DISSERTATION

NUMBER OF 4-CYCLES OF THE GENUS 2 SUPERSPECIAL ISOGENY GRAPH

Submitted by

Vladimir P. Sworski

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2024

Doctoral Committee:

Advisor: Rachel Pries

Alexander Hulpke
Sanjay Rajopadhye
Mark Shoemaker

ABSTRACT

NUMBER OF 4-CYCLES OF THE GENUS 2 SUPERSPECIAL ISOGENY GRAPH

The genus 2 superspecial degree-2 isogeny graph over a finite field of size p^2 is a network graph whose vertices are constructed from genus 2 superspecial curves and whose edges are the degree 2 isogenies between them. Flynn and Ti [1] discovered 4-cycles in the graph, which pose problems for applications in cryptography. Florit and Smith [2] constructed an atlas which describes what the neighborhood of each vertex looks like. We wrote a program in SageMath that can calculate neighborhoods of these graphs for small primes. Much of our work is motivated by these computations. We examine the prevalence of 4-cycles in the graph and, motivated by work of Arpin, et al. [3] in the genus 1 situation, in the subgraph called the spine. We calculate the number of 4-cycles that pass through vertices of 12 of the 14 kinds possible. This also resulted in constructing the neighborhood of all vertices two steps or fewer away for three special types of curves. We also establish conjectures about the number of vertices and cycles in small neighborhoods of the spine.

ACKNOWLEDGEMENTS

I would like to thank my advisor, Rachel Pries. Her guidance and understanding are a big part of the reason I am here today.

I would also like to thank Sanjay Rajopadhye for agreeing to (at a rather late date) serve as a replacement committee member.

DEDICATION

To my mother, whose faith in me never wavered.

TABLE OF CONTENTS

Chapter 1

Introduction

With the advent of quantum computers, modern cryptography is currently at risk of being broken. In 1994, Shor's algorithm was introduced to the world [4]. Given a quantum computer, it can break ECDSA - the current standard cryptosystem. As such, the National Institute for Standards in Technology (NIST) sent out a call for viable post-quantum cryptosystems to replace ECDSA. Such a cryptosystem would need to be both strong against classical attacks and quantum attacks, like Shor's algorithm, as well.

In July of 2022, NIST announced 4 finalists for the potential standardized cryptosystem. One of these made use of Supersingular Elliptic Isogeny graphs - and was called Supersingular Isogeny Key Encapsulation (SIKE). SIKE made use of graphs of supersingular elliptic curves with isogenies between them.

One can also look at graphs of superspecial hyperelliptic curves of genus 2, and their isogenies instead as a higher-dimensional analog. This analog however seemed computationally non-viable for use as the basis of a cryptosystem.

In late July 2022, Castryck and Decru [5] introduced an attack on SIKE using a splitting and gluing method for supersingular elliptic curves taking us through the genus 2 graph.

As such, both graphs have become even more of a topic of interest as cryptographers the world over seek to better understand if there are salvageable alternatives to the standard model for SIKE or to further understand/strengthen the Catryck/Decru attack.

The author of this paper, having already been interested in the genus 2 graph, seeks to better understand its properties. Said properties may be valuable in furthering the discussion around this topic.

Some work has already been done. Florit and Smith [2] for example developed an atlas of the behaviors of different types of vertices in the graph. The curves involved are well understood, and first documented by Ibukiyama, Katsura, and Oort [6].

While tools for calculating such isogenies exist for magma - the author is unaware of any such tools in SageMath. The author constructed a tool in SageMath that examines local neighborhoods of vertices in the graph and is able to classify said vertices by type.

In this paper, the author seeks to better understand the structure of the graph, especially over $\mathbb{F}_p$, and 4-cycles within the graph.

