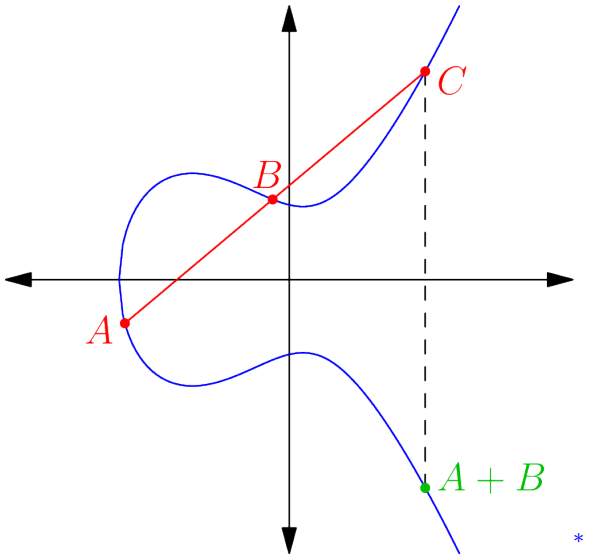
Supersingular isogeny graphs with level N structure and path problems on ordinary isogeny graphs

Megan Roda

Department of Mathematics and Statistics, McGill University, Montreal



A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Science.

April 2019

*https://usamo.wordpress.com/2015/07/05/linniks-theorem-for-sato-tate-laws-on-cm-elliptic-curves/

Acknowledgements

I would first like to thank my advisor, Professor Eyal Z Goren, for his support and mathematical insights, and for introducing me to such a beautiful subject. It has been an honour and privilege to have begun my journey in number theory with such a knowledgable mentor. Another big thank you to Professors Louigi Addario-Berry and Adrian Vetta for taking the time to mentor me in the beautiful subjects of combinatorics and random walk theory. Also, thank you to Professors Henri Darmon and Mike Lipnowski for being part of my committee. Last but not least, I would like to thank Professors Vojkan Jaksic, Dave Stephens, Jessica Lin, Jacques Hurtubise, Rustum Choksi, and Linan Chen for their guidance, either professionally or personally.

Thank you to my mother and grandparents for raising me to follow my dreams. Thank to my loving friends Cynthia, Michelle, Jinah, Andrea, Calla, Macarena and Tudor for their support (and french translation skills), and for reminding me to believe in myself during this intense year. Thank you to all my math buddies especially Aram, Reginald, Joe, and the number theory group, and my amazing officemates Wissam and Vincent.

Lastly, thank you to McGill University and NSERC for the financial support over this past year during this thesis, and during my undergraduate years.

Contents

Abstract

This thesis investigates both the structure of supersingular isogeny graphs with full level N structure, and random walks on the volcano-like graphs arising from ordinary isogeny graphs (known as isogeny volcanoes). In particular, this thesis uses strong approximation to explore the number of connected components in supersingular isogeny graphs with full level N structure and analyses a probability measure defined on the vertices of an isogeny volcano. This measure describes the probability that a certain vertex is reached in a simple random walk on the graph. The random walk represents the action of the Hecke operator on the ordinary elliptic curves given by the vertices of the graph.

Background to the problems described in this thesis is provided in the first chapter, thus making this thesis relatively self-contained. The constructions of the supersingular and ordinary isogeny graphs are provided, and are based on those of [Gor]. In the discussion we describe the interest in supersingular isogeny graphs in terms of cryptographic hash functions, and make comparisons between extremal cases of supersingular isogeny graphs with full level N structure (and variants of them) with a particular construction of the Ramanujan graphs given by [Lub].

Abrégé

Cette thèse porte sur la structure de graphes d'isogénies supersingulières avec structure de niveau N plein, ainsi que sur les balades aléatoires sur les volcans d'isogénies. En particulier, nous étudierons le nombre de composantes connexes dans les graphes d'isogénies supersingulières avec structure de niveau N plein et nous analyserons une mesure de probabilité definie sur les sommets d'un volcan d'isogénie. Cette mesure indique la probabilité qu'un certain sommet est atteint par une balade aléatoire sur le graphe. Cette balade aléatoire représente l'action d'un opérateur de Hecke sur les courbes elliptiques ordinaires obtenues à partir des sommets du graphe.

Le contexte des problèmes abordés dans cette thèse est décrit dans le premier chapitre. Les constructions de graphes d'isogénies ordinaires supersingulières sont basées sur celles de

[Gor]. De plus, nous décrirons dans la conclusion l'application des graphes d'isogénies supersingulières à la construction de fonctions de hashage cryptographique, et nous comparerons certains cas particuliers de graphes d'isogénies supersingulières avec structure de niveau N plein avec la construction de graphes de Ramanujan définie par [Lub].

0 Introduction

This thesis focuses on supersingular and ordinary isogeny graphs resulting from elliptic curves and isogenies between them. The exploration of these graphs in this thesis required a variety of different areas of mathematics spanning number theory, graph theory and combinatorics. Our focus on ordinary isogeny graphs is almost strictly combinatorial. We investigate problems dealing with paths on these volcano-like graphs (known as isogeny volcanoes). These paths have relations to the action of the Hecke operator on the ordinary elliptic curves representing each vertex. In terms of the supersingular isogeny graphs, we rely on number theory and graph theory to analyse these graphs when they have added layers of structure, i.e. level N structure (which will be defined and discussed in section 2.2. Lastly, in our discussion we make comparisons between variants of these supersingular isogeny graphs with level N structure and the construction of the Ramanujan graphs of [Lub].

The first section of this thesis strictly contains the background information necessary to establish the setting and notation, as well as important facts used in this thesis. Since a variety of facts used belong to a variety of different areas of math, we considered it necessary as most readers will most likely only have sufficient knowledge in one of these fields. We begin with a review of basics in number theory. We define adeles and ideles, and crucial information about elliptic curves and isogenies which make up the vertices and edges of our isogeny graphs. Further, we discuss basic definitions in graph theory and covering spaces, introduce the theory of expander graphs, and give the Ramanujan bound. The Ramanujan bound is the defining feature of Ramanujan graphs, which are optimal expander graphs and a serious object of interest in this thesis.

In the following section of this thesis, we give the construction of the ordinary and supersin-

gular isogeny graphs that will be examined. The setting and basic structure is established for each. In the third section, we begin with a description of a tool needed to calculate the number of connected components of supersingular isogeny graphs with level N structure, namely, strong approximation. We discuss algebraic groups and establish the necessary theorems for our calculations, and subsequently perform this calculation.

In the fourth section, we begin by examining two probability measures defined on the ordinary ℓ-isogeny volcano and its covering space, the $(\ell+1)$-infinite tree. In each case the probability measure is meant to demonstrate the weight held by a vertex in a random walkof fixed length starting from some fixed vertex, i.e. the probability the random walk ends on that vertex. We attempt to further characterize this random walk for the covering space and our isogeny volcano.

Lastly, our fifth section takes us into a discussion of the importance of supersingular isogeny graphs and their applications to pseudorandomness and cryptographic hash functions. In the third section we examined properties of supersingular isogeny graphs with level N structure and ask if they offer more security that the standard supersingular isogeny graph. Further, we derive a variant of these supersingular isogeny graphs with level N structure and draw comparisons with the construction of [Lub].

1 Background

Here we cover the concepts, theorems and notation required to understand the results presented in this thesis. This section contains no original material.

1.1 Number theory fundamentals

Throughout this subsection, we follow the presentation of [Gold] to establish the required notation.

1.1.1 Absolute Values and the p-adics

Definition 1. *Let K be a field, we define an* ***absolute value*** *to be a non-negative function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following properties:*

1. $|a| = 0 \iff a = 0$
2. $|ab| = |a| \cdot |b|$ *for all* $a,\ b \in K$
3. $|a + b| \leq |a| + |b|$ *for all* $a,\ b \in K$.

There are two types of absolute value. One says that an absolute value is **non-archimedian** if for all $a,\ b \in K$ it satisfies

$$|a + b| \leq \max\{|a|,\ |b|\},$$

otherwise we say its **archimedian**. The most obvious example of an archimedian absolute value would be the standard one on any field $K \subseteq \mathbb{R}$, i.e.

$$|a| = \begin{cases} a & a > 0 \\ -a & a < 0 \end{cases}.$$

More importantly, for every prime p, we can define the non-archimedian absolute value $|\cdot|_p$

on $\mathbb{Q}$ as follows: for every $a \in \mathbb{Q}$, $a = p^k \frac{m}{n}$, such that $m, n \in \mathbb{Z}$, $\gcd(p, m) = \gcd(p, n) = 1$,

$$|a|_p = p^{-k}.$$

By a theorem of Ostrowski, we know that $\{|\cdot|_p : p \text{ prime}\}$, and the previously defined archimedian absolute value are the only absolute values on $\mathbb{Q}$ up to equivalence [Kn67].

One can analytically construct the p-adic field, denoted $\mathbb{Q}_p$, by completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. We denote the $\mathbb{Z}_p$ the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. Note also that the completion of $\mathbb{Q}$ with respect to the standard archimedian absolute value that we defined is simply $\mathbb{R}$. We shall denote this $\mathbb{Q}_\infty$.

1.1.2 Adeles and Ideles

We define the **ring of adeles** over $\mathbb{Q}$, denoted $\mathbb{A}_\mathbb{Q}$ or $\mathbb{A}$, as

$$\mathbb{A}_\mathbb{Q} = \mathbb{R} \times \prod_p{}' \mathbb{Q}_p = \{\{x_\infty, x_2, x_3, \dots\} : x_v \in \mathbb{Q}_v \ \forall \ v \leq \infty, \ x_p \in \mathbb{Z}_p \ (\forall \text{ but finitely many } p)\},$$

where $\prod'$ denotes the restricted product, meaning that all but finitely many $x_v \in \mathbb{Z}_v$. Multiplication and addition of adeles is defined in the obvious component-wise manner.

The **ideles** are very similar, they are denoted $\mathbb{A}_\mathbb{Q}^\times$ or $\mathbb{A}^\times$ and are defined as

$$\mathbb{A}_\mathbb{Q}^\times = \{\{x_\infty, x_2, x_3, \dots\} \in \mathbb{A}_\mathbb{Q} : x_v \in \mathbb{Q}_v^\times \ \forall \ v, \ x_p \in \mathbb{Z}_p^\times \ (\forall \text{ but finitely many } p)\}.$$

We also need the notion of **finite adeles and ideles**, denoted $\mathbb{A}^f$ and $\mathbb{A}^{f\,\times}$ respectively, and defined as

$$\mathbb{A}^f = \{\{x_2, x_3, \dots\} : x_v \in \mathbb{Q}_v \ \forall \ v < \infty, \ x_p \in \mathbb{Z}_p \ (\forall \text{ but finitely many } p)\},$$

$$\mathbb{A}^{f\,\times} = \{\{x_2, x_3, \dots\} : x_v \in \mathbb{Q}_v^\times \ \forall \ v < \infty, \ x_p \in \mathbb{Z}_p^\times \ (\forall \text{ but finitely many } p)\}.$$

1.2 Elliptic Curves

1.2.1 Basic definitions

In this thesis we work with elliptic curves in characteristic p for some fixed prime p, in particular we define them over $\bar{\mathbb{F}}_p$. In this subsection, our discussion of elliptic curves uses results from [Sil]. Further information can be found in [Sil].

Firstly, every such curve over a field k (in our case $\bar{\mathbb{F}}_p$) is defined as a non-singular curve of genus one and can be written as the locus in $\mathbb{P}^2$ of a cubic equation with the base point $\mathcal{O} \in E(k)$ on the line at infinity. We can write it in Weierstrass form,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

regardless of p.

Taking our Weierstrass form we can go further, via a simple tranformation when the characteristic of the field is not 2. We can write it as

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

We can then define the **j-invariant** of an elliptic curve as

$$j(E) = \frac{c^3}{\Delta},$$

where

$$c = b_2^2 - 24b_4,\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

The importance of this function for our purposes stems from the well-known fact that elliptic curves defined over $\bar{\mathbb{F}}_p$ with the same j-invariant are isomorphic over $\bar{\mathbb{F}}_p$.

Morphisms $\varphi : E_1 \to E_2$ between elliptic curves (defined over $\bar{\mathbb{F}}_p$) that fix the base point $\mathcal{O}$ of

the elliptic curve are called **isogenies**. Isogenies also have **duals**; if $\varphi : E_1 \to E_2$, the dual, denoted $\widehat{\varphi}$, is the map $\widehat{\varphi} : E_2 \to E_1$ such that

$$\varphi \circ \widehat{\varphi} = \widehat{\varphi} \circ \varphi = [\ell],$$

where ℓ is the degree of the morphisms φ and $\widehat{\varphi}$, and $[\ell]$ denotes a multiplication by ℓ map. This map $[\ell]$ is defined for every natural number ℓ:

$$[\ell]P = \underbrace{P \oplus P \oplus P \cdots \oplus P}_{\ell \text{ times}}.$$

For an elliptic curve E over $\bar{\mathbb{F}}_p$, and a positive integer m we define

$$E[m](\bar{\mathbb{F}}_p) = \{P \in E : [m]P = \mathcal{O}\}.$$

However, we will mostly write $E[m]$ for $E[m](\bar{\mathbb{F}}_p)$. If m is non-zero in $\bar{\mathbb{F}}_p$ and $p \nmid m$ then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

In fact, since the characteristic of the base field is p, one of the following is true; either

$$E[p^e] = \{\mathcal{O}\}, \ \forall \ e \in \mathbb{N},$$

or

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}, \ \forall \ e \in \mathbb{N},$$

where per our notational convention, $E[p^e]$ is $E[p^e](\bar{\mathbb{F}}_p)$. In the first case the elliptic curve is called **supersingular** and in the second case the elliptic curve is called **ordinary**.

