On the complexity of modular equations in genus 2

Jean Kieffer

PhD supervisors: Damien Robert, Aurel Page
LFANT team, Institut de Mathématiques de Bordeaux

AGCCT online conference, 31 May – 4 June 2021

Elliptic modular polynomials

Let $\ell \geq 1$ be a prime. The elliptic modular polynomial of level ℓ

$$\Phi_\ell \in \mathbb{Z}[X, Y]$$

is an equation for the modular curve $X_0(\ell)$.
If k is a field of char. $\neq \ell$, and if E and E' are elliptic curves over k, then

$$\Phi_\ell(j(E), j(E')) = 0 \iff E \text{ and } E' \text{ are } \ell\text{-isogenous over } \bar{k}.$$

Algorithmic applications

- Detect ℓ-isogenies = navigate ℓ-isogeny graphs.
- Compute ℓ-isogenies without prior knowledge of the kernel: SEA.

Better complexities than computing the full ℓ-torsion of E.

Size bounds for elliptic modular polynomials

The height $h(F)$ of $F \in \mathbb{Q}(X_1, \ldots, X_n)$ is $\log(\max|c|)$, where c runs through the nonzero coefficients in an irreducible form of F.

Size bounds for Φ_ℓ

- Φ_ℓ has degree $\ell + 1$ in both variables X and Y.
- $h(\Phi_\ell) \sim 6\ell \log \ell$ [Cohen '84].

Storing Φ_ℓ costs $O(\ell^3 \log \ell)$ space. Large databases [Sutherland].

Plan

1. Higher-dimensional modular equations
2. Size bounds for modular equations
3. Evaluating modular equations for abelian surfaces

Higher-dimensional modular equations

PEL Shimura varieties

Moduli spaces for complex abelian varieties of fixed dimension g with a certain PEL structure: Polarization, Endomorphisms, Level.

Choose:

- two connected components $\mathcal{S}$ and $\mathcal{T}$ of a PEL Shimura variety, defined over a number field L;
- coordinates = modular functions: $j_1, \ldots, j_n$ defined over L.

Higher-dimensional modular equations

Modular equations describe Hecke correspondences H on $\mathcal{S} \times \mathcal{T}$: locus of abelian varieties linked by isogenies of a certain type.

- degree $d(H)$ = number of isogenies described by H;
- isogeny degree $l(H)$.

Analytic formulæ defining modular equations:

Products of $d(H)$ factors involving invariants of isogenous abelian varieties.

Concretely:

$$\Psi_{H,m} \in L(J_1, \ldots, J_n)[Y] \quad \text{for } 1 \leq m \leq n.$$

Roots of $\Psi_{H,1}$ are the values of j_1 at isogenous abelian varieties.
Then $\Psi_{H,2}$ gives j_2, etc: lexicographic Gröbner basis.

Example 1: Siegel spaces

$\mathcal{A}_g = \mathsf{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ classifies p.p.a.v.'s of dimension g; def. over $\mathbb{Q}$.

Case $g = 2$: Igusa invariants j_1, j_2, j_3 define a birational map $\mathcal{A}_2 \to \mathbb{P}^3$.

Siegel modular equations for abelian surfaces

$$\Psi_{\ell,m} \in \mathbb{Q}(J_1, J_2, J_3)[Y] \quad \text{for } 1 \leq m \leq 3.$$

They encode ℓ-isogenies between p.p. abelian surfaces, of degree ℓ^2.
[Dupont '06; Bröker, Lauter '09; Milio '15].

Example 2: Hilbert surfaces [1]

F fixed real quadratic field. Then

$$\Gamma(1)_F = \mathrm{SL}(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee) \subset \mathrm{SL}_2(F)$$

acts on $\mathbb{H}_1^2$. The Hilbert surface $\mathcal{A}_{2,F} = \Gamma(1)_F \backslash \mathbb{H}_1^2$ classifies p.p. abelian surfaces A with RM by $\mathbb{Z}_F$: i.e. $\mathbb{Z}_F \hookrightarrow \mathrm{End}(A)^\dagger$.
There is an involution σ of $\mathcal{A}_{2,F}$ given by Galois conjugation.

The case $F = \mathbb{Q}(\sqrt{5})$

Gundlach invariants g_1, g_2 define a birational map $\mathcal{A}_{2,F}/\langle\sigma\rangle \to \mathbb{P}^2$.
In general, use Igusa invariants.

Example 2: Hilbert surfaces [2]

Hilbert modular equations for abelian surfaces

Let $\beta \in \mathbb{Z}_F$ be a totally positive split prime, and $\ell = N_{F/\mathbb{Q}}(\beta)$.

For $F = \mathbb{Q}(\sqrt{5})$:

$$\Psi_{\beta,m} \in \mathbb{Q}(g_1, g_2)[Y] \quad \text{for } 1 \leq m \leq 2.$$

They encode β- and $\sigma(\beta)$-isogenies, both of degree ℓ [Martindale '20; Milio, Robert '20].

State of the art

We know how to:

- Compute modular equations of small levels, and examples of isogenous p.p. abelian surfaces.
- Generalize Atkin's method for point counting [Ballentine, Guillevic, Lorenzo-García, Martindale, Massierer, Smith, Top '16].
- Compute isogenies without prior knowledge of their kernels [K., Page, Robert 202?]. SEA for abelian surfaces?

Complexity bounds? Better than using the full ℓ-torsion?

Size bounds for modular equations

Main result

As before: H Hecke correspondence, degree $d(H)$, isogeny degree $l(H)$.

