PCMI Supersingular Isogeny Graphs Exercise Sheet 2

Exercises Lecture 2 & 3: Expander graphs, SIDH Quaternion algebras, Endomorphism rings

TA: Jana Sotáková **version July 25, 2022**

You can find hints and more explanation starting at a new page after the exercises.
Please note that we can use the Zulip stream on Drew's server to ask questions!
Jana will try to keep the Whova and PCMI websites up to date but quickest updates are here.

1. For small primes $p \equiv 1 \bmod 12$, denote the SIG 2-isogeny graph as $\mathcal{G}_2$.

   Note: the congruence condition means that $j = 0, 1728$ are not supersingular j-invariants, so we can make the isogeny graph undirected at all vertices.

   (a) Find the adjacency matrix A of $\mathcal{G}_2$;

   (b) Find the largest 2 eigenvalues of A;

   (c) Compute the spectral gap. Estimate the expansion/Cheegner constant c using the formula from the lecture. Compute it exactly and compare the two values.

   (d) Find the diameter of the graph.

   (e) What changes for $p \neq 1 \bmod 12$?

2. (Quaternion algebras and orders) For small primes p, define the quaternion algebra $B := B_{p,\infty} = \mathbb{Q}\langle 1, i, j, k\rangle$ with $i^2 = -r$ and $j^2 = -p$ and $ij = -ji = k$:

   (a) Use `QuaternionAlgebra< RationalField() | -r, -p >`;

   (b) For $p \equiv 3 \bmod 4$, use $-r = -1$;

   (c) For $p \equiv 5 \bmod 8$, use $-r = -2$;

   (d) Otherwise, find r as a prime $r \equiv 3 \bmod 4$ such that $\left(\frac{r}{p}\right) = -1$.

   Verify that B is only ramified at p and infinity (`RamifiedPrimes`). Find the discriminant of B. Note that again, ramified primes are those that divide the discriminant. In the last exercise 6, you will see one way which makes ramified primes special.

   Verify that $i^2 = -r$ and $j^2 = -p$. Find the norm, trace and the minimal polynomial of the element $w = 2 + i - 3j + 4k$.

   Maximal orders. Write down a maximal order in each of the quaternion algebras. You can find examples for different congruence conditions on p in Lemmas 2-4 in Kohel-Lauter-Petit-Tignol.

   (a) Using the Magma command `MaximalOrder`;

   (b) Using a basis and `QuaternionOrder`;

   Find the discriminant and the norm form of the maximal order. (Check the hint on how to get the correct norm form in Magma)

3. For $p = 67$, take any maximal order $\mathcal{O} \subset B_{p,\infty}$. Then:

   (a) Enumerate all the left-ideal classes in $\mathcal{O}$; `LeftIdealClasses`

(b) For every ideal class, pick a representative and find the right order of the ideal; `RightOrder`;

(c) Check how many isomorphism classes there are as right orders. Deduce the number of supersingular j-invariants in $\mathbb{F}_p$ and pairs of conjugate j-invariants in $\mathbb{F}_p^2$. Hint available.

(d) Compute the norm of all these ideals;

(e) Figure out which of these maximal orders correspond to elliptic curves defined over $\mathbb{F}_p$. Show that the following suffices:

i. Compute the norm form of these maximal orders; Hint available.

ii. Find out whether they represent p;

Check the count by looking at how many supersingular j-invariants there are in $\mathbb{F}_p$.

4. (SIDH key exchange)

(a) (Sanity check) Suppose both Alice and Bob choose points S_A, S_B from the same torsion group $E[2^n]$. Find the curve $E_{AB} := E/\langle S_A, S_B\rangle$ (with high probability).

(b) We will go through the SIDH key exchange:

i. For $p = 431$, we have $p + 1 = 432 = 2^4 \cdot 3^3$. Let $E : y^2 = x^3 + x/\mathbb{F}_p^2$.

ii. Verify that $E/\mathbb{F}_{p^2}$ has $(p + 1)^2$ points. Supersingular elliptic curves have very special group structure, which implies that $E[2^4], E[3^3] \subset E(\mathbb{F}_q)$ (see Theorem 3.7 of Schoof or, in more generality, Theorem 1.b) of Lenstra).

iii. Set up the parameters: find a basis $P_A, Q_A \subset E[2^4]$ and a basis $P_B, Q_B \subset E[3^3]$.

iv. Pick a secret point $S_A := m_A P_A + n_A Q_A$ for Alice; pick a secret point $S_B := m_B P_B + n_B Q_B$ for Bob. (Set $m_A = m_B = 1$, we do this in practice and it's easier.)