We define $\mathrm{Hom}(E_1, E_2)$ to be the group of isogenies between E_1 and E_2. Hence $\mathrm{End}(E)$ denotes the isogenies that are endomorphisms of E. It is important to note that the multiplication by m isogenies give an embedding of $\mathbb{Z}$ into the ring $\mathrm{End}(E)$ for every elliptic curve E.

With the exception of the zero isogeny, every isogeny is a finite map of curves and gives us an injection of the function fields,

$$\varphi^* : \bar{K}(E_2) \to \bar{K}(E_1).$$

If the extension $\bar{K}(E_1)$ over $\varphi^*(\bar{K}(E_2))$ is seperable, then we say the isogeny φ is **seperable**, and its degree is the degree of the extension.

Chapter 3 of [Sil] gives us the following result about seperable isogenies:

Proposition 1. *Let $\varphi : E_1 \to E_2$ be a non-zero isogeny then*

$$\ker(\varphi) = \varphi^{-1}(\mathcal{O})$$

is a finite group. In particular, if φ is seperable, and φ is unramified, then

$$|\ker(\varphi)| = deg(\varphi).$$

In our case we will be considering ℓ-isogenies of elliptic curves for some fixed prime ℓ. The following theorem gives us a way to construct these isogenies [Velu], see [Wash].

Theorem 1. *Let*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be an elliptic curve with the a_i in field k. Let C be a finite subgroup of $E(\bar{k})$, there exists E_2, an elliptic curve, and $I : E \to E_2$, a seperable isogeny such that $C = \ker(I)$. The isogeny I can be explicitly given as follows: Let $Q = (x_Q, y_Q) \in C$, $Q \neq \infty$, and define the following quantities,

$$
\begin{aligned}
g_Q^x &= 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q \\
g_Q^y &= -2y_Q - a_1x_Q - a_3 \\
v_Q &= \begin{cases} g_Q^x & \text{if } 2Q = \infty \\ 2g_Q^x - a_1g_Q^y & \text{if } 2Q \neq \infty \end{cases} \\
u_Q &= (g_Q^y)^2
\end{aligned}
$$

Now decompose the subgroup C as follows. Let C_2 be the set of points of order 2 in C, then pick R such that

$$C = \{\infty\} \cup C_2 \cup R \cup (-R),$$

and denote $S = R \cup C_2$. Let

$$v = \sum_{Q \in S} v_Q, \quad w = \sum_{Q \in S} (u_Q + x_Q v_Q).$$

Then we can write E_2 as

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

where the $A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3$ and

$$A_4 = a_4 - 5v, \quad A_6 = a_6 - (a_1^2 + 4a_2)v - 7w.$$

One then writes the isogeny I as

$$X = x + \sum_{Q \in S} \left(\frac{v_q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right)$$

$$Y = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1x + a_3}{(x - x_Q)^3} + v_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \right).$$

Conversely, given any isogeny of elliptic curves, the kernel is a finite subgroup.

Further, for our cases, given ℓ prime, $\ell \neq p$, there exists an $\ell + 1$ subgroups in $E[\ell]$ of order ℓ. Each is the kernel of a seperable isogeny of degree ℓ (an ℓ-isogeny). Every ℓ-isogeny arises this way [Sut].

1.2.2 Tate module

We have the following definition:

Definition 2. *Let E be an elliptic curve defined over $\bar{\mathbb{F}}_p$ and let $\ell \in \mathbb{N}$ be a prime. The (ℓ-adic) Tate module of E is the group*

$$T_\ell(E) = \lim_{\leftarrow n} E[\ell^n].$$

The inverse limit is taken with respect to the maps

$$[\ell] : E[\ell^{n+1}] \to E[\ell^n].$$

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, the Tate module has a $\mathbb{Z}_\ell$ structure.

The inverse limit topology of the Tate module is equivalent to the ℓ-adic topology given by the $\mathbb{Z}_\ell$-module structure. As $\mathbb{Z}_\ell$ modules, the Tate module has the following structure theorem:

Theorem 2. *As a $\mathbb{Z}_\ell$-module, the Tate module has the following structure:*

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Further if E is supersingular and $p = \mathrm{Char}(\bar{\mathbb{F}}_p)$, then

$$T_p(E) \cong \{0\}$$

and if E is ordinary

$$T_p(E) \cong \mathbb{Z}_p$$

as a $\mathbb{Z}_p$-module.

1.3 Graph theory fundamentals

1.3.1 Basic definitions

We keep our definitions consistent with those of [Gor].

Let $G = (V, E)$ be a graph, where V is the vertex set, and E is the set of edges. The **degree of a vertex** in the case that the graph G is undirected, is equal to the number of edges coming from the vertex. If there is a loop at a vertex (i.e. an edge between the vertex and itself) it only contributes one to the degree. If this undirected graph has the same degree, k, for each vertex we can define the **degree of the graph** to be k and we say the graph is **k-regular**.

Let G be an undirected graph. A **walk** on such a graph is a sequence of edges $\{e_i : v_i \to w_i\}_{i=1,\dots d} \subset E$ where $w_i = v_{i+1}$ for all i. It is closed if $v_1 = w_d$, and open otherwise. In the case that the walk does not have repeated vertices or edges we call this a **path**. By this definition, paths are inheritantly open walks. If for every pair of vertices, (v, w), there exists a path, i.e. a sequence of edges starting at v and ending at w, $e_1, \dots e_d$, such that $e_d \circ e_{d-1} \circ \dots e_1 : v \to w$, then we say the graph is **connected**.

We say a graph is **infinite** if the number of vertices it has is infinite. Using the same definition as [Gor], for a prime ℓ, we say that an infinite, connected, undirected graph $G = (V, E)$ is an **ℓ-volcano** if there exists a function $b : V \to \mathbb{N}$ such that

1. G is $(\ell + 1)$-regular.

2. $b^{-1}(0)$ with induced subgraph structure (which we call the **rim**) is a finite, regular, connected graph of degree at most 2

3. For each $i > 0$ each vertex in $b^{-1}(i)$ is connected to a unique vertex in $b^{-1}(i-1)$ and these edges account for every edge appearing outside the rim.

This structure will become important when we study ordinary isogeny graphs.

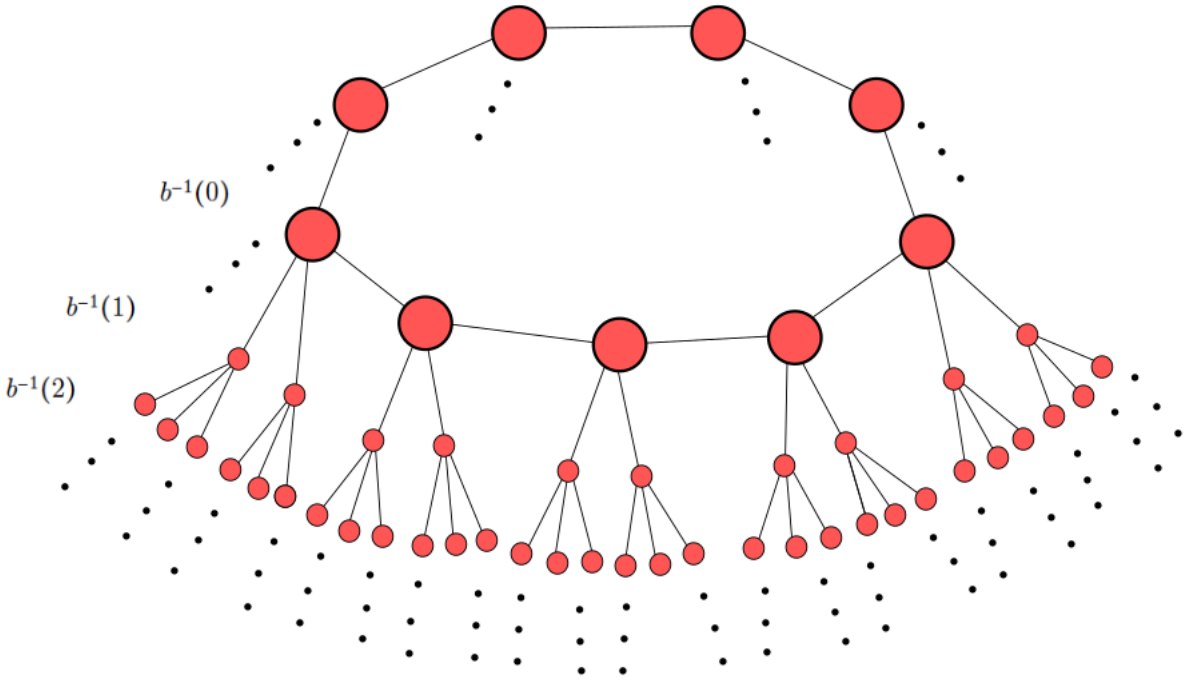


Figure 1: A ℓ-isogeny volcano with $\ell = 3$.

1.3.2 Covering Graphs

The theory of covering spaces is very applicable to connected graphs. Following [Mas], we can view an undirected graph as a Hausdorff space X, where the set of vertices V is a discrete, closed subspace and the following conditions are satisfied:

1. $X \setminus V$ is the disjoint union of open subsets e_i such that each e_i is homeomorphic to an open interval of $\mathbb{R}$. These e_i are the edges.

2. the boundary of each edge e_i, $\bar{e_i} \setminus e_i$ is a subset of V containing either 1 or 2 points, i.e. either the edge is a loop or it connected two vertices. In the case it connects two vertices, $\bar{e_i}$ is homeomorphic to $[0,1] \subset \mathbb{R}$ and e_i is homeomorphic to $]0,1[\subset \mathbb{R}$. Otherwise e_i is homeomorphic to $S^1 \setminus \{1\}$ and $\bar{e_i}$ is homeomorphic to S^1.

3. X has the weak topology, i.e. for $A \subset X$, it is closed if and only if $\bar{e_i} \cap A$ is closed for every edge e_i. Similarily for open.

Making this connection, we can define **covering graphs**, which are **covering spaces** of graphs when they are viewed as topological spaces.

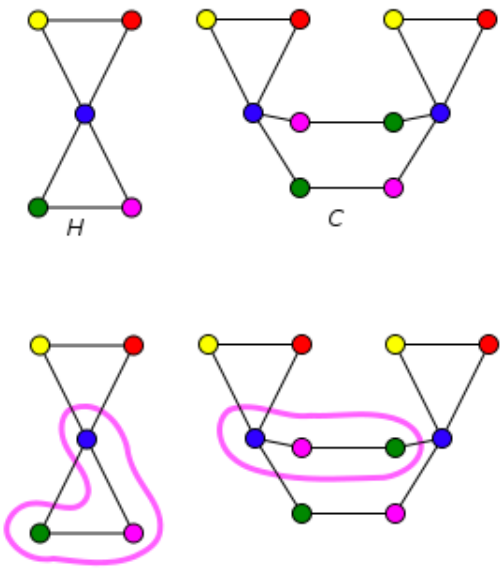
Definition 3. *A **covering space** of a topological space X is a topological space Y equipped a surjective continuous map $\rho : Y \to X$ such that for each $x \in X$ there exists U, an open neighbourhood of x such that $\rho^{-1}(U)$ is a union of disjoint open sets in Y, each isomorphic via ρ to U.*

Covering spaces of graphs are also graphs in the natural way: for X a graph with vertex set V viewed as a Hausdorff space, if Y is a covering space associated continuous map p, then Y is a graph and $p^{-1}(V) = U$ is its vertex set [Mas].

The following theorem from [Mas], helps us understand the fundamental groups of graphs.

Theorem 3. *The fundamental group of any graph is a free group.*

From the basics of covering space theory, we know that the **universal covering space** of a topological space X is the covering space of X with trivial fundamental group (i.e. it is **simply connected**).



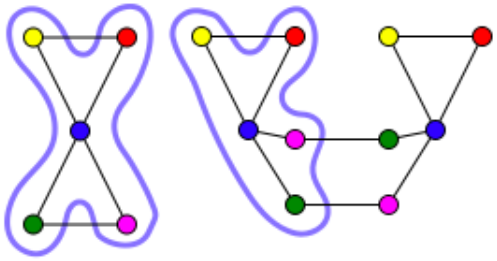


Figure 2: In the above figures, H is a graph and C is its covering space. In the second and third photos, one can see how exactly C maps surjectively onto H [†]

For our purposes, the best example is the universal covering of a k-regular graph, which is the k-infinite tree. It is well-known that the k-regular infinite tree has trivial fundamental group.

1.3.3 Expander Graphs

We digress to an important representation of a finite graph, its adjacency matrix. For such a graph we can enumerate the vertices in V as $\{v_1, \dots v_n\}$ and say $v_1 \sim v_2$ if there exists e_i in E, an edge between them. We define the matrix $\{a_{ij}\}$ as follows:

$$a_{ij} = \begin{cases} 1 & v_i \sim v_j \\ 0 \text{ otherwise} & \end{cases}$$

Definition 4. *A Symmetric matrix M is a matrix equal to its transpose, M^T. Note that M is symmetric if and only if with respect to the standard inner product on $\mathbb{R}^n$ we have $\langle x, My\rangle = \langle Mx, y\rangle$ for all x and $y \in \mathbb{R}$*

Definition 5. *A Hermitian Matrix M is a matrix equal to its own conjugate transpose denoted M^*.*

The following theorem is attributed to Augustin Cauchy:

Theorem 4. (Spectral Theorem) *Every real symmetric matrix M can be diagonalized by an orthogonal matrix, i.e. there exists an orthogonal matrix P such that $M = PDP^T$. Further, the diagonal entries of D are real valued.*

[†]https://en.wikipedia.org/wiki/Covering_graph

For a finite, undirected graph, the adjacency matrix is symmetric. Since it has real entries (0's and 1's) it is a Hermitian matrix, hence we can apply the spectral theorem. If M is an $n \times n$ adjacency matrix, then we have n real eigenvalues.

