Constructing genus 3 hyperelliptic Jacobians with CM

Jennifer Balakrishnan, Sorina Ionica, Kristin Lauter and Christelle Vincent

University of Oxford, Université de Picardie Jules Verne,
Microsoft Research, University of Vermont

ANTS 2016

Questions

- Given K be a CM sextic field, is there a genus 3 hyperelliptic curve with CM by K?
- If this is the case, can you write down a model for this hyperelliptic curve?

Genus 3 hyperelliptic curves

Over $\mathbb{C}$ the Jacobian is isom. to a complex torus $\mathbb{C}^3/\mathbb{Z}^3 + Z\mathbb{Z}^3$ with

$$\mathcal{H}_3 = \{Z \in M_{3\times 3}(\mathbb{C}) : Z^T = Z, \Im(Z) > 0\}.$$

We want:

- to find a period matrix with CM by K.
- decide if it is hyperelliptic. If so, compute a_i such that:

The Rosenhain model

$$y^2 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)(x - a_5)(x - a_6)(x - a_7).$$

Related work

Weng 2001

- If $\mathbb{Q}(i) \subset K$, then all Jacobians with CM by $\mathcal{O}_K$ are hyperelliptic.
- Compute the Shioda invariants and a model of the curve.

A. Weng :*If we start with a randomly chosen CM field K of degree 6, we do not expect that the set of principally polarized abelian varieties with CM by $\mathcal{O}_K$ contains the Jacobian of a hyperelliptic curve.*

Related work

$$\lambda_3 = \frac{(\alpha_{15}\alpha_3)^4 + (\alpha_{12}\alpha_1)^4 - (\alpha_{14}\alpha_2)^4}{2(\alpha_{15}\alpha_3)^4}$$

$$\lambda_4 = \frac{(\alpha_4\alpha_9)^4 + (\alpha_6\alpha_{11})^4 - (\alpha_{13}\alpha_8)^4}{2(\alpha_4\alpha_9)^4}$$

$$\lambda_5 = \frac{(\alpha_{10}\alpha_9)^4 + (\alpha_6\alpha_5)^4 - (\alpha_7\alpha_8)^4}{2(\alpha_{10}\alpha_9)^4}$$

$$\lambda_6 = \frac{(\alpha_{10}\alpha_3)^4 + (\alpha_{12}\alpha_5)^4 - (\alpha_{14}\alpha_7)^4}{2(\alpha_{10}\alpha_3)}$$

$$\lambda_7 = \frac{(\alpha_{15}\alpha_4)^4 + (\alpha_{11}\alpha_1)^4 - (\alpha_{13}\alpha_2)^4}{2(\alpha_{15}\alpha_4)^4}.$$

Table 1: Choice of the α_i in (4) depending on the theta constant θ with $\delta(\Omega) = 0$

