Heights on algebraic curves

T. Shaska [a] L. Beshaj [b,1]

[a] *Oakland University, Rochester, MI, USA; E-mail: shaska@oakland.edu*

[b] *Oakland University, Rochester, MI, USA; E-mail: beshaj@oakland.edu*

Abstract. In these lectures we cover basics of the theory of heights starting with the heights in the projective space, heights of polynomials, and heights of the algebraic curves. We define the minimal height of binary forms and moduli height for algebraic curves and prove that the moduli height of superelliptic curves $\mathfrak{H}(f) \leq c_0 \tilde{H}(f)$ where c_0 is a constant and $\tilde{H}$ the minimal height of the corresponding binary form. For genus $g = 2$ and 3 such constant is explicitly determined. Furthermore, complete lists of curves of genus 2 and genus 3 hyperelliptic curves with height 1 are computed.

Keywords. algebraic curves, heights, moduli height

Introduction

The heights of points on Abelian varieties have been used to prove important results on the theory of rational points on algebraic curves. In these lectures we give a quick review of some of the basic results of the classical theory of heights and introduce some new concepts of heights for algebraic curves with the intention of determining equations of curves with minimal height.

The material of the first lecture is classic and can be found in any of the excellent books [6, 8, 9, 11, 12]. We define affine and projective heights on the projective space, multiplicative and logarithmic heights, and absolute heights. We describe Northcott's theorem, Kronecker's theorem, and Segre embedding. Our main goal is to investigate how the height of a point changes under a change of coordinate. We describe the formula for changing coordinates in Thm. 7.

In the second lecture we cover the heights of polynomials, Gauss lemma on heights, Gelfand's inequality, and bounds on heights of homogenous polynomials acting on them by linear transformations on variables. The main focus of this lecture is on the heights of binary forms. These are interesting polynomials because they give equations of hyperelliptic and superelliptic curves which are the focus of this Summer School. For any binary form f we provide bounds for f^M when $M \in SL_2(K)$. This leads to the definition of the *minimal height* $\tilde{H}(f)$ and *moduli height* $\mathfrak{H}(f)$ for binary forms. We prove that $\mathfrak{H}(f) \leq c_0 \tilde{H}(f)^{n_0}$ for any binary form f, where c_0 and n_0 are constants depending only on the degree of the binary form f.

[1] Part of this paper was written when this author was visiting Department of Mathematics at Princeton University. This authors wants to thanks Princeton University for their hospitality.

In the third lecture we focus on heights of algebraic curves. Our main focus is in providing equations for the algebraic curves with "small" coefficients as continuation of our previous work [1, 2, 5, 15, 19, 19, 20, 23]. Hence, the concept of height is the natural concept to be used. For a genus $g \geq 2$ algebraic curve $\mathscr{X}_g$ defined over an algebraic number field K we define the height $H_K(\mathscr{X}_g)$ and show that this is well-defined. This is basically the minimum height among all curves which are isomorphic to $\mathscr{X}_g$ over K. $\bar{H}_K(\mathscr{X}_g)$ is the height over the algebraic closure $\bar{K}$. It must be noticed that our definition is on the isomorphism class of the curve and not on some equation of the curve. We provide an algorithm to determine the height of a curve C provided some equation for C. This algorithm is rather inefficient, but can be used for $g = 2$ and $g = 3$ hyperelliptic curves when the coefficients of the initial equation of C are not too large.

The moduli height of a curve is the height in the projective space of the moduli point corresponding to the curve. We prove that for a given constant c there are only finitely many curves (up to isomorphism) of moduli height $\leq c$.

A natural applications of the results of lecture 3 would be superelliptic curves. Such curves have equation $y^n = f(x)$ and their isomorphism classes are determined by the $GL_2(K)$-orbits on the space of degree d binary forms V_d, where $d = \deg f$. Hence, we apply the results from lecture 2 to study the heights of such curves.

For a genus 2 curve with equation $y^2 = f(x)$ the moduli height is bounded as follows

$$\mathfrak{H}(f) \leq 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot H(f)^{10}$$

Moreover we show that there are precisely 230 genus 2 curves with height 1, from which 186 have automorphism group of order 2, 28 of them have automorphism group isomorphic to the Klein 4-group, and the rest have automorphism group of order > 4. All these curves are listed in Tables 1-4.

Similar computations are done for genus 3 hyperelliptic curves where $GL_2(K)$-invariants $t_1, \dots, t_6$ are used as defined in [22]. In the last part of this lecture we present some open problems and conjectures.

For more references and classical results on the theory of heights the reader should check these timeless books [6–9, 11, 13, 14].

Notation: Throughout this paper by a curve we mean a smooth, irreducible algebraic curve. Unless otherwise noted a "curve" C means the isomorphism class of C over some field K. We fix the following notation throughout this paper.

K a number field,
$\mathscr{O}_K$ the ring of integers of K,
v an absolute value of K,
M_K the set of all absolute values of K,
M_K^0 the set of non-Archimedean absolute values of K,
M_K^∞ the set of Archimedean absolute values of K,
K_v the completion of K at v,
n_v the local degree $[K_v : \mathbb{Q}_v]$,
$G_\mathbb{Q}$ the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Part 1: Heights on the projective space

In this lecture we define different heights of a point on a projective space, culminating in the Northcott and Kronecker theorems. We discuss Segre's map and the d-uple embedding with the intention of establishing a bound for the height of a point after a change of coordinates.

1. Heights on the projective space

In this section we define the heights on the projective space over a number field K and give some basic properties of the heights function.

Let K be an algebraic number field and $[K:\mathbb{Q}]=n$. With M_K we will denote the set of all absolute values in K. For $v \in M_K$, the **local degree at** v, denoted n_v is

$$n_v = [K_v : \mathbb{Q}_v]$$

where $K_v, \mathbb{Q}_v$ are the completions with respect to v. The following are true for any number field K, see [9, pg. 171-172] for proofs.

i) **Degree formula**. Let L/K be an extension of number fields, and let $v \in M_K$ be an absolute value on K. Then

$$\sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] = [L:K]$$

ii) **Product formula**. Let K be a number field, and let $x \in K^\star$. Then we say that M_K satisfies the product formula if

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

Throughout this paper with $\overline{\mathbb{Q}}$ we will denote the algebraic closure of $\mathbb{Q}$ and with $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Given a point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ with homogenous coordinates $[x_0, \dots, x_n]$, the field of definition of P is

$$\mathbb{Q}(P) = \mathbb{Q}(x_o/x_j, \dots, x_n/x_j)$$

for any j such that $x_j \neq 0$.

Let K be a number field, $\mathbb{P}^n(K)$ the projective space, and $P \in \mathbb{P}^n(K)$ a point with homogenous coordinates $P = [x_0, \dots, x_n]$, for $x_i \in K$. The **multiplicative height** of P is defined as follows

$$H_K(P) := \prod_{v \in M_K} \max \left\{ |x_0|_v^{n_v}, \dots, |x_n|_v^{n_v} \right\}$$

The **logarithmic height** of the point P is defined as follows

$$h_K(P) := \log H_K(P) = \sum_{v \in M_K} \max_{0 \leq j \leq n} \left\{ n_v \cdot \log |x_j|_v \right\}.$$

Example 1. *Let $P = [x_0,\ldots,x_n] \in \mathbb{P}^n(\mathbb{Q})$. It is clear that P will have a representative $[y_0,\ldots,y_n]$ such that $y_i \in \mathbb{Z}$ for all i and $\gcd(y_0,\ldots,y_n) = 1$. With such representative for the coordinates of P, the non-Archimedean absolute values give no contribution to the height, and we obtain*

$$H_{\mathbb{Q}}(P) = \max_{0\le j\le n}\left\{\ |x_j|_\infty\right\}$$

Next we will give some basic properties of heights functions.

Lemma 1. *Let K be a number field and $P \in \mathbb{P}^n(K)$. Then the following are true:*

i) The height $H_K(P)$ is well defined, in other words it does not depend on the choice of homogenous coordinates of P

ii) $H_K(P) \ge 1$.

Proof. i) Let $P = [x_0,\ldots,x_n] \in \mathbb{P}^n(K)$. Since P is a point in the projective space, any other choice of homogenous coordinates for P has the form $[\lambda x_0,\ldots,\lambda x_n]$, where $\lambda \in K^*$. Then

$$\begin{aligned} H_K([\lambda x_0,\ldots,\lambda x_n]) &= \prod_{v\in M_K}\max_{0\le i\le n}\left\{\ |\lambda x_i|_v^{n_v}\right\} = \prod_{v\in M_K}|\lambda|_v^{n_v}\max_{0\le i\le n}\left\{\ |x_i|_v^{n_v}\right\} \\ &= \left(\prod_{v\in M_K}|\lambda|_v^{n_v}\right)\cdot\left(\prod_{v\in M_K}\max_{0\le i\le n}\left\{\ |x_i|_v^{n_v}\right\}\right) \end{aligned}$$

Applying the product formula we have

$$H_K([\lambda x_0,\ldots,\lambda x_n]) = \prod_{v\in M_K}\max_{0\le i\le n}\left\{\ |x_i|_v^{n_v}\right\} = H_K(P)$$

And this completes the proof of the first part.

ii) For every point $P \in \mathbb{P}^n(K)$ we can find a representative of P with homogenous coordinates such that one of the coordinates is 1. Let us reorder the coordinates of $P = [1,x_1,\ldots,x_n]$ and calculate the height.

$$H_K(P) = \prod_{v\in M_K}\max\left\{\ |x_0|_v^{n_v},\ldots,|x_n|_v^{n_v}\right\} = \prod_{v\in M_K}\max\left\{\ 1,|x_1|_v^{n_v},\ldots,|x_n|_v^{n_v}\right\}$$

Hence, every factor in the product is at least 1. Therefore, $H_K(P) \ge 1$. ☐

Lemma 2. *Let $P \in \mathbb{P}^n(K)$ and L/K be a finite extension. Then,*

$$H_L(P) = H_K(P)^{[L:K]}.$$

Proof. Let L be a finite extension of K and M_L the corresponding set of absolute values. Then,

$$
\begin{aligned}
H_L(P) &= \prod_{w \in M_L} \max_{0 \le i \le n} \left\{ |x_i|_w^{n_w} \right\} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max_{0 \le i \le n} \left\{ |x_i|_v^{n_w} \right\}, \qquad \text{since } x_i \in K \\
&= \prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i|_v^{n_v \cdot [L:K]} \right\}, \qquad \text{(product formula)} \\
&= \prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i|_v^{n_v} \right\}^{[L:K]} = H_K(P)^{[L:K]}
\end{aligned}
$$

This completes the proof. □

Using Lemma 2, part ii), we can define the height on $\mathbb{P}^n(\overline{\mathbb{Q}})$. The height of a point on $\mathbb{P}^n(\overline{\mathbb{Q}})$ is called the **absolute (multiplicative) height** and is the function

$$
\begin{aligned}
H &: \mathbb{P}^n(\bar{\mathbb{Q}}) \to [1, \infty) \\
&H(P) = H_K(P)^{1/[K:\mathbb{Q}]},
\end{aligned}
$$

where $P \in \mathbb{P}^n(K)$, for any K. The **absolute (logarithmic) height** on $\mathbb{P}^n(\overline{\mathbb{Q}})$ is the function

$$
\begin{aligned}
h &: \mathbb{P}^n(\bar{\mathbb{Q}}) \to [0, \infty) \\
&h(P) = \log H(P) = \frac{1}{[K:\mathbb{Q}]} h_K(P).
\end{aligned}
$$

Example 2. *Let $\alpha \in K$ be an algebraic number. The **height** of $\alpha \in K$ is the height of the corresponding projective point $(\alpha, 1) \in \mathbb{P}^1(K)$. Thus,*

$$
H_K(\alpha) = \prod_{v \in M_K} \max \left\{ 1, |\alpha|_v^{n_v} \right\}
$$

and similarly for $h_K(\alpha), H(\alpha), h(\alpha)$.

Lemma 3. *The height is invariant under Galois conjugation. In other words, for $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$ we have $H(P^\sigma) = H(P)$.*

Proof. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Let K be a finite Galois extension of $\mathbb{Q}$ such that $P \in \mathbb{P}^n(K)$. Let $\sigma \in G_{\mathbb{Q}}$. Then σ gives an isomorphism

$$
\sigma : K \to K^\sigma
$$

and also identifies the sets M_K, and M_{K^σ} as follows

$$
\begin{aligned}
\sigma &: M_K \to M_{K^\sigma} \\
&v \to v^\sigma
\end{aligned}
$$

Hence, for every $x \in K$ and $v \in M_K$, we have $|x^\sigma|_{v^\sigma} = |x|_v$. Obviously σ gives as well an isomorphism

$$
\sigma : K_v \to K^\sigma_{v^\sigma}
$$

Therefore $n_v = n_{v^\sigma}$, where $n_{v^\sigma} = [K^\sigma_{v^\sigma} : \mathbb{Q}_v]$. Then

$$\begin{aligned} H_{K^\sigma}(P^\sigma) &= \prod_{w \in M_{K^\sigma}} \max_{0 \le i \le n} \left\{ |x_i^\sigma|_w^{n_w} \right\} \\ &= \prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i^\sigma|_{v^\sigma}^{n_{v^\sigma}} \right\} = \prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i|_v^{n_v} \right\} = H_K(P) \end{aligned}$$

This completes the proof. □

The following is known in the literature as Northcott's theorem.

Theorem 1 (Northcott). *Let c_0 and d_0 be constants. Then the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \le c_0 \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \le d_0\}$$

contains only finitely many points. In particular for any number field K

$$\{P \in \mathbb{P}^n(K) : H_K(P) \le c_0\}$$

is a finite set.