The eigenvalues of the adjacency matrix are of vital importance. We use the eigenvalues of an adjacency matrix to determine whether it is a "good expander". Intiutively, good expander graphs are such that any "small" set of vertices chosen from the graph has a "large" boundary (is connected to many other points). For this discussion, we concern ourselves with k-regular graphs and ask what makes them good expanders.

Consider a subset $A \subseteq V$ of vertices. Denote ∂A as the **boundary** of A defined to be the set of all edges going from a vertex in A to a vertex outside of A, i.e.

$$\partial A = \{(v, v') \in E : v \in A,\ v' \in V \setminus A\}.$$

For our k-regular graphs we define the **Cheeger constant** (or the **expansion ratio**), denoted $h(G)$, as follows:

$$h(G) = \min\{\frac{|\partial A|}{|A|} : A \subseteq V, 0 < |A| \leq \frac{1}{2}V(G)\}.$$

Define the spectral gap to be $k - \lambda_2$ where λ_2 is the second largest eigenvalue. It turns out that $h(G)$ is bounded away from zero if and only if the spectral gap is bounded away from zero [Hoo]. Results of [Alon] and [Che][‡] prove the following inequality for k-regular graphs:

$$\frac{1}{2}(k - \lambda_2) \leq h(G) \leq \sqrt{2k(k - \lambda_2)}.$$

We see that the spectral gap provides an estimate on the expansion of a graph [Hoo]. Hence, a good expander graph is one with a small value for λ_2 (note that if our graph is not k-regular, this is not always enough).

[‡]Cheeger defined the "Cheeger constant" in the context of Riemannian manifolds and established the analogous inequality for eigenvalues of the Laplacian operator of such a manifold.

The Alon-Boppana theorem says that for all k-regular graphs "large enough" satisfy

$$\lambda_2 \geq 2\sqrt{k-1} - o_n(1),$$

where $o_n(1) \to 0$ as $n \to \infty$ (for fixed k) and n is the number of vertices [Hoo]. This motivates the following definition.

Definition 6. *A **Ramanujan graph** is a k-regular graph that satisfies the bound*

$$\lambda_2 \leq 2\sqrt{k-1}$$

This is consistent with the definition found in [Lub]. These Ramanujan graphs are very difficult to construct, but their uses are vast. These graphs are optimal expander graphs and have a wide variety of applications, for example, error-correcting codes, construction of fault-tolerant networks, and as we will see, post-quantum cryptography [Vad].

2 Isogeny graphs

As we have previously discussed, there are two different types of elliptic curves. These give rise to two different types of isogeny graphs: ordinary and supersingular. For both, we shall follow the construction of [Gor]; see also [Sut].

2.1 Ordinary ℓ-isogeny graphs

For this thesis, we are only interested in the simplest case of ordinary ℓ-isogeny graphs. In [Gor] one will notice that the construction is more complicated. We are concerned with the "level 1" construction of these graphs.

Fix two distinct primes ℓ and p. Consider an ordinary elliptic curve E defined over $\bar{\mathbb{F}}_p$. We may assume throughout that $\mathrm{End}^0(E) \not\cong \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, then all elliptic curves in the volcano have $\mathrm{Aut}(E) = \{\pm 1\}$. Now we construct our graph ordinary ℓ-isogeny graph $\Lambda(p, \ell, E)$ (for which we will simply write $\Lambda(p, \ell)$). Define the first vertex to be E, or its j-invariant.

Since E is ordinary, $E[p]$ is non-trivial and isomorphic to $(\mathbb{Z}/p\mathbb{Z})$. Additionally, since ℓ is coprime to p, we have

$$E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2 .$$

Consider the ℓ-isogenies of E. All non-zero isogenies induce a surjective group homomorphism with finite kernel; in this case the kernels have size ℓ and the isogenies are seperable. We distinguish isogenies up to an equivalence relation, we say $\varphi \sim \psi$ if they are isogenies between elliptic curves E_1 and E_2 with the same kernel.

It is a well-known fact that every finite subgroup of $E(\bar{\mathbb{F}}_p)$ is the kernel of a seperable isogeny and its uniquely determined up to the equivalence relation. Since we are concerned with ℓ-isogenies, we note that there are $\ell + 1$ cyclic subgroups of $E[\ell]$ each of which defines a seperable isogeny over $\bar{\mathbb{F}}_p$ [Sut]. As discussed before, every ℓ-isogeny of E arises this way. With this fact, we finish the construction of $\Lambda(p, \ell)$. We define the vertices to be elliptic

curves that arise in the graph when there is an ℓ-isogeny between it and another elliptic curve already existing in the graph. The edges are defined as these ℓ-isogenies. When computing the isogeny graph, we use Velu's formulae from the previous section to compute such isogenies.

Additionally, every ℓ-isogeny has a unique dual isogeny [Sut]. By identifying the ℓ-isogenies with the corresponding dual isogeny we construct an undirected graph that we still denote $\Lambda(p, \ell)$. This concludes our discussion of the construction of the graph. In terms of the structure of this graph, we have the following theorem (see [Sut]):

Theorem 5. *For E an ordinary elliptic curve defined over $\bar{\mathbb{F}}_p$ such that $End^0(E) \ncong \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, the graph $\Lambda(p, \ell)$ is an ℓ-volcano and is hence an infinite $\ell + 1$-regular graph.*

2.2 Supersingular Isogeny Graphs

The construction of the supersingular isogeny graphs is very similar to that of the ordinary ones. One fixes p and ℓ, two distinct primes, but this time we require $p \equiv 1 \mod 12$ to ensure that for any E, a supersingular elliptic curve defined over $\bar{\mathbb{F}}_p$, we still have that $\mathrm{Aut}(E) = \{\pm 1\}$. One still defines the vertices of the graph to be those elliptic curves ℓ-isogenous to another elliptic curve in the graph and the edges to be these ℓ-isogenies. To compute the graph, one still considers the $\ell + 1$ subgroups of $E[\ell]$ and uses Velu's formulae to construct ℓ-isogenies (and hence ends up with a $\ell + 1$-regular graph). However, for our purposes, we need to state a slightly more generalized construction in terms of the vertices, we call these supersingular isogeny graphs with "level N" structure.

Definition 7. *For N such that $\gcd(N, \ell) = 1$, we say a graph has **level** $\Gamma(N)$ **structure** **(full level** N **structure)** if associated to every vertex is a pair (E, α) where E is an elliptic curve with the structure discussed above and α is an isomorphism*

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N].$$

Again, these α are defined up to composition with automorphisms. An ℓ-isogeny, f, between elliptic curves E and E' defines an edge between the pairs (E, α) and $(E', f \circ \alpha)$.

3 Strong Approximation

3.1 Algebraic Groups

We follow [Kn67] Chapter 10 by M. Kneser.

Definition 8. *Let k be an algebraically closed field. An **algebraic group** defined over k is an algebraic variety G defined over k together with mappings $(x, y) \mapsto xy$ of $G \times G$ into G and $x \mapsto x^{-1}$ of G into G which are morphisms of algebraic varieties and satisfy the usual group axioms.*

An **algebraic subgroup** is a closed subgroup with respect to the Zariski topology. An algebraic group is **linear** if it is affine as an algebraic variety. An example of a linear algebraic group is $GL_n(k)$. The structure of $GL_n(k)$ as an affine algebraic group is [Pra]:

$$GL_n(k) = \left\{ \begin{pmatrix} A & 0 \\ 0 & a_{n+1} \end{pmatrix} : \det A \cdot a_{n+1} = 1 \right\}$$

where the multiplication map $m : GL_n(k) \times GL_n(k) \to GL_n(k)$ takes $(A)_{ij} \cdot (B)_{ij} \mapsto (C)_{ij}$.

A linear algebraic group G is called **unipotent** if every algebraic representation of G consists of unipotent matrices. A **unipotent matrix** A is a matrix such that $A - I$ is nilpotent, where I is the identity matrix [W]. A **connected algebraic group** that is projective as an algebraic variety is an **abelian variety**. Abelian varieties, as one would expect, are commutative. The best example of an abelian variety is an elliptic curve. Any algebraic group G has a connected component denoted G_0. It turns out that G_0 has a unique maximal linear connected algebraic subgroup denoted G_1. It is normal and G_0/G_1 is an abelian variety.

A homomorphism $\varphi : G \to H$ of connected groups of the same dimension is called an **isogeny** if the kernel of φ is finite. To exclude unpleasant phenomena, we define a **central isogeny**

to be an isogeny whose kernel is contained in the center of G. If $\varphi : G \to H$ is a central isogeny, we say that G is a **central covering** of H.

Definition 9. *An **almost simple group** G is a group with finite center C such that G/C is a simple group (i.e. has no non-trivial normal subgroups).*

Definition 10. *An algebraic group G over a field of characteristic zero is **simply connected** if there is no non-trivial central isogeny $H \to G$ where H is a connected algebraic group.*

3.2 Strong approximation

There are many perspectives we can consider when it comes to strong approximation. The first we consider will deal with the adeles over $\mathbb{Q}$, $\mathbb{A}_{\mathbb{Q}}$.

Following along with [Gold], we begin with a new definition:

Definition 11. *Let a group G act on a set X (say, on the left). We define a **fundamental domain** of this group action to be a subset D of X satisfying:*

1. *For each $x \in X$, there exists $d \in D$ and $g \in G$ such that $gx = d$*

2. *The choice of d is unique.*

Remark 1. *One could say that the fundamental domain is really a set of representatives from each orbit of G under the group action.*

Examining the fundamental domain is key to understanding this perspective on strong approximation. We let $\mathbb{Q}$ act on $\mathbb{A}_{\mathbb{Q}}$ as follows: embed $\mathbb{Q}$ in $\mathbb{A}_{\mathbb{Q}}$ by taking each $q \in \mathbb{Q}$ and viewing it as $\{q, q, \dots\}$. Since $|q|_v > 1$ for only finitely many $v \leq \infty$, we have $q \in \mathbb{Z}_p$ for all but finitely many p and hence $\{q, q, \dots\}$ is a valid element of $\mathbb{A}_{\mathbb{Q}}$. Then our action of $\mathbb{Q}$ on the set of adeles is defined to be additive, i.e. for $q \in \mathbb{Q}$ and $x = \{x_\infty, x_2, x_3 \dots\} \in \mathbb{A}_{\mathbb{Q}}$ the action is $q + x = \{q + x_\infty, q + x_2, q + x_3, \dots\}$.

Still following [Gold], constructing the fundamental domain for the above action turns out to be equivalent to a version of the Chinese Remainder Theorem in terms of p-adic absolute values. Also, we have the following theorems (theorem 1.4.4 and proposition 1.4.5 resp.

[Gold]) completing our discussion of strong approximation from the perspective of fundamental domains.

Theorem 6. *(Weak Approximation) Let $p_1, p_2, \dots p_n$ be distinct primes. Let $c_i \in \mathbb{Q}_{p_i}$. For every $\epsilon > 0$, there exists $\alpha \in \mathbb{Q}$ such that*

$$|\alpha - c_i|_{p_i} < \epsilon.$$

Theorem 7. *(Fundamental domain for the action of $\mathbb{Q}^\times$ on $\mathbb{A}_\mathbb{Q}^\times$) A fundamental domain D for the action of $\mathbb{Q}$ on $\mathbb{A}_\mathbb{Q}$ is*

$$D = \{\{x_\infty, x_2, x_3, \dots\} : 0 \le x_\infty < 1, x_p \in \mathbb{Z}_p \text{ for all finite primes } p\}.$$

There is also a strong approximation for the ideles, (proposition 1.4.6 [Gold]):

Theorem 8. *A fundamental domain D for $\mathbb{Q}^\times \setminus \mathbb{A}_\mathbb{Q}^\times$ is*

$$D = \left\{\{x_\infty, x_2, x_3, \dots\} : 0 < x_\infty < \infty,\ x_p \in \mathbb{Z}_p^\times \text{ for all finite primes } p\right\}.$$

Now, following [Rap] we consider a different perspective on strong approximation by viewing it as a lift of solutions to polynomial equations mod m to integer solutions.

Suppose we have a family of polynomials $\{f_\alpha(x_1, \dots x_d)\}_\alpha \in \mathbb{Z}[x_1, \dots x_d]$ where the $\alpha \in I$. We can use these polynomials to define a closed affine subscheme $X = \mathrm{Spec}(\mathbb{Z}[x_1, \dots x_d]/f_\alpha) \hookrightarrow \mathrm{Spec}(\mathbb{Z}[x_1, \dots x_d])$. Pick a $\mathbb{Z}$-algebra R, then

$$X(R) = \{(a_1, \dots a_d) \in R^d : f_\alpha(a_1, \dots a_d) = 0 \ \forall\ \alpha \in I\},$$

is the set of R-valued points of the scheme X.

Obviously, $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ are $\mathbb{Z}$-algebras for any m. Let

$$\rho_m : X(\mathbb{Z}) \to X(\mathbb{Z}/m\mathbb{Z}),$$

denote the map induced by the natural reduction map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. The question we deal with in strong approximation is whether this map is surjective (if its even a well-posed question, i.e. $X(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$). If the map ρ_m is surjective for all m, then we say X has strong approximation. For example, GL_2 does not have strong approximation, but SL_2 does.

To see that GL_2 does not have strong approximation is simple, note that for $m = 5$ the above map is not surjective. Matrices in the image of ρ_5 have determinant $\pm 1 \mod 5$ because the matrices of $GL_2(\mathbb{Z})$ have determinant ± 1. However, a matrix such as

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}$$

belongs to $GL_2(\mathbb{Z}/5\mathbb{Z})$ but does not belong to the image under ρ_5 of $GL_2(\mathbb{Z})$.

To see that SL_2 has strong approximation is not as trivial but is still simple, see [Rap] pg. 271.

