Ramanujan graphs in cryptography

Anamaria Costache[1], Brooke Feigon[2], Kristin Lauter[3], Maike Massierer[4], and Anna Puskás[5]

[1]Department of Computer Science, University of Bristol, Bristol, UK, anamaria.costache@bristol.ac.uk
[2]Department of Mathematics, The City College of New York, CUNY, NAC 8/133, New York, NY 10031, bfeigon@ccny.cuny.edu *
[3]Microsoft Research, One Microsoft Way, Redmond, WA 98052, klauter@microsoft.com
[4]School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia, maike.massierer@gmail.com †
[5]Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, puskas@math.umass.edu

Abstract

In this paper we study the security of a proposal for Post-Quantum Cryptography from both a number theoretic and cryptographic perspective. Charles–Goren–Lauter in 2006 [CGL06] proposed two hash functions based on the hardness of finding paths in Ramanujan graphs. One is based on Lubotzky–Phillips–Sarnak (LPS) graphs and the other one is based on Supersingular Isogeny Graphs. A 2008 paper by Petit–Lauter–Quisquater breaks the hash function based on LPS graphs. On the Supersingular Isogeny Graphs proposal, recent work has continued to build cryptographic applications on the hardness of finding isogenies between supersingular elliptic curves. A 2011 paper by De Feo–Jao–Plût proposed a cryptographic system based on Supersingular Isogeny Diffie–Hellman as well as a set of five hard problems. In this paper we show that the security of the SIDH proposal relies on the hardness of the SSIG path-finding problem introduced in [CGL06]. In addition, similarities between the number theoretic ingredients in the LPS and Pizer constructions suggest that the hardness of the path-finding problem in the two graphs may be linked. By viewing both graphs from a number theoretic perspective, we identify the similarities and differences between the Pizer and LPS graphs.

Keywords: Post-Quantum Cryptography, supersingular isogeny graphs, Ramanujan graphs
2010 Mathematics Subject Classification: Primary: 05C25, 14G50; Secondary: 22F70, 11R52

1 Introduction

Supersingular Isogeny Graphs were proposed for use in cryptography in 2006 by Charles, Goren, and Lauter [CGL06]. Supersingular isogeny graphs are examples of Ramanujan graphs, i.e. optimal expander graphs. This means that relatively *short* walks on the graph approximate the uniform distribution, i.e. walks of length approximately equal to the logarithm of the graph size. Walks

*Partially supported by National Security Agency grant H98230-16-1-0017 and PSC-CUNY.
†Partially supported by Australian Research Council grant DP150101689.

on expander graphs are often used as a good source of randomness in computer science, and the reason for using *Ramanujan* graphs is to keep the path length short. But the reason these graphs are important for cryptography is that *finding paths* in these graphs, i.e. *routing,* is hard: there are no known subexponential algorithms to solve this problem, either classically or on a quantum computer. For this reason, systems based on the hardness of problems on Supersingular Isogeny Graphs are currently under consideration for standardization in the NIST Post-Quantum Cryptography (PQC) Competition [PQC].

[CGL06] proposed a general construction for cryptographic hash functions based on the hardness of inverting a walk on a graph. The path-finding problem is the following: given fixed starting and ending vertices representing the start and end points of a walk on the graph of a fixed length, find a path between them. A hash function can be defined by using the input to the function as directions for walking around the graph: the output is the label for the ending vertex of the walk. Finding collisions for the hash function is equivalent to finding cycles in the graph, and finding pre-images is equivalent to path-finding in the graph. Backtracking is not allowed in the walks by definition, to avoid trivial collisions.

In [CGL06], two concrete examples of families of optimal expander graphs (Ramanujan graphs) were proposed, the so-called Lubotzky–Phillips–Sarnak (LPS) graphs [LPS88], and the Supersingular Isogeny Graphs (Pizer) [Piz98], where the path finding problem was supposed to be hard. Both graphs were proposed and presented at the 2005 and 2006 NIST Hash Function workshops, but the LPS hash function was quickly attacked and broken in two papers in 2008, a collision attack [TZ08] and a pre-image attack [PLQ08]. The preimage attack gives an algorithm to efficiently find paths in LPS graphs, a problem which had been open for several decades. The PLQ path-finding algorithm uses the explicit description of the graph as a Cayley graph in $\mathrm{PSL}_2(\mathbb{F}_p)$, where vertices are 2×2 matrices with entries in $\mathbb{F}_p$ satisfying certain properties. Given the swift discovery of attacks on the LPS path-finding problem, it is natural to investigate whether this approach is relevant to the path-finding problem in Supersingular Isogeny (Pizer) Graphs.

In 2011, De Feo–Jao–Plût [DFJP14] devised a cryptographic system based on supersingular isogeny graphs, proposing a Diffie–Hellman protocol as well as a set of five hard problems related to the security of the protocol. It is natural to ask what is the relation between the problems stated in [DFJP14] and the path-finding problem on Supersingular Isogeny Graphs proposed in [CGL06].

In this paper we explore these two questions related to the security of cryptosystems based on these Ramanujan graphs. In Part 1 of the paper, we study the relation between the hard problems proposed by De Feo–Jao–Plût and the hardness of the Supersingular Isogeny Graph problem which is the foundation for the CGL hash function. In Part 2 of the paper, we study the relation between the Pizer and LPS graphs by viewing both from a number theoretic perspective.

In particular, in Part 1 of the paper, we clearly explain how the security of the Key Exchange protocol relies on the hardness of the path-finding problem in SSIG, proving a reduction (Theorem 3.2) between the Supersingular Isogeny Diffie Hellmann (SIDH) Problem and the path-finding problem in SSIG. Although this fact and this theorem may be clear to the experts (see for example the comment in the introduction to a recent paper on this topic [AAM18]), this reduction between the hard problems is not written anywhere in the literature. Furthermore, the Key Exchange (SIDH) paper [DFJP14] states 5 hard problems, including (SSCDH), with relations proved between some but not all of them, and mentions the paper [CGL06] only in passing (on page 17), with no clear statement of the relationship to the overarching hard problem of path-finding in SSIG.

Our Theorem 3.2 clearly shows the fact that the security of the proposed post-quantum key

exchange relies on the hardness of the path-finding problem in SSIG stated in [CGL06]. Theorem 4.9 counts the chains of isogenies of fixed length. Its proof relies on elementary group theory results and facts about isogenies, proved in Section 4.

In Part 2 of the paper, we examine the LPS and Pizer graphs from a number theoretic perspective with the aim of highlighting the similarities and differences between the constructions.

Both the LPS and Pizer graphs considered in [CGL06] can be thought of as graphs on

$$\Gamma \backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l), \tag{1}$$

where Γ is a discrete cocompact subgroup, where Γ is obtained from a quaternion algebra B. We show how different input choices for the construction lead to different graphs. In the LPS construction one may vary Γ to get an infinite family of Ramanujan graphs. In the Pizer construction one may vary B to get an infinite family. In the LPS case, we always work in the Hamiltonian quaternion algebra. For this particular choice of algebra we can rewrite the graph as a Cayley graph. This explicit description is key for breaking the LPS hash function. For the Pizer graphs we do not have such a description. On the Pizer side the graphs may, via Strong Approximation, be viewed as graphs on adèlic double cosets which are in turn the class group of an order of B that is related to the cocompact subgroup Γ. From here one obtains an isomorphism with supersingular isogeny graphs. For LPS graphs the local double cosets are also isomorphic to adèlic double cosets, but in this case the corresponding set of adèlic double cosets is smaller relative to the quaternion algebra and we do not have the same chain of isomorphisms.

Part 2 has the following outline. Section 6 follows [Lub10] and presents the construction of LPS graphs from three different perspectives: as a Cayley graph, in terms of local double cosets, and, to connect these two, as a quotient of an infinite tree. The edges of the LPS graph are explicit in both the Cayley and local double coset presentation. In Section 6.4 we give an explicit bijection between the natural parameterizations of the edges at a fixed vertex. Section 7 is about Strong Approximation, the main tool connecting the local and adelic double cosets for both LPS and Pizer graphs. Section 8 follows [Piz98] and summarizes Pizer's construction. The different input choices for LPS and Pizer constructions impose different restrictions on the parameters of the graph, such as the degree. 6-regular graphs exist in both families. In Section 8.2 we give a set of congruence conditions for the parameters of the Pizer construction that produce a 6-regular graph. In Section 9 we summarize the similarities and differences between the two constructions.

1.1 Acknowledgments

This project was initiated at the Women in Numbers 4 (WIN4) workshop at the Banff International Research Station in August, 2017. The authors would like to thank BIRS and the WIN4 organizers. In addition, the authors would like to thank the Clay Mathematics Institute, PIMS, Microsoft Research, the Number Theory Foundation and the NSF-HRD 1500481 - AWM ADVANCE grant for supporting the workshop. We thank John Voight, Scott Harper, and Steven Galbraith for helpful conversations, and the anonymous referees for many helpful suggestions and edits.

Part 1
Cryptographic applications of supersingular isogeny graphs

In this section we investigate the security of the [DFJP14] key-exchange protocol. We show a reduction to the path-finding problem in supersingular isogeny graphs stated in [CGL06]. The hardness of this problem is the basis for the CGL cryptographic hash function, and we show here that if this problem is not hard, then the key exchange presented in [DFJP14] is not secure.

We begin by recalling some basic facts about isogenies of elliptic curves and the key-exchange construction. Then, we give a reduction between two hardness assumptions. This reduction is based on a correspondence between a path representing the composition of m isogenies of degree ℓ and an isogeny of degree ℓ^m.

2 Preliminaries

We start by recalling some basic and well-known results about isogenies. They can all be found in [Sil09]. We try to be as concrete and constructive as possible, since we would like to use these facts to do computations.

An elliptic curve is a curve of genus one with a specific base point $\mathcal{O}$. This latter can be used to define a group law. We will not go into the details of this, see for example [Sil09]. If E is an elliptic curve defined over a field K and $\mathrm{char}(\bar{K}) \neq 2, 3$, we can write the equation of E as

$$E : y^2 = x^3 + a \cdot x + b,$$

where $a, b \in K$. Two important quantities related to an elliptic curve are its discriminant Δ and its j-invariant, denoted by j. They are defined as follows.

$$\Delta = 16 \cdot (4 \cdot a^3 + 27 \cdot b^2) \quad \text{and} \quad j = -1728 \cdot \frac{a^3}{\Delta}.$$

Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.

Definition 2.1. *Let E_0 and E_1 be two elliptic curves. An isogeny from E_0 to E_1 is a surjective morphism*

$$\phi : E_0 \to E_1,$$

which is a group homomorphism.

An example of an isogeny is the multiplication-by-m map $[m]$,

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto m \cdot P. \end{aligned}$$

The degree of an isogeny is defined as the degree of the finite extension $\bar{K}(E_0)/\phi^*(\bar{K}(E_1))$, where $\bar{K}(*)$ is the function field of the curve, and ϕ^* is the map of function fields induced by the isogeny ϕ. By convention, we set

$$\deg([0]) = 0.$$

The degree map is multiplicative under composition of isogenies:

$$\deg(\phi \circ \psi) = \deg(\phi) \cdot \deg(\psi)$$

for all chains $E_0 \xrightarrow{\phi} E_1 \xrightarrow{\psi} E_2$, and for an integer $m > 0$, the multiplication-by-m map has degree m^2.

Theorem 2.2. *[Sil09] Let $E_0 \to E_1$ be an isogeny of degree m. Then, there exists a unique isogeny*

$$\hat{\phi} : E_1 \to E_0$$

such that $\hat{\phi} \circ \phi = [m]$ on E_0, and $\phi \circ \hat{\phi} = [m]$ on E_1. We call $\hat{\phi}$ the dual isogeny to ϕ. We also have that

$$\deg(\hat{\phi}) = \deg(\phi).$$

For an isogeny ϕ, we say ϕ is separable if the field extension $\bar{K}(E_0)/\phi^*(\bar{K}(E_1))$ is separable. We then have the following lemma.

Lemma 2.3. *Let $\phi : E_0 \to E_1$ be a separable isogeny. Then*

$$\deg(\phi) = \#\ker(\phi).$$

In this paper, we only consider separable isogenies and frequently use this convenient fact. From the above, it follows that a point P of order m defines an isogeny ϕ of degree m,

$$\phi : E \to E/\langle P \rangle.$$

We will refer to such an isogeny as a cyclic isogeny (meaning that its kernel is a cyclic subgroup of E). For ℓ prime, we also say that two curves E_0 and E_1 are ℓ-isogenous if there exists an isogeny $\phi : E_0 \to E_1$ of degree ℓ.

We define $E[m]$, the m-torsion subgroup of E, to be the kernel of the multiplication-by-m map. If $\mathrm{char}(K) > 0$ and $m \geq 2$ is an integer coprime to $\mathrm{char}(K)$, or if $\mathrm{char}(K) = 0$, then the points of $E[m]$ are

$$E[m] = \{P \in E(\bar{K}) : m \cdot P = \mathcal{O}\} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

If an elliptic curve E is defined over a field of characteristic $p > 0$ and its endomorphism ring over $\bar{K}$ is an order in a quaternion algebra, we say that E is supersingular. Every isomorphism class over $\bar{K}$ of supersingular elliptic curves in characteristic p has a representative defined over $\mathbb{F}_{p^2}$, thus we will often let $K = \mathbb{F}_{p^2}$ (for some fixed prime p).

We mentioned above that an ℓ-torsion point P induces an isogeny of degree ℓ. More generally, a finite subgroup G of E generates a unique isogeny of degree $\#G$, up to automorphism.

Supersingular isogeny graphs were introduced into cryptography in [CGL06]. To define a supersingular isogeny graph, fix a finite field K of characteristic p, a supersingular elliptic curve E over K, and a prime $\ell \neq p$. Then the corresponding isogeny graph is constructed as follows. The vertices are the $\bar{K}$-isomorphism classes of elliptic curves which are $\bar{K}$-isogenous to E. Each vertex is labeled with the j-invariant of the curve. The edges of the graph correspond to the ℓ-isogenies between the elliptic curves. As the vertices are isomorphism classes of elliptic curves, isogenies that differ by composition with an automorphism of the image are identified as edges of the graph. I.e. if E_0, E_1 are $\bar{K}$-isogenous elliptic curves, $\phi : E_0 \to E_1$ is an ℓ-isogeny and $\epsilon \in \mathrm{Aut}(E_1)$ is an automorphism, then ϕ and $\epsilon \circ \phi$ are identified and correspond to the same edge of the graph.

If $p \equiv 1 \mod 12$, we can uniquely identify an isogeny with its dual to make it an undirected graph. It is a multigraph in the sense that there can be multiple edges if no extra conditions are imposed on p. Three important properties of these graphs follow from deep theorems in number theory:

1. The graph is connected for any $\ell \neq p$ (special case of [CGL09, Theorem 4.1]).

2. A supersingular isogeny graph has roughly $p/12$ vertices. [Sil09, Theorem 4.1]

3. Supersingular isogeny graphs are optimal expander graphs, in particular they are Ramanujan. (special case of [CGL09, Theorem 4.2]).

Remark 2.4. In order to avoid trivial collisions in cryptographic hash functions based on isogeny graphs, it is best if the graph has no short cycles. Charles, Goren, and Lauter show in [CGL06] how to ensure that isogeny graphs do not have short cycles by carefully choosing the finite field one works over. For example, they compute that a 2-isogeny graph does not have double edges (i.e. cycles of length 2) when working over $\mathbb{F}_p$ with $p \equiv 1 \bmod 420$. Similarly, we computed that a 3-isogeny graph does not have double edges for $p \equiv 1 \bmod 9240$. Given that $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ and $9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, we conclude that neither the 2-isogeny graph nor the 3-isogeny graph has double edges for $p \equiv 1 \bmod 9240$.

