Humbert Surfaces and Applications

David Gruenewald

davidg@maths.usyd.edu.au

eRISCS-ÉSIL, Université de la Méditerranée

Réunion CHIC, 6th October 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 $\theta\left[{m' \atop m''}\right]/\theta\left[{n' \atop n''}\right]$ are modular functions for $\Gamma(4,8)$ where

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

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

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

Algebraic models

Runge's model

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

$$f_a = \theta \left[\begin{array}{c} a \\ (0,0) \end{array} \right] (2\tau), \; a \in \mathbb{Z}^2/2\mathbb{Z}^2$$

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

Algebraic models

Rosenhain model

A choice of $\Gamma(2)$-structure is given by three functions

$$\begin{aligned}
\lambda_1(\tau) &= \left(\frac{\theta\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right]}\right)^2 \ ,\\
\lambda_2(\tau) &= \left(\frac{\theta\left[\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]}\right)^2 \ ,\\
\lambda_3(\tau) &= \left(\frac{\theta\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right]\theta\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]}\right)^2
\end{aligned}$$

called Rosenhain invariants. These generate the function field of $\mathcal{A}_2(2) = \Gamma(2)\backslash\mathbb{H}_2$.

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 (Rosenhain model)

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

$$m(\Delta) = \begin{cases} 10 & \text{if } \Delta \equiv 1 \bmod 8 \\ 15 & \text{if } \Delta \equiv 0 \bmod 4 \\ 6 & \text{if } \Delta \equiv 5 \bmod 8 \end{cases}$$

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

Δ	1	4	5	8	9	12	13	16	17	20	21	24
$\deg(H_\Delta^{(i)})$	1	2	8	8	16	16	40	24	48	32	80	48

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

Rosenhain model

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

- Compute all monomials of degree $\leq d$ in the variables e_1, e_2, e_3.
- Substitute $e_i = \lambda_i(p, q) \in \mathbb{Z}[[p, q]]/(p^N, q^N)$ 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 e_i. This produces the polynomial relation $H_{\Delta}^{(i)}(e_1, e_2, e_3) = 0$ which defines a Humbert component.
- Once one component has been determined, the others can easily be found by looking at the Rosenhain (S_6) orbit of a component.

Runtime analysis

- There are:
  - $\binom{d+3}{3} = O(d^3)$ monomials to be evaluated
  - $O(N^2)$ coefficients of evaluated power series expressions of precision N.
- Runtime cost is dominated by the nullspace calculation: $O(d^6N^2) \geq O(d^9)$ to find a unique solution.
- Symmetries of the equation (arising from the fixed group of the humbert component) can be exploited to reduce the matrix size by a constant factor, giving a speedup by a constant factor.
- Not overly efficient, but least it's only a one time calculation..

Example

We calculate a component of H_5:

$$
\begin{aligned}
\lambda_1 &= 1 + 16p^4q^8 + O(p^{12}q^{12}) \\
\lambda_2 &= 1 + 4q^4 + 8q^8 - 8p^4q^4 - 24p^4q^8 + 4p^8q^8 + 48p^8q^8 + O(p^{12}q^{12}) \\
\lambda_3 &= 1 + 4q^4 + 8q^8 + 8p^4q^4 + 40p^4q^8 + 4p^8q^8 + 48p^8q^8 + O(p^{12}q^{12})
\end{aligned}
$$

Using power series with precision 65, we compute the Humbert component

$$
\begin{aligned}
&e_2^2e_3^2 - 2e_2^2e_3^3 + e_2^2e_3^4 + 2e_1e_2e_3^3 - 2e_1e_2e_3^4 - 2e_1e_2^2e_3 - 2e_1e_2^2e_3^2 + 4e_1e_2^2e_3^3 + 2e_1e_2^3e_3 \\
&\quad -2e_1e_2^3e_3^3 + e_1^2e_3^4 - 2e_1^2e_2e_3^3 + e_1^2e_2^2 + 4e_1^2e_2^2e_3 - 4e_1^2e_2^2e_3^2 - 2e_1^2e_2^3 - 2e_1^2e_2^3e_3 \\
&\quad +4e_1^2e_2^3e_3^2 + e_1^2e_2^4 - 2e_1^2e_2^4e_3 + e_1^2e_2^4e_3^2 - 2e_1^3e_3^3 - 2e_1^3e_2e_3 + 4e_1^3e_2e_3^2 + 2e_1^3e_2e_3^3 \\
&\quad -2e_1^3e_2^2e_3^2 + 2e_1^3e_2^3e_3 - 2e_1^3e_2^3e_3^2 + e_1^4e_3^2 - 2e_1^4e_2e_3^2 + e_1^4e_2^2e_3^2
\end{aligned}
$$

Part II: Applications and further directions

Endomorphism ring application

Let J be a genus 2 Jacobian defined over $\mathbb{F}_p$ and write $K = \mathbb{Q}(\pi)$ where π is the Frobenius endomorphism. We have

$$\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K$$

The complexity of standard algorithm for computing $\mathrm{End}(J)$ is determined by the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] = \prod \ell_i^{e_i}$.

