of $X_i(P-Q)X_j(P+Q)$ and write the square as a biquadratic polynomial in the even variables. Then use the method from the previous paragraph to convert this to a biquartic polynomial in $\mathbf{X}(P)$ and $\mathbf{X}(Q)$. Finally, take the square root.

They gave no suggestions as to how the square root could be computed, and this computation is far from trivial, since the resulting biquartic polynomial is not the square of a polynomial except modulo the ideal of the Jacobian.

One method for computing this square root is this: Express the square as a local series in $X_1(P)$, $X_2(P)$, $X_1(Q)$, and $X_2(Q)$. (It is computationally faster to write the polynomials $\Phi_{i,j}$ as local series, and then compute the square of $\Psi_{i,j}(\mathbf{X}(P),\mathbf{X}(Q))$ directly from these.) Since the local series are expressible in a unique way (unlike quadratic functions on the Jacobian), the resulting local series is the square of a local series. That is, the terms of lowest total degree form the square of a homogeneous polynomial in $X_1(P)$, $X_2(P)$, $X_1(Q)$, and $X_2(Q)$. Take one of the square roots of this polynomial. The sign can be determined later, after the full biquadratic form is recovered, by computing its value at some P and Q and checking the sign. The higher-order terms of the local series are easily determined from the usual formula for the square root of a power series. If the degree-n terms of the square are given by s_n, and the first term of the square root is r_k (of degree k), then for $n > k$, the degree-n terms r_n of the square root are given inductively by

$$(s_{n+k} - \sum_{i=k+1}^{n-1} r_i r_{n+k-i})/(2r_k).$$

At this point, the challenge is to convert the local series of the square root back into a biquadratic form in projective coordinates. This can be done using a variation of the method described in section 8.3. If the lowest-order terms have bi-order (i, j) (that is, order i in $X_1(P)$ and $X_2(P)$, and order j in $X_1(Q)$ and $X_2(Q)$) with $i \leq 8$ and $j \leq 8$, then they can easily be converted back to biquadratic forms since the leading terms of the basis elements given in section 8.3 have one term each. One can then subtract the local series given by the biquadratic forms determined in this way, and the result is a biquadratic form with order (at least) one higher.

When there are terms of lowest order that have bi-order (i, j) with, say, $i \geq 9$, then the biquadratic forms necessary to eliminate these terms is harder to compute, but it can be done using linear algebra. One generates a matrix expressing the coefficients of a basis for biquadratic forms of bi-order (i, j) (modulo those of higher order), augments the matrix with the coefficients sought, and solves. If $j < 9$, this can be done for each power of $X_1(Q)$, so the result is, at worst, a system of 10 equations in 10 variables. When $i \geq 9$ and $j \geq 9$, the system of equations can be as large as 100-by-100.

8.8 Derivatives

The complex points on the Jacobian $J(\mathbb{C})$ form a group isomorphic to $\mathbb{C}^2/\Lambda$ for a particular lattice Λ. The isomorphism

$$P + Q - \infty^+ - \infty^- \to (z_1, z_2) \mod \Lambda$$

is given by

$$z_1 = \int_{\infty^+}^{P} \frac{dx}{y} + \int_{\infty^-}^{Q} \frac{dx}{y} \tag{8.2}$$

$$z_2 = \int_{\infty^+}^{P} \frac{x\,dx}{y} + \int_{\infty^-}^{Q} \frac{x\,dx}{y}. \tag{8.3}$$

Note that

$$\left(2\int_{\infty^-}^{\infty^+} \frac{dx}{y},\, 2\int_{\infty^-}^{\infty^+} \frac{x\,dx}{y}\right) \in \Lambda,$$

so that switching P and Q does not change the image mod Λ.

We would like to take derivatives of functions $J \to \mathbb{C}$ with respect to z_1 and z_2. If we let $P = (a, b)$ and $Q = (c, d)$, then, away from the theta divisor or the curve where $P = Q$, the variables a, b, c, and d are determined locally by z_1 and z_2. We can, therefore, determine their derivatives by inverting the function

$$(a,\, b,\, c,\, d) \to (z_1,\, z_2).$$

From this, we can determine the derivatives of the 16 basis elements for the Jacobian, which will be polynomials in the same basis elements, and then the derivatives on the theta divisor and where $P = Q$ will follow by continuity.

Directly from the definitions of z_1 and z_2, and using the fact that P and Q are independent of one another, we compute

$$\begin{aligned}
\frac{\partial z_1}{\partial a} &= \frac{\partial}{\partial a}\int_{\infty^+}^{(a,b)} \frac{dx}{y} = \frac{1}{b} \\
\frac{\partial z_1}{\partial b} &= \frac{\partial}{\partial b}\int_{\infty^+}^{(a,b)} \frac{2\,dy}{f'(x)} = \frac{2}{f'(a)} \\
\frac{\partial z_1}{\partial c} &= \frac{\partial}{\partial c}\int_{\infty^+}^{(c,d)} \frac{dx}{y} = \frac{1}{d} \\
\frac{\partial z_1}{\partial d} &= \frac{\partial}{\partial d}\int_{\infty^+}^{(c,d)} \frac{2\,dy}{f'(x)} = \frac{2}{f'(c)} \\
\frac{\partial z_2}{\partial a} &= \frac{\partial}{\partial a}\int_{\infty^+}^{(a,b)} \frac{x\,dx}{y} = \frac{a}{b} \\
\frac{\partial z_2}{\partial b} &= \frac{\partial}{\partial b}\int_{\infty^+}^{(a,b)} \frac{2x\,dy}{f'(x)} = \frac{2a}{f'(a)} \\
\frac{\partial z_2}{\partial c} &= \frac{\partial}{\partial c}\int_{\infty^+}^{(c,d)} \frac{x\,dx}{y} = \frac{c}{d} \\
\frac{\partial z_2}{\partial d} &= \frac{\partial}{\partial d}\int_{\infty^+}^{(c,d)} \frac{2x\,dy}{f'(x)} = \frac{2c}{f'(c)}.
\end{aligned}$$

Considering a and b as functions of z_1 and z_2, and z_1 and z_2 as functions of a, b, c, and d, we get

$$\begin{aligned}
1 = \frac{\partial a}{\partial a} &= \frac{\partial a}{\partial z_1}\frac{\partial z_1}{\partial a} + \frac{\partial a}{\partial z_2}\frac{\partial z_2}{\partial a} \\
0 = \frac{\partial a}{\partial c} &= \frac{\partial a}{\partial z_1}\frac{\partial z_1}{\partial c} + \frac{\partial a}{\partial z_2}\frac{\partial z_2}{\partial c} \\
1 = \frac{\partial b}{\partial b} &= \frac{\partial b}{\partial z_1}\frac{\partial z_1}{\partial b} + \frac{\partial b}{\partial z_2}\frac{\partial z_2}{\partial b} \\
0 = \frac{\partial b}{\partial d} &= \frac{\partial b}{\partial z_1}\frac{\partial z_1}{\partial d} + \frac{\partial b}{\partial z_2}\frac{\partial z_2}{\partial d}.
\end{aligned}$$

Substituting the above formulas and solving, we compute

$$\begin{aligned}
\frac{\partial a}{\partial z_1} &= \frac{-bc}{a-c} & \frac{\partial a}{\partial z_2} &= \frac{b}{a-c}\\
\frac{\partial b}{\partial z_1} &= \frac{-cf'(a)}{2(a-c)} & \frac{\partial b}{\partial z_2} &= \frac{f'(a)}{2(a-c)}\\
\frac{\partial c}{\partial z_1} &= \frac{ad}{a-c} & \frac{\partial c}{\partial z_2} &= \frac{-d}{a-c}\\
\frac{\partial d}{\partial z_1} &= \frac{af'(c)}{2(a-c)} & \frac{\partial d}{\partial z_2} &= \frac{-f'(c)}{2(a-c)}.
\end{aligned}$$

Normalizing to $X_{14} = 1$, we can compute, for example,

$$\frac{\partial}{\partial z_1} X_{13} = \frac{\partial}{\partial z_1}(a+c) = \frac{\partial a}{\partial z_1} + \frac{\partial c}{\partial z_1} = \frac{-bc}{a-c} + \frac{ad}{a-c} = \frac{ad-bc}{a-c} = -X_8.$$

The derivatives of a few of the basis elements with respect to z_1 are

$$\begin{aligned}
\frac{\partial}{\partial z_1} X_8 &= (-4f_6X_{10}X_{13} - 3f_5X_{10}X_{14} - f_1X_{14}^2 - 2X_{14}X_4)/2\\
\frac{\partial}{\partial z_1} X_9 &= (-14f_6X_{10}X_{14} - 3f_5X_{11}X_{14} - 2f_4X_{12}X_{14} - 4f_6X_{12}X_{15} - X_{14}X_5)/2\\
\frac{\partial}{\partial z_1} X_{10} &= -2X_{12}X_7\\
\frac{\partial}{\partial z_1} X_{11} &= -X_{14}X_6 - 2X_{12}X_8\\
\frac{\partial}{\partial z_1} X_{12} &= -X_{14}X_7\\
\frac{\partial}{\partial z_1} X_{13} &= -X_{14}X_8\\
\frac{\partial}{\partial z_1} X_{14} &= 0\\
\frac{\partial}{\partial z_1} X_{15} &= 2X_{14}X_7 - 2X_{12}X_9.
\end{aligned}$$