For our experiments (described in Section 4), we were interested in studying short walks, for example of length 4, in a setting relevant to the Key-Exchange protocol described below. The smallest prime p with the property $p \equiv 1 \bmod 9240$ that also satisfies $2^4 \cdot 3^4 \mid p - 1$ is

$$p = 2^4 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 + 1.$$

3 The [DFJP14] key-exchange

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, where $p = \ell_A^n \cdot \ell_B^m \pm 1$, ℓ_A and ℓ_B are primes, and $n \approx m$ are approximately equal. We have players A (for Alice) and B (for Bob), representing the two parties who wish to engage in a key-exchange protocol with the goal of establishing a shared secret key by communicating via a (possibly) insecure channel. The two players A and B generate their public parameters by each picking two points P_A, Q_A such that $\langle P_A, Q_A \rangle = E[\ell_A^n]$ (for A), and two points P_B, Q_B such that $\langle P_B, Q_B \rangle = E[\ell_B^m]$ (for B).

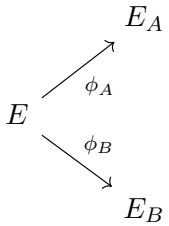
Player A then secretly picks two random integers $0 \leq m_A, n_A < \ell_A^n$. These two integers (and the isogeny they generate) will be player A's secret parameters. A then computes the isogeny ϕ_A

$$E \xrightarrow{\phi_A} E_A := E/\langle [m_A]P_A + [n_A]Q_A \rangle.$$

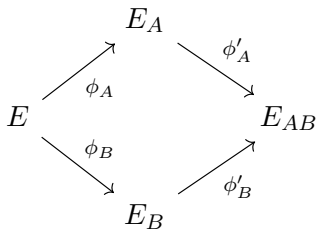
Player B proceeds in a similar fashion and secretly picks $0 \leq m_B, n_B < \ell_B^m$. Player B then generates the (secret) isogeny

$$E \xrightarrow{\phi_B} E_B := E/\langle [m_B]P_B + [n_B]Q_B \rangle.$$

So far, A and B have constructed the following diagram.



To complete the diamond, we proceed to the exchange part of the protocol. Player A computes the points $\phi_A(P_B)$ and $\phi_A(Q_B)$ and sends $\{\phi_A(P_B), \phi_A(Q_B), E_A\}$ along to player B. Similarly, player B computes and sends $\{\phi_B(P_A), \phi_B(Q_A), E_B\}$ to player A. Both players now have enough information to construct the following diagram,



(2)

where

$$E_{AB} \cong E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle.$$

Player A can use the knowledge of the secret information m_A and n_A to compute the isogeny ϕ'_B, by quotienting E_B by $\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$ to obtain E_{AB}. Player B can use the knowledge of the secret information m_B and n_B to compute the isogeny ϕ'_A, by quotienting E_A by $\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle$ to obtain E_{AB}. A separable isogeny is determined by its kernel, and so both ways of going around the diagram from E result in computing the same elliptic curve E_{AB}.

The players then use the j-invariant of the curve E_{AB} as a shared secret.

Remark 3.1. Given a list of points specifying a kernel, one can explicitly compute the associated isogeny using Vélu's formulas [Vél71]. In principle, this is how the two parties engaging in the key-exchange above can compute ϕ_A, ϕ_B, ϕ'_A, ϕ'_B [Vél71]. However, in practice for cryptographic size subgroups, this would be impossible, and thus a different approach is taken, based on breaking the isogenies into n (resp. m) steps, each of degree ℓ_A (resp. ℓ_B). This equivalence will be explained below.

3.1 Hardness assumptions

The security of the key-exchange protocol is based on the following hardness assumption, which was introduced in [DFJP14] and called the Supersingular Computational Diffie–Hellman (SSCDH) problem.

Problem 1. *(Supersingular Computational Diffie–Hellman (SSCDH)): Let p, ℓ_A, ℓ_B, n, m, E, E_A, E_B, E_{AB}, P_A, Q_A, P_B, Q_B be as above.*

Let ϕ_A be an isogeny from E to E_A whose kernel is equal to $\langle [m_A]P_A + [n_A]Q_A \rangle$, and let ϕ_B be an isogeny from E to E_B whose kernel is equal to $\langle [m_B]P_B + [n_B]Q_B \rangle$, where m_A,n_A (respectively m_B,n_B) are integers chosen at random between 0 and ℓ_A^m (respectively ℓ_B^n), and not both divisible by ℓ_A (resp. ℓ_B).

Given the curves E_A, E_B and the points $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$, find the j-invariant of

$$E_{AB} \cong E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle;$$

see diagram (2).

In [CGL06], a cryptographic hash function was defined:

$$h : \{0,1\}^r \to \{0,1\}^s$$

based on the Supersingular Isogeny Graph (SSIG) for a fixed prime p of cryptographic size, and a fixed small prime $\ell \neq p$. The hash function processes the input string in blocks which are used as directions for walking around the graph starting from a given fixed vertex. The output of the hash function is the j-invariant of an elliptic curve over $\mathbb{F}_{p^2}$ which requires $2\log(p)$ bits to represent, so $m = 2\lceil \log(p) \rceil$. For the security of the hash function, it is necessary to avoid the generic *birthday attack*. This attack runs in time proportional to the square root of the size of the graph, which is the *Eichler class number*, roughly $\lfloor p/12 \rfloor$. So in practice, we must pick p so that $\log(p) \approx 256$.

The integer r is the length of the bit string input to the hash function. If $\ell = 2$, which is the easiest case to implement and a common choice, then r is precisely the number of steps taken on the walk in the graph, since the graph is 3-regular, with no backtracking allowed, so the input is processed bit-by-bit. In order to assure that the walk reaches a sufficiently random vertex in the graph, the number of steps should be roughly $\log(p) \approx 256$. A CGL-hash function is thus specified by giving the primes p, ℓ, the starting point of the walk, and the integers $r \approx 256$, s. (Extra congruence conditions were imposed on p to make it an undirected graph with no small cycles.)

The hard problems stated in [CGL06] corresponded to the important security properties of *collision* and *preimage resistance* for this hash function. For preimage resistance, the problem [CGL06, Problem 3] stated was: given p, ℓ, $r > 0$, and two supersingular j-invariants modulo p, to find a path of length r between them:

Problem 2. *(Path-finding [CGL06]) Let p and ℓ be distinct prime numbers, $r > 0$, and E_0 and E_1 two supersingular elliptic curves over $\mathbb{F}_{p^2}$. Find a path of length r in the ℓ-isogeny graph corresponding to a composition of r ℓ-isogenies leading from E_0 to E_1 (i.e. an isogeny of degree ℓ^r from E_0 to E_1).*

It is worth noting that, to break the preimage resistance of the specified hash function, you must find a path of exactly length r, and this is analogous to the situation for breaking the security of the key-exchange protocol. However, the problem of finding *any* path between two given vertices in the SSIG graphs is also still open. For the LPS graphs, the algorithm presented in [PLQ08] did not find a path of a specific given length, but it was still considered to be a "break" of the hash function.

Furthermore, the diameter of these graphs, both LPS and SSIG graphs, has been extensively studied. It is known that the diameter of the graphs is roughly $\log(p)$ (it is $c\log(p)$, where c is a constant between 1 and 2, (see for example [Sar18])). That means that if r is greater than $c\log(p)$, then given two vertices, it is likely that a path of length r between them may exist. The fact that walks of length greater than $c\log(p)$ approximate the uniform distribution very closely means that you are not likely to miss any significant fraction of the vertices with paths of that length, because that would constitute a bias. Also, if $r \gg \log(p)$ then there may be many paths of length r. However, if r is much less than $\log(p)$, such as $\frac{1}{2}\log(p)$, there may be *no path* of such a short length between two given vertices. See [LP15] for a discussion of the "sharp cutoff" property of Ramanujan graphs.

But in the cryptographic applications, given an instance of the key-exchange protocol to be attacked, we *know* that there exists a path of length n between E and E_A, and the hard problem is to find it. The set-up for the key-exchange requires $p = \ell_A^n \ell_B^m \pm 1$, where n and m are roughly the

same size, and ℓ_A and ℓ_B are very small, such as $\ell_A = 2$ and $\ell_B = 3$. It follows that n and m are both approximately half the diameter of the graph (which is roughly $\log(p)$). So it is unlikely to find paths of length n or m between two random vertices. If a path of length n exists and Algorithm A finds a path, then it is very likely to be the one which was constructed in the key exchange. If not, then Algorithm A can be repeated any constant number of times. So we have the following reduction:

Theorem 3.2. *Assume as for the Key Exchange set-up that $p = \ell_A^n \cdot \ell_B^m + 1$ is a prime of cryptographic size, i.e. $\log(p) \geq 256$, ℓ_A and ℓ_B are small primes, such as $\ell_A = 2$ and $\ell_B = 3$, and $n \approx m$ are approximately equal. Given an algorithm to solve Problem 2 (Path-finding), it can be used to solve Problem 1 (Key Exchange) with overwhelming probability. The failure probability is roughly*

$$\frac{\ell_A^n + \ell_A^{n-1}}{p} \approx \frac{\sqrt{p}}{p}.$$

Proof. Given an algorithm (Algorithm A) to solve Problem 2, we can use this to solve Problem 1 as follows. Given E and E_A, use Algorithm A to find the path of length n between these two vertices in the ℓ_A-isogeny graph. Now use Lemma 4.4 below to produce a point R_A which generates the ℓ_A^n-isogeny between E and E_A. Repeat this to produce the point R_B which generates the ℓ_B^m-isogeny between E and E_B in the ℓ_B-isogeny graph. Because the subgroups generated by R_A and R_B have smooth order, it is easy to write R_A in the form $[m_A]P_A + [n_A]Q_A$ and R_B in the form $[m_B]P_B + [n_B]Q_B$. Using the knowledge of m_A, n_A, m_B, n_B, we can construct E_{AB} and recover the j-invariant of E_{AB}, allowing us to solve Problem 1.

The reason for the qualification "with overwhelming probability" in the statement of the theorem is that it is possible that there are multiple paths of the same length between two vertices in the graph. If there are multiple paths of length n (or m) between the two vertices, it suffices to repeat Algorithm A to find another path. This approach is sufficient to break the Key Exchange if there are only a small number of paths to try. As explained above, with overwhelming probability, there are *no* other paths of length n (or m) in the Key Exchange setting.

In the SSIG corresponding to (p, ℓ_A), the vertices E and E_A are a distance of n apart. Starting from the vertex E and considering all paths of length n, the number of possible endpoints is at most $\ell_A^n + \ell_A^{n-1}$ (See Corollary 4.8 below). Considering that the number of vertices in the graph is roughly $\lfloor p/12 \rfloor$, then the probability that a given vertex such as E_A will be the endpoint of one of the walks of length n is roughly

$$\frac{\ell_A^n + \ell_A^{n-1}}{p} \approx \frac{\sqrt{p}}{p} \leq 2^{-128}.$$

This estimate does not use the Ramanujan property of the SSIG graphs. While a generic random graph could potentially have a topology which creates a bias towards some subset of the nodes, Ramanujan graphs cannot, as shown in [LP15, Theorem 3.5]. □

4 Composing isogenies

Let k be a positive integer. Every separable k-isogeny $\phi : E_0 \to E_1$ is determined by its kernel up to composition with an automorphism of the elliptic curve E_1. Thus the edge corresponding to ϕ is uniquely determined by $\ker(\phi)$ and vice versa. This kernel is a subgroup of the k-torsion $E_0[k]$,

and the latter is isomorphic to $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ if k is coprime to the characteristic of the field we are working over.

Hence, fixing a prime ℓ and working over a finite field $\mathbb{F}_q$ which has characteristic different from ℓ, the number of ℓ-isogenies $\phi : E_0 \to E_1$ that correspond to different edges of the graph is equal to the number of subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ of order ℓ. It is well known that this number is equal to $\ell + 1$. In other words, E is ℓ-isogenous to precisely $\ell + 1$ elliptic curves.

However, some of these ℓ-isogenous curves may be isomorphic. Therefore, in the isogeny graph (where nodes represent isomorphism classes of curves), E has degree $\ell + 1$ and may have $\ell + 1$ neighbors or fewer.

Using Vélu's formulas, the equations for an edge can be computed from its kernel. Hence for computational purposes, it is important to write down this kernel explicitly. This is best done by specifying generators. Let $P, Q \in E_0$ be the generators of $E_0[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Then the subgroups of order ℓ are generated by Q and $P + iQ$ for $i = 0, \ldots, \ell - 1$.

We now study isogenies obtained by composition, and isogenies of degree a prime power. It turns out that these correspond to each other under certain conditions. The first condition is that the isogeny is cyclic. Notice that every prime order group is cyclic, therefore all ℓ-isogenies are cyclic (meaning they have cyclic kernel). However, this is not necessarily true for isogenies whose order is not a prime. The second condition is that there is no backtracking, defined as follows:

Definition 4.1. *For a chain of isogenies $\phi_m \circ \phi_{m-1} \circ \ldots \circ \phi_1$ ($\phi_i : E_{i-1} \to E_i$), we say that it has* no backtracking *if $\phi_{i+1} \neq \epsilon \circ \hat{\phi}_i$ for all $i = 1, \ldots, m-1$ and any $\epsilon \in \mathrm{Aut}(E_{i+1})$, since this corresponds to a walk in the ℓ-isogeny graph without backtracking.*

In the following, we show that chains of ℓ-isogenies of length m without backtracking correspond to cyclic ℓ^m-isogenies. Recall that we are only considering separable isogenies throughout.

Lemma 4.2. *Let ℓ be a prime, and let ϕ be a separable ℓ^m-isogeny with cyclic kernel. Then there exist cyclic ℓ-isogenies $\phi_1, \ldots, \phi_m$ such that $\phi = \phi_m \circ \phi_{m-1} \circ \ldots \circ \phi_1$ without backtracking.*

Proof. Assume that $\phi = E_0 \to E$, and that its kernel is $\langle P_0 \rangle \subseteq E_0$, where P_0 has order ℓ^m. For $i = 1, \ldots, m$, let

$$\phi_i : E_{i-1} \to E_i$$

be an isogeny with kernel $\langle \ell^{m-i} P_{i-1} \rangle$, where $P_i = \phi_i(P_{i-1})$.

We show that ϕ_i is an ℓ-isogeny for $i \in \{1, \ldots, m\}$ by observing that $\ell^{m-i} P_{i-1}$ has order ℓ. The statement is trivial for $i = 1$. For $i \geq 2$, clearly $\ell^{m-i} P_{i-1} = \ell^{m-i} \phi_{i-1}(P_{i-2}) = \phi_{i-1}(\ell^{m-i} P_{i-2}) \neq \mathcal{O}$, since $\ell^{m-i} P_{i-2} \notin \ker \phi_{i-1} = \langle \ell^{m-(i-1)} P_{i-2} \rangle = \{\ell^{m-(i-1)} P_{i-2}, 2\ell^{m-(i-1)} P_{i-2}, \ldots, (\ell-1)\ell^{m-(i-1)} P_{i-2}\}$. Furthermore, $\ell \cdot \ell^{m-i} P_{i-1} = \ell^{m-(i-1)} \phi_{i-1}(P_{i-2}) = \phi_{i-1}(\ell^{m-(i-1)} P_{i-2}) = \mathcal{O}$, using the definition of $\ker \phi_{i-1}$.

Next, we show by induction that $\phi_i \circ \ldots \circ \phi_1$ has kernel $\langle \ell^{m-i} P_0 \rangle$. Then it follows that $\phi_m \circ \ldots \circ \phi_1$ is the same as ϕ up to an automorphism ϵ of E, since the two have the same kernel. Replacing ϕ_m with $\epsilon \circ \phi_m$ if necessary we have $\phi = \phi_m \circ \phi_{m-1} \circ \ldots \circ \phi_1$. The case $i = 1$ is trivial: $\phi_1 : E_0 \to E_1$ has kernel $\langle \ell^{m-1} P_0 \rangle$ by definition. Now assume the statement is true for $i - 1$. Then, we have $\langle \ell^{m-i} P_0 \rangle \subseteq \ker \phi_i \circ \ldots \circ \phi_1$. Conversely, let $Q \in \ker \phi_i \circ \ldots \circ \phi_1$. Then $\phi_{i-1} \circ \ldots \circ \phi_i(Q) \in \ker \phi_i = \langle \ell^{m-i} P_{i-1} \rangle = \phi_{i-1}(\langle \ell^{m-i} P_{i-2} \rangle) = \ldots = \phi_{i-1} \circ \ldots \circ \phi_1(\langle \ell^{m-i} P_0 \rangle)$ and hence $Q \in \langle \ell^{m-i} P_0 \rangle + \ker \phi_{i-1} \circ \ldots \circ \phi_1 = \langle \ell^{m-i} P_0 \rangle + \langle \ell^{m-(i-1)} P_0 \rangle = \langle \ell^{m-i} P_0 \rangle$.