Proof. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ be a point such that some $x_{i_0} = 1$. Then for any absolute value v, and for all $0 \le i \le n$ we have

$$\max\left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\} \ge \max\left\{ 1, |x_i|_v^{n_v} \right\}.$$

Let $\mathbb{Q}(P)$ be the field of definition of P. Let us first estimate $H_{\mathbb{Q}(P)}(P)$.

$$\begin{aligned} H_{\mathbb{Q}(P)}(P) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max\left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\} \\ &\ge \prod_{v \in M_{\mathbb{Q}(P)}} \max\left\{ 1, |x_i|_v^{n_v} \right\}, \quad \text{for all } 0 \le i \le n. \\ &= H_{\mathbb{Q}(P)}(x_i), \quad \text{for all } 0 \le i \le n. \end{aligned}$$

Taking the $[\mathbb{Q}(P) : \mathbb{Q}]$-th root we have $H(x_i) \le H(P)$, for all $0 \le i \le n$. Clearly, $\mathbb{Q}(x_i) \subset Q(P)$, for all $0 \le i \le n$ and therefore $[\mathbb{Q}(x_i) : \mathbb{Q}] \le [\mathbb{Q}(P) : \mathbb{Q}]$. Then for all $0 \le i \le n$ we have,

$$H(x_i) \le c_0 \text{ and } [\mathbb{Q}(x_i) : \mathbb{Q}] \le d_0.$$

It suffices to show that for each $1 \le d \le d_0$ the set

$$\{x \in \overline{\mathbb{Q}} : H(x) \le c_0 \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$$

is finite (i.e we are considering the case when $n = 1$).

Assume, for some $x \in \overline{\mathbb{Q}}$, we have $[\mathbb{Q}(x) : \mathbb{Q}] = d$. Let $x_1, \ldots, x_d$ be the d conjugates of x in $\mathbb{Q}$. Then the minimal polynomial of x over $\mathbb{Q}$ is

$$f_x(t) = \min(x,\mathbb{Q},t) = \prod_{j=1}^{d}(t-x_j) = \sum_{r=0}^{d}(-1)^r s_r(x) t^{d-r}.$$

Then for any absolute value $v \in M_{\mathbb{Q}(x)}$ we have

$$|s_r(x)|_v = \left| \sum_{1\le i_1 \le \cdots \le i_r \le d} x_{i_1}\cdots x_{i_r} \right|_v \le |c(r,d)|_v \max_{1\le i_1 \le \cdots \le i_r \le d} \left\{ |x_{i_1}\cdots x_{i_r}|_v \right\} \le$$

$$\le |c(r,d)|_v \max_{1\le i \le d} \left\{ |x_i|_v^r \right\} \le |c(r,d)|_v \prod_{i=1}^{d} \left\{ |x_i|_v \right\}^r$$

Where, $c(r,d)$ represents the number of terms in a symmetric polynomial with degree r and d variables, and is $\binom{d}{r}$. Then,

$$|c(r,d)|_v = \begin{cases} \begin{pmatrix} d \\ r \end{pmatrix} & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ in non-Archimedean} \end{cases}$$

Hence, $c(r,d) = \binom{d}{r} \le 2^d$ when v is Archimedean, and 1 if v in non-Archimedean. Now let us take the maximum over all symmetric polynomials. We have

$$\max\left\{ |s_0(x)|_v, \ldots, |s_d(x)|_v \right\} \le |s_i(x)|_v, \qquad \text{(for some } 1 \le i \le d)$$

$$\le |c(d)|_v \prod_{i=1}^{d} \max\left\{ 1, |x_i|_v \right\}^d,$$

where, as above $|c(d)|_v = \binom{d}{r}$ when v is Archimedean and 1 otherwise. Now we can calculate the height of $(s_0(x),\ldots,s_d(x))$.

$$H_{\mathbb{Q}(x)}(s_0(x),\ldots,s_d(x)) = \prod_{v\in M_{\mathbb{Q}(x)}} \max_{0\le i\le d} \left\{ |s_i(x)|_v^{n_v} \right\} \le \prod_{v\in M_{\mathbb{Q}(x)}} |c(d)|_v^{n_v} \prod_{i=1}^{d} \max_i \left\{ |x_i|_v^{n_v}, 1 \right\}^d$$

Using the degree formula

$$\prod_{v\in M_{\mathbb{Q}(x)}} |c(d)|_v^{n_v} = \prod_{v\in M^{\infty}_{\mathbb{Q}(x)}} |c(d)|_v^{n_v} = c(d)^{[\mathbb{Q}(x):\mathbb{Q}]} \le 2^{d^2}$$

we have

$$H_{\mathbb{Q}(x)}(s_0(x),\ldots,s_d(x)) \le 2^{d^2} \prod_{i=1}^{d} H_{\mathbb{Q}(x)}(x_i)^d$$

Taking, $[\mathbb{Q}(x):\mathbb{Q}]$-th root of both sides we have

$$H(s_0(x),\ldots,s_d(x)) \le 2^d \prod_{i=1}^{d} H(x_i)^d$$

But the x_i's are conjugates and by Lemma 3 they all have the same height. Hence,

$$H(s_0(x),\ldots,s_d(x)) \le 2^d H(x)^{d^2} \le (2c_0^d)^d \quad \text{since } H(x) \le c_0$$

Since the s_i's are in $\mathbb{Q}$, is clear that for a given c and d there are only finitely many possibilities for the polynomial $f_x(t)$, and therefore only finitely many possibilities for x. Hence the set

$$\{x \in \overline{\mathbb{Q}} : H(x) \le c_0 \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$$

is finite. □

Lemma 4 (Kronecker's theorem)**.** *Let K be a number field, and let $P = [x_0,\ldots,x_n] \in \mathbb{P}^n(K)$. Fix any i_0 with $x_{i_0} \neq 0$. Then $H(P) = 1$ if and only if the ratio x_j/x_{i_0} is a root of unity or zero for every $0 \le j \le n$.*

Proof. Let $P = [x_0,\ldots,x_n] \in \mathbb{P}^n(K)$. Without loss of generality we can divide the coordinates of P by x_{i_0} and then reorder them. Assume, $P = [1, y_1,\ldots,y_n]$ where $y_1,\ldots,y_n$ are of the form x_j/x_{i_0}. If y_l is a root of unity for every $1 \le l \le n$ then $|y_l|_v = 1$ for every $v \in M_K$. Hence, $H(P) = 1$.

Assume $H(P) = 1$. Let $P^r = [x_0^r,\ldots,x_n^r]$, for $r = 1,2,3\ldots$. Then, from the definition of the height is clear that $H(P^r) = H(P)^r$, for every $r \ge 1$. But $P^r \in \mathbb{P}^n(K)$ and by Theorem 1 we have that

$$\{P^r \in \mathbb{P}^n(K) : H_K(P^r) \le c\}$$

is a finite set. In this case $c = 1$ and therefore the sequence $P, P^2, P^3, \ldots$ contains only finitely many distinct points. Choose integers $s > r \ge 1$ such that $P^s = P^r$. This implies that for each $1 \le j \le n$ we have $x_j^s = x_j^r$. Therefore, $x_j^{s-r} = 1$, where $s - r > 0$. Therefore, each x_j is a root of unity or is zero. □

2. Segre map and d-uple embedding

Let $m,n \ge 1$ and let $N = (n+1)(m+1) - 1$. The **Segre map** is the map

$$\begin{aligned} S_{n,m} :\ & \mathbb{P}^n(\overline{\mathbb{Q}}) \times \mathbb{P}^m(\overline{\mathbb{Q}}) \to \mathbb{P}^N(\overline{\mathbb{Q}}) \\ & (P,Q) \to [x_0y_0, x_0y_1,\ldots,x_iy_j,\ldots,x_ny_m] \end{aligned}$$

where $P = [x_0,\ldots,x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $Q = [y_0,\ldots,y_m] \in \mathbb{P}^m(\overline{\mathbb{Q}})$. The Segre maps are morphisms and give embeddings of the product $\mathbb{P}^n(\overline{\mathbb{Q}}) \times \mathbb{P}^m(\overline{\mathbb{Q}})$ into $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next we will see how some of the properties of the heights are carried over through Segre embeddings.

Lemma 5. *Let $S_{n,m}$ be the Segre embedding, $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, and $Q \in \mathbb{P}^m(\overline{\mathbb{Q}})$. Then,*

$$H(S_{n,m}(P,Q)) = H(P) \times H(Q).$$

Proof. Let K be some number field such that $P \in \mathbb{P}^n(K)$, and $Q \in \mathbb{P}^m(K)$, and $R = [z_0, \dots, z_N] = S_{n,m}(P,Q) \in \mathbb{P}^N(K)$. For every absolute value $v \in M_K$ the following is true

$$\max_{0 \le l \le N} \left\{ |z_l|_v \right\} = \max_{\substack{0 \le i \le n \\ 0 \le j \le m}} \left\{ |x_i y_j|_v \right\} \qquad \text{(by definition of Segre map)}$$

$$= \max_{\substack{0 \le i \le n \\ 0 \le j \le m}} \left\{ |x_i|_v \cdot |y_j|_v \right\} \text{ (by absolute value properties)}$$

$$= \left(\max_{0 \le i \le n} \left\{ |x_i|_v \right\} \right) \cdot \left(\max_{0 \le j \le m} \left\{ |y_j|_v \right\} \right)$$

Let us calculate

$$H_K(S_{n,m}(P,Q)) = \prod_{v \in M_K} \max_{0 \le l \le N} \left\{ |z_l|_v^{n_v} \right\} = \prod_{v \in M_K} \left(\max_{0 \le i \le n} \left\{ |x_i|_v^{n_v} \right\} \right) \cdot \left(\max_{0 \le j \le m} \left\{ |y_j|_v^{n_v} \right\} \right)$$

$$= \prod_{v \in M_K} \left(\max_{0 \le i \le n} \left\{ |x_i|_v^{n_v} \right\} \right) \cdot \prod_{v \in M_K} \left(\max_{0 \le j \le m} \left\{ |y_j|_v^{n_v} \right\} \right) = H_K(P) \cdot H_K(Q)$$

Taking $[K : \mathbb{Q}]$-root of both sides we obtain the desired result. $\square$

Let $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Let $M_0(x), \dots, M_N(x)$ be the complete collection of monomials of degree d in the variable $x = (x_0, \dots, x_n)$. Note that N is the number of monomials of degree d in $n+1$ variables minus 1, hence $N = \binom{n+d}{n} - 1$.

Then, the map

$$\phi_d : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^N(\overline{\mathbb{Q}})$$
$$P \to [M_0(x), \dots, M_N(x)]$$

is called the **d-uple embedding** of $\mathbb{P}^n(\overline{\mathbb{Q}})$. This is a morphism, and in fact is an embedding of $\mathbb{P}^n(\overline{\mathbb{Q}})$ into $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next we describe a formula for the height under a d-uple embedding.

Lemma 6. *Let $\phi_d : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^N(\overline{\mathbb{Q}})$ be the d-uple embedding. Then for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ we have*

$$H(\phi_d(P)) = H(P)^d.$$

Proof. Let P, and $\phi_d(P) = [M_0(x), \dots, M_N(x)]$ be as above. By definition $M_i(x)$ are all monomials of degree d in $n+1$ variables. It is clear that

$$|M_i(x)|_v \le \max_i \left\{ |x_i|_v^d \right\}$$

and since $x_0^d, \dots, x_n^d$ appear in the list we have

$$\max_{0 \le j \le N} \left\{ |M_j(x)|_v \right\} = \max_{0 \le i \le n} \left\{ |x_i|_v^d \right\}$$

Let K be a number field such that $P \in \mathbb{P}^n(K)$, and $\phi_d(P) \in \mathbb{P}^m(K)$. Then,

$$H_K(\phi_d(P)) = \prod_{v \in M_K} \max_{0 \le j \le N} \left\{ |M_j(x)|_v^{n_v} \right\} = \prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i|_v^{d \cdot n_v} \right\}$$
$$= \left(\prod_{v \in M_K} \max_{0 \le i \le n} \left\{ |x_i|_v^{n_v} \right\} \right)^d = H_K(P)^d$$

Taking $[K:\mathbb{Q}]$-th root of both sides we obtain the desired result. $\square$

For $P = [x_0, \ldots, x_n]$ and $m \ge 1$, let $P^{(m)}$ be the point whose projective coordinates are all the monomials of degree m in the x_i, and $P^m = [x_0^m, \ldots, x_n^m]$. Let K be a number field such that $P^m \in \mathbb{P}^n(K)$. Then,

$$H_K(P^m) = \prod_{v \in M_K} \max \left\{ |x_0^m|_v^{n_v}, |x_1^m|_v^{n_v}, \ldots, |x_n^m|_v^{n_v} \right\} = \prod_{v \in M_K} \max_i \left\{ |x_i^m|_v^{n_v} \right\}$$
$$= \prod_{v \in M_K} \max_i \left\{ |x_i|_v^{n_v} \right\}^m = H_K(P)^m$$

Then, $H(P^{(m)}) = H(P^m) = H(P)^m$.

3. Heights and change of coordinates on $\mathbb{P}^n$

In the next few paragraphs we will consider what happens to the height of a point after a transformation ϕ. Let

$$\begin{aligned} \phi : \qquad & \mathbb{P}^n(K) \to \mathbb{P}^r(K) \\ & [x_0, \ldots, x_n] \to [\phi_o, \ldots, \phi_r] \end{aligned}$$

be a rational map such that ϕ_i are rational functions of degree m. Define **the height of the map** ϕ , denoted by $H(\phi)$, to be the height of a point P in the projective space, where P is the sequence of coefficients of all the ϕ_i's.

Denote by $\mathscr{Z}$ be the set of common zeroes for all ϕ_i's. Then ϕ is defined on $\mathbb{P}^n(\overline{\mathbb{Q}}) \setminus \mathscr{Z}$. We have the following:

Lemma 7 (Formula for changing coordinates)**.** *The following are true:*

i) Let ϕ be as above, and ϕ_i homogenous polynomials of degree m. Then for each point $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}}) \setminus \mathscr{Z}$ we have

$$H(\phi(P)) \le ||N||_\infty H(\phi) H(P)^m$$

where N is the maximum number of monomials appearing in any one of the ϕ_i, and

$$||N||_\infty = \prod_{v \in M_K^\infty} |N|_v^{n_v}$$

ii) Let X be a closed subvariety of $\mathbb{P}^n(\overline{\mathbb{Q}})$ with the property that $X \cap \mathscr{Z} = \emptyset$. Thus ϕ defines a morphism $X \to \mathbb{P}^r(\overline{\mathbb{Q}})$. Then for every $P = [x_0, \ldots, x_n] \in X$ we have

$$H(\phi(P)) = c_0 \cdot H(P)^m.$$

for some constant c_0.