Without the normalization of $X_{14} = 1$, these may be written

$$\begin{aligned}
\frac{\partial}{\partial z_1}\frac{X_8}{X_{14}} =&(-4f_6X_{10}X_{13} - 3f_5X_{10}X_{14} - f_1X_{14}^2 - 2X_{14}X_4)/2X_{14}^2\\
\frac{\partial}{\partial z_1}\frac{X_9}{X_{14}} =&(-14f_6X_{10}X_{14} - 3f_5X_{11}X_{14} - 2f_4X_{12}X_{14} - 4f_6X_{12}X_{15} - X_{14}X_5)/2X_{14}^2\\
\frac{\partial}{\partial z_1}\frac{X_{10}}{X_{14}} =& - 2X_{12}X_7/X_{14}^2\\
\frac{\partial}{\partial z_1}\frac{X_{11}}{X_{14}} =&(-X_{14}X_6 - 2X_{12}X_8)/X_{14}^2\\
\frac{\partial}{\partial z_1}\frac{X_{12}}{X_{14}} =& - X_7/X_{14}\\
\frac{\partial}{\partial z_1}\frac{X_{13}}{X_{14}} =& - X_8/X_{14}\\
\frac{\partial}{\partial z_1}\frac{X_{14}}{X_{14}} =&0\\
\frac{\partial}{\partial z_1}\frac{X_{15}}{X_{14}} =&(2X_{14}X_7 - 2X_{12}X_9)/X_{14}^2.
\end{aligned}$$

The derivatives of a few of the basis elements with respect to z_2 are

$$\begin{aligned}
\frac{\partial}{\partial z_2}\frac{X_8}{X_{14}} =&(14f_6X_{10}X_{14} + 3f_5X_{11}X_{14} + 2f_4X_{12}X_{14} + 4f_6X_{12}X_{15} + X_{14}X_5)/2X_{14}^2\\
\frac{\partial}{\partial z_2}\frac{X_9}{X_{14}} =&(10f_6X_{11}X_{14} + 10f_5X_{12}X_{14} + 2f_4X_{13}X_{14}+\\
&f_3X_{14}^2 + 4f_6X_{13}X_{15} + 3f_5X_{14}X_{15})/2X_{14}^2\\
\frac{\partial}{\partial z_2}\frac{X_{10}}{X_{14}} =&2X_{12}X_8/X_{14}^2\\
\frac{\partial}{\partial z_2}\frac{X_{11}}{X_{14}} =&(X_{14}X_7 + 2X_{12}X_9)/X_{14}^2\\
\frac{\partial}{\partial z_2}\frac{X_{12}}{X_{14}} =&X_8/X_{14}\\
\frac{\partial}{\partial z_2}\frac{X_{13}}{X_{14}} =&X_9/X_{14}\\
\frac{\partial}{\partial z_2}\frac{X_{15}}{X_{14}} =&(-4X_{14}X_8 + 2X_{13}X_9)/X_{14}^2
\end{aligned}$$

Chapter 9

Application to Diophantine equations

9.1 The General Method

The lower bound for a linear form in logarithms on algebraic groups may be applied to solving certain Diophantine equations. By way of example, suppose that x and y are integers, and the point (x, y) belongs to a particular curve of genus two,

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

with $f_i \in \mathbb{Q}$. Either x (and therefore y) is relatively small, or the point (x, y) is near a point at infinity. In the first case, we can simply try all such x values. In the second, we use the following method:

First we choose an embedding of the curve into its Jacobian

$$\iota : C \to J.$$

If Q is a rational point on the curve, then we can take $\iota(x, y) = (x, y) + Q - \infty^+ - \infty^-$. (For example, in the case $f_6 = 0$, where $\infty = \infty^+ = \infty^-$, taking $Q = \infty$ is the same as using the embedding $\iota(x, y) = (x, y) - \infty$.) When no rational point is known, or it is more desirable not to distinguish any particular rational point (particularly when the points at infinity are not rational), we can still use the embedding $\iota(x, y) = 2(x, y) - \infty^+ - \infty^-$, although this generally doesn't give as favorable inequalities. We let P denote the image in the Jacobian of our point (x, y), $P = \iota(x, y)$.

Next we find a Mordell-Weil basis $P_1, \ldots, P_r$ for the rational points on the Jacobian. Then we know that

$$P = n_1 P_1 + n_2 P_2 + ... + n_r P_r + T$$

for some integers n_i and a torsion point T of the Jacobian. Furthermore, by finding the rational torsion subgroup of the Jacobian, we can get a small positive integer t such that

$$tT = 0$$

for all rational torsion points T. Now if we write

$$N = \max_{1 \leq i \leq r} |n_i|,$$

then we only need to find an upper bound N_0 for N, and then we can try all combinations

$$P = n_1 P_1 + n_2 P_2 + ... + n_r P_r + T$$

with $|n_i| < N_0$.

Let

$$\phi : J \to \mathbb{C}^2$$

be an inverse of the exponential map, so that reducing the image mod the lattice of periods Λ gives an isomorphism

$$\tilde{\phi} : J \to \mathbb{C}^2/\Lambda.$$

By equations 8.2

$$\phi((a,b) + (c,d) - \infty^+ - \infty^-) = \left(\int_{\infty^+}^{(a,b)} \frac{dx}{y} + \int_{\infty^-}^{(c,d)} \frac{dx}{y}, \int_{\infty^+}^{(a,b)} \frac{x\,dx}{y} + \int_{\infty^-}^{(c,d)} \frac{x\,dx}{y} \right).$$

Then we have

$$\phi(P) = n_1\phi(P_1) + n_2\phi(P_2) + ... + n_r\phi(P_r) + \phi(T) \mod \Lambda,$$

and since $t\phi(T) = \phi(tT) \in \Lambda$, we can write this as

$$\phi(P) = n_1\phi(P_1) + n_2\phi(P_2) + ... + n_r\phi(P_r).$$

If P is near, but not equal to, a point at infinity, then $\phi(P)$ will be near, but not equal to, $\phi(\infty^{\pm})$. The lower bound we have proven gives a condition on the m_i's which ultimately bounds them to a finite set.

More precisely, we will find positive constants c_i which verify the following inequalities:

$$\begin{aligned} c_2 N^2 &\leq \hat{\mathrm{h}}(P) \\ \hat{\mathrm{h}}(P) &\leq \mathrm{h}(P) + \log c_3 \\ \mathrm{h}(P) &\leq c_4 \log|x| + \log c_5 \\ c_6 \log|x| &\leq \log c_7 - \log\left|\phi(P) - \phi(\iota(\infty^{\pm}))\right|, \end{aligned}$$

which we can put together to get

$$N^2 \leq c_8 - c_9 \log\left|\phi(P) - \phi(\iota(\infty^{\pm}))\right|.$$

Then our lower bound will give us something of the form

$$\log\left|\phi(P) - \phi(\iota(\infty^{\pm}))\right| > c_{10}(\log N)^k,$$

and our upper bound for N will result from combining these inequalities

$$N^2 \leq c_8 - c_9 c_{10}(\log N)^k.$$

9.2 Proving the Inequalities

Lemma 9.1. *The canonical height on the Jacobian of our genus 2 curve satisfies*

$$\hat{\mathrm{h}}(P) \geq \lambda N^2$$

where λ is the smallest eigenvalue of the height matrix

$$\mathcal{H} = \left(\frac{1}{2}\langle P_i,\, P_j\rangle\right)_{r\times r}$$

and

$$\langle P,\, Q\rangle = \hat{\mathrm{h}}(P+Q) - \hat{\mathrm{h}}(P) - \hat{\mathrm{h}}(Q)$$

is the so-called Néron-Tate pairing.

Proof. Since

$$P = \sum_{i=1}^{r} n_i P_i + T,$$

we have

$$\hat{\mathrm{h}}(P) = \frac{1}{2}\sum_{i\leq i,j\leq r} \langle P_i,\, P_j\rangle\, n_i n_j$$

and therefore

$$\hat{\mathrm{h}}(P) = \mathbf{n}^T \mathcal{H} \mathbf{n}$$

where $\mathbf{n}$ is the column vector with components n_1, ..., n_r. Then since $\mathcal{H}$ is symmetric, if D is the diagonal matrix of eigenvalues of $\mathcal{H}$ then there is an orthogonal matrix $\mathcal{Q}$ such that

$$\mathcal{H} = \mathcal{Q}^T D \mathcal{Q}.$$

Now let $\mathbf{m} = \mathcal{Q}\mathbf{n}$, and then we have

$$\begin{aligned}\hat{\mathrm{h}}(P) = \mathbf{n}^T\mathcal{H}\mathbf{n} = \mathbf{n}^T\mathcal{Q}^T D\mathcal{Q}\mathbf{n} = \mathbf{m}^T D\mathbf{m} = \sum_{i=1}^{r} \lambda_i m_i^2 \\ \geq \lambda \sum_{i=1}^{r} m_i^2 = \lambda\mathbf{m}^T\mathbf{m} = \lambda\mathbf{n}^T\mathcal{Q}^T\mathcal{Q}\mathbf{n} = \lambda\mathbf{n}^T\mathbf{n} \\ = \lambda \sum_{i=1}^{r} n_i^2 \geq \lambda \max_{1\leq i\leq r} n_i^2 = \lambda N^2.\end{aligned}$$

□

Next to the rank r, which we have no control over, this constant λ is the most significant constant in our computations. In the article [35], the authors describe an algorithm by which a Mordell-Weil basis may be modified (if $r > 1$) to maximize λ.

Recall that we defined

$$\mathrm{h}(J) = \mathrm{h}(1, f_0, f_1, f_2, f_3, f_4, f_5, f_6).$$

Lemma 9.2. *The naïve height satisfies*

$$\hat{\mathrm{h}}(P) \leq \mathrm{h}(P) + \frac{4}{3}\mathrm{h}(J) + \frac{1}{3}\log 2744.$$

Proof. Theorem 3.4.1 of [4] gives biquadratic polynomials $B_{i,j}$ in ξ_i corresponding to a point A and ξ_i corresponding to a point B such that, projectively,

$$(\xi_i(A+B)\xi_j(A-B) + \xi_i(A-B)\xi_j(A+B)) = (2B_{i,j}(A,B)).$$

Taking $A = B$, we get a formula for the ξ_i corresponding to the point $2A$, namely

$$(2B_{4,1}(A,A), 2B_{4,2}(A,A), 2B_{4,3}(A,A), B_{4,4}(A,A)).$$

The result is four polynomials, homogeneous of degree 4 in the ξ_i (corresponding to the point A), of degree at most 4 in the f_i coefficients, and of lengths at most 2744.