θ	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}	α_{14}	α_{15}
θ_{00}	θ_{70}	θ_{12}	θ_{34}	θ_{01}	θ_{02}	θ_{14}	θ_{60}	θ_{76}	θ_{25}	θ_{33}	θ_{30}	θ_{05}	θ_{52}	θ_{67}	θ_{41}
θ_{04}	θ_{00}	θ_{75}	θ_{60}	θ_{43}	θ_{73}	θ_{61}	θ_{03}	θ_{14}	θ_{21}	θ_{33}	θ_{24}	θ_{20}	θ_{76}	θ_{55}	θ_{40}
θ_{02}	θ_{00}	θ_{66}	θ_{75}	θ_{21}	θ_{60}	θ_{67}	θ_{06}	θ_{01}	θ_{50}	θ_{57}	θ_{16}	θ_{42}	θ_{70}	θ_{24}	θ_{37}
θ_{06}	θ_{00}	θ_{25}	θ_{41}	θ_{30}	θ_{33}	θ_{21}	θ_{16}	θ_{04}	θ_{61}	θ_{73}	θ_{70}	θ_{01}	θ_{55}	θ_{16}	θ_{40}
θ_{01}	θ_{00}	θ_{57}	θ_{75}	θ_{33}	θ_{52}	θ_{76}	θ_{05}	θ_{21}	θ_{42}	θ_{66}	θ_{07}	θ_{06}	θ_{50}	θ_{16}	θ_{34}
θ_{05}	θ_{00}	θ_{34}	θ_{60}	θ_{12}	θ_{33}	θ_{30}	θ_{07}	θ_{04}	θ_{70}	θ_{73}	θ_{52}	θ_{20}	θ_{66}	θ_{61}	θ_{40}
θ_{03}	θ_{00}	θ_{57}	θ_{66}	θ_{67}	θ_{50}	θ_{55}	θ_{07}	θ_{02}	θ_{70}	θ_{75}	θ_{37}	θ_{43}	θ_{60}	θ_{61}	θ_{25}
θ_{07}	θ_{00}	θ_{25}	θ_{10}	θ_{41}	θ_{43}	θ_{70}	θ_{66}	θ_{55}	θ_{30}	θ_{03}	θ_{01}	θ_{50}	θ_{24}	θ_{75}	θ_{40}
θ_{40}	θ_{00}	θ_{05}	θ_{34}	θ_{67}	θ_{06}	θ_{76}	θ_{03}	θ_{73}	θ_{10}	θ_{60}	θ_{01}	θ_{52}	θ_{04}	θ_{57}	θ_{66}
θ_{42}	θ_{00}	θ_{16}	θ_{05}	θ_{61}	θ_{60}	θ_{57}	θ_{76}	θ_{41}	θ_{50}	θ_{67}	θ_{66}	θ_{02}	θ_{70}	θ_{61}	θ_{07}
θ_{41}	θ_{00}	θ_{67}	θ_{05}	θ_{33}	θ_{67}	θ_{06}	θ_{75}	θ_{61}	θ_{02}	θ_{16}	θ_{37}	θ_{01}	θ_{50}	θ_{66}	θ_{04}
θ_{43}	θ_{00}	θ_{37}	θ_{06}	θ_{52}	θ_{50}	θ_{75}	θ_{67}	θ_{42}	θ_{70}	θ_{55}	θ_{57}	θ_{03}	θ_{60}	θ_{34}	θ_{05}
θ_{20}	θ_{00}	θ_{07}	θ_{42}	θ_{16}	θ_{33}	θ_{52}	θ_{34}	θ_{55}	θ_{40}	θ_{21}	θ_{04}	θ_{50}	θ_{03}	θ_{57}	θ_{67}
θ_{24}	θ_{00}	θ_{75}	θ_{60}	θ_{33}	θ_{67}	θ_{50}	θ_{67}	θ_{25}	θ_{10}	θ_{52}	θ_{73}	θ_{20}	θ_{06}	θ_{55}	θ_{40}
θ_{21}	θ_{00}	θ_{67}	θ_{55}	θ_{03}	θ_{42}	θ_{66}	θ_{25}	θ_{01}	θ_{52}	θ_{76}	θ_{37}	θ_{61}	θ_{50}	θ_{06}	θ_{34}
θ_{25}	θ_{00}	θ_{07}	θ_{41}	θ_{10}	θ_{52}	θ_{61}	θ_{55}	θ_{66}	θ_{21}	θ_{67}	θ_{50}	θ_{01}	θ_{57}	θ_{06}	θ_{40}
θ_{60}	θ_{00}	θ_{52}	θ_{61}	θ_{03}	θ_{33}	θ_{67}	θ_{61}	θ_{40}	θ_{16}	θ_{37}	θ_{07}	θ_{10}	θ_{55}	θ_{42}	θ_{04}
θ_{66}	θ_{00}	θ_{05}	θ_{67}	θ_{41}	θ_{03}	θ_{73}	θ_{06}	θ_{76}	θ_{33}	θ_{43}	θ_{01}	θ_{52}	θ_{04}	θ_{57}	θ_{40}
