Problem 4

Optimal KLPT

by Péter Kutas

1 Introduction

The Deuring correspondence provides a relation between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and maximal orders of the rational quaternion algebra ramified at p and infinity. More precisely, it can be described as an equivalence of categories where on the geometry side one has supersingular elliptic curves modulo Galois conjugacy (i.e., a curve is considered to be equivalent to the image curve of the Frobenius isogeny) together with isogenies as the morphism. On the algebra side, one has maximal orders together with ideals that are left ideals of one maximal order (representing the domain of the isogeny) and right ideals of another maximal order (representing the codomain of the isogeny).

From a mathematical viewpoint, the Deuring correspondence allows one to move between algebra and geometry. The algebraic viewpoint is especially useful for proving theoretical statements such as the connectedness of isogeny graphs and the number of supersingular elliptic curves. Categorical equivalences are always powerful tools for proving statements, but one might wonder how one can algorithmically move between the quaternion and the elliptic curve worlds.

Computing the endomorphism ring of a supersingular elliptic curve is supposed to be a hard problem. This in the above language means that it is hard to move from geometry to algebra. As it turns out, there is a polynomial-time algorithm that computes a supersingular elliptic curve whose endomorphism ring is a given maximal order. In order to understand this problem, we need to understand variants of the isogeny problem on the quaternion side.

There is a standard terminology (using scheme theoretical kernels) that shows how the Deuring correspondence is obtained. Here, I will show a different viewpoint that is much more useful in understanding KLPT variants. Let E_1 and E_2 be supersingular elliptic curves and let $\phi : E_1 \to E_2$ be an isogeny. The goal is to associate an algebraic object to this isogeny. The trick is to compose ϕ with $\mathrm{Hom}(E_2, E_1)$ the collection of all isogenies from E_2 to E_1. Now we obtain a collection of endomorphisms of E_1 and this set is closed under addition and post-composition by an endomorphism of E_1. This is exactly the definition of a left ideal. If I compose ϕ with $\mathrm{Hom}(E_2, E_1)$ in the other direction I get a collection of endomorphisms of E_2 which now will have the structure of a right ideal of $\mathrm{End}(E_2)$.

This viewpoint essentially shows that taking any connecting ideal essentially parametrizes all isogenies between the two elliptic curves. Furthermore, every element of the left ideal has a degree that is divisible by the degree of ϕ. In

quaternion land this is translated into the definition of the norm of an ideal which is defined to be the greatest common divisor of all the norms in the ideal. This provides us with a definition of the quaternion isogeny path problem:

Problem 4.1: *Given two (isomorphism classes of) maximal orders O_1 and O_2, find a connecting ideal of norm l^k where l is given small prime.*

This definition while correct is not very useful in practice. It is much more useful to start out with some connecting ideal I which is actually very easy to find. the drawback now is that a priori we have no real control over the norm of I. However, as described before one ideal parametrizes all isogenies in some sense. One can now simply show that the quaternion path finding problem is equivalent to finding a single element $x \in I$ such that $n(x) = n(I)l^k$. From now on we focus on this problem, namely given an ideal I find an element of prescribed norm.

2 Description of KLPT

Now at this point we can ask ourselves two things. First, is there a polynomial-time algorithm to find any path where k can be bounded by a function of p (independent on the representation of the ideal). The second question, can we find a path where k is the smallest possible. The distinction is more evident in a graph theoretic language. The first problem asks for any path in the l-isogeny graph whereas the second asks for the shortest one. This leads us to the statement of "Optimal KLPT" as an optimal variant of Problem 4.1.

Problem 4: The Optimal Quaternion Isogeny Path Problem

Given a prime number p, a maximal order O and a left integral O-ideal I, find an equivalent ideal $J \sim I$ of norm $N(J) = \ell^e$ where e is as small as possible.