Therefore, we conclude that

$$\mathrm{h}(2P) \leq 4\,\mathrm{h}(P) + 4\,\mathrm{h}(J) + \log 2744.$$

By induction,

$$\mathrm{h}(2^n P) \leq 4^n\,\mathrm{h}(P) + 4\left(\frac{4^n - 1}{4 - 1}\right)\mathrm{h}(J) + \left(\frac{4^n - 1}{4 - 1}\right)\log 2744.$$

So we conclude that

$$\hat{\mathrm{h}}(P) = \lim_{n\to\infty} \frac{\mathrm{h}(2^n P)}{4^n} \leq \mathrm{h}(P) + \frac{4}{3}\,\mathrm{h}(J) + \frac{1}{3}\log 2744.$$

□

Lemma 9.3. *When $P = 2(x, y) - \infty^+ - \infty^-$, its naïve height satisfies*

$$\mathrm{h}(P) \leq 8\,\mathrm{h}(x) + 2\,\mathrm{h}(J) + \log 181.$$

Proof.

$$\begin{aligned}
&\mathrm{h}(\xi_1, \xi_2, \xi_3, \xi_4) = \mathrm{h}(X_{14}, X_{13}, X_{12}, X_5)\\
&=\mathrm{h}\left(1, 2x, x^2, \left(\frac{f'(x)}{2y}\right)^2 - (f_2 + 2xf_3 + 4x^2 f_4 + 6x^3 f_5 + 9x^4 f_6)\right)\\
&=\mathrm{h}(4f(x), 8xf(x), 4x^2 f(x), f'(x)^2 - 4f(x)(f_2 + 2xf_3 + 4x^2 f_4 + 6x^3 f_5 + 9x^4 f_6))
\end{aligned}$$

where each of those four expressions are polynomials in x of degree at most 8, in the f_i of degree at most 2, and the sums of the absolute values of the coefficients in the four polynomials are, respectively, 28, 56, 28, and 181. □

Notice that when x is an integer, $\mathrm{h}(x) = \log |x|$, so this provides the necessary inequality. This bound may be tightened in various ways. One way is to substitute the values for the f_i's into the formula

$$\mathrm{h}(4f(x), 8xf(x), 4x^2f(x), f'(x)^2 - 4f(x)(f_2 + 2xf_3 + 4x^2f_4 + 6x^3f_5 + 9x^4f_6)),$$

then clear denominators, eliminate any common factors, and replace

$$2\,\mathrm{h}(J) + \log 181$$

by the logarithm of the sum of the absolute values of the coefficients of the four polynomials.

Additionally, if x is assumed to be an integer of absolute value at least M for some number M, and any denominators in the f_i's have been cleared, then the height is the logarithm of the max of the four polynomials in x, and terms of degree less than 8 can be reduced by

$$|x|^i \leq |x|^8 / M^{8-i},$$

thereby reducing the upper bound (in the case where $f_i \in \mathbb{Z}$ to something slightly larger than $8 \log |x| + \log \max\{4f_6, f_5^2 - 4f_4f_6\}$.

Alternately, if there is a rational point on the curve, then one can get better results by using a different embedding. For example, if $f_6 = s^2$ is a square (such as zero), then we have:

Lemma 9.4. *When $P = (x, y) - \infty^-$, its naïve height satisfies*

$$\mathrm{h}(P) \leq 3\,\mathrm{h}(x) + \frac{3}{2}\,\mathrm{h}(J) + \frac{1}{2}\log 175.$$

If $f_6 = 0$, then we have the tighter bound

$$\mathrm{h}(P) \leq 2\,\mathrm{h}(x) + \mathrm{h}(f_5).$$

Proof.

$$\begin{aligned} \mathrm{h}(\xi_1,\xi_2,\xi_3,\xi_4) =& \mathrm{h}(0,1,x,2f_6x^3+f_5x^2-2sy) \\ \leq& \mathrm{h}(1,f_5,f_6)+\mathrm{h}(1,x,x^2,x^3,y)+\log 5, \end{aligned}$$

since $s^2 = f_6$, and we can bound the height of y as follows.

$$\begin{aligned} \mathrm{h}(1,x,x^2,x^3,y) =& \frac{1}{2}\,\mathrm{h}(1,x^2,x^4,x^6,f(x)) \\ \leq& \frac{1}{2}\left(\mathrm{h}(J)+6\,\mathrm{h}(x)+\log 7\right), \end{aligned}$$

and the result follows. When $f_6 = 0$, we also have $s = 0$ and

$$\begin{aligned} \mathrm{h}(\xi_1,\xi_2,\xi_3,\xi_4) =& \mathrm{h}(0,1,x,f_5x^2) \\ \leq& \mathrm{h}(f_5)+2\,\mathrm{h}(x). \end{aligned}$$

$$\mathrm{h}(\xi_1,\xi_2,\xi_3,\xi_4) = \mathrm{h}(0,1,x,f_5x^2) \leq \mathrm{h}(f_5)+2\,\mathrm{h}(x).$$

□

If we have a rational point (a,b) on the curve (not a point at infinity), then we can also use the embedding $(x,y) \to (x,y)+(a,b)-\infty^+-\infty^-$ and we have the following.

Lemma 9.5. *When $P = (x,y)+(a,b)-\infty^+-\infty^-$, its naïve height satisfies*

$$\mathrm{h}(P) \leq 3\,\mathrm{h}(x)+\frac{3}{2}\,\mathrm{h}(J)+\mathrm{h}(1,a^3,b)+4\log 2+\frac{1}{2}\log 7.$$

Proof.

$$\begin{aligned}
\mathrm{h}(\xi_1,\xi_2,\xi_3,\xi_4) &= \mathrm{h}(1,a+x,ax,(F_0(a,x)-2by)/(a-x)^2) \\
&= \mathrm{h}((a-x)^2,(a+x)(a-x)^2,ax(a-x)^2,F_0(a,x)-2by) \\
&\leq \mathrm{h}(J)+\mathrm{h}(1,a,a^2,a^3,b)+\mathrm{h}(1,x,x^2,x^3,y)+\log 16,
\end{aligned}$$

and we have already seen that

$$\mathrm{h}(1,x,x^2,x^3,y) \leq \frac{1}{2}\left(\mathrm{h}(J)+6\,\mathrm{h}(x)+\log 7\right).$$

□

Regarding the constants c_6 and c_7, we have the following two lemmas.

Lemma 9.6. *If $f_6 > 0$ and $|x|$ is bigger than two times the max of the absolute values of the six roots of $f(x)$, then*

$$\mathbf{z} = \phi(P) - \phi(\iota(\infty^{\pm})) \in \mathbb{C}^2$$

(where the sign of $\infty^{\pm}$ is the same as that of y/x^3) has

$$\begin{aligned}
2\log|x| &\leq \frac{1}{2}\log f_6 - 4\log 2 - \log|z_1| \\
\log|x| &\leq \frac{1}{2}\log f_6 - 3\log 2 - \log|z_2|
\end{aligned}$$

in the case where $\iota(x,y) = (x,y) + Q - \infty^+ - \infty^-$ and

$$\begin{aligned}
2\log|x| &\leq \frac{1}{2}\log f_6 - 3\log 2 - \log|z_1| \\
\log|x| &\leq \frac{1}{2}\log f_6 - 2\log 2 - \log|z_2|
\end{aligned}$$

in the case where $\iota(x,y) = 2(x,y) - \infty^+ - \infty^-$.

Proof. Suppose that $x > 0$. In the case where $\iota(x,y) = (x,y) + Q - \infty^+ - \infty^-$,

$$\begin{aligned}|z_1| &= \int_x^\infty \frac{dt}{\sqrt{f(t)}}\\ |z_2| &= \int_x^\infty \frac{t\,dt}{\sqrt{f(t)}}.\end{aligned}$$

In the case where $\iota(x,y) = 2(x,y) - \infty^+ - \infty^-$,

$$\begin{aligned}|z_1| =&2\int_x^\infty \frac{dt}{\sqrt{f(t)}}\\ |z_2| =&2\int_x^\infty \frac{t\,dt}{\sqrt{f(t)}}.\end{aligned}$$

Write

$$f(t) = f_6(t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4)(t-\alpha_5)(t-\alpha_6).$$

Then for $t \geq x$, we have

$$f(t) = f_6\,|t-\alpha_1|\,|t-\alpha_2|\,|t-\alpha_3|\,|t-\alpha_4|\,|t-\alpha_5|\,|t-\alpha_6| \geq f_6(t/2)^6,$$

and therefore (for $i = 0$ or $i = 1$)

$$\int_x^\infty \frac{t^i\,dt}{\sqrt{f(t)}} \leq \int_x^\infty 2^{-3} f_6^{1/2} t^{i-3} dt = \frac{\sqrt{f_6}}{8(2-i)} x^{i-2}.$$

When $x < 0$, we have the same result up to differences in sign, which does not affect the final result. □

Lemma 9.7. *If $f_6 = 0$, $f_5 > 0$, and x is bigger than two times the max of the absolute values of the five roots of $f(x)$, then*

$$\mathbf{z} = \phi(P) - \phi(\iota(\infty)) \in \mathbb{C}^2$$

has

$$\begin{aligned}\frac{3}{2}\log|x| \leq& \frac{1}{2}\log f_6 - \frac{3}{2}\log 2 - \log 5 - \log|z_1|\\ \frac{1}{2}\log|x| \leq& \frac{1}{2}\log f_6 - \frac{3}{2}\log 2 - \log 3 - \log|z_2|\end{aligned}$$

in the case where $\iota(x,y) = (x,y) + Q - 2\infty$ *and*

$$\begin{aligned}\frac{3}{2}\log|x| \leq& \frac{1}{2}\log f_6 - \frac{1}{2}\log 2 - \log 5 - \log|z_1|\\ \frac{1}{2}\log|x| \leq& \frac{1}{2}\log f_6 - \frac{1}{2}\log 2 - \log 3 - \log|z_2|\end{aligned}$$

in the case where $\iota(x,y) = 2(x,y) - 2\infty$*. We have the same result if* $f_6 = 0$*,* $f_5 < 0$*, and* $-x$ *is bigger than two times the max of the absolute values of the five roots of* $f(x)$*.*

