Minimal models for superelliptic curves with extra automorphisms.

L. Beshaj

United States Military Academy,
Department of Mathematical Sciences,
West Point, NY, USA

Outline

Motivation

Minimal equation of curves, height and moduli height

Minimal models

Binary quadratics
Julia invariant and quadratic of a binary form
Reduction of higher degree binary forms

Computing the Julia quadratic for curves with automorphism

Genus two curves with Aut $(\mathcal{X}) \equiv V_4$
Genus two curves with Aut $(\mathcal{X}) \equiv D_4$
Genus two curves with Aut $(\mathcal{X}) \equiv D_6$

Let k be an algebraically closed field (char $k = 0$) and $\mathcal{X}$ be a superelliptic curve, i.e. $y^n = f(x)$.

There are two main problems

1) Determine an equation for $\mathcal{X}$ over a minimal field of definition K.

2) Find the best equation (with smaller coefficients) over K

In general, it is an open problem to determine an equation for $\mathcal{X}$ over a minimal field of definition K.

However, we will consider the second question. Once an equation over a minimal field of definition is given, how can we make this minimal in some sense?

Height and moduli height of curves

Let $f(x, y) \in K[x, y]$ the **height** of $f(x, y)$ (or *naive height*) is the maximum of the absolute values of the coefficients.

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

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

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

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

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

For any algebraic curve $\mathcal{X}_g$ we have $\overline{H}_K(\mathcal{X}_g) \leq H_K(\mathcal{X}_g)$.

Let g be an integer $g \geq 2$ and $\mathcal{M}_g$ denote the coarse moduli space of smooth, irreducible algebraic curves of genus g. The moduli space $\mathcal{M}_g$ is embedded in $\mathbb{P}^{3g-2}$.

Let $\mathfrak{p} \in \mathcal{M}_g$. We call the moduli height $\mathfrak{h}(\mathfrak{p})$ the usual height $H(P)$ in the projective space $\mathbb{P}^{3g-2}$. Obviously, $\mathfrak{h}(\mathfrak{p})$ is an invariant of the curve.

Theorem

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

Genus 2

Example

Let $\mathcal{X}$ be a genus 2 curve with equation

$$y^2 = 7\,t^6 - \left(78 + 16\sqrt{5}\right) t^5 + \left(72\sqrt{5} + 617\right) t^4 - \left(320\sqrt{5} + 2148\right) t^3 + \left(4961 + 456\sqrt{5}\right) t^2 - \left(5214 + 672\sqrt{5}\right) t + 3167$$

Then, the traditional algorithm gives

$$y^2 = 359785557t^6 + 4935433518t^5 + 29692428795t^4 + 98737979076t^3 + 193917220155t^2 + 210507034158t + 100220296853$$

Can we get a ”better” equation? Can we get ”the best” equation?

With a reduction algorithm which will explain later we get

$$y^2 = t^6 + 2t^4 + t^2 + 3$$

Genus 2

Example

Let $\mathcal{X}$ be a genus 2 curve with equation

$$y^2 = 7\,t^6 - \left(78 + 16\sqrt{5}\right) t^5 + \left(72\sqrt{5} + 617\right) t^4 - \left(320\sqrt{5} + 2148\right) t^3 + \left(4961 + 456\sqrt{5}\right) t^2 - \left(5214 + 672\sqrt{5}\right) t + 3167$$

Then, the traditional algorithm gives

$$y^2 = 359785557t^6 + 4935433518t^5 + 29692428795t^4 + 98737979076t^3 + 193917220155t^2 + 210507034158t + 100220296853$$

Can we get a ”better” equation? Can we get ”the best” equation?

With a reduction algorithm which will explain later we get

$$y^2 = t^6 + 2t^4 + t^2 + 3$$

Reduction of binary quadratics

$V_{n,k}$ denotes the $(n+1)$-dimensional subspace of $k[X,Z]$ consisting of homogeneous polynomials.

$$f(X,Z) = a_0X^n + a_1X^{n-1}Z + \cdots + a_nZ^n \tag{1}$$

of degree n up to multiplication by a constant. Elements in $V_{n,k}$ are called **binary forms of degree** n. The group $GL_2(k)$ acts on $V_{n,k}$ by linear transformations on the variables.