Proof. Fix a field of definition K for ϕ, so $\phi_0, \dots, \phi_r \in K[X_0, \dots, X_n]$. We can write ϕ_i's as follows

$$\phi_i(X) = \sum_{\substack{j=(j_0,\dots,j_n)\in I \\ j_0+\cdots+j_n=m}} a_{i_j} X^j \quad \text{for all } 0 \le i \le r$$

where $X = X_0 X_1 \cdots X_n$ and $X^j = X_0^{j_0} \cdot X_1^{j_1} \cdots X_n^{j_n}$. For some $P = [x_0, \dots, x_n]$, we want to estimate $H(\phi(P))$ where $\phi(P) = (\phi_0(P), \dots, \phi_r(P))$.

$$\begin{aligned}
H_K(\phi(P)) &= \prod_{v\in M_K} \max\left\{ |\phi_0(P)|_v^{n_v}, \dots, |\phi_r(P)|_v^{n_v} \right\} = \prod_{v\in M_K} \max_{0\le i\le r} \left\{ |\phi_i(P)|_v^{n_v} \right\} \\
&= \prod_{v\in M_K} \max_{0\le i\le r} \left\{ \left| \sum_{\substack{j=(j_0,\dots,j_n)\in I \\ j_0+\cdots+j_n=m}} a_{i_j} x_0^{j_0} \cdot x_1^{j_1} \cdots x_n^{j_n} \right|_v^{n_v} \right\} \\
&\le \prod_{v\in M_K} N_v^{n_v} \cdot \max_{\substack{i,j_l \\ 0\le l\le n}} \left\{ \left| a_{i_{j_l}} x_0^{j_0} \cdot x_1^{j_1} \cdots x_n^{j_n} \right|_v^{n_v} \right\} \\
&\le \prod_{v\in M_K} N_v^{n_v} \cdot \max_{\substack{i,j_l \\ 0\le l\le n}} \left\{ |a_{i_{j_l}}|_v^{n_v} \right\} \cdot \max_{0\le l\le n} \left\{ |x_l|_v^{n_v} \right\}^m \\
&= ||N||_\infty \cdot H_K(\phi) \cdot H_K(P)^m
\end{aligned}$$

where N is the maximum number of monomials appearing in any one of the ϕ_i. Taking $[K:\mathbb{Q}]$-th root of both sides we obtain the desired result.

ii) In part (i) we proved that

$$H(\phi(P)) \le c_1 \cdot H(P)^m$$

where $c_1 = ||N||_\infty \cdot H(\phi)$, and it depends on ϕ but does not depend on the point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Now we want to show that for a point $P = [x_0, \dots, x_n] \in X(K)$ and a morphism $\phi = (\phi_0, \dots, \phi_r)$ on X the following holds

$$H(\phi(P)) \ge c_2 \cdot H(P)^m$$

Let $f_1, \dots, f_l$ be homogenous polynomials generating the ideal of X. Then, $f_1, \dots, f_l$, $\phi_0, \dots, \phi_r$ have no common zeros in $\mathbb{P}^n$. Let $\mathfrak{J} = \langle f_1, \dots, f_l, \phi_0, \dots, \phi_r \rangle$ and $\mathfrak{I} = \langle X_0, \dots, X_n \rangle$. From Nullstellensatz theorem we have that $\mathfrak{J}$ has a radical equal to $\mathfrak{I}$. Hence, for some polynomials $p_{i,j}, q_{i,j}$ and an exponent $t \ge m$ the following is true

$$p_{0,j}\phi_0 + \cdots + p_{r,j}\phi_r + q_{1,j} f_1 + \cdots + q_{l,j} f_l = X_j^t \qquad \text{for } 0 \le j \le n$$

Note that, since ϕ_i's have degree m then $p_{i,j}$'s have degree $t-m$. Extending K if necessary we can assume that $p_{i,j}$'s, and $q_{i,j}$'s have coefficients in K. Since $P \in X(K)$, then $f_i(P) = 0$, for all $0 \leq i \leq l$. Evaluating the above at the point P we have

$$p_{0,j}(P)\phi_0(P) + \cdots + p_{r,j}(P)\phi_r(P) = x_j^t, \qquad 0 \leq j \leq n$$

Hence,

$$\begin{aligned}
|P|_v^t &= \max_j \left\{ \, |x_j|_v^t \right\} = \max_j \left\{ \, |p_{0,j}(P)\phi_0(P) + \cdots + p_{r,j}(P)\phi_r(P)|_v \right\} \\
&\leq |r+1|_v \left(\max_{i,j} \left\{ \, |p_{i,j}(P)|_v \right\} \right) \left(\max_i \left\{ \, |\phi_i(P)|_x \right\} \right) \\
&\leq |r+1|_v \left(\left| \binom{t-m+n}{n} \right|_v |P|_v^{t-m} \max_{i,j} \left\{ \, |p_{i,j}|_v \right\} \right) \left(\max_i \left\{ \, |\phi_i(P)|_x \right\} \right)
\end{aligned}$$

Denoting by c_2 the following

$$c_2 = |r+1|_v \cdot \left| \binom{t-m+n}{n} \right|_v \cdot \max_{i,j} \left\{ \, |p_{i,j}|_v \right\}$$

and multiplying the above over all $v \in M_K$ and then taking $n_v/[K:\mathbb{Q}]$-th root we obtain

$$H(P)^t \leq c_2 \cdot H(P)^{t-m} H(\phi(P)).$$

This completes the proof. $\square$

Remark 1. *If the change of coordinates is done by an automorphism of $\mathbb{P}^n(K)$, say $M \in PGL_{n+1}(K)$, then*

$$H(P^M) \leq (n+1) \cdot H(M) \cdot H(P),$$

where $H(M)$ is

$$H(M) = \max\{a_{i,j}\},$$

for $1 \leq i \leq n+1$ and $1 \leq j \leq n+1$.

Part 2: Heights of polynomials

In this lecture we define the height of a polynomial. This is interesting to us since in the next section we will define the height of algebraic curves in terms of the height of a polynomial.

4. Heights of polynomials

Throughout this paper a polynomial with n variables will be denoted as follows

$$f(x_1,\dots,x_n) = \sum_{i=(i_1,\dots,i_n)\in I} a_i x_1^{i_1}\cdots x_n^{i_n}$$

where all $a_i \in K$, $I \subset \mathbb{Z}^{\geq 0}$, and I is finite. Let $\deg f$ denote the total degree of f. We will use lexicographic ordering to order the terms in a given polynomial, and $x_1 > x_2 > \cdots > x_n$.

The **(affine) multiplicative height of** f is defined as follows

$$H_K^{\mathbb{A}}(f) = \prod_{v\in M_K} \max\left\{ 1, |f|_v^{n_v} \right\}$$

where

$$|f|_v := \max_j \left\{ |a_j|_v \right\}$$

is called the **Gauss norm** for any absolute value v. The **(affine) logarithmic height of** f is defined to be

$$h_K^{\mathbb{A}}(f) = h_K([1,\dots,a_j,\dots]_{j\in I}).$$

Hence, the affine height of a polynomial is defined to be the height of its coefficients taken as affine coordinates. While, the **(projective) multiplicative height of a polynomial** is the height of its coefficients taken as coordinates in the projective space. Thus,

$$H_K(f) = \prod_{v\in M_K} |f|_v^{n_v}$$

and the **(projective) logarithmic height** is

$$h_K(f) = \sum_{v\in M_K} n_v \log|f|_v$$

The **(projective) absolute multiplicative height** is defined as follows

$$H : \mathbb{P}^n(\mathbb{Q}) \to [1,\infty)$$
$$H(f) = H_K(f)^{1/[K:\mathbb{Q}]},$$

and in the same way $h(f)$, $H^{\mathbb{A}}(f)$, $h^{\mathbb{A}}(f)$.

Example 3. *Let*

$$f(x,y) = 3x^3 + 3x^2 + 12xy + 6y^2 + 3y + 6.$$

Since $f(x,y)$ has integer coefficients the non-Archimedean absolute values give no contribution to the height, the (affine) height is

$$H^{\mathbb{A}}(3x^3 + 3x^2 + 12xy + 6y^2 + 3y + 6) = H^{\mathbb{A}}([1,3,3,12,6,3,6]) = 12.$$

The (projective) height is

$$H(3x^3 + 3x^2 + 12xy + 6y^2 + 3y + 6) = H([3,3,12,6,3,6]) = H(1,1,4,2,1,2) = 4.$$

Theorem 2. *Let be given $F(x,y) \in K[x,y]$. Then, there are only finitely many polynomials $G(x,y) \in K[x,y]$ such that $H_K(G) \leq H_K(F)$.*

Proof. Let

$$F(x,y) = \sum_{\substack{i=(i_1,i_2)\in I\\ i=i_1+i_2}} a_i x^{i_1} y^{i_2}$$

be a polynomial with coefficients in K and fix an ordering $x > y$. Let $H_K(F) = c$. By definition

$$H_K(F) = \prod_{v \in M_K} |f|_v^{n_v} = \prod_{v \in M_K} \max_i \left\{ \ |a_i|_v^{n_v} \right\} = H_K[a_0 \ldots, a_i, \ldots]_{i\in I}.$$

But, $P = [a_0 \ldots, a_i, \ldots]_{i\in I}$ is a point in $\mathbb{P}^s$ where s is the number of monomials of degree d in 2 variables. Hence, $s = \binom{d+1}{d}$.

From Theorem 1 we have that for any constant c the set

$$\{P \in \mathbb{P}^s(K) : H_K(P) \leq c\}$$

is finite. Hence there are finitely many polynomials $G(x,y)$ with content 1 corresponding to points P with height $H_K(G) \leq c = H_K(F)$. $\square$

Now we will study the height of the product of polynomials. At first we will deal with the case when the polynomials are in different variables, and then consider the case when they are polynomials in the same variable.

Proposition 1. *Let $f(x_0, \ldots, x_n)$ and $g(y_0, \ldots, y_n)$ be polynomials in different variables. Then, the projective height has the following property*

$$H(f \cdot g) = H(f) \cdot H(g)$$

Proof. The height of a polynomial is equal to the height of its coefficients in appropriate projective space. Let $H(f) = H(P)$, where $P \in \mathbb{P}^s$, and $H(g) = H(Q)$ for $Q \in \mathbb{P}^l$, where s, l is the number of monomials of f, g respectively. Then, $H(f \cdot g) = H(S_{s,l}(P, Q)) = H(P) \cdot H(Q)$ from Lemma 5. Therefore, $H(f \cdot g) = H(f) \cdot H(g)$. □

Before considering the height of polynomials in the same variables, we will consider $|f \cdot g|_v$. The following lemma is true for the product of a finite number of polynomials.

Lemma 8 (Gauss's lemma)**.** *Let K be a number field and $f, g \in K[x_1, \ldots, x_n]$. If v is not Archimedean, then $|fg|_v = |f|_v |g|_v$.*

The proof can be found in [6, pg. 22].

Gauss's lemma applies to all non-Archimedean absolute values but the Archimedean case is more complicated. An analogous Archimedean estimate is given by the following lemma. Gauss's lemma and the following are used to give an estimate of $H(f_1 f_2 \cdots f_r)$ in terms of $H(f_i)$ for $1 \leq i \leq r$ and $f_1, f_2, \ldots, f_r \in K[x_1, \ldots, x_n]$.

Lemma 9. *Let $f_1, f_2, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$. Denote by $f = f_1 \cdots f_r$ and $d_i = deg\ (f, x_i)$. Then, the following is true*

$$\prod_{i=1}^{r} |f_i|_v \leq e^{(d_1 + \cdots + d_n)} |f|_v. \tag{1}$$

The proof of this can be found in [9, pg. 232] and uses the concept of Mahler measure which is defined as follows.

Let $f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ be a polynomial in n variables. The **Mahler measure** of this polynomial is defined as follows

$$M(f) := \exp\left(\int_{\mathbb{T}^n} \log \left| f(e^{i\theta_1}, \ldots, e^{i\theta_n}) \right| d\mu_1 \cdots d\mu_n \right)$$

where $\mathbb{T}$ is the unit circle $\{e^{i\theta} | 0 \leq \theta \leq 2\pi\}$ equipped with the standard measure $d\mu = (1/2\pi) d\theta$

One of the most important properties of the Mahler measure is the multiplicative property.

$$M(fg) = M(f)M(g),$$

see [9, pg. 230] for proof.

The following is true for affine heights.

Lemma 10. *Let K be a number field and $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. Denote with deg f_j the total degree of f_j. Then the following are true*

i) The height of the product of $f_1, \cdots, f_r$ is bounded as follows

$$H^{\mathbb{A}}(f_1 f_2 \cdots f_r) \leq N \cdot \prod_{j=1}^{r} H^{\mathbb{A}}(f_j)$$

ii)The height of the sum of $f_1 + \cdots + f_r$ is bounded as

$$H^{\mathbb{A}}(f_1+f_2+\cdots+f_r) \leq \; r\cdot\prod_{j=1}^{r} H^{\mathbb{A}}(f_j).$$

iii) Suppose that $f_1,\ldots,f_r \in \mathscr{O}_K[x_1,\ldots,x_n]$ have coefficients in the ring of integers $\mathscr{O}_K$ of K. Then

$$H^{\mathbb{A}}(f_1+f_2+\cdots+f_r) \leq \; r\cdot \max_j \left\{ \; H^{\mathbb{A}}(f_j)\right\}^{[K:\mathbb{Q}]}.$$

This estimate is useful when K is fixed and r is large.