Chapters 2 through 4 discuss how to define the primary object of study for this paper, the superspecial isogeny graph of abelian varieties of genus g over $\mathbb{F}_{p^2}$. These sections are designed to provide the uninitiated with the background necessary for the rest of the paper. In Chapter 2, hyperelliptic curves are defined, as well as Jacobian varieties of hyperelliptic curves. We also discuss the notion of isomorphism class and introduce normal forms for our classes. Then, we introduce isogenies between abelian varieties and discuss how torsion points generate the kernels of these isogenies. We close out by discussing the invariants we use to index vertices in the graph and how to calculate them. In Chapter 3, we start by discussing automorphisms of hyperelliptic curves, how they affect isogenies, and the different types of superspecial genus 2 curves that are possible, sorted by the structure of their automorphism groups. Then, the terms supersingular and superspecial are officially defined, and we discuss some propositions in regards to them. Chapter 4 introduces the isogeny graph itself, and describes some of its properties. We then briefly recap the results of Florit and Smith [2] regarding the neighborhoods of different types of curves.

Chapter 5 is much less theoretical and serves as a primer on how to manually construct the $(2, 2)$-isogeny graph we use throughout the rest of the paper. Section 5.1 discusses how to calculate an isogeny between the Jacobians of two superspecial hyperelliptic curves, and then discusses how to deal with some edge cases we call 'dependent representatives.' Section 5.2 discusses what happens when the map goes to a product of supersingular elliptic curves instead. Section 5.3 discusses how these details are used to calculate neighborhoods of individual vertices on the graph algorithymically using sage. We also discuss various functionality the author's code maintains. All of said code will be available on Github by May 2024.

Chapter 6 presents the author's main results. In the graph, there are 14 types of vertices. We present the number of 4-cycles through 12 of these, as well as exactly which types of curves each cycle passes through.

We also provide extended graphs and visualizations thereof for some of the types beyond the work of Florit and Smith [2]. When relevant, we include the invariants in such graphs for each novel vertex.

Chapter 7 introduces out final object of study, the subgraph analogs for genus 2 of those found in Arpin, et al [3]. We then discuss results and data derived from the author's code for specific families of genus 2 starting vertices, and then form conjectures regarding the results.

Chapter 8 introduces potential future directions of study.

Appendix A includes a brief overview of the Diffie-Hellman protocol, the necessity of post-quantum cryptography and the SIKE cryptosystem. Finally, in Appendix B, we also discuss how it was broken by Castryck and Decru [5] in 2022.

Chapter 2

Background

Much of what is discussed in this chapter is covered in more detail in [7], [8], and [9].

Definition 2.1. *A hyperelliptic curve is an algebraic curve, i.e. an algebraic variety in dimension one, and a double cover of the project line,* $\mathbb{P}^1$. *Let k be a field,* $\mathrm{char(k)} \neq 2, 3$. *A hyperelliptic curve is of the form:*

$$H : y^2 = f(x)$$

where $f(x) \in k[x]$ *and* $\mathrm{deg(f)} = 2\mathrm{g} + 1$ *or* $2g + 2$ *where g is the genus of the curve. In the case where g is 1, H is an elliptic curve.*

In this paper we will use $g = 1$ for the sake of example and discussion, but will primarily focus on $g = 2$.

Definition 2.2. *A divisor of H is an element of the free group over the points of H.*

$$\mathfrak{r} = \sum_{m \in H} n_m[m], n_m \in \mathbb{Z}.$$

$\mathrm{Div(H)}$ *is the set of all divisors on H. The degree of a divisor is the sum of its coefficients,*

$$\mathrm{deg}(\mathfrak{r}) = \sum_{m \in H} n_m.$$

The degree cannot be infinite, as the support of an element of a free group must be finite. We call a divisor effective if all the $n_m \geq 0$. Now consider $f \in k(H)^*$. Using a local uniformizer, we can talk about the order of f at individual points $m \in H$.

Definition 2.3. *A principal divisor is a divisor over f given by:*

$$\mathrm{div(f)} = \sum_{\mathrm{m \in H}} \mathrm{ord_m(f)[m]}.$$

Principal divisors have degree zero according to the Riemann-Roch Theorem. We denote the set of degree zero divisors by $\mathrm{Div}^0(\mathrm{H})$ and the set of principal divisors by $\mathrm{PDiv}(\mathrm{H})$. Clearly the latter is a subgroup of the former, and we can form a quotient.