Note that, if $m|n$ then we have a natural map $\pi_m^n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We get an inverse system $\{\mathbb{Z}/m\mathbb{Z}, \pi_m^n\}$ with inverse limit denoted

$$\widehat{\mathbb{Z}} = \lim_{\leftarrow m} \mathbb{Z}/m\mathbb{Z} = \{(a_i) \in \prod_{m \in \mathbb{Z}} \mathbb{Z}/m\mathbb{Z} : \pi_i^j(a_i) = a_j\}.$$

Endowing each group $\mathbb{Z}/m\mathbb{Z}$ with the discrete topology and $\prod_m \mathbb{Z}/m\mathbb{Z}$ the product topology, we let $\widehat{\mathbb{Z}}$ have the induced topology as a subspace of $\prod_m \mathbb{Z}/m\mathbb{Z}$ [Klop].

Remark 2. *In fact, this makes $\widehat{\mathbb{Z}}$ into a profinite group, i.e. a totally disconnected, compact, Hausdorff topological group, but this is not needed for our discussion [Klop].*

By [Rap], the condition given in order to have strong approximation is proven to be equivalent to the condition that the natural embedding $X(\mathbb{Z}) \to X(\widehat{\mathbb{Z}})$ has a dense image under the topology we just described.

Remark 3. *There are some necessary but not sufficient conditions for X to satisfy if it is to have strong approximation. We see in GL_2 that there is an obstruction preventing it from having strong approximation! In order for an affine $\mathbb{Q}$-variety X to have strong*

approximation, $X(\mathbb{Z})$ must be Zariski-dense in X.

From [Kn66] and [Plat], we now take an approach to strong approximation that doesn't focus on algebraic varieties. Following [Kn66], let k be a finite extension of $\mathbb{Q}$, and S a finite set of places of k. Let G be an algebraic group over k, define the adele group of G as

$$G_A = \{g = (g_v) \in \prod_v {}'G(k_v)\},$$

where $\prod'$ denotes the restricted product meaning that all but finitely many $g_v \in G(\mathbb{Z}_v)$. Denote the S-adele group of G as

$$G_S = \{g = (g_v) \in \prod_{v \in S} {}'G(k_v)\}.$$

Lastly, let G_k be the set of k-rational points of G. Here we define strong approximation to be when $G_k G_S \subseteq G_A$ is dense in G_A.

[Kn66] describes the necessary conditions for which an algebraic group may have strong approximation to be

1. G is simply connected as an algebraic group

2. G_S is not compact

Going further, we have the following theorem of [Plat] that generalizes that of [Kn66]:

Theorem 9. *Let G be a simple, simply connected algebraic group such that G_S is not compact. Then G has the strong approximation property relative to S.*

Remark 4. *The theorem of [Kn66] is the same statement except we replace simple with absolutely almost simple. Note that because we are considering algebraic groups over an algebraically closed field, our definition of "almost simple" is the same as "absolutely almost simple". We will need this version in future discussions.*

In the following discussion, we will focus on the case that we will require for our application. Let B^1 be the norm 1 elements of a definite quaternion algebra B over $\mathbb{Q}$; this is an algebraic

group. Let ℓ be prime and let $S = \{\ell, \infty\}$ be the set of places.

Lemma 1. *B^1 is simply connected.*

Proof. Consider the map $\Phi : X \to B^1$ where X is a connected group and Φ is a central isogeny. i.e. $\ker(\Phi)$ is contained in the center. Over $\mathbb{C}$, $B^1(\mathbb{C}) \cong SL_2(\mathbb{C})$ because $B(\mathbb{C}) \cong M_2(\mathbb{C})$ (note that the norm 1 elements translate to determinant 1 elements when we view it as a matrix ring). Now, it is well known that $SL_2(\mathbb{C})$ has fundamental group $\{1\}$ and hence is simply connected as a topological manifold [Kna], and hence as an algebraic group because every central isogeny is a topological covering map. Because we have that $X(\mathbb{C})$ is connected and $\pi_1(SL_2(\mathbb{C})) = \{1\}$, we get that Φ is an isomorphism over $\mathbb{C}$. Thus $\ker(\Phi)(\mathbb{C}) = \{1\}$ and hence $\ker(\Phi)$ is trivial, and Φ is an isomorphism. Hence there are no non-trivial central isogenies to B^1 and it is simply connected.

□

Remark 5. *$G = B^1$ is absolutely almost simple. This is because*

$$Z(B^1) \subseteq Z(SL_2(\mathbb{C})) = \{\pm 1\}$$

(which gives us that the center is finite) and $B^1/\{\pm 1\}$ is a simple group because $SL_2(\mathbb{C})/\{\pm 1\}$ is simple.

Lemma 2. *If B is unramified at ℓ, then G_S is not compact.*

Proof. Since we are dealing with $S = \{\ell, \infty\}$, we have $G_S = G_\ell G_\infty$. B is a definite quaternion algebra not split at infinity, and hence is equal to $\mathbb{H}$ (the Hamilton quaternion algebra). Taking the units we see that $G_\infty = \mathbb{H}^1$ which is well known to be S^3, the unit sphere in 4-dimensional Euclidean space [Krish]. Now note that G_ℓ is not compact as it is equal to $G(\mathbb{Q}_\ell) \cong SL_2(\mathbb{Q}_\ell)$ (because B is unramified at ℓ). So $G_S = G(\mathbb{Q}_\ell)\mathbb{H}^1$ is the product of a compact topological group with a non-compact topological group. Altogether we see that the result is not compact because we can take the open cover of $G(\mathbb{Q}_\ell)$ that has no finite subcover and take its product with $\mathbb{H}^1$. It still does not have any finite subcover. □

Remark 6. *If B is not unramified at prime p, then*

$$B^1(\mathbb{Q}_p) = \left\{ \begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix} : aa^\sigma + pbb^\sigma = 1,\ a, b \in \mathbb{Q}_{p^2} \right\}.$$

Then $val(aa^\sigma) = 2val(a)$, $val(pbb^\sigma) = 1 + 2val(b)$. Hence

$$val(aa^\sigma + pbb^\sigma) = val(1) = 0,$$

but this is also equal to

$$\min\{2val(a),\ (1 + 2val(b))\}.$$

So we see that $val(a) = 0$ and $val(b) \geq 0$, and so $a \in \mathbb{Z}_{p^2}^\times$, $b \in \mathbb{Z}_{p^2}$. Hence $B^1(\mathbb{Q}_p)$ is a closed subset of $\mathbb{Z}_{p^2}^\times \times \mathbb{Z}_{p^2}$ which is compact. Hence $B^1(\mathbb{Q}_p)$ is compact.

By [Kn66] we have that $G = B^1$ has strong approximation when B is unramified at ℓ.

Now choose positive integers $a_1, \ldots a_n$ and primes $p_1, \ldots p_n$ and consider $p_1^{a_1} \cdot \cdots \cdot p_n^{a_n}$ where $p_i \neq \ell\ \forall\ i$. Let $\mathcal{O}$ be a maximal order in B, and for all q define $G(\mathbb{Z}_q)$ as the set of elements of norm 1 in $\mathcal{O} \otimes \mathbb{Z}_q$. Let $U = \prod_q U_q$, where

$$U_q = \begin{cases} G(\mathbb{Z}_q) & q \neq p_i \\ A \in G(\mathbb{Z}_q) : A \equiv I \mod p_i^{a_i} & q = p_i \end{cases}$$

This is an open subset in the adelic topology.

Now consider a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$. Since its supersingular, its endomorphism ring is an order $\mathcal{O}$ of a definite quaternion algebra B. We now take B^1 to be the norm 1 elements of this quaternion algebra and $\mathcal{O}$ to be $\mathrm{End}(E)$.

Using the theory of elliptic curves ([Sil], chapter 3, section 7) for all $r \neq p$ we can choose a basis for the Tate module and get

$$T_r(E) = \lim_{\leftarrow_n} E[r^n] \cong \mathbb{Z}_r \times \mathbb{Z}_r.$$

Using Theorem 7.7 from [Sil] we get

$$\mathcal{O} \otimes \mathbb{Z}_r = \mathrm{End}(E) \otimes \mathbb{Z}_r \cong \mathrm{Hom}(T_r(E), T_r(E))$$

and $\mathrm{Hom}(T_r(E), T_r(E)) \cong M_2(\mathbb{Z}_r)$.

Extending this, we get $B \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$ and from before, $\mathcal{O} \otimes \mathbb{Z}_q \cong M_2(\mathbb{Z}_q)$, $q = p_i^{a_i}$. Hence we can write our open set from before as when $q = p_i$:

$$U_q = \{A = I + p_i^{a_i} M_2(\mathbb{Z}_{P_i^{a_i}}) : \det(A) = 1\}$$

and

$$UG_\ell = \{(u_q)_{\text{primes } q} : u_{p_i} \in U_{p_i}, u_\ell \in G_\ell, \text{ else } u_q \in G(\mathbb{Z}_q)\}.$$

For any such choice of $U = \prod_q U_q$, given $A \in B^1$, we can represent A as $A = (A, A, A \dots) \in B^1(\mathbb{A}^f)$.

Strong approximation gives us that

$$B^1(\mathbb{Q}) \cap A \cdot UG(\mathbb{Q}_\ell) \neq \varnothing.$$

We use the elements in this set to approximate elements of $\prod_i B^1(\mathbb{Z}_{p_i})$ whose reduction is our path of interest in the super-singular isogeny graph.

3.3 Application: number of connected components in supersingular isogeny graphs with level N structure

We begin with the same setup; E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, such that $\mathrm{End}(E) = \mathcal{O}$ is an order in a definite quaternion algebra B, B^1 is the subset of B of norm 1 elements and has strong approximation as explained above. We are given α, $\beta : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$ and want to see if the vertices (E, α) and (E, β) are connected in the supersingular isogeny graph with level N structure, i.e. we want to see if they are in the same connected component. Note that for every (E', α') in the graph, there is an α such

that (E, α) is connected to (E', α') since the level 1 supersingular isogeny graph is connected [Gor].

Let $N = p_1^{a_1} \dots p_n^{a_n}$, $p_i \neq \ell$ for all i, $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$. By the Chinese Remainder Theorem, we get

$$\alpha = \alpha_{p_1^{a_1}} \times \cdots \times \alpha_{p_n^{a_n}}$$

where the $\alpha_{p_i^{a_i}} : (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^2 \to E[p_i^{a_i}]$.

We are given a map β and we want $f \in \mathrm{End}(E)$ such that $\deg(f) = \ell^r$ for some r and $\beta = f \circ \alpha$. Viewing f as a matrix on $E[N]$, this occurs if and only if $\alpha^{-1} \circ \beta = f$. We see that $\alpha^{-1} \circ \beta \in \mathrm{Aut}(E[N]) \cong GL_2(\mathbb{Z}/N\mathbb{Z})$.

For all r we can choose a sympletic basis (relative to the Weil pairing) for $T_r(E)$, $T_r(E) \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$ then

$$\mathcal{O} \otimes \mathbb{Z}_r \cong M_2(\mathbb{Z}_r).$$

Then for all N there is a basis for $E[N]$ providing the isomorphism

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z},$$

such that the Weil pairing is sympletic, i.e. $\langle (1,0), (0,1) \rangle_{Weil} = \zeta_N$. Then any map $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N] = (\mathbb{Z}/N\mathbb{Z})^2$ is some matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})^\times.$$

So we define the determinant of α to be $ad - bc$ as per usual.

Case 1

Suppose that $\alpha^{-1}\beta$ has determinant 1. Then $\alpha^{-1} \circ \beta \in SL_2(\mathbb{Z}/N\mathbb{Z})$.

Note that

$$\prod_{i=1}^{n} SL_2(\mathbb{Z}_{p_i}) = \prod_{i=1}^{n} B^1(\mathbb{Z}_{p_i}),$$

and then by [Shim] we have

$$SL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{n} SL_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}).$$

Also, there is a natural surjective map

$$\prod_{i=1}^{n} SL_2(\mathbb{Z}_{p_i}) \twoheadrightarrow \prod_{i=1}^{n} SL_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}).$$

Choose $\gamma \in \prod_{i=1}^{n} B^1(\mathbb{Z}_{p_i})$ such that the reduction of γ is $\alpha^{-1}\beta$. We want to use strong approximation to approximate γ by an element x of $B^1(\mathbb{Q})$ such that $x \in \prod_i^n B^1(\mathbb{Z}_{p_i})$ reduces to $\alpha^{-1}\beta$ i.e.

$$x \equiv \gamma \mod p_i^{a_i} \ \forall \ i$$

and x is integral at all $q \neq \ell$.

This $x \in B$ is a rational endomorphism of E of norm 1, integral at any prime except perhaps at ℓ. Also, $x \in B(\mathbb{Q}_\ell) \cong M_2(\mathbb{Q}_\ell)$. For all $k >> 0$, $\ell^k \cdot x$ integral at all q, hence we have that $\ell^k \cdot x \in \mathcal{O} = \mathrm{End}(E)$ and has norm ℓ^{2k}.

Choose k such that $\ell^k \equiv 1 \mod N$ and large enough to satisfy integrality as before. Let $y = \ell^k \cdot x \in \mathrm{End}(E)$. This has degree ℓ^{2k} and $y \equiv \alpha^{-1}\beta \mod N$. Hence we have that α and β connected by a path in the ℓ-isogeny graph, i.e. the points (E, α) and (E, β) are connected by a path.

Case 2

Now we generalize to allow $\det(\alpha^{-1} \circ \beta)$ to not necessarily be 1, i.e. we don't necessarily have that $\det(\alpha) = \det(\beta) \mod N$. Let $f = [\ell]$, then $\det(\beta) = \ell^2 \det(\alpha)$. For all $r >> 0$ there exists f such that $\deg(f) = \ell^{2r+1}$, this is because the supersingular isogeny graph is connected and bipartite [Gor]. Hence we get that $\det(\beta) = \det(f \circ \alpha) = \ell^{2r+1} \det(\alpha)$ in $(\mathbb{Z}/N\mathbb{Z})^\times$. Now note

that $\langle \ell^2, \ell^{2r+1} \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ is equal to $\langle \ell \rangle$. We arrive at the conclusion that α is connected to β if $\det(\alpha^{-1}\beta) \in \langle \ell \rangle$ and vice versa. So we see that as sets, the set of all path connected components is the same as $(\mathbb{Z}/N\mathbb{Z})^\times / \langle \ell \rangle$.