Finally, we show that there is no backtracking in $\phi_m \circ \ldots \circ \phi_1$. Contrarily, assume that there is an $i \in \{1, \ldots, m-1\}$ and $\epsilon \in \mathrm{Aut}(E_{i+1})$ such that $\phi_{i+1} = \epsilon \circ \hat{\phi}_i$. Then, since $\ker(\phi_{i+1} \circ \phi_i) = \ker(\epsilon \circ \hat{\phi}_i \circ$

$\phi_i) = \ker[\ell]$, we have $\ker(\phi_{i+1} \circ \phi_i \circ \phi_{i-1} \circ \ldots \circ \phi_1) = \ker([\ell] \circ \phi_{i-1} \circ \ldots \circ \phi_1)$. Notice that $[\ell]$ commutes with all ϕ_j, and hence $E_0[\ell] \subseteq \ker(\phi_{i+1} \circ \phi_i \circ \phi_{i-1} \circ \ldots \circ \phi_1) \subseteq \ker(\phi_m \circ \phi_i \circ \phi_{i-1} \circ \ldots \circ \phi_1) = \ker \phi$. Since $E_0[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, the kernel of ϕ cannot be cyclic, a contradiction. □

Remark 4.3. It is clear that in the above lemma, if ϕ is defined over a finite field $\mathbb{F}_q$, then all ϕ_i are also defined over this field. Namely, if E_0 is defined over $\mathbb{F}_q$ and the kernel is generated by an $\mathbb{F}_q$-rational point, then by Vélu we obtain $\mathbb{F}_q$-rational formulas for ϕ_1, which means that ϕ_1 is defined over $\mathbb{F}_q$, and so on.

Lemma 4.4. *Let ℓ be a prime, let E_i be elliptic curves for $i = 0, \ldots, m$, and let $\phi_i : E_{i-1} \to E_i$ be ℓ-isogenies for $i = 1, \ldots, m$ such that $\phi_{i+1} \neq \epsilon \circ \hat{\phi}_i$ for $i = 1, \ldots, m-1$ and any $\epsilon \in \mathrm{Aut}(E_{i+1})$ (i.e. there is no backtracking). Then $\phi_m \circ \ldots \circ \phi_1$ is a cyclic ℓ^m-isogeny.*

Proof. The degree of isogenies multiplies when they are composed, see e.g. [Sil09, Ch. III.4]. Hence we are left with proving that the composition of the isogenies is cyclic.

First note that all ϕ_i are cyclic since they have prime degree, and denote by $P_{i-1} \in E_{i-1}$ the generators of the respective kernels. Let Q_{m-1} be a point on E_{m-1} such that $\ell Q_{m-1} = P_{m-1}$. Notice that such a point always exists over the algebraic closure of the field of definition of the curve. Let $R_{m-2} = \hat{\phi}_{m-1}(Q_{m-1})$, where the hat denotes the dual isogeny. Then $\phi_m \circ \phi_{m-1}(R_{m-2}) = \phi_m \circ \phi_{m-1} \circ \hat{\phi}_{m-1}(Q_{m-1}) = \phi_m \circ [\ell](Q_{m-1}) = \phi_m(\ell Q_{m-1}) = \phi_m(P_{m-1}) = \mathcal{O}$, and hence R_{m-2} is in the kernel of $\phi_m \circ \phi_{m-1}$.

Next we show that R_{m-2} has order ℓ^2, which implies that it generates the kernel of $\phi_m \circ \phi_{m-1}$. Suppose that $\ell R_{m-2} = \mathcal{O}$. Then $\mathcal{O} = \ell R_{m-2} = \ell \hat{\phi}_{m-1}(Q_{m-1}) = \hat{\phi}_{m-1}(P_{m-1})$. Since P_{m-1} has order ℓ, this implies that P_{m-1} generates the kernel of $\hat{\phi}_{m-1}$. However, P_{m-1} also generates the kernel of ϕ_m, so $\epsilon \circ \hat{\phi}_{m-1} = \phi_m$ for some $\epsilon \in \mathrm{Aut}(E_m)$. But this is a contradiction to the assumption of no backtracking.

By iterating this argument, we obtain a point R_0 which generates the kernel of $\phi_m \circ \ldots \circ \phi_1$, and hence this isogeny is cyclic. □

Combining Lemmas 4.2 and 4.4, we obtain the following correspondence.

Corollary 4.5. *Let ℓ be a prime and m a positive integer. There is a one-to-one correspondence between cyclic separable ℓ^m-isogenies and chains of separable ℓ-isogenies of length m without backtracking. (Here we do not distinguish between isogenies that differ by composition with an automorphism on the image.)*

Next, we investigate how many such isogenies there are. We start by studying ℓ^m-isogenies. The following group theory result is crucial.

Lemma 4.6. *Let ℓ be a prime and m a positive integer. Then the number of subgroups of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order ℓ^m is $\frac{\ell^{m+1}-1}{\ell-1}$, and $\ell^m + \ell^{m-1}$ of these subgroups are cyclic.*

Proof. Every subgroup of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$ for $0 \leq i \leq j \leq m$. The number of subgroups which are isomorphic to $\mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$ is 1 if $i = j$ and $\ell^{j-i} + \ell^{j-i-1}$ otherwise.

A direct consequence of the above statement is that there are

$$\sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} \ell^{m-2i} + \ell^{m-2i-1} + \epsilon_m = \sum_{t=0}^{m} \ell^t$$

subgroups, where $\epsilon_m = 0$ if k is odd and 1 otherwise. This proves the first statement.

For the second statement, let H be a cyclic subgroup of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order l^m. Then H is generated by an element of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order l^m, and contains $l^m - l^{m-1}$ elements of order l^m. Therefore, the number of such subgroups is the number of elements of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order l^m divided by $l^m - l^{m-1}$.

Let (a, b) be an element of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order l^m. Then one of a or b has order l^m. If a has order l^m, then there are $\varphi(\ell^m) = l^m - l^{m-1}$ choices for a, and l^m for b. That is, there are $l^m \cdot (l^m - l^{m-1})$ choices in total.

Otherwise, there are l^{m-1} choices for a (representing the number of elements of order at most l^{m-1}), and $l^m - l^{m-1}$ choices for b. That is, there are $l^{m-1} \cdot (l^m - l^{m-1})$ choices in total. This means the total number of cyclic subgroups of $\mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$ of order l^m is

$$\frac{l^m \cdot (l^m - l^{m-1}) + l^{m-1} \cdot (l^m - l^{m-1})}{l^m - l^{m-1}} = l^m + l^{m-1}.$$

□

Remark 4.7. One could also see the first statement in the lemma above by noting that this is the same as the degree of the Hecke operator T_{ℓ^m} which is $\sigma_1(\ell^m)$. We thank the referee for pointing this out.

Corollary 4.8. *There are $\frac{\ell^{m+1}-1}{\ell-1}$ separable ℓ^m-isogenies originating at a fixed elliptic curve, and $\ell^m + \ell^{m-1}$ of them are cyclic. (Here we are counting isogenies as different if they differ even after composition with any automorphism of the image.)*

Using the correspondence from Corollary 4.5, we then obtain the following.

Theorem 4.9. *The number of chains of ℓ-isogenies of length m without backtracking is $\ell^m + \ell^{m-1}$. (Here we do not distinguish between isogenies that differ by composition with an automorphism on the image.)*

This last result can be observed in a much more elementary way, which is also enlightening. We consider chains of ℓ-isogenies of length m. To analyze the situation, it is helpful to draw a graph similar to an ℓ-isogeny graph but that does *not* identify isomorphic curves. This graph is an $(\ell+1)$-regular tree of depth m. The root of the tree has $\ell+1$ children, and every other node (except the leaves) has ℓ children. The leaves have depth m. It is easy to work out that the number of leaves in this tree is $(\ell+1)\ell^{m-1}$, and this is also equal to the number of paths of length m without backtracking, as stated in Theorem 4.9.

Finally, this graph also helps us count the number of chains of ℓ-isogenies of length m including those that backtrack. By examining the graph carefully, we can see that the number of such walks is $\ell^m + \ell^{m-1} + \ldots + \ell + 1$, and according to Corollary 4.8, this corresponds to the number of ℓ^m-isogenies that are not necessarily cyclic.

These results were also observed experimentally using Sage. The numbers match the results of our experiments for small values of ℓ and m, over various finite fields and for different choices of elliptic curves, see Table 1. Notice that the images under isogenies with distinct kernels may be isomorphic, leading to double edges in an isogeny graph that identifies isomorphic curves. Hence, the number of isomorphism classes of images (i.e. the number of neighbors in the isogeny graph) may be smaller than the number of isogenies stated in the table.

ℓ	m	number of isogenies without backtracking	number of isogenies with backtracking
2	4	24	31
2	5	48	63
2	6	96	127
2	7	192	255
3	4	108	121
3	5	324	364

Table 1: For small fixed ℓ and m, values obtained experimentally for the number of ℓ-isogeny-chains of length m starting at a fixed elliptic curve E without and with backtracking.

Part 2
Constructions of Ramanujan graphs

In this section we review the constructions of two families of Ramanujan graph, LPS graphs and Pizer graphs. Ramanujan graphs are optimal expanders; see Section 5 for some related background. The purpose is twofold. On the one hand we wish to explain how equivalent constructions on the same object highlight different significant properties. On the other hand, we wish to explicate the relationship between LPS graphs and Pizer graphs.

Both families (LPS and Pizer) of Ramanujan graphs can be viewed (cf. [Li96, Section 3]) as a set of "local double cosets", i.e. as a graph on

$$\Gamma\backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l), \tag{3}$$

where Γ is a discrete cocompact subgroup. In both cases, one has a chain of isomorphisms that are used to show these graphs are Ramanujan, and in both cases one may in fact vary parameters to get an infinite family of Ramanujan graphs.

To explain this better, we introduce some notation. Let us choose a pair of distinct primes p and l for an $(l+1)$-regular graph whose size depends on p. (An infinite family of Ramanujan graphs is formed by varying p.) Let us fix a quaternion algebra B defined over $\mathbb{Q}$ and ramified at exactly one finite prime and at ∞, and an order of the quaternion algebra $\mathcal{O}$. Let $\mathbb{A}$ denote the adèles of $\mathbb{Q}$ and $\mathbb{A}_f$ denote the finite adèles. For precise definitions see Section 5.

In the case of Pizer graphs, let $B = B_{p,\infty}$ be ramified at p and ∞, and take $\mathcal{O}$ to be a maximal order (i.e. an order of level p).[1] Then we may construct (as in [Piz98]) a graph by giving its adjacency matrix as a Brandt matrix. (The Brandt matrix is given via an explicit matrix representation of a Hecke operator associated to $\mathcal{O}$.) Then we have (cf. [CGL09, (1)]) a chain of isomorphisms connecting (3) with supersingular isogeny graphs (SSIG) discussed in Part 1 above:

$$(\mathcal{O}[l^{-1}])^\times\backslash \mathrm{GL}_2(\mathbb{Q}_l)/\mathrm{GL}_2(\mathbb{Z}_l) \cong B^\times(\mathbb{Q})\backslash B^\times(\mathbb{A}_f)/B^\times(\hat{\mathbb{Z}}) \cong \mathrm{Cl}\mathcal{O} \cong \mathrm{SSIG}. \tag{4}$$

This can be used (cf. [CGL09, 5.3.1]) to show that the supersingular l-isogeny graph is connected, as well as the fact that it is indeed a Ramanujan graph.

[1] A similar construction exists for a more general $\mathcal{O}$. However, to relate the resulting graph to supersingular isogeny graphs, we require $\mathcal{O}$ to be maximal.

In the case of LPS graphs the choices are very different. Let $B = B_{2,\infty}$ now be the Hamiltonian quaternion algebra. The group Γ in (3) is chosen as a congruence subgroup dependent on p. This leads to a larger graph whose constructions fits into the following chain of isomorphisms:

$$\mathrm{PSL}_2(\mathbb{F}_p) \cong \Gamma(2p)\backslash\Gamma(2) \cong \Gamma(2p)\backslash T \cong \Gamma(2p)\backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l) \cong G'(\mathbb{Q})\backslash H_{2p}/G'(\mathbb{R})K_0^{2p}. \quad (5)$$

The isomorphic constructions and their relationship will be made explicit in Sections 6.1-6.3 and Section 7.2. We shall also explain how properties of the graph, such as its regularity, connectedness and the Ramanujan property, are highlighted by this chain of isomorphisms. For now we give only an overview, to be able to compare this case with that of Pizer graphs. The quotient $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ has a natural structure of an infinite tree T. This tree can be defined in terms of homothety classes of rank two lattices of $\mathbb{Q}_l \times \mathbb{Q}_l$ (see Section 6.2). One may define a group $G' = B^\times/Z(B^\times)$ and its congruence subgroups $\Gamma(2)$ and $\Gamma(2p)$, and show that the discrete group $\Gamma(2)$ acts simply transitively on the tree T, and hence $\Gamma(2p)\backslash T$ is isomorphic to the finite group $\Gamma(2)/\Gamma(2p)$. Using the Strong Approximation theorem, this turns out to be isomorphic to the group $\mathrm{PSL}_2(\mathbb{F}_p)$. The latter has a structure of an $(l+1)$-regular Cayley graph. A second application of the Strong Approximation Theorem with K_0^{2p}, an open compact subgroup of $G'(\mathbb{A}_f)$, shows that H_{2p} is a finite index normal subgroup of $G'(\mathbb{A})$.

Note that an immediate distinction between Pizer and LPS graphs is that the quaternion algebras underlying the constructions are different: they ramify at different finite primes (p and 2, respectively). In addition, the size of the discrete subgroup Γ determining the double cosets of (3) is different in the two cases. Accordingly, the size of the resulting graphs is different as well. We shall see that (under appropriate assumptions on p and l) the Pizer graph has $\frac{p-1}{12}$ vertices, while the LPS graph has order $|\mathrm{PSL}_2(\mathbb{F}_p)| = \frac{p(p^2-1)}{2}$. One may consider an order $\mathcal{O}_{LPS}$ such that $(\mathcal{O}_{LPS}[l^{-1}])^\times \cong \Gamma(2p)$ analogously to the relationship of $\mathcal{O}$ and Γ in the Pizer case and (4). However, this order $\mathcal{O}_{LPS}$ is unlike the Eichler order from the Pizer case. (It has a much higher level.) In particular, there is a discrepancy between the order of the class set $\mathrm{Cl}\mathcal{O}_{LPS}$ and the order of the LPS graph. This is a numerical obstruction indicating that an analogue of the chain (4) for LPS graphs is at the very least not straightforward.

The rest of the paper has the following outline. In Section 6 we explore the isomorphic constructions of LPS graphs from (5). We give the construction as a Cayley graph in Section 6.1. The infinite tree of homothety classes of lattices is given in Section 6.2. In Section 6.3 we explain how local double cosets of the Hamiltonian quaternion algebra connect these constructions. Section 6.4 makes one step of the chain of isomorphisms in (5) completely explicit in the case of $l = 5$ and $l = 13$, and describes how the same can be done in general. In Section 7 we give an overview of how Strong Approximation plays a role in proving the isomorphisms and the connectedness and Ramanujan property of the graphs. In Section 8 we turn briefly to Pizer graphs. We summarize the construction, and explain how various restrictions on the prime p guarantee properties of the graph. Section 8.2 contains the computation of a prime p where the existence of both an LPS and a Pizer construction is guaranteed (for $l = 5$). In Section 9 we say a bit more of the relationship of Pizer and LPS graphs, having introduced more of the objects mentioned in passing above.

