Contemporary Mathematics

Reduction of superelliptic Riemann surfaces

Tanush Shaska

Abstract. For a superelliptic curve $\mathcal{X}$, defined over $\mathbb{Q}$, let $\mathfrak{p}$ denote the corresponding moduli point in the weighted moduli space. We describe a method how to determine a minimal integral model of $\mathcal{X}$ such that: i) the corresponding moduli point $\mathfrak{p}$ has minimal weighted height, ii) the equation of the curve has minimal coefficients. Part i) is accomplished by reduction of the moduli point which is equivalent with obtaining a representation of the moduli point $\mathfrak{p}$ with minimal weighted height, as defined in [5], and part ii) by the classical reduction of the binary forms.

1. Introduction

Let k be an algebraic number field and $\mathcal{O}_k$ its ring of integers. The isomorphism class of a smooth, irreducible, planar, algebraic curve $\mathcal{X}$, defined over $\mathcal{O}_k$, is determined by its set of invariants which are homogenous polynomials in coefficients of $\mathcal{X}$. The best understood case is when $\mathcal{X}$ is a hyperelliptic. In [14, 24] the authors make the case that superelliptic curves are a natural generalization of hyperelliptic curves and asked if many questions and arithmetic results of hyperelliptic curves can be extended to superelliptic curves. Here we focus on minimal models for the curve and minimal representation for the corresponding moduli point.

By a *superelliptic curve* we mean a smooth, irreducible, plannar, algebraic curve $\mathcal{X}$, defined over k, with projective equation $z^m y^{d-m} = f(x, y)$, where $f(x, y)$ is a degree d binary form of nonzero discriminant $\Delta_f \neq 0$. We assume that such curves have a normal equation over $\mathcal{O}_k$, in other words $f(x, y) \in \mathcal{O}_k[x, y]$; see [24] for details. The isomorphism class of such curves is determined by the set of invariants of the degree d binary forms. These invariants are generators of the invariant ring of binary forms of fixed degree; see [22] among other places.

Given a binary form $f(x, y)$, there are two main *reduction* problems. Determine $g(x, y)$, $\mathrm{GL}_2(k)$-equivalent to $f(x, y)$, such that $g(x, y)$ has minimal:

a) invariants
b) coefficients

Explaining what *minimal* means will be the main focus of this paper. Completing of each task we will call **reduction type a)** or **moduli reduction** and **reduction type b)** or **classical reduction**. For the purposes of this paper we will focus on the case when $k = \mathbb{Q}$, even though many of the results follow for any number field k.

Key words and phrases. Superelliptic curve and Minimal invariants and weighted height.

1.1. Reduction a): Minimality of the moduli point. The isomorphism class of $\mathcal{X}$ correspond to the equivalence class of a binary form $f(x, y)$. Thus, the isomorphism classes of superelliptic curves over $\bar{k}$) are determined by the set of generators of the ring of invariants $\mathcal{R}_d$ of degree $d \geq 2$ binary forms, in other words by $\mathrm{SL}_2(\mathcal{O}_k)$-invariants. By Hilbert's basis theorem $\mathcal{R}_d$ is finitely generated. Let $I_0, \ldots, I_n$ be the generators of $\mathcal{R}_d$ such that the homogenous degree of I_i is q_i for each $i = 0, \ldots, n$. We denote by $\mathcal{I} := (I_0, \ldots, I_n)$ the tuple of invariants and by $\mathcal{I}(f) = (I_0(f), \ldots, I_n(f))$ such invariants evaluated at the binary form f. The corresponding set of invariants $\mathcal{I}(f)$ determines a point $\mathfrak{p} = [\mathcal{I}(f)]$ in the weighted projective space $\mathbb{WP}^n_{\mathbf{w}}(k)$ (cf. Section 2.2) with weights $\mathbf{w} = (q_0, \ldots, q_n)$; see [5,24] for details. Denote the weighted greatest common divisor of the weighted tuple $\mathcal{I}(f)$ by $wgcd(\mathcal{I}(f))$ and by $\overline{wgcd}(\mathcal{I}(f))$ its absolute weighted greatest common divisor (cf. Eq. (13). The curve $\mathcal{X}$ is said to have a **minimal modular model** over $\mathcal{O}_k$ when it has minimal height (cf. Eq. (14)) in the weighted moduli space $\mathbb{WP}^n_{\mathbf{w}}(k)$. In other words, when the weighted valuation of the tuple $\mathcal{I}(f)$ for each prime $p \in \mathcal{O}_k$, $\mathbf{val}_p(\mathcal{I}(f)) := \max\{\nu_p(I_i(f)) \text{ for all } i = 0, \ldots, n\}$ is minimal, where $\nu_p(I_i(f))$ is the valuation at p of $I_i(f)$. The weighted moduli point $\mathfrak{p} = [\mathcal{I}(f)]$ is called **normalized** when $wgcd(\mathcal{I}(f)) = 1$. There are two main tasks:

(i) determine an equation of a curve $\mathcal{X}'$, defined over $\mathcal{O}_k$, and k-isomorphic to $\mathcal{X}$, with *minimal modular model*.

(ii) determine an equation of a curve $\mathcal{X}''$, defined over $\mathcal{O}_k$ and $\bar{k}$-isomorphic to $\mathcal{X}$ with minimal modular model, in other words a twist of $\mathcal{X}$ with minimal modular model.

Our main result is Thm. 5, which says that a minimal modular model for superelliptic curves exist. Moreover, an equation $\mathcal{X} : z^m y^{d-m} = f(x, y)$ is a minimal modular 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 $\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2}\, q_i$, for all $i = 0, \ldots, n$. Additionally, for $\lambda = wgcd(\mathcal{I}(f))$ with respect the weights $\left(\left\lfloor \frac{dq_0}{2} \right\rfloor, \ldots, \left\lfloor \frac{dq_n}{2} \right\rfloor \right)$ the transformation $(x, y, z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z \right)$ gives a minimal model of $\mathcal{X}$ over $\mathcal{O}_k$. If $m|d$ then this isomorphism is defined over k.

Such minimal modular models can be found not only up to k-isomorphism, but also over its algebraic closure $\bar{k}$. We call them *minimal modular twists*. In Thm. 7 we prove that minimal modular twists of superelliptic curves exist. An equation $\mathcal{X} : \; z^m y^{d-m} = f(x, y)$ is a minimal modular twist over $\mathcal{O}_k$, if for every prime $p \in \mathcal{O}_k$ such that $p \mid \overline{wgcd}\,(\mathcal{I}(f))$, the valuation $\mathbf{val}_p$ of $\mathcal{I}(f)$ at p satisfies $\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2}\, q_i$, for all $i = 0, \ldots, n$.

Thm. 5 makes it possible to create a database of superelliptic curves defined over $\mathcal{O}_k$, by storing only the curves with minimal weighted moduli point and Thm. 7 does this also for all their twists as well. Our motivation of exploring such reduction came from genus 2 curves; see [6].

1.2. Reduction b): Minimality of coefficients. Let $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(\mathbb{Q})$ be a normalized moduli point via *reduction a)* and $\mathcal{X}$ the corresponding superelliptic curve. Assume that $\mathcal{X}$ has equation $z^m y^{d-m} = f(x, y)$ over some minimal field of definition k. Determining such equation is part of the math folklore for elliptic curves. One of the main concerns when obtaining such equations is to have coefficients as small as possible. This comes down to what historically is referred to as reduction of binary forms and goes back to Hermite for quadratic forms and Julia

[21] for cubic forms. In [33] such reduction was considered again for cubics and quartics and in [1–3] for $d \geq 3$.

Let $f(x,y)$ be a degree $d \geq 2$ binary form with real coefficients. Then its **Julia quadratic** $\mathfrak{J}_f$ is defined as in Eq. (56). It is a positive definite quadratic and therefore has one root in the upper-half complex plane $\mathcal{H}_2$, say α_f. Since $\mathfrak{J}(f)$ is an $\mathrm{SL}_2(\mathbb{Z})$-covariant, then bringing α_f to the fundamental domain $\mathcal{F}$ by a matrix $M \in \mathrm{SL}_2(\mathbb{Z})$, induces an action $f \to f^M$ on binary forms. The form f^M is called **reduction of** f. In [3] is given an approach of how to determine a minimal model for any degree binary form $f(x,y)$ and a minimal twist of $f(x,y)$ (cf. Section 3.1).

1.3. Birch and Swinnerton-Dyer computations. After the first draft of this paper was written we discovered that a reduction combining both methods described above had been used in the seminal paper of Birch and Swinnerton-Dyer in [7] and [8] for computations with elliptic curves. While the case of the elliptic curves is simpler, it is also the only case that is fully understood, since only for cubics and quartics we have precise results of the Julia reduction [21] as described in the work of Cremona and Stoll in [33] and by Beshaj in [1–3] as remarked above.

The initial computations in [7] start with reduction a). Let $f(x,y) = ax^4+bx^3+cx^2+dx+e$, where a,b,c,d,e are rational integers, and I_4, I_6 its invariants. If $p \in \mathbb{Z}$ is a prime such that $p \neq 2,3$, and $p|\, wgcd_{4,6}(I_4, I_6)$, there there a quartic integral binary form $g(x,y)$, $\mathrm{GL}_2(\mathbb{Z})$ equivalent to $f(x,y)$ with invariants $(p^{-4}I_4, p^{-6}I_6)$. Birch and Swinnerton-Dyer go to a case by case analysis to prove this result; see [7, Lemma 3]. However, this is an immediate consequence of the reduction a) described in Section 3.2. Lemma 4 and Lemma 5 in [7] give the reduction for $p=2$ and 3 respectively.

Minimal integral models give the "nicest" equation of the paper over a global field, since the corresponding invariants are non-zero for as many primes $p \in \mathcal{O}_k$ as possible. It is a topic of interest to explore the stability of such curves. Adjusting the method of reduction a) would give a method of obtaining a stable or semistable form for any binary form; see [12].