4 Path problem on the ordinary ℓ-isogeny volcano

Let p and ℓ be distinct primes, and let $d = \ell + 1$. Pick an ordinary elliptic curve E such that $\mathrm{End}^0(E) \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$. Recall the construction of the ordinary isogeny graph $\Gamma(p, \ell)$, giving us an undirected ℓ-isogeny volcano as described previously. The universal covering space of this graph is the d-regular tree.

We consider the action of the Hecke Operator T_ℓ. It takes an ordinary elliptic curve E and maps it to one of the $d = \ell + 1$ adjacent vertices defined by the ℓ-isogeny graph. If we raise it to the power of r, we are taking a path of length r from our starting vertex represented by E to some other vertex within range. Obviously, there are d^r paths in total because each step along the path has d choices (allowing backtracking). The vertices within range have certain multiplicities associated to them, i.e. there may be more than one path of length r that exists to reach them. In this section, we are interested in the probability that we reach a vertex (represented by some E') of some exact distance m away from the fixed starting vertex.

Let $\mathrm{multi}_{v_0}(r, v)$ be the number of paths of length r reaching a vertex v from some fixed starting vertex v_0. We define our probability measure to be

$$\mathbb{P}(v, r) = \frac{1}{d^r}\mathrm{multi}_{v_0}(r, v).$$

Note that this is a probability measure because for fixed r

$$\sum_{v \in V} \mathbb{P}(v, r) = 1.$$

This is because d^r is the total number of possible paths of length r. Since our infinite tree has symmetries, if v is a vertex of exact distance m away from v_0, the quantity $\mathrm{multi}(v, r)$ depends only on r and m =distance(v, v_0), which we denote $\mu(m, r)$. We will explore this function μ to achieve our ultimate goal, which is to analysis this measure.

4.1 Path counting on the d-infinite tree

Fix two integers $m, r \geq 0$, and fix a vertex v_0 in the d-regular tree. Define $\nu(m, r)$ to be the number of paths of length r from the vertex v_0 to a vertex of exact distance m from it.

Proposition 2. *The function $\nu(m, r)$ has the following obvious properties:*

1. *If $m = 0$, $\nu(m, r)$ counts the number paths of length r that start and end at v_0.*

2. *If $r = 0$, these are paths of length zero which we define as*

$$\nu(m, 0) = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{otherwise} \end{cases}.$$

3. *Along the same lines, it is easily seen that $\nu(m, r) = 0$ if $m > r$, and $\nu(m, r) = 1$ if $m = r$.*

4. *If m is even and r is odd, or vice versa, $\nu(m, r) = 0$.*

5. *Further, our function satisfies the following recursion equations:*

$$\nu(0, r) = d\nu(1, r - 1),$$

$$\nu(m, r) = \nu(m - 1, r - 1) + (d - 1)\nu(m + 1, r - 1),$$

for $m > 0$ and $r > 0$.

We will now hand compute a few of the values and then use the recursion equations from property 5 of our proposition to generate a table of values. Property 2 in the proposition generates all values for $r = 0$. From property 3, we see that if $r = 1$ we get 0 if $m = 0$ and $m > 1$, and 1 if $m = 1$. For $r = 2$, if $m = 0$ we are making cycles back to v_0 and hence have d choices. If $m = 1$, property 4 tells us this is 0, and if $m = 2$ we use property 5 to tell us that this is 1. Then all other values of m give $\nu(m, 2) = 0$. We now have the following information:

r/m	0	1	2	3	4	5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	d	0	1	0	0	0

Now applying the recursion relation, we can get a larger table of initial values.

r/m	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	d	0	1	0	0	0	0
3	0	$2d-1$	0	1	0	0	0
4	$2d^2-d$	0	$3d-2$	0	1	0	0
5	0	$5d^2-6d+2$	0	$4d-3$	0	1	0
6	$5d^3-6d^2+2d$	0	$9d^2-13d+5$	0	$5d-4$	0	1
7	0	$14d^3-28d^2+20d-5$	0	$14d^2-22d+9$	0	$6d-5$	0

Finding explicit formulae for $\nu(m,r)$ proved challenging, however there are many patterns in the coefficients of the polynomials that give us $\nu(m,r)$ with d as the variable. We will address this later. First we shall connect the number of paths of length r on the d-infinite tree to the paths on the isogeny volcano it covers.

4.2 Covering

Consider the ℓ-isogeny volcano, it is a $d=\ell+1$-regular graph and has a rim of some length $n>0$. Label the vertices on the rim 1 through n and pick an arbitary, infinite length path in the d-infinite tree with no backtracking. Along this path pick a vertex and label it 1, on one side of this vertex label it n, then $n-1$,... so on. On the other side of the 1 vertex, label it 2, 3,... and so on. See the diagram below for an illustration using colors.

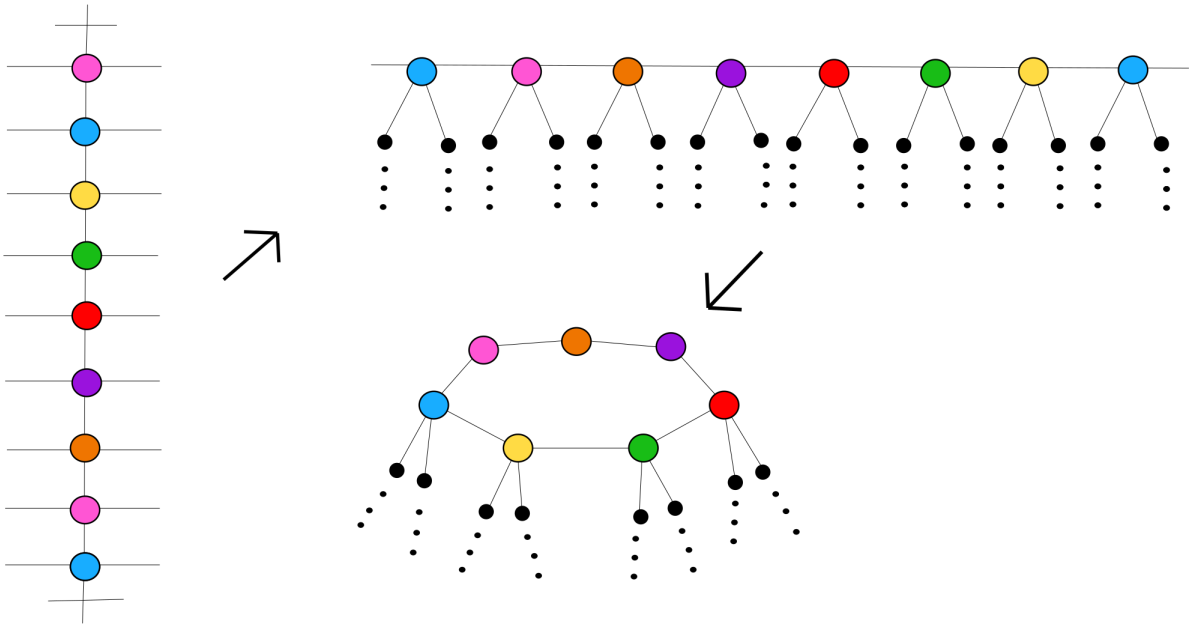


Figure 3: Mapping the infinite 4-regular tree onto the 4-regular 3-isogeny volcano with rim length 7

4.3 Path counting on the isogeny volcano

Let $n > 0$ be the length of the rim of the isogeny volcano. We need more variables to describe the location of vertices relative to the fixed vertex v_0.

4.3.1 Fixed vertex v_0 is on the rim

We begin by setting our initial vertex v_0 to be on the rim of the isogeny volcano. As explained in the previous section, we can cover the isogeny volcano with the d-infinite tree where the 1 label is placed at v_0. We need variables $m_1 \geq 0$, $m_2 \geq 0$ to describe another vertex's distance from v_0, so we call our function $\mu(m_1, m_2, r)$. m_2 is the depth within the volcano from the rim, and m_1 describes where on the rim we begin our descent. We only define $m_1 \in \{0, 1, \ldots \frac{n+1}{2} - 1\}$ if n is odd or $m_1 \in \{0, 1, \ldots \frac{n}{2} - 1\}$ if n is even. To better understand this, consider the following example. If $n = 7$ a vertex on the rim that is four steps away clockwise from our fixed vertex v_0 that is also on the rim is really only three steps away counter-clockwise. We exploit the symmetries present in our graph and let $m_1 = 3$ in this case.

We shall start with the $m_1 = m_2 = 0$ case. It is easy to see that for the first n values of r, $r = 0, \dots n-1$ we will have the same result as we did for the infinite d-regular tree, i.e.

$$\mu(0,0,0) = \nu(0,0), \quad \mu(0,0,1) = \nu(0,1), \dots \ \mu(0,0,n-1) = \nu(0,n-1).$$

Exploring further, we see that when we reach n we now have two new paths to deal with, i.e. a full turn clockwise around the rim of the volcano and a full turn counter-clockwise. We can write this as follows

$$\mu(0,0,n) = \nu(0,n) + 2\nu(n,n).$$

We can say this because the full turn described before is the same as reaching a point of distance n away from our original, but doing so clockwise or counter-clockwise gives us a factor of two. Following the same pattern we see

$$\mu(0,0,n+1) = \nu(0,n+1) + 2\nu(n,n+1)$$

$$\vdots$$

$$\mu(0,0,2n) = \nu(0,2n) + 2\nu(n,2n) + 2\nu(2n,2n)$$

$$\vdots$$

In general we find the following proposition

$$\mu(0,0,kn+\ell) = \nu(0,kn+\ell) + 2\nu(n,kn+\ell) + \cdots + 2\nu(kn,kn+\ell).$$

Now dealing with the more general case, it is not hard to see that if we write $r = kn + a$, in general, our function μ satisfies the relation stated in the following proposition:

Proposition 3. *For the function $\mu(m_1, m_2, r)$, $r = kn + a$ ($a,\ k \in \mathbb{N}_0$), where the starting vertex v_0 is on the rim of length n, we have the following relation:*

$$\mu(m_1,m_2,r) = \nu(m_1+m_2, kn+a) + \nu\big((n-m_1)+m_2, kn+a\big) +$$

$$\nu(m_1 + m_2 + n, kn + a) + \nu((2n - m_1) + m_2, kn + a) + \dots$$

$$= \sum_{t=0}^{\infty} \nu(tn + m_1 + m_2, kn + a) + \nu(((t+1)n - m_1) + m_2, kn + a) < \infty.$$

Remark 7. *This converges because $r = kn+a$ is fixed and as t increases, eventually the value for 'm' in the formula for ν is larger than the value of r, and hence contributes zero. Hence there are only finitely many terms in the sum.*

4.3.2 Fixed vertex v_0 is some depth s within the volcano

Now consider v_0, our fixed vertex, with some depth s within the volcano. As explained in the section on covering the isogeny volcano with the d-infinite tree, because of all the symmetries at play, we can always label the rim with 1 starting at the location directly above v_0.

We consider a more general function $\mu(s, m_1, m_2, r)$ which is the number of paths of length r of distance m_1 along the rim and m_2 is the depth of the other vertex away from the rim. We have handled the case $s = 0$, so now we handle the cases for $s > 0$:

Case 1: $m_1 = 0, m_2 \geq 0$

Since $m_1 = 0$, we are on the same branch from the rim, we are simply moving up or down the branch from our starting vertex. If $m_2 < s$ then the other vertex v is above our fixed v_0, and if $m_2 > s$ then v_0 is above v. The exact distance between our vertices is $|s - m_2|$. Hence we need to include the term $\nu(|s-m_2|, r)$. Then we need to take the rim into account, we can go from v_0 up and all away around the rim clockwise or counter-clockwise after $n + s + m_2$ steps. Another turn around the rim gives us $2n + s + m_2$, and so forth. We find that in general

$$\mu(s, 0, m_2, r) = \nu(|s - m_2|, r) + \sum_{t=0}^{\infty} 2\nu(tn + s + m_2, r).$$

Case 2: $m_2 = 0$, $m_1 > 0$ (for the restrictions on m_1 as described previously)

Now let us consider the case where were are trying to reach v, a vertex on the rim that m_1 distance away from the label 1 (where 1 is the place on the rim that branches down s steps to our fixed vertex v_0).

The exact distance between fixed vertex v_0 and v is $m_1 + s$. However, for $m_1 \neq 0$, the opposite direction around the rim gives a distance $s + n - m_1$. Continuing like this we find

$$\mu(s, m_1, 0, r) = \sum_{t=0}^{\infty} \nu(tn + m_1 + s, r) + \nu((t+1)n - m_1 + s, r).$$

Case 3: For general s, m_2 and $m_1 > 0$ (for the restrictions on m_1 as described previously)

Our vertices v_0 and v in this case have exact distance $s + m_1 + m_2$. After that, one must take into account turns along the rim. The first to consider is of course $s + m_2 + (n - m_1)$, then $s + m_2 + m_1 + n$, and so forth.

We find that

$$\mu(s, m_1, m_2, r) = \sum_{t=0}^{\infty} \nu(tn + m_1 + m_2 + s, r) + \nu((t+1)n - m_1 + m_2 + s, r).$$

Note that this formula does not hold for $m_1 = 0$ unless $m_2 = 0$ too (where it reconciles with Case 1). For the case where $m_1 = 0,\ m_2 > 0$ then the case 1 formula is the only formula that works.

