Humbert Surfaces and Isogeny Relations

David Gruenewald

davidg@maths.usyd.edu.au

The University of Sydney $\cdots \longrightarrow$ eRISCS, Université de la Méditerranée

AGCT 2009

The Siegel upper half plane

Definition

The Siegel upper half plane of degree g is

$$\mathbb{H}_g = \{\tau \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \mid {}^t\tau = \tau \ , \quad \mathrm{Im}\,(\tau) > 0\}\,.$$

- Each $\tau \in \mathbb{H}_g$ corresponds to a PPAV $A_\tau/\mathbb{C}$ with period matrix $(\tau\ I_g) \in \mathrm{Mat}_{g\times 2g}(\mathbb{C})$.
- $A_\tau \cong A_{\tau'} \Leftrightarrow \exists M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $\tau' = M \cdot \tau := (a\tau + b)(c\tau + d)^{-1}$.
- $\mathcal{A}_g = \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ is a moduli space for dimension g PPAV's.
- $\dim \mathcal{A}_g = \frac{1}{2}g(g+1)$. In particular, $\dim \mathcal{A}_2 = 3$ and $\mathcal{A}_2$ is called the Siegel modular threefold.

Extra endomorphisms

Let A be a PPAS ($g = 2$). Then $\mathrm{End}(A)$ is an order in $\mathrm{End}(A) \otimes \mathbb{Q}$ which isomorphic to one of the following algebras:

(0) quartic CM field

(1) indefinite quaternion algebra over $\mathbb{Q}$

(2) real quadratic field

(3) $\mathbb{Q}$

The irreducible components of the corresponding moduli spaces in $\mathcal{A}_2$ which have "extra endomorphisms" are known as

(0) CM points

(1) Shimura curves

(2) Humbert surfaces

Humbert's equation

Humbert showed that any $\begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathcal{A}_2$ satisfying the equation

$$k\tau_1 + \ell\tau_2 - \tau_3 = 0$$

defines a Humbert surface H_Δ of discriminant $\Delta = 4k + \ell > 0$.

Example

$H_1 = \mathrm{Sp}_4(\mathbb{Z}) \backslash \left\{ \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_3 \end{pmatrix} \right\} = \mathrm{Sp}_4(\mathbb{Z}) \backslash \left\{ \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_3 \end{pmatrix} \right\}$, the set of abelian varieties which split as a product of elliptic curves.

Task: Find "useful" algebraic models for H_Δ.

Algebraic models

- The function field of $\mathcal{A}_2$ (and hence $\mathcal{M}_2$) is $\mathbb{C}(j_1, j_2, j_3)$ where j_i are the absolute Igusa invariants.
- There exists an irreducible polynomial $H_\Delta(j_1, j_2, j_3)$ whose zero set is the Humbert surface of discriminant Δ.

Unfortunately, working with j_i is impractical (enormous degrees, giant coefficients).
Solution: add some level structure.

Algebraic models

Consider theta functions of half integral (even) characteristics

$$\theta \begin{bmatrix} m' \\ m'' \end{bmatrix} (\tau) = \sum_{x \in \mathbb{Z}^2} e^{2\pi i \left(\frac{1}{2}(x+\frac{m'}{2}) \cdot \tau \cdot {}^t(x+\frac{m'}{2}) + (x+\frac{m'}{2}) \cdot {}^t(\frac{m''}{2}) \right)}$$

where $m', m'' \in \mathbb{Z}^2/2\mathbb{Z}^2$ satisfy $m' \cdot {}^t m'' = 0 \pmod 2$.
The quotients $\theta[{}^{m'}_{m''}]/\theta[{}^{n'}_{n''}]$ are modular functions for $\Gamma(4,8)$ where

$$\Gamma(4,8) = \{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(4) \mid (\alpha\, {}^t\beta)_0 \equiv (\gamma\, {}^t\delta)_0 \equiv 0 \pmod 8 \} \supset \Gamma(8)$$

