Implementing the Genus 2 CM Method: Computing a Running Time

David Freeman* and Kristin Lauter

University of California, Berkeley and Microsoft Research

AMS Special Session on
Low Genus Curves and Applications
January 7, 2008

Outline

1. Introduction
   - Genus 2 Curves
   - Applications
2. Computing Igusa Class Polynomials
3. Analyzing the Complex-Analytic Method
   - Invariants and Modular Functions
   - Progress Towards a Bound

Genus 2 Curves and CM

- A genus 2 curve C (over a field of char $\neq 2$) is a curve of the form
$$y^2 = f(x)$$
where $\deg f = 5$ or 6 and f has no multiple roots.
- The Jacobian $J(C)$ of a genus 2 curve C is a 2-dimensional principally polarized abelian variety.
- We consider the case where $\mathrm{End}(J(C))$ is the ring of integers $\mathcal{O}_K$ of a (primitive) degree-4 CM field K.
  - $K = \mathbb{Q}(\sqrt{d})(\sqrt{-a + b\sqrt{d}})$.
  - We say $J(C)$ (or just C) has CM by $\mathcal{O}_K$.

Application: Group Orders of Abelian Surfaces over $\mathbb{F}_q$

- Let $J(C)$ be the Jacobian of a genus 2 curve C over $\mathbb{F}_q$ with CM by $\mathcal{O}_K$ (K a primitive quartic CM field).
- The Frobenius endomorphism π satisfies $f(\pi) = [0]$, where

$$f(x) = x^4 - sx^3 + tx^2 - sqx + q^2$$

  and $K \cong \mathbb{Q}[x]/(f(x))$.
- We can thus view π as an element of $\mathcal{O}_K$, and we have

$$\#J(C)(\mathbb{F}_q) = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1) = f(1).$$

- Conclusion: (curve $C/\mathbb{F}_q$ with CM by $\mathcal{O}_K$) + (Frobenius $\pi \in \mathcal{O}_K$) gives $\#J(C)(\mathbb{F}_q)$.
  - If K, q are fixed, π for a given C is easy to determine, even when q is large.

Application: Abelian Surfaces for Cryptography

- For cryptographic applications (e.g. Diffie-Hellman key exchange), we want $\#J(C)(\mathbb{F}_q)$ to be prime or almost-prime.
  - Naïve method: Choose random curves over $\mathbb{F}_q$ and count points — but genus 2 point counting is very slow!
  - Faster method: fix a CM curve in char 0, reduce modulo various q and use CM property to count points.
- Genus 2 curves for pairing-based cryptography (e.g. Boneh-Franklin IBE):
  - Random curves almost never have the desired properties, so we must use CM curves.
  - See recent work of F., F.-Stevenhagen-Streng.

Constructing CM Curves via Igusa Class Polynomials

- Recall: Igusa invariants of curves $C/\overline{\mathbb{Q}}$ with CM by $\mathcal{O}_K$ are roots of Igusa class polynomials for K.
- Equations for curves C can be computed easily from Igusa invariants.
- Reduction of curves in char 0 with CM by $\mathcal{O}_K$ gives full set of curves in char p with CM by $\mathcal{O}_K$.
- Problem of generating curves $C/\mathbb{F}_q$ whose Jacobians have a known number of points is reduced to computing Igusa class polynomials for K.

Three Known Methods

- Known methods for computing Hilbert class polynomials (genus 1) have all been generalized to genus 2.
- Complex-analytic method (Spallek, van Wamelen, Weng):
  - Igusa invariants are modular functions on a Siegel upper half-space.
  - Use Fourier expansions to evaluate functions to desired precision.
- Chinese Remainder Theorem method (Eisenträger-Lauter):
  - Test all genus 2 $C/\mathbb{F}_p$ to see which have CM by $\mathcal{O}_K$ (efficiently implemented by F.-Lauter).
  - Use Igusa invariants to construct class polynomials mod p.
  - Repeat modulo many small p, combine via CRT.
- p-adic (AGM) method (Gaudry et al):
  - Find all genus 2 $C/\mathbb{F}_{p^d}$ with CM by $\mathcal{O}_K$ (d small).
  - Compute the canonical lifts of C to desired p-adic precision.

When do we stop?

- All three methods give approximations to the Igusa class polynomials, computed to a prescribed precision.
- Igusa class polynomials have rational coefficients, so to compute the required precision we need to know
  1. An upper bound on the denominators of the coefficients. (CRT method also requires info on factorization of denominators.)
  2. An upper bound on the absolute values of the coefficients (equivalently, on the absolute values of the roots).
- Goren-Lauter have given a result for (1).
- A bound (2) comes from analysis of the complex-analytic method.
  (Work in progress with Lauter, Streng.)

j-Invariants as Modular Functions

- Recall that we can define an elliptic curve E as $\mathbb{C}/\Lambda$.
- We can write $\Lambda = \langle 1, \tau \rangle$ for some $\tau \in \mathcal{H}$, the upper half-plane.
- If E has CM by $\mathcal{O}_K$ then $\tau \in K$.
- The j-invariant is a modular function on $\mathcal{H}/\operatorname{PSL}_2(\mathbb{Z})$:

$$j(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + 744 + 196884q + \cdots .$$

($g_2 =$ Eisenstein series; $\Delta =$ cusp form; $q = e^{2\pi i \tau}$.)

