The KLPT path-finding algorithm

Overview

The KLPT algorithm is a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular ℓ-isogeny graphs. The main result is an algorithm for the following. Let $B_{p,\infty}$ be a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Let ℓ be a fixed prime, typically 2 or 3. Given a maximal quaternion order $\mathcal{O}$ in $B_{p,\infty}$ and a left $\mathcal{O}$-ideal I, compute an equivalent left $\mathcal{O}$-ideal $J = I\beta$ with norm ℓ^n for some n. This algorithm runs in practice and heuristically (based on a hypothesis of equidistribution of primes) in probabilistic polynomial time. The algorithm is described in terms of a special maximal order, but extends to any maximal order by passing through such a special order.

1. A supersingular motivation

Let $\mathcal{O}$ be the endomorphisms ring of a fixed supersingular elliptic curve $E_0/\mathbb{F}_q$, where $q = p^2$, which we suppose to be an order in a quaternion algebra B.

Equivalence of categories. Let $\mathbf{SS}(\mathbb{F}_q)$ be the category of supersingular elliptic curves over $\mathbb{F}_q$ in the isogeny class of E_0, and let $\mathbf{Proj}_r(\mathcal{O})$ be the category of right projective modules of rank 1 over $\mathcal{O} = \mathrm{End}(E_0)$.

$$\mathrm{Hom}(E_0, -) : \mathbf{SS}(\mathbb{F}_{p^2}) \longrightarrow \mathbf{Proj}_r(\mathcal{O})$$

determines an equivalence of categories.

For a more detailed description (with attention to the relative base field and isogeny class determined by Frobenius), see Chapter 5, §5.3 of my thesis [4], and [2] for a generalization to higher dimension.

Thinking elliptically. We first explore how to interpret concretely this equivalence of categories with the algebraic category $\mathbf{Proj}_r(\mathcal{O})$ in terms of the context of elliptic curves.

Exercises. Let $\varphi : E_1 \to E_2$ be an isogeny. The choice of left or right projective modules is arbitrary in the sense that the categories are dual to one another.

(1) Show that the functor $\mathrm{Hom}(E_0, -)$ is a covariant functor to $\mathbf{Proj}_r(\mathcal{O})$.

(2) Show that the functor $\mathrm{Hom}(-, E_0)$ is a contravariant functor to $\mathbf{Proj}_l(\mathcal{O})$.

(3) Show that the dual isogeny induces a contravariant functor on the images of these functors, exchanging objects $\mathrm{Hom}(E_0, E_i)$ with $\mathrm{Hom}(E_i, E_0)$ and morphisms

$$\mathrm{Hom}(E_0, \varphi) = \varphi_* : \mathrm{Hom}(E_0, E_1) \longrightarrow \mathrm{Hom}(E_0, E_2),$$

with

$$\mathrm{Hom}(\bar{\varphi}, E_0) = \varphi^* : \mathrm{Hom}(E_0, E_2) \longrightarrow \mathrm{Hom}(E_0, E_1).$$

where $\varphi_*(\psi) = \varphi\psi$ and $\varphi^*(\psi) = \psi\varphi$.

The algebraic dual $M \mapsto \mathrm{Hom}_{\mathcal{O}}(M, O)$ is an isomorphism (equivalence of categories) between $\mathbf{Proj}_r(\mathcal{O})$ and $\mathbf{Proj}_l(\mathcal{O})$, extending the duality determined by the dual isogeny.

The category $\mathbf{Proj}_r(\mathcal{O})$ permits us to discuss the objects of the form $\mathrm{Hom}(E_0, E_1)$ without choice of embedding in $\mathcal{O} = \mathrm{End}(E_0)$. In practice the KLPT algorithm works with a category of left (or right) ideals. Every module in $\mathbf{Proj}_r(\mathcal{O})$ can be embedded as a right $\mathcal{O}$-ideal and every such ideal is of the form $\varphi\mathrm{Hom}(E_0, E_1)$ for an isogeny $\varphi : E_1 \to E_0$, and similarly every left ideal is of the form $\mathrm{Hom}(E_1, E_0)\varphi$ for some $\varphi : E_0 \to E_1$.