They are useful "building blocks" for constructing modular forms and functions with less level structure.
For example, $j_1 = I_2^5/I_{10}, \quad j_2 = I_2^3 I_4/I_{10}, \quad j_3 = I_2^2 I_6/I_{10}$ where

$$I_{10} = \prod_{\text{even}} \theta \begin{bmatrix} m' \\ m'' \end{bmatrix}^2 .$$

Runge's model

Runge uses level $\Gamma^*(2,4)$-structure, with four theta functions:

$$f_a = \theta \begin{bmatrix} a \\ (0,0) \end{bmatrix} (2\tau),\ a \in \mathbb{Z}^2/2\mathbb{Z}^2$$

The homogeneous coordinate ring for $\mathcal{A}_2^*(2,4) = \Gamma^*(2,4)\backslash\mathbb{H}_2$ is rational, generated by the four functions $\{f_a\}$.

For convenience, set

$$\begin{aligned} t_0 &= f_{(0,0)} \\ t_1 &= f_{(0,1)} \\ t_2 &= f_{(1,0)} \\ t_3 &= f_{(1,1)}. \end{aligned}$$

Runge's method

Let $\phi : \mathcal{A}' \to \mathcal{A}_2$ be a finite cover of $\mathcal{A}_2$. Then

$$\phi^{-1} H_\Delta = \bigcup_{\text{finite}} H_\Delta^{(i)} .$$

Given functions $\{f_i(\tau)\}_{i=1,\ldots,n}$ generating the function field of $\mathcal{A}'$, compute $H_\Delta^{(i)}(f_1, \ldots, f_n)$ as follows:

1. Calculate the degree of the Humbert components $H_\Delta^{(i)}$ (using a formula of van der Geer '82).
2. Compute power series representations of the $f_i(\tau)$ restricted to $H_\Delta \subset \mathbb{H}_2$.
3. Solve $H_\Delta^{(i)}(f_1, \ldots, f_n) = 0$ in the power series ring (truncated series with large precision) using linear algebra.

Step 1 - degree formula (Runge's model)

Fortunately much arithmetic-geometric information is known about Humbert surfaces (van der Geer '82). The number of Humbert components in $\mathcal{A}_2^*(2,4)$ is

$$m(\Delta) = \begin{cases} 10 & \text{if } \Delta \equiv 1 \bmod 8 \\ 60 & \text{if } \Delta \equiv 0 \bmod 4 \\ 6 & \text{if } \Delta \equiv 5 \bmod 8 \end{cases}$$

(see Runge '99).
Here are the degrees for small discriminants:

Δ	1	4	5	8	9	12	13	16	17	20	21	24	25
$\deg(H_\Delta^{(i)})$	2	1	8	2	24	4	40	8	48	8	80	12	120

Step 2 - power series

Write $\Delta = 4k + \ell$ where ℓ is either 0 or 1, and k is uniquely determined. The Humbert surface of discriminant Δ can be defined by the set

$$H_\Delta = \mathrm{Sp}_4(\mathbb{Z}) \backslash \left\{ \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & k\tau_1 + \ell\tau_2 \end{pmatrix} \in \mathbb{H}_2 \right\}.$$

Restrict $\theta\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to H_Δ to get a Laurent series

$$\theta\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right](\tau) = \sum_{(x_1,x_2)\in\mathbb{Z}^2} e^{\pi i(x_1 c + x_2 d)} r^{(2x_1+a)^2 + k(2x_2+b)^2} q^{2(2x_1+a)(2x_2+b) + \ell(2x_2+b)^2}$$

where $r = e^{2\pi i \tau_1/8}$ and $q = e^{2\pi i \tau_2/8}$.