Definition 2.4.

$$\mathrm{Jac}(\mathrm{H}) \cong \mathrm{Pic}^0(\mathrm{H}) := \mathrm{Div}^0(\mathrm{H})/\mathrm{PDiv}(\mathrm{H}).$$

This quotient is sometimes called the Picard Variety, and what we will call the Jacobian Variety.

Notice that for any point $m = (x, y) \in H$, there is a conjugate point $\overline{m} = (x, -y) \in H$. If $y = 0$, then $m = \overline{m}$.

For an elliptic curve, i.e. g=1, we define the group law on the Elliptic Curve as such: consider $m_1, m_2 \in H$. The line $\overline{m_1 m_2}$ is degree one, and the elliptic curve can be regarded as degree 3. By Bezout's Theorem, there are three intersection points. Two of these will be m_1, m_2. We define the third point to be $\overline{m_3}$ and

$$m_1 + m_2 = -\overline{m_3}.$$

If we add m_3 to $\overline{m_3}$ we should get the point at infinity, O. We may arbitrarily choose our identity point. For simplicity we choose O to be the identity. But then, this implies:

$$\overline{m_3} = -m_3$$

and as such our group law simplifies to,

$$m_1 + m_2 = m_3.$$

If we define the map

$$\phi : H \to \mathrm{Jac}(\mathrm{H}),$$

$$m \mapsto [m],$$

we see that the Jacobian can directly inherit the structure of H and that

$$H \cong \mathrm{Jac(H)}$$

as it is typically defined.

The above process is less clear in the genus 2 case. Here, rather than defining the group law on the curve, we do so directly on its Jacobian. According to Riemann-Roch, the canonical divisor on H has degree 2. We note that the intersection of the line $x = x_0$, with the curve for generic $x_0 \in k$ results in two points:

$$\mathfrak{r} = (x_0, y_0), \overline{\mathfrak{r}} = (x_0, -y_0).$$

Any two divisors of the form $\mathfrak{R} = \{\mathfrak{r}, \overline{\mathfrak{r}}\}$ are linearly equivalent (differ by a principal divisor). We denote this element of $\mathrm{Pic}^2(\mathrm{H})$ by $\mathfrak{D}$.

A divisor is considered effective if all of its coefficients are non-negative. Riemann-Roch implies that each divisor class has a unique effective divisor. We will henceforth use the effective divisor as the class representative.

Consider now the map:

$$\psi : \mathrm{Pic}^0(\mathrm{H}) \to \mathrm{Pic}^2(\mathrm{H}),$$

$$\mathfrak{R} \mapsto \mathfrak{R} + \mathfrak{D}$$

where the image is identified with the unique effective divisor of degree two, we will usually denote $\mathfrak{A}$. Note that, 0 is sent to $\mathfrak{D}$.

We now define the group law on the curve. Let $\mathfrak{A}, \mathfrak{B}$ be effective divisors in $\mathrm{Pic}^2(\mathrm{H})$ consisting of the points $(\mathfrak{r}, \overline{\mathfrak{r}})$ and $(\mathfrak{s}, \overline{\mathfrak{s}})$ respectively. Through these four points, one can construct a unique degree three curve. Such a curve intersects H in two further points: $(\mathfrak{t}, \overline{\mathfrak{t}})$ which we label $\mathfrak{C}$. We then define a simplified form of our group law,

$$\mathfrak{A} + \mathfrak{B} + \mathfrak{C} = \mathfrak{D}.$$

2.1 Isomorphism Classes

We wish to think about isomorphism classes of Abelian surfaces when constructing our isogeny graph. Isomorphisms take the form of Linear Fractional Transformations (LFTs).

Definition 2.5. *A Linear Fractional Transformation is an invertible map* $\Phi : \mathbb{P}(\bar{\mathbb{F}_p}^1) \to \mathbb{P}(\bar{\mathbb{F}_p}^1)$ *s.t. for* $a, b, c, d \in \bar{\mathbb{F}_p}$

$$\Phi([x : y]) = [ax + b : cy + d].$$

We note when taken over affine space, this map has the familiar form

$$\Phi(z) = \frac{az + b}{cz + d},$$

with the point at infinity being sent to a/c.

