# Weighted heights and moduli space of Abelian covers

T. Shaska

Oakland University

November 12, 2019

# Weighted greatest common divisors I

Let $\mathbf{x} = (x_0, \ldots x_n) \in \mathbb{Z}^{n+1}$ be a tuple of integers, not all equal to zero. Their greatest common divisor, denoted by $\gcd(x_0, \ldots, x_n)$, is defined as the largest integer $d$ such that $d | x_i$, for all $i = 0, \ldots, n$.

The concept of the **weighted greatest common divisor** of a tuple for the ring of integers $\mathbb{Z}$ was defined in [13]. Let $q_0, \ldots, q_n$ be positive integers. A set of weights is called the ordered tuple

$$\mathfrak{w} = (q_0, \ldots, q_n).$$

Denote by $r = \gcd(q_0, \ldots, q_n)$ the greatest common divisor of $q_0, \ldots, q_n$. A **weighted integer tuple** is a tuple $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ such that to each coordinate $x_i$ is assigned the weight $q_i$. We multiply weighted tuples by scalars $\lambda \in \mathbb{Q}$ via

$$\lambda \star (x_0, \ldots, x_n) = (\lambda^{q_0} x_0, \ldots, \lambda^{q_n} x_n)$$

For an ordered tuple of integers $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$, whose coordinates are not all zero, the **weighted greatest common divisor with respect to the set of weights** $\mathfrak{w}$ is the largest integer $d$ such that

$$d^{q_i} \mid x_i, \quad \text{for all } i = 0, \ldots, n.$$

The first natural question arising from this definition is to know if such integer $d$ does exist for any tuple $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$. Clearly, it does exist because $x_i \leq d^{q_i}$ for all $i = 0, \ldots, n$ and the largest integer is unique.

We will denote by $wgcd(x_0, \ldots, x_n) = wgcd(\mathbf{x})$.

# Weighted greatest common divisors II

Given integer $a$ and non-zero integer $b$, the integer part of the real number $\frac{a}{b}$ is denote by $\left\lfloor \frac{a}{b} \right\rfloor$, that is, it is the unique integer satisfying:

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r, \quad 0 \leq r < b.$$

The next result provides an algorithm to compute the weighted greatest common divisor.

### Proposition

*For a weighted integer tuple $\mathbf{x} = (x_0, \ldots, x_n)$ with weights $\mathfrak{w} = (q_0, \ldots, q_n)$ let the factorization of the integers $x_i$, $(i = 0, \ldots, n)$ into primes:*

$$x_i = \prod_{j=1}^{t} p_j^{\alpha_{j,i}}, \quad \alpha_{j,i} \geq 0, \; j = 1, \ldots, t$$

*Then, the weighted greatest common divisor $d = wgcd(\mathbf{x})$ is given by*

$$d = \prod_{j=1}^{t} p_j^{\alpha_j} \tag{1}$$

*where,*

$$\alpha_j = \min \left\{ \left\lfloor \frac{\alpha_{j,i}}{q_i} \right\rfloor, \; i = 0, \ldots, n \right\} \textit{ and } j = 1, \ldots, t. \tag{2}$$

Next we illustrate the method by a toy example:

# Weighted greatest common divisors III

**Example**

*Consider the set of weights* $\mathfrak{w} = (3, 2)$ *and the tuple*

$$\mathbf{x} = (1440, 700) = \left(2^5 \cdot 3^2 \cdot 5 \cdot 7^0,\ 2^2 \cdot 3^0 \cdot 5^2 \cdot 7\right) \in \mathbb{Z}^2.$$

*Then,* $wgcd(\mathbf{x}) = d = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4}$*, where*

$$\alpha_1 = \min\left\{\left\lfloor \frac{5}{3} \right\rfloor, \left\lfloor \frac{2}{2} \right\rfloor\right\} = 1, \quad \alpha_2 = \min\left\{\left\lfloor \frac{2}{3} \right\rfloor, \left\lfloor \frac{0}{2} \right\rfloor\right\} = 0,$$
$$\alpha_3 = \min\left\{\left\lfloor \frac{1}{3} \right\rfloor, \left\lfloor \frac{0}{2} \right\rfloor\right\} = 0, \quad \alpha_4 = \min\left\{\left\lfloor \frac{0}{3} \right\rfloor, \left\lfloor \frac{1}{2} \right\rfloor\right\} = 0.$$

*Then* $d = 2$*.*

□

An integer tuple $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ such that its weighted gcd is $wgcd(\mathbf{x}) = 1$ is called **normalized**.

# Absolute weighted greatest common divisor I

The **absolute weighted greatest common divisor** of $\mathbf{x} = (x_0, \dots, x_n)$ with respect to $\mathfrak{w}$ is the largest **real number** $d$ such that

$$d^{q_i} \in \mathbb{Z} \quad \text{and} \quad d^{q_i} \mid x_i, \quad \text{for all } i = 0, \dots n.$$

Again, the natural question is to know if such real number $d$ does exist for any tuple $\mathbf{x}$.

### Proposition

*For a given* $\mathbf{x} = (x_0, \dots, x_n)$ *with* $\mathfrak{w} = (q_0, \dots, q_n)$ *let the factorization of* $x_i$ *be*

$$x_i = \prod_{j=1}^{t} p_j^{\alpha_{j,i}}, \quad \alpha_{j,i} \geq 0, \ j = 1, \dots, t$$

*Then,*

$$\overline{wgcd}(\mathbf{x}) = \left( \prod_{j=1}^{t} p_j^{\alpha_j} \right)^{\frac{1}{q}}$$

*where,* $q = \gcd(q_0, \dots, q_n)$, $\ q_i = q \cdot \bar{q}_i$ *and*

$$\alpha_j = \min \left\{ \left\lfloor \frac{\alpha_{j,i}}{\bar{q}_i} \right\rfloor, i = 0, \dots, n \right\} \text{ and } j = 1, \dots, t.$$

# Absolute weighted greatest common divisor II

**Example**

*Consider the set of weights* $\mathfrak{w} = (6, 8)$ *and the tuple*

$$\mathbf{x} = (2^{15} \cdot 5^{12}, 2^{26} \cdot 5^{13}) \in \mathbb{Z}^2.$$

*Then* $q = \gcd(6, 8) = 2$, $p_1 = 2$, $p_2 = 5$, $t = 2$ *and* $\bar{q}_1 = 3, \bar{q}_2 = 4$. *Then,* $\overline{wgcd}(\mathbf{x}) = d = (2^{\alpha_1} \cdot 5^{\alpha_2})^{\frac{1}{2}}$*, where*

$$\alpha_1 = \min \left\{ \left\lfloor \frac{15}{3} \right\rfloor, \left\lfloor \frac{26}{4} \right\rfloor \right\} = 5, \qquad \alpha_2 = \min \left\{ \left\lfloor \frac{12}{3} \right\rfloor, \left\lfloor \frac{13}{4} \right\rfloor \right\} = 3.$$

*Hence* $d = 2^{\frac{5}{2}} \cdot 5^{\frac{3}{2}} = \sqrt{2^5 \cdot 5^3}$. *On the other hand,* $wgcd(\mathbf{x}) = 2^2 \cdot 5$. *As expected,* $wgcd(\mathbf{x}) \leq \overline{wgcd}(\mathbf{x})$.

The next example comes from the theory of invariants of binary sextics.