Both reductions can be performed for all superelliptic curves, providing that we explicitly know the generators of the ring of invariants $\mathcal{R}_d$. For non-superelliptic curves this is a much more difficult problem which requires the full arsenal of GIT. An explicit description of the moduli point is not known in general. Moreover, there is no known algorithm to determine the equation of the curve starting with the moduli point even in the case a planar curves.

Acknowledgments: I would like to thank Mike Fried for helpful comments and discussions.

2. Preliminaries

2.1. Superelliptic curves. A a genus $g \geq 2$ smooth, irreducible, algebraic curve $\mathcal{X}$ defined over an algebraically closed field k is called a **superelliptic curve of level** n if there exist an element $\tau \in \mathrm{Aut}\,(\mathcal{X})$ of order n such that τ is central and the quotient $\mathcal{X}/\langle\tau\rangle$ has genus zero; see [24] for details. Superelliptic curves have affine equation

$$\mathcal{X}:\ y^n = f(x) = \prod_{i=1}^{d}(x-\alpha_i), \qquad \text{for} \quad \Delta_f \neq 0. \tag{1}$$

Denote by $\sigma : \mathcal{X} \to \mathcal{X}$ the superelliptic automorphism, i.e. $\sigma(x, y) \to (x, \xi_n y)$, where ξ_n is a primitive n-th root of unity. Notice that σ fixes 0 and the point at infinity in $\mathbb{P}^1_y$. The natural projection $\pi : \mathcal{X} \to \mathbb{P}^1_x = \mathcal{X}/\langle\sigma\rangle$ is called the **superelliptic projection**. It has $\deg \pi = n$ and $\pi(x, y) = x$. This cover is branched at exactly at the roots $\alpha_1, \ldots, \alpha_d$ of $f(x)$. Then the affine equation is $\mathcal{X} :\ z^m = \prod_{i=1}^d (x - \alpha_i)$. Denote the projective equation of $\mathcal{X}$ by

$$z^m y^{d-m} = f(x, y) = a_d x^d + a_{d-1} x^{d-1} y + \cdots + a_1 x y^{d-1} + a_0 y^d \tag{2}$$

defined over a field k. Hence, $f(x, y)$ is a binary form of degree $\deg f = d$.

Let $k[x, y]$ be the polynomial ring in two variables and $V_d(k)$ denote 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. The general linear group $\mathrm{GL}_2(k)$ acts as a group of automorphisms on $k[x, y]$.

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 $I \in k[a_0, \ldots, a_d]$ and $M \in \mathrm{GL}_2(k)$, define $I^M \in k[a_0, \ldots, a_d]$ as $I^M(f) := I(f^M)$, for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and we have an action of $\mathrm{GL}_2(k)$ on $k[a_0, \ldots, a_d]$ (cf. Eq. (4)). A homogeneous polynomial $I \in k[a_0, \ldots, a_d, x, y]$ is called a **covariant** of index s if $I^M(f) = \lambda^s I(f)$, where $\lambda = \det(M)^d$. The homogeneous degree in $a_0, \ldots, a_d$ is called the **degree** of I, and the homogeneous degree in x, y is called the **order** of I. A covariant of order zero is called **invariant**. From Hilbert's basis theorem the ring of invariants $\mathcal{R}_d$ of degree d binary forms is finitely generated. Let $I_0, \ldots, I_n$ be the generators of $\mathcal{R}_d$ with degrees $q_0, \ldots, q_n$ respectively. Usually we assume an ordering $q_0 < q_1 < \ldots < q_n$ of degrees. Denote the ordered tuple of invariants by $\mathcal{I} := (I_0, \ldots, I_n)$. Over the algebraic closure we have

$$f(x, y) = (y_1 x - x_1 y) \cdots (y_d x - x_d y) = \prod_{i=1}^d \det \begin{pmatrix} x & x_i \\ y & y_i \end{pmatrix}, \tag{3}$$

where (x_i, y_i) are the homogenous coordinates of the roots in $\mathbb{P}^1$. For $M \in \mathrm{GL}_2(k)$, denote by $\delta = \det M$ and by f^M the action of M on f. Each root (x_i, y_i) goes to $M \begin{bmatrix} x_i \\ y_i \end{bmatrix}$ and $\begin{pmatrix} x & x_i \\ y & y_i \end{pmatrix} \to M \begin{pmatrix} x & x_i \\ y & y_i \end{pmatrix}$. Hence, we have

$$f^M(x, y) = \prod_{i=1}^d \det \left(M \cdot \begin{pmatrix} x & x_i \\ y & y_i \end{pmatrix} \right) = (\det M)^d \ f(x, y). \tag{4}$$

Hence, all the coefficients a_i, $i = 0, \ldots, d$ are multiplied by δ^d. Since an invariant of degree s is a homogenous polynomial of degree s in terms of a_i,

$$I_s = \sum a_0^{\alpha_0} \ldots a_d^{\alpha_d} \tag{5}$$

where $\alpha_i = 0, \ldots, d$ and $\alpha_0 + \cdots + \alpha_d = s$, then $I(f^M) = \delta^{ds}\, I_s(f)$. However, it is more difficult if we want to determine $f^M(x, y)$ when $f(x, y)$ is given as in Eq. (2). Such expressions of invariants in terms of coefficients are determined via *transvections* and *umbral calculus*; see [**22**] among many other sources.

Consider $f(x, y)$ as in Eq. (2), $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}_2(k)$, and $f^M(x, y) := f(\alpha x + \beta y, \gamma x + \delta y)$. We want to determine the invariants of $f^M(x, y)$ in terms of the invariants of $f(x, y)$. The following result is fundamental to our approach.

PROPOSITION 1. *Let $f \in V_d(k)$, $M \in \mathrm{GL}_2(k)$, and $I_0, \dots I_n$ be the generators of $\mathcal{R}_d$ with degrees $q_0, \dots, q_n$ respectively. Then for each $i = 0, \dots, n$*

$$I_i\left(f^M(x,y)\right) = \lambda^{q_i}\, I_i(f) \tag{6}$$

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

PROOF. Let J be a covariant of degree $\deg J = s$, order ord (J), and weight wt (J). Recall that the **weight** of a covariant is the integer r such that

$$J\left(f\left(\alpha x + \beta y, \gamma x + \delta y\right)\right) = (\alpha\delta - \beta\gamma)^r J(f(x,y)). \tag{7}$$

We know that

$$\deg J + 2\mathrm{wt}\ (J) = (\deg f + 2\mathrm{wt}\ f)\,\mathrm{ord}(J), \tag{8}$$

see [26, Prop. 2.29]. Let I be an invariant of order ord $(I) := s$. Then $\deg I = 0$, wt $(f) = 0$ and we have 2wt $(I) = ds$. So the weight of any invariant is $\frac{d}{2}s$. This completes the proof. □

2.2. Proj $\mathcal{R}_d$ as a weighted projective space. Since all $I_0, \dots, I_i, \dots, I_n$ are homogenous polynomials then $\mathcal{R}_d$ is a graded ring and Proj $\mathcal{R}_d$ is a weighted projective space. Let $\mathbf{w} := (q_0, \dots, q_n) \in \mathbb{Z}^{n+1}$ be the fixed ordered 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 $\mathbb{WP}^n_{\mathbf{w}}(k)$. 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 will denote a point $\mathfrak{p} \in \mathbb{WP}^n_w(k)$ by $\mathfrak{p} = [x_0 : x_1 : \dots : x_n]$. For proofs of the following two results see [24].

PROPOSITION 2. *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 weighted moduli point*

$$\mathcal{I}(f) := [I_0(f), I_1(f), \dots, I_n(f)] \in \mathbb{WP}^n_{\mathbf{w}}(k). \tag{9}$$

Moreover, $f = g^M$ for some $M \in \mathrm{GL}_2(K)$ if and only if $\mathcal{I}(f) = \lambda \star \mathcal{I}(g)$, for $\lambda = (\det A)^{\frac{d}{2}}$.

Since the isomorphism class of a superelliptic curve $\mathcal{X} : z^m y^{d-m} = f(x,y)$ is determined by the equivalence class of binary form $f(x,y)$ we denote the set of invariants of $\mathcal{X}$ by $\mathcal{I}(\mathcal{X}) := \mathcal{I}(f)$.

COROLLARY 1. *Let $\mathcal{X}$ be as in Eq. (2). The $\bar{k}$-isomorphism class of $\mathcal{X}$ is determined by the weighted moduli point $\mathfrak{p} := [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathbf{w}}(k)$.*

2.3. Heights. If we want to create a list of all isomorphism classes of superelliptic curves we have to create a database of points in $\mathbb{WP}^n_{\mathbf{w}}(k)$. Obviously, we would prefer to take for each point $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(k)$ its *smallest* representative and also want to order such points. We struggled with both such tasks in [6], until we were able to define a height function on $\mathbb{WP}^n_{\mathbf{w}}(k)$, which solves both problems. This is due to a Northcott like theorem for this weighted height, which says that there are only finitely many points for a bounded height. Also the representation of the point $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(k)$ with *smallest coordinates* correspond precisely to the tuple $(x_0, \dots, x_n)$ such that its weighted greatest common divisor is $= 1$. These ideas were developed in detail in [5].

Fix the following notation: k is a number field, $\mathcal{O}_k$ is ring of integers of k, M_k is a complete set of absolute values of k, M_k^0 is the set of all non-archimedian places in M_k, M_k^∞ is the set of Archimedean places, and $\mathcal{X}/k$ is a smooth projective superelliptic curve defined over k. 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 and the Weil height for $x \in k$ is $H(x) = \prod_\nu \max\{1, |x|_\nu\}$.

For $P = [x_0, \dots, x_n] \in \mathbb{P}^n(k)$ the **multiplicative height** of P is defined as follows

$$H_k(P) := \prod_{v \in M_k} \max\left\{ |x_0|_v^{n_v}, \dots, |x_n|_v^{n_v} \right\}, \tag{10}$$

where n_v is the **local degree at** v given by $n_v = [k_v : \mathbb{Q}_v]$ for k_v and $\mathbb{Q}_v$ are the completions with respect to v. The height $H_k(P)$ is well defined, in other words it does not depend on the choice of homogenous coordinates of P. Moreover, $H_k(P) \geq 1$. If L/k is a finite extension, then $H_L(P) = H_k(P)^{[L:k]}$. Hence, we can define the height on $\mathbb{P}^n(\overline{\mathbb{Q}})$, which is called the **absolute (multiplicative) height** and is the function $H : \mathbb{P}^n(\bar{\mathbb{Q}}) \to [1, \infty)$, such that $H(P) = H_k(P)^{1/[k:\mathbb{Q}]}$. The height is invariant under Galois conjugation. In other words, if $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_\mathbb{Q}$, then $H(P^\sigma) = H(P)$. The following are the two main results in the theory of heights on projective spaces; see [9] or [19].