Proof. i) Let $i=(i_1,\ldots,i_n)$ and write f_j's as follows

$$f_j=\sum_i a_{ji}x_1^{i_1}\cdots x_n^{i_n}$$

for all $j=1,\ldots,r$. Then

$$\begin{aligned} f_1f_2\cdots f_r &= \left(\sum_i a_{1i}x_1^{i_1}\cdots x_n^{i_n}\right)\cdot\left(\sum_i a_{2i}x_1^{i_1}\cdots x_n^{i_n}\right)\cdots\left(\sum_i a_{ri}x_1^{i_1}\cdots x_n^{i_n}\right)\\ &=\sum_i\left(\sum_{i_1+\cdots+i_r=i} a_{1i_1}\cdot a_{2i_2}\cdots a_{ri_r}\right)x^i \end{aligned}$$

where $x^i=x_1^{i_1}\cdots x_n^{i_n}$. Then, for every $v\in M_K$ the Gauss norm is

$$|f_1f_2\cdots f_r|_v=\max_i\left\{\left|\sum_{i_1+\cdots+i_r=i} a_{1i_1}\cdot a_{2i_2}\cdots a_{ri_r}\right|_v\right\}.$$

Let N be an upper bound for the number of non-zero terms in the sums, and let

$$N_v=\begin{cases} N & \text{if } v \text{ is Archimedean}\\ 1 & \text{if } v \text{ is non-Archimedean}\end{cases}$$

Then,

$$\begin{aligned} |f_1f_2\cdots f_r|_v &\leq \max_i\left\{\sum_{i_1+\cdots+i_r=i}|a_{1i_1}\cdot a_{2i_2}\cdots a_{ri_r}|_v\right\}\\ &\leq \max_i\left\{N_v\cdot \max_{\substack{i_j\\ i_1+\cdots+i_r=i}}\left\{\;|a_{1i_1}\cdots a_{ri_r}|_v\right\}\right\}\\ &\leq N_v\prod_{j=1}^{r}\max_{i_j}\left\{\;1,|a_{ji_j}|_v\right\}\leq N_v\prod_{j=1}^{r}\max_j\left\{\;1,|f_j|_v\right\}. \end{aligned}$$

Raising to the n_v power and taking the product over all valuations $v\in M_K$ we have the following

$$H_K^{\mathbb{A}}(f_1\cdots f_r) = \prod_{v\in M_K} \max\left\{ 1, |f_1\cdots f_r|_v^{n_v} \right\} \leq \prod_{v\in M_K} \left\{ N_v \prod_{j=1}^{r} \max_j \left\{ 1, |f_j|_v \right\} \right\}^{n_v}$$

$$\leq N^{[K:\mathbb{Q}]} \prod_{j=1}^{r} H_K(f_j), \qquad \left(\text{since} \sum_{v\in M_K^\infty} n_v = [K:\mathbb{Q}] \right)$$

Taking $[K:\mathbb{Q}]$-th root we obtain the desired result.

ii) Let f_j be as above. Then,

$$f_1+\cdots+f_r = \sum_{(i_1,\ldots,i_n)=i} (a_{1i}+\cdots+a_{ri})x^i$$

Thus, for every absolute value $v\in M_K$,

$$|f_1+\cdots+f_r|_v = \max_i \left\{ |a_{1i}+\cdots+a_{ri}|_v \right\}.$$

Letting,

$$r_v = \begin{cases} r & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

we have

$$|f_1+\cdots+f_r|_v \leq r_v \max_{j,i} \left\{ 1, |a_{ji}|_v \right\} \qquad (\text{ for } j,i \text{ as above})$$

$$\leq r_v \prod_{j=1}^{r} \max_i \left\{ 1, |a_{ji}|_v \right\}.$$

Raising to the $n_v/[K:\mathbb{Q}]$ power and taking the product over all valuations $v\in M_K$ we have the following

$$H^{\mathbb{A}}(f_1+\cdots+f_r) \leq r \prod_{j=1}^{r} H^{\mathbb{A}}(f_j).$$

And we are done.

iii) We have that $f_1,\ldots,f_r$ have coefficients in the ring of integers $\mathcal{O}_K$ of K. Then, $f_1+\cdots+f_r$ will have integer coefficients as well. Hence, for any non-Archimedean absolute value v, and any j we have that $|f_j|_v \leq 1$ and therefore the following is true

$$\max\left\{ 1, |f_1+\cdots+f_r|_v \right\} = \max\left\{ 1, |f_1|_v \right\} = \cdots = \max\left\{ 1, |f_r|_v \right\} = 1.$$

Hence the non-Archimedean absolute values do not contribute to $H_K(f_1+\cdots+f_r)$, and we have

$$
\begin{aligned}
H_K^{\mathbb{A}}(f_1+\cdots+f_r) &= \prod_{v\in M_k^\infty} \max\left\{ 1, |f_1+\cdots+f_r|_v^{n_v} \right\} \\
&\le \prod_{v\in M_k^\infty} r\cdot \max_{1\le j\le r}\left\{ 1, |f_j|_v^{n_v} \right\}, \qquad \text{from absolute value properties} \\
&\le r^{[K:\mathbb{Q}]}\cdot \max_{1\le j\le r}\left\{ \max_{v\in M_K^\infty}\left\{ 1, |f_j|_v^{n_v} \right\}^{[K:\mathbb{Q}]} \right\}, \qquad \text{since } \#M_K^\infty \le [K:\mathbb{Q}] \\
&\le r^{[K:\mathbb{Q}]}\cdot \max_{1\le j\le r}\left\{ H_K^{\mathbb{A}}(f_j)^{[K:\mathbb{Q}]} \right\}
\end{aligned}
$$

Taking $[K:\mathbb{Q}]$-th root of both sides we obtain the desired result. □

The converse inequality for the inequality in part (i) is known as Gelfand's inequality. This inequality is true if we use projective polynomial heights.

Lemma 11 (Gelfand's inequality)**.** *Let $f_1,\dots,f_r \in \overline{\mathbb{Q}}[x_1,\dots,x_n]$ be polynomials, with degree $d_1,\dots,d_r$ respectively, such that deg $(f_1\cdots f_r, x_i) \le d_i$ for each $1\le i\le r$. Then*

$$
\prod_{i=1}^r H(f_i) \le e^{(d_i+\cdots+d_n)}\cdot H(f_1\cdots f_r).
$$

Proof. From Lemma 9 the following is true

$$
\prod_{i=1}^r |f_i|_v \le e^{(d_1+\cdots+d_n)}|f|_v. \tag{2}
$$

Then, assuming the above we have

$$
\begin{aligned}
\prod_{i=1}^r H_K(f_i) &= \prod_{i=1}^r \prod_{v\in M_K} |f_i|_v^{n_v} = \prod_{v\in M_K}\prod_{i=1}^r |f_i|_v^{n_v} = \prod_{v\in M_K}\left(|f_1|_v^{n_v}|f_2|_v^{n_v}\cdots|f_r|_v^{n_v}\right) \\
&\le \prod_{v\in M_K^0} |f_1\cdots f_r|_v^{n_v}\cdot \prod_{v\in M_K^\infty} e^{n_v(d_1+\cdots+d_n)}|f_1\cdots f_r|_v^{n_v} \\
&\le e^{[K:\mathbb{Q}](d_1+\cdots+d_n)} H_K(f_1\cdots f_r).
\end{aligned}
$$

Taking $[K:\mathbb{Q}]$-th root of both sides we obtain Gelfand's inequality. □

Lemma 12. *Let K be a number field, v an absolute value on K, and $f\in K[x_1,\dots,x_n]$ a polynomial. Then,*

$$
\left|\frac{\partial f}{\partial x_j}\right|_v \le |deg\ f|_v\cdot |f|_v.
$$

Proof. Let the polynomial f be as follows

$$
f(x_1,\dots,x_n) = \sum_{i=(i_1,\dots,i_n)\in I} a_i x_1^{i_1}\cdots x_n^{i_n}.
$$

Then every coefficient of $\partial f/\partial x_j$ has the form $c\cdot a_i$ for some positive integer $c\le \deg f$ and some multi index i. Therefore,

$$\left|\frac{\partial f}{\partial x_j}\right|_v \leq \max_i \left\{ \max_{c \leq \deg f} \left\{ |c a_i|_v \right\} \right\} = |\deg f|_v \cdot |f|_v.$$

This completes the proof. $\square$

Let $b = (b_1, \ldots, b_n) \in K^n$. Denote with $|b|_v = \max\left\{ |b_i|_v \right\}$.

Lemma 13. *Let K be a number field, $f \in K[x_1, \ldots, x_n]$ a polynomial of degree d, and $b = (b_1, \ldots, b_n) \in K^n$. Then,*

$$|f(b)|_v \leq \min\left\{ |2d|_v^n, |2|_v^d \right\} \cdot \max\{1, |b|_v\}^d \cdot |f|_v.$$

The prof can be found in [9, pg. 236].

Next we will consider bounds for the Gauss norm of a polynomial $f(x) \in K[x_1, \ldots, x_n]$, first when we shift $x = (x_1, \ldots, x_n)$ with a vector $b = (b_1, \ldots, b_n) \in K^n$, then when we multiply x with $u = (u_1, \ldots, u_n)$, and then when we combine them.

Let $b = (b_1, \ldots, b_n) \in K^n$, $|b|_v$ as above, and define a **shifted polynomial** as follows

$$f_b(x) = f(x+b) = f(x_1 + b_1, \ldots, x_n + b_n).$$

Lemma 14. *Let K be a number field, $f \in K[x_1, \ldots, x_n]$ such that $\deg f = d$. The following statements are true.*

i) Let $b = (b_1, \ldots, b_n) \in K^n$ and $|b|_v$ as above. The height of the shifted polynomial $f_b(x)$ is bounded by

$$|f_b(x)|_v \leq |2|_v^{2d} \cdot \max\{1, |b|_v\}^d \cdot |f|_v. \tag{3}$$

ii) Let $u = (u_1, \ldots, u_n)$ and define $f_u(x) = f(u \cdot x) = f(u_1 x_1, \ldots, u_n x_n)$. Then,

$$|f_u(x)|_v \leq \max\{1, |u|_v\}^d \cdot |f|_v.$$

iii) For b, and u as above define $f(ux+b) = f(u_1 x_1 + b_1, \ldots, u_n x_n + b_n)$. Then,

$$|f(ux+b)|_v \leq |2|_v^{2\deg f} \cdot \max\{1, |u|_v\}^d \cdot \max\{1, |b|_v\}^d \cdot |f|_v.$$

Proof. i) Let

$$f(x_1, \ldots, x_n) = \sum_{i=(i_1,\ldots,i_n)\in I} a_i x_1^{i_1} \cdots x_n^{i_n}.$$

and compute

$$\begin{aligned}
f_b(x) &= \sum_i a_i (x+b)^i \\
&= \sum_i a_i \left(\sum_{j_1=0}^{i_1} \binom{i_1}{j_1} x_1^{j_1} b^{i_1 - j_1} \right) \cdots \left(\sum_{j_n=0}^{i_n} \binom{i_n}{j_n} x_n^{j_n} b^{i_n - j_n} \right) \\
&= \sum_{j_1=0}^{d_1} \cdots \sum_{j_n=0}^{d_n} \left(\sum_{\substack{i_1,\ldots,i_n \\ j_l \leq i_l \leq d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} \times b_1^{i_1 - j_1} \cdots b_n^{i_n - j_n} \right) \times x_1^{j_1} \cdots x_n^{j_n}
\end{aligned}$$

Then, for every $v \in M_K$ the Gauss norm is

$$\left| f_b(x) \right|_v = \max_{\substack{j_1,\ldots,j_n \\ 0\le j_l\le d_l}} \left| \sum_{\substack{i_1,\ldots,i_n \\ j_l\le i_l\le d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1-j_1} \cdots b_n^{i_n-j_n} \right|_v .$$

If we denote by N be number of the terms in the last sum, then N is at most $\prod_{l=1}^n (d_l + 1) \le \prod_{l=1}^n 2^{d_l} = 2^d$. Estimate the binomial coefficients we have,

$$\binom{i_1}{j_1} \cdots \binom{i_n}{j_n} \le 2^{i_1} \cdots 2^{i_n} = 2^{i_1+\cdots+i_n} \le 2^{d_1\cdots d_n} = 2^d$$

Letting

$$N_v = \begin{cases} N \le 2^d & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

and using the above estimates we have

$$\begin{aligned}
\left| f_b(x) \right|_v &= \max_{\substack{j_1,\ldots,j_n \\ 0\le j_l\le d_l}} \left\{ \left| \sum_{\substack{i_1,\ldots,i_n \\ j_l\le i_l\le d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1-j_1} \cdots b_n^{i_n-j_n} \right|_v \right\}. \\
&\le N_v \cdot \max_{i,j} \left\{ 1, \left| a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1-j_1} \cdots b_n^{i_n-j_n} \right|_v \right\}. \\
&\le N_v \cdot 2_\infty^d \cdot \max\{1, |b_1^{i_1-j_1} \cdots b_n^{i_n-j_n}|_v\} \cdot \max\{|a_i|_v\} \\
&\le 2_\infty^{2d} \cdot \max\{1, |b_1|_v^{i_1-j_1}\} \cdots \max\{1, |b_n|_v^{i_n-j_n}\} \cdot \max\{|a_i|_v\} \\
&\le 2_\infty^{2d} \cdot \max\{1, |b_1|_v^d\} \cdots \max\{1, |b_n|_v^d\} \cdot \max\{|a_i|_v\} \\
&= 2_\infty^{2d} \cdot \max\{1, |b|_v^d\} \cdot |f|_v.
\end{aligned}$$

This completes the proof.

ii) Let us evaluate

$$\begin{aligned}
f_u(x) &= f(u_1 \cdot x_1, \ldots, u_n \cdot x_n) \\
&= \sum_{i=(i_1,\ldots,i_n)\in I} a_i (u_1 x_1)^{i_1} \cdots (u_n x_n)^{i_n} \\
&= \sum_{i=(i_1,\ldots,i_n)\in I} a_i \cdot (u_1^{i_1} \cdots u_n^{i_n}) \cdot (x_1^{i_1} \cdots x_n^{i_n})
\end{aligned}$$

Then, for every $v \in M_K$ the Gauss norm is

$$
\begin{aligned}
|f_u(x)|_v &= \max_i \left\{ \, |a_i u_1^{i_1} \cdots u_n^{i_n}|_v \right\} \\
&\leq \max_i \left\{ \, |a_i|_v \right\} \cdot \max \left\{ \, 1, |u_1^{i_1} \cdots u_n^{i_n}|_v \right\} \\
&\leq \max_i \left\{ \, |a_i|_v \right\} \cdot \max \left\{ \, 1, |u_1|_v^d \right\} \cdots \max \left\{ \, 1, |u_n|_v^d \right\} \\
&= \max\{1, |u|_v\}^d \cdot |f|_v.
\end{aligned}
$$

iii) Combining part (i) and (ii) we have the following

$$
\begin{aligned}
|f(u \cdot x + b)|_v &\leq 2_\infty^{2d} \cdot \max\{1, |b|_v\}^d \cdot |f_u(x)|_v \\
&\leq 2_\infty^{2d} \cdot \max\{1, |b|_v\}^d \cdot \max\{1, |u|_v\}^d \cdot |f|_v,
\end{aligned}
$$

□

Remark 2. *If we convert the above bounds into bounds for heights we have the following.*

i) $H(f_b(x)) \leq 4^d \cdot H(b)^d \cdot H(f)$
ii) $H(f_u(x)) \leq H(u)^d \cdot H(f)$
iii) $H(f(ux+b)) \leq 4^d \cdot H(u)^d \cdot H(b)^d \cdot H(f)$

Proof. We prove i) and then the rest follows in the same way. Raising Eq. (4) to the n_v power and taking the product over all valuations we have

$$
\begin{aligned}
H_K(f_b(x)) &= \prod_{v \in M_K} |f_b(x)|_v^{n_v} \\
&\leq \prod_{v \in M_K} \left(\, 2_\infty^{2d} \cdot \max\{1, |b|_v^d\} \cdot |f|_v \right)^{n_v} \\
&\leq 2^{2d^2} \cdot H_K(b)^d \cdot H_K(f)
\end{aligned}
$$

Now, taking $[K : \mathbb{Q}]$-th root of both sides we obtain

$$
H(f_b(x)) \leq 4^d \cdot H(b)^d \cdot H(f).
$$

□

4.1. Homogenous polynomials

Next we focus on homogenous polynomials. The following lemma gives a bound for the homogenous polynomial evaluated at a point.