**Example**

*Consider the set of weights* $\mathfrak{w} = (2, 4, 6, 10)$ *and a tuple*

$$\mathbf{x} = (3 \cdot 5^2, 3^2 \cdot 5^4, 3^3 \cdot 5^6, 3^5 \cdot 5^{10}) \in \mathbb{Z}^4.$$

*Then,* $wgcd(\mathbf{x}) = 5$ *and* $\overline{wgcd}(\mathbf{x}) = 5 \cdot \sqrt{3}$.

An integer tuple $\mathbf{x}$ with $\overline{wgcd}(\mathbf{x}) = 1$ is called **absolutely normalized**. We summarize in the following lemma.

# Absolute weighted greatest common divisor III

**Lemma**

*For any weighted integral tuple* $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ *such that* $\mathfrak{w}(x_i) = q_i$, $i = 0, \ldots, n$, *the tuple* $\mathbf{y} = \frac{1}{wgcd(\mathbf{x})} \star \mathbf{x}$, *is integral and normalized. Moreover, the tuple* $\bar{\mathbf{y}} = \frac{1}{\overline{wgcd}(\mathbf{x})} \star \mathbf{x}$, *is also integral and absolutely normalized.*

Normalized tuples are unique up to a multiplication of $q$-root of unity, where $q = \gcd(q_0, \ldots, q_n)$.

It is worth noting that a normalized tuple is a tuple with ”smallest” integer coordinates (up to multiplication by a unit). We will explore this idea of the ”smallest coordinates” in the coming sections.

There are a few natural questions that arise with the weighted greatest common divisor of a tuple of integers. We briefly mention the two main ones:

**Problem 1:** The greatest common divisor can be computed in polynomial time using the Euclidean algorithm. Determine the fastest way to compute the weighted greatest common divisor and the absolute weighted greatest common divisor.

**Problem 2:** The greatest common divisor is uniquely determined for unique factorization domains. Define the concept of the weighted greatest common divisor in terms of ring theory and determine the largest class of rings where it is uniquely defined (up to multiplication by a unit).

# Complexity of computing the weighted greatest common divisor

Prop. 1 and Prop. 2 provide a method to compute $wgcd(\mathbf{x})$ and $\overline{wgcd}(\mathbf{x})$. In both, integer factorization is involved.

There are several indications that we can not avoid factoring. For instance, we have that $wgcd(0,\dots,0,x_n)$ is $wgcd(x_n)$, then we are looking for the largest factor $d$ of $x_n$ such that $d^{q_n}$ divides $x_n$.

Alternatively, we can factor only an integer, instead of $n+1$, and then recombining factors in an appropriate and clever way gives us the following.

**Lemma**

*Let $g = \gcd(x_0,\dots,x_n)$ and $g = \prod_{i=1}^{r} p_i^{s_i}$ its prime factorization.*

1. *For $i = 1,\dots,r$, let*

$$\beta_i = \min\left\{ \left\lfloor \frac{s_i}{q_j} \right\rfloor \,:\, j = 0,\dots,n \right\}.$$

*Then, $wgcd(\mathbf{x}) = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $\alpha_i$ are the largest integers such that $d^{q_i}$ divides $x_i$ and $\alpha_i \le \beta_i$.*

2. *Let $q = \gcd(q_0,\dots,q_n)$, $q_j = q \cdot \bar{q}_j$, $j = 0,\dots,n$ and for $i = 1,\dots,r$ let*

$$\beta_i = \min\left\{ \left\lfloor \frac{s_i}{\bar{q}_j} \right\rfloor,\, j = 0,\dots,n \right\}$$

*Then, $\overline{wgcd}(\mathbf{x}) = \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)^{\frac{1}{q}}$, where $\alpha_i$ are the largest integers such that $d^{q_i}$ divides $x_i$ and $\alpha_i \le \beta_i$.*

# Weighted greatest common divisor over general rings

Let $R$ be a commutative ring with identity. Consider a tuple $\mathbf{x} = (x_0, \ldots, x_n) \in R^{n+1}$. The **weighted greatest common divisor ideal** is defined as

$$\mathfrak{J}(\mathbf{x}) = \bigcap_{(\mathfrak{p}^{q_i}) \supset (x_i)} \mathfrak{p}$$

over all primes $\mathfrak{p}$ in $R$. If $R$ is a PID then the $wgcd(\mathbf{x})$ is the generator of the principal ideal $\mathfrak{J}(\mathbf{x})$.

In general, for $R$ a unique factorization domain, for any point $\mathbf{x} \in R^n$ we let $r = \gcd(x_0, \ldots, x_n)$. Factor $r$ as a product of primes, say $r = u \cdot \prod_{i=1}^{s} \mathfrak{p}_i$, where $u$ is a unit and $\mathfrak{p}_1, \ldots \mathfrak{p}_s$ are primes. Then the weighted gcd $wgcd(\mathbf{x})$ is defined as

$$wgcd(\mathbf{x}) = \prod_{\substack{i=1 \\ p^{q_i} | x_i}}^{s} \mathfrak{p}$$

Thus, $wgcd(\mathbf{x})$ is defined up to multiplication by a unit. The **absolute weighted greatest common divisor ideal** is defined as

$$\bar{\mathfrak{J}}(\mathbf{x}) = \bigcap_{\left(\mathfrak{p}^{\frac{q_i}{r}}\right) \supset (x_i)} \mathfrak{p}$$

over all primes $\mathfrak{p}$ in $R$. The above definitions can be generalized to GCD domains. An integral domain $R$ is called a **GCD domain** if any two elements of $R$ have a greatest common divisor; see [10] for more details.

# Weighted projective spaces I

## Abelian Orbifolds

An **orbifold** of dimension $n$ is a complex analytic space which admits an open covering $\{U_i\}$, such that $U_i$ is analytically isomorphic to $B_i/G_i$, where $B_i \subset \mathbb{C}^i$ is an open ball and $G_i$ a finite subgroup of $GL_n(\mathbb{C})$.
We will be interested in Abelian orbifolds where the quotient spaces $B_i/G_i$ are given by finite Abelian groups.
Let $d_1, \dots, d_r \in \mathbb{Z}$ and

$$\mathbf{d} := (d_1, \dots, d_r).$$

Denote by $\mu_{\mathbf{d}} = \mu_{d_1} \times \cdots \mu_{d_r}$ the finite Abelian group written as a product of finite cyclic groups, where each $\mu_{d_i}$ is the cyclic group of $d_i$-th roots of unity in $\mathbb{C}$.
Let $\xi_{d_i}$ a primitive $d_i$-th root of unity and $\xi_{\mathbf{d}} := (\xi_{d_1}, \dots, \xi_{d_r})$ and $A := (a_{i,j})_{i,j} \in Mat_{r\times n}(\mathbb{Z})$. We have a group action

$$\mu_{\mathbf{d}} \times \mathbb{C}^n \to \mathbb{C}^n$$
$$((\xi_{d_1}, \dots, \xi_{d_r}), (x_1, \dots, x_n)) \to \left(\xi_{d_1}^{a_{11}} \cdots \xi_{d_r}^{a_{r1}} x_1, \dots, \xi_{d_1}^{a_{1n}} \cdots \xi_{d_r}^{a_{rn}} x_n\right)$$

The set of all orbits of this action is called the **quotient space of type** $(\mathbf{d}, A)$ and denoted by $X(\mathbf{d}, A)$.