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

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \leq c_0 \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d_0\} \tag{11}$$

has finitely many points. In particular, $\{P \in \mathbb{P}^n(k) : H_k(P) \leq c_0\}$ is a finite set.

Theorem 2 (Kronecker's theorem). *Let $P = [x_0, \dots, x_n] \in \mathbb{P}^n(k)$. 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 $0 \leq j \leq n$.*

Amazingly, the above theory can be extended to weight projective spaces with necessary adjustments. We give a quick recapture here; see [5] for details. Let $\mathbf{x} = (x_0, \dots x_n) \in \mathbb{Z}^{n+1}$ be a tuple of integers, not all equal to zero. A *weighted integer tuple* is a tuple $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ such that to each coordinate x_i is assigned the weight q_i and $\mathbf{w} := (q_0, \dots, q_n)$ is called the *set of weights*. We multiply weighted tuples by scalars $\lambda \in \mathbb{Q}$ via

$$\lambda \star (x_0, \dots, x_n) = (\lambda^{q_0} x_0, \dots, \lambda^{q_n} x_n) \tag{12}$$

For an ordered tuple of integers $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$, whose coordinates are not all zero, the **weighted greatest common divisor with respect to the set of weights w** is the largest integer d such that $d^{q_i} \mid x_i$, for all $i = 0, \dots, n$. For a weighted tuple $\mathbf{x} = (x_0, \dots, x_n) \in \mathcal{O}_k^{n+1}$ the weighted greatest common divisor is given by

$$wgcd(\mathbf{x}) = \prod_{p \in \mathcal{O}_k} p^{\min\left\{ \left\lfloor \frac{\nu_p(x_0)}{q_0} \right\rfloor, \dots, \left\lfloor \frac{\nu_p(x_n)}{q_n} \right\rfloor \right\}} \tag{13}$$

where ν_p is the valuation corresponding to the prime p. We call a point $\mathfrak{p} \in \mathbb{WP}^n_\mathbf{w}(k)$ a **normalized point** if the weighted greatest common divisor of its coordinates is 1. For any point $\mathfrak{p} \in \mathbb{WP}^n_w(k)$, there exists its normalization given by $\mathfrak{q} = \frac{1}{wgcd(\mathfrak{p})} \star \mathfrak{p}$. Moreover, this normalization is unique up to a multiplication by a q-root of unity, where $q = \gcd(q_0, \dots, q_n)$, see [5]. The **absolute weighted greatest common**

divisor of $\mathbf{x} = (x_0, \dots, x_n)$ is the largest real number d such that $d^{q_i} \in \mathbb{Z}$ and $d^{q_i} \mid x_i$, for all $i = 0, \dots n$. We denote it by $\overline{wgcd}(x_0, \dots, x_n)$.

Let $\mathfrak{p} = [x_0, \dots, x_n] \in \mathbb{WP}^n(k)$. Without any loss of generality we can assume that $\mathfrak{p}$ is normalized. The **weighted multiplicative height** of $\mathfrak{p}$ is

$$\mathfrak{h}_k(\mathfrak{p}) := \prod_{v \in M_k} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \dots, |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{14}$$

The height $\mathfrak{h}_k(\mathfrak{p})$ is well defined, in other words it does not depend on the choice of coordinates of $\mathfrak{p}$ and $\mathfrak{h}_k(\mathfrak{p}) \geq 1$; see [5]. Denote by $K = k(\overline{wgcd}(\mathfrak{p}))$. Then, over K, the weighted greatest common divisor is the same as the absolute greatest common divisor, $wgcd_K(\mathfrak{p}) = \overline{wgcd}_K(\mathfrak{p})$. Moreover, $[K : k] < \infty$ and we have the following.

Proposition 3 ([5]). *If $\mathfrak{p}$ is normalized in K, then*

$$\mathfrak{h}_K(\mathfrak{p}) = \mathfrak{h}_\infty(\mathfrak{p}) = \max_{0 \leq i \leq n} \left\{ |x_i|_\infty^{n_\nu / q_i} \right\}. \tag{15}$$

Moreover, if L/K is a finite extension, then $\mathfrak{h}_L(\mathfrak{p}) = \mathfrak{h}_K(\mathfrak{p})^{[L:K]}$.

Using Prop. 3, we can define the height on $\mathbb{WP}^n(\overline{\mathbb{Q}})$. The height of a point on $\mathbb{WP}^n(\overline{\mathbb{Q}})$ is called the **absolute (multiplicative) weighted height** and is the function

$$\tilde{\mathfrak{h}} : \mathbb{WP}^n(\bar{\mathbb{Q}}) \to [1, \infty), \tag{16}$$

such that

$$\tilde{\mathfrak{h}}(\mathfrak{p}) = \mathfrak{h}_K(\mathfrak{p})^{1/[K:\mathbb{Q}]}, \tag{17}$$

where $\mathfrak{p} \in \mathbb{WP}^n(K)$, for any K which contains $\mathbb{Q}(\overline{wgcd}(\mathfrak{p}))$. Moreover, for $\mathfrak{p} \in \mathbb{WP}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$ we have $\mathfrak{h}(\mathfrak{p}^\sigma) = \mathfrak{h}(\mathfrak{p})$. The **field of definition** of $\mathfrak{p}$ is defined as $\mathbb{Q}(\mathfrak{p}) := \mathbb{Q}\left(\left(\frac{x_0}{x_i}\right)^{\frac{q_0}{q}}, \dots, 1, \dots, \left(\frac{x_n}{x_i}\right)^{\frac{q_n}{q}} \right)$ For any point $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(\overline{\mathbb{Q}})$, we have $[\mathbb{Q}(\mathfrak{p}) : \mathbb{Q}] \leq q \cdot [\mathbb{Q}(\phi(\mathfrak{p})) : \mathbb{Q}]$. The following result is analogue to Northcott's theorem for weighted projective spaces; see [5] for the proof.

Theorem 3 ([5]). *Let $c_0, d_0 \in \mathbb{R}$. Then the set*

$$\{\mathfrak{p} \in \mathbb{WP}^n_w(\overline{\mathbb{Q}}) : \mathfrak{h}_{\mathbb{Q}}(\mathfrak{p}) \leq c_0 \text{ and } [\mathbb{Q}(\mathfrak{p}) : \mathbb{Q}] \leq d_0\} \tag{18}$$

contains only finitely many points.

Hence, $\{\mathfrak{p} \in \mathbb{WP}^n_w(\overline{\mathbb{Q}}) : \mathfrak{h}_{\bar{\mathbb{Q}}}(\mathfrak{p}) \leq c_0\}$ is a finite set for any constant c_0. For any number field k, the set $\{\mathfrak{p} \in \mathbb{WP}^n_w(k) : \ \mathbb{Q}(\mathfrak{p}) \subset k \ \text{ and } \ \mathfrak{h}_k(\mathfrak{p}) \leq c_0\}$, is a finite set. The next result is the analogue of Kronecker's theorem; see [5].

Theorem 4 ([5]). *Fix any i with $x_i \neq 0$. Then $\mathfrak{h}(\mathfrak{p}) = 1$ if the ratio $x_j / \xi_i^{q_j}$, where ξ_i is the q_i-th root of unity of x_i, is a root of unity or zero for every $0 \leq j \leq n$ and $j \neq i$.*

Now we have the following two problems in terms of curves.

Problem 1. *Given a curve $\mathcal{X} : z^m y^{d-m} = d(x, y)$ defined over $\mathcal{O}_k$, determine $\mathcal{X}'$, k-isomorphic to $\mathcal{X}$, such that defined over $\mathcal{O}_k$, say $\mathcal{X}' : z^m y^{d-m} = g(x, y)$, such that $\mathfrak{p} := [\mathcal{I}(g)] \in \mathbb{WP}^n_{\mathbf{w}}(k)$ has minimal height over k.*

Problem 2. *Determine a twist $\mathcal{Y}$ of $\mathcal{X}$ such that $\mathfrak{p} := [\mathcal{I}(\mathcal{Y})] \in \mathbb{WP}^n_{\mathbf{w}}(k)$ has minimal height over the algebraic closure $\bar{k}$.*

The above problems are equivalent of finding a model for the superelliptic curve such that the corresponding weighted moduli point has minimal possible weighted height or finding a twist with such property.

3. Reduction of the moduli point

The reduction of superelliptic curves consists of two steps. On the first step we perform the necessary coordinate changes so we have a minimal weighted moduli point, and the second step is to minimize the coefficients of the equation of the curve. Both of these steps are possible due to the fact that a superelliptic curve can be written as a curve with projective equation $y^n z^{d-n} = f(x,z)$, such that f is a binary form of degree $\deg f = d$ with nonzero discriminant.

The first step is based on the concept of weighted heights in weighted projective spaces as defined in [5]. The second step is well known by work of Hermite for quadratics and extended by Julia for higher degree forms. For more recent work on this type of reduction see work of Cremona, Stoll [33] and Beshaj [1–3].

3.1. Minimal integral models of binary forms. We say that a binary form $f(x,y)$ has a **integral minimal model** over k if it is integral (i.e. $f \in \mathcal{O}_k[x,y]$) and $\mathbf{val}_p(\mathcal{I}(f))$ is minimal for every prime $p \in \mathcal{O}_k$.

Let $f \in \mathcal{O}_k$ and $\mathbf{x} := \mathcal{I}(f) \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ 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

$$\mathbf{val}_p(\mathbf{x}) := \max \left\{ j \,|\, p^j \text{ divides } x_i^{q_i} \text{ for all } i = 0, \dots n \right\}, \tag{19}$$

Then we have the following.