Ultimately Case 1 and 3 are the best we can do to have a general formula (Case 2 reconciles with Case 3). We have fully related the path problem on the isogeny volcano to that of the d-infinite tree and we state it as the following theorem:

Theorem 10. *Let $\nu(m, r)$ be the function counting the number of paths in the d-infinite tree between a fixed vertex and a vertex of exact distance m with r steps. Let $\mu(s, m_1, m_2, r)$ be the function counting the number of paths in the ℓ-isogeny volcano (where $d = \ell + 1$) between a fixed vertex with depth s in the volcano and another vertex in a branch m_1 steps away on the rim and m_2 steps down that branch. The following relation exists:*

If $m_1 > 0$,

$$\mu(s, m_1, m_2, r) = \sum_{t=0}^{\infty} \nu(tn + m_1 + m_2 + s, r) + \nu((t+1)n - m_1 + m_2 + s, r).$$

If $m_1 = 0$,

$$\mu(s, 0, m_2, r) = \nu(|s - m_2|, r) + \sum_{t=0}^{\infty} 2\nu(tn + s + m_2, r).$$

Now that we have characterized $\mu(s, m_1, m_2, r)$ in terms of ν we can look at our probability measure and its properties.

4.4 Limiting measure $r \to \infty$ in the d-infinite tree and ℓ-isogeny volcano

Paths in the ℓ-isogeny volcano have unique lifts to paths in the d-infinite tree once you choose a fixed lift of the starting point of the path. Hence we first consider the limiting measure of the covering space. As before, we define our probability measure to be

$$\mathbb{P}(v, r) = \frac{1}{d^r} \nu(m, r),$$

where v is an arbitary vertex of exact distance m from v_0 our fixed vertex. We will analyse what happens as $r \to \infty$ in order to understand the weight that each vertex holds in the graph in terms of how many times it is visited as the length of the path increases.

We turn to the standard approach in the theory of random walks and introduce the terminology required to study the generating function of the random walk on the d-infinite tree. Following the notation of [Woe], such a generating function, denoted $G(x, y|z)$ is a power series in the variable z of the form

$$G(x, y|z) = \sum_{n=0}^{\infty} p^{(n)}(x, y) z^n,$$

where $p^{(n)}(x, y)$ is the probability that the vertex x reaches the vertex y on the nth step of the random walk. [Woe] gives the following lemma regarding the generating function of the

simple random walk on the d-infinite tree:

Lemma 3. *An explicit expression for $G(x, y|z)$ of a simple random walk on the d-infinite tree is given by*

$$G(x, y|z) = \frac{2(d-1)}{d-2+\sqrt{d^2-4(d-1)z^2}} \cdot \left(\frac{d-\sqrt{d^2-4(d-1)z^2}}{2(d-1)z} \right)^m,$$

where m is the exact distance between x and y.

In terms of our notation, we have a fixed vertex v_0 and another vertex v of exact distance m away from v_0, so it turns out that $p^{(n)}(v_0, v) = \frac{1}{d^n}\nu(m, n) = \mathbb{P}(v, n)$ in our notation. Hence are problem can be rephrased as isolating the $p^{(n)}(v_0, v)$ and taking n to infinity.

One can take derivatives to help isolate the $p^{(n)}(v_0, v)$. Note that

$$\left.\frac{\partial^k G(x, y|z)}{\partial z^k}\right|_{z=0} = k! \cdot p^{(k)}(x, y), \quad \forall k \in \mathbb{N}.$$

However, we are concerned with the limit of the $p^{(k)}(v_0, v)$ as $k \to \infty$. Since $G(v_0, v|z)$ converges for $|z| < \frac{1}{\rho} = r$, where $\rho = \frac{2\sqrt{M-1}}{M}$, we have that for $M > 2$, $r > 1$. Hence $G(v_0, v|1)$ converges, and so the $p^{(k)}(v_0, v) \to 0$ and $k \to \infty$. In fact, one can see that $p^{(k)}(v_0, v)$ converges to zero exponentially fast, because $M^k p^{(k)}(v_0, v) \to 0$ as $k \to \infty$, and so $p^{(k)}(v_0, v) = o(M^{-k})$.

Now we want to relate this back to our measure on the isogeny volcano. Using theorem 10, we see that for fixed s, m_1, m_2, and r, $\mu(s, m_1, m_2, r)$ is simply a finite sum of values taken on by ν. However, as r increases, the number of terms in the sum increases. Still, despite the increase in the number of terms, each term still converges to zero as $r \to \infty$, hence overall our limiting measure in this case is also zero.

4.5 Characterizing the random walk

We would like to further explore this random walk on our graph. In the case of the infinite tree, we create plots to demonstrate the behaviour of the measure for varying r and fixed

d. Here we denote $P(m,r) = P(v,r)$ where v is a vertex of exact distance m from our fixed vertex v_0. We begin by plotting $P(m,r) \cdot d \cdot (d-1)^{m-1}$, notice that for $d > 2$ we have a Gaussian-like distribution.

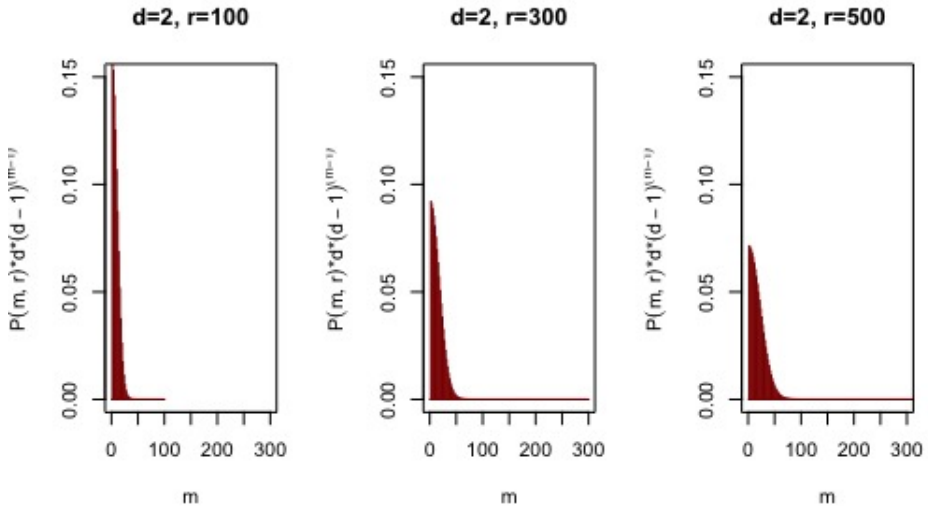


Figure 4: Above is the value of our probability measure $P(m,r) \cdot d \cdot (d-1)^{m-1}$ for different fixed values of r in the $d = 2$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis.

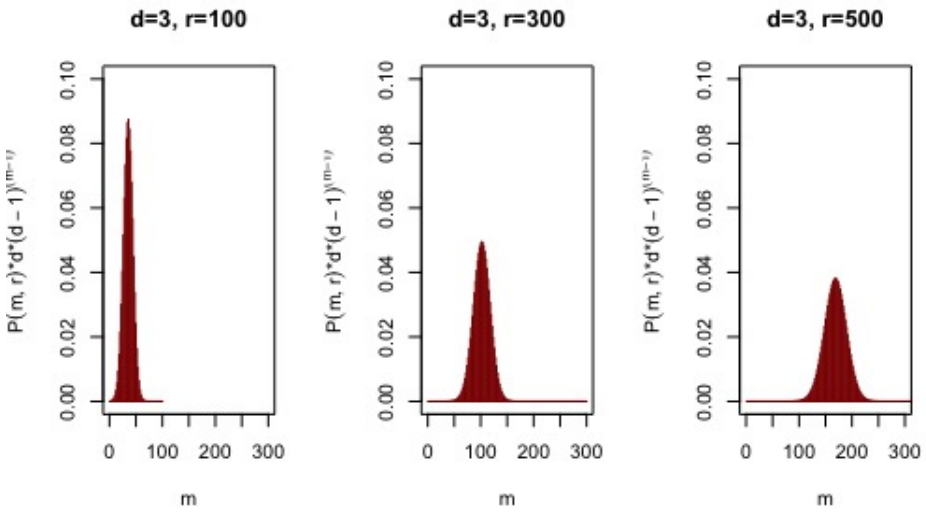


Figure 5: Above is the value of our probability measure $P(m,r) \cdot d \cdot (d-1)^{m-1}$ for different fixed values of r in the $d = 3$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis.

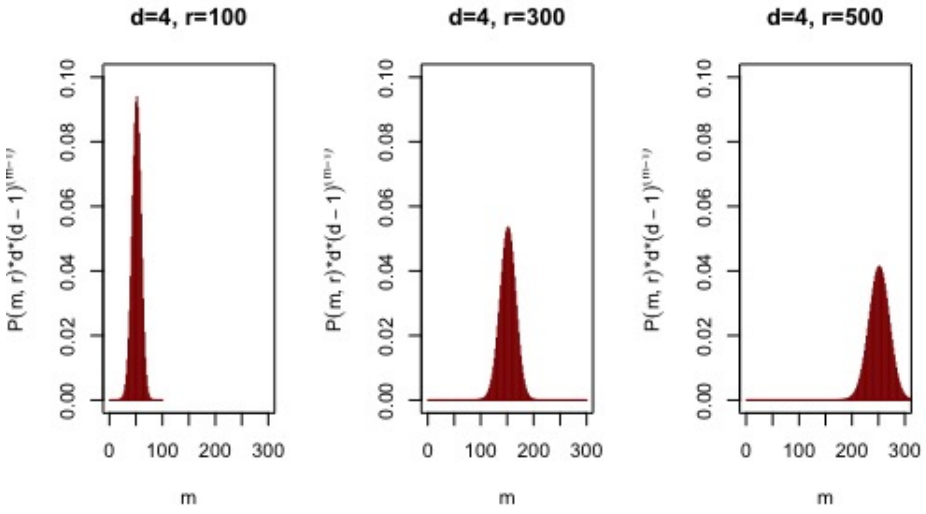


Figure 6: Above is the value of our probability measure $P(m,r) \cdot d \cdot (d-1)^{m-1}$ for different fixed values of r in the $d = 4$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis. Above $d = 4$, R cannot preform the calculation to generate further plots due to magnitude of the numbers used in generating operations.

Now examine the plot of $P(m, r)$ in the case of the d-infinite tree for fixed d and varying r. Be careful to note the y-axis limit in each graph as they are not the same.

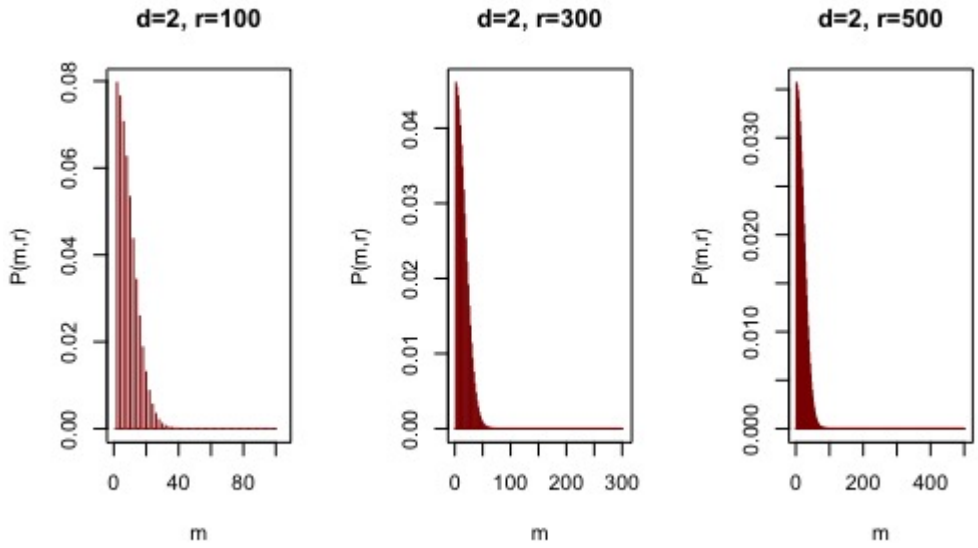


Figure 7: Above is the value of our probability measure $P(m, r)$ for different fixed values of r in the $d = 2$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis.

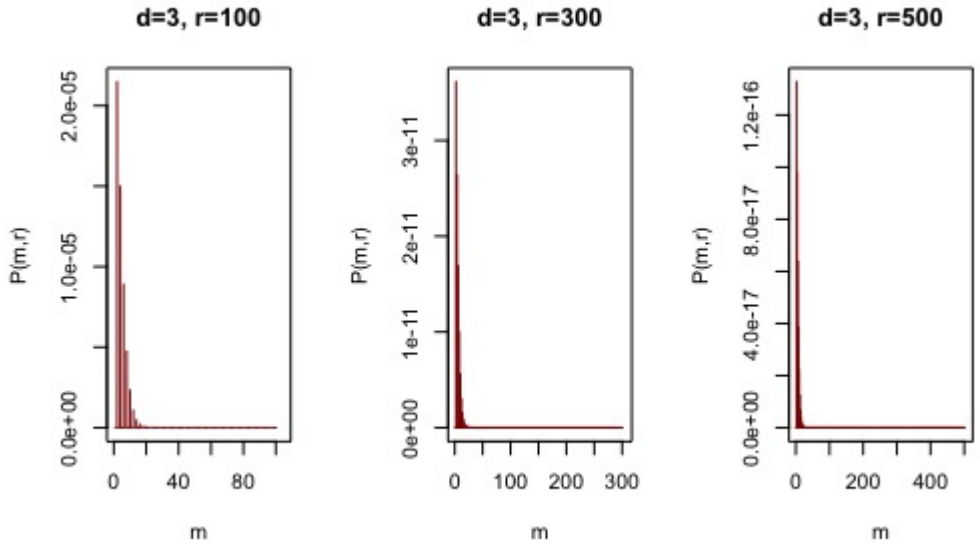


Figure 8: Above is the value of our probability measure $P(m, r)$ for different fixed values of r in the $d = 3$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis.

