Computing Siegel modular forms

Kristin Lauter

Microsoft Research

Women in SAGE project
July 16, 2012

Loss of precision in floating point computation

Multiplication of real numbers approximated through truncation

Let α_t be a truncation of α such that $\alpha - \alpha_t < 10^{-t}$.

Same for β_t.

What about $\alpha\beta - \alpha_t\beta_t$?

Example: $\beta = 10$, $\alpha = 0.859$

Compute with 2 digits of precision, $t = 2$

Result: lose one digit of precision in the product.

Evaluating the j-function at a CM point

$q = exp(2 * Pi * I * (1 + (-163)^{0.5})/2)$

$-3.8089809370076523382262315 15E^{-18} + 5.192218628E^{-45} * I$

$1/q + 744 + 196884 * q$

$=$

$-262537412640768000.0000000001 - 0.0000000003578783058 * I$

$\text{round}(\text{real}(\ )) = -262537412640768000 = -2^{18} * (3 * 5 * 23 * 29)^3$

Product expansion

Using the Dedekind η-function $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$,

$$j(z) = \left(\frac{(\eta(z/2)/\eta(z))^{24} + 16}{(\eta(z/2)/\eta(z))^{8}}\right)^3.$$

The sparsity of the q-expansion of the η-function makes it very efficient for explicit computations.

The Siegel moduli space

The Siegel moduli space $\mathcal{A}_2$ parameterizes abelian surfaces with principal polarization.

Let $\mathrm{Sp}_2(\mathbb{Z})$ be the symplectic group over $\mathbb{Z}$ of genus two, consisting of 4×4-integral matrices M satisfying

$$MJM^t = J, \quad J = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$$

where I_2 is the identity matrix of order 2. Let

$$\mathbb{H}_2 = \{\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in M_2(\mathbb{C}) : \Im\tau > 0\}$$

be the Siegel upper half-plane of genus two, and let

$$X_2 = \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$$

be the open Siegel modular 3-fold.

The Siegel moduli space

Here $\mathrm{Sp}_2(\mathbb{Z})$ acts on $\mathbb{H}_2$ via

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \tau = (A\tau + B)(C\tau + D)^{-1}.$$

For a given CM field K we can give explicit representatives for all the CM points on $\mathcal{A}_2(\mathbb{C})$:

$$\{\tau : \ \mathbb{C}^2/\langle \mathrm{I}_2 \ \tau \rangle \text{ has CM by } \mathcal{O}_K\}/\mathrm{Sp}_4(\mathbb{Z})$$

Siegel modular functions

A holomorphic function $f : \mathbb{H}_2 \to \mathbf{C}$ is called a *Siegel modular form* of weight $w \geq 0$ if it satisfies

$$f(\begin{pmatrix} A & B \\ C & D \end{pmatrix}\tau) = \det(C\tau + D)^w f(\tau)$$

for all τ and all matrices in the subgroup $\mathrm{Sp}_4(\mathbf{Z}) \subset \mathrm{Sp}_4(\mathbf{R})$. The integer w is called the *weight* of the form f.

Theta functions

$$\theta[\epsilon_1\epsilon_2](z,\tau) = \sum_{n\in\mathbf{Z}^g} \exp(\pi i(n+\epsilon_1/2)\tau^t(n+\epsilon_1/2)+2\pi i(n+\epsilon_1/2)^t(z+\epsilon_2/2)$$

Thetanullwerte when $z = 0$

The even theta characteristics are those such that $\epsilon_1 \cdot^t \epsilon_2 \equiv 0 \pmod 2$

Eisenstein series

For $w \geq 4$ even, Eisenstein series E_w defined by

$$E_w(\tau) = \sum_{c,d} (c\tau + d)^{-w}$$

The sum ranges over all co-prime symmetric 2×2-integer matrices c, d that are non-associated with respect to left-multiplication by $\mathrm{GL}(2, \mathbf{Z})$.

Fourier expansion

Any Siegel modular form f admits a Fourier expansion

$$f(\tau) = \sum_{T} a(T) \exp(2\pi i \operatorname{Tr}(T\tau)) \tag{1.3}$$

where T ranges over certain 2×2-matrices with coefficients in $\frac{1}{2}\mathbf{Z}$.

Truncate the sum in (1.3) to only include matrices with trace below some bound.