Theorem (K. 202?)

1. *The degree of modular equations is $O(d(H))$.*
2. *The height of modular equations is $O(d(H) \log l(H))$.*

Constants depend on the choice of invariants.

Examples

Corollary

	Degree	Height	# Variables	Total size
Φ_ℓ	$O(\ell)$	$O(\ell \log \ell)$	2	$O(\ell^3 \log \ell)$
Siegel	$O(\ell^3)$	$O(\ell^3 \log \ell)$	4	$O(\ell^{15} \log \ell)$
Hilbert	$O_F(\ell)$	$O_F(\ell \log \ell)$	3	$O_F(\ell^4 \log \ell)$

Recall: $\ell = N_{F/\mathbb{Q}}(\beta)$.

Remark

In the Siegel case, and in the Hilbert case for $F = \mathbb{Q}(\sqrt{5})$: we can obtain explicit constants.

Degree bounds are tight, height bounds are not.

Ideas of proof: degree bounds

We identify an explicit denominator of modular equations.

Example: Φ_ℓ

- The denominator of j is Δ. Coefficients of $\Phi_\ell(j(\tau), Y)$ are of the form f/g_ℓ where

$$g_\ell(\tau) = \prod_{\gamma \in \Gamma^0(\ell) \backslash \mathrm{SL}_2(\mathbb{Z})} (\gamma^* \tau)^{-12} \Delta(\tfrac{1}{\ell}\gamma\tau).$$

- g_ℓ has weight $\mathrm{wt}(g_\ell) = d(H)\,\mathrm{wt}(\Delta) = 12(\ell+1)$.
- Write $\dfrac{f}{g_\ell} = \dfrac{P(E_4, E_6)}{Q(E_4, E_6)}$; then $\deg(P), \deg(Q) \in O(\ell)$.
- Replace $E_6^2 \to E_4^3(1 + 1/j)$ and simplify. We obtain a rational fraction in j of degree $O(\ell)$.

Ideas of proof: height bounds

Evaluation-interpolation strategy

In the case of Φ_ℓ: [Pazuki '19]

1. Evaluations of modular equations at "small points" have height $O(d(H) \log l(H))$.
2. If a rational fraction F of degree d satisfies $h(F(x)) \leq H$ for a lot[1] of points x, then $h(F)$ is roughly $\leq H + O(d \log d)$ [K. 202?].

In Step 1, use the modular interpretation:

- The difference in Faltings heights is $O(\log l(H))$;
- The Faltings height is related to the the height of invariants, via Theta heights [Pazuki '12]

[1] depending on d and H.

Complexity of modular equations

No asymptotic improvements on point counting or isogenies using modular equations for abelian surfaces written in full.

But!

In practice, we only need evaluations of modular equations and their derivatives at fixed points over a finite/number field.
These evaluations have a smaller total size: $O(\ell^6(h(j_1, j_2, j_3) + \log \ell))$ in the Siegel case.

Evaluating modular equations for abelian surfaces

Complex approximations

Outline of the evaluation algorithm

Siegel case, over $\mathbb{Q}$: let $j_1, j_2, j_3 \in \mathbb{Q}$ of height H.

1. Find $\tau \in \mathbb{H}_2$ with these Igusa invariants.
2. Enumerate isogenous period matrices and compute Igusa invariants (via theta constants).
3. Compute evaluated modular equations analytically.
4. Recognize rational numbers.

Steps 1 and 2 can be heuristically done in quasi-linear time in the required precision for fixed arguments [Dupont '06].
Here the arguments depend on H, and so does the required precision.

Precisions on the algorithm

- Make a heuristic on the computation of theta constants on a fixed compact set of τ's. For other values, reduction to the fundamental domain + duplication formulæ.
- Use the structure of Siegel modular forms over $\mathbb{Z}$ to recognize integers instead of rational numbers.
- Analyze precision losses. Provably correct output.

Results

Theorem (K., 202?, under heuristic)

1. *We can evaluate Hilbert modular equations of level* β *for* $F = \mathbb{Q}(\sqrt{5})$ *at* $(g_1, g_2) \in \mathbb{Q}^2$ *of height at most* H *in time* $\widetilde{O}(\ell H^2 + \ell^2 H)$.
2. *We can evaluate Siegel modular equations of level* ℓ *at* $(j_1, j_2, j_3) \in \mathbb{Q}^3$ *of height at most* H *in time* $\widetilde{O}(\ell^3 H^2 + \ell^6 H)$.

Almost quasi-linear time. For general F, heuristic rational reconstruction.

Consequences on point counting

Hilbert case

We can heuristically count points on p.p. abelian surfaces $A/\mathbb{F}_p$ with RM by $\mathbb{Z}_F$ in time $\widetilde{O}_F(\log^4 p)$ on average.

- Same asymptotic complexity as SEA up to a constant factor.
- Improves on Schoof's method in $\widetilde{O}_F(\log^5 p)$ [Gaudry, Kohel, Smith '11].

Siegel case

If A is a p.p. abelian surface over $\mathbb{F}_p$ with small invariants (e.g. reduction of a fixed abelian surface over a number field), then we can heuristically count points on A in time $\widetilde{O}(\log^7 p)$.

- Improves on Schoof's methof in $\widetilde{O}(\log^8 p)^*$ [Gaudry, Harley '00; Gaudry, Schost '12]
- No asymptotic improvement for a general $A/\mathbb{F}_p$.

Questions

Thank you for listening!

Any questions?