Let $Q(X,Z) = aX^2 + bXZ + cZ^2$ be a binary quadratic in $\mathbb{R}[X,Z]$. $Q(X,Z)$ is **positive definite** if $a > 0$ and $\Delta = b^2 - 4ac < 0$.

Denote the set of positive definite binary quadratics with $V^+_{2,\mathbb{R}}$, i.e.

$$V^+_{2,\mathbb{R}} = \left\{ Q(X,Z) \in \mathbb{R}[X,Z] \;\middle|\; Q(X,Z) \textit{ is positive definite} \right\}.$$

Modular Group and the Fundamental Domain

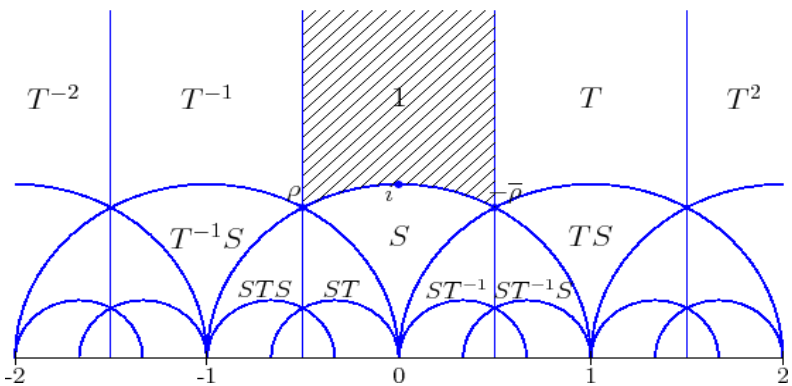
Let $\mathcal{H}_2 = \{z = x + iy \in \mathbb{C} \mid \ y > 0\} \subset \mathbb{C}$.

The group $\Gamma = SL_2(\mathbb{Z})/\{\pm I\}$ is called the **modular group**. Γ acts on $\mathcal{H}_2$ via linear fractional transformations

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z = \frac{\alpha z + \beta}{\gamma z + \delta} \tag{2}$$

where $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ and $z \in \mathcal{H}_2$.

The group Γ acting on $\mathcal{H}_2$ has a **fundamental domain** $\mathcal{F}$, i.e. a subset such that:
i) any point in $\mathcal{H}_2$ is Γ-equivalent to some point in $\mathcal{F}$,
ii) no two points in the interior of $\mathcal{F}$ are Γ-equivalent.



$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \to z + 1$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \to -\frac{1}{z}$$

A positive definite quadratic has exactly one root in $\mathcal{H}_2$.

Consider the following map which is called the **zero map**

$$\begin{aligned} \xi : V_{2,\mathbb{R}}^{+} &\to \mathcal{H}_2 \\ [Q] &\to \xi(Q) = \frac{-b}{2a} + \frac{\sqrt{|\Delta|}}{2a} i \end{aligned} \tag{3}$$

This map ξ is a bijection and an equivariant map (i.e., for every matrix $M \in \Gamma$, $\xi(Q^M) = \xi(Q)^{M^{-1}}$).

A quadratic $Q(X, Z)$ is said to be **reduced** if $\xi(Q) \in \mathcal{F}$.

Theorem

Every reduced quadratic has minimal height in its Γ*-orbit.*

Julia invariant and quadratic of a binary form

Let $f(x, y) \in \mathbb{R}[x, y]$ be a degree n binary form given as follows

$$f(X, Z) = a_0 X^n + a_1 X^{n-1} Z + \cdots + a_n Z^n$$

and suppose that $a_0 \neq 0$. Let the real roots of $f(X, Z)$ 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 $r + 2s = n$. The form can be factored as

$$f(X, Z) = \prod_{i=1}^{r} (X - \alpha_i Z) \cdot \prod_{i=1}^{s} (X - \beta_i Z)(X - \bar{\beta}_i Z). \tag{4}$$