Unfortunately q has negative exponents. Substitute $r = pq$ to get

$$\sum_{(x_1,x_2)\in\mathbb{Z}^2} (-1)^{x_1c+x_2d} p^{(2x_1+a)^2+k(2x_2+b)^2} q^{(2x_1+a+2x_2+b)^2+(k+\ell-1)(2x_2+b)^2}$$

which is a power series with integer coefficients.

Using this representation we can compute the restriction of theta functions (hence modular forms and functions) to a Humbert surface as elements of $\mathbb{Z}[[p,q]]/(p^N, q^N)$.

Step 3 - linear algebra (Runge's model)

Let $d = \deg(H_\Delta^{(i)})$. To find the algebraic relation $H_\Delta^{(i)}$:

- Compute all homogeneous monomials of degree d in the variables $t_0, \ldots, t_3$.
- Substitute $t_i = t_i(p, q) \in \mathbb{Z}[[p, q]]/(p^N, q^N)$ in each monomial.
- Use linear algebra to find linear dependencies between the power series monomials $p^m q^n$ (compute null space of a big matrix).

With high enough precision there will be exactly one linear relation between the monomials t_i. This produces the polynomial relation $H_\Delta^{(i)}(t_0, t_1, t_2, t_3) = 0$ which defines a Humbert component.

Part II: Improving CRT method for computing Igusa class polynomials

Using:

- Humbert surfaces
- (p, p)-isogeny relations $(p = 3)$. Joint work with Reinier Bröker and Kristin Lauter.

Igusa class polynomials

Notation: $K =$ primitive quartic CM field with Galois closure L,
$\Phi = \{\varphi_1, \varphi_2\}$ and Φ' are CM types,
$K_{\Phi'} \cong K_\Phi$ is the reflex field.

For an ideal $I \subseteq \mathcal{O}_K$, the quotient $A_I = \mathbb{C}^2/\Phi(I^{-1})$ is an abelian variety of dimension 2. It has endomorphism ring $\mathcal{O}_K$.

Fact: *We can choose I such that A_I is principally polarized.*

Theorem (weak version): *The field $K_\Phi(j_1(A_I), j_2(A_I), j_3(A_I))$ is a subfield of the Hilbert class field of K_Φ. The polynomial*

$$P_K = \prod_{\{[A/\mathbb{C}] \,|\, \mathrm{End}(A) \cong \mathcal{O}_K\}} (X - j_1(A))$$

has rational coefficients. Similarly for the polynomials Q_K, R_K giving the j_2 and j_3-invariants.

Igusa class polynomials mod q

Let q be a rational prime which splits completely into principal ideals in K_Φ. Then P_K, Q_K, R_K split completely over $\mathbb{F}_q$, so we can compute the Igusa class polynomials mod q by finding all $(j_1, j_2, j_3) \in \mathbb{F}_q^3$ having CM by $\mathcal{O}_K$:

1. Construct a genus 2 curve C with invariants $(j_1, j_2, j_3) \in \mathbb{F}_q^3$ using Mestre's algorithm.
2. Compute its Weil polynomial (point counting) $w_C(X) = X^4 - tX^3 + sX^2 - tqX + q^2$.
3. If $\mathbb{Q}[X]/w_C(X)$ is isomorphic to K (easy), determine whether $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$ using the algorithm of Freeman and Lauter (hard).

The runtime is dominated by the size of the search space $\mathbb{F}_q^3$.

An improvement using Humbert equations

The CM points lie on the Humbert surface of discriminant $\Delta(K^+)$ where K^+ is the real quadratic subfield.

$\Rightarrow$ the search space is reduced to $H_{\Delta(K^+)}(\mathbb{F}_q)$ which has size $O(q^2)$.

Remark: In his thesis, P. Gaudry has some ideas for improving point counting on such "RM curves" of genus 2 which could be potentially used to speed up the Weil polynomial calculation. See his ECC 2007 talk slides for details.