Proposition 4. *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 $p \,|\, wgcd(\mathcal{I}(f))$ the following holds*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i, \quad \textit{for all} \quad i = 0, \dots, n. \tag{20}$$

Moreover, for every integral binary form f its minimal model exist.

Proof. Let $\mathbf{x} = \mathcal{I}(f)$. From Eq. (6) we know that for any $M \in \mathrm{GL}_2(\mathcal{O}_k)$, $\mathcal{I}(f^M) = (\det M)^{\frac{d}{2}} \mathcal{I}(f)$. Hence, for every prime $p \in \mathcal{O}_k$ which divides $wgcd(\mathbf{x})$ we must "multiply" $\mathbf{x}$ by the maximum exponent j such that $\left(p^{\frac{d}{2}}\right)^j$ divides $wgcd(\mathbf{x})$.

For a given binary form f we pick $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$, where λ is the weighted greatest common divisor of $\mathcal{I}(f)$ 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 $x \to \frac{x}{\lambda}$ gives a minimal model of f over $\mathcal{O}_k$. This completes the proof. ∎

Remark 1. *If a prime $p \in \mathcal{O}_k$ divides $wgcd(\mathbf{x})$ then p^{q_i} divides x_i, so $p^{q_i^2}$ divides $x_i^{q_i}$. Taking $q_t = \min(q_0, \dots, q_n)$, we have a lower bound for the weighted valuation of the point $\mathcal{I}(f) = (x_0, \dots, x_n)$, that is $\mathbf{val}_p(\mathcal{I}(f)) \geq q_t^2$.*

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 $\mathrm{GL}_2(\mathcal{O}_k)$-orbit as f. For example, the transformation $(x,y) \to \left(\frac{1}{\lambda^{\frac{2}{d}}} x, \frac{1}{\lambda^{\frac{2}{d}}} y \right)$, 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 [5].

Corollary 2. *If $f(x,y) \in \mathcal{O}_k[x,y]$ is a binary form such that $\mathcal{I}(f) \in \mathbb{WP}^n_{\mathbf{w}}(k)$ is normalized over k, then f is a minimal model over $\mathcal{O}_k$.*

We see an example for binary sextics.

Example 1. *Let be given the sextic*

$$f(x,y) = 7776x^6 + 31104x^5y + 40176x^4y^2 + 25056x^3y^3 + 8382x^2y^4 + 1470xy^5 + 107y^6 \tag{21}$$

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

$$\begin{aligned} J_2 &= 2^{15}\cdot 3^5,\ J_4 = -2^{12}\cdot 3^9\cdot 101\cdot 233,\ J_6 = 2^{16}\cdot 3^{13}\cdot 29\cdot 37\cdot 8837, \\ J_{10} &= 2^{26}\cdot 3^{21}\cdot 11\cdot 23\cdot 547\cdot 1445831 \end{aligned} \tag{22}$$

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

$$\frac{1}{p^3} \star [J_2 : J_4 : J_6 : J_{10}] = \left[\frac{1}{p^6}J_2 : \frac{1}{p^{12}}J_4 : \frac{1}{p^{18}}J_6 : \frac{1}{p^{30}}J_{10}\right] \tag{23}$$

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 $\mathcal{O}_k$. □

Corollary 3. *The transformation of $f(x,y)$ by the matrix*

$$M = \begin{bmatrix} \varepsilon_d \frac{1}{(wgcd(I(f)))^{\frac{2}{d}}} & 0 \\ 0 & \varepsilon_d \frac{1}{(wgcd(I(f)))^{\frac{2}{d}}} \end{bmatrix} \tag{24}$$

where ε_d is a d-primitive root of unity, will always give a minimal set of invariants.

3.2. Reduction a): Moduli points with minimal weighted height. Let $\mathcal{X}$ be as in Eq. (2) and $\mathfrak{p} = [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathbf{w}}(k)$. Let us assume that for a prime $p \in \mathcal{O}_k$, we have $\nu_p(wgcd(\mathfrak{p})) = \alpha$. If we use the transformation $x \to \frac{x}{p^\beta}x$, for $\beta \le \alpha$, then from Eq. (6) 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 β such that $p^{\frac{\beta d}{2}}$ divides $p^{\nu_p(x_i)}$ for $i = 0, \dots, n$. Hence, we must pick β as the maximum integer such that $\beta \le \frac{2}{d}\nu_p(x_i)$, for all $i = 0, \dots, n$. This is the same β as in Prop. 4. 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 Eq. (6) 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 $\mathbb{WP}^n_{\mathbf{w}}(k)$ since β is not necessarily equal to α. This motivates the following definition.

Definition 1. Let $\mathcal{X}$ be a superelliptic curve defined over an integer ring $\mathcal{O}_k$ and $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ 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

$$\mathbf{val}_p(\mathfrak{p}) := \max\{\nu_p(x_i) \text{ for all } i = 0, \dots n\}, \tag{25}$$

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

THEOREM 5. *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*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i, \tag{26}$$

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

PROOF. Let $\mathcal{X}$ be a superelliptic curve given by Eq. (2) over $\mathcal{O}_k$ and $\mathfrak{p} = \mathcal{I}(f) \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ with weights $\mathbf{w} = (q_0, \dots, q_n)$. Then $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ and from Prop. 4 exists $M \in \mathrm{GL}_2(\mathcal{O}_k)$ such that $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$ and λ as in the theorem's hypothesis. By Prop. 4 we have that Eq. (26) holds.

Let us see how the equation of the curve $\mathcal{X}$ changes when we apply the transformation by M. We have

$$z^m y^{d-m} = f\left(\frac{x}{\lambda}, y\right) = a_d \frac{x^d}{\lambda^d} + a_{d-1} \frac{x^{d-1}}{\lambda^{d-1}} y + \dots + a_1 \frac{x}{\lambda} y^{d-1} + a_0 y^d \tag{27}$$

Hence,

$$\mathcal{X}' : \ \lambda^d z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \dots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d \tag{28}$$

This equation has coefficients in $\mathcal{O}_k$. Its weighted moduli point is $\mathcal{I}(f^M) = \frac{1}{\lambda^{\frac{d}{2}}} \star \mathcal{I}(f)$, which satisfies Eq. (26). It is a twist of the curve $\mathcal{X}$ since λ^d is not necessary a m-th power in $\mathcal{O}_k$. The isomorphism of the curves over the field $k\left(\lambda^{\frac{d}{m}}\right)$ is given by $(x, y, z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z\right)$. If $m|d$ then this isomorphism is defined over k and $\mathcal{X}'$ has equation

$$\mathcal{X}' : \ z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \dots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d \tag{29}$$

□

Then we have the following.

COROLLARY 4. *There exists a curve $\mathcal{X}'$ given in Eq. (28) isomorphic to $\mathcal{X}$ over the field $K := k\left(wgcd(\mathfrak{p})^{\frac{d}{m}}\right)$ with minimal invariants. Moreover, if $m \mid d$ then $\mathcal{X}$ and $\mathcal{X}'$ are k-isomorphic.*

A simple observation from the above is that in the case of hyperelliptic curves we have $m = 2$ and $d = 2g + 2$. Hence, the curves $\mathcal{X}$ and $\mathcal{X}'$ would always be isomorphic over k. So we have the following.

COROLLARY 5. *Given a hyperelliptic curve defined over a ring of integers $\mathcal{O}_k$. There exists a curve $\mathcal{X}'$ k-isomorphic to $\mathcal{X}$ with minimal invariants.*

Thm. 5 above provides an algorithm which is described next. Given a superelliptic curve $\mathcal{X}$ defined over $\mathcal{O}_k$, we denote the corresponding point in the weighted moduli space by $\mathfrak{p} = [x_0 : \cdots : x_n]$.

Algorithm: Computing an equation of the curve with minimal moduli point.

Input: A curve $\mathcal{X} : z^m y^{d-m} = f(x, y)$, $\deg(f) = d$ and $f \in \mathcal{O}_k[x, y]$.
Output: A curve $\mathcal{Y} : \lambda^d z^m = g(x, y)$, defined over $\mathcal{O}_k$ and k-isomorphic to $\mathcal{X}$ such that $\mathbf{val}_p \, \mathcal{I}(g)$ is minimal for each prime $p \in \mathcal{O}_k$.

Step 1: Compute the generating set $\mathcal{I} := [I_{q_0}, \dots, I_{q_n}]$ for $\mathcal{R}_n$.
Step 2: Compute the moduli point $\mathfrak{p} \in \mathbb{WP}^n_w(k)$ for $\mathcal{X}$ by evaluating $\mathcal{I}(f)$.
Step 3: Computing $\lambda = wgcd(\mathcal{I}(f)) \in \mathcal{O}_k$ with respect the weights $\left(\left\lfloor \frac{dq_0}{2} \right\rfloor, \dots, \left\lfloor \frac{dq_n}{2} \right\rfloor \right)$
Step 4: Compute f^M, where $M := \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$. We have $g(x) := \lambda^d \cdot f\left(\frac{x}{\lambda}\right)$.
Step 5: Return the curve $\mathcal{X}'$ with equation $\lambda^d z^m y^{d-m} = g(x, y)$.

Let us illustrate for $g = 1, 2$.

3.2.1. *Elliptic curves.* Technically elliptic curves are not superelliptic curves, but the method will work the same. Let E be an elliptic curve with Weierstrass equation as in Birch/Swinnerton-Dyer [7]

$$E: \quad z^2 y^2 = f(x, y) = ax^4 + bx^3 y + ex^2 y^2 + cxy^3 + dy^4. \tag{30}$$

Invariants of the binary quartic $f(x, y)$ are

$$I_2 = 12ae - 3bd + c^2, \quad I_3 = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 \tag{31}$$

The corresponding weighted moduli space is $\mathbb{WP}_{(2,3)}(k)$. Isomorphism classes of elliptic curves over k correspond to points in $\mathbb{WP}_{(2,3)}(k)$.

