Asymptotically faster point counting for abelian surfaces

Jean Kieffer (Harvard)

Explicit Methods for Modularity, April 11–15, 2022

The point counting problem

A, p.p. abelian variety of dimension g over $\mathbb{F}_q$.

We can attach to A its characteristic polynomial of Frobenius χ_A.

- $\chi_A \in \mathbb{Z}[X]$,
- monic of degree $2g$,
- complex roots have absolute value $\sqrt{q}$.

The point-counting problem

Given A, compute χ_A. Determines $\#A(\mathbb{F}_{q^r})$, isogeny class of A, local factor of L-function if A comes from a number field.

Schoof's polynomial time algorithm

For small primes $\ell \ll p$, look at the Galois representation on $A[\ell]$:

- Compute an explicit equation for $A[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$.
- Compute the characteristic polynomial of Frobenius on $A[\ell]$: this is $\chi_A \in (\mathbb{Z}/\ell\mathbb{Z})[X]$.

Conclude using the Weil bounds.

Complexity for abelian surfaces: $\widetilde{O}(\log^8 q)$, essentially because the algorithm manipulates polynomials of large degree $O(\ell^4)$.

Elkies's method

Attempt to replace $A[\ell]$ by some subgroup:

- Compute an abelian variety A' that is ℓ-isogenous to A. There exists $f\colon A \to A'$, of degree ℓ^g, with isotropic kernel.
- Compute f as an explicit rational map.
- Obtain $K \subset A[\ell]$ as $\ker f$.

Elkies (90's) describes this strategy in the case of elliptic curves.

Goal

Extend these methods to higher dimensions, and improve the complexity of point counting for abelian surfaces.

Main result

Theorem (K.)

Let K be a number field. Let A/K be a p.p. abelian surface over K of height at most H. Let $q \geq 1$. Then, under the heuristic that Elkies's method applies to sufficiently many small primes:

- Given a good prime $\mathfrak{p}$ of norm $N(\mathfrak{p}) = q$, one can compute $\chi_{A \bmod \mathfrak{p}}$ in $\widetilde{O}_K(H \log^7 q)$ binary operations.
- Given $\Theta(H \log q)$ distinct good primes $\mathfrak{p}_i$ such that $\log N(\mathfrak{p}_i) = O(\log q)$, one can compute all polynomials $\chi_{A \bmod \mathfrak{p}_i}$ in $\widetilde{O}_K(\log^6 q)$ binary operations on average.

Besides this result, develop explicit methods for isogenies in higher dimensions. In other words: study Galois representations on $A[\ell]$ without writing down the full subgroup.

Higher-dimensional modular equations

Diagram of moduli spaces

$\mathcal{A}_g$: p.p. abelian varieties of dimension g.
$\mathcal{A}_g^0(\ell)$: p.p. abelian varieties with the kernel of an ℓ-isogeny.

$$\begin{array}{ccc} & \mathcal{A}_g^0(\ell) & \\ {\scriptstyle \text{keep } A} \swarrow & & \searrow {\scriptstyle \text{keep } A'} \\ \mathcal{A}_g & & \mathcal{A}_g \end{array}$$

ℓ-isogeny $f: A \to A'$

A and A' are ℓ-isogenous $\iff$ (A, A') lies in the image of $\mathcal{A}_g^0(\ell)$.

Modular equations of Siegel type

Explicit equations for the image of $\mathcal{A}_g^0(\ell)$ in $\mathcal{A}_g \times \mathcal{A}_g$.

Examples of modular equations

- Dimension 1: isomorphism $j\colon \mathcal{A}_1 \to \mathbb{A}^1$.
  The modular polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$ is a birational equation for $\mathcal{A}_1^0(\ell)$, i.e. $X_0(\ell)$.
  To find elliptic curves that are ℓ-isogenous to E, simply look for roots of $\Phi_\ell(j(E), Y)$.
- Dimension 2: birational isomorphism $\mathcal{A}_2 \simeq \mathbb{P}^3$ given by three Igusa invariants j_1, j_2, j_3.
  Modular equations of Siegel type are three rational fractions in four variables $\Psi_{\ell,k} \in \mathbb{Q}(J_1, J_2, J_3)[Y]$, for $1 \leq k \leq 3$.

State of the art

Previous works

Compute modular equations of small levels for $g = 2$ (very large!), and examples of isogenous p.p. abelian surfaces. [Dupont '06; Bröker, Lauter '09; Milio '15].

In this work

- Compute isogenies without prior knowledge of their kernels, using modular equations.
- Size bounds for modular equations.
- Efficient evaluation algorithms via complex approximations.

In combination: Elkies's method for p.p. abelian surfaces.