The group of all LFT's over $\bar{\mathbb{F}_p}$ is isomorphic to $\mathrm{PGL}_1(\bar{\mathbb{F}}_\mathrm{p})$. As a three-dimensional family, this implies that, in general, there are three degrees of freedom in choosing the equation for a hyperelliptic curve.

In genus 1, elliptic curves take the generic form

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)(x - \lambda_4),$$

for $\lambda_i \in \bar{\mathbb{F}_p}$. Thus they have 4 degrees of freedom (for the degree 3 representation of an elliptic curve, the fourth point is the point at infinity) and thus the moduli space of elliptic curves is 1-dimensional. We can then fix two of the curve's roots and find a representative of our elliptic curve of the form

$$y^2 = x(x - 1)(x - \lambda),$$

$\lambda \in \bar{\mathbb{F}_p}$. as is standard.

We will represent the isomorphism class of an algebraic variety C, by $[C]$.

For the sake of simplicity of calculation and representation we choose to represent our hyperelliptic curves via special kinds of representatives, akin to that for elliptic curves. One is a degree 5 representative, and the other a degree 6.

Definition 2.6. *Let $g = 2$. A representative of an isomorphism class, [H] of a Hyperelliptic Curve is said to be in Rosenhain Normal Form (RNF) if it takes the form*

$$H : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

for $\lambda_i \in \bar{\mathbb{F}}_p$.

Definition 2.7. *Let $g = 2$. A representative of an isomorphism class, [H] of a Hyperelliptic Curve is said to be in Reverse Rosenhain Normal Form (RRNF) if it takes the form*

$$H : y^2 = x(x-1)(x+1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

for $\lambda_i \in \bar{\mathbb{F}}_p$.

We note that it is always possible to find a representative in RNF. If our curve is of the form:

$$H : y^2 = \prod_{i=1}^{n}(x-\alpha_i)\prod_{j=1}^{3}(x-\beta_i),$$

then we can find a representative for it in RNF by applying the following LFT to H if $n = 2$:

$$\frac{z-\alpha_1}{\alpha_2-\alpha_1},$$

or, if $n = 3$:

$$\frac{\alpha_3-\alpha_1}{\alpha_3-\alpha_2}\frac{z-\alpha_2}{z-\alpha_1}.$$

Similarly, it is always possible to find a representative in RRNF. Assume H is in RNF form with roots $0, 1, \lambda_1, \lambda_2, \lambda_3$. Then we apply one of the following LFTs:

$$\frac{1}{1-2z}, \quad \frac{z-1}{z+1}, \quad \frac{z}{2-z}.$$

The first applies as long as no $\lambda_i = \frac{1}{2}$, the second if no $\lambda_i = -1$, and the last if no $\lambda_i = 2$. On the off chance that all three of these values are one of the λ_i, then the RRNF form is:

$$y^2 = x(x-1)(x+1)(x-\frac{1}{3})(x-\frac{1}{5})(x-\frac{1}{2}).$$

While this leads to a computationally simple representations of our vertices, the problem remains that our choices for the roots used to construct the first LFT, (versus those affected by it,) remain arbitrary. There are $\binom{6}{3}$ ways to select the set of α_i's, but its permutations produce different results. Hence there are 120 unique LFTs to RNF form from an arbitrary H.

However, every $[H]$ does not contain 120 unique polynomials in RNF form. (Although the mass majority, in fact do.) Rather, due to the automorphism group of $[H]$ there are only

$$\frac{120 \cdot 2}{|\mathrm{Aut}([\mathrm{H}])|}$$

unique representatives, for both RNF and RRNF. (The '2' will become clear in Chapter 3.)

However, this is enough to conclude that the RNF and RRNF forms cannot serve as a curve invariant in the same way that $y^2 = x(x-1)(x-\lambda)$ usually does for elliptic isomorphism classes. This will serve as inspiration for developing actual invariants for our curves in Section 2.3.

2.2 Isogenies and Torsion

We now turn our attention to morphisms of abelian varieties.

Definition 2.8. *We define an isogeny of abelian varieties as a surjective map with finite kernel that preserves identity.*

Such a map leads to the following short exact sequence:

$$0 \to K \hookrightarrow H \twoheadrightarrow H' \cong H/K \to 0.$$

As K is finite, it must be part of the torsion subgroup of H.