Corollary 6. *The equation in Eq. (30) is a minimal models if for every prime $p \in \mathbb{Z}$, $p \neq 2, 3$ which divides $p |\, wgcd(I_2, I_3)$, the valuation $\mathbf{val}_p(I_2, I_3)$ satisfies $\mathbf{val}_p(I_2, I_3) < 2q_i$, for $q_i = 2, 3$.*

Hence, we can reduce any prime $p \neq 2, 3$ such that $p^\alpha | I_2$ and $p^\beta | I_3$ when $\alpha \geq 4$ and $\beta \geq 6$. The above result was proved in [7] using a case by case analysis; see [7, Lem. 3]. Lemma 4 and Lemma 5 in [7] describe the cases when $p = 2$ and $p = 3$ respectively. Then we have the following; see [7, Theorem 1].

Theorem 6 (Birch, Swinnerton-Dyer). *If E is an elliptic curve, and U is a non-trivial 2-covering of E then U can be represented by a curve $z^2 y^2 = g(x, y)$, where $g(x, y)$ is reduced. The reduced $g(x, y)$ of a given E are finite in number and computable.*

3.2.2. *Genus 2 curves.* Let $\mathcal{X}$ be a genus 2 curve with equation $z^2 y^4 = f(x, y)$ as in Example 1. By applying the transformation $(x, y, z) \to \left(\frac{x}{6}, y, 6^3 \cdot z\right)$ we get the equation

$$z^2 = x^6 + 24x^5 + 186x^4 + 696x^3 + 1397x^2 + 1470x + 642. \tag{32}$$

Computing the moduli point of this curve we get

$$\mathfrak{p} = [2^{11} \cdot 3 : -2^4 \cdot 3 \cdot 101 \cdot 233 : 2^4 \cdot 3 \cdot 29 \cdot 37 \cdot 8837 : 2^6 \cdot 3 \cdot 11 \cdot 23 \cdot 547 \cdot 1445831], \tag{33}$$

which is obviously normalized in $\mathbb{WP}^3_{\mathbf{w}}(\mathbb{Q})$ since $wgcd(\mathfrak{p}) = 1$. Hence, the Eq. (32) is a minimal model.

3.3. Minimal integral twists. Let k be a field of characteristic zero and $\mathrm{Gal}(\bar{k}/k)$ the Galois group of $\bar{k}/k$. Let $\mathcal{X}$ a genus $g \geq 2$ smooth, projective algebraic curve defined over k. We denote by Aut $(\mathcal{X})$ the automorphism group of $\mathcal{X}$ over the algebraic closure $\bar{k}$. By Aut $_k(\mathcal{X})$ is denoted the subgroup of automorphisms of $\mathcal{X}$ defined over k. A **twist** of $\mathcal{X}$ over k is a smooth projective curve $\mathcal{X}'$ defined over k which is isomorphic to $\mathcal{X}$ over $\bar{k}$. We will identify two twists which are isomorphic over k. The set of all twists of $\mathcal{X}$, modulo k-isomorphism, is denoted by Twist $(\mathcal{X}/k)$.

Let $\mathcal{X}$ and $\mathcal{X}'$ be twists of each other over k. Hence, there is an isomorphism $\phi : \mathcal{X}' \to \mathcal{X}$ defined over $\bar{k}$. For any $\sigma \in \mathrm{Gal}(\bar{k}/k)$ there exists the induced map $\phi^\sigma : \mathcal{X}' \to \mathcal{X}$. To measure the failure of ϕ being defined over k one considers the map $\xi : \ \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}\ (\mathcal{X})$ such that $\xi(\sigma) = \phi^\sigma \phi^{-1}$ for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$. The following is the main result on twists; see [**32**, Th. 2.2. pg. 285]

Proposition 5. *The following are true:*

(i) *ξ is a 1-cocycle*

(ii) *The cohomology class $\{\xi\}$ is determined by the k-isomorphism class of $\mathcal{X}'$ and is independent of ϕ. Hence, there is a natural map*

$$\theta : \mathit{Twist}\ (\mathcal{X}/k) \to \mathrm{Hom}^1 \left(\mathrm{Gal}(\bar{k}/k), \mathit{Aut}\ (\mathcal{X}) \right) \tag{34}$$

(iii) *The map θ is a bijection.*

As noted by Silverman in [**32**, Remark 2.3, pg. 285], $\mathrm{Hom}^1 \left(\mathrm{Gal}(\bar{k}/k), \mathrm{Aut}\ (\mathcal{X}) \right)$ is not necessarily a group since Aut $(\mathcal{X})$ is not necessarily Abelian. For nonabelian Galois cohomology we refer to [**27**].

Fix an integer $n \geq 2$. Let k be a number field which contains all primitive n-th roots of unity ξ_n and $\mathcal{O}_k$ its ring of integers. Consider a smooth superelliptic curve $\mathcal{X}$ defined over $\mathcal{O}_k$ with equation $y^n = f(x)$ where f is a separable polynomial in k. The multiplicative group of n-th roots of unity will be denoted by μ_n. Then, μ_n is embedded in Aut $(\mathcal{X})$ in the obvious way. Hence, Aut $(\mathcal{X})$ is an extension of the group μ_n. The list of isomorphism classes of such groups is determined; see [**10**]. Thus, determining the set Twist $(\mathcal{X}/k)$ is equivalent to determining $\mathrm{Hom}^1 \left(\mathrm{Gal}(\bar{k}/k), \mathrm{Aut}\ (\mathcal{X}) \right)$ for each possible group Aut $(\mathcal{X})$.

Lemma 1. *Let $\mathcal{X}$ be as in Eq. (2). Any twist $\mathcal{X}'$ of $\mathcal{X}$ has equation $\lambda y^n = f(x)$, for some $\lambda \in k$ such that $\lambda^{1/n} \in k$. Moreover, the isomorphism $\phi : \mathcal{X} \longrightarrow \mathcal{X}'$ is given by $(x, y) \longrightarrow (x, \sqrt[n]{\lambda}\, y)$.*

Proof. Two curves $\mathcal{X}$ and $\mathcal{X}'$, with equations $y^n = f(x)$ and $v^n = g(u)$, where $\deg f = \deg g = s$, are isomorphic over $\bar{k}$, if and only if

$$x = \frac{au+b}{cu+d}, \; y = \frac{\lambda\, v}{(cu+d)^{s/n}}, \;\; \text{where} \;\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k), \; \lambda \in k^* \tag{35}$$

Let $f(x)$ be given by $f(x) = \sum_{i=0}^s a_i x^i$ then

$$f\left(\frac{au+b}{cu+d} \right) = a_0 + a_1 \left(\frac{au+b}{cu+d} \right) + \cdots + a_s \left(\frac{au+b}{cu+d} \right)^s = \frac{1}{(cu+d)^s}\, g(u), \tag{36}$$

where $g(u)$ is of degree s in u. hence, the equation of the curve becomes $(cu + d)^s\, y^n = g(u)$. Replacing y as above we get $\lambda^n\, v^n = g(u)$. □

THEOREM 7. *Minimal twists of minimal models of superelliptic curves exist. An equation $\mathcal{X} : z^m y^{d-m} = f(x,y)$ is a minimal twist over $\mathcal{O}_k$, if for every prime $p \in \mathcal{O}_k$ which divides $p \mid \overline{wgcd}\,(\mathcal{I}(f))$, the valuation $\mathbf{val}_p$ of $\mathcal{I}(f)$ at p satisfies*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2}\, q_i, \tag{37}$$

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

PROOF. Let $\mathcal{X}$ be a superelliptic curve given by Eq. (2) over $\mathcal{O}_k$ and $\mathfrak{p} = \mathcal{I}(f) \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ with weights $\mathbf{w} = (q_0, \dots, q_n)$. Then $\mathfrak{p} \in \mathbb{WP}^n_{\mathbf{w}}(\mathcal{O}_k)$ and from Prop. 4 exists $M \in \mathrm{GL}_2(\mathcal{O}_k)$ such that $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$ and λ as in the theorem's hypothesis.

Let us see how the equation of the curve $\mathcal{X}$ changes when we apply the transformation by M. We have

$$z^m y^{d-m} = f\left(\frac{x}{\lambda}, y\right) = a_d \frac{x^d}{\lambda^d} + a_{d-1}\frac{x^{d-1}}{\lambda^{d-1}} y + \cdots + a_1 \frac{x}{\lambda} y^{d-1} + a_0 y^d \tag{38}$$

Hence,

$$\mathcal{X}' :\ \lambda^d z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \cdots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d \tag{39}$$

This equation has coefficients in $\mathcal{O}_k$. Its weighted moduli point is

$$\mathcal{I}(f^M) = \frac{1}{\lambda^{\frac{d}{2}}} \star \mathcal{I}(f), \tag{40}$$

which satisfies Eq. (37). It is a twist of the curve $\mathcal{X}$ since λ^d is not necessary a m-th power in $\mathcal{O}_k$. The isomorphism of the curves over the field $k\left(\lambda^{\frac{d}{m}}\right)$ is given by $(x,y,z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z\right)$. If $m|d$ then this isomorphism is defined over k and $\mathcal{X}'$ has equation

$$\mathcal{X}' :\ z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \cdots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d \tag{41}$$

This completes the proof. □

Further work on the reduction of moduli points of higher degree binary forms is intended in [**12**].

4. Reduction of coefficients of binary forms

Next we will focus on the reduction of coefficients of a binary form. This is an old problem starting with Julia's thesis in [**21**] and continued with more recent papers [**2**], [**3**], [**31**], [**4**], [**1**]. Along similar lines a new reduction of binary forms via the hyperbolic centroid was introduced in [**13**], which seems to have different results from the approach in previous papers (cf. Section 4.3).

A non-homogenous polynomial with n variables will be denoted as

$$f(x_1, \dots, x_n) = \sum_{i=(i_1,\dots,i_n)\in I} a_i x_1^{i_1} \cdots x_n^{i_n}, \tag{42}$$

where all $a_i \in k$, $I \subset \left(\mathbb{Z}^{\geq 0}\right)^n$, 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

$$\mathrm{H}_k^{\mathbb{A}}(f) = \prod_{v \in M_k} \max\left\{ 1, |f|_v^{n_v} \right\}, \tag{43}$$

where $|f|_v := \max_j \left\{ |a_j|_v \right\}$ is called the **Gauss norm** for any absolute value v and n_v is the **local degree at** v given by $n_v = [k_v : \mathbb{Q}_v]$ for k_v and $\mathbb{Q}_v$ are the completions with respect to v; see Section 2.3. Hence, the affine height of a polynomial is defined to be the height of its coefficients taken as affine coordinates.