The ordered pair (r, s) of numbers r and s is called the **signature** of the form f.
We associate to f the two quadratic forms $T_r(X, Z)$ and $S_s(X, Z)$ of degree r and s respectively given by the formulas

$$T_r(X, Z) = \sum_{i=1}^{r} t_i^2 (X - \alpha_i Z)^2, \quad \textit{and} \quad S_s(X, Z) = \sum_{j=1}^{s} 2u_j^2 (X - \beta_j Z)(X - \bar{\beta}_j Z), \tag{5}$$

where t_i, u_j are to be determined.

Proposition

$Q_f = T_r + S_s$ is a positive definite quadratic form with discriminant $\mathfrak{D}_\mathfrak{f}$

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

We define the θ_0 of a binary form as follows

$$\theta_0(f) = \frac{a_0^2 \cdot |\mathfrak{D}_\mathfrak{f}|^{n/2}}{\prod_{i=1}^r t_i^2 \prod_{j=1}^s u_j^4}.$$

We pick $t_1, \ldots, t_r, u_1, \ldots, u_s$ such that θ_0 obtains a minimum.

Proposition (Julia 1917)

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

The quadratic $\mathcal{J}_f := Q_f(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)(X, Z)$ is called the **Julia's quadratic** of f and $\theta_f := \theta_0(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)$ is called the **Julia invariant**.

Theorem

i) θ_f is an $SL_2(\mathbb{C})$ invariant
iii) $\mathcal{J}_f(X, Z) \in \mathbb{R}[X, Z]$ is a positive definite quadratic.

Thus, to each binary form f we associate a unique positive definite binary quadratic form $\mathcal{J}_f$ and therefore a unique point in $\mathcal{H}_2$.

Reduction of higher degree binary forms

Define the zero map for a binary form as

$$\begin{aligned} \bar{\xi} : V_{n,\mathbb{R}} &\longrightarrow V_{2,\mathbb{R}}^{+} \longrightarrow \mathcal{H}_2 \\ f &\longrightarrow \mathcal{J}_f \longrightarrow \xi(\mathcal{J}_f) \end{aligned}$$

Proposition

The map $\bar{\xi} : V_{n,\mathbb{R}} \to \mathcal{H}_2$ is $SL_2(\mathbb{C})$-equivariant (i.e., for every matrix $M \in SL_2(\mathbb{C})$, $\bar{\xi}(Q^M) = \bar{\xi}(Q)^{M^{-1}}$). .

A binary form $f \in \mathbb{R}[X, Z]$ is said to be a **reduced binary form** if $\bar{\xi}(f) \in \mathcal{F}$. We denote by **red** (f) the reduction form of f.

Determining the Julia quadratic

Let be given a binary form $f \in V_{n,\mathbb{C}}$ Then, $f(X,1)$ can be factored as

$$f(X,1) = a_0(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n), \tag{6}$$

Let $\alpha_{i,j} = |\alpha_i - \alpha_j|^2$, $i<j$ and $w = t_i^2$ we have

$$\begin{cases} n\cdot w_1\left(w_2\alpha_{1,2}+w_3\alpha_{1,3}+\cdots+w_n\alpha_{1,n}\right)-2\cdot\sum_{i<j}w_iw_j\alpha_{i,j}=0 \\ n\cdot w_2\left(w_1\alpha_{1,2}+w_3\alpha_{2,3}+\cdots+w_n\alpha_{2,n}\right)-2\cdot\sum_{i<j}w_iw_j\alpha_{i,j}=0 \\ \vdots \\ n\cdot w_n\left(w_1\alpha_{2,n}+w_3\alpha 3,n+\cdots+w_{n-1}\alpha_{n-1,n}\right)-2\cdot\sum_{i<j}w_iw_j\alpha_{i,j}=0 \\ w_1\cdot w_2\cdots w_n-1=0 \end{cases} \tag{7}$$

For totally real binary forms the Julia quadratic is the unique quadratic factor of the homogenous polynomial $G(x,y)$ which has degree $d=(n-1)(n-2)$ and is defined as follows

$$G(x,y) = \frac{(x\cdot f_x(-f_y(x,y),f_x(x,y))+y\cdot f_y(-f_y(x,y),f_x(x,y)))}{n\,f(x,y)} \tag{8}$$

Then

In this example we show how these coefficients are picked in the case of binary cubics with reals roots.