Improvement using the Galois action

The Galois action on the CM moduli is given by isogenies.
Any $\mathcal{O}_K$-ideal $\mathfrak{a}$ naturally acts on A_I via

$$\mathbb{C}^2/\Phi(I^{-1}) \longrightarrow \mathbb{C}^2/\Phi(\mathfrak{a}I^{-1}).$$

The right hand side has a principal polarization if and only if $\mathfrak{a}$ lies in the kernel of

$$\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}^+(K^+).$$

Writing $\mathfrak{a}\overline{\mathfrak{a}} = \alpha > 0$, the polarization changes from ξ to $\xi\alpha$.
The group $\mathfrak{C}(K)$ consisting of isomorphism classes of pairs $(\mathfrak{a}, \alpha)$ naturally acts on the PPAS's that have CM by $\mathcal{O}_K$. It fits in an exact sequence

$$1 \longrightarrow \overbrace{(\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*)}^{\text{order 1 or 2}} \longrightarrow \mathfrak{C}(K)$$

$$\longrightarrow \mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}^+(K^+) \longrightarrow 1.$$

The Galois action

$\mathrm{Gal}(H(K_\Phi)/K_\Phi) \overset{\text{Artin}}{\cong} \mathrm{Cl}(\mathcal{O}_{K_\Phi})$ acts on $\mathfrak{C}(K)$ via the map

$$\begin{array}{rcl} m : \mathcal{O}_{K_\Phi} & \to & \mathfrak{C}(K) \quad \text{given by} \\ \mathfrak{p} & \mapsto & \left(N_\Phi(\mathfrak{p}), N_{K_\Phi/\mathbb{Q}}(\mathfrak{p})\right) \end{array}$$

where $N_\Phi(\mathfrak{p}) := \mathfrak{p}^{\varphi_1}\mathfrak{p}^{\varphi_2}$ is the typenorm.
Suppose $\mathfrak{p} \subset \mathcal{O}_{K_\Phi}$ has norm p. Then $N_\Phi(\mathfrak{p}) \mid (p) \subset \mathcal{O}_K$ and we get a 2-dimensional $\mathbb{F}_p$-vector subspace

$$V = \{P \in A_I \mid \forall \alpha \in N_\Phi(\mathfrak{p}) : \alpha(P) = 0\} \subset A[p]$$

which is Weil-isotropic. The ideal $\mathfrak{p} \in \mathcal{O}_{K_\Phi}$ acts on A_I via a (p,p)-isogeny

$$A_I \mapsto A_I/V.$$

Task: Find (p,p)-isogeny relations!

(p,p)-correspondences

We would like to construct a defining ideal for $Y_0^{(2)}(p) \subset \mathcal{A}_2 \times \mathcal{A}_2$ which parametrizes PPAS's with a (p,p)-isogeny to another PPAS. Write $I_p :=$ ideal generated by all algebraic relations between

$$\{j_1(\tau), j_2(\tau), j_3(\tau), j_1(p\tau), j_2(p\tau), j_3(p\tau)\}.$$

- $p = 2$ was computed by R. Dupont. It is huge; it takes 50 megabytes to store it.
- $p > 2$ has not yet been computed.

Idea: *Use smaller functions to get something reasonable.*

Add some level structure!

Using Fourier expansions of Runge's theta functions, we can search for relations between $\{t_i(\tau)\}$ and $\{t_i(p\tau)\}$. The full relation ideal I_p^t defines (the Satake compactification of) the moduli space

$$Y(t;p) = \{(A, L, G) |\, (A, L) \in \mathcal{A}_2^*(2, 4),\ G \subset A[p] \text{ iso., } \dim G = 2\}.$$

Let $p \neq 2$ be prime. A (p, p)-isogeny $A \to A'$ induces an isomorphism $A[4] \xrightarrow{\sim} A'[4]$. Thus on $\mathcal{A}_2^*(2, 4)$, we get a natural map ("lift")

$$(A, L) \to (A', L')$$

for every (p, p)-isogeny.