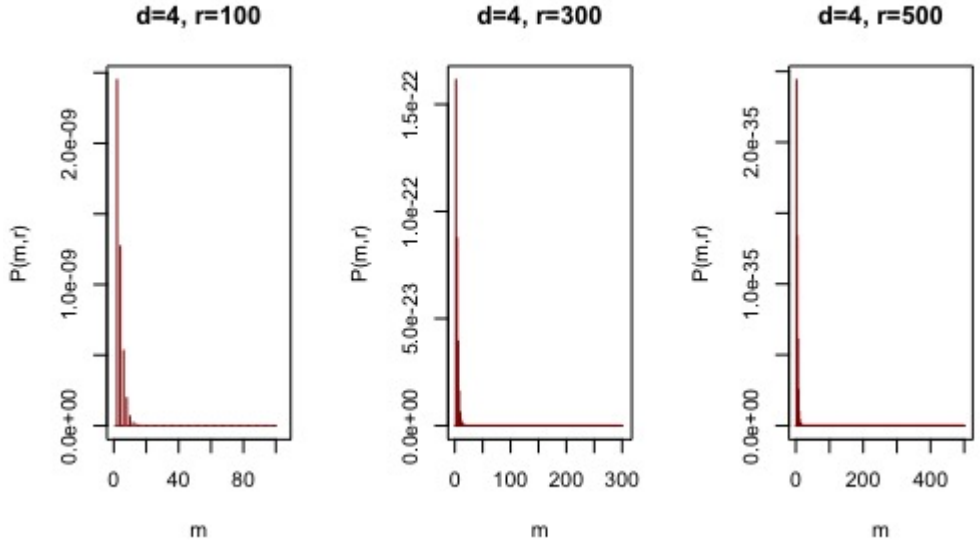


Figure 9: Above is the value of our probability measure $P(m, r)$ for different fixed values of r in the $d = 4$ case. The distance of v from the fixed vertex v_0 is given by m on the x-axis. Above $d = 4$, R cannot preform the calculation to generate further plots due to magnitude of the numbers used in generating operations.

We can also consider the following arrangement of the d-infinite tree along $\mathbb{Z}$. Place the root v_0 at 0 on $\mathbb{Z}$ and allow an infinite path to line $\mathbb{Z}$ with subtrees growing from each point arranged on $\mathbb{Z}$. Then similar to our notions of m_1 and m_2 on the isogeny volcano, for a vertex v on our tree let ℓ_1 be the value of $\mathbb{Z}$ representing the subtree v belongs to. Let ℓ_2 be the exact distance of the vertex v to the root of the subtree at ℓ_1. We define the height of v, $H(v)$, to be $\ell_1(v) + \ell_2(v) \in \mathbb{Z}$. We see that for a random walk on our d-infinite tree, $w_1 w_2 \dots w_r$ from v_0 to the vertex w_r, $H(w_1)H(w_2)\dots H(w_r)$ is then a random walk on $\mathbb{Z}$.

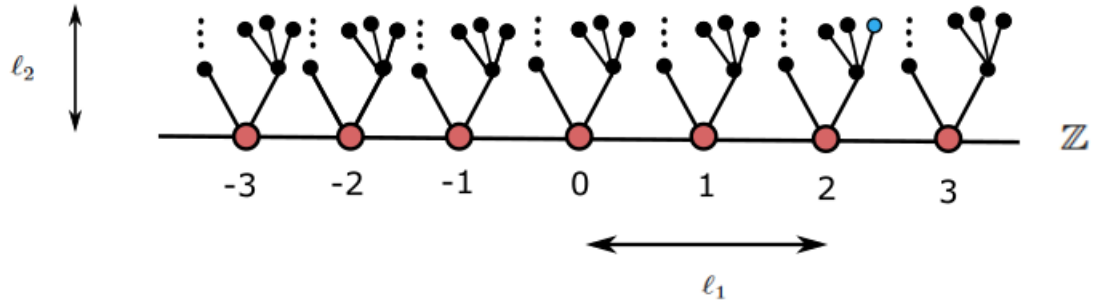


Figure 10: This figure depicts the arrangement of the 4-infinite tree along $\mathbb{Z}$ as described above. For the blue vertex $\ell_1 = 2$ and $\ell_2 = 2$ and hence the height is 4

The central limit theorem in this case is clear. We can write

$$H(w_r) = \sum_{i=1}^{r} \zeta_i, \qquad \zeta_i \in \{-1, 1\}, \quad \mathbb{P}(\zeta_i = 1) = \frac{d-1}{d},$$

and compute the expectation of ζ_i to be $\frac{d-2}{d}$. The variance is $\sigma^2 = 1 - \left(\frac{d-2}{d}\right)^2$, and then by the central limit theorem we have

$$\frac{1}{\sqrt{r}} H(w_r) - \sqrt{r} \cdot \frac{d-2}{d} \to N(0, \sigma^2).$$

Define $X(w_r)$ to be the distance of the vertex w_r from the root v_0 in the d-infinite tree. It

is clear that while $H(w_r) = \ell_1(w_r) + \ell_2(w_r)$, $X(w_r) = |\ell_1(w_r)| + \ell_2(w_r)$ and hence $X(w_r) = |H(w_r) - \ell_2(w_r)| + \ell_1(w_r)$. So we see that $X(w_r)$ is approximately normal with a shift in the mean of the Gaussian.

To do a similar procedure for the isogeny volcano has proved challenging. Below are some plots demonstrating the structure probability measure on the isogeny volcano; in each plot we fixed n, r, m_1, d and s, and varied m_2. We had to use the log scale due to computational difficulties, we plotted $\log(\mu(s, m_1, m_2, r)) - \log(d^r)$.

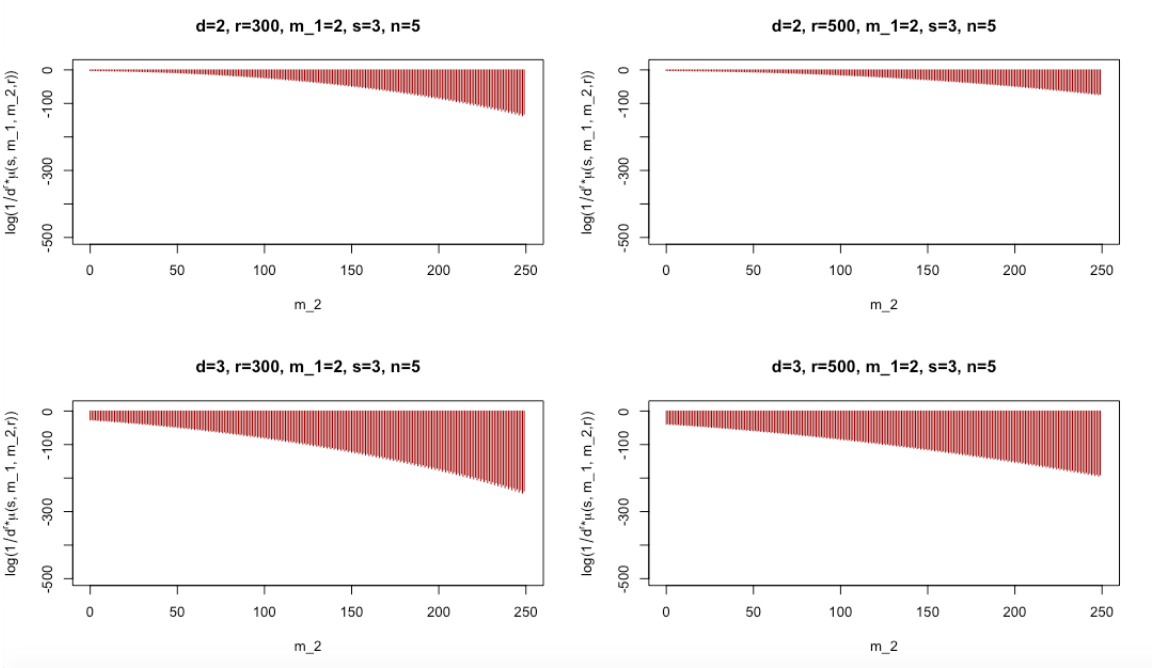


Figure 11: Above are plots characterizing the measure on the isogeny volcano. We fix every parameter as specified in the title of each plot and vary m_2.

These plots were computationally the best one could do to mimick the earlier plots of the d-infinite tree.

5 Discussion

5.1 Constructing Hash Functions – An application of SSI graphs

Supersingular isogeny graphs give rise to Ramanujan graphs which have a variety of applications [Cost]. The original construction due to [Piz] is the level 1 case of the construction in previous sections. They are optimal expanders, which gives them excellent mixing properties that are coveted in computer science. In particular, they are often used for applications requiring pseudorandomness [Vad]. Pizer's supersingular isogeny graphs were introduced into cryptography by the authors of [Cha] at the NIST competition in 2005 [Lau]. The construction of Ramanujan graphs from [Lub] was also proposed for cryptographic use, but was defeated in 2008 by [Til] and [Pet]. The idea of [Cha] for a cryptographic primitive was computing isogenies between supersingular elliptic curves, which is believed to be a hard problem [Lau]. The best known algorithm solves this in $O(\sqrt{p}\log^2 p)$ time [Cha]. This gives us a technique to construct "good" **hash functions**. In order to explain what it is to be a "good" hash function, we shall begin with some basic definitions [Hof]:

Definition 12. *A **hash function** takes arbitarily long input D and outputs a short string of bits that we denote H.*

We would like the hash function to have the following properties:

1. The computation of the hash H is linear time.

2. Inversion of the hash function should be difficult, i.e. exponential time, i.e. given H a hash, its difficult to find an input D such that its hash is H. This is called being **preimage resistant**.

3. It is difficult to find two inputs D_1 and D_2 that have the same hash H. This is called **collision resistant**.

In the construction of an appropriate supersingular isogeny graph from the earlier section, we require the prime p to be of cryptographic size, i.e. p of at least 256 bits, and for ℓ to be a small prime [Lau]. With this d-regular graph, one uses the input to the hash function as directions to walk around the graph, the output is the vertex at the end of the walk (no

backtracking) [Cha]. To execute said random walk, pick a starting vertex and convert the input of the hash function into a base $d-1$ number. This allows one to interpret which of the $d-1$ vertices to traverse next by establishing an ordering on the $\ell+1$ ($d=\ell+1$) torsion subgroups at each node (see [Cha] for an exposition of how this is done in $\ell=2$ and $\ell\neq 2$ cases). [Cha] relate the collision and preimage resistance properties of this hash function to the problem of finding isogenies between elliptic curves and argue why this problem is hard.

In our exploration of supersingular isogeny graph constructions, we focus on supersingular isogeny graphs with full level N structure. The natural question is whether hash functions created on these graphs would provided added security, particular in a post-quantum world. Certainly as our graphs with full level N structure provide a cover for the level 1 construction traditionally used for these hash functions, they provide at least as much security as the original hash functions of [Cha]. Assuming one can break the level 1 case, one asks whether the level N case is compromised or secure. We have already examined one of the properties of these supersingular isogeny graphs with full level N structure, i.e. the number of connected components. Now, we enter into further discussion of these graphs by making comparisons with the construction of [Lub].

5.2 Extremal cases of the supersingular isogeny graphs with level N structure

In this subsection, we will briefly describe the similarities between [Lub] Ramanujan graphs and variants of our supersingular isogeny graphs with full level N structure in the extremal case where the characteristic over which the elliptic curve is defined is 2.

In the [Lub] construction of Ramanujan graphs they work with Cayley graphs. For $\left(\frac{\ell}{N}\right)=1$, $\ell, N \equiv 1 \mod 4$ distinct primes, they construct the Cayley graph of $PGL_2(\mathbb{Z}/N\mathbb{Z})$ relative to the $\ell+1$ elements derived from the set S, where

$$S=\{(a_0,a_1,a_2,a_3): a_0>0 \text{ odd}, a_1,a_2,a_3 \text{ even}, \ a_0^2+a_1^2+a_2^2+a_3^2=\ell\}.$$

The matrices constructed from S used to define the Cayley graph through action on $PGL_2(\mathbb{Z}/N\mathbb{Z})$

are of the form

$$\begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix},$$

where $i^2 \equiv -1 \mod N$. If $\left(\frac{\ell}{N}\right) = -1$, then we form the Cayley graph of $PSL_2(\mathbb{Z}/N\mathbb{Z})$ relative to S because the generators all lie in $PSL_2(\mathbb{Z}/N\mathbb{Z})$. These graphs have well known bounds on diameter and other properties. Now we investigate a similar, (though not exactly the same) construction of supersingular isogeny graphs with full level N structure.

Let $p = 2$, we will consider the ℓ-isogeny graphs (with $\ell \equiv 1 \mod 4$, prime) with level N ($N \equiv 1 \mod 4$, prime, distinct from ℓ) structure in characteristic p. Recall that in our construction of supersingular isogeny graphs with level N structure that $\gcd(p\ell, N) = 1$. Note that $p \not\equiv 1 \mod 12$, and hence the automorphism group of the unique supersingular elliptic curve defined over $\bar{\mathbb{F}}_p$ is not $\{\pm 1\}$, in fact it has order 24. More specifically,

$$\mathrm{End}(E) = \mathbb{Z}\left[1, i, j, k, \frac{1 + i + j + k}{2}\right].$$

Hence the automorphism group $\mathrm{Aut}(E) = \mathrm{End}(E)^\times$ has 24 elements [Gor]. This is the first difficulty in relating the [Lub] construction to the construction above.