Throughout this part of the paper we aim to only include technical details if we can make them fairly self-contained and explicit, and otherwise to give a reference for further information.

5 Background on Ramanujan graphs and adèles

In this section we fix notation and review some definitions and facts that we will be using for the remainder of Part 2.

Expander graphs are graphs where small sets of vertices have many neighbors. For many applications of expander graphs, such as in Part 1, one wants $(l+1)$-regular expander graphs X with l small and the number of vertices of X large. If X is an $(l+1)$-regular graph (i.e. where every vertex has degree $l+1$), then $l+1$ is an eigenvalue of the adjacency matrix of X. All eigenvalues λ satisfy $-(l+1) \leq \lambda \leq (l+1)$, and $-(l+1)$ is an eigenvalue if and only if X is bipartite. Let $\lambda(X)$ be the second largest eigenvalue in absolute value of the adjacency matrix. The smaller $\lambda(X)$ is, the better expander X is. Alon–Boppana proved that for an *infinite* family of $(l+1)$-regular graphs of increasing size, $\liminf_{(X)} \lambda(X) \geq 2\sqrt{l}$ [Alo86]. An $(l+1)$-regular graph X is called Ramanujan if $\lambda(X) \leq 2\sqrt{l}$. Thus an infinite family of Ramanujan graphs are optimal expanders.

For a finite prime p, let $\mathbb{Q}_p$ denote the field of p-adic numbers and $\mathbb{Z}_p$ its ring of integers. Let $\mathbb{Q}_\infty = \mathbb{R}$. We denote the adèle ring of $\mathbb{Q}$ by $\mathbb{A}$ and recall that it is defined as a restricted direct product in the following way,

$$\mathbb{A} = \prod_p{}' \mathbb{Q}_p = \left\{ (a_p) \in \prod_p \mathbb{Q}_p : a_p \in \mathbb{Z}_p \text{ for all but a finite number of } p < \infty \right\}.$$

We denote the ring of finite adèles by $\mathbb{A}_f$, that is

$$\mathbb{A}_f = \prod_{p<\infty}{}' \mathbb{Q}_p = \left\{ (a_p) \in \prod_{p<\infty} \mathbb{Q}_p : a_p \in \mathbb{Z}_p \text{ for all but a finite number of } p \right\}.$$

Let $\mathbb{A}^\times$ denote the idèle group of $\mathbb{Q}$, the group of units of $\mathbb{A}$,

$$\mathbb{A}^\times = \prod_p{}' \mathbb{Q}_p = \left\{ (a_p) \in \prod_p \mathbb{Q}_p^\times : a_p \in \mathbb{Z}_p^\times \text{ for all but a finite number of } p < \infty \right\}.$$

Let B be a quaternion algebra over $\mathbb{Q}$, $B^\times$ the invertible elements of B and $\mathcal{O}$ an order of B. For a prime p let $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Then let

$$B^\times(\mathbb{A}) = \prod_p{}' B^\times(\mathbb{Q}_p) = \left\{ (g_p) \in \prod_p B^\times(\mathbb{Q}_p) : g_p \in \mathcal{O}_p^\times \text{ for all but a finite number of } p < \infty \right\}.$$

More generally for an indexed set of locally compact groups $\{G_v\}_{v \in I}$ with a corresponding indexed set of compact open subgroups $\{K_v\}_{v \in I}$ we may define the restricted direct product of the G_v with respect to the K_v by the following

$$G := \prod_{v \in I}{}' G_v = \left\{ (g_v) \in \prod_{v \in I} G_v : g_v \in K_v \text{ for all but a finite number of } v \right\}.$$

If we define a neighborhood base of the identity as

$$\left\{ \prod_v U_v : U_v \text{ neighborhood of identity in } G_v \text{ and } U_v = K_v \text{ for all but a finite number of } v \right\}$$

then G is a locally compact topological group.

6 LPS Graphs

We describe the LPS graphs used in [CGL06] for a proposed hash function. They were first considered in [LPS88], for further details see also [Lub10]. We shall examine the objects and isomorphisms in (5) in more detail. We review constructions of these graphs in turn as Cayley graphs and graphs determined by rank two lattices or, equivalently, local double cosets. Throughout this section, let l and p be distinct, odd primes both congruent to 1 modulo 4. We shall give constructions of $(l+1)$-regular Ramanujan graphs whose size depends on p. We shall also assume for convenience[2] that $\left(\frac{p}{l}\right) = 1$, i.e. that p is a square modulo l.

6.1 Cayley graph over $\mathbb{F}_p$.

This description follows [LPS88, Section 2]. The graph we are interested in is the Cayley graph of the group $\mathrm{PSL}_2(\mathbb{F}_p)$. We specify a set of generators S below. The vertices of the graph are the $\frac{p(p^2-1)}{2}$ elements of $\mathrm{PSL}_2(\mathbb{F}_p)$. Two vertices $g_1, g_2 \in \mathrm{PSL}_2(\mathbb{F}_p)$ are connected by an edge if and only if $g_2 = g_1 h$ for some $h \in S$.

Next we give the set of generators S. Since $l \equiv 1 \mod 4$ it follows from a theorem of Jacobi [Lub10, Theorem 2.1.8] that there are $l+1$ integer solutions to

$$l = x_0^2 + x_1^2 + x_2^2 + x_3^2; \quad 2 \nmid x_0; \quad x_0 > 0. \tag{6}$$

In this case we will also have $2|x_i$ for all $i > 0$. Let S be the set of solutions of (6). Since $p \equiv 1 \mod 4$ we have $\left(\frac{-1}{p}\right) = 1$. Let $\varepsilon \in \mathbb{Z}$ such that $\varepsilon^2 \equiv -1 \mod p$. Then to each solution of (6) we assign an element of $\mathrm{PGL}_2(\mathbb{Z})$ as follows:

$$(x_0, x_1, x_2, x_3) \mapsto \begin{pmatrix} x_0 + x_1\varepsilon & x_2 + x_3\varepsilon \\ -x_2 + x_3\varepsilon & x_0 - x_1\varepsilon \end{pmatrix}. \tag{7}$$

Note that the matrix on the right-hand side has determinant $l \mod p$. Since $\left(\frac{l}{p}\right) = 1$ this determines an element of $\mathrm{PSL}_2(\mathbb{F}_p)$. The $l+1$ elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ determined by (7) form the set of Cayley generators. Let us abuse notation and denote this set with S as well. This graph is connected. To prove this fact, one may use the theory of quadratic Diophantine equations [LPS88, Proposition 3.3]. Alternately, the chain of isomorphisms (5) proves this fact by relating this Cayley graph to a quotient of a connected graph [Lub10, Theorem 7.4.3]: the infinite tree we shall describe in the next section.

The solutions (x_0, x_1, x_2, x_3) and $(x_0, -x_1, -x_2, -x_3)$ correspond to elements of S that are inverses in $\mathrm{PSL}_2(\mathbb{F}_p)$. Since $|S| = l+1$ this implies that the generators determine an undirected $(l+1)$-regular graph.

6.2 Infinite tree of lattices

Next we shall work over $\mathbb{Q}_l$. We give a description of the same graph in two ways: in terms of homothety classes of rank two lattices, and in terms of local double cosets of the multiplicative group

[2] If p is not a square modulo l, then the constructions described below result in bipartite Ramanujan graphs with twice as many vertices.

of the Hamiltonian quaternion algebra. The description follows [Lub10, 5.3, 7.4]. Let $B = B_{2,\infty}$ be the Hamiltonian quaternion algebra defined over $\mathbb{Q}$.

First we review the construction of an $(l+1)$-regular infinite tree on homothety classes of rank two lattices in $\mathbb{Q}_l \times \mathbb{Q}_l$ following [Lub10, 5.3]. The vertices of this infinite graph are in bijection with $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$. To talk about a finite graph, we shall then consider two subgroups $\Gamma(2)$ and $\Gamma(2p)$ in $B^\times/Z(B^\times)$. It turns out that $\Gamma(2)$ acts simply transitively on the infinite tree, and orbits of $\Gamma(2p)$ on the tree are in bijection with the finite group $\Gamma(2)/\Gamma(2p)$. Under our assumptions the latter turns out to be in bijection with $\mathrm{PSL}_2(\mathbb{F}_p)$ above and the finite quotient of the tree is isomorphic to the Cayley graph above.

First we describe the infinite tree following [Lub10, 5.3]. Consider the two dimensional vector space $\mathbb{Q}_l \times \mathbb{Q}_l$ with standard basis $\mathbf{e}_1 = {}^t\langle 1, 0\rangle$, $\mathbf{e}_2 = {}^t\langle 0, 1\rangle$. A *lattice* is a rank two $\mathbb{Z}_l$-submodule $L \subset \mathbb{Q}_l \times \mathbb{Q}_l$. It is generated (as a $\mathbb{Z}_l$-module) by two column vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Q}_l \times \mathbb{Q}_l$ that are linearly independent over $\mathbb{Q}_l$. We shall consider homothety classes of lattices, i.e. we say lattices L_1 and L_2 are equivalent if there exists an $0 \neq \alpha \in \mathbb{Q}_l$ such that $\alpha L_1 = L_2$. Writing $\mathbf{u}, \mathbf{v}$ in the standard basis $\mathbf{e}_1, \mathbf{e}_2$ maps the lattice L to an element $M_L \in \mathrm{GL}_2(\mathbb{Q}_l)$. Let $\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2 \in \mathbb{Q}_l \times \mathbb{Q}_l$ and let $L_i = \mathrm{Span}_{\mathbb{Z}_l}\{\mathbf{u}_i, \mathbf{v}_i\}$ $(i = 1, 2)$ be the lattices generated by these respective pairs of vectors, with M_{L_1} and M_{L_2} the corresponding matrices. Let $M \in \mathrm{GL}_2(\mathbb{Q}_l)$ so that $M_{L_1} M = M_{L_2}$. Then $L_1 = L_2$ (as subsets of $\mathbb{Q}_l \times \mathbb{Q}_l$) if and only if $M \in \mathrm{GL}_2(\mathbb{Z}_l)$. It follows that the homothety classes of lattices are in bijection with $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$. Equivalently, we may say that $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ acts simply transitively on homothety classes of lattices.

The vertices of the infinite graph T are homothety classes of lattices. The classes $[L_1], [L_2]$ are adjacent in T if and only if there are representatives $L_i' \in [L_i]$ $(i = 1, 2)$ such that $L_2' \subset L_1'$ and $[L_1' : L_2'] = l$. We show that this relation defines an undirected $(l+1)$-regular graph. By the transitive action of $\mathrm{GL}_2(\mathbb{Q}_l)$ on lattices we may assume that $L_1' = \mathbb{Z}_l \times \mathbb{Z}_l = \mathrm{Span}_{\mathbb{Z}_l}\{\mathbf{e}_1, \mathbf{e}_2\}$, the *standard lattice* and $L_2' \subset \mathbb{Z}_l \times \mathbb{Z}_l$. The map $\mathbb{Z}_l \to \mathbb{Z}_l/l\mathbb{Z}_l \cong \mathbb{F}_l$ induces a map from $\mathbb{Z}_l \times \mathbb{Z}_l$ to $\mathbb{F}_l^2$. Since the index of L_2' in $\mathbb{Z}_l \times \mathbb{Z}_l$ is l, the image of L_2' is a one-dimensional vector subspace of $\mathbb{F}_l^2$. This implies that $L_2' \supset \{l\mathbf{e}_1, l\mathbf{e}_2\}$, i.e. $L_2' \supset lL_1'$ and the graph is undirected.[3] Furthermore, since there are $l+1$ one-dimensional subspaces of $\mathbb{F}_l^2$, the graph is $(l+1)$-regular.

The $l+1$ neighbors of the standard lattice can be described explicitly by the following matrices:

$$M_l = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}, \; M_h = \begin{pmatrix} l & h \\ 0 & 1 \end{pmatrix} \text{ for } 0 \leq h \leq l-1 \tag{8}$$

For any of the matrices M_t $(0 \leq t \leq l)$ the columns of M_t span a different one-dimensional subspace of $\mathbb{F}_l \times \mathbb{F}_l$. The matrices determine the neighbors of any other lattice by a change of basis in $\mathbb{Q}_l \times \mathbb{Q}_l$.

By the above we can already see that T is isomorphic to the graph on $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ with edges corresponding to multiplication by generators (8) above. To show that T is a tree it suffices to show that there is exactly one path from the standard lattice $\mathbb{Z}_l \times \mathbb{Z}_l$ to any other homothety class. This follows from the uniqueness of the Jordan–Hölder series in a finite cyclic l-group as in [Lub10, p. 69].

In the next section, we show that the above infinite tree is isomorphic to a Cayley graph of a subgroup of $B^\times/Z(B^\times)$. In Section 6.4 we give an explicit bijection between the Cayley generators and the matrices given in (8) above.

[3] I.e. the adjacency relation defined above is symmetric.

6.3 Hamiltonian quaternions over a local field

To turn the above infinite tree into a finite, $(l+1)$-regular graph we shall define a group action on its vertices. Let B be the algebra of Hamiltonian quaternions defined over $\mathbb{Q}$. Let G' be the $\mathbb{Q}$-algebraic group $B^\times/Z(B^\times)$. In this subsection we shall follow [Lub10, 7.4] to define normal subgroups $\Gamma(2p) \subset \Gamma(2)$ of $\Gamma = G'(\mathbb{Z}[l^{-1}])$ such that $\Gamma(2)$ acts simply transitively on the graph T. The quotient $\Gamma(2p)\backslash T$ will be isomorphic to the Cayley graph of the finite quotient group $\Gamma(2)/\Gamma(2p)$. This graph is isomorphic to the Cayley graph of $\mathrm{PSL}_2(\mathbb{F}_p)$ defined in Section 6.1 above. Thus we have the following equation.

$$\mathrm{PSL}_2(\mathbb{F}_p) \cong \Gamma(2p)\backslash\Gamma(2) \cong \Gamma(2p)\backslash T \cong \Gamma(2p)\backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l). \tag{9}$$

We first define the groups Γ, $\Gamma(2)$, $\Gamma(2p)$ and then examine their relationship with T. Recall that $B = B_{2,\infty}$, i.e. B is ramified at 2 and ∞. For a commutative ring R define $B(R) = \mathrm{Span}_R\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ where $\mathbf{i}^2 = \mathbf{j}^2 = -1$ and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. We introduce the notation $b_{x_0,x_1,x_2,x_3} := x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$. Recall that for $b = b_{x_0,x_1,x_2,x_3}$ we may define $\bar{b} = b_{x_0,-x_1,-x_2,-x_3}$ and the *reduced norm* of b as $N(b) = b\bar{b} = x_0^2 + x_1^2 + x_2^2 + x_3^2$. For a (commutative, unital) ring R an element $b \in B(R)$ is invertible in $B(R)$ if and only if $N(b)$ is invertible in R. (Then $b^{-1} = (N(b))^{-1}\bar{b}$.) Furthermore

$$[b_{x_0,x_1,x_2,x_3}, b_{y_0,y_1,y_2,y_3}] = 2(x_2y_3 - x_3y_2)\mathbf{i} + 2(x_3y_1 - x_1y_3)\mathbf{j} + 2(x_1y_2 - x_2y_1)\mathbf{k}, \tag{10}$$

and hence if R has no zero divisors then $Z(B(R)) = R$. In particular $Z(B^\times(\mathbb{Z}[l^{-1}])) = \{\pm l^k \mid k \in \mathbb{Z}\}$.