Example

Let $f(X) = aX^3 + bX^2 + cX + d$ be a binary cubic with three real roots $\alpha_1, \alpha_2, \alpha_3$. We pick t_1, t_2, t_3 as follows:

$$t_1 = (\alpha_2 - \alpha_3)^2, t_2 = (\alpha_3 - \alpha_1)^2, t_3 = (\alpha_1 - \alpha_2)^2$$

and Julia quadratic is as follows

$$\mathcal{J}_f(X, Z) = (\alpha_2 - \alpha_3)^2(X - \alpha_1)^2 + (\alpha_3 - \alpha_1)^2(X - \alpha_2)^2 + (\alpha_1 - \alpha_2)^2(X - \alpha_3)^2$$

We can express the Julia quadratic covariant in terms of the coefficient of $f(X)$ as follows

$$\mathcal{J}_f(X, Z) = (b^2 - 3ac)X^2 + (bc - 9ad)X + (c^2 - 3bd)$$

up to a constant factor.

Julia quadratic of genus two curves with extra automorphisms

What about the general case when the standard form is not defined over a ring of integers?

By definition the Julia quadratic depends on the roots of the binary form.

Since we want to compute the Julia quadratic for each curve, then first we would like to determine the Weierstrass points of the given curve.

The following result gives a choice for the set of Weierstrass points.

Lemma

Let $\mathcal{X}$ be a genus 2 curve defined over a field k such that char k $\neq 2$ and W be the set of Weierstrass points. Then the following hold:

i) If Aut $(\mathcal{X}) \equiv V_4$, then $W = \{\pm\alpha, \pm\beta, \pm\frac{1}{\alpha\beta}\}$

ii) If Aut $(\mathcal{X}) \equiv D_4$, then $W = \{\pm 1, \pm\alpha, \pm\frac{1}{\alpha}\}$.

iii) If Aut $(\mathcal{X}) \equiv D_6$, then $W = \{1, \epsilon_3, \epsilon_3^2, I, I\epsilon_3, I\epsilon_3^2\}$, where I is a parameter and ϵ_3 is a primitive third root of unity.

The case of V_4 group

The set of Weierstrass points is $W = \{\pm\alpha, \pm\beta, \pm\frac{1}{\alpha\beta}\}$ and since α and β are distinct the only two cases that can happen are the following:
i) α and β are conjugates of each other and $W = \{\pm\alpha, \pm\overline{\alpha}, \pm\frac{1}{||\alpha||^2}\}$
ii) $\alpha, \beta \in \mathbb{R}$, i.e. all roots are real and $W = \{\pm\alpha, \pm\beta, \pm\frac{1}{\alpha\beta}\}$

In the first case the Julia quadratic can be computed solving the system.

In the second case the equation of the curve $\mathcal{X}$ is a totally real binary form. For a totally real binary form we can perform reduction using the polynomial $G(x, z)$ defined in Eq. (8).

Computations show that $G_f(x, z)$ is factored in three factors. One has degree 2, one degree 6, and one degree 12 as follows

$$G_f(x,1) = 1024\, u^6 \left(4\, u^3 - v^2\right)^3 \cdot g_0(x,1) \cdot g_1(x,1) \cdot g_2(x,1)$$