Lemma 15. *Let K be a number field, $f \in K[x_0, \ldots, x_n]$ a homogenous polynomial of degree d, and $\alpha = (\alpha_0, \ldots, \alpha_n) \in \overline{K}^{n+1}$. Then, the following hold:*

i) $|f(\alpha)|_v \leq |c(d,n)|_v \cdot \max_j \left\{ \, |\alpha_j|_v \right\}^d \cdot |f|_v$*, where* $|c(d,n)|_v$ *is* $\binom{n+d}{d}$ *is v is non-Archimedean and 1 otherwise.*

ii) $H(f(\alpha)) \leq c_0 \cdot H(\alpha)^d \cdot H(f)$.

Proof. Write f as follows

$$f(x_0,\dots,x_n)=\sum_{\substack{i_0+\dots+i_n=d\\ i=(i_0,\dots,i_n)}} a_i x_0^{i_0}\cdots x_n^{i_n}.$$

Let v be an absolute value on K, extended in some way to $\overline{K}$. Since f is a homogenous polynomial in n variables of degree d, then the number of terms of f is at most the number of monomials of degree d in $n+1$ variables, and this is equal to $\binom{n+d}{n}$. We want to evaluate $H(f(\alpha))$.
Let

$$|c(d,n)|_v=\begin{cases}\binom{n+d}{n} & \text{if } v \text{ is Archimedean}\\ 1 & \text{if } v \text{ is non-Archimedean}\end{cases}$$

then, the Gauss's norm is

$$\begin{aligned}|f(\alpha)|_v &= \left|\sum_i a_i\alpha_0^{i_0}\cdots\alpha_n^{i_n}\right|_v \qquad i=(i_0,\dots,i_n) \text{ and } i_0+\dots+i_n=d\\ &\le |c(d,n)|_v\cdot\max_i\left\{\,|a_i\alpha_0^{i_0}\cdots\alpha_n^{i_n}|_v\right\}\\ &\le |c(d,n)|_v\cdot\max_j\left\{\,|\alpha_j|_v\right\}^d\cdot\max_i\left\{\,|a_i|_v\right\}\end{aligned}$$

So we conclude,

$$|f(\alpha)|_v\le|c(d,n)|_v\cdot\max_j\left\{|\alpha_j|_v\right\}^d\cdot|f|_v.$$

Taking the product over all absolute values of K, and then $[K:\mathbb{Q}]$-th root of both sides we get the inequality

$$H(f(\alpha))\le c_0\cdot H(\alpha)^d\cdot H(f)$$

and c_0 can be bounded as

$$c_0=\binom{n+d}{n}\le\min\left\{(n+d)^n,2^{n+d}\right\}.$$

□

In the next session we will use Lemma 15 to determine the height of the $SL_2(K)$ invariants of binary forms.

Corollary 1. *Let K be a number field, $f\in K[x,z]$ a homogenous polynomial of degree d as follows*

$$y=f(x,z)=a_dx^d+a_{d-1}x^{d-1}z+\dots+a_0z^d,$$

and let $\alpha = (\alpha_0, \alpha_1) \in \overline{K}^2$. *Then,*

$$H(f(\alpha)) \leq \min\left\{d+1, 2^{d+1}\right\} \cdot H(\alpha)^d \cdot H(f).$$

5. Heights on binary forms

In this section we use some of the results of the heights on polynomials to study heights on binary forms.

In this section we define the action of $GL_2(k)$ on the space of binary forms and discuss the basic notions of their invariants. Most of this section is a summary of section 2 in [10]. Throughout this section k denotes an algebraically closed field.

Let $k[X,Z]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $k[X,Z]$ consisting of homogeneous polynomials.

$$f(X,Z) = a_0 X^d + a_1 X^{d-1} Z + \cdots + a_d Z^d \tag{4}$$

of degree d. Elements in V_d are called **binary forms of degree** d.

Since k is algebraically closed, the binary form $f(X,Z)$ can be factored as

$$f(X,Z) = (z_1 X - x_1 Z) \cdots (z_d X - x_d Z) = \prod_{1 \leq i \leq d} det \begin{pmatrix} X & x_i \\ Z & z_i \end{pmatrix} \tag{5}$$

The points with homogeneous coordinates $(x_i, z_i) \in \mathbb{P}^1(k)$ are called the **roots of the binary form** in Eq. (4).

5.1. *Action of* $GL_2(k)$ *on binary forms.*

We let $GL_2(k)$ act as a group of automorphisms on $k[X,Z]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \ then \quad M \begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix}. \tag{6}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d. Let $A_0, A_1, \ldots, A_d$ be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, ..., A_d]$. For $I \in k[A_0, ..., A_d]$ and $M \in GL_2(k)$, define $I^M \in k[A_0, ..., A_d]$ as follows

$$I^M(f) := I(M(f)) \tag{7}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (7) defines an action of $GL_2(k)$ on $k[A_0, ..., A_d]$.

Remark 3. *It is well known that* $SL_2(k)$ *leaves a bilinear form (unique up to scalar multiples) on* V_d *invariant. This form is symmetric if* d *is even and skew symmetric if* d *is odd.*

Definition 1. *Let* $\mathscr{R}_d$ *be the ring of* $SL_2(k)$ *invariants in* $k[A_0, \ldots, A_d]$*, i.e., the ring of all* $I \in k[A_0, \ldots, A_d]$ *with* $I^M = I$ *for all* $M \in SL_2(k)$.

Note that if I is an invariant, so are all its homogeneous components. So $\mathscr{R}_d$ is graded by the usual degree function on $k[A_0, \dots, A_d]$.

Thus, for $M \in GL_2(k)$ we have

$$M(f(X,Y)) = (det(M))^d (z_1' X - x_1' Z) \cdots (z_d' X - x_d' Z).$$

where

$$\begin{pmatrix} x_i' \\ z_i' \end{pmatrix} = M^{-1} \begin{pmatrix} x_i \\ z_i \end{pmatrix} \tag{8}$$

Theorem 3. *[Hilbert's Finiteness Theorem] $\mathscr{R}_d$ is finitely generated over k.*

A homogeneous polynomial $I \in k[A_0, \dots, A_d, X, Y]$ is called a **covariant** of index s if

$$I^M(f) = \delta^s I(f)$$

where $\delta = \det(M)$. The homogeneous degree in $A_1, \dots, A_n$ is called the **degree** of I, and the homogeneous degree in X, Z is called the **order** of I. A covariant of order zero is called **invariant**. An invariant is a $SL_2(k)$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$\begin{aligned} f(X,Z) &:= \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \\ g(X,Z) &:= \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i \end{aligned} \tag{9}$$

be binary forms of degree n and m respectively in $k[X,Z]$. We define the **r-transvection**

$$(f,g)^r := c_k \cdot \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k} \, \partial Z^k} \cdot \frac{\partial^r g}{\partial X^k \, \partial Z^{r-k}} \tag{10}$$

where $c_k = \frac{(m-r)!\,(n-r)!}{n!\,m!}$. It is a homogeneous polynomial in $k[X,Z]$ and therefore a covariant of order $m+n-2r$ and degree 2. In general, the r-transvection of two covariants of order m,n (resp., degree p,q) is a covariant of order $m+n-2r$ (resp., degree $p+q$).

For the rest of this paper $F(X,Z)$ denotes a binary form of order $d := 2g+2$ as below

$$F(X,Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{11}$$

where $b_i = \frac{(n-i)!\,i!}{n!} \cdot a_i$, for $i = 0, \dots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order). $GL_2(k)$-invariants are called **absolute invariants**. They are given as ratios of $SL_2(k)$-invariants where the numerator and denominator have the same degree.

Two binary forms f and f' of the same degree d are called **equivalent** or $GL_2(k)$-conjugate if there is an $M \in GL_2(k)$ such that $f' = f^M$.

The main goal of this section is to determine how the height of f^M changes for any given $M \in GL_2(k)$.

Lemma 16. *Let f be a degree n binary form*

$$f(x,z) = \sum_{i=0}^{n} a_i x^i z^{n-i}$$

and $a,b,c,d \in K$ such that $ad - bc \neq 0$. Then the following is true

$$\left| f^M \right|_v \leq 2_v^n \cdot c(n)_v \cdot \max\left\{ 1, |M|_v \right\}^n \cdot |f|_v.$$

Proof. Let us first evaluate $f(ax+bz, cx+dz)$, where $f(x,z)$ is given and $a,b,c,d \in K^n$

$$\begin{aligned}
f^M &= \sum_{i=0}^{n} a_i (ax+bz)^i (cx+dz)^{n-i} \\
&= \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{i} \binom{i}{k} (ax)^k (bz)^{i-k} \right) \cdot \left(\sum_{l=0}^{n-i} \binom{n-i}{l} (cx)^l (dz)^{n-i-l} \right) \\
&= \sum_{\substack{k+l \leq n \\ 0 \leq k \leq n \\ 0 \leq l \leq n}} \left(\sum_{k \leq i \leq n-l} a_i \binom{i}{k} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right) \cdot x^{k+l} \cdot z^{n-(k+l)}
\end{aligned}$$

Now let us estimate the Gauss's norm for this polynomial.

$$\left| f^M \right|_v = \max_{\substack{k,l \\ 0 \leq k \leq n \\ 0 \leq l \leq n}} \left| \sum_{k \leq i \leq n-l} a_i \binom{i}{k} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right|_v$$

Let us denote the maximum number of terms in the sum with $c(n)$. Then $c(n) \leq n+1$. Estimating the binomial coefficients we have

$$\binom{i}{k} \binom{n-i}{l} \leq 2^i \cdot 2^{n-i} = 2^n$$

Denote by $|M|_v = \max\left\{ |a|_v, |b|_v, |c|_v, |d|_v \right\}$. Using these observations and notation we obtain the following estimation

$$
\begin{aligned}
\left| f^M \right|_v &\leq c(n)_v \cdot \max_{i,k,l} \left\{ 1, \left| a_i \binom{i}{k} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right|_v \right\} \\
&\leq c(n)_v \cdot 2_v^n \cdot \max_{0 \leq i \leq n} \left\{ |a_i|_v \right\} \max_{0 \leq k,l \leq n} \left\{ 1, |a^k b^{i-k} c^l d^{n-i-l}|_v \right\} \\
&\leq 2_v^n \cdot c(n)_v \cdot \max_i \left\{ |a_i|_v \right\} \max_{k,l} \left\{ 1, |a|_v^k |b|_v^{i-k} |c|_v^l |d|_v^{n-i-l} \right\} \\
&\leq 2_v^n \cdot c(n)_v \cdot \max_i \left\{ |a_i|_v \right\} \max \left\{ 1, |a|_v^i |b|_v^i |c|_v^{n-i} |d|_v^{n-i} \right\} \\
&\leq 2_v^n \cdot c(n)_v \cdot \max \left\{ 1, |M|_v \right\}^n \cdot |f|_v
\end{aligned}
$$

where $c(n)_v$ and 2_v are respectively $n+1$ and 2 when v is Archimedean, and 1 otherwise. □

Theorem 4. *Let $M \in GL_2(K)$ and $f(x,z) \in K[x,z]$ be a degree d binary form and $H(f)$ denote the absolute height of f. Then,*

$$
H(f^M) \leq 2^n \cdot (n+1) \cdot H(M)^n \cdot H(f)
$$

Proof. From Lemma 16 for each $v \in M_k$ we have that

$$
\left| f^M \right|_v \leq 2_v^n \cdot c(n)_v \cdot \max \left\{ 1, |M|_v \right\}^n \cdot |f|_v.
$$

Taking the product for all valuations we obtain

$$
\begin{aligned}
H_K(f^M) &= \prod_{v \in M_K} \left| f^M \right|_v^{n_v} \\
&\leq \prod_{v \in M_K} \left(2_v^n \cdot c(n)_v \cdot \max \left\{ 1, |M|_v \right\}^n \cdot |f|_v \right)^{n_v} \\
&\leq 2^{n[K:\mathbb{Q}]} \cdot (n+1)^{[K:\mathbb{Q}]} \cdot H_K(M)^n \cdot H_K(f)
\end{aligned}
$$

Taking $[K:\mathbb{Q}]$-th root we obtain the desired result. □

Next we follow a different approach. First this technical lemma.