Recall that S was the set of $l+1$ integer solutions of (6). Any solution x_0, x_1, x_2, x_3 determines a $b = b_{x_0,x_1,x_2,x_3} \in B(\mathbb{Z}[l^{-1}])$ such that $N(b) = l$. Since l is invertible in $\mathbb{Z}[l^{-1}]$ we in fact have $b \in B^\times(\mathbb{Z}[l^{-1}])$. Let $\Gamma = G'(\mathbb{Z}[l^{-1}]) = B^\times(\mathbb{Z}[l^{-1}])/Z(B^\times(\mathbb{Z}[l^{-1}]))$ and let us denote the image of S in Γ by S as well. Since $B^\times(\mathbb{Z}[l^{-1}]) = \{b \in B(\mathbb{Z}[l^{-1}]) \mid N(b) = l^k,\ k \in \mathbb{Z}\}$, if $[b] \in \Gamma$ for $b \in B^\times(\mathbb{Z}[l^{-1}])$ then it follows from [Lub10, Corollary 2.1.10] that b is a unit multiple of an element of $\langle S\rangle$. It follows that $\Gamma = \langle S\rangle\{[1], [\mathbf{i}], [\mathbf{j}], [\mathbf{k}]\}$ and the index of $\langle S\rangle$ in Γ is 4. In fact observe that if $b \in S$ then $b^{-1} \in S$ and [Lub10, Corollary 2.1.11] states that $\langle S\rangle$ is a free group on $\frac{l+1}{2}$ generators. We shall see that $\langle S\rangle$ agrees with a congruence subgroup $\Gamma(2)$.

Now let $N = 2M$ be coprime to l and let $R = \mathbb{Z}[l^{-1}]/N\mathbb{Z}[l^{-1}]$. The quotient map $\mathbb{Z}[l^{-1}] \to R$ determines a map $B(\mathbb{Z}[l^{-1}]) \to B(R)$. This restricts to a map $B^\times(\mathbb{Z}[l^{-1}]) \to B^\times(R)$. Observe that if $M = 1$ then $B^\times(R)$ is commutative. If $M = p$ then the subgroup

$$Z := \left\{b_{x_0,0,0,0} \in B^\times(\mathbb{Z}[l^{-1}]/2p\mathbb{Z}[l^{-1}]) \mid p \nmid x_0, 2 \nmid x_0\right\}$$

(cf. [LPS88, p. 266]) is central in $B^\times(R)$. Consider the commutative diagram:

$$\begin{array}{ccccc} B(\mathbb{Z}[l^{-1}])^\times & \longrightarrow & B^\times(\mathbb{Z}[l^{-1}]/2\mathbb{Z}[l^{-1}]) & \longrightarrow & B^\times(\mathbb{Z}[l^{-1}]/2p\mathbb{Z}[l^{-1}]) \\ \downarrow & & \downarrow & & \downarrow \\ \Gamma & \xrightarrow{\pi_2} & B^\times(\mathbb{Z}[l^{-1}]/2\mathbb{Z}[l^{-1}]) & \xrightarrow{\pi_p} & B^\times(\mathbb{Z}[l^{-1}]/2p\mathbb{Z}[l^{-1}])/Z \end{array} \tag{11}$$

and define[4] $\pi_{2p} := \pi_p \circ \pi_2$ and $\Gamma(2) := \ker \pi_2$ and $\Gamma(2p) = \ker \pi_{2p}$. Observe that by the congruence conditions (cf. (6)) $S \subseteq \Gamma$ is contained in $\Gamma(2)$ and in fact $\langle S\rangle = \Gamma(2) \supseteq \Gamma(2p)$. As mentioned above this implies that $\Gamma(2)$ is a free group with $\frac{l+1}{2}$ generators.

[4]The definition here agrees with the choices in [LPS88] as well as $\Gamma(N) = \ker(G'(\mathbb{Z}[l^{-1}]) \to G'(\mathbb{Z}[l^{-1}]/N\mathbb{Z}[l^{-1}]))$ in [Lub10]. Here $G' = B^\times/Z(B^\times)$ as a $\mathbb{Q}$-algebraic group. Note however that by (10) the center $Z(B^\times(R))$ for $R = \mathbb{Z}[l^{-1}]/N\mathbb{Z}[l^{-1}]$, $N = 2M$ may not be spanned by $1 + N\mathbb{Z}[l^{-1}]$. In fact from (10) $B^\times(R)$ is commutative for $M = 1$ and for $M = p$ we have $Z(B^\times(R)) = Z \oplus [p]\mathbf{i} + [p]\mathbf{j} + [p]\mathbf{k}$. However the image of $\langle S\rangle$ in $B^\times(R)$ is trivial if $M = 1$ and intersects the center in Z when $M = p$.

To see the action of $\Gamma(2)$ on T note that B splits over $\mathbb{Q}_l$ and hence $B(\mathbb{Q}_l) \cong M_2(\mathbb{Q}_l)$. Since $-1 \in (\mathbb{F}_l^\times)^2$ there exists an $\epsilon \in \mathbb{Z}_l$ such that $\epsilon^2 = -1$. Then we have an isomorphism $\sigma : B(\mathbb{Q}_l) \to M_2(\mathbb{Q}_l)$ [Lub10, p. 95] given by

$$\sigma(x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}) = \begin{pmatrix} x_0 + x_1\epsilon & x_2 + x_3\epsilon \\ -x_2 + x_3\epsilon & x_0 - x_1\epsilon \end{pmatrix}. \tag{12}$$

Observe that $\sigma(B^\times(\mathbb{Z}[l^{-1}])) \subseteq \mathrm{GL}_2(\mathbb{Q}_l)$ and σ maps elements of the center into scalar matrices, and hence this defines an action of Γ (and hence $\Gamma(2), \Gamma(2p)$) on T. This action preserves the graph structure. Then we have the following. Observe that σ maps the elements of $\langle S \rangle \subseteq \Gamma$ into the congruence subgroup of $\mathrm{PGL}_2(\mathbb{Z}_l)$ modulo 2.

Proposition 6.1. *[Lub10, Lemma 7.4.1] The action of* $\Gamma(2)$ *on the tree* $T = \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ *is simply transitive (and respects the graph structure).*

Proof. See *loc.cit.* for details of the proof. Transitivity follows from the fact that T is connected and elements of S map a vertex of T to its distinct neighbors. The group $\Gamma(2) = \langle S \rangle$ is a discrete free group, hence its intersection with a compact stabilizer $\mathrm{PGL}_2(\mathbb{Z}_l)$ is trivial. This implies that the neighbors are distinct and the stabilizer of any vertex is trivial. □

The above implies that the orbits of $\Gamma(2p)$ on T have the structure of the Cayley graph $\Gamma(2)/\Gamma(2p)$ with respect to the generators S. We can see from the maps in (11) that $\Gamma(2)/\Gamma(2p)$ is isomorphic to a subgroup of $G'(\mathbb{Z}/2p\mathbb{Z}) \cong G'(\mathbb{Z}/2\mathbb{Z}) \times G'(\mathbb{Z}/p\mathbb{Z})$. (This last isomorphism follows from the Chinese Remainder Theorem.) Since the image of $\Gamma(2)$ in $G'(\mathbb{Z}/2\mathbb{Z})$ is trivial, we may identify $\Gamma(2)/\Gamma(2p)$ with a subgroup of $G'(\mathbb{Z}/p\mathbb{Z})$. Here $G'(\mathbb{Z}/p\mathbb{Z}) \cong \mathrm{PGL}_2(\mathbb{F}_p)$. (For an explicit isomorphism take an analogue of σ in (12) with $\epsilon \in \mathbb{Z}/p\mathbb{Z}$ such that $\epsilon^2 = -1$.) The image of $\Gamma(2)$ agrees with $\mathrm{PSL}_2(\mathbb{F}_p)$ as a consequence of the Strong Approximation Theorem [Lub10, Lemma 7.4.2]. We shall discuss this in the next section.

We summarize the contents of this section.

Theorem 6.2. *[Lub10, Theorem 7.4.3] Let* l *and* p *be primes so that* $l \equiv p \equiv 1 \mod 4$ *and* l *is a quadratic residue modulo* $2p$*. Let* $S \subset \mathrm{PSL}_2(\mathbb{F}_p)$ *be the* $(l+1)$*-element set corresponding to the solutions of* (6) *via the map* (7) *and* $Cay(\mathrm{PSL}_2(\mathbb{F}_p), S)$ *the Cayley graph determined by the set of generators* S *on the group* $\mathrm{PSL}_2(\mathbb{F}_p)$*. Let* T *be the graph on* $\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ *with edges corresponding to multiplication by elements listed in* (8)*. Let* B *be the Hamiltonian quaternion algebra over* $\mathbb{Q}$ *and* $\Gamma(2p)$ *the kernel of the map* π_{2p} *in* (11) *(a cocompact congruence subgroup). Then* $\Gamma(2p)$ *acts on the infinite tree* T *and we have the following isomorphism of graphs:*

$$Cay(\mathrm{PSL}_2(\mathbb{F}_p), S) \cong \Gamma(2p) \backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l). \tag{13}$$

These are connected, $(l+1)$ *regular, non-bipartite, simple, graphs on* $\frac{p^3-p}{2}$ *vertices.*

6.4 Explicit isomorphism between generating sets

We have seen above that the LPS graph can be interpreted as a finite quotient of the infinite tree of homothety classes of lattices. In this case, the edges are given by matrices that take a $\mathbb{Z}_l$-basis of one lattice to a $\mathbb{Z}_l$-basis of one of its neighbors. On the other hand, the edges can be given in terms of the set of generators S. Proposition 6.1 states that $\langle \sigma(S) \rangle = \Gamma(2) \subset G'(\mathbb{Z}[l^{-1}])$ acts simply

transitively on the tree T. The proof of the proposition (cf. [Lub10, Lemma 7.4.1]) implicitly shows that there exists a bijection between elements of $\sigma(S) \subset \mathrm{PGL}_2(\mathbb{Z}_l)$ and the matrices given in (8).

In this section we wish to make this bijection more explicit. For a fixed $\alpha \in S$ we find the matrix from the list (8) determining the same edge of T. As in Section 6.3 we write $\sigma(\alpha) \in \mathrm{PGL}_2(\mathbb{Z}_l)$ for the elements of $\sigma(S)$. This amounts to finding the matrix M from the list in (8) such that $\sigma(\alpha)^{-1}M \in \mathrm{PGL}_2(\mathbb{Z}_l)$.

To pair up matrices from (8) with the corresponding elements of S, we introduce the following notation. Let us number the solutions to $\alpha\overline{\alpha} = l$ as $\alpha_0, \ldots, \alpha_{l-1}, \alpha_l$ so that we have the correspondence $\sigma(\alpha_h)^{-1}M_h \in \mathrm{PGL}_2(\mathbb{Z}_l)$ for $0 \leq h \leq l$. By giving an explicit correspondence, we mean that given an $\alpha \in \sigma^{-1}(S)$, we determine $0 \leq h \leq l$ such that $\alpha = \alpha_h$.

Elements of $\sigma(S) \subset \mathrm{PGL}_2(\mathbb{Z}_l)$ are given in terms of an $\epsilon \in \mathbb{Z}_l$ such that $\epsilon^2 = -1$. Let a, b be the positive integers such that $a^2 + b^2 = l$ and a is odd. Let $0 \leq e \leq l-1$ so that $eb = a$. Then in $\mathbb{Z}_l$ we have either $\epsilon \in e + l\mathbb{Z}_l$ and $\epsilon^{-1} = -\epsilon \in -e + l\mathbb{Z}_l$ or $\epsilon \in -e + l\mathbb{Z}_l$ and $\epsilon^{-1} = -\epsilon \in e + l\mathbb{Z}_l$.

Let $\alpha = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ so that $\sigma(\alpha) \in S$, and a, b, e, ϵ are as above. Let

$$\alpha_h = x_0^{(h)} + x_1^{(h)}\mathbf{i} + x_2^{(h)}\mathbf{j} + x_3^{(h)}\mathbf{k}$$

for $0 \leq h \leq l$. Here x_0, x_1, x_2, x_3 are integers; it is convenient to think about them (as well as $x_0^{(h)}, x_1^{(h)}, x_2^{(h)}, x_3^{(h)}$ for $0 \leq h \leq l$) as being in $\mathbb{Z} \subset \mathbb{Z}_l$. Then

$$\sigma(\alpha)^{-1} = \frac{1}{l}\begin{pmatrix} x_0 - x_1\epsilon & -x_2 - x_3\epsilon \\ x_2 - x_3\epsilon & x_0 + x_1\epsilon \end{pmatrix} \tag{14}$$

and

$$\begin{aligned} \sigma(\alpha)^{-1} \cdot \begin{pmatrix} l & h \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} x_0 - x_1\epsilon & l^{-1}\left(h(x_0 - x_1\epsilon) + (-x_2 - x_3\epsilon)\right) \\ x_2 - x_3\epsilon & l^{-1}\left(h(x_2 - x_3\epsilon) + (x_0 + x_1\epsilon)\right) \end{pmatrix} \\ \sigma(\alpha)^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} &= \begin{pmatrix} l^{-1}(x_0 - x_1\epsilon) & -x_2 - x_3\epsilon \\ l^{-1}(x_2 - x_3\epsilon) & x_0 + x_1\epsilon \end{pmatrix} \end{aligned} \tag{15}$$

Then by (15) we have that $x_0^{(l)} - x_1^{(l)}\epsilon$ and $x_2^{(l)} - x_3^{(l)}\epsilon$ are in $l\mathbb{Z}_l$. Hence $x_0^{(l)} \in x_1^{(l)}\epsilon + l\mathbb{Z}_l$, and thus $(x_0^{(l)})^2 \in (x_1^{(l)}\epsilon)^2 + l\mathbb{Z}_l = -x_1^2 + l\mathbb{Z}_l$, whence $(x_0^{(l)})^2 + (x_1^{(l)})^2 \in l\mathbb{Z}_l$. Note that since $(x_0^{(l)})^2 + (x_1^{(l)})^2 + (x_2^{(l)})^2 + (x_3^{(l)})^2 = l$ and x_0 is positive, this implies that $(x_0^{(l)})^2 + (x_1^{(l)})^2 = l$ and $(x_2^{(l)})^2 + (x_3^{(l)})^2 = 0$, i.e. $x_2^{(l)} = x_3^{(l)} = 0$ and $x_0^{(l)} = a$, $|x_1^{(l)}| = b$. Note that by the assumptions in Section 6.1, $a \pm bi, a \pm bj, a \pm bk \in S$. A straightforward computation now shows the following.

$$\begin{aligned} &\epsilon \in e + l\mathbb{Z}_l \Rightarrow \alpha_l = a + b\mathbf{i},\ \alpha_0 = a - b\mathbf{i},\ \alpha_e = a - b\mathbf{j},\ \alpha_{l-e} = a + b\mathbf{j},\ \alpha_1 = a - b\mathbf{k},\ \alpha_{l-1} = a + b\mathbf{k} \\ &\epsilon \in -e + l\mathbb{Z}_l \Rightarrow \alpha_l = a - b\mathbf{i},\ \alpha_0 = a + b\mathbf{i},\ \alpha_e = a - b\mathbf{j},\ \alpha_{l-e} = a + b\mathbf{j},\ \alpha_1 = a + b\mathbf{k},\ \alpha_{l-1} = a - b\mathbf{k} \end{aligned} \tag{16}$$

Now let us assume that for $\alpha = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ we have that $x_0 - x_1\epsilon \notin l\mathbb{Z}_l$. This implies that It remains to determine the h such that $\alpha = \alpha_h$ when α is not one of the solutions covered by (16). In that case, we may assume $h \notin \{0, 1, e, l-e, l-1, l\}$ and we have

$$h(x_0 - x_1\epsilon) + (-x_2 - x_3\epsilon) \in l\mathbb{Z}_l; \tag{17}$$

$$h(x_2 - x_3\epsilon) + (x_0 + x_1\epsilon) \in l\mathbb{Z}_l. \tag{18}$$

A straightforward computation based on $\alpha\overline{\alpha} = l$ shows that (17) and (18) are satisfied by the same element in $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$. The element

$$\overline{h} = \frac{x_2 + x_3\epsilon}{x_0 - x_1\epsilon} \in \mathbb{F}_l \tag{19}$$

is well defined, since $x_0 - x_1\epsilon \notin l\mathbb{Z}_l$, furthermore, it uniquely determines an $0 \leq h \leq l$. For a fixed α not covered by (16), one may thus find h such that $\alpha = \alpha_h$.

We give two explicit examples.