Proof. Suppose that $f_5 > 0$. (The other case is the same except for a few differences in sign.) In the case where $\iota(x,y) = (x,y) + Q - 2\infty$,

$$\begin{aligned}z_1 =& -\int_x^\infty \frac{dt}{\sqrt{f(t)}}\\ z_2 =& -\int_x^\infty \frac{t\,dt}{\sqrt{f(t)}}.\end{aligned}$$

In the case where $\iota(x,y) = 2(x,y) - 2\infty$,

$$\begin{aligned}z_1 =& -2\int_x^\infty \frac{dt}{\sqrt{f(t)}}\\ z_2 =& -2\int_x^\infty \frac{t\,dt}{\sqrt{f(t)}}.\end{aligned}$$

As before, write

$$f(t) = f_5(t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4)(t-\alpha_5).$$

Then for $t \geq x$, we have

$$f(t) = f_5\,|t-\alpha_1|\,|t-\alpha_2|\,|t-\alpha_3|\,|t-\alpha_4|\,|t-\alpha_5| \geq f_5(t/2)^5,$$

and therefore (for $i = 0$ or $i = 1$)

$$\int_x^\infty \frac{t^i\,dt}{\sqrt{f(t)}} \leq \int_x^\infty 2^{-5/2} f_5^{1/2} t^{i-5/2} dt = \frac{\sqrt{2f_5}}{4(5-2i)} x^{i-3/2}.$$

□

Finally, we need to apply Theorem 1.6 to get a lower bound on the linear form $\phi(P)$, so we need to compute the parameters used in that theorem.

We are using the basis $\{dx/y,\, x\,dx/y\}$ for the space of one-forms on C (elsewhere denoted $H^0(C, \Omega_1)$, but we will have a different meaning for Ω_1). Let $(\Omega_1,\, \Omega_2)$ be the period matrix for this basis with respect to some symplectic basis of $H_1(C, \mathbb{Z})$. Then $\Omega = \Omega_1^{-1}\Omega_2 \in \mathbb{H}_2$, and the analytic Jacobian is given by

$$J(\mathbb{C}) \cong \mathbb{C}^2/(\Omega_1\mathbb{Z}^2 + \Omega_2\mathbb{Z}^2),$$

which is precisely the tangent space $T_J(\mathbb{C})$ mod the kernel of the exponential map. The analytic Jacobian is isomorphic (via the isomorphism $\mathbf{z} \to \Omega_1^{-1}\mathbf{z}$) to

$$J(\mathbb{C}) \cong \mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2).$$

In order to compute H^- and H^+, we need to relate Φ_j to the theta functions on J. By the comment at the end of section 8.2, the projective coordinates $X_0, \ldots, X_{15}$ generate the same line bundle as the 16 theta functions

$$\vartheta[\eta](\mathbf{z}, \Omega),$$

for all 2-by-2 matrices η with entries that are either 0 or 1/2. If we let $\eta_0, \ldots, \eta_{15}$ be an enumeration of such matrices, then we can find an invertible matrix A such that

$$\begin{bmatrix} \Phi_0(\mathbf{z}) \\ \vdots \\ \Phi_{15}(\mathbf{z}) \end{bmatrix} = A \begin{bmatrix} \vartheta[\eta_0](\mathbf{z}, \Omega) \\ \vdots \\ \vartheta[\eta_{15}](\mathbf{z}, \Omega) \end{bmatrix}. \tag{9.1}$$

Since this determines A only up to a scalar multiple, we can choose the scalar by assuming that $\Phi_0(0) = 1$.

One way to compute A is the following: Choose (at least) 17 points on the Jacobian. Compute the projective coordinates $(X_0, \ldots, X_{15})$ for each point, as well as the analytic coordinates $\mathbf{z} = (z_1, z_2)$. Evaluate the 16 theta functions $\vartheta[\eta_j](\mathbf{z}, \Omega)$ at each point. Each point gives 15 linear equations in the entries of A by substituting the rows from the right side of 9.1 into the equation

$$\Phi_0 X_j = X_0 \Phi_j.$$

This system of equations, together with $\Phi_0(0) = 1$, can be solved for A.

The number $\hbar$ can be computed using the method of [31].

One lower bound H^- for

$$\max\{|\Phi_0(\mathbf{z})|, \ldots, |\Phi_{15}(\mathbf{z})|\}$$

is given by a lower bound for

$$\max\{|\vartheta[\eta_0](\mathbf{z}, \Omega)|, \ldots, |\vartheta[\eta_{15}](\mathbf{z}, \Omega)|\}$$

divided by the max (over the rows) of the sum of the absolute values of the entries in a row of A^{-1}. An upper bound H^+ for

$$\max\{|\Phi_0(\mathbf{z})|, \ldots, |\Phi_{15}(\mathbf{z})|\}$$

is given by an upper bound for

$$\max\{|\vartheta[\eta_0](\mathbf{z},\Omega)|\,,\dots,|\vartheta[\eta_{15}](\mathbf{z},\Omega)|\}$$

multiplied by the max (over the rows) of the sum of the absolute values of the entries in a row of A. An upper bound for

$$|\vartheta[\eta](\mathbf{z},\Omega)|$$

can be determined as follows. Since $\operatorname{Im}\Omega$ is symmetric positive definite, $\operatorname{Im}\Omega = Q^T DQ$ with Q orthogonal ($Q^T Q = I$) and D the diagonal matrix of (positive) eigenvectors (say $\geq \lambda$). So if $\mathbf{s} = Q\mathbf{n}$ then

$$\begin{aligned}\mathbf{n}^T(\operatorname{Im}\Omega)\mathbf{n} &= \mathbf{n}^T Q^T DQ\mathbf{n} = \mathbf{s}^T D\mathbf{s} = \lambda_1 s_1^2 + \lambda_2 s_2^2\\ &\geq \lambda(s_1^2+s_2^2) = \lambda\mathbf{s}^T\mathbf{s} = \lambda\mathbf{n}^T Q^T Q\mathbf{n} = \mathbf{n}^T\mathbf{n}.\end{aligned}$$

Furthermore, if $a > 0$, and $[b]$ denotes the fractional part of b in the range $[-1/2, 1/2]$, then

$$\begin{aligned}\sum_{n\in\mathbb{Z}}\exp(-a(n+b)^2) &< \exp(-a[b]^2) + \int_{-\infty}^{+\infty}\exp(-a(x+b)^2)\,dx\\ &\leq \exp(-a/4) + \sqrt{\pi/a}\end{aligned}$$

Therefore,

$$\begin{aligned}
|\vartheta(\mathbf{z},\Omega)| &= \left|\sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(\pi i \mathbf{n}^T\Omega\mathbf{n} + 2\pi i \mathbf{n}^T\mathbf{z})\right| \\
&\le \sum_{\mathbf{n}\in\mathbb{Z}^2} \left|\exp(\pi i \mathbf{n}^T\Omega\mathbf{n} + 2\pi i \mathbf{n}^T\mathbf{z})\right| \\
&= \sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(\operatorname{Re}(\pi i \mathbf{n}^T\Omega\mathbf{n} + 2\pi i \mathbf{n}^T\mathbf{z})) \\
&= \sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(-\pi \mathbf{n}^T(\operatorname{Im}\Omega)\mathbf{n} - 2\pi \mathbf{n}^T\operatorname{Im}\mathbf{z})) \\
&\le \sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(-\pi\lambda \mathbf{n}^T\mathbf{n} - 2\pi \mathbf{n}^T\operatorname{Im}\mathbf{z})) \\
&= \sum_{\mathbf{n}\in\mathbb{Z}^2} \prod_{i=1}^{2} \exp(-\pi\lambda n_i^2 - 2\pi n_i \operatorname{Im} z_i)) \\
&= \prod_{i=1}^{2} \sum_{n\in\mathbb{Z}} \exp(-\pi\lambda n^2 - 2\pi n \operatorname{Im} z_i)) \\
&= \prod_{i=1}^{2} \sum_{n\in\mathbb{Z}} \exp(-\pi\lambda (n + \frac{\operatorname{Im} z_i}{\lambda})^2 + \frac{\pi}{\lambda}(\operatorname{Im} z_i)^2) \\
&< \prod_{i=1}^{2} \left(\exp(-\pi\lambda/4) + \sqrt{1/\lambda}\right) \exp(\frac{\pi}{\lambda}(\operatorname{Im} z_i)^2) \\
&\le \left(\exp(-\pi\lambda/4) + \sqrt{1/\lambda}\right)^2 \exp(\frac{\pi}{\lambda}|\mathbf{z}|^2)
\end{aligned}$$

Consequently, we can take $A^+ = \pi/\lambda$, $B^+ = 0$, and C^+ given by the matrix A described above, plus the number

$$2\log\left(\exp(-\pi\lambda/4) + \sqrt{1/\lambda}\right).$$

Next, one takes $\mathbf{u}_i = \phi(P_i)$ for $1 \le i \le r$, and $\mathbf{u}_{r+1} = \phi(\infty^\pm)$. Then $k = r+1$, $\gamma_i = P_i$ for $i \le r$, and $\gamma_{r+1} = \infty^\pm$. Set $K = \mathbb{Q}$ (so $D = 1$), and $G_i = J$ for $1 \le i \le k$, so $\mathbb{G} = \mathbb{G}_a \times J^k$. Then we will have two different linear forms. For the first, set

$(\beta_0, \ldots, \beta_{2k}) = (n_1, 0, n_2, 0, \ldots, n_r, 0, -1, 0)$ so that

$$\mathcal{L}_1(\mathbf{u}) = n_1 u_{1,1} + 0u_{1,2} + \ldots + n_r u_{r,1} + 0u_{r,2} - u_{r+1,1} + 0u_{r+1,2}.$$

For the second, set $(\beta_0, \ldots, \beta_{2k}) = (0, n_1, 0, n_2, \ldots, 0, n_r, 0, -1)$ so that

$$\mathcal{L}_2(\mathbf{u}) = 0u_{1,1} + n_1 u_{1,2} + \ldots + 0u_{r,1} + n_r u_{r,2} + 0u_{r+1,1} - u_{r+1,2}.$$

These are precisely the two coordinates of $\phi(P) - \phi(\iota(\infty^{\pm}))$. Both are nonzero, since they are given by the integrals in 9.6 and 9.7. We can use either one to get our upper bound on N.