θ_{61}	θ_{00}	θ_{37}	θ_{05}	θ_{43}	θ_{42}	θ_{76}	θ_{75}	θ_{41}	θ_{52}	θ_{66}	θ_{67}	θ_{21}	θ_{50}	θ_{16}	θ_{24}
θ_{67}	θ_{00}	θ_{34}	θ_{70}	θ_{02}	θ_{41}	θ_{20}	θ_{75}	θ_{61}	θ_{60}	θ_{01}	θ_{42}	θ_{30}	θ_{76}	θ_{04}	θ_{40}
θ_{10}	θ_{00}	θ_{07}	θ_{75}	θ_{43}	θ_{33}	θ_{37}	θ_{34}	θ_{30}	θ_{67}	θ_{16}	θ_{66}	θ_{50}	θ_{61}	θ_{57}	θ_{25}
θ_{14}	θ_{00}	θ_{25}	θ_{60}	θ_{52}	θ_{42}	θ_{01}	θ_{67}	θ_{24}	θ_{41}	θ_{02}	θ_{67}	θ_{20}	θ_{37}	θ_{05}	θ_{40}
θ_{12}	θ_{00}	θ_{76}	θ_{55}	θ_{01}	θ_{60}	θ_{57}	θ_{16}	θ_{21}	θ_{50}	θ_{67}	θ_{06}	θ_{52}	θ_{70}	θ_{24}	θ_{07}
θ_{16}	θ_{00}	θ_{75}	θ_{30}	θ_{52}	θ_{42}	θ_{03}	θ_{37}	θ_{76}	θ_{43}	θ_{02}	θ_{67}	θ_{70}	θ_{67}	θ_{05}	θ_{40}
θ_{50}	θ_{00}	θ_{04}	θ_{76}	θ_{61}	θ_{01}	θ_{24}	θ_{05}	θ_{20}	θ_{42}	θ_{67}	θ_{07}	θ_{10}	θ_{03}	θ_{61}	θ_{66}
θ_{52}	θ_{00}	θ_{16}	θ_{75}	θ_{01}	θ_{60}	θ_{37}	θ_{76}	θ_{21}	θ_{40}	θ_{07}	θ_{66}	θ_{67}	θ_{70}	θ_{04}	θ_{67}
θ_{55}	θ_{00}	θ_{24}	θ_{60}	θ_{67}	θ_{73}	θ_{30}	θ_{57}	θ_{61}	θ_{70}	θ_{33}	θ_{52}	θ_{20}	θ_{76}	θ_{04}	θ_{40}
θ_{57}	θ_{00}	θ_{75}	θ_{10}	θ_{01}	θ_{03}	θ_{70}	θ_{76}	θ_{05}	θ_{30}	θ_{43}	θ_{41}	θ_{50}	θ_{34}	θ_{25}	θ_{40}
θ_{30}	θ_{00}	θ_{16}	θ_{75}	θ_{52}	θ_{02}	θ_{06}	θ_{61}	θ_{10}	θ_{03}	θ_{07}	θ_{57}	θ_{70}	θ_{41}	θ_{66}	θ_{05}
θ_{34}	θ_{00}	θ_{25}	θ_{60}	θ_{73}	θ_{67}	θ_{50}	θ_{37}	θ_{75}	θ_{10}	θ_{52}	θ_{33}	θ_{20}	θ_{16}	θ_{05}	θ_{40}
θ_{33}	θ_{00}	θ_{67}	θ_{75}	θ_{02}	θ_{50}	θ_{75}	θ_{37}	θ_{12}	θ_{70}	θ_{55}	θ_{07}	θ_{73}	θ_{60}	θ_{14}	θ_{05}
θ_{37}	θ_{00}	θ_{24}	θ_{70}	θ_{02},	θ_{01}	θ_{20}	θ_{25}	θ_{04}	θ_{60}	θ_{41}	θ_{42}	θ_{30}	θ_{66}	θ_{61}	θ_{40}
θ_{70}	θ_{00}	θ_{07}	θ_{14}	θ_{42}	θ_{52}	θ_{57}	θ_{55}	θ_{50}	θ_{73}	θ_{76}	θ_{66}	θ_{30}	θ_{61}	θ_{37}	θ_{24}
θ_{76}	θ_{00}	θ_{14}	θ_{01}	θ_{50}	θ_{12}	θ_{61}	θ_{06}	θ_{75}	θ_{21}	θ_{52}	θ_{10}	θ_{41}	θ_{04}	θ_{55}	θ_{40}
θ_{75}	θ_{00}	θ_{57}	θ_{10}	θ_{01}	θ_{43}	θ_{30}	θ_{61}	θ_{67}	θ_{70}	θ_{03}	θ_{41}	θ_{50}	θ_{16}	θ_{07}	θ_{40}
θ_{73}	θ_{00}	θ_{10}	θ_{01}	θ_{37}	θ_{50}	θ_{02}	θ_{40}	θ_{67}	θ_{05}	θ_{57}	θ_{30}	θ_{06}	θ_{20}	θ_{16}	θ_{07}