Example 6.3. When $l = 5$, then $a = 1$, $b = 2$ and $e = 3$. Then (20) gives the bijection between the list in (8) and solutions of $\alpha\overline{\alpha} = 5$ in $B(\mathbb{Q}_5)$. In this case the list in (16) is exhaustive.

h		0	1	2	3	4	5
$\epsilon \in 3 + 5\mathbb{Z}_5$	α_h	$1 - 2\mathbf{i}$	$1 - 2\mathbf{k}$	$1 + 2\mathbf{j}$	$1 - 2\mathbf{j}$	$1 + 2\mathbf{k}$	$1 + 2\mathbf{i}$
$\epsilon \in 2 + 5\mathbb{Z}_5$		$1 + 2\mathbf{i}$	$1 + 2\mathbf{k}$	$1 + 2\mathbf{j}$	$1 - 2\mathbf{j}$	$1 - 2\mathbf{k}$	$1 - 2\mathbf{i}$

(20)

Example 6.4. When $l = 13$, we have $a = 3$, $b = 2$ and $e = 8$. The cases listed in (16) are no longer exhaustive. The correspondence is given in Table 2.

h	α_h
0	$3 - 2\mathbf{i}$
1	$3 - 2\mathbf{k}$
2	$1 - 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}$
3	$1 - 2\mathbf{i} + 2\mathbf{j} - 2\mathbf{k}$
4	$1 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}$
5	$3 + 2\mathbf{j}$
6	$1 + 2\mathbf{i} - 2\mathbf{j} + 2\mathbf{k}$
7	$1 + 2\mathbf{i} + 2\mathbf{j} - 2\mathbf{k}$
8	$3 - 2\mathbf{j}$
9	$1 + 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}$
10	$1 - 2\mathbf{i} - 2\mathbf{j} + 2\mathbf{k}$
11	$1 - 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}$
12	$3 + 2\mathbf{k}$
13	$3 + 2\mathbf{i}$

h	α_h
0	$3 + 2\mathbf{i}$
1	$3 + 2\mathbf{k}$
2	$1 + 2\mathbf{i} - 2\mathbf{j} + 2\mathbf{k}$
3	$1 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}$
4	$1 - 2\mathbf{i} + 2\mathbf{j} - 2\mathbf{k}$
5	$3 + 2\mathbf{j}$
6	$1 - 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}$
7	$1 - 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}$
8	$3 - 2\mathbf{j}$
9	$1 - 2\mathbf{i} - 2\mathbf{j} + 2\mathbf{k}$
10	$1 + 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}$
11	$1 + 2\mathbf{i} + 2\mathbf{j} - 2\mathbf{k}$
12	$3 - 2\mathbf{k}$
13	$3 - 2\mathbf{i}$

Table 2: The correspondence when $\epsilon \in 8 + 13\mathbb{Z}_{13}$ (left) and when $\epsilon \in 5 + 13\mathbb{Z}_{13}$ (right).

7 Strong Approximation

In this section we briefly explain the significance of Strong Approximation to Ramanujan graphs and particularly the LPS graphs above. As discussed in Section 5 we may consider $G(\mathbb{A})$, the adelic points of a linear algebraic group G defined over $\mathbb{Q}$. The group $G(\mathbb{Q})$ embeds diagonally into $G(\mathbb{A})$, and it is a discrete subgroup. The groups $G(\mathbb{Q}_v)$ are also subgroups of $G(\mathbb{A})$, and $G(\mathbb{A})$ has a well-defined projection onto $G(\mathbb{Q}_v)$. Similarly, for a finite set of places S we may take G_S, the direct product of $G(\mathbb{Q}_v)$ for $v \in S$.

Strong Approximation (when it holds) is the statement that for a group G and a finite set of places S the subgroup $G(\mathbb{Q})G_S$ is *dense* in $G(\mathbb{A})$. This implies that

$$G(\mathbb{A}) = G(\mathbb{Q})G_S K \text{ for any open subgroup } K \leq G(\mathbb{A}). \tag{21}$$

For example, Strong Approximation holds for $G = \mathrm{SL}_2$ and any set of places $S = \{v\}$. However, in the form written above it *does not hold* for GL_2 or PGL_2. However one can prove results similar to (21) for GL_2 adding restrictions on the subgroup K:

$$G(\mathbb{A}) = G(\mathbb{Q})G_S K \text{ for an open subgroup } K \leq G(\mathbb{A}) \text{ if } K \text{ is "sufficiently large."} \tag{22}$$

Here we shall have

$$K = \prod_{v \notin S} K_v;\ K_v \leq G(\mathbb{Z}_v) \tag{23}$$

and the condition of being "sufficiently large" can be made precise by requiring that the determinant map $\det : K_v \to \mathbb{Z}_v^\times$ be surjective for all $v \notin S$.

Strong Approximation holds for the algebraic group of elements of a quaternion algebra of unit norm [Vig80, Théorème 4.3]. We shall use this statement to prove a statement like (22) for the algebraic group of invertible quaternions. A similar statement then holds for $G' = B^\times/Z(B^\times)$ and a subgroup K' that is not quite "large enough." The implications for Pizer graphs and LPS graphs will be discussed in Sections 7.2 and 7.3 below.

These statements coming from Strong Approximation are crucial for proving that the various constructions produce Ramanujan graphs. As seen in Section 5 the Ramanujan property of a graph can be expressed in terms of its eigenvalues. Given a graph (constructed e.g. via local double cosets as seen above) the Strong Approximation theorem can be used to relate its spectrum to the representation theory of $G(\mathbb{A})$. In that context a theorem of Deligne resolves the issue by proving a special case of the Ramanujan conjecture (see [Lub10, Theorem 6.1.2, Theorem A.1.2, Theorem A.2.14] and [Del71]).

7.1 Approximation for invertible quaternions

The argument below is adapted from [Gel75, Section 3] and [Lub10, 6.3].[5]

Let B be a (definite) quaternion algebra over $\mathbb{Q}$, $B^\times$ its invertible elements and $B^1 = \{b \in B \mid N(b) = 1\}$ its elements of reduced norm 1, recall $N(b) = b\bar{b}$. Let l be a prime where B is split. Then by [Vig80, Théorème 4.3] we have that $B^1(\mathbb{Q})B^1(\mathbb{Q}_l)$ is dense in $B^1(\mathbb{A})$ thus $B^1(\mathbb{A}) = B^1(\mathbb{Q})B^1(\mathbb{Q}_l)K$ for any open subgroup $K \leq B^1(\mathbb{A})$. An open subgroup $K \leq B^1(\mathbb{A})$ is of the form $K = \prod_v K_v$ where $K_v \leq B_v^1$ is open and $K_v = B^1(\mathbb{Z}_v)$ for all but finitely many places v. It follows that given *any* open subgroups $K_v^{(B^1)} \leq B^1(\mathbb{Z}_v)$ $(v \neq l)$ such that $K_v^{(B^1)} = B^1(\mathbb{Z}_v)$ for all but finitely many places v we have that

$$B^1(\mathbb{A}) = B^1(\mathbb{Q})B^1(\mathbb{Q}_l)\prod_{v \neq l} K_v^{(B^1)}. \tag{24}$$

To make a similar statement for $B^\times$ it will be necessary to impose a restriction on the open subgroups K_v.

[5] In fact, since at every split place v we have $B^\times(\mathbb{Q}_v) \cong \mathrm{GL}_2(\mathbb{Q}_v)$ with the reduced norm on $B^\times$ corresponding to the determinant on GL_2 [Vig80, p. 3] this is the "same argument at all but finitely many places."

Theorem 7.1. *Let $K_v \leq B^\times(\mathbb{Z}_v)$ for every place $l \neq v < \infty$ so that $K_v = B^\times(\mathbb{Z}_v)$ for all but finitely many v, and the norm map $N : K_v \to {\mathbb{Z}_v}^\times$ is surjective for every place v. Then*

$$B^\times(\mathbb{A}) = B^\times(\mathbb{Q})B^\times(\mathbb{R})B^\times(\mathbb{Q}_l) \prod_{l \neq v < \infty} K_v. \tag{25}$$

Note that by [Voi18, Lemma 13.4.6] the norm map $N : B^\times(\mathbb{Z}_v) \to {\mathbb{Z}_v}^\times$ is surjective for every nonarchimedean v.

Proof. Let $b \in B^\times(\mathbb{A})$, we need to show b is contained on the right-hand side. To write b as a product according to the right-hand side of (25) we shall use (24), strong approximation for B^1. Observe first that it suffices to show that any $b \in B^\times(\mathbb{A})$ can be written as

$$b = rhk, \text{ where } r \in B^\times(\mathbb{Q}),\ h \in B^1(\mathbb{A}),\ \text{and } k \in B^\times(\mathbb{R})B^\times(\mathbb{Q}_l) \prod_{l \neq v < \infty} K_v. \tag{26}$$

This is because the intersections $K_v \cap B^1(\mathbb{Q}_v)$ are open subgroups of $B^1(\mathbb{Z}_v)$ (and $B^\times(\mathbb{Z}_v) \cap B^1(\mathbb{Z}_v) = B^1(\mathbb{Z}_v)$ at all but finitely many places). It thus follows from (24) (choosing $K_v^{(B^1)} := K_v \cap B^1(\mathbb{Q}_v)$) that the factor $h \in B^1(\mathbb{A}) \subseteq B^\times(\mathbb{A})$ from (26) is contained on the right-hand side of (25). It follows that then $b = rhk$ is contained on the right-hand side of (25) as well. (Note that here the factors of h and k belonging to different components $B^\times(\mathbb{Q}_v)$ commute.)

So we must show that any $b \in B^\times(\mathbb{A})$ decomposes as in (26). Let $b = (b_v)_v$ for $b_v \in B^\times(\mathbb{Q}_v)$ and set $n_v := N(b_v)$. For all but finitely many places v we have $b_v \in B^\times(\mathbb{Z}_v)$ and hence $n_v \in {\mathbb{Z}_v}^\times$. At a finite set T of finite places we may write $n_v \in v^{m_v}{\mathbb{Z}_v}^\times$. Let us take

$$n_{\mathbb{Q}} = \prod_{v \in T} v^{m_v}. \tag{27}$$

Then $n_{\mathbb{Q}} \in \mathbb{Q}_{>0}$, $n_{\mathbb{Q}} \in {\mathbb{Z}_v}^\times$ for every $v \notin T$, $v < \infty$ and hence $n_{\mathbb{Q}}^{-1} n_v \in {\mathbb{Z}_v}^\times$ for *every* finite place v.

It is a fact that there is an $r \in B^\times(\mathbb{Q})$ such that $N(r) = n_{\mathbb{Q}}$. Then for this r we have that the norm of $r^{-1}b \in B^\times(\mathbb{A})$ is in ${\mathbb{Z}_v}^\times$ for every finite place v.

Let us write $(r^{-1}b)_v$ for the component of $r^{-1}b \in B^\times(\mathbb{A})$ at a place v. There exists a $k \in B^\times(\mathbb{R})B^\times(\mathbb{Q}_l)\prod_{l \neq v < \infty} K_v$, $k = (k_v)_v$ such that $k_l = (r^{-1}b)_l$ and $k_\infty = (r^{-1}b)_\infty$ and $N(k_v) = N((r^{-1}b)_v)$ every other place. This follows from the fact that the norm map $N : K_v \to {\mathbb{Z}_v}^\times$ is surjective.

Now let $h = r^{-1}bk^{-1}$. We show $h \in B^1(\mathbb{A})$. Write $h = (h_v)_v$ for $h_v \in B^\times(\mathbb{Q}_v)$. It follows from the choice of k that h_l and h_∞ are the identity element of $B^\times(\mathbb{Q}_l)$ and $B^\times(\mathbb{R})$ respectively, and $N(h_v) = 1$ at every other place v. This implies that indeed $h \in B^1(\mathbb{A})$. This completes the proof that a decomposition as in (26) exists, and in turn the proof of (25). □

7.2 Strong Approximation for LPS graphs

This section is based on [Lub10, 6.3]. (In particular, we recall and elaborate on the proof of the first statements in [Lub10, Proposition 6.3.3] in the special case when $N = 2p$. This is relevant to understanding the last step in (5).) We apply a similar formula to (25) with a particular choice of open subgroups K_v' to prove a statement that relates double cosets such as in (9) to adelic double cosets. Let $B = B_{2,\infty}$ be the algebra of Hamiltonian quaternions, ramified at 2 and ∞. Recall from

Section 6.3 that G' is the $\mathbb{Q}$-algebraic group $B^\times/Z(B^\times)$. Let us fix the prime $l \equiv 1 \mod 4$ as in Section 6. In a similar manner to the proof of (25) is follows that

$$G'(\mathbb{A}) = G'(\mathbb{Q})G'(\mathbb{R})G'(\mathbb{Q}_l) \prod_{l \neq v < \infty} G'(\mathbb{Z}_v). \tag{28}$$

Recall that since B splits at l we have $G'(\mathbb{Q}_l) \cong \mathrm{PGL}_2(\mathbb{Q}_l)$. We wish to have a statement similar to (28) above, replacing $G'(\mathbb{Z}_v)$ at $v = 2$ and $v = p$ by congruence subgroups K_2' and K_p'. (This p is the one fixed above in Section 6.) Then isomorphism will no longer hold, but the right-hand side will be a finite index normal subgroup of $G'(\mathbb{A})$.

The choice of the smaller subgroups K_2' and K_p' is as follows. For $v \in \{2, p\}$ let

$$K_v' = \ker\left(G'(\mathbb{Z}_v) \to G'(\mathbb{Z}_v/v\mathbb{Z}_v)\right). \tag{29}$$

Here $\mathbb{Z}_v/v\mathbb{Z}_v = \mathbb{F}_v$ is a finite field, hence $G'(\mathbb{Z}_v/v\mathbb{Z}_v)$ is finite. It follows that the index $[K_v : K_v']$ is finite. In fact since $B_{2,\infty}$ splits over p we have that $G'(\mathbb{Z}_p/v\mathbb{Z}_p) \cong \mathrm{PGL}_2(\mathbb{F}_p)$, hence $[K_p : K_p'] = p(p^2 - 1)$. At $v = 2$ we have $G'(\mathbb{F}_2) = B^\times(\mathbb{F}_2)$ hence $[K_2 : K_2'] = 8$.

Let us set K_v' as above if $v \in \{2, p\}$ and $K_v' = K_v = G'(\mathbb{Z}_v)$ otherwise, and let us define

$$H_{2p} := \left(G'(\mathbb{Q})G'(\mathbb{R})G'(\mathbb{Q}_l) \prod_{l \neq v < \infty} K_v'\right). \tag{30}$$

By [Lub10, Proposition 6.3.3] Strong Approximation proves that H_{2p} is a finite index normal subgroup of $G'(\mathbb{A})$.

From the definition of H_{2p} in equation (30) we have a surjection from

$$G'(\mathbb{Q}_l) \to G'(\mathbb{Q})\backslash H_{2p}/G'(\mathbb{R}) \prod_{l \neq v < \infty} K_v'.$$

If g_l and $g_l' \in G'(\mathbb{Q}_l)$ are mapped to the same coset on the right hand side then there exists $g_q \in G'(\mathbb{Q}), g_r \in G'(\mathbb{R})$ and $k = \prod_{l \neq v < \infty} k_v \in \prod_{l \neq v < \infty} K_v'$ such that $g_l = g_q g_l' g_r k$. This is equivalent to saying $g_l = g_q g_l'$ and $g_q \in K_v'$ for all $l \neq v < \infty$. By the definitions of the K_v's this last condition implies $g_q \in \Gamma(2p)$. Thus we see that

$$\Gamma(2p)\backslash G'(\mathbb{Q}_l)/G'(\mathbb{Z}_l) \cong G'(\mathbb{Q})\backslash H_{2p}/G'(\mathbb{R}) \prod_{v < \infty} K_v'. \tag{31}$$

Strong approximation in the manner discussed above is used to prove that LPS graphs are Ramanujan. First one shows that the finite $(l+1)$-regular graph $\Gamma(2p)\backslash T$ is Ramanujan if and only if all irreducible infinite-dimensional unramified unitary representations of $\mathrm{PGL}_2(\mathbb{Q}_l)$ that appear in $L^2(PGL_2(\mathbb{Q}_l)/\Gamma(2p))$ are tempered [Lub10, Corollary 5.5.3]. Then by the isomorphism above which follows from Strong Approximation, one can extend a representation ρ_l' of $\mathrm{PGL}_2(\mathbb{Q}_l)$ to an automorphic representation ρ' of $G'(\mathbb{A})$ in $L^2(G'(\mathbb{Q})\backslash G'(\mathbb{A}))$. By the Jacquet–Langlands correspondence, ρ' corresponds to a cuspidal representation ρ of $\mathrm{PGL}_2(\mathbb{A})$ in $L^2(\mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A}))$ such that ρ_v is discrete series for all v where B ramifies (so in our case, 2 and ∞) [Lub10, Theorem 6.2.1]. Finally, Deligne has proved the Ramanujan–Peterson conjecture in this case of holomorphic modular forms [Lub10, Theorem 6.1.2], [Del71], [Del74] which says that for ρ a cuspidal representation of $\mathrm{PGL}_2(\mathbb{A})$ in $L^2(\mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A}))$ with ρ_∞ discrete series, ρ_l is tempered [Lub10, Theorems 7.1.1 and 7.3.1]. Under the Jacquet–Langlands correspondence, the adjacency matrix of our graph X corresponds to the Hecke operator T_l [Lub10, 5.3] and the Ramanujan conjecture is equivalent to saying that $|\lambda| \leq 2\sqrt{l}$ for all of its eigenvalues $\lambda \neq \pm(l+1)$.