Conversely, given a left $\mathcal{O}$-ideal I, coprime to p, we define

$$E_0[I] = \{P \in E_0(\bar{\mathbb{F}}_p) \mid \varphi(P) = O \text{ for all } \varphi \in I\},$$

and set $E_1 = E_0/E_0[I]$. Given two such ideals $I_1 \supseteq I_2$, we define $J = I_1^{-1}I_2$, a left $\mathcal{O}_1$-ideal, where $\mathcal{O}_1 = \mathrm{End}(E_1)$ is the right order of I_1, giving an isogeny

$$\varphi_J : E_1 \to E_2,$$

where $\ker(\varphi_J) = E_1[J]$.

The restriction to ideals coprime to p, avoids the need for the definition of $E_0[I]$ as a group scheme and to deal with inseperable isogenies. To understand general ideals, we note that every maximal order (and every Eichler order) is locally at p equal to the unique maximal order $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, a noncommutative discrete valuation ring. The orders $\mathcal{O} = \mathcal{O}_0$ and $\mathcal{O}_1 = \mathrm{End}(E_1)$ have unique maximal (2-sided) ideals $\mathfrak{P}_i \subset \mathcal{O}_i$ over $p\mathbb{Z}$ such that $\mathfrak{P}_i^2 = p\mathcal{O}_i$. An left $\mathcal{O}$-ideal factors uniquely as $I = \mathfrak{P}_1^e I_s = I_s \mathfrak{P}_0^e$, where I_s is an ideal coprime to p.

Exercises. The following series of results develop and expand on the connection between supersingular elliptic curves and chains of left $\mathcal{O}$-ideals.

(4) Let $\mathcal{O} \supset I_1 \supset \cdots \supset I_n = I$ be a chain of left $\mathcal{O}$-ideals, and set $J_i = I_{i-1}^{-1}I_i$. Observe that we obtain an isogeny chain

$$E_0 \longrightarrow E_1 \longrightarrow \cdots \longrightarrow E_n$$

defined by $\varphi_{J_i} : E_{i-1} \to E_i$, where $E_i = E_0/E_0[I_i]$.

(5) Let $E_0[\ell]$ the ℓ-torsion subgroup of E_0. With respect to a basis (P, Q) for $E_0[\ell]$, show that the endomorphism ring $\mathcal{O}$, acting on $E_0[\ell]$ induces an isomorphism $\mathcal{O}/\ell\mathcal{O} \cong \mathbb{M}_2(\mathbb{F}_\ell)$.

(6) Extending $(P, Q) = (P_1, Q_1)$ to a basis (P_n, Q_n) for each $E_0[\ell^n]$, such that $(\ell P_n, \ell Q_n) = (P_{n-1}, Q_{n-1})$, show that one obtains an isomorphism

$$\mathcal{O}/\ell^n\mathcal{O} \cong \mathbb{M}_2(\mathbb{Z}/\ell^n\mathbb{Z}) = \mathrm{End}(E_0[\ell^n]),$$

In the projective limit, deduce an injection

$$\mathcal{O} \longrightarrow \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E_0)),$$

where $T_\ell(E_0)$ is the ℓ-th Tate module of E_0.

(7) The $\ell + 1$ cyclic ℓ-isogenies φ from E_0 are in bijection with the left ideals $I \subset \mathbb{M}_2(\mathbb{F}_\ell)$ stabilizing the subgroup $\ker(\varphi) \subset E_0[\ell]$.

(8) In passing to ℓ-chains of left ideals $\mathcal{O} \supset I_1 \supset \cdots \supset I_n = I$ we obtain a bijection of the set of ℓ-chains of lenth n and projective points

$$\mathbb{P}(E_0[\ell^n]) = \frac{(E_0[\ell^n] \backslash E_0[\ell^{n-1}])}{\mathbb{Z}/\ell^n\mathbb{Z}^*} \cong \mathbb{P}^1(\mathbb{Z}/\ell^n\mathbb{Z}),$$

and, in the limit, infinite ℓ-chains are in bijection with $\mathbb{P}(T_\ell(E_0)) \cong \mathbb{P}^1(\mathbb{Z}_\ell)$.