One approach to the period matrix

Let $H_1(C, \mathbb{Z})$ be the first homology group of C.
Choose a (non-unique!) *symplectic basis* of $H_1(C, \mathbb{Z})$:

$$A_1, A_2, A_3, B_1, B_2, B_3$$

There is a *unique* basis $\omega_1, \omega_2, \omega_3$ of holomorphic 1-forms of C such that

$$\int_{A_i} \omega_j = \delta_{ij}.$$

Then we form the *period matrix* Z by

$$Z_{ij} = \int_{B_i} \omega_j.$$

The Abel-Jacobi map

$$AJ\colon Jac(C) \to \mathbb{C}^g/\mathbb{Z}^3 + Z\mathbb{Z}^3$$

$$D = \sum_{P\in C} n_P P \mapsto \left(\sum_{P\in C}\int_{P_\infty}^{P} \omega_j\right)_{j=1,2,3} \pmod{\mathbb{Z}^3 + Z\mathbb{Z}^3}$$

Mumford's fundamental system of theta characteristics

Let P_i, $i \in \{1, \ldots, 2g+1\}$, $P_\infty = \infty$ be the branch points.

Mumford computed $AJ(P_i - P_\infty) = (\eta_i)_2 + Z(\eta_i)_1$ with

$$\eta_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \eta_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\eta_3 = \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \eta_4 = \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$\eta_5 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \eta_6 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\eta_7 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad \eta_\infty = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The 2-torsion

$$Jac(X)[2](C) \longrightarrow (1/2)\mathbb{Z}^6/\mathbb{Z}^6$$

$$\sum_{i\in S} P_i - (\#S)P_\infty \longmapsto \eta_S = \sum_{i\in S} \eta_i$$

for all S with $\#S \equiv 0 \pmod 2$.

The theta constants

For $\delta, \epsilon \in (1/2)\mathbb{Z}^3/\mathbb{Z}^3$, we define a theta constant by

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix}(Z) = \sum_{n \in \mathbb{Z}^3} \exp\left(\pi i (n + \frac{1}{2}\delta)^t Z (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon)\right),$$

where $Z \in \mathcal{H}_3$ and $\exp(z) = e^z$.

A theta constant is **even** if $\delta^t \epsilon \equiv 0$ and **odd** otherwise.

Odd theta constants vanish and even ones determine completely the Jacobian.

Computing a model for the curve

The Rosenhain equation is
$y^2 = x(x-1)(x-a_3)(x-a_4)(x-a_5)(x-a_6)(x-a_7)$.

Let $B = \{1, 2, 3, 4, 5, 6, 7, \infty\}$ and $U = \{1, 3, 5, 7\}$.

Theorem (Mumford, Takase)

Let $B = V \sqcup W \sqcup \{1, 2, m\}$ with $\#V = \#W = 2$, we have

$$a_m = \left(\frac{\theta[\eta_{U \circ (V \cup \{1,m\})}](Z) \cdot \theta[\eta_{U \circ (W \cup \{1,m\})}](Z)}{\theta[\eta_{U \circ (V \cup \{1,2\})}](Z) \cdot \theta[\eta_{U \circ (W \cup \{1,2\})}](Z)} \right)^2$$

Second approach : period matrix with CM

Choose embeddings $\Phi = (\phi_1, \phi_2, \phi_3)$ of K in $\mathbb{C}$ and let $\mathfrak{a}$ be a fractional ideal of K.

Consider the lattice $\Phi(\mathfrak{a}) = \{(\phi_1(x), \phi_2(x), \phi_3(x)) : x \in \mathfrak{a}\}$.

Assume there is $\xi \in K$ such that $\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}} = (\xi^{-1})$. Then

$$E(z, w) = \sum_{i=1}^{3} \phi_i(\xi)(\bar{z}_i w_i - z_i \bar{w}_i), \qquad \text{for } z, w \in \mathbb{C}^3$$

is a Riemann form on $\mathbb{C}^3/\Phi(\mathfrak{a})$.

The period matrix Z comes as the matrix giving a symplectic basis for this form.

Towards actual computations

Definition

We say that a system of characteristics $\eta_i \in (1/2)\mathbb{Z}^6/\mathbb{Z}^6$ is associated to the period matrix $Z \in \mathcal{H}_3$ if there is a labeling of the branch points s.t. for all i we have $AJ(P_i - P_\infty) = (\eta_i)_2 + Z(\eta_i)_1$, where the Abel-Jacobi map is defined by the symplectic basis of the homology used to compute the period matrix Z.

Systems of characteristics

$\eta_i \in \frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$, $i \in B$, is a system of characteristics iff:

- $\eta_\infty = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
- $e_2(\eta_i, \eta_j) = -1$, for all $i \neq j$ in $B - \{\infty\}$.
- The set U given by $\{i | \eta_i \text{ is odd}\} \cup \{\infty\}$ has cardinality divisible by 4.
- $\sum_{i=1}^{7} \eta_i = 0$ and $span(\eta_i) = \frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$.

Fact (C. Poor): $Sp(6, \mathbb{F}_2)$ acts transitively on systems of characteristics.

The vanishing theorem

Theorem (Mumford, Poor)

Z is the period matrix. Then

- There are $\eta_i \in (1/2)\mathbb{Z}^6/\mathbb{Z}^6$ and U such that $Z \in \mathcal{H}_3$ satisfies
$$\vartheta[\eta_U](Z) = 0.$$
and this is the only vanishing even theta constant.
- There is a hyperelliptic curve whose Jacobian has period matrix Z and η is associated to this matrix.