Set $E = e$ and

$$V_i = \exp\max\{\hat{\mathrm{h}}(\gamma_i),\ A^{+}\left|\mathbf{u}_i\right|^2 e^2\}.$$

Now, either $B = N$ is smaller than

$$\exp\max\{e,\ \log V_i,\ \exp(\mathrm{h}(J)),\ \exp(\hbar/((2k+1)!2^{4k}))\},$$

which gives an upper bound on N, or

$$\log|\mathcal{L}_i(\mathbf{u})| > -C_1(\log B)(\log\log B)^{2k+1}\prod_{i=1}^{k}(\log V_i)^2,$$

for at least one of the two linear forms (whichever is nonzero), where C_1 is given in Section 1.3.

Combining this inequality with the ones determined previously, we get an upper bound for N.

9.3 Lattice Reduction

We currently have constants K_1, K_2, and N_0 such that

$$|\phi(P)| < K_1\exp(-K_2 N^2)$$

and

$$N < N_0.$$

Consider the $(r+1)$-dimensional lattice generated by the columns of the matrix

$$\mathcal{A} = \begin{bmatrix} 1 & ... & 0 & 0 \\ 0 & ... & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & ... & 1 & 0 \\ [K_0\phi(P_1)] & ... & [K_0\phi(P_r)] & K_0 \end{bmatrix}$$

for some large integer K_0 that we will choose momentarily, and consider the lattice point

$$\mathbf{y} = \mathcal{A} \begin{bmatrix} tn_1 \\ \vdots \\ tn_r \\ tn_0 + s \end{bmatrix} = \begin{bmatrix} tn_1 \\ \vdots \\ tn_r \\ \beta \end{bmatrix}$$

where

$$\beta = tn_1[K_0\phi(P_1)] + ... + tn_r[K_0\phi(P_r)] + (tn_0 + s)K_0.$$

Notice that this

$$\beta = tn_1[K_0\phi(P_1)] + ... + tn_r[K_0\phi(P_r)] + (tn_0 + s)K_0.$$

would be exactly $K_0 t\phi(P)$ if not for the rounding; then

$$|\beta - K_0 t\phi(P)| \leq rtN \leq rtN_0.$$

and therefore

$$\begin{aligned} |\mathbf{y}|^2 &\leq t^2(n_1^2 + ... + n_r^2) + \beta^2 \\ &\leq rt^2N_0^2 + t^2(K_0\,|\phi(P)| + rN_0)^2. \end{aligned}$$

But lattice reduction guarantees (see [16] or [42]) that the first element of the reduced basis $\mathbf{b}_1$ has

$$\left|\mathbf{b}_1\right| \leq 2^{r/2}\left|\mathbf{y}\right|.$$

Therefore

$$\begin{aligned} K_0\left|\phi(P)\right| &\geq \sqrt{t^{-2}2^{-r}\left|\mathbf{b}_1\right|^2 - rN_0^2} - rN_0 \\ &= S \end{aligned}$$

$$N^2 \leq K_2^{-1}\left(\log(K_0K_1) - \log S\right)$$

provided S is positive, which is equivalent to

$$\left|\mathbf{b}_1\right| > 2^{r/2}tN_0\sqrt{r^2+r}.$$

Heuristically, $\left|\mathbf{b}_1\right|$ is approximately $K_0^{1/(r+1)}$, so we should choose K_0 to be large enough to satisfy the above inequality. Then we have a smaller bound for N. Replace N_0 by this smaller bound and repeat.

But what do we do if $\phi(\iota(\infty^{\pm}))$ is nonzero? Then our linear form has another term, so that we have

$$\left|\phi(P) - \phi(\iota(\infty^{\pm}))\right| < K_1\exp(-K_2N^2)$$

and

$$N < N_0.$$

Let $\mathcal{A}$ be as before, and reduce the basis of the same $(r+1)$-dimensional lattice as before. Now write the vector

$$\mathbf{x} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ -t[K_0\phi(\iota(\infty^{\pm}))] \end{bmatrix}$$

in terms of the reduced basis, so that

$$\mathbf{x} = \mathcal{B} \begin{bmatrix} x_1 \\ \vdots \\ x_{r+1} \end{bmatrix}$$

In fact, de Weger's algorithm provides matrices $\mathcal{U}$ and $\mathcal{V}$ so that

$$\mathcal{B} = \mathcal{A}\mathcal{U}\mathcal{V} = \mathcal{U}^{-1}$$

so that we can compute the coordinates x_j from

$$\begin{bmatrix} x_1 \\ \vdots \\ x_{r+1} \end{bmatrix} = \mathcal{V}\mathcal{A}^{-1}\mathbf{x}.$$

By Lemma 3.5 of [42],

$$d(\mathbf{x}, \Gamma) \geq 2^{r/2} \left|\mathbf{b}_1\right| \min \left|x_i - [x_i]\right|.$$

Then we have

$$2^{r/2} \left|\mathbf{b}_1\right| \min \left|x_i - [x_i]\right| \leq \left|\mathbf{y} - \mathbf{x}\right|$$

which we can combine as before with our upper bound

$$\begin{aligned} \left|\mathbf{y} - \mathbf{x}\right|^2 &\leq t^2(n_1^2 + ... + n_r^2) + \beta^2 \\ &\leq rt^2N_0^2 + t^2(K_0\left|\phi(P)\right| + 1 + rN_0)^2, \end{aligned}$$

and the rest follows exactly as before.

9.4 A Worked Example

The Mordell-Weil groups of Jacobians of several genus-two curves are computed in [10]. For our example, we shall choose one of these curves with positive rank, namely, their curve 67, which we give here in normal form:

$$y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1.$$

We will use the embedding $\iota : C \to J$ given by

$$\iota(x, y) = (x, y) - \infty^- = (x, y) + \infty^+ - \infty^+ - \infty^-.$$

The group of rational points on the Jacobian has trivial torsion (so we can take $t = 1$) and rank $r = 2$, with generators

$$\begin{aligned} P_1 =& (0, 1) - \infty^- = (0, 1) + \infty^+ - \infty^+ - \infty^- \\ P_2 =& (0, 1) - (0, -1) = (0, 1) + (0, 1) - \infty^+ - \infty^-. \end{aligned}$$

The canonical heights of these points (rounded to 30 digits) are computed as

$$\begin{aligned} \hat{\mathrm{h}}(P_1) =& 0.048085773597485665955583000680 \\ \hat{\mathrm{h}}(P_2) =& 0.066600709944344287365293031597, \end{aligned}$$

and the full height matrix is

$$\left[\begin{array}{cc} < P_1, P_1 > & < P_1, P_2 > \\ < P_2, P_1 > & < P_2, P_2 > \end{array}\right] = \left[\begin{array}{cc} 0.04808577360 & 0.01851493635 \\ 0.01851493635 & 0.06660070994 \end{array}\right],$$

whose eigenvalues are

$$\begin{aligned} \lambda_1 =& 0.036642913635586225512212594948 5 \\ \lambda_2 =& 0.0780435699062437278086634373282. \end{aligned}$$

Consequently, we have the inequality

$$0.03664291363 N^2 \leq \hat{\mathrm{h}}(P).$$

Next, we compute the height of the Jacobian as

$$\mathrm{h}(J) = \mathrm{h}(1, 4, 2, 2, 1, -2, 1) = \log 4,$$

and Lemma 9.2 gives

$$\hat{\mathrm{h}}(P) \leq \mathrm{h}(P) + \frac{4}{3}\log 4 + \frac{1}{3}\log 2744 < \mathrm{h}(P) + 4.4874498111.$$

By Lemma 9.4, we have

$$\mathrm{h}(P) \leq 3\,\mathrm{h}(x) + \frac{3}{2}\log 4 + \frac{1}{2}\log 175 < 3\,\mathrm{h}(x) + 4.6618345286.$$

The polynomial

$$f(x) = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$$

has the following six roots:

$$\begin{aligned}
\alpha_1 =& -3.55960470656323123930\\
\alpha_2 =& -1.10047510431777050721\\
\alpha_3 =& -0.07883178855112289558 - 1.01818842047917064311i\\
\alpha_4 =& -0.07883178855112289558 + 1.01818842047917064311i\\
\alpha_5 =& 0.40887169399162376884 3 - 0.27856491979615507041i\\
\alpha_6 =& 0.40887169399162376884 3 + 0.27856491979615507041i.
\end{aligned}$$

The root with the largest absolute value is α_1. Therefore, Lemma 9.6 tells us that if $|x| \geq 8$, then

$$\mathbf{z} = \phi(P) - \phi(\iota(\infty^{\pm})) \in \mathbb{C}^2$$

(where the sign of $\infty^{\pm}$ is the same as that of y/x^3) has

$$\begin{aligned} 2\log|x| &\leq -4\log 2 - \log|z_1| \\ \log|x| &\leq -3\log 2 - \log|z_2|\,. \end{aligned}$$

Putting these together, we have either $|x| \leq 7$ or

$$\begin{aligned} 0.03664291363N^2 \leq &4.990401257 - 1.5\log|z_1| \\ 0.03664291363N^2 \leq &2.910959715 - 3\log|z_2|\,. \end{aligned}$$

Furthermore, it turns out that

$$2P_1 - P_2 = \infty^+ - \infty^-.$$

This is not surprising, since f_6 is a square and consequently $\infty^+ - \infty^-$ is a rational point of the Jacobian, and P_1 and P_2 generate the group of rational points, but it means that since $P = n_1P_1 + n_2P_2$

$$\phi(P) - \phi(\iota(\infty^+)) = (n_1 - 2)P_1 + (n_2 + 1)P_2$$

and

$$\phi(P) - \phi(\iota(\infty^-)) = n_1P_1 + n_2P_2.$$

This simplifies our calculations, since it allows us to eliminates one term in our linear form by taking $B = N + 2$.