v. Compute the 16-isogeny $\varphi_A : E \to E_A := E/\langle R_A\rangle$ and the images of P_B, Q_B under φ_A. In practice, such isogenies are computed as chains of 2-isogenies, which is rather efficient.

vi. Symmetrically, compute the 27-isogeny $\varphi_B : E \to E_B := E/\langle R_B\rangle$ and the images of P_A, Q_A under φ_B.

vii. Compute the 16-isogeny $E_B \to E_{BA} := E_B/\langle m_A\varphi_B(P_A) + n_A\varphi_B(Q_A)\rangle$, which is the isogeny Alice computes to complete the SIDH square.

viii. Compute the isogeny 27-isogeny $E_A \to E_{AB} := E_A/\langle m_B\varphi_A(P_B) + n_B\varphi_A(Q_B)\rangle$, which is the isogeny Bob computes to complete the SIDH square.

ix. Finally, compare the j-invariants of E_{AB} and E_{BA}.

5. ("Effective Deuring Correspondence") This is an open-ended exercise to let you think about how to match maximal orders and ideals to supersingular elliptic curves. The state of the art version of translating ideals to isogenies underlines the SQISign signature scheme (eprint 2020/1240).

For your favourite small prime, $p = 67$, determine the endomorphism rings of all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$:

(a) List all the maximal orders in $B_{p,\infty}$;

(b) Find the connecting ideals for some of these orders;

Note that you can build them as follows: for maximal orders $\mathcal{O}_1, \mathcal{O}_2$:

- Let $N = [\mathcal{O}_1 : \mathcal{O}_1 \cap \mathcal{O}_2]$. Compute intersections using `O1 meet O2;`

- Then take $I := N\mathcal{O}_1 + N\mathcal{O}_1\mathcal{O}_2$.
  You can define such ideals using `LeftIdeal(Order ,Generators)` where Generators is any tuple.
- Verify that this ideal is integral.
- Verify that it is a left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal;
- Compute its norm.

(c) List all the supersingular j-invariants;

(d) Start from an elliptic curve with 'known' endomorphism ring, e.g. $E : y^2 = x^3 - x$;

(e) For small ℓ, compare the ℓ-isogenies between the elliptic curves and ideals of norm ℓ. Use (3e) to narrow down the orders for elliptic curves defined over $\mathbb{F}_p$.

(f) Note that for curves for which you do know the endomorphism ring, you can use the kernel ideals. Every isogeny φ corresponds to the kernel ideal $I_\varphi := \{\alpha \in \mathcal{O} : \alpha_{|\ker\varphi} = 0\}$. For instance, the ideal $(\ell, \pi - 1) \leftrightarrow (\ell, j - 1)$ corresponds to the subgroup of E on which Frobenius acts like identity. This approach can help you identify some of the edges (especially for curves over $\mathbb{F}_p$).

You can find more things that will help you distinguish the orders and match them to elliptic curves in Cervino and Lauter and McMurdy and in the WIN-4 collaboration.

6. (Quaternion algebras and Matrix rings) Let B be a quaternion algebra over $\mathbb{Q}$ with basis $1, i, j, k$ with $i^2 = a$ and $j^2 = b$ and $ij = -ji$. Check that B embeds into the matrix ring

$$B \to M_2(\mathbb{Q}(\sqrt{a})),$$
$$x + yi + zj + wk \mapsto \begin{pmatrix} x + y\sqrt{a} & b(z + t\sqrt{a}) \\ z - t\sqrt{a} & x - y\sqrt{a} \end{pmatrix}.$$

so quaternion algebras naturally live in matrix rings. Moreover, localizing we almost always get the matrix ring

$$B \otimes \mathbb{Q}_\ell = M_2(\mathbb{Q}_\ell);$$

this holds for all but finitely many primes, which we call the ramified primes - these are exactly the primes that divide the discriminant.

Hints, comments, commands

1. (a) Supersingular isogeny graphs are $k = \ell + 1$-regular, so the largest two eigenvalues of the adjacency matrix are $k = \ell + 1$ and μ_1.
   From Kristin's lecture, we know that $\mu_1 \leq 2\sqrt{k-1} = 2\sqrt{\ell}$.

   (b) The spectral gap is $k - \mu_1$, the expansion constant is bounded below by $\frac{2(k-\mu_1)}{3k-2\mu_1}$. The smaller the eigenvalue, the better the expansion constant. You can compute it in Sage using `.cheegner_constant()`.