where

$$
\begin{aligned}
g_0(x) =& x^2 - (v^2 - 4\,u^3) \\
g_1(x) =& \left(-u^2 - 3\,v\right) x^6 + \left(36\,u^3 - 2\,u^2 v - 18\,v^2\right) x^5 \\
&+ \left(-4\,u^5 + 180\,u^3 v + u^2 v^2 - 45\,v^3\right) x^4 \\
&+ \left(-480\,u^6 - 16\,u^5 v + 360\,u^3 v^2 + 4\,u^2 v^3 - 60\,v^4\right) x^3 + \\
&+ \left(16\,u^8 - 720\,u^6 v - 8\,u^5 v^2 + 360\,u^3 v^3 + u^2 v^4 - 45\,v^5\right) x^2 + \\
&+ \left(576\,u^9 - 32\,u^8 v - 576\,u^6 v^2 + 16\,u^5 v^3 + 180\,u^3 v^4 - 2\,u^2 v^5 - 18\,v^6\right) x + \\
&+ 64\,u^{11} + 192\,u^9 v - 48\,u^8 v^2 - 144\,u^6 v^3 + 12\,u^5 v^4 + 36\,u^3 v^5 - u^2 v^6 - 3\,v^7
\end{aligned}
\tag{9}
$$

while we don't display $g_2(x)$.

Genus two curves with Aut $(\mathcal{X}) \equiv D_4$

The set of Weierstrass points is $W = \{\pm 1, \pm\alpha, \pm\frac{1}{\alpha}\}$.Hence, we have the following two cases:
i) If $||\alpha||^2 = 1$ then α and $\frac{1}{\alpha}$ are conjugates of each other and $W = \{\pm 1, \pm\alpha, \pm\overline{\alpha}\}$
ii) otherwise all roots are real and $W = \{\pm 1, \pm\alpha, \pm\frac{1}{\alpha}\}$

In the first case the Julia quadratic can be computed solving the system.

In the second case, if $\alpha \in \mathbb{R}$ the binary form corresponding to $\mathcal{X}$ is a totally real form. Computing the polynomial $G_f(x, z)$ defined in Eq. (8) for this curves we have

$$G_f(x,1) = \left(5\,x^4 + x^2 - 3\,s\right) \cdot \left(25\,s x^8 + (12 - 10\,s)x^6 + (37\,s - 70\,s^2)x^4 + 14\,s^2 x^2 + s^3\right)$$

For a given binary form the Julia quadratic will be the unique quadratic factor of G_f.

Genus two curves with Aut $(\mathcal{X}) \equiv D_6$

In an analogue way the polynomial $G_f(x, z)$ for curves with automorphism group D_6 is

$$G_f(x,1) = 972\,x\,\left(x^6 - w\right) \left(8\,wx^{12} + (12\,w+1)x^9 + 12\,wx^6 + (12\,w+1)wx^3 + 8\,w^3\right) \tag{10}$$

For a given binary form the Julia quadratic will be the unique quadratic factor of G_f.

Hence, for genus two curves with extra involution we can conclude the following.

Theorem

Let $\mathcal{X}$ be a genus two curve with Aut $(\mathcal{X}) > 2$, affine equation $y^2 = f(x)$, and F its field of moduli. Then, the following are true

i) If Aut $(C) \equiv V_4$, then the Julia quadratic is the unique quadratic factor of $G_f(x, z)$ as defined in Eq. (9).

ii) If Aut $(C) \equiv D_4$, then the Julia quadratic is the unique quadratic factor of

$$G_f(x,1) = \left(5\,x^4 + x^2 - 3\,s\right) \cdot \left(25\,sx^8 + (12 - 10\,s)x^6 + (37\,s - 70\,s^2)x^4 + 14\,s^2x^2 + s^3\right)$$

iii) If Aut $(C) \equiv D_6$, then the Julia quadratic is the unique quadratic factor of

$$G_f(x,1) = 972\,x\,\left(x^6 - w\right)\left(8\,wx^{12} + (12\,w + 1)x^9 + 12\,wx^6 + (12\,w + 1)wx^3 + 8\,w^3\right) \tag{11}$$

Work in progress

Theorem (B-, Steward)

Let $\mathcal{X}$ be a superelliptic curve with an extra involution and Weierstrass equation

$$y^n = x^{2n} + \sum_{i=0}^{n-1} a_i x^{2i} + 1$$

over a ring of integers $\mathfrak{O}_K$. Then, $\mathcal{X}$ has minimal absolute height.

Thank you for your attention!