### Lemma

*For any finite Abelian subgroup $G < GL_n(\mathbb{C})$, the space $\mathbb{C}^n/G$ is isomorphic to some quotient space of type $X(\mathbf{d}, A)$. Moreover, the space $X(\mathbf{d}, A)$ can always be represented by some upper triangular matrix $A \in Mat_{(n-1)\times n}(\mathbb{Z})$.*

We will be interested in some very special orbifolds, namely weighted projective spaces.

# Weight projective spaces I

Let $k$ be a field of characteristic zero and $\mathfrak{w} = (q_0, \dots, q_n) \in \mathbb{Z}^{n+1}$ a fixed tuple of positive integers called **weights**. Consider the action of $k^\star = k \setminus \{0\}$ on $\mathbb{A}^{n+1}(k)$ as follows

$$\lambda \star (x_0, \dots, x_n) = (\lambda^{q_0} x_0, \dots, \lambda^{q_n} x_n)$$

for $\lambda \in k^*$.

The quotient of this action is called a **weighted projective space** and denoted by $\mathbb{WP}^n_{(q_0,\dots,q_n)}(K)$. It is the projective variety $Proj\,(k[x_0, ..., x_n])$ associated to the graded ring $k[x_0, \dots, x_n]$ where the variable $x_i$ has degree $q_i$ for $i = 0, \dots, n$.
We denote greatest common divisor of $q_0, \dots, q_n$ by $\gcd(q_0, \dots, q_n)$. The space $\mathbb{WP}^n_w$ is called **well-formed** if

$$\gcd(q_0, \dots, \hat{q}_i, \dots, q_n) = 1, \quad \text{for each } \; i = 0, \dots, n.$$

We will denote a point $\mathfrak{p} \in \mathbb{WP}^n_w(K)$ by $\mathfrak{p} = [x_0 : x_1 : \dots : x_n]$. A common reference for weighted projective spaces is [5].

Weighted heights

# Heights on weighted projective varieties I

First let's review heights on projective spaces; see [3], [9]

Let $k$ be an algebraic number field, $[k:\mathbb{Q}]=n$, $\mathcal{O}_k$ the ring of integers of $k$, $M_k$ the complete set of absolute values of $k$, $M_k^0$ the set of all non-archimedean places in $M_k$, and $M_k^\infty$ the set of all archimedean places.

For $v \in M_k$, the **local degree at** $v$ is $n_v := [k_v : \mathbb{Q}_v]$, where $k_v, \mathbb{Q}_v$ are the completions with respect to $v$. Let $L/k$ be an extension of number fields, and let $v \in M_k$ be an absolute value on $k$. Then

$$\sum_{\substack{w \in M_L \\ w|v}} [L_w : k_v] = [L:k] \quad \text{and} \quad \prod_{v \in M_k} |x|_v^{n_v} = 1$$

are known as the **degree formula** and the **product formula** (for $x \in k^\star$).
For a place $\nu \in M_k$, the corresponding absolute value is denoted by $|\cdot|_\nu$, normalized with respect to $k$ such that the product formula holds. The Weil height is

$$H(x) = \prod_\nu \max\{1, |x|_\nu\}.$$

For a point $\mathbf{x} \in k^{n+1}$ and a place $\nu \in M_k$ we define $|\mathbf{x}|_\nu = \max\{|x_i|_\nu\}_{i=0}^n$. For $\mathbf{x} = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k)$ we define the **height** of $\mathbf{x}$ defined as

$$H(\mathbf{x}) = \prod_\nu \max\{|x_0|_\nu, \dots, |x_n|_\nu\} = \prod_\nu |\mathbf{x}|_\nu$$

The height of $\mathbf{x}$ is well defined.

# Heights on weighted projective varieties I

## Local heights on projective varieties

Let $k$ be a field and $|\cdot|$ a fixed absolute value on $k$. Let $\mathcal{X}$ be a projective variety over $k$, which we assume that is irreducible.
Let $D$ be a Cartier divisor on $\mathcal{X}$ with associated bundle $O(D)$ and meromorphic section $s_D$. Then there are line bundles on $\mathcal{X}$ such that

$$O(D) \cong L \otimes M^{-1}.$$

Choose global sections $s_0, \dots, s_n$ of $L$ and $t_0, \dots, t_m$ of $M$. The data

$$\mathcal{D} := (s_D; L, s; M, t),$$

where $(s) := (s_0, \dots, s_n)$ and $\mathbf{t} := (t_0, \dots, t_m)$ is called a **presentation** of the Cartier divisor $D$.
For $P \in \mathcal{X} \setminus \operatorname{supp}(D)$, we define

$$\lambda_{\mathcal{D}}(P) := \max_k \min_l \log \left| \left(s_k \otimes (t_l \otimes s_D)^{-1}\right)(P) \right|$$

Notice that $\left(s_k \otimes (t_l \otimes s_D)^{-1}\right)$ is a rational function on $\mathcal{X}$. We call $\lambda_{\mathcal{D}}(P)$ the **local height** of $P$ relative to the presentation $\mathcal{D}$ of $D$ and by abusing notation sometimes simply *relative to* $D$.

# Heights on weighted projective varieties I

## Global heights

Consider now the case when $k$ is a number field. As above $\mathcal{X}$ is an irreducible projective variety defined over $k$ and $D$ a Cartier divisor on $\mathcal{X}$ with presentation as above. Let $F$ be a number field with $k \subset F \subset \bar{k}$ and $P \in \mathcal{X}(F) \setminus \mathrm{supp}(D)$. For $\nu \in M_F$ we define the local height as

$$\lambda_{\mathcal{D}}(P, \nu) := \max_k \min_l \log \left| \left( s_k \otimes (t_l \otimes s_D)^{-1} \right) (P) \right|_\nu$$

For $P \in \mathcal{X}$ there exists $s_j$ and $t_l$ such that $s_j(P) \neq 0$ and $t_l(P) \neq 0$. So we can find a meromorphic function of $O(D)$ such that $P$ is not contained in the support of the Cartier divisor $D(s)$. Then $\mathcal{D}(s) = (s; L, \mathbf{s}; M, \mathbf{t})$ is a presentation of $\mathcal{D}(s)$ and

$$\lambda_{\mathcal{D}(s)} = \lambda_{\mathcal{D}} + \lambda_f,$$

where $f$ is the rational function $s \otimes s_D$.
If $F$ is a finite extension of $k$ such that $P \in \mathcal{X}(F)$, the local height $\lambda_{\mathcal{D}(s)}(P, \nu)$ is finite for any $\nu \in M_L$, because $P \notin \mathrm{supp}(\mathcal{D}(s))$. Hence, we define th global height of $P$ relative to $\lambda_{\mathcal{D}}$ as

$$h(P) := \sum_{\nu \in M_F} \lambda_{\mathcal{D}(s)}(P, \nu).$$

### Proposition

*The global height $h$ is independent of the choices of $F$ and of the section $s$.*

See [3, Prop. 2.3.4].

# Heights on weighted projective varieties I

## Weil heights

Let $\mathcal{X}$ be a projective variety over $\bar{k}$ and

$$\varphi : \mathcal{X} \to \mathbb{P}^n(\bar{k}),$$

a morphism over $\bar{k}$. The **Weil height** of $P \in \mathcal{X}(\bar{k})$, relative to $\varphi$ is defined as the

$$h_\varphi(P) := H(\varphi(P)),$$

where $H$ is the usual height on $\mathbb{P}^n(\bar{k})$. Every Weil height may be viewed as a global height. Conversely, we can write any global height as a difference of two Weil height.