The defining ideal I_3^t has 85 homogeneous degree 6 polynomials (G. '06). It takes only 35Kb to store it and the coefficients are 8-smooth!

Example

Put $K = \mathbb{Q}[X]/(X^4 + 22X^2 + 73)$. We have that:

- $\mathrm{Gal}(L/\mathbb{Q}) = D_4$.
- $K_\Phi = \mathbb{Q}[X]/(X^4 + 11X^2 + 12)$.
- $K^+ = \mathbb{Q}(\sqrt{3})$.
- $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/4\mathbb{Z}$.
- $\mathrm{Gal}(H(K_\Phi)/K_\Phi) \cong \mathrm{Cl}(\mathcal{O}_{K_\Phi}) \cong \mathbb{Z}/4\mathbb{Z}$.
- $(3) = \mathfrak{q}_1^2\mathfrak{q}_2^2$ in $\mathcal{O}_K$.
- $(3) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ in $\mathcal{O}_{K_\Phi}$, each $\mathfrak{p}_i$ has norm 3.

The images under the typenorm N_Φ are given by

$$\begin{aligned} N_\Phi(\mathfrak{p}_1) &= \mathfrak{q}_1^2 \\ N_\Phi(\mathfrak{p}_2) &= \mathfrak{q}_2^2 \\ N_\Phi(\mathfrak{p}_3) &= \mathfrak{q}_1\mathfrak{q}_2. \end{aligned}$$

These yield three distinct $(3,3)$-isogenies.

Example

The prime $q = 1609$ splits as $\pi_1\pi_2\pi_3\pi_4$ in $\mathcal{O}_{K_\Phi}$. It splits completely in $H(K_\Phi)$.

Bounds on the denonimators (Lauter, Goren) yield that 1609 does not divide the denominators of P_K, Q_K, R_K.

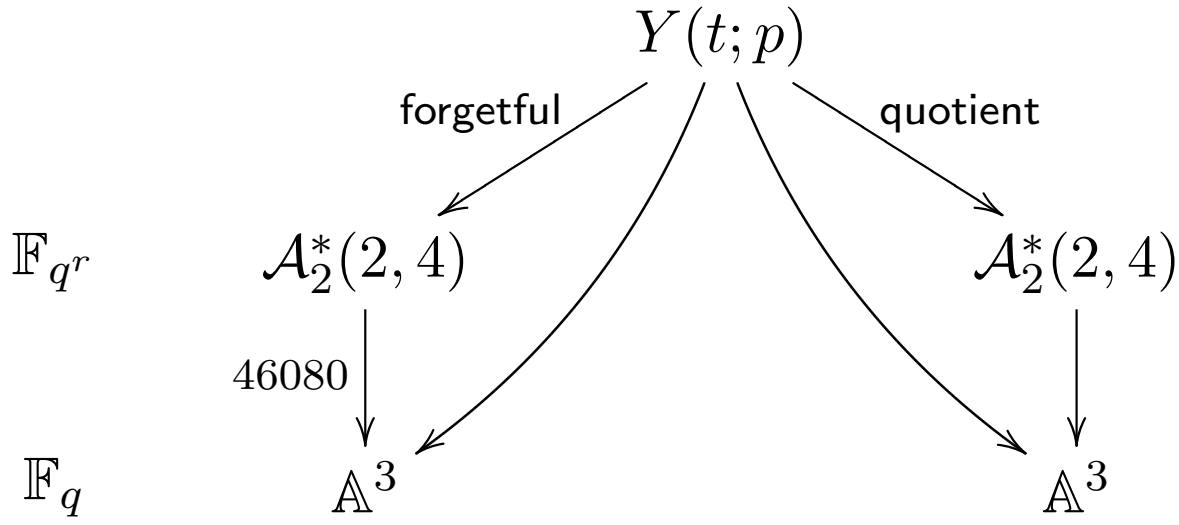
$\Rightarrow$ the polynomials P_K, Q_K, R_K factor completely modulo q.