The lattice of periods for the analytic Jacobian is generated by the four vectors

$$(2.023851408 + 2.880842014i,\ 0.9511809806 - 0.1302478509i)$$

$$(1.072670427 + 4.267624951i,\ -2.023851408 - 5.133416484i)$$

$$(-2.25257447055313i,\ -0.996039384338332i)$$

$$(-1.25653508621480i,\ 2.252574470553133i)$$

Our period matrices are

$$\Omega_1 = \begin{bmatrix} 2.023851408 + 2.880842014i & 1.072670427 + 4.267624951i \\ 0.9511809806 - 0.1302478509i & -2.023851408 - 5.133416484i \end{bmatrix}$$
$$\Omega_2 = \begin{bmatrix} -2.25257447055313i & -1.25653508621480i \\ -0.996039384338332i & 2.252574470553133i \end{bmatrix}$$
$$\Omega = \Omega_1^{-1}\Omega_2 = \begin{bmatrix} -1 + 0.909640610271125i & -1/2 - 0.0200406724789979i \\ -1/2 - 0.0200406724789979i & -5/2 + 0.889599937792127i \end{bmatrix}$$

and Ω has eigenvalues 0.877214121 and 0.922026427. Therefore, we have $A^+ = \pi/0.877214121 = 3.58132932$. We can also compute the analytic coordinates of P_1 and P_2, which are

$$\mathbf{u}_1 = \phi(P_1) = (0.9462002887 + 3.509109557i, 2.112372748 - 1.256535086i)$$

$$\mathbf{u}_2 = \phi(P_2) = (-0.8626596409 - 1.754554778i,\ -0.8676403328 + 0.6282675431i).$$

These have norms

$$|\mathbf{u}_1| = 4.38749859$$

$$|\mathbf{u}_2| = 2.22938646.$$

Since these are much bigger than the canonical heights of P_1 and P_2, we take

$$\log V_1 = A^+ \left|\mathbf{u}_1\right|^2 e^2 = 101.848779$$

$$\log V_2 = A^+ \left|\mathbf{u}_2\right|^2 e^2 = 51.7516494.$$

With $k = 2$, Theorem 1.6 gives

$$\log |z_i| > -1.9 \times 10^{120} (\log B)(\log \log B)^5.$$

Combining this with our earlier inequalities

$$0.03664291363 N^2 \leq 4.990401257 - 1.5 \log |z_1|$$

$$0.03664291363 N^2 \leq 2.910959715 - 3 \log |z_2|,$$

and recalling that $B = N + 2$, we get

$$N^2 \leq 137 + 7.8 \times 10^{121} (\log(N+2))(\log\log(N+2))^5$$

$$N^2 \leq 80 + 1.6 \times 10^{122} (\log(N+2))(\log\log(N+2))^5.$$

This gives an upper bound for N. For example, Lemma 2 of [11] gives $N < 10^{72}$ in either case. Then we can iterate:

$$N \leq \sqrt{137 + 7.8 \times 10^{121} (\log(10^{72}+2))(\log\log(10^{72}+2))^5} < 6.72 \times 10^{63}$$

Iterating the second inequality gives $N < 9.62 \times 10^{63}$. (Successive iterations improve this only negligibly; one iteration after the first upper bound is generally sufficient.)

Next, we perform a lattice reduction. We choose $K_0 = 10^{196}$ and compute $\operatorname{Re} \phi_1(P_1)$ and $\operatorname{Re} \phi_1(P_2)$ to at least 196 digits of precision in order to construct the matrix that generates the lattice. After performing lattice reduction, we have

$$|\mathbf{b}_1| > 7.8 \times 10^{64}$$

and therefore we have

$$|z_1| \geq 2.4 \times 10^{-132}.$$

Returning again to our inequality

$$0.03664291363N^2 \leq 4.990401257 - 1.5 \log |z_1| ,$$

we get the new (much improved) estimate

$$N < 112.$$

At this point, we could choose to do lattice reduction again (using $K_0 = 2.5 \times 10^8$ gives $N < 28$), but this bound is already small enough to exhaust.

Since we needed to assume that $|x| \geq 8$ to get our inequalities, we check those 15 integers with $-7 \leq x \leq 7$ and see which give squares for $f(x)$. It turns out that three do, which gives six integer points on our curve

$$(-1, -1)$$

$$(-1,\ 1)$$

$$(0, -1)$$

$$(0,\ 1)$$

$$(1, -3)$$

$$(1,\ 3)$$

Next, we compute all Jacobian points

$$n_1P_1 + n_2P_2$$

with $|n_1|, |n_2| < 112$. The only ones that have the form $\iota(x,\, y)$ for some point $(x,\, y)$ on the curve are the following nine:

$$\begin{aligned}
-2P_1 + 0P_2 &= (1,3) - \infty^- \\
-1P_1 + 3P_2 &= (1/2, -7/8) - \infty^- \\
0P_1 - 2P_2 &= (-1,1) - \infty^- \\
1P_1 - 1P_2 &= (0,-1) - \infty^- \\
1P_1 + 0P_2 &= (0,1) - \infty^- \\
2P_1 - 1P_2 &= \infty^+ - \infty^- \\
2P_1 + 1P_2 &= (-1,-1) - \infty^- \\
3P_1 - 4P_2 &= (1/2, 7/8) - \infty^- \\
4P_1 - 1P_2 &= (1,-3) - \infty^-
\end{aligned}$$

We conclude, therefore, that the six points determined previously are the only integer points on the curve

$$y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1.$$

Appendix A

Index of Notation

- β_i is a coefficient of the linear form $\mathcal{L}$; after chapter 1, it is assumed that $\beta_0 = -1$.

- $\gamma_i \in G_i$, for $1 \leq i \leq k$, is the image, under the exponential map $\gamma_i = \exp_{G_i}(\mathbf{u}_i) \in G_i(K)$

- δ is a bound on the size of the solution given by the Thue-Siegel Lemma 2.3.

- $\boldsymbol{\vartheta} = (\vartheta_{i,1}, \dots, \vartheta_{i,v_i})$ is a finite list of parameters describing the group G_i. In the genus-two case, $\boldsymbol{\vartheta} = (f_0, \dots, f_6)$.

- κ_i is a positive integer such that $\kappa_i Q_{k,l}^{(i,j)}$ has integer coefficients.

- μ is the number of equations in the linear system defined in chapter 2.

- ν is the number of unknowns in the linear system defined in chapter 2.

- ν_i: $|\Phi_{i,\nu_i}(s\mathbf{u})| = \max_j |\Phi_{i,j}(s\mathbf{u})|$

- ρ is the rank of the linear system defined in chapter 2.

- $\Phi_{i,j} : \mathbb{C}^{d_i} \to \mathbb{C}$

- $\boldsymbol{\Phi}_i : \mathbb{C}^{d_i} \to \mathbb{C}^{N_i+1}$

- $\boldsymbol{\Phi} = (\boldsymbol{\Phi}_0, \dots, \boldsymbol{\Phi}_k)$

- $\mathbf{\Psi}_i : \mathbb{C}^{d_i} \to \mathbb{C}^{N_i}$
- $\Psi_{i,j} = \Phi_{i,j}/\Phi_{i,0}$
- $\mathbf{\Psi} = (\mathbf{\Psi}_0, \ldots, \mathbf{\Psi}_k)$
- A_i^+: See H_i^+.
- B_i^+: See H_i^+.
- C_i^+: See H_i^+.
- c_i is the degree of $R_j^{(i)}$ in the X variables, and the degree in the X' variables.
- c_i' is the degree of $R_j^{(i)}$ in the parameters $\vartheta_{i,n}$.
- $c = \max\{c_i\}$.
- $\mathbb{C}[\bar{\mathbb{P}}]$ is the space of multihomogeneous polynomials with complex coefficients.
- $(\mathbb{C}[\bar{\mathbb{P}}]/I(\mathbb{G}))_{(L_0,\ldots,L_k)}$ is the vector subspace of those with multidegree $(L_0, \ldots, L_k)$.
- $D = [K : \mathbb{Q}]$ is the degree of K over $\mathbb{Q}$.
- $d = 1 + d_1 + d_2 + ... + d_k$ is the dimension of the algebraic group $\mathbb{G}$.
- $\tilde{d}$ is the dimension of $\tilde{\mathbb{G}}$.
- d_i is the dimension of the algebraic group G_i; equivalently, it is the dimension of $T_{G_i}(\mathbb{C})$ which is therefore isomorphic to $\mathbb{C}^{d_i}$.
- $\mathbf{e}_i = (\beta_i, 0, \ldots, 0, 1, 0, \ldots, 0)$, so $(\mathbf{e}_1, \ldots, \mathbf{e}_{d-1})$ give a basis for W.

- $(\mathbf{f}_1, \ldots, \mathbf{f}_{d-1})$ is a basis for W with the property that $(\mathbf{f}_1, \ldots, \mathbf{f}_{\tilde{d}})$ is a basis for $T_{\tilde{\mathbb{G}}}(\mathbb{C})$.

- $\exp_{G_i} : T_{G_i}(\mathbb{C}) \to G_i$ is the exponential map on G_i

- $\exp_{\mathbb{G}} : T_{\mathbb{G}}(\mathbb{C}) \to \mathbb{G}$ is the exponential map on $\mathbb{G}$

- $\mathbb{G} = \mathbb{G}_a \times G_1 \times ... \times G_k$

- $\tilde{\mathbb{G}}$ is a group minimizing a certain function given in chapter 2.

- $\mathbb{G}_a$ is the additive algebraic group, whose exponential map is the identity map, and whose embedding into projective 1-space is given by $g \to (1, g)$.

- G_i, for $1 \le i \le k$, is the ith algebraic group, and $G_0 = \mathbb{G}_a$.

- $\mathrm{h}(G_i) = \mathrm{h}(1, \vartheta_{i,1}, \ldots, \vartheta_{i,v_i})$.