# Weighted Heights I

Let $\mathfrak{w} = (q_0, \ldots, q_n)$ be a set of heights and $\mathbb{WP}^n_{\mathfrak{w}}(k)$ the weighted projective space over a number field $k$. Let $\mathfrak{p} \in \mathbb{WP}^n(\bar{k})$ a point such that $\mathfrak{p} = [x_0, \ldots, x_n]$. We follow the definitions of [2] to define the weighted height in $\mathbb{WP}^n_{\mathfrak{w}}(\bar{k})$.

The **weighted multiplicative height** of $\mathfrak{p}$ is defined as

$$\mathfrak{h}(\mathfrak{p}) := \prod_{v \in M_k} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \ldots, |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{3}$$

and the **logarithmic weighted height** as

$$\log \mathfrak{h}(\mathfrak{p}) := \log \mathfrak{h}_k(\mathfrak{p}) = \sum_{v \in M_k} \max_{0 \le j \le n} \left\{ \frac{n_v}{q_j} \cdot \log |x_j|_v \right\}. \tag{4}$$

Then we have the following.

### Proposition

*The following are true:*
*i)* $\mathfrak{h}_k(\mathfrak{p})$ *does not depend on the choice of coordinates of* $\mathfrak{p}$*.*
*ii)* $\mathfrak{h}_k(\mathfrak{p}) \geq 1$*.*

Next we will interpret the weighted height on weighted varieties in an analogue way to Weil height on projective varieties.

# Weighted Heights I

## Local heights on weighted projective varieties

Let $k$ be a field and $|\cdot|$ a fixed absolute value on $\bar{k}$. Let $\mathcal{X}$ be a weighted projective variety over $k$, which we assume that is irreducible.
Let $D$ be a Cartier divisor on $\mathcal{X}$ with associated bundle $O(D)$ and meromorphic section $s_D$. Then there are line bundles on $\mathcal{X}$ such that

$$O(D) \cong L \otimes M^{-1}.$$

Choose global sections $s_0, \dots, s_n$ of $L$ and $t_0, \dots, t_m$ of $M$. The data

$$\mathcal{D} := (s_D; L, s; M, t),$$

where $(s) := (s_0, \dots, s_n)$ and $\mathbf{t} := (t_0, \dots, t_m)$ is called a **presentation** of the Cartier divisor $D$.
For $P \in \mathcal{X} \setminus \text{supp}(D)$, we define

$$\lambda_{\mathcal{D}}(P) := \max_r \min_s \log \left| \left( s_r \otimes (t_s \otimes s_D)^{-1} \right) (P) \right|$$

Notice that $\left( s_k \otimes (t_l \otimes s_D)^{-1} \right)$ is a rational function on $\mathcal{X}$. We call $\lambda_{\mathcal{D}}(P)$ the **local height** of $P$ relative to the presentation $\mathcal{D}$ of $D$ and by abusing notation sometimes simply *relative to* $D$.
Let $F$ be a number field such that $k \subset F \subset \bar{k}$ and let $\mathfrak{p} \in \mathcal{X}(F) \setminus \text{supp}(D)$. For $\nu \in M_F$ we define the **local height**

$$\lambda_{\mathcal{D}}(\mathfrak{p}, \nu) := \max_r \min_s \log \left| \left( s_r \otimes (t_s \otimes s_D)^{-1} \right) (P) \right|_\nu$$

# Weighted Heights II

## Local heights on weighted projective varieties

Let $p \in \mathbb{Q}$ be the prime such that the restriction of $\nu|$ to $\mathbb{Q}$ is equal to $| \ |_p$. Let $| \ |_\mu$ be an absolute value on $\bar{k}$, such that its restriction to $k$ is equivalent to $| \ |_\nu$. Then,

$$\lambda_{\mathcal{D}}(\mathfrak{p}, \nu) = \frac{[F_\nu : \mathbb{Q}_p]}{[F : \mathbb{Q}]} \lambda_{\mathcal{D}}(\mathfrak{p}, \mu),$$

where $\lambda_{\mathcal{D}}(\mathfrak{p}, \mu)$ is the local height relative to the absolute value $| \ |_\mu$. So the theory of local heights over $\bar{k}$ can be applied to any norm on $k$.

The hyperplane $\{x_i = 0\}$ in $\mathbb{WP}^n_{\mathfrak{w}}(k)$ has the presentation

$$\mathcal{D} = \left( x_i : \mathcal{O}_{\mathbb{WP}^n_{\mathfrak{w}}}(1), x_0, \dots, x_n; \mathcal{O}_{\mathbb{WP}^n_{\mathfrak{w}}}, 1 \right)$$

For a point $\mathfrak{p} \in \mathbb{WP}^n_{\mathfrak{w}}(F)$ with $x_i(\mathfrak{p}) \neq 0$ and $\nu \in M_F$ the corresponding **local weighted height** is

$$\lambda_{\mathcal{D}}(\mathfrak{p}, \nu) := \max \left\{ \log |x_0|_v^{\frac{n_v}{q_0}}, \dots, \log |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{5}$$

and the product formula becomes

$$h(\mathfrak{p}) = \sum_{\nu \in M_F} \lambda_{\mathcal{D}}(\mathfrak{p}, \nu).$$

### Proposition

*The height defined in Eq.* (5) *is a local height.*

# Weighted Heights I

## Global heights on weighted projective varieties

Let $k$ be a number field, $\mathcal{X}$ is an irreducible projective variety defined over $k$, and $D$ a Cartier divisor on $\mathcal{X}$ with presentation as above. Let $F$ be a number field with $k \subset F \subset \bar{k}$ and $P \in \mathcal{X}(F) \setminus \text{supp}(D)$. For $\nu \in M_F$ we define the local height as

$$\lambda_{\mathcal{D}}(P, \nu) := \max_k \min_l \log \left| \left( s_k \otimes (t_l \otimes s_D)^{-1} \right) (P) \right|_\nu$$

For $P \in \mathcal{X}$ there exists $s_j$ and $t_l$ such that $s_j(P) \neq 0$ and $t_l(P) \neq 0$. So we can find a meromorphic function of $O(D)$ such that $P$ is not contained in the support of the Cartier divisor $D(s)$. Then $\mathcal{D}(s) = (s; L, \mathbf{s}; M, \mathbf{t})$ is a presentation of $\mathcal{D}(s)$ and

$$\lambda_{\mathcal{D}(s)} = \lambda_{\mathcal{D}} + \lambda_f,$$

where $f$ is the rational function $s \otimes s_D$.