The **(projective) multiplicative height of a polynomial** is the height of its coefficients taken as coordinates in the projective space. Thus,

$$\mathrm{H}_k(f) = \prod_{v \in M_k} |f|_v^{n_v} \tag{44}$$

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

$$\mathrm{H} : \mathbb{P}^n(\mathbb{Q}) \to [1, \infty), \tag{45}$$

such that $\mathrm{H}(f) = \mathrm{H}_k(f)^{1/[k:\mathbb{Q}]}$. The following is [31, Thm. 2, Prop. 1].

Lemma 2. *The following hold true:*

- (i) *Let $f \in k[x, y]$. Then there are only finitely many polynomials $g \in k[x, y]$ such that $\mathrm{H}_k(g) \le \mathrm{H}_k(f)$.*
- (ii) *Let $f(x_0, \ldots, x_n)$ and $g(y_0, \ldots, y_n)$ be polynomials in different variables. Then, $\mathrm{H}(f \cdot g) = \mathrm{H}(f) \cdot \mathrm{H}(g)$.*

The following lemma is true for the product of a finite number of polynomials.

Lemma 3 (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 [9, pg. 22]. Gauss's lemma applies to all non-Archimedean absolute values but the Archimedean case is more complicated. The following gives a bound for the homogenous polynomial evaluated at a point; see [31, Lem. 15].

Lemma 4. *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) *$|f(\alpha)|_v \le |c(d, n)|_v \cdot \max_j \left\{ |\alpha_j|_v \right\}^d \cdot |f|_v$, where $|c(d, n)|_v$ is $\binom{n+d}{d}$ if v is non-Archimedean and 1 otherwise.*
- (ii) *$\mathrm{H}(f(\alpha)) \le c_0 \cdot \mathrm{H}(\alpha)^d \cdot \mathrm{H}(f)$.*

Then we have the immediate corollary; see [31, Cor. 1].

Corollary 7. *Let k be a number field, $f \in k[x, z]$ a homogenous polynomial of degree d as $f(x, z) = \sum_{i=1}^d a_i x^i z^{d-i}$ and $\alpha = (\alpha_0, \alpha_1) \in \overline{k}^2$. Then,*

$$\mathrm{H}(f(\alpha)) \le \min\left\{ d + 1, 2^{d+1} \right\} \cdot \mathrm{H}(\alpha)^d \cdot \mathrm{H}(f). \tag{46}$$

We will use Lemma 4 to bound the height of the invariants on V_d; see [31, Thm. 4] for the proof.

Theorem 8. *Let $M = [a_{i,j}] \in \mathrm{GL}_2(k)$, $f \in k[x_1, \ldots, x_n]$, $f \in V_d(k)$, and $\mathrm{H}(f)$ the absolute height of f. Then,*

$$\mathrm{H}(f^M) \le 2^n \cdot (n + 1) \cdot \mathrm{H}(M)^n \cdot \mathrm{H}(f), \tag{47}$$

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

Let k be an algebraic number field, and $f(x, y)$ and $\bar{f}(x, y) := f(ux + w, y)$. Then from [31, Thm. 5] we have:

THEOREM 9. (i) *For any valuation $v \in M_k$ we have*

$$|\bar{f}|_v \leq 2_v^d \cdot c(d)_v \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{0 \leq i \leq d} \left\{ |b_i|_v \right\} \tag{48}$$

(ii) *The height of the form is bounded as follows*

$$\mathrm{H}(\bar{f}) \leq (d+1) \cdot 2^d \cdot u^d \cdot w^d \cdot \mathrm{H}(f) \tag{49}$$

Denote by $\mathrm{Orb}(f)$ the $\mathrm{GL}_2(k)$-orbit of f in V_d and $\mathrm{H}(f)$ its height. Note that there are only finitely many $f' \in \mathrm{Orb}(f)$ such that $\mathrm{H}(f') \leq \mathrm{H}(f)$. Define the *minimum height* of the binary form $f(x, y)$ as follows

$$\tilde{\mathrm{H}}(f) := \min \left\{ \mathrm{H}(f') | f' \in \mathrm{Orb}(f), \, \mathrm{H}(f') \leq \mathrm{H}(f) \right\}. \tag{50}$$

We naturally have the following problem:

PROBLEM 3. *For every f let f' be the binary form such that $f' \in \mathrm{Orb}(f)$ and $\tilde{\mathrm{H}}(f) = \mathrm{H}(f')$. Determine a matrix $M \in \mathrm{GL}_2(k)$ such that $f' = f^M$.*

This can be fully solved for quadratics (cf. crefbinary-quad). There is a connection between the height of the moduli point $\mathfrak{p}_f$ (considered as a projective point in $\mathbb{P}^n(k)$) and $\tilde{\mathrm{H}}(f)$ as described in [31, Thm. 6]. We have

$$\mathrm{H}(\mathfrak{p}) \leq c \cdot \tilde{\mathrm{H}}(f), \tag{51}$$

for some constant c. For binary sextics this constant was computed in [31] as $c = 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$; see [31, Lem. 20].

4.1. Quadratic forms. The case of quadratic forms is well known and goes back to Lagrange, Gauss [15, 16], Hermite and many others. A **quadratic form over** $\mathbb{R}$ is a function $\mathfrak{q} : \mathbb{R}^n \to \mathbb{R}$ that has the form $\mathfrak{q}(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}$ where A is a symmetric $n \times n$ matrix called the **matrix of the quadratic form**. Let f, g be quadratic forms and A_f, A_g their corresponding matrices. Then, $f \sim g$ if and only if A_f is similar to A_g.

Let $\mathfrak{q}(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic in $\mathbb{R}[x, y]$. We will use the following notation to represent the binary quadratic, $\mathfrak{q}(x, y) = [a, b, c]$. The **discriminant** of $\mathfrak{q}$ is $D = b^2 - 4ac$ and $\mathfrak{q}(x, y)$ is positive definite if $a > 0$ and $D < 0$. Denote the *set of positive definite binary quadratics* with $V_2^+(\mathbb{R})$. Let $\mathrm{SL}_2(\mathbb{R})$ acts as usual on the set of positive definite binary quadratic forms $V_2^+(\mathbb{R})$.

Consider the following map $\xi : V_2^+(\mathbb{R}) \to \mathcal{H}_2$, which is called the **zero map**:

$$[a, b, c] \to \xi(\mathfrak{q}) = \frac{-b + \sqrt{\Delta}}{2a}. \tag{52}$$

It is a bijection since given $z = x + iy$, we can find a, b, c such that $\mathfrak{q}(x, y)$ is positive definite given as $[1, -2x, x^2 + y^2]$. The map ξ gives us a one to one correspondence between positive definite quadratic forms and points in $\mathcal{H}_2$. Let Γ be the modular group acting on $\mathcal{H}_2$ and on V_2^+ as described above. Then, from [2], the zero map ξ is a Γ-equivariant map (i.e. $\xi(\mathfrak{q}^M) = M^{-1}\xi(\mathfrak{q})$, for any $M \in \Gamma$).

Define $\mathfrak{q} \in V_2^+(\mathbb{R})$ to be **reduced** if $\xi(\mathfrak{q}) \in \mathcal{F}$. The following are facts are well known. We suggest [2] among many other references.

(i) A quadratic form $\mathfrak{q} \in V_2^+(\mathbb{R})$ is reduced if and only if $|b| \leq a \leq c$.

(ii) Let $\mathfrak{q}$ be reduced with discriminant $\Delta = -D$. Then, $b \leq \sqrt{D/3}$.
(iii) The number of reduced forms of a fixed discriminant $\Delta = -D$ is finite.
(iv) Every $\mathfrak{q} \in V_2^+(\mathbb{R})$ is equivalent to a reduced form of the same discriminant.

Then we have the following; see [1, 2] among other places.

THEOREM 10. *Let $f(x,y) = ax^2 + bxy + cy^2$ be reduced. Then,* $\mathrm{H}(f) = c$. *Moreover, f obtains it absolute minimal height in its Γ-orbit.*

REMARK 2. *Lagrange proved that for every value Δ, there are only finitely many classes of binary quadratic forms with discriminant Δ. Their number is the **class number** of discriminant Δ. He described an algorithm, called* reduction, *for constructing a canonical representative in each class, the reduced form, whose coefficients are the smallest in a suitable sense. Gauss [15, 16] gave a better reduction algorithm in Disquisitiones Arithmeticae. For a more modern treatment for reduction of quadratics see also [34].*

4.2. Reduction of higher degree binary forms in their Γ-orbit. Let $f \in V_d(k)$ and $\Gamma_{\mathcal{O}_k} := \mathrm{SL}_2(\mathcal{O}_k)/\{\pm I\}$. To every binary form f it is associated a positive definite quadratic $\mathfrak{J}_f$ called the *Julia quadratic*. In [21] is proved that this is a covariant of the degree d binary forms and we can develop reduction theory using this quadratic. A degree d binary form is called *reduced* when $\xi(\mathfrak{J}_f)$ is in the fundamental domain of the action of the modular group Γ on $\mathcal{H}_2$.