- Analogous statements hold for abelian surfaces and Igusa invariants:

Igusa Invariants as Modular Functions

- An abelian surface $A = J(C)$ can be defined as $\mathbb{C}^2/\Lambda$.
- We can write $\Lambda = \langle Id, \tau \rangle$ for some period matrix $\tau \in \mathcal{H}^2$, the Siegel upper half-space:

$$\tau = \begin{pmatrix} \tau_1 & \epsilon \\ \epsilon & \tau_2 \end{pmatrix}, \quad \tau_1, \tau_2, \epsilon \in \mathbb{C}, \quad \text{Im}\,\tau \text{ positive-definite}$$

- The Igusa invariants of the associated curve C are modular functions on $\mathcal{H}^2 / \text{Sp}_2(\mathbb{Z})$:

$$i_i = 2 \cdot 3^5 \cdot \frac{\chi_{12}^5}{\chi_{10}^6}, \quad i_2 = \frac{3^3}{2^3} \cdot \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4}, \quad i_3 = \frac{3}{2^5} \cdot \frac{\psi_6 \chi_{12}^2}{\chi_{10}^3} + \frac{3^2}{2^3} \cdot \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4},$$

- ψ_4, ψ_6 are genus 2 Eisenstein series; χ_{10}, χ_{12} are cusp forms.

Bounding the Igusa Invariants

- Goal: compute an upper bound on $|i_1| = 2 \cdot 3^5 \cdot |\frac{\chi_{12}(\tau)^5}{\chi_{10}(\tau)^6}|$ in terms of numerical invariants of CM field K (e.g. discriminant).
- Ingredients:
  1. Upper and lower bounds on entries of τ in terms of invariants of K.
  2. Upper bound on χ_{12} in terms of entries of τ.
  3. Lower bound on χ_{10} in terms of entries of τ.

The Fundamental Domain

- Since Igusa invariants are modular functions, we can apply an element of the modular group $\mathrm{Sp}_2(\mathbb{Z})$ to move τ into a fundamental domain.
- Fundamental domain for $\tau = \left(\begin{smallmatrix} \tau_1 & \epsilon \\ \epsilon & \tau_2 \end{smallmatrix}\right)$ defined by 28 inequalities:

$$\begin{gathered} -1/2 \leq \mathrm{Re}\,\tau_1, \mathrm{Re}\,\tau_2, \mathrm{Re}\,\epsilon \leq 1/2 \\ \mathrm{Im}\,\tau_1 \geq \mathrm{Im}\,\tau_2 \geq 2|\mathrm{Im}\,\epsilon| \geq 0 \\ \text{19 more} \end{gathered}$$

- We've computed some bounds, but are missing upper bound on $\mathrm{Im}\,\tau_1$ and lower bound on $|\epsilon|$.
- Streng: alternatively, compute bounds by enumerating reduced quadratic forms corresponding to relative ideal classes of $\mathcal{O}_K/\mathcal{O}_{K^+}$. (Work in progress.)

Bounding the Modular Forms

- Looking for (asymptotic) upper bound on $|i_1| = 2 \cdot 3^5 \cdot |\frac{\chi_{12}(\tau)^5}{\chi_{10}(\tau)^6}|$.
- Need to bound modular forms $\chi_{12}(\tau)$ from above and $\chi_{10}(\tau)$ from below in terms of τ.
- Method 1: Use theta functions

$$\chi_{12} = (\vartheta_0\vartheta_1\vartheta_2\vartheta_4\vartheta_8\vartheta_{15})^4 + (\vartheta_0\vartheta_1\vartheta_2\vartheta_6\vartheta_9\vartheta_{12})^4 + 13 \text{ more}$$

  - Theta functions are simple modular forms; easier to bound in terms of input (from above and below).
  - Dupont, Streng: achieved rigorous upper and lower bounds; Streng currently working on improving them.

Bounding the Modular Functions

- Method 2: Use Fourier series

$$\chi_{12}(\tau) = \sum_N A_N e^{2\pi i \operatorname{Tr} N\tau}$$

($N =$ pos. def. sym. half-integer matrices; A_N = Fourier coefficients)

  - Leading terms of Fourier series dominate as $\operatorname{Im}\tau$ gets large.

$$\chi_{12}(\tau) \approx (5 + 10(e^{2\pi i \tau_1} + e^{2\pi i \tau_2}) \cos 4\pi\epsilon + \cos 2\pi\epsilon)/6$$

  - Experimentally, leading terms provide very good estimate of actual value of Igusa invariants.
  - Not yet achieved rigorous asymptotic results.
  - Can method be used to give lower bounds?

The (Expected) Result

- Our analysis gives:
  - $\log|i_1|$, $\log|i_2|$, and $\log|i_3|$ are $\tilde{O}(\Delta)$ ($\Delta =$ discriminant of K).
  - This result $+$ Goren-Lauter bounds on denominators $\Rightarrow$ Igusa class polynomials can be computed in time $\tilde{O}(h^3\Delta^2)$ ($h =$ class number of K).
  - Equivalently, Igusa class polynomials can be computed in time $\tilde{O}(\Delta^{7/2})$.
- Compare with $\tilde{O}(\Delta)$ for Hilbert class polynomials.
- Bounds on the denominators are the biggest obstacle to improving the bound. (See next talk!)