If $F$ is a finite extension of $k$ such that $P \in \mathcal{X}(F)$, the local height $\lambda_{\mathcal{D}(s)}(P, \nu)$ is finite for any $\nu \in M_L$, because $P \notin \text{supp}(\mathcal{D}(s))$. Hence, we define the **global height** of $P$ relative to $\lambda_{\mathcal{D}}$ as

$$h(P) := \sum_{\nu \in M_F} \lambda_{\mathcal{D}(s)}(P, \nu).$$

### Proposition

*The global height $h$ is independent of the choices of $F$ and of the section $s$.*

# Weighted Heights II

## Global heights on weighted projective varieties

### Definition

The **weighted multiplicative height** of $\mathfrak{p}$ as

$$\mathfrak{h}_k(\mathfrak{p}) := \prod_{v \in M_k} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \dots, |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{6}$$

The **logarithmic height** of the point $\mathfrak{p}$ is defined as follows

$$\mathfrak{h}'_k(\mathfrak{p}) := \log \mathfrak{h}_k(\mathfrak{p}) = \sum_{v \in M_k} \max_{0 \leq j \leq n} \left\{ \frac{n_v}{q_j} \cdot \log |x_j|_v \right\}. \tag{7}$$

### Proposition

*The height defined in Eq.* (6) *is a global height.*

Let $\mathcal{X}$ be a weighted projective variety over $\bar{k}$ and $\varphi : \mathcal{X} \to \mathbb{WP}^n(\bar{k})$ a morphism. The **weighted Weil height** of $\mathfrak{p} \in \mathcal{X}(\bar{k})$, relative to $\varphi$, is defined as

$$wh_\varphi(\mathfrak{p}) := \mathfrak{h}(\varphi(\mathfrak{p})).$$

### Proposition

*Every weighted Weil height can be is a global height. Moreover, every global height can be written as a difference of two weighted Weil heights.*

## Applications to superelliptic curves

# Binary forms I

Let $\mathcal{X}_g$ be a superelliptic curve of genus $g \geq 2$ with affine equation

$$z^m y^{d-m} = f(x, y) = a_d x^d + a_{d-1} x^{d-1} y + \cdots + a_1 x y^{d-1} + a_0 y^d \tag{8}$$

defined over and algebraic number field $k$; see [8].
Isomorphism classes of such curves are classified by the invariants of binary forms, since they are invariants under any coordinate change.
Let $k[x, y]$ be the polynomial ring in two variables and $V_d$ the $(d+1)$-dimensional subspace of $k[x, y]$ consisting of homogeneous polynomials $f(x, y)$ of degree $d$. Elements in $V_d$ are called **binary forms** of degree $d$.
$GL_2(k)$ acts as a group of automorphisms on $k[x, y]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \text{ then } \quad M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \tag{9}$$

Denote by $f^M$ the binary form $f^M(x, y) := f(ax + by, cx + dy)$. It is well known that $SL_2(k)$ leaves a bilinear form (unique up to scalar multiples) on $V_d$ invariant.
Consider $a_0, a_1, \ldots, a_d$ as parameters (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 $I^M \in k[a_0, \ldots, a_d]$ as follows

$$I^M(f) := I(f^M) \tag{10}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (10) defines an action of $GL_2(k)$ on $k[a_0, \ldots, a_d]$. A homogeneous polynomial $I \in k[a_0, \ldots, a_d, x, y]$ is called a **covariant** of index $s$ if $I^M(f) = \delta^s I(f)$, where $\delta = \det(M)$. The

# Binary forms II

homogeneous degree in $a_0, \dots, a_d$ 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 $V_d$.
One of the most important results of the classical invariants theory is Hilbert's theorem that says that the ring of invariants of binary forms is finitely generated. We denote by $\mathcal{R}_d$ the ring of invariants of the binary forms of degree $d$.

### Proposition

*i) $\mathcal{R}_d$ is finitely generated*
*ii) $\mathcal{R}_d$ is a graded ring*

Let us see what happens to the invariants when we change the coordinates, in other words when we act on the binary form $g(x, y)$ via $M \in GL_2(k)$. Let $I_0, \dots, I_n$ be the generators of $\mathcal{R}_d$ with degrees $q_0, \dots, q_n$ respectively. We denote the tuple of invariants by $\mathcal{I} := (I_0, \dots, I_n)$. The following result is fundamental to our approach.

### Proposition

*For any two binary formal $f$ and $g$, $f = g^M$, $M \in GL_2(k)$, if and only if*

$$(I_0(f), \dots I_i(f), \dots, I_n(f)) = (\lambda^{q_0}\, I_0(g), \dots, \lambda^{q_i}\, I_i(g), \dots, \lambda^{q_n}\, I_n(g), ) \, ,$$

*where $\lambda = (\det M)^{\frac{d}{2}}$.*

Next we give a brief description for cases of binary sextics and binary octavics, no only because of their significance in cryptography, but also to show that such approach is concrete and constructive.

# Binary sextics I

If $\deg f = 6$ binary forms are called *binary sextics* and their invariants are $J_2, J_4, J_6, J_{10}$, which are called *arithmetic invariants*.

**Lemma**
*$J_{2i}$ are homogeneous polynomials in $k[a_0, \dots, a_6]$ of degree $2i$, for $i = 1, 2, 3, 5$. Moreover, they generate $\mathcal{R}_6$.*

For a genus two curve $C$ with projective equation $z^2y^4 = f(x, y)$ we denote by $J_{2i}(C) := J_{2i}(f)$, for $i = 1, 2, 3, 5$.

**Lemma**
*Two genus 2 curves $C$ and $C'$ are isomorphic over $\bar{k}$ if and only if there exists an $\lambda \neq 0$ such that*

$$J_{2i}(C) = \lambda^{2i} \cdot J_{2i}(C'), \qquad \textit{for} \quad i = 1, 2, 3, 5.$$

*Moreover, if the transformation between binary sextics is given through a matrix $M$, then $\lambda = (\det M)^3$.*

Hence, to study isomorphism classes of genus 2 curves it is equivalent as considering tuples of invariants $(J_2, J_4, J_6, J_{10})$.

# Binary octavics I

If $\deg f = 8$, then $f(x, y)$ is called a binary octavic. Invariants of $V_8$ are denoted by $J_2, J_3, \dots, J_8$. They are primitive homogeneous polynomials $J_i \in k[a_0, \dots, a_8]$ of degree $i$, for $i = 2, \dots, 10$. For any $M = \in GL_2(k)$, we have

$$J_i(f^M) = (\det M)^{4i}\, J_i(f),$$

for $i = 2, \dots, 10$. $\mathcal{R}_8$ is finitely generated as a module over $k[J_2, \dots, J_7, J_8]$. Moreover, invariants $J_2, \dots, J_8$ satisfy the following equation

$$J_8^5 + \frac{I_8}{3^4 \cdot 5^3} J_8^4 + 2 \cdot \frac{I_{16}}{3^8 \cdot 5^6} J_8^3 + \frac{I_{24}}{2 \cdot 3^{12} \cdot 5^6} J_8^2 + \frac{I_{32}}{3^{16} \cdot 5^{10}} J_8 + \frac{I_{40}}{2^2 \cdot 3^{20} \cdot 5^{12}} = 0, \tag{11}$$

where $I_{8j}$ are invariants of degree $8j$ for $j = 1, \dots, 5$.
Hence, the isomorphism class of a binary octavic corresponds to a tuple of invariants $(J_2, \dots, J_7, J_8)$ which satisfy the equation above. In terms of genus 3 hyperelliptic curves we have the following.