Let $f \in V_d(\mathbb{R})$ as in Eq. (2). We consider f as a polynomial in a single variable $f(x,1)$. Let the real roots of $f(x,y)$ be α_i, for $1 \leq i \leq r$ and the pair of complex roots β_j, $\bar{\beta}_j$ for $1 \leq j \leq s$, where $r + 2s = d$. Then

$$f(x,1) = \prod_{i=1}^{r}(x-\alpha_i) \cdot \prod_{i=1}^{s}(x-\beta_i)(x-\bar{\beta}_i). \tag{53}$$

The ordered pair (r,s) of numbers r and s is called the **signature** of f. We associate to f two quadratic forms, which we are writing as polynomials, namely $T_r(x,1)$ and $S_s(x,1)$ of degree r and s respectively given by the formulas

$$T_r(x,1) = \sum_{i=1}^{r} t_i^2 (x-\alpha_i)^2, \quad \textit{and} \quad S_s(x,1) = \sum_{j=1}^{s} 2u_j^2 (x-\beta_j)(x-\bar{\beta}_j), \tag{54}$$

where t_i, u_j are to be determined; see [1]. Then,

$$\begin{aligned} T_r(x,1) &= \left(\sum_{i=1}^{r} t_i^2\right) x^2 - 2\left(\sum_{i-1}^{r} t_i^2 \alpha_i\right) x + \left(\sum_{i-1}^{r} t_i^2 \alpha_i^2\right) \\ S_s(x,1) &= 2\left(\sum_{j=1}^{s} u_j^2\right) x^2 - 4\left(\sum_{j=1}^{s} u_j^2 \operatorname{Re}(\beta_j)\right) x + 2\left(\sum_{j=1}^{s} u_j^2 \cdot ||\beta_j||^2\right). \end{aligned} \tag{55}$$

For a binary form $f(x,1)$ of signature (r,s) the quadratic form $\mathfrak{q}_f$ is defined as

$$\mathfrak{q}_f(x,1) := T_r(x,1) + S_s(x,1) \tag{56}$$

The discriminant of $\mathfrak{q}_f$ is a degree 4 homogenous polynomial in $t_1, \dots t_r$, $u_1, \dots, u_s$. We would like to pick values for $t_1, \dots t_r, u_1, \dots, u_s$ such that this discriminant is square free and minimal. Then we can use the reduction theory of quadratics (with square free, minimal discriminant) to determine the reduced form for $\mathfrak{q}_f$.

For quadratics T and S in Eq. (54) we define

$$\theta_T = \frac{a_0^2 \cdot \Delta_T}{t_1^2 \cdots t_r^2}, \qquad \theta_S = \frac{a_0^2 \cdot \Delta_S}{u_1^4 \cdots u_s^4} \tag{57}$$

Notice that T_r and S_s are given recursively as

$$T_r = T_{r-1} + t_r^2 (x-\alpha_r))^2, \qquad S_s = S_{s-1} + u_s^4 \left(x^2 - 2a_s x + (a_s^2 + b_s^2) \right) \tag{58}$$

Fort $f \in V_{d,\mathbb{R}}$ with signature (r, s) and equation Eq. (53), $\mathfrak{q}_f$ is a positive definite quadratic form with discriminant $\mathfrak{D}_f$ given by the formula

$$\mathfrak{D}_f = \Delta(T_r) + \Delta(S_s) - 8 \sum_{i,j} t_i^2 u_j^2 \left((\alpha_i - a_j)^2 + b_j^2 \right), \tag{59}$$

see [1]. Let θ_0 of a binary form be

$$\theta_0(f) := \frac{a_0^2 \cdot |\mathfrak{D}_f|^{d/2}}{\prod_{i=1}^r t_i^2 \prod_{j=1}^s u_j^4} \tag{60}$$

and consider $\theta_0(t_1, \dots, t_r, u_1, \dots, u_s)$ as a multivariable function in the variables $t_1, \dots, t_r$, $u_1, \dots, u_s$. We would like to pick such variables such that $\mathfrak{q}_f$ is a reduced quadratic, hence $\mathfrak{D}_f$ is minimal. This is equivalent with $\theta_0(t_1, \dots, t_r, u_1, \dots, u_s)$ obtaining a minimal value.

Lemma 5. *The function $\theta_0 : \mathbb{R}^{r+s} \to \mathbb{R}$ obtains a minimum at a unique point $(\bar{t}_1, \dots, \bar{t}_r, \bar{u}_1, \dots, \bar{u}_s)$.*

Julia in his thesis [21] proves existence and Stoll and Cremona prove uniqueness in [33]. Choosing $(\bar{t}_1, \dots, \bar{t}_r, \bar{u}_1, \dots, \bar{u}_s)$ that make θ_0 minimal gives a unique positive definite quadratic $\mathfrak{q}_f(x, y)$. We call this unique quadratic $\mathfrak{q}_f(x, y)$ for such a choice of $(\bar{t}_1, \dots, \bar{t}_r, \bar{u}_1, \dots, \bar{u}_s)$ the **Julia's quadratic** of $f(x, y)$, denote it by $\mathfrak{J}_f(x, y)$, and the quantity $\theta_f := \theta_0(\bar{t}_1, \dots, \bar{t}_r, \bar{u}_1, \dots, \bar{u}_s)$ the **Julia invariant**.

Lemma 6. *Consider $\mathrm{GL}_2(\mathbb{C})$ acting on $V_{d,\mathbb{R}}$. Then, θ is an invariant and $\mathfrak{J}$ is a covariant of order 2.*

4.2.1. *Minimal height of a binary form in its $\mathrm{SL}_2(\mathcal{O}_k)$-orbit.* Consider f a degree d binary form and k its minimal field of definition. Let $M \in \mathrm{SL}_2(\mathcal{O}_k)$ be a matrix such that f^M is reduced, i.e. $\bar{\xi}(f^M) \in \mathcal{F}_k$ where $\mathcal{F}_k$ is the fundamental domain of $\mathrm{SL}_2(\mathcal{O}_k)$ acting on $\mathcal{H}_3$; see [3] for details. A bound on the height of the reduced binary form with respect to Julia invariant is given below.

Lemma 7. *Let $f(x, 1) = a_0 \prod_{i=1}^d (x - \alpha_i)$ be a reduced binary form where α_i are the roots. Then, the height of this form can be bounded by Julia's invariant as*

$$H(f) \leq c \cdot \theta_f^{d/2}, \quad \text{where} \quad c = \left(\frac{1}{3}\right)^{\frac{d^2}{4}} \left(\frac{4}{d-1}\right)^{\frac{d(d-1)}{2}} \frac{1}{a_0^d} \tag{61}$$

Let f be a binary form and $\mathbb{F}$ its minimal field of definition. If f is reduced over $\mathbb{F}$, then it has minimal height in its $\Gamma_{\mathbb{F}}$-orbit. For a degree d binary form f defined over $\mathbb{F}$, $\mathfrak{D}_f$ its discriminant, and $L = \mathbb{F}(\mathfrak{D}_f)$. Then, $[L : \mathbb{F}] \leq d$.

4.3. Reduction of binary forms via the hyperbolic centroid. Another reduction method was introduced in [13] following the general idea of [21]. The main difference is the definition of the zero map in Eq. (52). We briefly summarize it here. Let $V^+_{2n,\mathbb{R}}(0,n)$ denote the set of degree $2n$ binary forms with real coefficients and no real roots (for the case of binary forms with real roots see [13]). Such binary forms are called **totally complex**. Every $f(x,z) \in V^+_{2n,\mathbb{R}}(0,n)$ can be factored as

$$f(x,z) = \prod_{j=1}^{n} \mathfrak{q}_{\alpha_j}(x,z), \tag{62}$$

where $\alpha_j = x_j + \mathbf{i}y_j$ and $\mathfrak{q}_{\alpha_j}(x,z) = (x-\alpha_j z)(x-\overline{\alpha_j}z)$ are quadratics with real coefficients. The **hyperbolic centroid**, $\mathcal{C}_\mathcal{H}(\alpha_1, \alpha_2, ..., \alpha_n)$ of the collection of a set of points in the upper-half plane $\{\alpha_j = x_j + \mathbf{i}y_j \in \mathcal{H}_2 \mid j = 1,2,...,n\}$ is the unique point $t + \mathbf{i}u \in \mathcal{H}_2$ that minimizes

$$\sum_{j=1}^{n} \frac{(t-x_j)^2 + (u-y_j)^2}{uy_j}, \tag{63}$$

see [13, Definition 5]. Let $\mathfrak{s}_j$ denote the j-th symmetric polynomial in $y_1, \dots, y_n$. It follows from ([13, Prop. 10]) that the centroid $\mathcal{C}_\mathcal{H} = t + \mathbf{i}u \in \mathcal{H}_2$ of $\alpha_1, \alpha_2, ..., \alpha_n$ satisfies

$$\begin{aligned} t &= \sum_{i=1}^{n} \left(\frac{y_1 y_2 \cdots y_{i-1} y_{i+1} \cdots y_n}{\mathfrak{s}_{n-1}(y_1, y_2, ..., y_n)} \right) x_i \\ |\mathcal{C}_\mathcal{H}|^2 &= \sum_{i=1}^{n} \left(\frac{y_1 y_2 \cdots y_{i-1} y_{i+1} \cdots y_n}{\mathfrak{s}_{n-1}(y_1, y_2, ..., y_n)} \right) |\alpha_i|^2 \\ \mathfrak{q}_{\mathcal{C}_\mathcal{H}}(x,z) &= \sum_{i=1}^{n} \left(\frac{y_1 y_2 \cdots y_{i-1} y_{i+1} \cdots y_n}{\mathfrak{s}_{n-1}(y_1, y_2, ..., y_n)} \right) \mathfrak{q}_{\alpha_i}(x,z). \end{aligned} \tag{64}$$

The **centroid zero map** $\xi_\mathcal{C} : V^+_{2n,\mathbb{R}}(0,n) \to \mathcal{H}_2$ is defined via

$$\xi_\mathcal{C}(f) := \mathcal{C}_\mathcal{H} = \mathcal{C}_\mathcal{H}(\alpha_1, \alpha_2, ..., \alpha_n). \tag{65}$$

The form

$$\mathfrak{J}^\mathcal{C}_f := (x - \mathcal{C}_\mathcal{H} z)(x - \overline{\mathcal{C}_\mathcal{H}} z) = \sum_{j=1}^{n} \left(\frac{y_1 y_2 \cdots y_{j-1} y_{j+1} \cdots y_n}{\mathfrak{s}_{n-1}(y_1, y_2, ..., y_n)} \right) \mathfrak{q}_{\alpha_j}(x,z) \tag{66}$$

is called the **centroid quadratic** of f. The reduction theory based on the centroid proceeds as before. Let $f(x,z)$ be a real binary form with no real roots. If $\xi_\mathcal{C}(f) \in \mathcal{F}$ then f is reduced. Otherwise, let $M \in \mathrm{SL}_2(\mathbb{R})$ such that $M^{-1}\xi_\mathcal{C}(f) \in \mathcal{F}$. The form f reduces to $f^M(x,z)$.