In the next section we consider the quadratic forms associated to quaternion ideals, given by the reduced norm, with the goal of producing an isogeny in $\mathrm{Hom}(E_0, E_1)$ of degree ℓ^n.

2. Quadratic forms

The KLPT algorithm is essentially about finding a representation of a number of the form ℓ^n by a quaternary quadratic form. In terms of supersingular elliptic curves, the positive definite quadratic form is the degree map on $\mathrm{Hom}(E_0, E_1)$

$$\deg : \mathrm{Hom}(E_0, E_1) \longrightarrow \mathbb{Z}$$

And in terms of ideal classes, the quadratic form is the normalized reduced norm $n_I : I \longrightarrow \mathbb{Z}$ defined by $f_I(\alpha) = \mathrm{Nrd}(\alpha)/\mathrm{Nrd}(I)$. The associated theta series

$$\theta_I(q) = \sum_{\alpha \in I} q^{n_I(\alpha)} = \sum_{m=1}^{\infty} a_m q^m,$$

is a modular form of weight 2 whose coefficients a_m are counting functions for the number of representations of m by n_I — we say that n_I represents m if there exists $\alpha \in I$ such that $n_I(\alpha) = m$.

Notation. We refer to a $\mathbb{Z}$-module M equipped with a quadratic form $f : M \to \mathbb{Z}$ as a quadratic module. For our purposes, all of the quadratic forms we consider (attached to definite quaternion algebra or imaginary quadratic ideal classes) will be positive definite. The inner product associated to f is:

$$\langle x, y \rangle = f(x+y) - f(x) - f(y)$$

and f is recovered from the inner product by $f(x) = \langle x, x \rangle/2$. For certain quadratic forms, like the discriminant module of a quaternion order, it is convenient to set $f(x) = \langle x, x \rangle$ an instead normalize the inner product by dividing by 2. The Gram matrix of the quadratic form, in terms of an ordered basis $(x_1, \dots, x_r)$, is the matrix

$$\big(\langle x_i, x_j \rangle\big).$$

If L is an orthogonal direct product $L = M \oplus N$, then in terms of a basis $\mathcal{B} = \mathcal{B}_M \cup \mathcal{B}_N$ which is the union of bases for M and N, the Gram matrix of L is the block matrix with Gram matrices of $\mathcal{B}_M$ and $\mathcal{B}_N$ along the diagonal. The quadratic form of L is a sum, $f_L(x+y) = f_M(x) + f_N(y)$ for $x \in M$ and $y \in N$ and the theta function if a product:

$$\theta_L(q) = \theta_M(q)\theta_N(q).$$

Thinking quadratically. The following exercises concern the quadratic forms

Exercises.

(9) Observe that for any left (or right) $\mathcal{O}$-ideal I, the quadratic form n_I is independent of the representative of the ideal class. In particular, if

$$I = \mathrm{Hom}(E_1, E_0)\varphi \subset \mathcal{O} = \mathrm{End}(E_0),$$

then $n_I(\psi\varphi) = \deg(\psi)$.

(10) The supersingular elliptic curves E with j-invariant in $\mathbb{F}_p$ are those elliptic curves which admit a subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ with $\pi^2 = -p$, of discriminant $-4p$. If $p = 1 \bmod 4$, this imaginary quadratic order is maximal. If $p = 3 \bmod 4$, then these curves are partitioned into those for which this embedding is primitive (not contained in a larger order) and those for which $(1+\pi)/2 \in \mathrm{End}(E)$.

The curve with $j = 12^3$ (admitting an embedding of the Gaussian integers), lies in the two classes, isomorphic over $\mathbb{F}_{p^2}$ but quadratic twists in $\mathbb{F}_p$. The total number of such elliptic curves is

$$\big(h(-p) + h(-4p)\big)/2 \sim \sqrt{p}.$$

This follows, for example, from a result of Kaneko [3] proves that the product of the Hilbert class polynomials

$$H_{-p}(x)H_{-4p}(x) \equiv S(x)^2 \bmod p$$

is the square of a square-free polynomial $S(x)$, in which $x - 12^3$ is the only common factor (when $p = 3 \bmod 4$). For consistency we set $H_{-p}(x) = 1$ and $h(-p) = 0$ when $p = 1 \bmod 4$.