Note that the level N structures on E in our construction correspond to $GL_2(\mathbb{Z}/N\mathbb{Z})$, i.e. pick some $\alpha : \mathbb{Z}/N\mathbb{Z} \to E[N]$, any other such alpha is $M \circ \alpha$ where $M \in GL_2(\mathbb{Z}/N\mathbb{Z})$. These comprise the vertices of the graph. Now we construct the edges (which creates a variant of our original construction): consider the norm of the endomorphisms of E, $\mathrm{Norm}(a_0 + a_1 i + a_2 j + a_3 k) = a_0^2 + a_1^2 + a_2^2 + a_3^2$, and the set

$$S = \{(a_0, a_1, a_2, a_3) : a_0 > 0 \text{ odd}, \ a_i \text{ even}, \ a_0^2 + a_1^2 + a_2^2 + a_3^2 = \ell\},$$

which has $\ell + 1$ elements. Note that composing any of these endomorphisms with any of the 24 automorphisms perserves the kernel and degree of the map. Additionally, from [Gor] example 4.2.5 we know that the automorphisms are solutions to

$$x^2 + y^2 + z^2 + w^2 = 4,$$

and hence are given by all permutations of the vectors

$$\{(\pm 2, 0, 0, 0),\ (\pm 1, \pm 1, \pm 1, \pm 1)\}.$$

Further it is clear from direct calculation that composition with these automorphisms does not take any element of S to any other element of S. Obviously any permutation of $(\pm 2, 0, 0, 0)$ makes every coefficient in the resulting element even, however a_0 needs to be odd. Additionally multiplication by any of the 16 elements that are the permutations of $(\pm 1, \pm 1, \pm 1, \pm 1)$ give rise to elements where the a_i, $i \neq 1$ are not even. Hence we view these up to composition by automorphisms.

These endomorphisms of E must take a vertex (E, α) to some (E, α'). Since $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$, to get α', one must fix a basis for $E[N]$, then for $f \in T$, f acts by sending

$$f = a_0 + a_1 i + a_2 j + a_3 k \mapsto \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix} = M_f,$$

and then α gets sent to $f \circ \alpha = M_f \circ \alpha$.

Fixing a starting α_0, we see our graph amounts to a Cayley graph of $GL_2(\mathbb{Z}/N\mathbb{Z})$ with S as the set of generators. Now our issue in relating these graphs to the [Lub] construction is that we are dealing with the Cayley graph of $GL_2(\mathbb{Z}/N\mathbb{Z})$ whereas [Lub] deals with $PGL_2(\mathbb{Z}/N\mathbb{Z})$. Now we explore a further variant of our construction in attempt to bringing us closer to relating the two graphs.

For convenience we will switch from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{F}_N$ since N is prime. Consider the short exact sequence

$$\mathbb{F}_N^\times \cdot SL_2(\mathbb{F}_N) \to GL_2(\mathbb{F}_N) \to \mathbb{F}_N^\times / \mathbb{F}_N^{\times,2},$$

where the second map is the determinant map. The quotient at the end contains two elements. Further,

$$1 \to \mathbb{F}_N^\times \cdot SL_2(\mathbb{F}_N)/\mathbb{F}_N^\times \to GL_2(\mathbb{F}_N)/\mathbb{F}_N^\times \to \mathbb{F}_N^\times / {\mathbb{F}_N^\times}^2 \to 1,$$

is exact and hence so is,

$$1 \to PSL_2(\mathbb{F}_N) \to PGL_2(\mathbb{F}_N) \twoheadrightarrow \mathbb{F}_N^\times/\mathbb{F}_N^{\times,2} \to 1.$$

Note that if t is not a square $\mod N$, then $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$ is in $PGL_2(\mathbb{F}_N)$, but not in $PSL_2(\mathbb{F}_N)$. We arrive at the isomorphism

$$PGL_2(\mathbb{F}_N)/PSL_2(\mathbb{F}_N) \cong \mathbb{F}_N^\times/\mathbb{F}_N^{\times,2}.$$

However, this quotient should really be viewed as

$$(GL_2(\mathbb{F}_N)/\mathbb{F}_N^\times)/(\mathbb{F}_N^\times \cdot SL_2(\mathbb{F}_N)/\mathbb{F}_N^\times).$$

Let $\left(\frac{\ell}{N}\right) = -1$, with our fixed α_0 and starting vertex (E, α_0) we construct a variant of the above graph where the other vertices are $(E, M \circ \alpha_0)$ with $M \in GL_2(\mathbb{F}_N)$ and $\det(M) \in \mathbb{F}_N^{\times,2}$. We denote the set of matrices in $GL_2(\mathbb{F}_N)$ such that $\det(M) \in \mathbb{F}_N^{\times,2}$ as $GL_2(\mathbb{F}_N)^\square$. Like before, let

$$S = \{f = a_0 + a_1 i + a_2 j + a_3 k : a_0 > 0 \text{ odd}, \, a_i \text{ even } i = 1,2,3, \; a_0^2 + a_1^2 + a_2^2 + a_3^2 = \ell^2\}.$$

Again, let these f act as matrices M_f defined by

$$\begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}.$$

Note that since $i^2 \equiv -1 \mod N$, $a_0^2 + a_1^2 + a_2^2 + a_3^2 = \ell^2$, and $\left(\frac{\ell}{N}\right) = -1$, the determinant of these matrices is a square and hence $M_f \in GL_2(\mathbb{F}_N)^\square$. Now from our starting vertex (E, α_0) we consider the Cayley graph of $GL_2(\mathbb{F}_N)^\square$ being acted upon by S. Let us denote this as $\Gamma = \text{Cayley}(GL_2(\mathbb{F}_N)^\square, S)$.

Now we want to explore the connection between Γ and graph of the [Lub] construction. We no longer examine the [Lub] Cayley graphs from $PGL_2(\mathbb{F}_N)$, but rather those of $PSL_2(\mathbb{F}_N)$ when $\left(\frac{\ell}{N}\right) = -1$. One can view the set S inside $PSL_2(\mathbb{F}_N)$ which is equal to $PGL_2(\mathbb{F}_N)^\square$,

and hence we can make a better comparison this way.

Now we concern ourselves with the projection of Γ onto $\text{Cayley}(PGL_2(\mathbb{F}_N)^\square, S)$, the degree of which is $|\mathbb{F}_N^\times|$ (one degree for each scalar multiple of any given matrix M). [Lub] gives us that $\text{Cayley}(PSL_2(\mathbb{F}_N), S)$ is connected, but this graph is also equal to $\text{Cayley}(PGL_2(\mathbb{F}_N)^\square, S)$. We ask how many connected components the cover Γ has.

One can analysing the number of connected components of Γ. If M_1, M_2 are in the same component of Γ, then for f_i endomorphisms in S,

$$M_1 = f_t \circ f_{t-1} \circ \cdots \circ f_1 \circ M_2,$$

hence

$$\det(M_1) = \det(M_2) \cdot \ell^t.$$

Without loss of generality, we can replace M_2 with another matrix in the same connected component and get that

$$\det(M_1 M_2^{-1}) = 1 \mod N,$$

and hence

$$M_1 M_2^{-1} \in SL_2(\mathbb{F}_N).$$

Then we see that

$$M_1 M_2^{-1} = f_t \circ f_{t-1} \circ \ldots f_1 \cdot \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

for $a \in \mathbb{F}_N^\times$. Then M_1 and M_2 are connected in Γ if and only if any such $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ is a product of elements of S.

Using a standard result about Cayley graphs (i.e. Lagrange's theorem) even when S does not generate the group, we know that the number of connected components to the size of the group divided by the size of the set of generators. So long as S is the minimal generating

set of this Cayley graph, this gives us that the number of connected components of Γ as

$$|GL_2(\mathbb{F}_N)^{\square}|/|S|.$$

Certainly one can go further along the lines of this investigation, however, a year is all that is permitted for this thesis.

There are many other questions to be asked about the relations between these graphs. We have seen that this variant of the supersingular isogeny graph with full level N structure provides a cover of the [Lub] graph. What is its second largest eigenvalue? Does it satisfy the Ramanujan bound? These questions require investigation, and this is only the extremal case! Certainly there is more work to be done on the properties of supersingular isogeny graphs with level N structure and the cryptographic security of their hash functions. Additionally, the characterization of the random walk of the ℓ-isogeny volcano still requires work. Hopefully the efforts in this thesis establish some useful results towards accomplishing these goals.

References

[Alon] Alon, Noga; Milman, Vitali D : $\lambda 1$, isoperimetric inequalities for graphs, and superconcentrators. Journal of Combinatorial Theory, Series B. 38, 1 (1985), 73–88. Elsevier.

[Che] Cheeger, Jeff: A lower bound for the smallest eigenvalue of the Laplacian. Proceedings of the Princeton conference in honor of Professor S. Bochner. (1969).

[Cha] Charles, Denis X.; Lauter, Kristin E.; Goren, Eyal Z : Cryptographic hash functions from expander graphs. Journal of Cryptology. 22, 1 (2009), 93–113. Springer.

[Cost] Costache, Anamaria; Feigon, Brooke; Lauter, Kristin; Massierer, Maike; Puskás, Anna : Ramanujan graphs in cryptography. arXiv preprint arXiv:1806.05709, (2018).

[Di] Diestel, Reinhard: Graph theory, (2000). Springer-Verlag New York, Incorporated.

[Ful] Fulton, William: An Introduction to Algebraic Geometry. (2008).

[Gold] Goldfeld, Dorian; Hundley, Joseph: Automorphic representations and L-functions for the general linear group, 1 (2011). Cambridge University Press.

[Gor] Goren, Eyal Z; Kassaei, Payman L: p-adic Dynamics of Hecke Operators on Modular Curves. arXiv preprint arXiv:1711.00269, (2017).

[Gort] Görtz, Ulrich; Wedhorn, Torsten : Algebraic geometry. (2010). Springer.

[Hart] Hartshorne, Robin : Algebraic geometry. 52 (2013). Springer Science & Business Media.

[Hof] Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H : An introduction to mathematical cryptography. 1 (2008). Springer.

[Hoo] Hoory, Shlomo; Linial, Nathan; Wigderson, Avi : Expander graphs and their applications. Bulletin of the American Mathematical Society. 43, 4 (2006), 439–561.

[Klop] Klopsch, Benjamin; Nikolov, Nikolay; Voll, Christopher: Lectures on profinite topics in group theory. Cambridge University Press. 77 (2011).

[Kna] Knapp, Anthony W.: Lie groups beyond an introduction. Springer Science & Business Media. 140 (2013).

[Kn66] Kneser, Martin: Algebraic groups and Discontinuous Subgroups. Proceedings of Symposia in Pure Mathematics. 9, (1966).

[Kn67] Kneser, Martin: Algebraic number theory: proceedings of an instructional conference. 250–264, International Congress of Mathematicians, (1967).

[Krish] Krishnaswami, Govind S; Sachdev, Sonakshi: Algebra and geometry of Hamiltons quaternions. Resonance, 21 (2016). 529–544.

[Lau] Lauter, Kristin : Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs. IEEE Security & Privacy. 15, 4 (2017), 22–27. IEEE.

[Lub] Lubotzky, Alexander; Phillips, Ralph; Sarnak, Peter : Ramanujan graphs. Combinatorica. 8, 3 (1988), 261–277. Springer.

[Mar] Marcus, Adam; Spielman, Daniel A.; Srivastava, Nikhil: Interlacing families I: Bipartite Ramanujan graphs of all degrees. 2013 IEEE 54th Annual Symposium on Foundations of computer science. (2013), 529–537. IEEE.

[Mas] Massey, William S.: Algebraic topology: an introduction. (1967). Harcourt, Brace & World.

[Pet] Petit, Christophe; Lauter, Kristin; Quisquater, Jean-Jacques : Full cryptanalysis of LPS and Morgenstern hash functions. International Conference on Security and Cryptography for Networks. (2008), 263–277. Springer.

[Piz] Pizer, Arnold K.: Ramanujan graphs and Hecke operators. Bulletin of the American Mathematical Society. 23, 1 (1990), 127–137.

[Plat] Platonov, Vladimir Petrovich: The problem of strong approximation and the Kneser-Tits conjecture for algebraic groups. Izvestiya: Mathematics, Turpion Ltd., 3 (1969). 1139–1147.

[Pra] Prasad, Dipendra : Lectures on Algebraic Groups.(2002).

[Lub] Lubotzky, Alexander; Phillips, Ralph; Sarnak, Peter : Ramanujan graphs. Combinatorica. 8, 3 (1988), 261–277. Springer.

[Rap] Rapinchuk, Andrei S: Strong approximation for algebraic groups. Thin groups and superstrong approximation. 61, (2014). 269–298.

[W] Rowland, Todd: A Wolfram Web Resource, created by Eric W. Weisstein.

[Shim] Shimura, Goro: Automorphic functions and number theory. 54 (2006). Springer.

[Sil] Silverman, Joseph H.: The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Sut] Sutherland, Andrew V.: Isogeny volcanoes. ANTS X–Proceedings of the Tenth Algorithmic Number Theory Symposium, 507–530, Open Book Ser., 1, Math. Sci. Publ., Berkeley, CA, 2013.

[Til] Tillich, Jean-Pierre; Zémor, Gilles : Collisions for the LPS expander graph hash function. Annual International Conference on the Theory and Applications of Cryptographic Techniques. (2008), 254–269. Springer.

[Vad] Vadhan, Salil P : Pseudorandomness. Foundations and Trends® in Theoretical Computer Science. 7, 1 – 3 (2012), 1–336. Now Publishers, Inc.

[Velu] Vélu, Jacques : Isogénies entre courbes elliptiques. CR Acad. Sci. Paris, Séries A. 273, (1971), 305–347.

[Wash] Washington, Lawrence C. : Elliptic curves: number theory and cryptography. (2003). Chapman and Hall/CRC.

[Woe] Woess, Wolfgang : Random walks on infinite graphs and groups–a survey on selected topics. Bulletin of the London Mathematical Society. 26, 1 (1994). Wiley Online Library.