Lemma 17. *Let K be an algebraic number field, and $f \in K[x,z]$ a degree d binary form given as follows*

$$
f(x,z) = \sum_{i=0}^{d} b_i x^{d-i} z^i.
$$

and

$$
f(u\bar{x} + w, \bar{z}) = \sum_{i=0}^{d} \bar{b}_i \bar{x}^{d-i} \bar{z}^i.
$$

for $u, w \in K$. Then

$$\bar{b}_i = \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!\,(d-i+k)!}{k!\,d!} b_{i-k} w^k.$$

Proof. We have that

$$f(x,z) = \sum_{i=0}^{d} b_i x^{d-i} z^i = \sum_{i=0}^{d} a_i \binom{d}{i} x^{d-i} z^i.$$

and

$$f(u\bar{x}+w,\bar{z}) = \sum_{i=0}^{d} \bar{b}_i \bar{x}^{d-i} \bar{z}^i = \sum_{i=0}^{d} \bar{a}_i \binom{d}{i} \bar{x}^{d-i} \bar{z}^i.$$

where $\bar{a}_i = u^{d-i} \sum_{k=0}^{i} \binom{i}{k} a_{i-k}\, w^k$. Then,

$$\begin{aligned}
\bar{b}_i = \binom{d}{i} \bar{a}_i &= \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \binom{i}{k} a_{i-k}\, w^k \\
&= \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \binom{i}{k} \frac{1}{\binom{d}{i-k}} b_{i-k} w^k = \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!(d-i+k)!}{k!d!} b_{i-k} w^k
\end{aligned}$$

□

Theorem 5. *Let K be an algebraic number field, and $f, \bar{f}$ as above. The following are true:*

i) For any valuation $v \in M_K$ we have

$$|\bar{f}|_v \leq 2_v^d \cdot c(d)_v \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{0 \leq i \leq d} \left\{ \, |b_i|_v \right\}$$

ii)

$$H(\bar{f}) \leq (d+1) \cdot 2^d \cdot u^d \cdot w^d \cdot H(f)$$

Proof. i) For any valuation $v \in M_K$ we have the following

$$\begin{aligned}
|f(ux+w,z)|_v &= \max_{0 \leq i \leq d} \left\{ \, |b_i|_v \right\} \\
&= \max_{0 \leq i \leq d} \left\{ \, \left| \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!(d-i+k)!}{k!d!} b_{i-k} w^k \right|_v \right\} \\
&\leq c(d)_v \cdot \max_{0 \leq i \leq d} \left\{ \, \left| \binom{d}{i} \frac{i!(d-i+k)!}{k!d!} u^{d-i} b_{i-k}\, w^k \right|_v \right\} \\
&= c(d)_v \cdot \max_{0 \leq i \leq d} \left\{ \, \left| \binom{d+k-i}{k} u^{d-i}\, w^k\, b_{i-k} \right|_v \right\} \\
&\leq c(d)_v \cdot 2^d \cdot \max_{0 \leq i \leq d} \left\{ \, 1, \left| u^{d-i}\, w^k\, b_{i-k} \right|_v \right\} \\
&\leq c(d)_v \cdot 2^d \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{i} \left\{ \, 1, |b_i|_v \right\}
\end{aligned}$$

where $c(d)$ is the number of terms in the sum, and $c(d)_v$ is equal to $d+1$ when v is Archimedean and 1 otherwise.

ii) Taking the product over all valuations $v \in M_K$ we have the following

$$
\begin{aligned}
H_K(f(ux+w,z)) &= \prod_{v \in M_K} |f(ux+w,z)|_v^{n_v} \\
&\leq \prod_{v \in M_K} \left(2_v^d \cdot c(d)_v \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{0 \leq i \leq d} \left\{ |b_i|_v \right\} \right)^{n_v} \\
&= \left(2^d \cdot (d+1) \cdot u^d \cdot w^d \right)^{[K:\mathbb{Q}]} \prod_{v \in M_K} \max_{0 \leq i \leq d} \left\{ |b_i|_v \right\}^{n_v} \\
&= \left(2^d \cdot (d+1) \cdot u^d \cdot w^d \right)^{[K:\mathbb{Q}]} \cdot H_K(f)
\end{aligned}
$$

Taking $[K:\mathbb{Q}]$-th root of both sides gives the desired result. $\square$

6. Minimal and moduli heights of forms

Let $f(x,y)$ be a binary form and $Orb(f)$ its $GL_2(K)$-orbit in V_d. Let $H(f)$ be the height of f as defined in the previous section.

Remark 4. *There are only finitely many $f' \in Orb(f)$ such that $H(f') \leq H(f)$.*

Define the height of the binary form $f(x,y)$ as follows

$$
\tilde{H}(f) := \min \left\{ H(f') | f' \in Orb(f), H(f') \leq H(f) \right\}
$$

we want to consider the following problem. For every f let f' be the binary form such that $f' \in Orb(f)$ and $\tilde{H}(f) = H(f')$. Determine a matrix $M \in GL_2(K)$ such that $f' = f^M$.

6.1. Moduli height of a binary form

Let $\mathscr{B}_d$ be the moduli space of degree d binary forms defined over an algebraically closed field k. Then $\mathscr{B}_d$ is a quasi-projective variety with dimension $d-3$. We denote the equivalence class of f by $\mathfrak{f} \in B_d$. The **moduli height** of $f(x,z)$ is defined as

$$
\mathfrak{H}(f) = H(\mathfrak{f})
$$

where $\mathfrak{f}$ is considered as a point in the projective space $\mathbb{P}^{d-3}$. A natural question would be to investigate if the minimal height $\tilde{H}(f)$ has any relation to the moduli height $\mathfrak{H}(f)$.

Let $\left\{ I_{i,j} \right\}_{j=1}^{j=s}$ be a basis of $\mathscr{R}_d$. Here the subscript i denotes the degree of the homogenous polynomial $I_{i,j}$. The fixed field of invariants is the space $V_d^{GL_2(K)}$ and is generated by rational functions $t_1, \ldots t_r$ where each of them is a ratio of polynomials in $I_{i,j}$ such that the combined degree of the numerator is the same as that of the denominator.

Lemma 18. *For any $SL_2(k)$-invariant I_i of degree i we have that*

$$H\left(I_i(f)\right) \leq c \cdot H(f)^d \cdot H(I_i)$$

Proof. $I_i(f)$ is a homogenous polynomial of degree i evaluated at f. Then the result follows from Lemma 15. The constant c represents the number of monomials of $I_i(f)$. $\square$

Theorem 6. *Let f be a binary form. Then,*

$$\mathfrak{H}(f) \leq c \cdot \tilde{H}(f),$$

for some constant c.

Proof. Let $\left\{I_{i,j}\right\}_{j=1}^{j=s}$ be a basis of $\mathscr{R}_d$. Here the subscript i denotes the degree of the homogenous polynomial $I_{i,j}$. The fixed field of invariants is the space $V_d^{GL_2(K)}$ and is generated by rational functions $t_1, \dots t_r$ where each of them is a ratio of polynomials in $I_{i,j}$ such that the combined degree of the numerator is the same as that of the denominator.

Without loss of generality we can assume that f has minimal height. So $H(f) = \tilde{H}(f)$. Let $d_1, \dots, d_r$ denote the degrees of each $t_1, \dots, t_r$ respectively. Then,

$$\mathfrak{H}(f) = H[t_1(f), \dots, t_r(f), 1] = \prod \max\{|t_i(f)|_v\}_{i=1}^{i=r}.$$

By reordering, we can assume that

$$\mathfrak{H}(f) = |t_1(f)|_{v_1} \cdots |t_m(f)|_{v_m}$$

However, for each $j = 1, \dots m$, we have

$$|t_j(f)|_{v_j} \leq H(t_j) \cdot H(f),$$

where $H(t_j)$ is a fixed constant. This completes the proof. $\square$

Remark 5. *Notice that for a given degree d the constant c of the theorem can be explicitly computed. See for example the case of binary sextics in Section 9.1, where this constant is*

$$c = 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$$

Part 3: Heights of algebraic curves

In this lecture we focus on heights of algebraic curves. Our main focus is in providing equations for the algebraic curves with ”small” coefficients as continuation of our previous work [2, 5, 17, 18, 21]. Hence, the concept of height is the natural concept to be used. For a genus $g \geq 2$ algebraic curve $\mathcal{X}_g$ defined over an algebraic number field K we define the height $H_K(\mathcal{X}_g)$ and show that this is well-defined. This is basically the minimum height among all curves which are isomorphic to $\mathcal{X}_g$ over K. $\bar{H}_K(\mathcal{X}_g)$ is the height over the algebraic closure $\bar{K}$. It must be noticed that our definition is on the isomorphism class of the curve and not on some equation of the curve. We provide an algorithm to determine the height of a curve C provided some equation for C. This algorithm is rather inefficient, but can be used for $g = 2$ and $g = 3$ hyperelliptic curves when the coefficients of the initial equation of C are not too large.

7. Heights of algebraic curves

In this section we want to define heights on algebraic curves given by some affine equation. For this we will use the heights of polynomials as in Section 4. As before K denotes an algebraic number field and $\mathcal{O}_K$ its ring of integers.

Let $\mathcal{X}_g$ be an irreducible algebraic curve with affine equation $F(x,y) = 0$ for $F(x,y) \in K[x,y]$. We define the **height of the curve over** K to be

$$H_K(\mathcal{X}_g) := \min\{H_K(G) : H_K(G) \leq H_K(F)\}.$$

where the curve $G(x,y) = 0$ is isomorphic to $\mathcal{X}_g$ over K.

If we consider the equivalence over $\bar{K}$ then we get another height which we denote it as $\overline{H}_K(\mathcal{X}_g)$ and call it **the height over the algebraic closure**. Namely,

$$\overline{H}_K(\mathcal{X}_g) = \min\{H_K(G) : H_K(G) \leq H_K(F)\},$$

where the curve $G(x,y) = 0$ is isomorphic to $\mathcal{X}_g$ over $\overline{K}$.

In the case that $K = \mathbb{Q}$ we do not write the subscript K and use $H(\mathcal{X}_g)$ or $\overline{H}(\mathcal{X}_g)$. Obviously, for any algebraic curve $\mathcal{X}_g$ we have $\overline{H}_K(\mathcal{X}_g) \leq H_K(\mathcal{X}_g)$.

Lemma 19. *Let K be a number field such that $[K : \mathbb{Q}] = d$. Then, $H_K(\mathcal{X}_g)$ and $\overline{H}_K(\mathcal{X}_g)$ are well defined.*

Proof. Let $\mathcal{X}_g$ be an algebraic curve with affine equation $F(x,y) = 0$, for $F(x,y) \in K[x,y]$. We want to show that $H_K(\mathcal{X}_g)$ does not depend on the choice of the polynomial $F(x,y) = 0$. Let $F'(x,y) = 0$ be another polynomial representing our algebraic curve $\mathcal{X}_g$. We can calculate $H_K(F')$ using the formula of height of a polynomial and then we search for all polynomials $G(x,y) = 0$ which are isomorphic with $F'(x,y) = 0$ over K and such that $H_K(G) \leq H_K(F')$. Then,

$$\begin{aligned} H_K(\mathcal{X}_g) &= \min\left\{H_K(G) : H_K(G) \leq H_K(F')\right\}, \text{ such that } G(x,y) = 0 \\ &\qquad \text{is isomorphic over } K \text{ with } F'(x,y) = 0 \\ &= \min\left\{H_K(G) : H_K(G) \leq H_K(F)\right\}, \text{ such that } G(x,y) = 0 \\ &\qquad \text{is isomorphic over } K \text{ with } F(x,y) = 0 \end{aligned}$$

This completes the proof. $\square$

Theorem 7. *Let K be a number field such that $[K:\mathbb{Q}] \leq d$. Given a constant c there are only finitely many curves (up to isomorphism) such that $H_K(\mathscr{X}_g) \leq c$.*

Proof. Let C be an algebraic curve with height $H_K(C) = c$. By definition, the height of C is equal to the height of a polynomial $G(x,y) = 0$, i.e $H_K(G(x,y) = 0) = c$. By Theorem 2 there are only finitely many polynomials with height less then c. Therefore, there are at most finitely many algebraic curves $\mathscr{X}_g$ corresponding to such polynomials with height $H_K(\mathscr{X}_g) \leq c$. $\square$

7.1. Computing the height $H(\mathscr{X}_g)$ of a genus $g \geq 2$ curve $\mathscr{X}_g$.

Algorithm 1. ***Input:*** *algebraic curve $\mathscr{X}_g : F(x,y) = 0$ F has degree d and is defined over K*

Output: *algebraic curve $\mathscr{X}_g' : G(x,y) = 0$ such that $\mathscr{X}_g' \cong_K \mathscr{X}_g$ and $\mathscr{X}_g'$ has minimum height.*

Step 1: *Compute $c_0 = H_K(F)$*
Step 2: *List all points $P \in \mathbb{P}^s(K)$ such that $H_K(P) \leq c_0$.*
Note: *s is the number of terms of F which is the number of monomials of degree d in n variables, and this is equal to $\binom{d+n-1}{d}$. From theorem (1) there are only finitely many such points assume $P_1, \ldots, P_r$.*
Step 3: *for $i = 1$ to r do*
Let $G_i(x,y) = p_i$;
if $g(G_i(x,y)) = g(\mathscr{X}_g)$ then
if $G_i(x,y) = 0 \cong_K F(x,y) = 0$
then add G_i to the list L
end if;
end if;
Step 4:*Return all entries of L of minimum height , L has curves isomorphic over K to $\mathscr{X}_g$ of minimum height.*

8. Moduli height of curves

In this section we define the height in the moduli space of curves and investigate how this height can be used to study the curves. Our main goal is to investigate if the height of the moduli point has any relation to the height of the curve.