- H_i^+ and $H_i^- : \mathbb{R}^+ \to \mathbb{R}$ are functions such that for all $R \ge 0$ and all $\mathbf{z} \in \mathbb{C}^{d_i}$ with $|\mathbf{z}| \le R$, one has

  $$H_i^-(R) \le \log \max\{\Phi_{i,0}(\mathbf{z}), \ldots, \Phi_{i,N_i}(\mathbf{z})\} \le H_i^+(R).$$

  It is assumed that H_i^- is constant, and H_i^+ is quadratic, given by

  $$H_i^+(R) = A_i^+ R^2 + B_i^+ R + C_i^+.$$

- $\mathrm{H}(\mathbb{G}; L_0, ..., L_k)$ is $(\dim \mathbb{G})!$ times the terms of highest degree of the Hilbert polynomial for $\mathbb{G}$, which is a homogeneous polynomial of degree $\dim \mathbb{G}$ with positive integer coefficients.

- $\mathrm{Hf}(\mathbb{G}; L_0, ..., L_k)$ is the multiprojective Hilbert function for $\mathbb{G}$.

- $\mathrm{Hp}(\mathbb{G}; L_0, ..., L_k)$ is the Hilbert polynomial for $\mathbb{G}$, which is a polynomial of degree $\dim \mathbb{G}$.

- K is a number field over which $\mathbb{G}$ and the β_i are defined.

- k is the number of algebraic groups, or the number of independent logarithms.

- $\mathcal{L}(\mathbf{z}) = \beta_0 z_0 + \beta_1 z_1 + ... + \beta_{d-1} z_{d-1}$

- m_i is the degree of G_i so that $\mathrm{H}(G_i; x) = \frac{m_i}{d_i!} x^{d_i}$.

- $m = d! \prod_{i=0}^{k} (m_i/d_i!)$.

- M is a bound on the size of the coefficients in the linear system defined in chapter 2.

- N_i is the dimension of the projective space into which G_i embeds; that is, G_i is an algebraic subset of $\mathbb{P}^{N_i}$.

- P is a polynomial

- $\bar{\mathbb{P}} = \mathbb{P}^1 \times \mathbb{P}^{N_1} \times ... \times \mathbb{P}^{N_k}$

- p is a bound on the size of the linear forms given by the Thue-Siegel Lemma 2.3.

- $Q_{k,l}^{(i,j)}(X_{i,0}, \ldots, X_{i,N_i})$ is a polynomial giving the k'th partial derivative of the variable $X_{i,l}$ in the group G_i, i.e. satisfying

$$\frac{\partial}{\partial z_j} \frac{\Phi_{i,l}}{\Phi_{i,j}} = Q_{k,l}^{(i,j)}(\Phi_{i,0}, \ldots, \Phi_{i,N_i}) / \Phi_{i,j}^{q_i}.$$

- q_i is the degree of $Q_{k,l}^{(i,j)}$ in the X variables.

- q_i' is the degree of $Q_{k,l}^{(i,j)}$ in the parameters $\vartheta_{i,n}$.

- $\tilde{r}$ is the codimension of $T_{\tilde{\mathbb{G}}}(\mathbb{C})$ in W, or one less than the codimension of $\tilde{\mathbb{G}}$ in $\mathbb{G}$.

- $R_j^{(i)}(X_{i,0},\ldots,X_{i,N_i},X'_{i,0},\ldots,X'_{i,N_i})$ is a polynomial giving the group law on G_i, i.e. satisfying
$$\Phi_{i,j}(\mathbf{z}+\mathbf{z}') = R_j^{(i)}(\mathbf{\Phi}_i(\mathbf{z}),\mathbf{\Phi}_i(\mathbf{z}')).$$

- r_i is the length (sum of the absolute values of the integer coefficients) of $R_j^{(i)}$.

- r_i' is the length (sum of the absolute values of the integer coefficients) of $\kappa_i Q_{k,l}^{(i,j)}$.

- $\mathbf{u} = (u_0,\mathbf{u_1},\ldots,\mathbf{u}_k) \in \mathbb{C}^d$ (where $u_0 \in \mathbb{C}$ and $\mathbf{u}_i \in \mathbb{C}^{d_i}$) is a d-tuple of complex numbers which are the independent logarithms whose linear combination interests us.

- $W = \ker \mathcal{L}$

- $\mathbf{w} \in W \subset \mathbb{C}^d$ is the projection of $\mathbf{u}$ onto W; $\mathbf{w} = \sum_{i=1}^{d-1}\beta_i\mathbf{e}_i$ or (equivalently) $\mathbf{w} = \mathbf{u} + (\mathcal{L}(\mathbf{u}),0,\ldots,0)$.

- $\mathbf{X}^{\boldsymbol{\lambda}} = \prod_{i,j} X_{i,j}^{\lambda_{i,j}}$.

- $\mathbf{z} \in \mathbb{C}^d$ is an element of $T_{\mathbb{G}}(\mathbb{C})$

Appendix B

Program for Computing Local Series

```
(*

 Compute the local series expansions:

 u = x + h
 v^2 = f(x + h) = polynomial in x and h of (total) degree 6
 v = power series in h (whose coefficients are rational
         functions in x and y) whose first term is -y

 But let’s write these as power series in k = h/(4y^2).

*)

(* Increase this number to get more terms for all local series *)

seriesdepth = 8

(* compute the z coordinates in terms of x and u *)
xyevals = {
z15 -> (x-u)^2,
z14 -> 1,
z13 -> x+u,
z12 -> x*u ,
z11 -> x*u*(x+u),
z10 -> (x*u)^2,
z9 -> (y-v)/(x-u),
z8 -> (u*y-x*v)/(x-u),
z7 -> (u^2*y-x^2*v)/(x-u),
z6 -> (u^3*y-x^3*v)/(x-u),
z5 -> ((2*f0+f1*(x+u)+2*f2*(x*u)+f3*(x+u)*(x*u)+2*f4*(x*u)^2+
f5*(x+u)*(x*u)^2+2*f6*(x*u)^3)-2*y*v)/((x-u)^2),
z4 -> ((f0*(x+u)+2*f1*(x*u)+f2*(x+u)*(x*u)+2*f3*(x*u)^2+f4*(x+
u)*(x*u)^2+2*f5*(x*u)^3+f6*(x+u)*(x*u)^3)-(x+u)*y*v)/((x-u)^2),
z3 -> (x*u)*((2*f0+f1*(x+u)+2*f2*(x*u)+f3*(x+u)*(x*u)+2*f4*
(x*u)^2+f5*(x+u)*(x*u)^2+2*f6*(x*u)^3)-2*y*v)/((x-u)^2),
z2 -> ((f0*4+f1*(x+3*u)+f2*(2*x*u+2*u^2)+f3*(3*x*u^2+u^3)+
f4*(4*x*u^3)+f5*x*(x*u^3+3*u^4)+f6*2*x*(x*u^4+u^5))*y-(f0*4+
f1*(u+3*x)+f2*(2*u*x+2*x^2)+f3*(3*u*x^2+x^3)+f4*(4*u*x^3)+
f5*u*(u*x^3+3*x^4)+f6*2*u*(u*x^4+x^5))*v)/((x-u)^3),
z1 -> ((f0*2*(x+u)+f1*u*(3*x+u)+f2*4*x*u^2+f3*x*u^2*(x+3*u)+
f4*2*x*u^3*(x+u)+f5*x*u^4*(3*x+u)+f6*4*x^2*u^5)*y-(f0*2*(u+
x)+f1*x*(3*u+x)+f2*4*u*x^2+f3*u*x^2*(u+3*x)+f4*2*u*x^3*(u+x)+
f5*u*x^4*(3*u+x)+f6*4*u^2*x^5)*v)/((x-u)^3),
z0 -> (((2*f0+f1*(x+u)+2*f2*(x*u)+f3*(x+u)*(x*u)+2*f4*(x*
u)^2+f5*(x+u)*(x*u)^2+2*f6*(x*u)^3)-2*y*v)/((x-u)^2))^2}


(* define the sextic *)
f[t_] := f6*t^6 + f5*t^5 + f4*t^4 + f3*t^3 + f2*t^2 + f1*t + f0

(* compute a power series (in k) square root for v/y *)
vts = Range[seriesdepth+1]
vts[[1]] = -1/2
For[i=1, i <= seriesdepth, i++,
  vts[[i+1]] = Factor[Sum[vts[[j+1]]*vts[[i-j+1]], {j, 1, i-1}] -
            (4*f[x])^(i-1)*Coefficient[f[x-h],h,i]]
  ]
voy = Sum[2*vts[[i+1]]*k^i, {i, 0, seriesdepth}] +
      O[k]^(seriesdepth+1);

(* compute the z coordinates as power series in k *)
u = x-(4*f[x]*k)

f0xu = 2*f0+f1*(x+u)+2*f2*(x*u)+f3*(x+u)*(x*u)+2*f4*(x*u)^2+
f5*(x+u)*(x*u)^2+2*f6*(x*u)^3;
f1xu = f0*(x+u)+2*f1*(x*u)+f2*(x+u)*(x*u)+2*f3*(x*u)^2+
f4*(x+u)*(x*u)^2+2*f5*(x*u)^3+f6*(x+u)*(x*u)^3;
gxu = f0*4+f1*(x+3*u)+f2*(2*x*u+2*u^2)+f3*(3*x*u^2+u^3)+
f4*(4*x*u^3)+f5*x*(x*u^3+3*u^4)+f6*2*x*(x*u^4+u^5);
gux = f0*4+f1*(u+3*x)+f2*(2*u*x+2*x^2)+f3*(3*u*x^2+x^3)+
f4*(4*u*x^3)+f5*u*(u*x^3+3*x^4)+f6*2*u*(u*x^4+x^5);
hxu = f0*2*(x+u)+f1*u*(3*x+u)+f2*4*x*u^2+f3*x*u^2*(x+3*u)+
f4*2*x*u^3*(x+u)+f5*x*u^4*(3*x+u)+f6*4*x^2*u^5;
hux = f0*2*(u+x)+f1*x*(3*u+x)+f2*4*u*x^2+f3*u*x^2*(u+3*x)+
f4*2*u*x^3*(u+x)+f5*u*x^4*(3*u+x)+f6*4*u^2*x^5;

z15 = (x-u)^2/(4*f[x]);
z14 = 1;
z13 = x+u;
z12 = x*u ;
z11 = x*u*(x+u);
```

```
z10 = (x*u)^2;
z9 = 2*f[x]*(1-voy)/(x-u);
z8 = 2*f[x]*(u-x*voy)/(x-u);
z7 = 2*f[x]*(u^2-x^2*voy)/(x-u);
z6 = 2*f[x]*(u^3-x^3*voy)/(x-u);
z5 = 4*f[x]*(f0xu-2*voy*f[x])/((x-u)^2);
z4 = 4*f[x]*(f1xu-(x+u)*voy*f[x])/((x-u)^2);
z3 = (x*u)*z5;
z2 = 8*f[x]^2*(gxu-gux*voy)/((x-u)^3);
z1 = 8*f[x]^2*(hxu-hux*voy)/((x-u)^3);
z0 = z5^2;

(* Compute the inverse of z0: *)
(*   Faster than:   *)
(* d = 1/z0; *)
(* d[[3]] = Together[d[[3]]];  *)
(*   is:   *)
numterms = z0[[5]]-z0[[4]]
d = 1 + k^(numterms-1) + O[k]^(numterms)
d[[3,1]] = Together[1/z0[[3,1]]]
For[i=1, i < numterms, i++, d[[3,i+1]] =
 Together[-d[[3,1]]*Sum[z0[[3,j+1]]*d[[3,i-j+1]], {j,1,i}]]]
d[[4]] = -z0[[4]]
d[[5]] = d[[4]] + numterms
(* 73 sec (5), 154 sec (6), 316 sec (7), 625 sec (8) *)

z1 = z1*d;
z2 = z2*d;
z1[[3]] = Together[z1[[3]]];
z2[[3]] = Together[z2[[3]]];

terms = Table[0, {16}]
terms[[1]] = {1}
terms[[2]] = {0, s1}
terms[[3]] = {0, s2}
For[i = 4, i <= 16, i++, Block[{fn, j, parity, stopat},
  fn = {z0, z1, z2, z3, z4, z5, z6, z7, z8,
        z9, z10, z11, z12, z13, z14, z15}[[i]]*d;
  parity = {0, 1, 1, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 6}[[i]];
  (* fn = z_{i-1}/(z_0*(2y)^parity); *)
  stopat = fn[[5]]; (* = parity + seriesdepth *)
  terms[[i]] = Table[0, {stopat}];
  fn[[3]] = Map[Together, fn[[3]]];
  (* Print[{i, 0}]; *)
  For[j = parity, j < stopat, j = j+2,
    (* fn = (z_{i-1} - portion already in "terms")/(z_0*(2y)^j); *)
    polyx = Together[Coefficient[fn, k, j]];
    terms[[i,j+1]] = Together[(polyx /. {x -> s1/s2})*s2^j];
    If[j<stopat-1,
        (* fn = fn - (terms[[i,j+1]] /. {s1 -> z1, s2 -> z2}); *)
        pow=1+O[k]^(stopat - j);
        dfn=Coefficient[polyx,x,0]+O[k]^(stopat - j);
        For[l=1, l<=j, l++,
          pow = pow*(z1 + O[k]^(stopat - j + 1));
          pow[[3]] = Together[pow[[3]]];
          c = Coefficient[polyx,x,l];
          dfn = dfn*(z2 + O[k]^(stopat - j + 1));
          dfn[[3]] = Together[dfn[[3]]];
          dfn = dfn + c*pow;
          dfn[[3]] = Together[dfn[[3]]];
        ];
        fn = fn - dfn;
        fn = fn/(4*f[x]);
        fn[[3]] = Together[fn[[3]]];
        (* Print[{i, j}] *)
    ]
  ]
]]

terms >> locals.txt
```