Computing $\mathrm{End}(J)$ relies on computing a basis for $J[\ell_i^{e_i}]$ over its splitting field. Expensive!
But if we know that J has real multiplication by $\mathcal{O}_{K^+}$ where K^+ is the real quadratic subfield, then

$$\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_{K^+}[\pi, \overline{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K$$

and the index $[\mathcal{O}_K : \mathcal{O}_{K^+}[\pi, \overline{\pi}]]$ can be smaller.

GLV using real multiplication

If $\sqrt{d} \in \mathrm{End}(J)$ is explicit and efficient then we can use GLV methods for families of hyperelliptic curves having RM.

Basic idea of GLV:

- Let G be a cyclic subgroup of $J_C(\mathbb{F}_p)$ of size n. Then $\sqrt{d} = [\lambda]_G$ for $\lambda \in \mathbb{Z}/n\mathbb{Z}$. Find small k_1, k_2 (not unique!) of size $O(\sqrt{n})$ such that

$$[k]_G = [k_1 + k_2\sqrt{d}]_G = [k_1] + [k_2]\sqrt{d}.$$

Currently we have explicit real multiplication for discriminants

- $\Delta = 2$: Bending
- $\Delta = 5$: Takashima, Kohel-Smith.

Only two! More would be nice..

Gaudry's work

Ref: See Gaudry's ECC 2007 talk slides.

Let C be a genus 2 curve over $\mathbb{F}_p$ having RM by $\mathbb{Q}(\sqrt{d})$. Assume $J_C = \mathrm{Jac}(C)$ is ordinary and absolutely simple.

To determine $\#J_C$ we need to determine the coefficients s_i of the characteristic polynomial of Frobenius π:

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - p s_1 t + p^2, \qquad \chi(1) = \#J_C.$$

The Weil bounds give us: $|s_1| \leq 4\sqrt{p}$ and $|s_2| \leq 6p$.

Use random divisors $D \in J_C(\mathbb{F}_p)$, by construction $\pi(D) = D$.
"Plug" D into $\chi(t)$:

$$[1 - s_1 + s_2 - ps_1 + p^2]D = 0.$$

Use the baby-step giant-step algorithm to search for compatible pairs (s_1, s_2) such that $\chi(1)$ lies in the Weil inverval

$$[(\sqrt{p} - 1)^4, (\sqrt{p} + 1)^4].$$

$\Rightarrow$ search space has size $O(p^{3/2})$
$\Rightarrow$ number of group operations is $O(p^{3/4})$.

Gaudry's work

Improvement: $\pi + \overline{\pi} \in \mathbb{Q}(\sqrt{d})$ with minimal polynomial

$$P(t) = t^2 - s_1 t + (s_2 - 2p)$$

$\mathrm{disc}(P) = (s_1^2 - 4s_2 + 8p) = n^2 d$ for some integer n.

Idea: search for s_1 and n (and deduce s_2).

Bounds on s_1, s_2 give

$$n \in \{1, \ldots, \sqrt{48p/d}\}.$$

Gaudry's work

hocus pocus

Since $\mathrm{disc}(P) = ((\pi + \overline{\pi}) - (s_1 - (\pi + \overline{\pi})))^2 = n^2 d$ we have

$$(2(\pi + \overline{\pi}) - s_1)^2 = n^2 d$$

Multiply both sides by π^2 and use $\pi\overline{\pi} = p$ to get:

$$(2(\pi^2 + p) - s_1\pi)^2 = n^2 d\pi^2$$

Let D be a random divisor defined over $\mathbb{F}_p$. Since $\pi(D) = D$ we obtain

$$(2(1 + p) - s_1)^2 D = n^2 dD$$

$\Rightarrow$ the search space is reduced to $O(p)$, hence complexity $O(\sqrt{p})$.

Combine with Schoof's algorithm: determine (s_1, s_2) mod prime powers and use CRT.

Challenge

The point counting record (June 2008) for a hyperelliptic curve is defined over $\mathbb{F}_p$ where $p = 2^{127} - 1$, and produces a 254-bit Jacobian. The characteristic polynomial of Frobenius π has

$$s_1 = -15671660075779706640,$$
$$s_2 = 86154286096042006774781271889300357630$$

The discriminant of $\pi + \overline{\pi}$ factors as

$$2^8 \cdot 2017 \cdot 24442884947291255330096176263756 73$$

Challenge: Count the number of points on a curve which lies on a Humbert surface of small discriminant, defined over a prime field of ~ 192 bits.