EXAMPLE 2 (Totally complex sextics). *Let $f(x,z) \in \mathbb{Z}[x,z]$ be a totally complex sextic factored over $\mathbb{R}$ as*

$$f(x,z) = (x^2 + a_1 xz + b_1 z^2)(x^2 + a_2 xz + b_2 z^2)(x^2 + a_3 xz + b_3 z^2).$$

Let $d_j = \sqrt{4b_j - a_j^2}$, $\mathbf{d} = (d_1, d_2, d_3)$, $\mathbf{a} = (a_1, a_2, a_3)$, $\mathbf{b} = (b_1, b_2, b_3)$. *The centroid zero map* $\xi_\mathcal{C}(f) = t + \mathbf{i}u \in H_2$ *of* f *is determined by*

$$
\begin{aligned}
t &= -\frac{1}{2}\left(\frac{d_2 d_3}{\mathfrak{s}_2(d_1,d_2,d_3)} a_1 + \frac{d_1 d_3}{\mathfrak{s}_2(d_1,d_2,d_3)} a_2 + \frac{d_1 d_2}{\mathfrak{s}_2(d_1,d_2,d_3)} a_3 \right), \\
|\xi_\mathcal{C}(f)|^2 &= \frac{d_2 d_3}{\mathfrak{s}_2(d_1,d_2,d_3)} b_1 + \frac{d_1 d_3}{\mathfrak{s}_2(d_1,d-2,d_3)} b_2 + \frac{d_1 d_2}{\mathfrak{s}_2(d_1,d_2,d_3)} b_3.
\end{aligned}
\tag{67}
$$

The centroid quadratic of f *is given by*

$$
\begin{aligned}
\mathfrak{J}_f^\mathcal{C} =& \frac{1}{\mathfrak{s}_2(d_1,d_2,d_3)} \left(d_2 d_3 (x^2 + a_1 xz + b_1 z^2) + d_1 d_3 (x^2 + a_2 xz + b_2 z^2) \right. \\
& \left. + d_1 d_2 (x^2 + a_3 xz + b_3 z^2) \right).
\end{aligned}
\tag{68}
$$

The reduction is defined over $\mathbb{Q}(d_1, d_2, d_3)$*; see* [13, Prop. 11]

This is generalized to any degree in [13, Prop. 12]. Let $f(x,z)$ be a totally complex form factored over $\mathbb{R}$ as below

$$
f(x,z) = \prod_{i=1}^n (x^2 + a_i xz + b_i z^2)
$$

and $d_i := \sqrt{4b_i - a_i^2}$, for $i = 1, \dots, n$. Let $\mathfrak{s}_{n-1} := \sum_{i=1}^r d_1 \cdots d_{i-1} \hat{d}_i d_{i+1} \cdots d_r$ where $\hat{d}_i$ denote a missing d_i. The centroid quadratic of $f(x,z)$ is given by

$$
\mathfrak{J}_f^\mathcal{C} = \sum_{i=1}^n \left(\frac{d_1 d_2 \cdots d_{i-1} d_{i+1} \cdots d_n}{\mathfrak{s}_{n-1}} \right) (x^2 + a_i xz + b_i z^2).
\tag{69}
$$

The centroid zero map $\xi_\mathcal{C}(f) = t + \mathbf{i}u \in \mathcal{H}_2$ is given by

$$
\begin{aligned}
t &= -\frac{1}{2} \sum_{i=1}^n \frac{d_1 \cdots d_{i-1} d_{i+1} \cdots d_n}{\mathfrak{s}_{n-1}} a_i, \\
u^2 &= \frac{1}{4\mathfrak{s}_{n-1}^2} \prod_{i=1}^n d_i \left(\mathfrak{s}_{n-1} \sum_{i=1}^n d_i + \sum_i d_1 \cdots \hat{d}_i \cdots \hat{d}_j \cdots d_n \, (a_i - a_j)^2 \right) \\
|\xi_\mathcal{C}(f)|^2 &= \sum_{i=1}^n \frac{d_1 \cdots d_{i-1} d_{i+1} \cdots d_n}{\mathfrak{s}_{n-1}} b_i.
\end{aligned}
\tag{70}
$$

The reduction is defined over $\mathbb{Q}(d_1, d_2, ..., d_n)$. As pointed out in [13], expressing $\xi_\mathcal{C}(f)$ in terms of invariants of f or symmetries of the roots of f, would be interesting problems on their own. It is shown in [13] that this hyperbolic reduction is different from the reduction method in [1,3,21] even though they both seem to find correctly the binary form with minimal height.

5. Concluding remarks

The methods described in this paper are new, as far as we are aware, and give a new approach for bookkeeping of points in the moduli space of superelliptic curves, provided that we have explicit descriptions of invariants of binary forms. For example, for genus $g = 2$, since we know explicitly the Igusa arithmetic invariants J_2, J_4, J_6, J_{10} we can explicitly list all points in $\mathbb{WP}_2^3(k)$ of a given weighted moduli height, including their twists. This makes it possible to study the arithmetic of the moduli space $\mathcal{M}_2$ and its rational points; see [6]. A similar approach can be used for any moduli space of curves when the corresponding invariants are explicitly known. To our knowledge, the only time when these two types of reduction have been combined is in seminal work of Birch and Swinnerton-Dyer in [**7**, **8**] for their computation with elliptic curves in an attempt to verify their famous conjecture. While in this paper we concerned ourselves with a generic superelliptic curve, cases when the moduli point is a singular point or equivalently the curve has a large automorphism group (see [**11**, **18**, **23**, **29**]) are even more interesting.

We must point out that the reduction of coefficients is build on the analogy with quadratics and seems to work fine in all the cases. However, they is no known proof as far as we are aware that this reduction will guarantee the binary form with smallest hight in the sense of [**31**]. This seems as a problem worth investigating.

The reader interested in further details from both geometric and arithmetic aspects of these problems can check [**12**, **17**, **20**, **25**, **28**, **30**].

References

[1] L. Beshaj, *Reduction theory of binary forms*, Advances on superelliptic curves and their applications, 2015, pp. 84–116. MR3525574

[2] ———, *Integral binary forms with minimal height*, ProQuest LLC, Ann Arbor, MI, 2016. Thesis (Ph.D.)–Oakland University. MR3579531

[3] ———, *Absolute reduction of binary forms*, Albanian J. Math. **12** (2018), no. 1, 36–77. MR3914348

[4] ———, *Minimal integral Weierstrass equations for genus 2 curves*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 63–82. MR3782460

[5] L. Beshaj, J. Gutierrez, and T. Shaska, *Weighted greatest common divisors and weighted heights*, J. Number Theory **213** (2020), 319–346. MR4091944

[6] L. Beshaj, R. Hidalgo, S. Kruk, A. Malmendier, S. Quispe, and T. Shaska, *Rational points in the moduli space of genus two*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 83–115. MR3782461

[7] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25. MR146143

[8] ———, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. MR179168

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

[10] A. Broughton, T. Shaska, and A. Wootton, *On automorphisms of algebraic curves*, Algebraic curves and their applications, 2019, pp. 175–212. MR3916740

[11] S. Allen Broughton, Charles Camacho, Jennifer Paulhus, Rebecca R. Winarski, and Aaron Wootton, *Using strong branching to find automorphism groups of n-gonal surfaces*, Albanian J. Math. **12** (2018), no. 1, 89–129. MR3914346

[12] E. Curri and T. Shaska, *On the stability of binary forms*, 2021. in preparation.

[13] A. Elezi and T. Shaska, *Reduction of binary forms via the hyperbolic centroid*, Lobachevskii J. Math. **42** (2021), no. 1, 84–95 (English).

[14] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and cryptography*, Algebraic curves and their applications, 2019, pp. 279–344. MR3916746

[15] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Lipsiae, 1801.

[16] ———, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966. MR0197380

[17] Ruben Hidalgo and Tony Shaska, *On the field of moduli of superelliptic curves*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 47–62. MR3782459

[18] Rubén A. Hidalgo and Milagros Izquierdo, *On the connectedness of the Branch locus of the Schottky space*, Albanian J. Math. **12** (2018), no. 1, 131–136. MR3914345

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

[20] M. Izquierdo and T. Shaska, *Cyclic curves over the reals*, Advances on superelliptic curves and their applications, 2015, pp. 70–83. MR3525573

[21] Gaston Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes.*, Mémories de lAcadémie des Sciences de lInsitut de France **55** (1917), 1–296.
[22] Joseph P. S. Kung and Gian-Carlo Rota, *The invariant theory of binary forms*, Bull. Amer. Math. Soc. (N.S.) **10** (1984), no. 1, 27–85. MR722856
[23] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, 2002, pp. 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371
[24] A. Malmendier and T. Shaska, *From hyperelliptic to superelliptic curves*, Albanian J. Math. **13** (2019), no. 1, 107–200. MR3978315
[25] A. Obus and T. Shaska, *Superelliptic curves with many automorphisms and CM Jacobians*, 2020.
[26] Peter J. Olver, *Classical invariant theory*, London Mathematical Society Student Texts, vol. 44, Cambridge University Press, Cambridge, 1999. MR1694364
[27] Jean-Pierre Serre, *Galois cohomology*, English, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author. MR1867431
[28] T. Shaska, *Computational aspects of hyperelliptic curves*, Computer mathematics, 2003, pp. 248–257. MR2061839
[29] ———, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 2003, pp. 248–254. MR2035219
[30] ———, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084
[31] T. Shaska and L. Beshaj, *Heights on algebraic curves*, Advances on superelliptic curves and their applications, 2015, pp. 137–175. MR3525576
[32] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210
[33] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647
[34] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag, Berlin-New York, 1981. Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text]. MR631688

Research Institute of Science and Technology (RISAT), Vlorë, ALBANIA
Email address: shaska@risat.org