   (c) SIGs have very short diameters, about $\log(p)$. However, paths used in SIDH/SIKE have significantly shorter length, about $e \approx 1/2 \log p$. The subgraph reached in e steps in the ℓ-isogeny graph is very close to a tree (so looks nothing like an expander!), see for instance eprint 2020/439.

   Note on $p \equiv 1 \bmod 12$. For $p \not\equiv 1 \bmod 12$, these definitions are no longer completely correct, because the graph is no longer $\ell + 1$-regular, because of the choice we need to make at the vertices with extra automorphisms.
   To make the isogeny graphs undirected, we identify an isogeny with its dual. Hence, we identify isogenies up to *post-composition* with automorphisms. Now, let ρ be an automorphism of a curve E with $\rho \neq \pm 1$ (the map $P \mapsto -P$ is a non-trivial automorphism, but it preserves subgroups, hence it preserves kernels of isogenies). Take any isogeny φ. Then if $\rho \ker \varphi \neq \varphi$, then the isogenies φ and $\varphi \circ \rho$ are different. But, taking dual isogenies:

   $$\widehat{\varphi \circ \rho} = \hat{\rho} \circ \hat{\varphi},$$

   which is an isogeny *post-composed* with an automorphism. Hence, it is equivalent in the supersingular isogeny graph to $\hat{\varphi}$. So we are forced to identify the edges corresponding to the isogenies $\varphi \sim \hat{\varphi} \sim \widehat{\varphi\rho} \sim \varphi \circ \rho$. So there will not be enough edges from the vertices with special automorphisms.

2. The choice of r should be familiar to you if you have tried to find supersingular elliptic curves using the CM method: you were looking for a supersingular reduction of an elliptic curve with CM by an order in $\mathbb{Q}(\sqrt{-r})$. Moreover, because $r \equiv 3 \bmod 4$ and the class number of such an order is odd (exercise!), there will be a curve E with j-invariant already in $\mathbb{F}_p$.

   But the reduction of isogenies is injective, so you know that $\mathbb{Q}(\sqrt{-r}) \hookrightarrow B_{p,\infty} = \mathrm{End}(E) \otimes \mathbb{Q}$. Moreover, this imaginary quadratic field cannot commute with Frobenius, because these endomorphisms of E cannot be defined over $\mathbb{F}_p$: we know that $\mathrm{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p})$ with $\sqrt{-p} \leftrightarrow \mathrm{Frob}$. You still need to argue that $\sqrt{-r}$ anticommutes with Frobenius.

   Discriminants. There is a notion of discriminant for all orders in the quaterion algebra. Moreover, an order is maximal if and only if its discriminant is equal to the discriminant of the quaternion algebra. For orders in inclusion, you can read off the relative index from the discriminant, for Magma it is just the cofactor. You can easily check inclusion, for instance by simple checking membership for each basis member.

3. Deuring's correspondence can be written in two ways:

   - j-invariants (up to conjugation in $\mathbb{F}_{p^2}$, that is, $j \mapsto j^p$) correspond to maximal orders up to isomorphism of maximal orders (that is, conjugation in the quaternion algebra B - Skolem Noether);

- Starting from an elliptic curve E, the left ideal classes in $\mathcal{O} := \mathrm{End}(E)$ correspond to supersingular elliptic curves, such that if $E1 \leftrightarrow \mathcal{O}_1$ then the right order can be identified with $O_R(I) = \mathrm{End}(O_1)$.

For j-invariants in $\mathbb{F}_p^2$, the endomorphism rings of supersingular elliptic curves with j-invariants j and j^p are isomorphic as orders in the quaternion algebra, even though the curves are not isomorphic. So if you find 6 left ideal classes and 4 non-isomorphic maximal orders, you see that exactly 2 supersingular j-invariants are in $\mathbb{F}_p$.

Curves over $\mathbb{F}_p$. Curves over $\mathbb{F}_p$ have the Frobenius endomorphism in their endomorphism ring, which is an endomorphism of norm p and trace 0.

You can use the `GramMatrix`, which is the Gram matrix for the inner product $\langle x, y\rangle$ on the maximal order satisfying

$$\langle x, y\rangle = \mathrm{Norm}(x + y) - \mathrm{Norm}(x) - \mathrm{Norm}(y),$$

So we have $\mathrm{Norm}(x) = \frac{1}{2}\langle x, x\rangle$.

You can create a quadratic form for the order O : `QuadraticForm(GramMatrix(O));`.

So you need to represent the element $2p$ in this quadratic form. Note that $\mathrm{Tr}(x) = 0$ means that the first coordinate can be set to 0 (if the order has 1 in its basis). But Magma doesn't naturally create orders with 1 in the basis, so you can't just set $a = 0$.