Eichler-Zagier

Theorem. Let $T = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in \mathrm{Mat}(\frac{1}{2}\mathbf{Z})$ be a positive semi-definite matrix with integer entries on the diagonal. Write $D = b^2 - 4ac \leq 0$ and let D_0 be the discriminant of $\mathbb{Q}(\sqrt{D})$. Then the Fourier coefficient $a(T)$ equals 1 for $a = b = c = 0$ and

$$\frac{-2w}{B_w} \sum_{d \mid \gcd(a,b,c)} d^{w-1} c(D/d^2)$$

otherwise. Here, B_k is the kth Bernoulli number and c is defined by $c(0) = 1$ and

$$c(D') = \frac{1}{\zeta(3-2w)} L_{D_0}(2-w) \sum_{d|f} \mu(d) \left(\frac{D_0}{d}\right) d^{w-2} \sigma_{2w-3}(f/d)$$

where $D_0 f^2 = D'$, ζ denotes the Dedekind ζ-function, L_{D_0} is the quadratic Dirichlet L-series, μ is the Mobius function, $\sigma_n(x)$ is the sum of the nth powers of the divisors of x.

CM points on the moduli space

K = quartic primitive CM field.

A curve C over $\mathbb{C}$ *has CM* by $\mathcal{O}_K$ if $\mathcal{O}_K$ embeds in the endomorphism ring of $\mathrm{Jac}(C)$.

CM points on the moduli space of principally polarized abelian surfaces correspond to isomorphism classes of CM curves.

Absolute Igusa invariants

Igusa gave 3 Siegel modular functions h_1, h_2, h_3, the absolute Igusa invariants.

$$h_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6},$$

$$h_2 = \frac{3^3}{2^3} \frac{E_4 \chi_{12}^3}{\chi_{10}^4},$$

$$h_3 = \frac{3}{2^5} \left(\frac{E_6 \chi_{12}^2}{\chi_{10}^3} + 2^2 \cdot 3 \frac{E_4 \chi_{12}^3}{\chi_{10}^4} \right).$$

$$\chi_{10} = -43867 \cdot 2^{-12} \cdot 3^{-5} \cdot 5^{-2} \cdot 7^{-1} \cdot 53^{-1}(E_4 E_6 - E_{10})$$

$$\chi_{12} = 131{\cdot}593{\cdot}2^{-13}{\cdot}3^{-7}{\cdot}5^{-3}{\cdot}7^{-2}{\cdot}337^{-1}(3^2{\cdot}7^2 E_4^3 + 2{\cdot}5^3 E_4^6 - 691 E_{12}),$$

Igusa class polynomials

Definition

The Igusa class polynomials

$$H_i(x) = \prod_{\frac{\{\tau :\, \mathbb{C}^2/\langle \mathrm{I}_2\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \qquad i = 1, 2, 3.$$

Constructing genus 2 curves for cryptography

C smooth, projective, irreducible genus 2 curve over $\mathbb{F}_p$.

$J(C)$ the Jacobian variety.

$J(C)(\mathbb{F}_p)$ can be used in cryptography as the group with a hard Discrete Log Problem (DLP) if the group has a subgroup of large prime order (roughly size p^2)

Advantage: p of size 2^{128} instead of 2^{256} as for elliptic curves.

Applications: key exchange, digital signatures, encryption, ...

Challenge:

Generate $C/\mathbb{F}_q$ with $\#J(C)(\mathbb{F}_q) = N$, N a large prime.

Strategy: Construct curves with a known order using complex multiplication (CM) techniques.

1. Given $N_1 = \#C(\mathbb{F}_q)$ and $N_2 = \#C(\mathbb{F}_{q^2})$ $\mathbb{F}_p$, this determines a quartic CM number field K by the characteristic polynomial of Frobenius.

2. Compute "modular invariants" associated to the field K.

3. Reconstruct the curve from its invariants via Mestre's algorithm.

Computing the CM field K

For an ordinary genus 2 curve C over a prime field $\mathbb{F}_q$, let $N_1 = \#C(\mathbb{F}_q)$ and $N_2 = \#C(\mathbb{F}_{q^2})$. Then

$$\#J(C)(\mathbb{F}_q) = (N_1^2 + N_2)/2 - q. \tag{1}$$

Set

$$s_1 := q + 1 - N_1$$

and

$$s_2 := \frac{1}{2}\left(s_1^2 + N_2 - 1 - q^2\right).$$

Then the quartic polynomial satisfied by the Frobenius endomorphism of the Jacobian is $f(t) = t^4 - s_1 t^3 + s_2 t^2 - q s_1 t + q^2$.

Thus the Jacobian of the curve has endomorphism ring equal to an order in the quartic CM field $K = \mathbb{Q}[t]/(f(t))$.