Thomae's formule in genus 3

Thomae's formulae

If Z be a hyperelliptic period matrix and η_i a system of characteristics attached to it. Then

$$a_m = \left(\frac{\theta[\eta_{U\circ(V\cup\{1,m\})}](Z) \cdot \theta[\eta_{U\circ(W\cup\{1,m\})}](Z)}{\theta[\eta_{U\circ(V\cup\{1,2\})}](Z) \cdot \theta[\eta_{U\circ(W\cup\{1,2\})}](Z)} \right)^2$$

where U is the set of is s.t. η_i is odd and ∞.

Note: in Weng, Weber etc $U = \{1, 3, 5, 7\}$.

See example in our paper for which $U = \{1, 2, 3, 4, 5, 6, 7, \infty\}$.

The algorithm

1. Given an ideal $\mathfrak{a}$, write down the period matrix.

2. Search for the characteristic γ giving the even vanishing theta constant.

3. Take η_i Mumford's system of char. Find $M \in \mathrm{Sp}(6, \mathbb{F}_2)$ such that for $\bar{\eta}_i = M\eta_i$, for $i \in \{0 \ldots 6\}$ we have

$$\bar{\eta}_U = \gamma$$

4. Compute theta constants with enough precision and recognize the Rosenhain coefficients as algebraic integers.

Precision issues and error bound

Approximate $\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix}(Z)$ by

$$S_B = \sum_{n \in [-B,B]^3} \exp\left(\pi i((n+\frac{1}{2}\delta)^t Z(n+\frac{1}{2}\delta) + 2(n+\frac{1}{2}\delta)^t(\frac{1}{2}\epsilon))\right)$$

- Error bounds are not known.
- In experiments, we set precision t bits and computed S_B for several B until we obtained $|S_B - S_{B'}| < 2^{-t}$.

Let $K_0 = \mathbb{Q}[x]/(x^3 - x^2 - 2x + 1)$ and $K = K_0[x]/(x^2 + 7)$.

$$\begin{aligned} h_3(x) &= x^6 - 5x^5 + 11x^4 - 13x^3 + 9x^2 - 3x + 1 \\ h_4(x) &= x^6 - 2x^5 + 4x^4 - 8x^3 + 9x^2 - 4x + 1 \\ h_5(x) &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \\ h_6(x) &= x^6 - 3x^5 + 9x^4 - 13x^3 + 11x^2 - 5x + 1 \\ h_7(x) &= x^6 - 4x^5 + 9x^4 - 8x^3 + 4x^2 - 2x + 1 \end{aligned}$$

Validating results

- Take p a "good" prime number, s.t. $h_3, h_4, \ldots h_7$ split in $\mathbb{F}_p$.
- Take $a_3, a_4, \ldots, a_7$ roots of these polynomials and construct the curve/ $\mathbb{F}_p$
- Compute the number of points and check it equals $N_{K/\mathbb{Q}}(\pi - 1)$.

What invariants?

Let $K = K_0(i)$, with K_0 given by the polynomial $X^3 - X^2 - 2X + 1$.

$$\begin{aligned} h_3 &= x^3 + 22x^2 - 16x - 8 \\ h_4 &= x^3 - 4x^2 + 3x + 1 \\ h_5 &= -8x^3 + 8x^2 + 2x - 1 \\ h_6 &= x^3 - 9x^2 - x + 1 \\ h_7 &= x^3 + 2x^2 - x - 1 \end{aligned}$$

Weng computed Shioda invariants:

$$\begin{aligned} h_3(x) &= 1048576x - 2187 \\ h_4(x) &= 131072x - 24373629 \\ h_5(x) &= 16384x + 11632436487 \\ h_6(x) &= 16384000000000x + 2952169653573 \\ h_7(x) &= 2048000000000000x - 1168038669244419 \end{aligned}$$

Timings

1. computing 36 even theta constants - 3 min.
2. correcting the fundamental system of characteristics - 1 min
3. computing the Rosenhain coefficients - 1 min.
4. recognizing coefficients as algebraic integers with the PARI/GP algdep function - less than 1 min.

Source code available on github

`https://github.com/christellevincent/genus3`

- Compute larger class number examples - with Christelle Vincent
- Bounding primes appearing in the denominators of class polynomials- Lorenzo Garcia, Newton, Streng, ...
- Precision and complexity estimate - group project at WINE 2016.