### Lemma

*Two genus 3 hyperelliptic curves $C$ and $C'$ given by equations $C: \; z^2 = f(x, y)$ and $C': \; z^2 = g(x, y)$ are isomorphic over $\bar{k}$ if and only if there exists some $\lambda \in k \setminus \{0\}$ such that*

$$J_i(C) = \lambda^i \cdot J_i(C'), \; \textit{for} \;\; i = 2, \dots, 8.$$

# Proj $\mathcal{R}_d$ as a weighted projective space I

Since $I_0, \dots, I_i, \dots, I_n$ are homogenous polynomials, then $\mathcal{R}_d$ is a graded ring. Hence, Proj $\mathcal{R}_d$ is a weighted projective space $\mathbb{WP}^n_{\mathfrak{w}}(k)$ for

$$\mathfrak{w} = (\deg I_0, \deg I_1, \dots, \deg I_i, \dots, \deg I_n)\,.$$

**Lemma**

*Let $I_0, I_1, \dots, I_n$ be the generators of the ring of invariants $\mathcal{R}_d$ of degree $d$ binary forms. A $k$-isomorphism class of a binary form $f$ is determined by the point*

$$\mathcal{I}(f) := [I_0(f), I_1(f), \dots, I_n(f)] \in \mathbb{WP}^n_{\mathfrak{w}}(k).$$

*Moreover $f = g^M$ for some $M \in GL_2(K)$ if and only if $\mathcal{I}(f) = \lambda \star \mathcal{I}(g)$, for $\lambda = (\det A)^{\frac{d}{2}}$.*

**Corollary**

*Let $\mathcal{X}$ be a superelliptic curve with equation as in Eq.* (8)*. The $\bar{k}$-isomorphism class of $\mathcal{X}$ is determined by the weighted moduli point $\mathfrak{p} := [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathfrak{w}}(k)$.*

Hence we have the following problem.

**Problem**

*Let $\mathcal{X}$ be a given superelliptic curve with equation $z^m = f(x)$, $\deg f = d$, defined over $\mathcal{O}_k$, and with corresponding moduli point $\mathfrak{p} := [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathfrak{w}}(k)$. Find a representation of $\mathfrak{p} \in \mathbb{WP}^n_{\mathfrak{w}}(k)$ with smallest coordinates.*

# Integral binary forms with smallest moduli height I

**Problem**

*Determine an equation of the curve $\mathcal{X}$, say $z^m y^{d-m} = g(x,y)$, defined over $\mathcal{O}_k$, such that $g(x,y)$ has minimal invariants.*

We say that a binary form $f(x,y)$ has a **minimal model** over $k$ if it is integral (i.e. $f \in \mathcal{O}_k[x,y]$) and $\mathfrak{s}(\mathcal{I}(f))$ is minimal. Let $f \in \mathcal{O}_k$ and $\mathbf{x} := \mathcal{I}(f) \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{O}_k)$ its corresponding weighted moduli point. We define the **weighted valuation** of the tuple $\mathbf{x} = (x_0, \dots x_n)$ at the prime $p \in \mathcal{O}_k$ as

$$\mathbf{val}_p(\mathbf{x}) := \max \left\{ j \mid p^j \text{ divides } x_i^{q_i} \text{ for all } i = 0, \dots n \right\},$$

Then we have the following.

**Proposition**

*A binary form $f \in V_d$ is a minimal model over $\mathcal{O}_k$ if for every prime $p \in \mathcal{O}_k$ such that $p \mid wgcd(\mathcal{I}(f))$ the following holds*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i$$

*for all $i = 0, \dots, n$. Moreover, for every integral binary form $f$ its minimal model exist.*

Notice that it is possible to find a twist of $f$ with ”smaller” invariants. In this case the new binary form is not in the same $SL_2(\mathcal{O}_k)$-orbit as $f$. For example, the transformation

$$(x,y) \to \left( \frac{1}{\lambda^{\frac{2}{d}}} x, \frac{1}{\lambda^{\frac{2}{d}}} y, \right). \tag{12}$$

## Integral binary forms with smallest moduli height II

will give us the form with smallest invariants, but not necessarily $k$-isomorphic to $f$.
It is worth noting that for a binary form $f$ given in its minimal model, the point $\mathcal{I}(f)$ is not necessarily normalized as in the sense of [2].

### Corollary

*If $f(x,y) \in \mathcal{O}_k[x,y]$ is a binary form such that $\mathcal{I}(f) \in \mathbb{WP}^n_{\mathfrak{w}}(k)$ is normalized over $k$, then $f$ is a minimal model over $\mathcal{O}_k$.*

### Example

*Let be given the sextic*

$$f(x,y) = 7776x^6 + 31104x^5y + 40176x^4y^2 + 25056x^3y^3 + 8382x^2y^4 + 1470xy^5 + 107y^6$$

*Notice that the polynomial has content 1, so there is no obvious substitution here to simplify sextic. The moduli point is $\mathfrak{p} = [J_2 : J_4 : J_6 : J_{10}]$, where*

$$\begin{aligned} J_2 &= 2^{15} \cdot 3^5, \\ J_4 &= -2^{12} \cdot 3^9 \cdot 101 \cdot 233, \\ J_6 &= 2^{16} \cdot 3^{13} \cdot 29 \cdot 37 \cdot 8837, \\ J_{10} &= 2^{26} \cdot 3^{21} \cdot 11 \cdot 23 \cdot 547 \cdot 1445831 \end{aligned}$$

□

# Integral binary forms with smallest moduli height III

Recall that the transformation $(x, y) \to \left(\frac{1}{p}x, y\right)$ will change the representation of the point $\mathfrak{p}$ via

$$\frac{1}{p^3} \star [J_2 : J_4 : J_6 : J_{10}] = \left[\frac{1}{p^6} J_2 : \frac{1}{p^{12}} J_4 : \frac{1}{p^{18}} J_6 : \frac{1}{p^{30}} J_{10}\right]$$

So we are looking for prime factors $p$ such that $p^6 | J_2$, $p^{12} | J_4$, $p^{18} | J_6$, and $p^{30} | J_{10}$. Such candidates for $p$ have to be divisors of $wgcd(\mathfrak{p}) = 2^2 \cdot 3^2$.
Obviously neither $p = 2$ or $p = 3$ will work. Thus, $f(x, y)$ is in its minimal model over $\mathcal{O}_k$.

$\square$

### Corollary

*The transformation of $f(x, y)$ by the matrix*

$$M = \begin{bmatrix} \varepsilon_d \frac{1}{(wgcd(I(f)))^{\frac{2}{d}}} & 0 \\ 0 & \varepsilon_d \frac{1}{(wgcd(I(f)))^{\frac{2}{d}}} \end{bmatrix}$$

*where $\varepsilon_d$ is a $d$-primitive root of unity, will always give a minimal set of invariants.*

# Weierstrass equations with minimal moduli height I

Now we will consider the minimal models of curves over $\mathcal{O}_k$. Let $\mathcal{X}$ be as in Eq. (8) and $\mathfrak{p} = [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathfrak{w}}(k)$. Let us assume that for a prime $p \in \mathcal{O}_k$, we have $\nu_p\left(wgcd(\mathfrak{p})\right) = \alpha$. If we use the transformation $x \to \frac{x}{p^\beta} x$, for $\beta \leq \alpha$, then from Prop. 10 the set of invariants will become

$$\frac{1}{p^{\frac{d}{2}\beta}} \star \mathcal{I}(f)$$

To ensure that the moduli point $\mathfrak{p}$ is still with integer coefficients we must pick $\beta$ such that $p^{\frac{\beta d}{2}}$ divides $p^{\nu_p(x_i)}$ for $i = 0, \ldots, n$. Hence, we must pick $\beta$ as the maximum integer such that $\beta \leq \frac{2}{d}\nu_p(x_i)$, for all $i = 0, \ldots, n$. This is the same $\beta$ as in Prop. 11. The transformation

$$(x, y) \to \left( \frac{x}{p^\beta}, y \right),$$

has corresponding matrix $M = \begin{bmatrix} \frac{1}{p^\beta} & 0 \\ 0 & 1 \end{bmatrix}$ with $\det M = \frac{1}{p^\beta}$. Hence, from Prop. 10 the moduli point $\mathfrak{p}$ changes as $\mathfrak{p} \to \left(\frac{1}{p^\beta}\right)^{d/2} \star \mathfrak{p}$, which is still an integer tuple. We do this for all primes $p$ dividing $wgcd(\mathfrak{p})$. Notice that the new point is not necessarily normalized in $\mathbb{WP}^n_{\mathfrak{w}}(k)$ since $\beta$ is not necessarily equal to $\alpha$. This motivates the following definition.