A solution consists of either: the description of a polynomial-time algorithm, ***OR****, a solution shows that such an algorithm cannot exist.*

The good news is that the easier problem can be solved in polynomial time via the KLPT algorithm. The high level idea of the KLPT algorithm is the following. Let N be the norm of the ideal I. Now we want to find an element in I whose norm is Nl^k. First we choose an endomorphism σ of degree Nl^k and look at the left ideal J generated by σ and N. Now J is great as it comes equipped with an element that we would like. The problem is we want this element in I. The idea is to rotate J into I in some sense. Both I and J are locally principal ideals. When one looks at maximal orders modulo N they become isomorphic to the ring of 2×2 matrices over $\mathbb{Z}/N\mathbb{Z}$. For simplicity, KLPT uses an initial connecting ideal of prime norm, so ideals in the matrix ring are a bit easier to handle. Now viewing I and J modulo N we can view them as left ideals in the matrix ring. Due to the way I and J were chosen they both represent non-trivial ideals (neither 0 nor the whole ring) and since

2 is a very small number every left ideal that is not trivial is 1-dimensional. Furthermore, every two non-trivial ideals differ by right multiplication by an invertible element. So now I can choose an element like that and multiply J from the right to get to I (this is my local rotation). Luckily J was nice so if this rotator matrix has norm l^k I would be done. Unfortunately, this should not be the case usually. On the other hand there are two hopeful things:

1. The rotator matrix is not unique, there are several invertible elements that take one left ideal to the other
2. These elements live in O/NO, so when considered as quaternion they have infinitely many lifts to choose from

KLPT uses both observations. It chooses a very special rotator matrix and then lifts it to a power of l norm quaternion.

3 Problems and Improvements

The drawback of KLPT is that the path that it returns is way longer than the optimal path. How inherent is that from the method itself. Given that I is generated by some element z and N it is natural to consider some form of lifting. The element z can be viewed as a 2×2 matrix that needs to be lifted to a quaternion of norm l^k. However, in KLPT this z was obtained as a product of very special structure. So whilst lifting is some inherent in the problem, the fact that the verbatim KLPT approach can't be improved further is not a roadblock to better algorithms. Furthermore, KLPT makes several choices to ensure that the associated Diophantine equation is solvable with elementary methods. It is highly likely, that major improvements will not come from mild adjustments of KLPT.

A different approach is laid out in [BKM+24] and [AAF+25]. As described before the entire problem can be written down by one simple norm equation: representing Nl^k by the norm form of the ideal. Actually when one writes down this norm equation one can simply divide out by N and then one obtains the quadratic form associated to $\mathrm{Hom}(E_1, E_2)$ representing the integer l^k. If l^k is small, more precisely, smaller than $\sqrt{p}$, then this approach works very easily as it will likely be the shortest isogeny in $\mathrm{Hom}(E_1, E_2)$ and thus LLL will reveal it. If one computes an LLL reduced basis of $\mathrm{Hom}(E_1, E_2)$, then the coordinates of a short isogeny are also somewhat short. This leads to the idea of solving the quaternion norm equation using Coppersmith methods. As it turns out, if $l^k < p^{2/3-\epsilon}$ for any $\epsilon > 0$, this approach works. Unfortunately, for two random curves the expected lower bound should be around p so the above method only works in special circumstances. The drawback of this method is it treats the problem as a random Diophantine equation and likely the problem has more structure to exploit.

4 Conclusion

An optimal pathfinding algorithm would have many great applications. It would simplify maximal order to elliptic curve computations. This is of course polynomial time but costly in practice. The second application would be likely the best available SQIsign variant with all the good properties of all SQIsign variants. In some sense it would be the "Book" version of SQIsign using the terminology of Erdős.

The lack of an optimal KLPT algorithm is a major gap in our algorithmic understanding of the Deuring correspondence. In my humble of opinion, as the SIDH showed the right way to interpret torsion point information, an optimal KLPT will show how to properly view the Deuring correspondence.

Acknowledgements. Péter Kutas is partially supported by Engineering and Physical Sciences Research Council (EPSRC) grant number EP/V011324/1. Péter Kutas is supported by the Ministry of Culture and Innovation and the National Research, Development, and Innovation Office within the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004). Péter Kutas is also supported by the NRDIO grant "EXCELLENCE-151343".

References

[AAF+25] Marius A Aardal, Diego F Aranha, Yansong Feng, Yiming Gao, and Yanbin Pan. "Better Bounds for Finding Fixed-Degree Isogenies via Coppersmith's Method". In: *Cryptology ePrint Archive* (2025) (cit. on p. 3).

[BKM+24] Benjamin Benčina, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Miha Stopar, and Charlotte Weitkämper. "Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves". In: *Annual International Cryptology Conference*. Springer. 2024, pp. 183–217 (cit. on p. 3).