Let g be an integer $g \geq 2$ and $\mathscr{M}_g$ denote the coarse moduli space of smooth, irreducible algebraic curves of genus g. It is known that $\mathscr{M}_g$ is a quasi projective variety of dimension $3g-3$. Hence, $\mathscr{M}_g$ is embedded in $\mathbb{P}^{3g-2}$. Let $\mathfrak{p} \in \mathscr{M}_g$. We call the moduli height $\mathfrak{H}(\mathfrak{p})$ the usual height $H(P)$ in the projective space $\mathbb{P}^{3g-2}$. Obviously, $\mathfrak{H}(\mathfrak{p})$ is an invariant of the curve.

Theorem 8. *For any constant $c \geq 1$, degree $d \geq 1$, and genus $g \geq 2$ there are finitely many superelliptic curves $\mathscr{X}_g$ defined over the ring of integers $\mathscr{O}_K$ of an algebraic number field K such that $[K:\mathbb{Q}] \leq d$ and $\mathfrak{H}(\mathscr{X}_g) \leq c$.*

Proof. Let $\mathscr{X}_g$ be a genus g superelliptic curve with equation

$$y^n = x^{s+1} + a_s x^s + \cdots + a_1 x + a_0,$$

defined over K, where $[K : \mathbb{Q}] \leq d$. Then, $H(\mathscr{X}_g) = H(P)$, where $P := [a_0, \ldots, a_s] \in \mathbb{P}^s(K)$. From [9, Thm. B.2.3] we know that there are finitely such points in the projective space.

To prove the result for the moduli height we consider the moduli point $\mathfrak{p} = [\mathscr{X}_g]$ in the corresponding moduli space of superelliptic curves of genus $g \geq 2$. This point corresponds to a tuple $\mathfrak{p} = [J_0, \ldots, J_r] \in \mathbb{P}^r(K)$ of $SL_2(K)$ invariants in the space of binary forms of degree s. Again from [9, Thm. B.2.3] there are only finitely many such points. □

9. Applications to hyperelliptic and superelliptic curves

In this section we apply some of the results above to genus 2 curves and genus 3 hyperelliptic curves.

9.1. Genus 2 case

Let C be a genus 2 curve defined over an algebraic number field K. Then there is a degree 2 map $\pi : C \to \mathbb{P}^1(K)$, which is called the hyperelliptic projection. Let the equation of C be given by

$$y^2 = a_6 x^6 + \cdots + a_0$$

where $a_0, \ldots, a_6 \in K$. The isomorphism classes of genus 2 curves are on one to one correspondence with the orbits of the $GL_2(K)$-action on the space of binary sextics. The invariant ring $\mathbb{R}_6$ is generated by the Igusa invariants J_2, J_4, J_6, J_{10}; see Section 5 and [2] for details. Note that Igusa J-invariants $\{J_i\}$ are homogenous polynomials of degree i in $k[a_0, \ldots, a_6]$.

Let $\mathscr{M}_2$ be the moduli space of genus 2 curves considered as a projective variety, and i_1, i_2, i_3 be $GL_2(K)$-invariants given as in [2]. A point in $\mathscr{M}_2$ is given by (i_1, i_2, i_3) and as a projective point by

$$\mathfrak{p} = [J_4 J_2^3, (J_2 J_4 - 3J_6) J_2^2, J_{10}, J_2^5].$$

Notice that each $\mathfrak{p}[i]$ is a degree 10 polynomial evaluated at f, i.e degree 10 polynomial given in $k[a_0, \cdots, a_6]$. Denote with $F_i(f) = \mathfrak{p}[i]$. Then, from Lemma 15 we have

$$H(F_i(f)) \leq c_0 \cdot H(F_i) \cdot H(f)^{10}$$

where $c_0 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$ is the number of monomials of a degree 10 homogenous polynomial in seven variables. Computations of $H(F_i)$ is done in Maple and we get

$$H(F_1) = 2^{14} \cdot 3^7 \cdot 5^4, \; H(F_2) = 2^{21} \cdot 3^7 \cdot 5^4 \cdot 43, H(F_3) = 2^6 \cdot 3^5 \cdot 5, \; H(F_4) = 2^{20} \cdot 3^5 \cdot 5^5$$

The maximum is $H(F_2)$. The moduli height of f is computed as follows

$$\mathfrak{H}(f) = \max\{H(F_1(f),\dots,H(F_4(f))\} \leq c_0 \cdot H(F_2) \cdot H(f)^{10}.$$

Hence we have proved the following

Lemma 20. *For a genus 2 curve with equation $y^2 = f(x)$ the moduli height is bounded as follows*

$$\mathfrak{H}(f) \leq 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot H(f)^{10}$$

We denote the above constant by M_2. From now on we write that $\mathfrak{H}(H) \leq M_2 H(f)^{10}$. Since the above result holds for any binary form equivalent to f then we have that

$$\mathfrak{H}(f) \leq M_2 \cdot \tilde{H}(f)^{10}$$

While choosing this coordinate in $\mathscr{M}_2$ has benefits because the degree is 10, it creates many issues also when $J_2 = 0$. It is more convenient in many ways to use the following absolute invariants:

$$t_1 = \frac{J_2^5}{J_{10}}, \quad t_2 = \frac{J_4^5}{J_{10}^2}, \quad t_3 = \frac{J_6^5}{J_{10}^3}$$

The moduli point $\mathfrak{p} = (t_1, t_2, t_3)$ is defined everywhere in $\mathscr{M}_2$.

Remark 6. *All our previous papers about genus 2 curves have used the invariants i_1, i_2, i_3. However, our genus 2 package in Sage and the tables of genus 2 curves are done using invariants t_1, t_2, t_3.*

9.2. Genus 2 curves with height 1

Next we want to study genus 2 curves with height 1. Such curves will have minimal equations with coefficients 0 or ± 1. We list all of such curves and then group them according to the moduli point. In this paper we do not list all the twists of a given height.

By the algorithm of the previous section we get 230 such curves listed in the Tables 1-4. The curves are labeled 1-230 and presented by the vector of their coefficients $[a_0, \dots, a_6]$. They are organized in a dictionary in Sage, where the key is the triple (t_1, t_2, t_3). Indeed, our database of curves in Sage has over one million curves and can easily be accessed.

Next, we briefly discuss all the cases according to their automorphism group.

9.2.1. Curves with automorphism group of order 2

There are 186 genus 2 curves of height 1 which have automorphism groups G isomorphic to the group of order 2. They are all displayed in Table 1.

1	-1,-1,-1,-1,-1,-1,0	2	-1,-1,-1,-1,-1,1,0	3	-1,-1,-1,-1,0,-1,0	4	-1,-1,-1,-1,0,1,0
5	-1,-1,-1,-1,1,-1,0	6	-1,-1,-1,-1,1,1,0	7	-1,-1,-1,0,-1,-1,0	8	-1,-1,-1,0,-1,1,0
9	-1,-1,-1,0,0,-1,0	10	-1,-1,-1,0,0,1,0	11	-1,-1,-1,0,1,-1,0	12	-1,-1,-1,0,1,1,0
13	-1,-1,-1,1,-1,-1,0	14	-1,-1,-1,1,-1,1,0	15	-1,-1,-1,1,0,-1,0	16	-1,-1,-1,1,0,1,0
17	-1,-1,-1,1,1,-1,0	18	-1,-1,0,-1,-1,-1,0	19	-1,-1,0,-1,-1,1,0	20	-1,-1,0,-1,0,-1,0
21	-1,-1,0,-1,0,1,0	22	-1,-1,0,-1,1,-1,0	23	-1,-1,0,-1,1,1,0	24	-1,-1,0,0,-1,-1,0
25	-1,-1,0,0,-1,1,0	26	-1,-1,0,0,0,-1,0	27	-1,-1,0,0,0,1,0	28	-1,-1,0,0,1,-1,0
29	-1,-1,0,1,-1,-1,0	30	-1,-1,0,1,-1,1,0	31	-1,-1,0,1,0,-1,0	32	-1,-1,0,1,0,1,0
33	-1,-1,0,1,1,-1,0	34	-1,-1,0,1,1,1,0	35	-1,-1,1,-1,-1,-1,0	36	-1,-1,1,-1,-1,1,0
37	-1,-1,1,-1,0,-1,0	38	-1,-1,1,-1,0,1,0	39	-1,-1,1,-1,1,-1,0	40	-1,-1,1,-1,1,1,0
41	-1,-1,1,0,-1,-1,0	42	-1,-1,1,0,-1,1,0	43	-1,-1,1,0,0,-1,0	44	-1,-1,1,0,0,1,0
45	-1,-1,1,0,1,-1,0	46	-1,-1,1,0,1,1,0	47	-1,-1,1,1,-1,-1,0	48	-1,-1,1,1,-1,1,0
49	-1,-1,1,1,0,-1,0	50	-1,-1,1,1,0,1,0	51	-1,-1,1,1,1,-1,0	52	-1,-1,1,1,1,1,0
53	-1,0,-1,-1,-1,-1,0	54	-1,0,-1,-1,-1,1,0	55	-1,0,-1,-1,0,-1,0	56	-1,0,-1,-1,0,1,0
57	-1,0,-1,-1,1,-1,0	58	-1,0,-1,-1,1,1,0	59	-1,0,-1,0,-1,-1,0	60	-1,0,-1,0,1,-1,0
61	-1,0,0,-1,-1,-1,0	62	-1,0,0,-1,-1,1,0	63	-1,0,0,-1,0,-1,0	64	-1,0,0,-1,0,1,0
65	-1,0,0,-1,1,-1,0	66	-1,0,0,-1,1,1,0	67	-1,0,1,-1,-1,-1,0	68	-1,0,1,-1,-1,1,0
69	-1,0,1,-1,0,-1,0	70	-1,0,1,-1,1,-1,0	71	-1,0,1,-1,1,1,0	72	-1,0,1,0,-1,-1,0
73	-1,0,1,0,1,-1,0	74	0,-1,-1,-1,-1,1,0	75	0,-1,-1,-1,0,-1,0	76	0,-1,-1,-1,0,1,0
77	0,-1,-1,-1,1,1,0	78	0,-1,-1,0,0,-1,0	79	0,-1,-1,0,0,1,0	80	0,-1,-1,1,0,-1,0
81	-1,-1,-1,-1,-1,-1,1	82	-1,-1,-1,-1,-1,0,-1	83	-1,-1,-1,-1,-1,0,1	84	-1,-1,-1,-1,-1,1,-1
85	-1,-1,-1,-1,-1,1,1	86	-1,-1,-1,-1,0,-1,-1	87	-1,-1,-1,-1,0,-1,1	88	-1,-1,-1,-1,0,0,-1
89	-1,-1,-1,-1,0,0,1	90	-1,-1,-1,-1,0,1,-1	91	-1,-1,-1,-1,0,1,1	92	-1,-1,-1,-1,1,-1,-1
93	-1,-1,-1,-1,1,0,1	94	-1,-1,-1,-1,1,1,-1	95	-1,-1,-1,-1,1,1,1	96	-1,-1,-1,0,-1,-1,1
97	-1,-1,-1,0,-1,0,-1	98	-1,-1,-1,0,-1,0,1	99	-1,-1,-1,0,-1,1,1	100	-1,-1,-1,0,0,-1,-1
101	-1,-1,-1,0,0,-1,1	102	-1,-1,-1,0,0,0,-1	103	-1,-1,-1,0,0,0,1	104	-1,-1,-1,0,0,1,-1
105	-1,-1,-1,0,0,1,1	106	-1,-1,-1,0,1,-1,-1	107	-1,-1,-1,0,1,0,-1	108	-1,-1,-1,0,1,0,1
109	-1,-1,-1,0,1,1,-1	110	-1,-1,-1,1,-1,-1,1	111	-1,-1,-1,1,-1,0,-1	112	-1,-1,-1,1,-1,0,1
113	-1,-1,-1,1,-1,1,1	114	-1,-1,-1,1,0,-1,-1	115	-1,-1,-1,1,0,-1,1	116	-1,-1,-1,1,0,0,-1
117	-1,-1,-1,1,0,0,1	118	-1,-1,-1,1,0,1,-1	119	-1,-1,-1,1,0,1,1	120	-1,-1,-1,1,1,-1,-1
121	-1,-1,-1,1,1,0,-1	122	-1,-1,-1,1,1,0,1	123	-1,-1,-1,1,1,1,-1	124	-1,-1,0,-1,-1,-1,1
125	-1,-1,0,-1,-1,0,-1	**126**	-1,-1,0,-1,-1,0,1	127	-1,-1,0,-1,-1,1,1	128	-1,-1,0,-1,0,0,-1
129	-1,-1,0,-1,0,0,1	130	-1,-1,0,-1,0,1,-1	131	-1,-1,0,-1,0,1,1	132	-1,-1,0,-1,1,-1,-1
133	-1,-1,0,-1,1,0,-1	134	-1,-1,0,-1,1,0,1	135	-1,-1,0,-1,1,1,-1	136	-1,-1,0,0,-1,-1,1
137	-1,-1,0,0,-1,0,-1	138	-1,-1,0,0,-1,0,1	139	-1,-1,0,0,-1,1,1	140	-1,-1,0,0,0,0,-1
141	-1,-1,0,0,0,0,1	142	-1,-1,0,0,1,-1,-1	143	-1,-1,0,0,1,0,-1	144	-1,-1,0,0,1,0,1
145	-1,-1,0,0,1,1,-1	146	-1,-1,0,1,-1,-1,1	147	-1,-1,0,1,-1,0,-1	148	-1,-1,0,1,-1,0,1
149	-1,-1,0,1,-1,1,1	150	-1,-1,0,1,0,0,-1	151	-1,-1,0,1,0,0,1	152	-1,-1,0,1,1,-1,-1
153	-1,-1,0,1,1,0,-1	154	-1,-1,0,1,1,0,1	155	-1,-1,0,1,1,1,-1	156	-1,-1,1,-1,-1,0,-1
157	-1,-1,1,-1,-1,0,1	158	-1,-1,1,-1,-1,1,1	159	-1,-1,1,-1,0,0,-1	160	-1,-1,1,-1,0,0,1
161	-1,-1,1,-1,1,0,-1	162	-1,-1,1,-1,1,0,1	163	-1,-1,1,-1,1,1,-1	164	-1,-1,1,0,-1,0,-1
165	-1,-1,1,0,-1,0,1	166	-1,-1,1,0,0,0,-1	167	-1,-1,1,0,0,0,1	168	-1,-1,1,0,1,0,-1
169	-1,-1,1,0,1,0,1	170	-1,-1,1,1,-1,0,-1	171	-1,-1,1,1,-1,0,1	172	-1,-1,1,1,0,0,-1
173	-1,-1,1,1,0,0,1	174	-1,-1,1,1,1,0,-1	175	-1,-1,1,1,1,0,1	176	-1,0,-1,-1,-1,0,1
177	-1,0,-1,-1,0,0,-1	178	-1,0,-1,-1,0,0,1	179	-1,0,-1,-1,1,0,-1	180	-1,0,0,-1,-1,0,1
181	0,-1,-1,1,0,1,0	182	-1,-1,0,1,0,0,-1	183	-1,0,-1,0,0,-1,0	184	-1,0,0,0,-1,-1,0
185	-1,0,0,0,1,-1,0	186	-1,0,1,0,0,-1,0				

Table 1. Curves with height 1 and automorphism group of order 2

9.2.2. *Curves with automorphism group the Klein 4-group*

In Table tab2 we display all genus 2 curves with automorphism group V_4 and height 1. The curves of genus 2 with automorphism group V_4 are uniquely determine by the pair of Shaska-invariants (u, v) as defined in [16]. There are 28 of such curves (up to isomorphism over $\mathbb{C}$) which are displayed in Table 2. In the last column of the Table 2 we display the moduli height of these curves.