# Weierstrass equations with minimal moduli height II

### Definition

Let $\mathcal{X}$ be a superelliptic curve defined over an integer ring $\mathcal{O}_k$ and $\mathfrak{p} \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{O}_k)$ its corresponding weighted moduli point. We say that $\mathcal{X}$ has a **minimal model** over $\mathcal{O}_k$ if for every prime $p \in \mathcal{O}_k$ the **valuation of the tuple** at $p$

$$\mathbf{val}_p(\mathfrak{p}) := \max\{\nu_p(x_i) \text{ for all } i = 0, \dots n\},$$

is minimal, where $\nu_p(x_i)$ is the valuation of $x_i$ at the prime $p$.

### Theorem

*Minimal models of superelliptic curves exist. An equation $\mathcal{X} : z^m y^{d-m} = f(x, y)$ is a minimal model over $\mathcal{O}_k$, if for every prime $p \in \mathcal{O}_k$ which divides $p \mid wgcd(\mathcal{I}(f))$, the valuation $\mathbf{val}_p$ of $\mathcal{I}(f)$ at $p$ satisfies*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i, \tag{13}$$

*for all $i = 0, \dots, n$. Moreover, then for $\lambda = wgcd(\mathcal{I}(f))$ with respect the weights $\left(\left\lfloor \frac{dq_0}{2} \right\rfloor, \dots, \left\lfloor \frac{dq_n}{2} \right\rfloor\right)$ the transformation*

$$(x, y, z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z\right)$$

*gives the minimal model of $\mathcal{X}$ over $\mathcal{O}_k$. If $m|d$ then this isomorphism is defined over $k$.*

Let us see an example from curves of genus 2.

# Weierstrass equations with minimal moduli height III

**Example**

*Let $\mathcal{X}$ be a genus 2 curve with equation $z^2y^4 = f(x,y)$ as in **??** 4. By applying the transformation*

$$(x,y,z) \to \left(\frac{x}{6}, y, 6^3 \cdot z\right)$$

*we get the equation*

$$z^2 = x^6 + 24x^5 + 186x^4 + 696x^3 + 1397x^2 + 1470x + 642. \tag{14}$$

*Computing the moduli point of this curve we get*

$$\mathfrak{p} = [2^{11} \cdot 3 : -2^4 \cdot 3 \cdot 101 \cdot 233 : 2^4 \cdot 3 \cdot 29 \cdot 37 \cdot 8837 : 2^6 \cdot 3 \cdot 11 \cdot 23 \cdot 547 \cdot 1445831],$$

*which is obviously normalized in $\mathbb{WP}^3_{\mathfrak{w}}(\mathbb{Q})$ since $wgcd(\mathfrak{p}) = 1$. Hence, the Eq.* (14) *is a minimal model.* □

**Corollary**

*There exists a curve $\mathcal{X}'$ given in **??** isomorphic to $\mathcal{X}$ over the field $K := k\left(wgcd(\mathfrak{p})^{\frac{d}{m}}\right)$ with minimal $SL_2(\mathcal{O}_k)$-invariants. Moreover, if $m|d$ then $\mathcal{X}$ and $\mathcal{X}'$ are $k$-isomorphic.*

For hyperelliptic curves: $m = 2$ and $d = 2g + 2$. Hence, $\mathcal{X}$ and $\mathcal{X}'$ would always be isomorphic over $k$.

**Corollary**

*Given a hyperelliptic curve $\mathcal{X}$ defined over a ring of integers $\mathcal{O}_k$. There exists a curve $\mathcal{X}'$ $k$-isomorphic to $\mathcal{X}$ with minimal $SL_2(\mathcal{O}_k)$-invariants.*

# Generalized greatest common divisors I

The following setup is taken from [14].
For any two elements $\alpha, \beta \in \mathcal{O}_k$ the **greatest common divisor** is defined as

$$\gcd(\alpha, \beta) := \prod_{p \in \mathcal{O}_k} p^{\min\{\nu_p(\alpha), \nu_p(\beta)\}}$$

The **logarithmic greatest common divisor** is

$$\log \gcd(\alpha, \beta) := \sum_{\nu \in M_k^0} \min\left\{\mathfrak{v}(\alpha), v(\beta)\right\}$$

For a valuation $\nu \in M_k$, we define the **extension of $\nu$ to $k$** as

$$\begin{aligned} \nu^+ : k &\longrightarrow [0, \infty], \\ \alpha &\longrightarrow \max\{v(\alpha), 0\}. \end{aligned}$$

The **generalized logarithmic greatest common divisor** of two elements $\alpha, \beta \in k$ is defined as

$$\operatorname{hgcd}(\alpha, \beta) := \sum_{\nu \in M_k} \min\{\nu^+(\alpha), \nu^+(\beta)\}.$$

# Generalized greatest common divisors II

Notice that $\nu^+$ can be viewed as a height function on $\mathbb{P}^1(k) = k \cup \{\infty\}$, where we set $\nu^+(\infty) = 0$. This leads to the generalized logarithmic greatest common divisor being viewed also as a height function:

$$\begin{aligned} G_\nu : \mathbb{P}^1(k) \times \mathbb{P}^1(k) &\to [0, \infty] \\ (\alpha, \beta) &\to \min\{\nu^+(\alpha), \nu^+(\beta)\} \end{aligned}$$

In view of the above we have

$$\operatorname{hgcd}(\alpha, \beta) = \sum_{\nu \in M_k} G_\nu.$$

In [14] it was given a theoretical interpretation of the function $G_\nu$ in terms of blowups.

**Theorem (Silverman 2004)**

*The generalized logarithmic gcd of $\alpha$ and $\beta$ is equal to the Weil height of $(\alpha, \beta)$ on a blowup of $(\mathbb{P}^1)^2$ with respect to the exceptional divisor of the blowup.*

So we generalize the notion of the greatest common divisor to any variety blowup along an arbitrary subvariety.