Bibliography

[1] A. Baker, "Linear Forms in the Logarithms of Algebraic Numbers (I through IV)," (I) *Mathematika* **13**: 204–216, 1966, (II) *ibid.* **14**: 102–107, 1967, (III) *ibid.* **14**: 220–228, 1967, (IV) *ibid.* **15**: 204–216, 1968.

[2] A. Baker and G. Wüstholz, "Logarithmic forms and group varieties," *J. Reine Angew. Math.* **442**: 19–62, 1993.

[3] D. Cantor, "Computing in the Jacobian of a hyperelliptic curve," *Math. Comp.* **48**(177): 95–101, 1987.

[4] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc., Lecture Note Series **230**, Cambridge Univ. Press, Cambridge, 1996.

[5] M. Chardin, *Contributions à l'algèbre commutative effective et à la théorie de l'élimination*, Thèse de doctorat, Université de Paris VI, 1990.

[6] M. Chardin, "Une majorarion de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique," *Bull. Soc. Math. France* **117**: 305–318, 1989.

[7] P. L. Cijsouw and M. Waldschmidt, "Linear forms and simultaneous approximations," *Compositio Math.* **34**: 173–197, 1977.

[8] S. David, "Minorations de formes linéaires de logarithmes elliptiques," *Mém. Soc. Math. France* **62**, Soc. Math. France, Paris, 1995.

[9] L. Denis, "Lemmes de multiplicités et intersections," *Comment. Math. Helv.* **70**: 235–247, 1995.

[10] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, "Empirical Evidence for the Birch and Swinnerton-Dyer Conjectures for Modular Jacobians of Genus 2 Curves," *Math. Comp.* **70**(236): 1675–1697, 2001.

[11] J. Gebel, A. Pethö, and H. G. Zimmer, "Computing integral points on elliptic curves," *Acta Arith.* **68**: 171–192, 1994.

[12] J. Harris, *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992, lecture 13.

[13] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, 1977.

[14] N. Hirata-Kohno, "Formes linéaires de logarithmes de points algébriques sur les groupes algébriques," *Invent. Math.* **104**: 401–433, 1991.

[15] K. Lauter, "The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves," *Topics in Algebraic and Noncommutative Geometry*, AMS Contemporary Mathematics Series **324**: 165–171, 2003.

[16] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.* **261**: 515-534, 1982.

[17] D. Masser, "Heights, Transcendence, and Linear Independence on Commutative Group Varieties," in: *Diophantine Approximation*, Lecture Notes in Mathematics **1819**, Springer Berlin / Heidelberg, 2003.

[18] D. Masser and G. Wüstholz, "Zero estimates on group varieties II," *Invent. Math.* **80**: 233–267, 1985.

[19] D. Mumford, *Tata Lectures on Theta I*, Progress in Mathematics **43**, Birkhäuser Boston, MA, 1984.

[20] D. Mumford, *Tata Lectures on Theta, II*, Progress in Mathematics **43**, Birkhäuser Boston, MA, 1984.

[21] D. Mumford, *Tata Lectures on Theta III*, Progress in Mathematics **43**, Birkhäuser Boston, MA, 1984.

[22] D. Mumford, "On the equations defining abelian varieties I, II, III," (I) *Invent. Math.* **1**: 287–354, 1966, (II) *ibid.* **3**: 75–125, 1967, (III) *ibid.* **3**: 215–244, 1967.

[23] Y. Nesterenko, "Estimates for the characteristic function of a prime ideal," *Math. Sbornik* **123** (165, no. 1): 11–34, 1984, *Math. USSR. Sbornik* **51** (1): 9–32, 1985.

[24] P. Philippon, “Lemmes de zéros dans les groupes algébriques commutatifs,” *Bull. Soc. Math. France* **114**: 355–383, 1986, Errata et Addenda, *ibid.* **115**: 397–398, 1987.

[25] P. Philippon, “Nouveaux lemmes de zéros dans les groupes algébriques commutatifs,” *Rocky Mountain J. Math.* **26**: 1069–1088, 1996.

[26] P. Philippon and M. Waldschmidt, “Formes linéaires de logarithmes sur les groupes algébriques commutatifs,” *Ill. J. Math.* **32**: 281–314, 1988.

[27] P. Philippon and M. Waldschmidt, “Lower bounds for linear forms in logarithms,” in: New Advances in Transcendence Theory edited by A. Baker, Cambridge University Press, Cambridge (1988), 288.

[28] N. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts **41**, Cambridge University Press, Cambridge, 1998.

[29] M. Sombra, “Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz,” *Journal of Pure and Applied Algebra* **117** & **118**: 565–599, 1997.

[30] M. Stoll, “Implementing 2-descent for Jacobians of hyperelliptic curves,” *Acta Arith.* **98**(3): 243–277, 2001.

[31] M. Stoll, “On the height constant for curves of genus two,” *Acta Arith.* **90**: 183–201, 1999.

[32] M. Stoll, “On the height constant for curves of genus two, II,” *Acta Arith.* **104**(2): 165–182, 2002.

[33] R. J. Stroeker and B. M. M. de Weger, “Solving elliptic diophantine equations: the general cubic case,” *Acta Arith.* **87**: 339–365, 1999.

[34] R. J. Stroeker and N. Tzanakis, “Computing all integer solutions of a genus 1 equation,” *Math. Comp.* **72**: 1917–1933, 2003.

[35] R. J. Stroeker and N. Tzanakis, “On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an improvement,” *Experim. Math.* **8**: 135–149, 1999.

[36] R. J. Stroeker and N. Tzanakis, “Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms,” *Acta Arith.* **67**: 177–196, 1994.

[37] N. Tzanakis, “Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms: the case of quartic equations,” *Acta Arith.* **75**: 165–190, 1996.

[38] B. L. Van der Waerden, “On Hilbert’s function, series of composition of ideals and a generalization of the theorem of Bezout,” *Proc. Royal Acad. Amsterdam* **31**: 749–770, 1928.

[39] M. Waldschmidt, "A lower bound for linear forms in logarithms," *Acta Arith.* **37**: 257–283, 1980.

[40] M. Waldschmidt, "Approximation diophantienne dans les groupes algébriques commutatifs," *J. Reine Angew. Math.* **493**: 61–113, 1997.

[41] M. Waldschmidt, "Nombres transcendants et groupes algébriques," *Astérisque* **69–70**, 1979.

[42] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI Tract 65, Centre for Mathematics and Computer Science, Amsterdam, 1989.