Table 2. Genus 2 curves with height 1 and automorphism group V_4

#	curve	sh-invariants (u, v)	mod. height
187	1 1 -1 -1 -1 1 1	-855 , -84266	257^6
188	0 1 1 -1 -1 1 0	53/13 , -410/169	$3^4 \cdot 13^2 \cdot 31^5$
189	1 0 1 0 1 0 -1	-1 , 0	$2^5 \cdot 11^3 \cdot 199^5$
190	1 1 1 0 -1 1 -1	281 , 7430	$2^7 \cdot 3^{25} \cdot 13^5$
191	1 1 0 -1 0 1 -1	73 , 201702/169	$2^2 \cdot 13^4 \cdot 37^5 \cdot 43^5$
192	1 0 1 0 0 0 1	0 , 1	$2^4 \cdot 3^5 \cdot 4999^5$
193	0 1 1 -1 1 1 0	-55 , -8794/9	$3^2 \cdot 7^5 \cdot 11^5$
194	1 1 -1 0 1 1 -1	221/5 , 12406/25	$2^7 \cdot 3 \cdot 7^{10} \cdot 13^5$
195	1 1 -1 0 -1 1 1	-231 , -7930	79^6
196	1 1 1 1 1 1 1	105 , 2198	$3^5 \cdot 37^5$
197	1 1 -1 -1 1 1 -1	833/25 , 239414/625	$3^5 \cdot 41^5 \cdot 467^5$
198	1 1 1 -1 1 1 1	41 , 74546/75	$3 \cdot 5^4 \cdot 977^5$
199	1 1 0 1 0 1 -1	1069/5 , 112966/25	$2^6 \cdot 29^5 \cdot 47^5$
200	1 1 0 1 0 1 1	-851/5 , 10182/25	$2^6 \cdot 5^6 \cdot 17^5 \cdot 37^2$
201	1 1 1 1 -1 1 -1	1193 , 75478	104021^5
202	0 1 1 1 1 1 0	9 , -754/5	$3^5 \cdot 5^3$
203	1 1 0 -1 0 1 1	731/3 , 94246/9	$2^9 \cdot 7^5 \cdot 167^5$
204	1 1 -1 1 1 1 -1	953/17 , 118806/289	$5^2 \cdot 7^3 \cdot 13^5 \cdot 23^5$
205	1 1 1 -1 -1 1 -1	1073/9 , 42322/27	$3^{13} \cdot 13^{10} \cdot 19^5$
206	1 1 -1 1 -1 1 1	-325/3 , -43694/27	$3^2 \cdot 107^6$
207	1 0 1 1 -1 0 -1	1033 , -18378	43759^5
208	1 0 1 1 1 0 1	155/3 , 39166/45	$5^2 \cdot 7^5 \cdot 313^5$
209	1 0 -1 1 1 0 -1	793/17 , 155510/289	$3^5 \cdot 14797^5$
210	1 1 1 0 1 1 1	57 , 9046/9	$2^7 \cdot 3^{12} \cdot 43^5$
211	0 1 1 0 -1 1 0	13 , -18	$2^{11} \cdot 7^9$
212	1 0 1 0 0 0 -1	0 , -1	$2^4 \cdot 3^5 \cdot 7^5 \cdot 23^3 \cdot 31^5$
213	1 0 -1 1 -1 0 1	-1015 , 18486	$229^2 \cdot 337^5$
214	0 1 1 1 -1 1 0	173/5 , -58/25	$5^2 \cdot 11^4 \cdot 31^5$

For all genus 2 curves with automorphism group V_4 the field of moduli is a field of definition, which implies that there exists an equation of the curve given in terms of the Shaska-invariants $u, v)$. Such equation is given explicitly in [2]. However, this equation does not give a curve with minimal height, indeed far from it. For example, if we take curve C_{187} and find it equation over $\mathbb{Q}$ based on $u = -885$ and $v = -84266$ we get a curve with Weierstrass equation

$$
\begin{aligned}
y^2 = & 6656217643t^6 - 1147848127638528t^5 - 2242554574419331276 80t^4 + 531100797557087672886886 40t^3 \\
& - 2153046205567184961085196206080t^2 - 1058047313654615098577319167608750 08t + 5890586015659177610234918599810915237888
\end{aligned}
$$

This equation is obviously far from the equation of height 1

$$y^2 = x^6 + x^5 - x^4 - x^3 - x^2 + x + 1$$

even though these two curves are isomorphic.

9.2.3. Curves with automorphism group the dihedral group of order 8

The D_8-locus is 1-dimensional in $\mathcal{M}_2$, which implies that such curves can be described by a single invariant s which we display in the last column of Table 3. The equations of such curves for a given s is given by

$$y^2 = x^5 + x^3 + sx$$

There are 11 such curves as displayed in Table 3. It can be seen from the table that only curves C_{218} and C_{220} have height 1 when we use the equation given from s as above.

Table 3. Genus 2 curves with height 1 and automorphism group D_8

#	curve	mod. height	s
215	0 1 1 0 -1 -1 0	$2^9 \cdot 3^2$	$-\frac{3}{4}$
216	1 1 0 0 0 1 -1	$3^5 \cdot 5^5 \cdot 13^5 \cdot 233^5$	$\frac{13}{100}$
217	1 1 0 0 0 -1 -1	5^{15}	$\frac{1}{20}$
218	0 1 0 1 0 1 0	$2^4 \cdot 3^2 \cdot 23^5$	1
219	1 1 -1 0 -1 -1 1	$2^7 \cdot 383^5$	$\frac{5}{16}$
220	0 1 0 1 0 -1 0	$2^4 \cdot 5^4 \cdot 17^5$	-1
221	0 1 1 0 1 -1 0	$2^9 \cdot 5 \cdot 7^5$	$\frac{5}{4}$
222	1 1 1 0 1 -1 1	$2^{14} \cdot 409^5$	$\frac{1}{18}$
223	1 0 1 0 1 0 1	$2^{11} \cdot 97^5$	$\frac{1}{36}$
224	1 1 1 0 -1 -1 -1	$2^7 \cdot 3 \cdot 5^{15}$	$\frac{3}{16}$
225	1 1 0 0 0 -1 1	$3^3 \cdot 5^5 \cdot 233^5$	$\frac{13}{100}$

9.2.4. Curves with automorphism group of order ≥ 10

The rest of the curves with larger automorphism group are displayed in Table 4. In the form column we have displayed the Gap identity of the group; see [2] for details. In the last column is displayed the rational model of the curve obtained with methods in [2].

Table 4. Genus 2 curves with height 1 and automorphism group $|G| \geq 10$

#	curve	mod. height	Aut(C)	$y^2 = f(t)$
226	1 0 0 1 0 0 -1	$3^3 \cdot 677^5$	[12, 6]	$t^6 + t^3 - 745849/194481$
227	1 0 0 1 0 0 1	$3^3 \cdot 89^5$	[12, 6]	$t^6 + t^3 + 11389/2601$
228	1 0 0 0 0 0 1	$2^4 \cdot 3^3 \cdot 5^5 \cdot 37^5$	[24, 8]	$t^6 - 1$
229	0 1 0 0 0 1 0	$2^8 \cdot 5^5$	[48, 5]	$t^5 - t$
230	1 0 0 0 0 1 0	1	[10, 1]	$t^6 - t$

From the previous Lemma 20 when $H(C) = 1$ we get that for any curve C, the moduli height is $\mathfrak{H}(C) \leq M_2$. Indeed the biggest moduli height for all 230 curves of height 1 is

$$\mathfrak{H}(C_{126}) = 2^7 \cdot 3^2 \cdot 5^2 \cdot 151^2 \cdot 3863 < M_2 = 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$$

which occurs for curve C_{126} on the table. The curve with smallest moduli height is the curve C_{230} with $\mathfrak{H}(C) = 1$. In [3] we classify all curves with "small" moduli height and give some estimates on the number of curves with bounded moduli height.

Remark 7. *There are 96660 $\mathbb{C}$-isomorphism classes of genus 2 curves defined over $\mathbb{Z}$ and height ≤ 3. From those, 230 have height 1, 8830 have height 2, and 88600 have height 3.*

9.3. Genus 3 case

Let C be a genus 3 curve defined over an algebraic number field K. Then there is a degree 2 map $\pi : C \to \mathbb{P}^1(K)$, which is called the hyperelliptic projection. Let the equation of C be given by

$$y^2 = a_8 x^8 + \cdots + a_1 x + a_0$$

where $a_0, \ldots, a_8 \in K$, and $\Delta(f) \neq 0$. The invariant ring R_8 is generated by nine $SL_2(K)$-invariants $J_2, \ldots, J_{10}$; see [22] for details.

Let $\mathscr{M}_3$ be the moduli space of genus 3 curves considered as a projective variety, and $t_1, \ldots, t_6$ be $GL(2,k)$-invariants given as follows

$$t_1 := \frac{J_3^2}{J_2^3}, \quad t_2 := \frac{J_4}{J_2^2}, \quad t_3 := \frac{J_5}{J_2 \cdot J_3}, \quad t_4 := \frac{J_6}{J_2 \cdot J_4}, \quad t_5 := \frac{J_7}{J_2 \cdot J_5}, \quad t_6 := \frac{J_8}{J_2^4},$$

Let

$$\mathfrak{p} = \left[J_2 J_3^2 J_4 J_5,\, J_2^2 J_3 J_4^2 J_5,\, J_2^3 J_4 J_5^2,\, J_2^3 J_3 J_5 J_6,\, J_2^3 J_3 J_4 J_7,\, J_3 J_4 J_5 J_8, J_2^4 J_3 J_4 J_5 \right]$$

be a point in $\mathscr{M}_3$. Each $\mathfrak{p}[i]$ is a degree 20 polynomial evaluated at f, i.e degree 20 polynomial given in $k[a_0, \ldots, a_8]$. Denote with $F_i(f) = \mathfrak{p}[i]$. Then, from Lemma 15 we have

$$H(F_i(f)) \leq c_0 \cdot H(F_i) \cdot H(f)^{20}$$

where $c_0 =$ is the number of monomials of a degree 20 homogenous polynomial in nine variables.

The proof of the following lemma is provided in [3]

Lemma 21. *For a genus 3 curve with equation $y^2 = f(x)$, where $f(x)$ is a degree 8 polynomials the moduli height is bounded as follows*

$$\mathfrak{H}(f) \leq c \cdot H(f)^{20}$$

We denote the above constant by M_3. From now on we write that $\mathfrak{H}(H) \leq M_3 \cdot H(f)^{20}$. Since the above result holds for any binary form equivalent to f then we have that $\mathfrak{H}(f) \leq M_3 \cdot \tilde{H}(f)^{20}$.

10. Final remarks

A continuation of this work and proving some of the results here is intended in [3] and [4], where we also improve the algorithm to find an equation of the curve with minimal height.

References

[1] L. Beshaj, *Reduction theory of binary forms* (2015), available at http://arxiv.org/abs/1502.06289.

[2] L. Beshaj and T. Shaska, *The arithmetic of genus two curves*, Information security, coding theory and related combinatorics, 2011, pp. 59–98. MR2963126

[3] ______, *Algebraic curves with minimal height*, in preparation (2015).

[4] ______, *Integral models of minimal height for binary forms*, 2015. work in progress.

[5] L. Beshaj and F. Thompson, *Equations for superelliptic curves over their minimal field of definition*, Albanian J. Math. **8** (2014), no. 1, 3–8. MR3253208

[6] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 (2007a:11092)

[7] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Schappacher, and Ulrich Stuhler, *Rational points*, Third, Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984, With an appendix by Wüstholz. MR1175627 (93k:11060)

[8] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003. MR1999383 (2004f:11034)

[9] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 (2001e:11058)

[10] Vishwanath Krishnamoorthy, Tanush Shaska, and Helmut Völklein, *Invariants of binary forms*, Progress in Galois theory, 2005, pp. 101–122. MR2148462 (2006b:13015)

[11] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983. MR715605 (85j:11005)

[12] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[13] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. MR1002324 (90e:11086)

[14] ______, *Topics in Galois theory*, Second, Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008. With notes by Henri Darmon. MR2363329 (2008i:12010)

[15] Rachel Shaska, *Equations of curves with minimal discriminant* (2014), available at http://arxiv.org/abs/1407.7064.

[16] T. Shaska, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993

[17] ______, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), 2002, pp. 205–218. MR2041085 (2005e:14048)

[18] ______, *Computational aspects of hyperelliptic curves*, Computer mathematics, 2003, pp. 248–257. MR2061839 (2005h:14073)

[19] ______, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 2003, pp. 248–254 (electronic). MR2035219 (2005c:14037)

[20] ______, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, 2005, pp. 206–231. MR2182041 (2006g:14051)

[21] ______, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319. MR2367221 (2008k:14108)

[22] ______, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084

[23] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120 (2004m:14047)