Isogeny algorithms and their complexities

Computing isogenies

Theorem (K., Page, Robert)

Let ℓ be prime. Let k be a field s.t. char $k = 0$ or $> 8\ell + 7$. Given:

- two generic ℓ-isogenous p.p. abelian surfaces A, A' over k,
- the values of all derivatives of Siegel modular equations $\Psi_{\ell,k}$ of level ℓ at (A, A'),

one can compute an explicit description of an ℓ-isogeny $f\colon A \to A'$:

- Genus 2 curve equations $\mathcal{C}, \mathcal{C}'$ (maybe over an extension k'/k).
- The rational map

$$\mathcal{C} \xhookrightarrow{\text{base pt}} \mathrm{Jac}(\mathcal{C}) \xrightarrow{f} \mathrm{Jac}(\mathcal{C}') \overset{\sim}{\dashrightarrow} \mathrm{Sym}^2(\mathcal{C}') \xrightarrow{\text{coords}} \mathbb{A}^4.$$

The cost is $\widetilde{O}(\ell)$ operations in k'.

Outline of the isogeny algorithm

- Compute $\mathcal{C}$, $\mathcal{C}'$. The choice of equations encodes a choice of basis for $\Omega^1(A)$ and $\Omega^1(A')$, or equivalently $T_0(A)$ and $T_0(A')$.
- By the Kodaira–Spencer isomorphism $\mathrm{Sym}^2 T_0(A) \simeq T_A(\mathcal{A}_g)$, we obtain deformations of A, A'.
- Derivatives of modular equations tell us how to modify $\mathcal{C}, \mathcal{C}'$ so that deformations remain ℓ-isogenous. The isogeny f is then normalized: $\mathrm{Sym}^2(df) = \ell \cdot I_3$.
- Write a differential system satisfied by f and solve it using standard computer algebra techniques: Newton iterations on power series + rational reconstruction.

This relies on an explicit Kodaira–Spencer isomorphism: identify derivatives of Igusa invariants in terms of coefficients of $\mathcal{C}$.

Size bounds for modular equations

Theorem (K. 2021)

The modular equations of Siegel type $\Psi_{\ell,k}$ have:

- *total degree $O(\ell^3) = O(\#$ of ℓ-isogenies from a given $A)$;*
- *height $O(\ell^3 \log \ell)$.*

Remarks

- Total size of $\Psi_{\ell,k}$ is $O(\ell^{15} \log \ell)$.
  Compare with $g = 1$: size of Φ_ℓ is $O(\ell^3 \log \ell)$.
- Can obtain explicit constants. Degree bounds are tight, height bounds are horrific.
- Analogous result holds for modular equations encoding any Hecke correspondence on any Shimura variety of PEL type.

Evaluation of modular equations

We only need evaluations of modular equations and their derivatives at fixed points over a finite/number field.

- Size of $\Psi_{\ell,k}(j_1, j_2, j_3) \in \mathbb{Q}[Y]$ is $\widetilde{O}(\ell^6\, h(j_1, j_2, j_3))$.
- They can be computed in quasi-linear time using complex approximations.

Key input: certified, uniform, quasi-linear time algorithm for the evaluation of genus 2 theta constants at a given complex period matrix, building on works of Dupont and Labrande–Thomé.

Implementation results

Time (s) to evaluate modular equations of level $\ell = 2, 3, \ldots$ at $(159/239, -19/28, -193/246)$:

2	3	5	7	11	13	17
1.34	5.12	96.7	$1.23 \cdot 10^3$	$3.97 \cdot 10^4$	$1.57 \cdot 10^5$	$1.12 \cdot 10^6$

Closely matches $0.002\, \ell^6 \log(\ell)^3 \log\log\ell$.

Implementation results

Time (s) to evaluate modular equations of level $\ell = 2, 3, \ldots$ at $(159/239, -19/28, -193/246)$:

2	3	5	7	11	13	17
1.34	5.12	96.7	$1.23 \cdot 10^3$	$3.97 \cdot 10^4$	$1.57 \cdot 10^5$	$1.12 \cdot 10^6$

Closely matches $0.002\, \ell^6 \log(\ell)^3 \log\log \ell$.

Analogous case of p.p. abelian surfaces with RM by a fixed quadratic field F. Cyclic, degree ℓ isogenies exist when $\ell = \mathfrak{b}\overline{\mathfrak{b}}$ splits in F and $\mathfrak{b}$ is trivial in the narrow class group. Case $F = \mathbb{Q}(\sqrt{5})$:

11	19	29	$\cdots$	101	109	$\cdots$	479	491	499
2.45	4.14	9.67		256	315		16800	17900	22100

Future directions?

- Isogeny algorithm for Jacobians of plane quartics ($g = 3$), using the relation between Siegel modular forms and "concomitants" [Cléry, Faber, van der Geer '20].
- Better choices of birational models of $\mathcal{A}_2^0(\ell)$? Could bring large speedups in practice. Cf. many papers in dimension 1.
- Distribution of Elkies primes in higher dimensions? Dimension 1 case by Shparlinski–Sutherland ['14,'15].
- Certifying the evaluation algorithm for modular equations involves a good understanding of the associated graded rings of modular forms over $\mathbb{Z}$.
  Examples in the literature are sparse, but there is an ongoing effort in the Collaboration to compute such graded rings.