(11) In the particular case $p = 11$, the Hilbert class polynomials are:

$$H_{-11}(x) = x + 32768 \equiv x - 1 \bmod p$$

and

$$\begin{aligned} H_{-44}(x) &= x^3 - 1122662608x^2 + 270413882112x - 653249011576832 \\ &\equiv (x-1)x^2 \bmod p. \end{aligned}$$

Observe that $j = 12^3 \equiv 1 \bmod p$ and $j = 0 \bmod p$ are the two supersingular j-invariants in characteristic p.

(12) It follows that there are exactly two maximal orders $\mathcal{O}_0 = \mathrm{End}(E_0)$ and $\mathcal{O}_1 = \mathrm{End}(E_1)$ exactly (up to isomorphism) in the definite quaternion algebra ramified at 11. The unit groups are both cyclic, of orders $|\mathcal{O}_0^*| = 6$ and $|\mathcal{O}_1^*| = 4$.

There is a third quadratic module M of interest, namely $\mathrm{Hom}(E_0, E_1)$, isomorphic to $\mathrm{Hom}(E_1, E_0)$ by the dual isogeny. The respective Gram matrices (for a Minkowski-reduced basis) are:

$$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 8 & 4 \\ 0 & 1 & 4 & 8 \end{pmatrix} \quad \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 6 & 0 \\ 1 & 0 & 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 4 & 2 & 1 & 0 \\ 2 & 4 & 1 & 1 \\ 1 & 1 & 4 & 2 \\ 0 & 1 & 2 & 4 \end{pmatrix}$$

Observe that the middle quadratic form is an orthogonal sum, with orthogonal bases $\{1, (1+\pi)/2\}$ and $\{i, i(1+\pi)/2\}$, where $i^2 = -1$ and $\pi^2 = -11$.

(13) The theta series of the three quadratic module are, respectively,

$$\begin{aligned} \theta_{\mathcal{O}_0}(q) &= 1 + 6(q + q^3 + 4q^4 + 3q^5 + 6q^6 + 2q^7 + 6q^8 + 4q^9 + \cdots) \\ \theta_{\mathcal{O}_1}(q) &= 1 + 4(q + q^2 + 2q^3 + 5q^4 + 4q^5 + 8q^6 + 4q^7 + 9q^8 + 7q^9 + \cdots) \\ \theta_M(q) &= 1 + 12(q^2 + q^3 + q^4 + q^5 + 2q^6 + 2q^7 + 3q^8 + 3q^9 + \cdots) \end{aligned}$$

Observe that the second form is the square of the theta series of the binary quadratic form $x^2 + xy + 3y^2$, and

$$f_E(q) = \frac{1}{6}\big(\theta_{\mathcal{O}_0}(q) - \theta_M(q)\big) = \frac{1}{4}\big(\theta_{\mathcal{O}_1}(q) - \theta_M(q)\big)$$

is the weight 2 cusp form of the unique isogeny class of elliptic curves of conductor 11. In particular the three theta series satisfy a linear dependence.

(14) When $p \equiv 3 \bmod 4$, show that the norm modules for the maximal orders containing $(1+\pi)/2$, are othogonal direct sums $R \oplus \mathfrak{a}$ where $R = \mathbb{Z}[(1+\pi)/2]$ and $\mathfrak{a}$ runs through representatives of $\mathcal{C}\ell(R)/\{\pm 1\}$.

3. The KLPT algorithm

References

[1] D. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons (1989).

[2] B. Jordan, A. Keeton, B. Poonen, E. Rains, N. Shepherd-Barron, J. Tate. Abelian varieties isogenous to a power of an elliptic curve, *Compositio Mathematica*, **154** (5), (2018) 934–959.

[3] M. Kaneko. Supersingular j-invariants as singular moduli mod p, Osaka J. Math., **26** (1989) 849–855.

[4] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley (1996).

[5] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. On the quaternion ℓ-isogeny path problem, *LMS Journal of Computational Mathematics*, **17** (2014), 418–432.