7.3 Strong Approximation for Pizer graphs

Now we turn to discussing how strong approximation is useful in establishing the bijections in (4). In Section 8 we will discuss Pizer's construction of Ramanujan graphs. These graphs are isomorphic to supersingular isogeny graphs. Their vertex set is the class group of a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$. This set is in bijection with an adelic double coset space, which in turn is in bijection with a set of local double cosets.

Let $B = B_{p,\infty}$ be a quaternion algebra (over $\mathbb{Q}$) ramified exactly at ∞ and at a finite prime p. At every finite prime v, $B(\mathbb{Q}_v)$ has a unique maximal order up to conjugation [Vig80, Lemme 1.4]. Given a maximal order $\mathcal{O}$ of B, one may define the adelic group $B^\times(\mathbb{A}_f)$ as a restricted direct product of the groups $B^\times(\mathbb{Q}_v)$ over the finite places, with respect to $\mathcal{O}_v^\times$. (Recall that this means that any element of $B^\times(\mathbb{A}_f)$ is a vector indexed by the finite places v; the component at v is in $B^\times(\mathbb{Q}_v)$ and in fact in $\mathcal{O}_v^\times$ at all but finitely many places.) This adelic object does not in fact depend on the choice of the maximal ideal $\mathcal{O}$. In particular, at any prime $l \neq p$ where B splits we have $B^\times(\mathbb{Q}_l) \cong \mathrm{GL}_2(\mathbb{Q}_l)$ and $\mathcal{O}_l^\times \cong \mathrm{GL}_2(\mathbb{Z}_l)$.

Let us now fix a prime l where B splits. The same argument as in Section 7.1 works restricted to $B^\times(\mathbb{A}_f)$ (the finite adèles). It follows that we have

$$B^\times(\mathbb{A}_f) = B^\times(\mathbb{Q})B^\times(\mathbb{Q}_l) \prod_{l \neq v < \infty} B^\times(\mathbb{Z}_v). \tag{32}$$

Proposition 7.2. *We have the bijections (cf. [CGL09, (1)])*

$$\begin{aligned} B^\times(\mathbb{Q})\backslash B^\times(\mathbb{A}_f)/\prod_{v<\infty} B^\times(\mathbb{Z}_v) \cong & (\mathcal{O}(\mathbb{Z}[l^{-1}]))^\times \backslash B^\times(\mathbb{Q}_l)/B^\times(\mathbb{Z}_l) \\ \cong & (\mathcal{O}(\mathbb{Z}[l^{-1}]))^\times \backslash \mathrm{GL}_2(\mathbb{Q}_l)/\mathrm{GL}_2(\mathbb{Z}_l). \end{aligned} \tag{33}$$

Proof. The first bijection follows from (32) and an argument similar to the proof of (31). Indeed, (32) implies that there is a surjection

$$B^\times(\mathbb{Q}_l) \to B^\times(\mathbb{Q})\backslash B^\times(\mathbb{A}_f)/\prod_{l \neq v < \infty} B^\times(\mathbb{Z}_v). \tag{34}$$

Now two elements $g_l, g_l' \in B^\times(\mathbb{Q}_l)$ land in the same double coset via this bijection if and only if $g_l = g_q g_l' k$ in $B^\times(\mathbb{A}_f)$. Then $g_l = g_q g_l'$ (from equality at the place l) and $g_q \in B^\times(\mathbb{Z}_v)$ (from equality at the places $l \neq v < \infty$). Consider the element $g_q \in B(\mathbb{Q})$, for example in terms of its coordinates in the standard basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ of B. Since $g_q \in B^\times(\mathbb{Z}_v)$ we have that $g_q \in \mathcal{O}(\mathbb{Z}[l^{-1}])$, and $g_q \in B^\times(\mathbb{Q}_l)$ implies that in fact $g_q \in (\mathcal{O}(\mathbb{Z}[l^{-1}]))^\times$. This completes the proof of the first bijection in (33).

Now the second bijection follows from the fact that B splits at the prime l and hence $B^\times(\mathbb{Q}_l) \cong \mathrm{GL}_2(\mathbb{Q}_l)$ with the unique maximal order $\mathrm{GL}_2(\mathbb{Z}_l)$. □

Finally, we wish to also address the bijection between the adelic double coset object and the class group of the maximal order $\mathcal{O}$. This fact follows from the fact that ideals of $\mathcal{O}$ are locally principal. We omit defining ideals of an order $\mathcal{O}$ or defining the class group here and instead refer the reader to [Vig80, §4], [Che10, §2.3] or [Voi18]. For the statement about the bijection between the class group $\mathrm{Cl}(\mathcal{O})$ and the adelic double cosets in (33) above, see for example [Che10, Theorem 2.6].

8 Pizer Graphs

In this section we give an overview of Pizer's [Piz98] construction of a Ramanujan graph. The graphs constructed by Pizer are isomorphic to the graphs of supersingular elliptic curves over $\mathbb{F}_{p^2}$ [CGL09, Section 2]. These graphs were considered by Mestre [Mes86] and Ihara [Iha66] before (cf. [JMV05]), but Pizer's construction reveals their connection to quaternion algebras, proving their Ramanujan property. In Section 9 we shall compare the resulting graphs to the LPS construction described above.

Pizer's description is in terms of a quaternion algebra and a pair of prime parameters p, l. We shall aim to keep technical details to a minimum, and focus on the choice of quaternion algebra and parameters. This elucidates the connection with the LPS construction. Recall that the meaning of the parameters is similar in both cases: the resulting graphs are $(l+1)$-regular and their size depends on the value of p. Varying p (subject to some constraints) produces an infinite family of $(l+1)$-regular Ramanujan graphs. However, we shall see that the constraints imposed on the parameters $\{p, l\}$ by the LPS and Pizer constructions do *not* agree. In Section 8.2 we give an explicit comparison between the admissible values of the parameter p in the example when $l = 5$.

First we wish to summarize the construction via Pizer [Piz98]. In particular we wish to explain the elements of [Piz98, Theorem 5.1]. Details are kept to a minimum; the reader is encouraged to consult *op.cit.* for details, in particular [Piz98, 4.]. We mention one feature of Pizer's approach in advance: we shall see that here the graph is given via its adjacency matrix. Note that this is of a different flavor from the LPS case. There the edges of the graph were specified "locally:" given a vertex of the graph (as an element of a group in Section 6.1 or as a class of lattices in Section 6.2), its neighbors were specified directly. (See Section 6.4 for an explicit parametrization of the edges at a vertex.) In Pizer's approach the adjacency matrix, a Brandt matrix (associated to an Eichler order in the quaternion algebra) specifies the edge structure of the graph.

8.1 Overview of the construction

Let us fix $B = B_{p,\infty}$ to be the quaternion algebra over $\mathbb{Q}$ that is ramified precisely at p and at infinity. We shall consider orders $\mathcal{O}$ of level $N = pM$ and $N = p^2M$ in B, where M is coprime to p. The vertex set of our graph $G(N, l)$ shall be in bijection with (a subset of) the class group of $\mathcal{O}$. The class number of $\mathcal{O}$ depends only on the level of the order and hence we may write $H(pM)$ or $H(p^2M)$ for the size of such a graph. In the case where $M = 1$ by the Eichler class number formula [Piz98, Proposition 4.4] we have:

$$H(p) = \frac{p-1}{12} + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right); \tag{35}$$

$$H(p^2) = \frac{p^2-1}{12} + \begin{cases} 0 & \text{if } p \geq 5 \\ \frac{4}{3} & \text{if } p = 3 \end{cases} \tag{36}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.

The vertex set of $G(N, l)$ shall have $H(N)$ elements when $N = pM$ and when $N = p^2M$ and l is a quadratic nonresidue modulo p. (Note that in this case the graph $G(p^2M, l)$ is bipartite.) For $N = p^2M$ and l a quadratic residue modulo p the graph $G(p^2M, l)$ is non-bipartite of size $\frac{H(p^2M)}{2}$. Recall that a similar dichotomy (between bipartite and non-bipartite cases) exists in the

LPS construction as well. The following table summarizes the size of $G(p,l)$ and $G(p^2,l)$ for the case where $\left(\frac{l}{p}\right)=1$ (and $p>3$).

$p \mod 12$	$H(p)$	$\frac{H(p^2)}{2}$
1	$\frac{p-1}{12}$	
5	$\frac{p+7}{12}$	$\frac{p^2-1}{12}$
7	$\frac{p+5}{12}$	
11	$\frac{p+13}{12}$	

(37)

The edge structure of the graph $G(N,l)$ is determined via the adjacency matrix. Recall that the rows and columns of the adjacency matrix of a graph are indexed by the vertex set. One entry of the matrix determines the number of edges between the vertices corresponding to its indices. The edge structure of $G(N,l)$ is given by a *Brandt matrix*. There is a space of modular forms associated to the order $\mathcal{O}$ of the quaternion algebra. This space has dimension as in (37) and it carries the action of a Hecke algebra. For every integer l (coprime to p) the Brandt matrix $B(N,l)$ describes the explicit action of a particular Hecke operator (T_l) on this space.

Restrictions on the parameters p and l guarantee that $B(N,l)$ is in fact the adjacency matrix of a graph. Properties of the resulting graph (e.g. the graph being simple and connected, as well as statements about its spectrum and girth) can be phrased as statements about the Brandt matrices $B(N,l)$ and in turn studied as statements about modular forms.

To ensure the edges of the graph $G(N,l)$ are undirected, $B(N,l)$ must be symmetric. By [Piz98, Proposition 4.6] this is the case for $N=pM$ if $p\equiv 1 \mod 12$ and for $N=p^2M$ if $p>3$.

To ensure the graph has no loops we must have $\mathrm{tr}B(N,l)=0$, and for no multiple edges $\mathrm{tr}(B(N,l))^2=0$. By [Piz98, Proposition 4.8] these translate to the conditions $\mathrm{tr}B(N,l)=0$, $\mathrm{tr}B(N,l^2)=H(N)$. (This depends on the relationship of the traces within a family of Brandt matrices $B(N,l)$ for fixed N and varying l.) These traces can be given in terms of parameters dependent on the order $\mathcal{O}$ [Piz98, Proposition 4.9].

It turns out that the above conditions together already guarantee that $B(N,l)$ determines a Ramanujan graph. This is the content of the following theorem.

Theorem 8.1. *[Piz98, Theorem 5.1] Let l be a prime coprime to pM and let $N=pM$. Consider the graph $G(N,l)$ determined by the Brandt matrix $B(N,l)$ as its adjacency matrix. Assume that $B(N,l)$ is symmetric, $\mathrm{tr}B(N,l)=0$ and $\mathrm{tr}B(N,l^2)=H(N)$. Then $G(N,l)$ is a non-bipartite $(l+1)$-regular simple Ramanujan graph on $H(N)$ vertices.*

Similarly, let $N=p^2M$ and assume the above conditions $\mathrm{tr}B(N,l)=0$ and $\mathrm{tr}B(N,l^2)=H(N)$ hold. If l is a quadratic nonresidue modulo p then $B(N,l)$ is the adjacency matrix of a bipartite $(l+1)$-regular simple Ramanujan graph on $H(N)$ vertices. If l is a quadratic residue modulo p then $B(N,l)$ is the adjacency matrix of two copies of an $(l+1)$-regular simple non-bipartite Ramanujan graph on $\frac{H(N)}{2}$ vertices.

Recall that the quaternion algebra B underlying the construction above is ramified at exactly two places, p and ∞. This uniquely determines the algebra $B=B_{p,\infty}$ (cf. [Piz98, Proposition 4.1]). Given a specific l one may ask for what p primes and $N=p$ are the conditions $\mathrm{tr}B(N,l)=0$ and $\mathrm{tr}B(N,l^2)=H(N)$ satisfied. This can be answered by translating the conditions to modular conditions on p. This is carried out for $l=2$ in [Piz98, Example 2]. In the LPS construction above we were interested in $l+1$ regular graphs where $l\equiv 1 \mod 4$. To compare the families of

Ramanujan graphs emerging from the two constructions, in the next section we carry out the same computation for $l = 5$.

8.2 The size of a six-regular Pizer graph

We wish to consider a special case of Pizer's construction in [Piz98, Section 5] where the order $\mathcal{O}$ is a (level p) maximal order in $B_{p,\infty}$ and the Ramanujan graph is $l+1$ regular. In particular, we are interested in the case where $l = 5$. (Since the LPS construction discussed in Section 6 requires $l \equiv 1 \mod 4$, this is the smallest l where a comparison can be made.) In this section we follow the methods of [Piz98, Example 2] to give explicit modular conditions on p to satisfy Pizer's construction. The Brandt matrix $B(p;5)$ associated to the maximal order $\mathcal{O} \subset B_{p,\infty}$ (of level p) is a square matrix of size $H(p)$. It follows from Theorem 8.1 [Piz98, Proposition 5.1] that it is the adjacency matrix of a 6-regular simple Ramanujan graph if the following conditions hold:

1. $p \equiv 1 \mod 12$
2. $\mathrm{tr}B(p,5) = 0$
3. $\mathrm{tr}B(p,5^2) = \mathrm{Cl}\mathcal{O}$

Note that here Condition 1 guarantees that the graph is symmetric, and Condition 2 that it has no loops. By [Piz98, Proposition 4.4] the condition $p \equiv 1 \mod 12$ gives $\mathrm{Cl}(\mathcal{O}) = Mass\mathcal{O} = \frac{p-1}{12}$.

The Conditions 2 and 3 concern the trace of the Brandt matrices $B(p,5)$ and $B(p,25)$ associated to $\mathcal{O}$ of level p. These can be computed using [Piz98, Proposition 4.9]. In particular, *loc. cit.* guarantees that Conditions 2 and 3 hold under certain conditions. To state these conditions we must introduce some notation. For $m = 5$ and $m = 25$ respectively, let s be an integer such that $\Delta = s^2 - 4m$ is negative. Let t and r be chosen such that

$$\Delta = s^2 - 4 \cdot m = \begin{cases} t^2 r & 0 > r \equiv 1 \mod 4 \\ t^2 4r & 0 > r \equiv 2,3 \mod 4 \end{cases} \tag{38}$$

Let f be any positive divisor of t and $d := \frac{\Delta}{f^2}$. Let $c(s,f,p)$ denote the number of embeddings of $\mathcal{O}_p^d$ into $\mathcal{O}_p$ that are inequivalent modulo the unit group $U(\mathcal{O}_p)$. By [Piz98, Proposition 4.9] we have that

$$\text{Condition 2 is satisfied} \iff c(s,f,p) = 0 \text{ for every } s, f \text{ with } m = 5 \tag{39}$$

$$\text{Condition 3 is satisfied} \iff c(s,f,p) = 0 \text{ for every } s, f \text{ with } m = 5^2 \tag{40}$$

The integers $c(s,f,p)$ are given in tables in [Piz76, pp. 692-693]. We use information in these tables to translate the conditions (39) and (40) into modular conditions on p.