Let $\mathcal{X}/k$ be a smooth variety and $\mathcal{Y}/k \subset \mathcal{X}/k$ be a subvariety of codimension $r \geq 2$. Let $\pi : \tilde{\mathcal{X}} \to \mathcal{X}$ be the blowup of $\mathcal{X}$ along $\mathcal{Y}$ and let $\tilde{\mathcal{Y}} = \pi^{-1}(\mathcal{Y})$ be the exceptional divisor of the blowup. For any $P \in \mathcal{X} \setminus \mathcal{Y}$, denote by $\tilde{P} = \pi^{-1}(P) \in \tilde{\mathcal{X}}$. Then,

$$\operatorname{hgcd}(P; \mathcal{Y}) = h_{\tilde{\mathcal{X}}, \tilde{\mathcal{Y}}}(\tilde{P}).$$

# Generalized weighted greatest common divisors I

Details can be found in [11]. Let $\mathbf{x} = (x_0, \ldots, x_n) \in \mathcal{O}_k^{n+1}$. Then,

$$wgcd_{\mathfrak{w}}(\mathbf{x}) = \prod_{p \in \mathcal{O}_k} p^{\min\left\{ \left\lfloor \frac{\nu_p(x_0)}{q_0} \right\rfloor, \ldots, \left\lfloor \frac{\nu_p(x_n)}{q_n} \right\rfloor \right\}}$$

The logarithmic weighted greatest common divisor is

$$\log wgcd_{\mathfrak{w}}(\mathbf{x}) = \sum_{\nu \in M_k^0} \min \left\{ \left\lfloor \frac{\nu_p(x_0)}{q_0} \right\rfloor, \ldots, \left\lfloor \frac{\nu_p(x_n)}{q_n} \right\rfloor \right\}$$

For a valuation $\nu \in M_k$, we define the **extension of $\nu$ to $k$** as

$$\begin{aligned} \nu^+ : k &\longrightarrow [0, \infty], \\ \alpha &\longrightarrow \max\{v(\alpha), 0\}. \end{aligned}$$

Consider now $\mathbf{x} = (x_0, \ldots, x_n) \in k^{n+1}$. The **generalized weighted greatest common divisor** is defined as

$$\mathrm{hwgcd}_{\mathfrak{w}}(\mathbf{x}) = \prod_{p \in \mathcal{O}_k} p^{\min\left\{ \left\lfloor \frac{\nu_p^+(x_0)}{q_0} \right\rfloor, \ldots, \left\lfloor \frac{\nu_p^+(x_n)}{q_n} \right\rfloor \right\}}$$

# Generalized weighted greatest common divisors II

and the logarithmic generalized weighted greatest common divisor is

$$\log \operatorname{hwgcd}_{\mathfrak{w}}(\mathbf{x}) = \sum_{\nu \in M_k^0} \min \left\{ \left\lfloor \frac{\nu_p^+(x_0)}{q_0} \right\rfloor, \dots, \left\lfloor \frac{\nu_p^+(x_n)}{q_n} \right\rfloor \right\}$$

Now we have

$$\begin{aligned} T_\nu : \quad & \mathbb{WP}_{\mathfrak{w}}^n(k) \to [0, \infty] \\ & (x_0, \dots, x_n) \to \min \left\{ \left\lfloor \frac{\nu_p^+(x_0)}{q_0} \right\rfloor, \dots, \left\lfloor \frac{\nu_p^+(x_n)}{q_n} \right\rfloor \right\} \end{aligned}$$

Then we have

$$\operatorname{hwgcd}(\mathbf{x}) = \sum_{\nu \in M_k} T_\nu(\mathbf{x})$$

Let $\pi : \tilde{\mathcal{X}} \to \mathbb{WP}_{\mathfrak{w}}^n(k)$ be the blowup of $\mathbb{WP}_{\mathfrak{w}}^n(k)$ at the point $O = (0, \dots, 0)$ and let $E := \pi^{-1}(O)$ be the exceptional divisor for this blowup.

# Generalized weighted greatest common divisors III

**Lemma**

*Let $\mathcal{X}$ be a weighted projective variety and $\mathcal{Y} \subset \mathcal{X}$ a closed subvariety. The blow-up $\pi : \tilde{\mathcal{X}} \to \mathcal{X}$ of $\mathcal{Y}$ has the following properties:*
*i)* $\pi\,|_{\pi^{-1}(\mathcal{X}\setminus\mathcal{Y})} \,:\, \pi^{-1}(\mathcal{X} \setminus \mathcal{Y}) \to \mathcal{X} \setminus \mathcal{Y}$ *is an isomorphism.*
*ii) the exceptional divisor* $E = \pi^{-1}(\mathcal{Y})$ *is an effective Cartier divisor on* $\tilde{\mathcal{X}}$.

**Lemma**

*Let $\nu \in M_k$. Then the local weighted height function on $\tilde{\mathcal{X}}$ for the divisor $E$, corresponding to $\nu$, is given by the formula*

$$\lambda_{\tilde{\mathcal{X}},E}(\pi^{-1}(\alpha_0, \dots, \alpha_n), \nu) = \min \left\{ \left\lfloor \frac{\nu_p^+(\alpha_0)}{q_0} \right\rfloor, \dots, \left\lfloor \frac{\nu_p^+(\alpha_n)}{q_n} \right\rfloor \right\}$$

*for all* $(\alpha_0, \dots, \alpha_n) \in \mathcal{X}(k) \setminus \{(0, \dots, 0)\}$.

Then we have the following; see [11].

**Theorem (Sh-19)**

*The generalized logarithmic weighted greatest common divisor is equal to the weighted height of $\mathbf{x}$ on a blowup of $\mathbb{WP}^n_{\mathfrak{w}}(k)$ with respect to the exceptional divisor of the blowup. In other words*

$$\log \operatorname{hwgcd}(\mathbf{x}) = \sum_{\nu \in M_k} \lambda_{\tilde{\mathcal{X}},E}(\pi^{-1}(\mathbf{x}), \nu) = \lambda_{\tilde{\mathcal{X}},E}\left(\pi^{-1}(\mathbf{x}), \nu\right)$$

# References I


[1] E. Artal Bartolo, J. Martin-Morales, and J. Ortigas-Galindo, *Cartier and Weil divisors on varieties with quotient singularities*, Internat. J. Math. **25** (2014), no. 11, 1450100, 20.

[2] L. Beshaj, J. Gutierrez, and T. Shaska, *Weighted greatest common divisors and weighted heights*, 2019. submitted.

[3] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, 2006.

[4] P. Corvaja and U. Zannier, *Some cases of Vojta's conjecture on integral points over function fields*, J. Algebraic Geom. **17** (2008), no. 2, 295–333.

[5] Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981), 1982, pp. 34–71.

[6] J. Gutierrez and T. Shaska, *An algorithm for determining equations for superelliptic curves with minimal invariants*, arXiv:1904.08905 (2019).

[7] J. Hausen, S. Keicher, and A. Laface, *On blowing up the weighted projective plane*, Math. Z. **290** (2018), no. 3-4, 1339–1358.

[8] R. Hidalgo, S. Quispe, and T. Shaska, *On generalized superelliptic riemann surfaces*, Manuscripta Math. **to appear** (2019).

[9] M. Hindry and J. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000.

[10] Irving Kaplansky, *Commutative rings*, The University of Chicago Press, 1974.

[11] T. Shaska, *Minimal models for superelliptic curves*, 2019. In progress.

[12] ______, *Weighted greatest common divisors and local heights on wps blown-up at a point, relative to the exceptional divisor*, 2019. In progress.

[13] T. Shaska and J. Mandili, *Computing heights on weighted projective spaces*, Algebraic curves and their applications, 2019, pp. 149–160.

[14] J. H. Silverman, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monatsh. Math. **145** (2005), no. 4, 333–350.

[15] Joseph H. Silverman, *Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture*, J. Number Theory **133** (2013), no. 9, 2948–2963.

[16] J. Steenbrink, *On the Picard group of certain smooth surfaces in weighted projective spaces*, Algebraic geometry, 1982, pp. 302–313.

[17] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[18] A. Turchet, *Fibered threefolds and Lang-Vojta's conjecture over function fields*, Trans. Amer. Math. Soc. **369** (2017), no. 12, 8537–8558.

[19] Yu Yasufuku, *Vojta's conjecture on rational surfaces and the $abc$ conjecture*, Forum Math. **30** (2018), no. 3, 631–649.