A random search over $(j_1, j_2, j_3) \in \mathbb{F}_q^3$ with the aid of the Humbert surface H_{12} yields an abelian surface $A/\mathbb{F}_q$ with

$$(j_1(A), j_2(A), j_3(A)) = (1563, 789, 704)$$

has endomorphism ring $\mathcal{O}_K$.

Example



- Choose a point $(w,x,y,z) \in \mathbb{F}_{q^r}$ lying over $(j_1,j_2,j_3) = (1563, 789, 704) \in \mathbb{F}_q^3$. In fact $\mathbf{r \leq 24}$.
- Specializing the ideal I_3^t in w,x,y,z yields a system of equations in 4 variables over $\mathbb{F}_{q^r}$.
- It has 40 solutions over $\overline{\mathbb{F}_q}$ (= number of (p,p) Weil-isotropic subgroups $= \frac{p^3-1}{p-1}$ when $p=3$). We only require the solutions over $\mathbb{F}_{q^r}$ (= field of definition for the level structure).

Example

Map all 'Runge-tuples' down to Igusa triples. Over $\mathbb{F}_q$ we find

$$(1563, 789, 704), (587, 1085, 931),$$

$$(961, 509, 36), (1396, 1200, 1520),$$

$$(1350, 1316, 1483), (1310, 1550, 449), (1442, 671, 281).$$

Some of these triples are invariants of PPAS's with endomorphism ring $\mathcal{O}_K$, some are not.

We run an 'endomorphism ring check' to decide which ones are roots of $P_K, Q_K, R_K \in \mathbb{F}_q[X]$.

Example

We compute

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathfrak{C}(K) \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

A close examination yields $\mathfrak{C}(K) \cong \mathbb{Z}/4\mathbb{Z} = \langle g \rangle$.
Under this identification, we have

$$m(\mathfrak{p}_1) = g, \quad m(\mathfrak{p}_2) = g^{-1}, \quad m(\mathfrak{p}_3) = 1.$$

The ideal $\mathfrak{p}_3$ explains why we got the original point $(1563, 789, 704)$ back when we looked at all $(3, 3)$-isogenous varieties.

The other 2 ideals yield elements of order 4 in $\mathfrak{C}(K)$.
Note: Under the typenorm map to $\mathrm{Cl}(\mathcal{O}_K)$ they have order 2.

Example

We compute

$$(1563, 789, 704) \xrightarrow{\mathfrak{p}_1} (1396, 1200, 1520) \xrightarrow{\mathfrak{p}_1}$$

$$(1276, 1484, 7) \xrightarrow{\mathfrak{p}_1} (1350, 1316, 1483) \xrightarrow{\mathfrak{p}_1}$$

$$\xrightarrow{\mathfrak{p}_1} (1563, 789, 704).$$

The polynomial $(X - 1563) \cdot \ldots \cdot (X - 1350) \in \mathbb{F}_q[X]$ divides the degree 8 polynomial P_K.
To find the other degree 4 factor, we do a 2nd random search. In the end, we compute

$$P_K = X^8 + 455X^7 + 410X^6 + 259X^5 + 323X^4$$

$$+153X^3 + 289X^2 + 942X + 416 \mod 1609.$$

Summary

Our approach works in general, there is no assumption on K.

Right now, we can only compute the CM-action for ideals of norm 2 and norm 3. The norm 5 ideals are computationally out of reach: it is too hard to compute I_5^t.

The map $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$ need not be surjective. This means we have to do several random searches.

Future research:

- Can we efficiently compute I_p^g for primes $p \geq 5$ using modular forms $\{g_i\}$ which have a different level structure?
- Understanding the (p,p)-isogeny graph structure better would speed up the algorithm (some endomorphism ring information is encoded in the graph).