First, if $m = 5$ the possible values of s, Δ, r, t and f are as follows:

s	0	1	2		3	4
Δ	-20	-19	-16		-11	-4
t	1	1	2		1	1
r	-5	-19	-1		-11	-1
f	1	1	1	2	1	1
d	-20	-19	-16	-4	-11	-4

It follows from Condition 1 that $p \nmid d = \frac{\Delta}{f^2}$. It follows from the tables in [Piz76, pp. 692–693] that $c(s,f,p) = c(s,f,p)_{p^{2\cdot 0+1}} = 0$ if and only if d is the square of a unit in $\mathbb{Z}_p$, i.e. a quadratic residue modulo p. By Condition 1 we certainly have $\left(\frac{-4}{p}\right) = \left(\frac{-16}{p}\right) = 1$ and by quadratic reciprocity $\left(\frac{d}{p}\right) = 1$ is equivalent to $\left(\frac{p}{d}\right) = 1$. It follows that by (39) that Condition 2 is satisfied if in addition to Condition 1 p satisfies the following modular conditions.

$c(s,f,p)$	$\Delta = d$	condition
$c(0,1,p)$	-20	$p \in \{1,4\} \mod 5$
$c(1,1,p)$	-19	$p \in \{1,4,5,6,7,9,11,16,17\} \mod 19$
$c(3,1,p)$	-11	$p \in \{1,3,4,5,9\} \mod 11$

(41)

Second, to guarantee that the conditions in (40) are satisfied, let $m = 25$. Then the possible values of s, Δ, r, t and f are as follows:

s	0	1	2	3	4	5	6	7	8	9
Δ	-100	-99	-96	-91	-84	-75	-64	-51	-36	-19
t	5	3	4	1	1	5	4	1	3	1
r	-1	-11	-6	-91	-21	-3	-1	-51	-1	-19
f	$1,5$	$1,3$	$1,2,4$	1	1	$1,5$	$1,2,4$	1	$1,3$	1

(42)

By (1) and (41) we have that $p \nmid d$ for any of the above values of Δ and $d = \frac{\Delta}{f^2}$. Then it again follows from the tables in [Piz76, pp. 692–693] that (40) is satisfied if and only if for any such d $\left(\frac{d}{p}\right) = 1$ or, equivalently by (1), $\left(\frac{p}{d}\right) = 1$. By properties of the Legendre symbol and the previously imposed conditions on the residue class of p modulo 12, 5, 11 and 19 this is true for $\Delta \in \{-100, -99, -75, -64, -36, -19\}$. The remaining cases amount to the following additional modular conditions on p :

Δ	$d = \frac{\Delta}{f^2}$	condition
-96	$-96,\ -24$ or -6	$p \in \{1,7\} \mod 8$
-51	$-51 = -3 \cdot 17$	$p \in \{1,2,4,8,9,13,15,16\} \mod 17$
-84	$-84 = -12 \cdot 7$	$p \in \{1,2,4\} \mod 7$
-91	$-91 = -7 \cdot 13$	$p \in \{1,3,4,9,10,12\} \mod 13$

(43)

We summarize the modular conditions on p in the following corollary.

Corollary 8.2. *The Brandt matrix $B(p;5)$ associated to a maximal order in $B_{p,\infty}$ by Pizer [Piz98] is the adjacency matrix of a 6-regular simple, connected, non-bipartite Ramanujan graph if and only if p satisfies the following congruence conditions:*

Modulus	*Remainders allowed*
24	1
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16
19	1, 4, 5, 6, 7, 9, 11, 16, 17

(44)

These conditions are equivalent to saying that $p \equiv 1 \mod 24$ *and* p *is a quadratic residue modulo the primes* $5, 7, 11, 13, 17, 19$. *Note that* p *may belong to one of* $1 \cdot 2 \cdot 3 \cdot 5 \cdot 6 \cdot 8 \cdot 9 = 12\ 960$ *residue classes modulo* $24 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 38\ 798\ 760$.

The Corollary describes the set of primes p for which $G(p, 5)$ is a six-regular Ramanujan graph. The condition $p \equiv 1 \mod 4$, $p \equiv 1, 4 \mod 5 = l$ guarantees that for these primes the LPS construction is a six-regular graph as well.

Remark 8.3. The smallest prime satisfying all the congruence conditions of Corollary 8.2 is 53881. This corresponds to a 6-regular Pizer graph with 4490 vertices. Amongst the first one million primes, 1670 satisfy all these congruence conditions.

9 Relationship between LPS and Pizer constructions

We wish to compare the two different approaches to constructing Ramanujan graphs that we have discussed. Throughout the previous sections, we have seen that the constructions of LPS and Pizer (recall the latter agree with supersingular isogeny graphs for particular choices) have similar elements. In this section, we wish to further highlight these similarities, as well as the discrepancies between the two approaches.

First let us revisit the chains of graph isomorphisms/bijections that the respective constructions fit into. These are as follows:

(LPS) $\mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_p), S) \cong \Gamma(2p)\backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l) \cong G'(\mathbb{Q})\backslash H_{2p}(\mathbb{A}_f)/K_0^{2p}$

$(\mathcal{O}[l^{-1}])^\times \backslash \mathrm{GL}_2(\mathbb{Q}_l)/\mathrm{GL}_2(\mathbb{Z}_l) \cong B^\times(\mathbb{Q})\backslash B^\times(\mathbb{A}_f)/B^\times(\hat{\mathbb{Z}}) \cong \mathrm{Cl}\mathcal{O} \cong \mathrm{SSIG}$ **(Pizer)**

Recall that in the first line, we have the LPS construction in terms of a Cayley graph on the group $\mathrm{PSL}_2(\mathbb{F}_p)$; it corresponds to the "local double coset graph" defined by taking a finite quotient of an infinite tree of homothety classes of lattices. The vertex set of this graph is in bijection with the adelic double cosets on the right-hand side. (For the sake of this comparison we omitted the infinite place.)

On the right-hand end of the second line, we have the supersingular isogeny graphs discussed in Part 1. These are symmetric simple graphs isomorphic to $G(p, l)$ constructed by Pizer (see Section 8) when $p \equiv 1 \mod 12$. The vertex set of $G(p, l)$ is the class group of a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$. This set is in bijection with the adelic double cosets. Via strong approximation (see Section 7.3) these adelic double cosets are in bijection with local double cosets, which at a place l where $B_{p,\infty}$ splits can be written as the left-hand side object.

Despite the similarities between these chains of bijections, there are significant discrepancies between the two objects. First of all, there is a discrepancy in the underlying quaternion algebras. For the LPS graphs we considered the underlying algebra of Hamiltonian quaternions ($B_{2,\infty}$). Varying the parameter p we get different Ramanujan graphs by changing the congruence subgroup $\Gamma(2p)$ without ever changing the underlying algebra. On the other hand the Pizer graphs were constructed using $B = B_{p,\infty}$. The underlying quaternion algebra varies with the choice of the parameter p. We note that the construction in LPS can be carried out for any B ramified at ∞ and split at l, and would still result in Ramanujan graphs (see [Lub10, Theorem 7.3.12]). However, in this more general case we do not have a clear path for obtaining an explicit description of these graphs as Cayley graphs. For additional details see [Lub10, Remark 7.4.4(iv)]. If one took $B_{p,\infty}$ for both the LPS and Pizer cases, the infinite families of Ramanujan graphs formed would differ

because the LPS family is formed by varying the subgroup $\Gamma(2p)$ (or more generally $\Gamma(N)$ for l a quadratic residue mod N) while the Pizer family is formed by varying the quaternion algebra $B_{p,\infty}$.

Let us consider the choice of parameters next. For the LPS graphs we required only that $l \equiv 1 \mod 4$ and that p is odd and prime to l. If -1 is a quadratic residue modulo p then the resulting graph is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ [Lub10, Theorem 7.4.3]. Furthermore, if l is a quadratic residue modulo $2p$ then this graph is non-bipartite and isomorphic to the Cayley graph of $\mathrm{PSL}_2(\mathbb{F}_p)$ with $\frac{p^3-p}{2}$ elements.

In the case of the Pizer graphs $G(N,l)$ we must have $N = pM$ coprime to l. Further congruence conditions on N guarantee properties of the resulting graph (see Section 8), e.g. $p \equiv 1 \mod 12$ guarantees that the adjacency matrix is symmetric. The number of vertices in $G(N,l)$ is then $H(N)$, the class number of an order of level N in $B_{p,\infty}$. For example if $N = p \equiv 1 \mod 12$, then this results in a graph of size $\frac{p-1}{2}$.

To compare the two in the simplest case when $l \equiv 1 \mod 4$, i.e. $l = 5$, recall that Corollary 8.2 gives the exact congruence conditions on p so that the Pizer construction of the graph $G(p,5)$ is a six-regular Ramanujan graph on $\frac{p-1}{12}$ vertices. For these primes, the LPS construction also produces a Ramanujan graph. The size of the two graphs is very different. Notice however that when both graphs exist the size of the LPS graph is divisible by the size of the Pizer graph (cf. Remark 8.3).

Let us turn our attention to the local double coset objects in the above chain of bijections. In the second line, corresponding to Pizer graphs, we have $(\mathcal{O}[l^{-1}])^\times$ appearing where $\mathcal{O}$ is an order of the quaternion algebra $B_{p,\infty}$. For the graph $G(p,l)$ this $\mathcal{O}$ is an order of level p, i.e. a maximal order. The corresponding subgroup $(\mathcal{O}[l^{-1}])^\times$ of $B^\times(\mathbb{Z}[l^{-1}])$ is analogous to the subgroup $\Gamma = G'(\mathbb{Z}[l^{-1}])$ for the LPS construction. This is much larger than the congruence subgroup $\Gamma(2p) \leq \Gamma$ that appears in the local double coset objects in that case.

The fact that the LPS construction involves this *smaller* congruence subgroup $\Gamma(2p)$ also accounts for the discrepancy between the two lines at the adelic double cosets. Recall from Section 7.2 that H_{2p} was not the entire $G'(\mathbb{A})$ but instead a finite index normal subgroup of it. We note that if one replaced $\Gamma(2p)$ in the LPS construction with $\Gamma(2N)$, where $p \mid N$, the LPS graph $\Gamma(2N)\backslash\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ is a finite cover of $\Gamma(2p)\backslash\mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l)$ [Li96, Section 3].

One may wonder if an object analogous to $\mathrm{Cl}(\mathcal{O})$ could be appended to the chain of bijections for LPS graphs. Or even if, in the local double coset object for LPS graphs $\Gamma(2p)$ could be written as $(\mathcal{O}_{2p}(\mathbb{Z}[l^{-1}]))^\times$ as well, for a quaternion order $\mathcal{O}_{2p}$. (More precisely, if $\Gamma(2p)$ agrees with the image of $(\mathcal{O}_{2p}(\mathbb{Z}[l^{-1}]))^\times$ under the map $B^\times \to G'$ for some order $\mathcal{O}_{2p}$.)

The answer to the second question is affirmative. Using the basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ for $B = B_{2,\infty}$ the requisite relationship holds between $\mathcal{O}_{2p}$ and $\Gamma(2p)$ for the order $\mathcal{O}_{2p}$ spanned by $\{1, 2p\mathbf{i}, 2p\mathbf{j}, 2p\mathbf{k}\}$. Note that this order has level 2^5p^3, hence it is not an Eichler order.

We remark that the size of the class set of this $\mathcal{O}_{2p}$ can be computed using [Piz80, Theorem 1.12] and it turns out to be $\frac{4p^2(p+1)+4}{3}$ or $\frac{4p^2(p+1)}{3}$ if $p \equiv 1 \mod 3$ or $p \equiv 2 \mod 3$ respectively. This is clearly different from the size of $\mathrm{PSL}_2(\mathbb{F}_p)$ which is a numerical obstruction to extending the chain of isomorphisms for LPS graphs analogously to the row for Pizer graphs.

References

[AAM18] Gora Adj, Omran Ahmadi, and Alfred Menezes, *On isogeny graphs of supersingular elliptic curves over finite fields*, Cryptology ePrint Archive, Report 2018/132, 2018, `https://eprint.iacr.org/2018/132`.

[Alo86] Noga Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), no. 2, 83–96, Theory of computing (Singer Island, Fla., 1984). MR 875835

[CGL06] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter, *Cryptographic hash functions from expander graphs*, J. Cryptology **22** (2009), no. 1, 93–113, available at `https://eprint.iacr.org/2006/021.pdf`. MR 2496385

[CGL09] ———, *Families of Ramanujan graphs and quaternion algebras*, Groups and symmetries, CRM Proc. Lecture Notes, vol. 47, Amer. Math. Soc., Providence, RI, 2009, pp. 53–80. MR 2500554

[Che10] Gaëtan Chenevier, *Lecture notes*, 2010, `http://gaetan.chenevier.perso.math.cnrs.fr/coursIHP/chenevier_lecture6.pdf`, retrieved August 13, 2017.

[Del71] Pierre Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki. Vol. 1968/69, vol. 179, Lecture Notes in Math., no. 355, Springer, Berlin, 1971, pp. 139–172.

[Del74] ———, *La conjecture de Weil. I*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **43** (1974), no. 1, 273–307.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), no. 3, 209–247. MR 3259113

[Gel75] Stephen S. Gelbart, *Automorphic forms on adele groups*, no. 83, Princeton University Press, 1975.

[Iha66] Yasutaka Ihara, *Discrete subgroups of* PL(2, $k_\wp$), Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 272–278. MR 0205952

[JMV05] David Jao, Stephen D Miller, and Ramarathnam Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2005, pp. 21–40.

[Li96] Wen-Ch'ing Winnie Li, *A survey of Ramanujan graphs*, Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, 1996, pp. 127–143. MR 1394930

[LP15] Eyal Lubetzky and Yuval Peres, *Cutoff on all Ramanujan graphs*, Geometric and Functional Analysis **26** (2016), no. 4, 1190–1216.

[LPS88] Alexander Lubotzky, Richard L. Phillips, and Peter Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277. MR 963118 (89m:05099)

[Lub10] Alexander Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Modern Birkhäuser Classics, Birkhäuser Verlag, Basel, 2010, With an appendix by Jonathan D. Rogawski, Reprint of the 1994 edition. MR 2569682

[Mes86] Jean-Francois Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, pp. 217–242. MR 891898

[MS11] Dustin Moody and Daniel Shumow, *Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves*, Cryptology ePrint Archive, Report 2011/430, 2011, `https://eprint.iacr.org/2011/430`.

[PLQ08] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater, *Full cryptanalysis of LPS and Morgenstern hash functions*, Security and Cryptography for Networks (Berlin, Heidelberg) (Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, eds.), Springer Berlin Heidelberg, 2008, pp. 263–277.

[Piz76] Arnold Pizer, *The representability of modular forms by theta series*, Journal of the Mathematical Society of Japan **28** (1976), no. 4, 689–698.

[Piz80] ———, *An algorithm for computing modular forms on* $\Gamma_0(N)$, Journal of Algebra **64** (1980), no. 2, 340–390.

[Piz98] ———, *Ramanujan graphs*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 159–178. MR 1486836

[PQC] *Post-Quantum Cryptography Standardization*, `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`, Accessed: 2018-04-14.

[Sar18] Naser T. Sardari, *Diameter of Ramanujan graphs and random Cayley graphs*, (2018). Combinatorica, 1–20. `https://doi.org/10.1007/s00493-017-3605-0`

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Berlin–Heidelberg–New York, 2009.

[TZ08] Jean-Pierre Tillich and Gilles Zémor, *Collisions for the LPS expander graph hash function*, Advances in Cryptology – EUROCRYPT 2008 (Nigel Smart, ed.), Springer, 2008, pp. 254–269.

[Vél71] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR 0294345

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980. MR 580949

[Voi18] John Voight, *Quaternion algebras*, 2018, `https://math.dartmouth.edu/~jvoight/quat-book.pdf`, retrieved October 20, 2017.