Definition 2.9. *The size of K is called the degree of the isogeny.*

One important isogeny is a polarization - a map from a variety to its dual.

$$\phi : H \to H^\vee.$$

There also exists a dual map

$$\phi^\vee : H^\vee \to H$$

which composes so that

$$\phi^\vee \circ \phi = [\deg(\phi)]_H, \quad \phi \circ \phi^\vee = [\deg(\phi)]_{H^\vee}.$$

If the composition is equal to the identity, i.e. $\deg(\phi) = 1$, we say that H is principally polarized. Jacobian varieties are always principally polarized. In genus 1, a curve is dual to its Jacobian. Hence, Elliptic Curves are isomorphic to their Jacobian Varieties. This however, is not true of higher genuses.

Varieties in this paper are always taken to be paired with a polarization. The principal polarization on a Jacobian variety is given by its theta divisor, associated to the varieties' associated Riemann Theta function.

Genus 1

Consider now an elliptic curve, E. We can generate an isogeny of prime order, p, by setting $K = \langle P \rangle$ for $P \in E[p]$, the p-torsion subgroup of E.

$$E' \cong E/\langle P \rangle.$$

With this, we can count the number of p-isogenies of E by counting the number of order p subgroups of E. Let us consider 2-torsion for an example.

Definition 2.10. *A 2-torsion point is a point of the form*

$$[R] + [R] = [O].$$

This can only happen if

$$[R] = [\overline{R}],$$

i.e $(x, y) = (x, -y)$. This occurs at the zeroes of $f(x)$, as well as the point at infinity. Thus we acquire three 2-torsion subgroups of size 2, each generated by a different zero of $f(x)$.

In the case of 3-torsion, we need to identify the points where

$$3[R] = [O].$$

This is manageable, but more difficult. However, larger p are too computationally taxing to be useful for applications.

Genus 2

We again turn our attention to $g = 2$. Recall that rather than working over H we must work over $\mathrm{Jac(H)}$ as this is where our group structure lies. Again, turning to 2-torsion points, we note

that $\mathrm{Jac}(\mathrm{H})[2]$ is more complicated than the 2-torsion of an elliptic curve. Let

$$\mathfrak{A} = (a_1, a_2).$$

Since $\overline{\mathfrak{A}} = -\mathfrak{A}$, it follows that

$$\mathfrak{A} + \overline{\mathfrak{A}} = \mathfrak{D}.$$

Hence two torsion points occur for $\mathfrak{A} \neq \mathfrak{D}$, where $\mathfrak{A} = \overline{\mathfrak{A}}$. This occurs precisely for pairings of the six roots of H. e.g.

$$\mathfrak{A} = \{(\theta_1, 0), (\theta_2, 0)\}.$$

We also note that since

$$\{(\theta_1, 0), (\theta_2, 0)\} + \{(\theta_3, 0), (\theta_4, 0)\} = \{(\theta_5, 0), (\theta_6, 0)\},$$

we can generate a 2-torsion subgroup of $\mathrm{Jac}(\mathrm{H})$ from two divisors $\mathfrak{A}, \mathfrak{B} \in \mathrm{Jac}(\mathrm{H})[2]$. Hence, such subgroups are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. An isogeny of the form

$$\phi : \mathrm{Jac}(\mathrm{H}) \to \mathrm{Jac}(\mathrm{H})/\mathfrak{A}$$

for $\mathfrak{A}$ as described above is called a $(2, 2)$-isogeny. We note that there are $\binom{6}{2} = 15$ possible elements in $\mathrm{Jac}(\mathrm{H})$ of degree two [9], and further there are also 15 possible $(2, 2)$-isogenies. In Chapter 5 we will further examine how to calculate these isogenies.

Remark. *More broadly, we refer to a genus 2 isogeny constructed from p-torsion points as a (p, p)-isogeny.*

2.3 Invariants

In this section we will be investigating how to differentiate between curves using invariants.

Genus 1

We can tell when two elliptic curves over k are isomorphic by their j-invariant.

Definition 2.11. *Consider an elliptic curve over k of the form* $E : y^2 = x^3 + ax + b$. *Let*

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{2.1}$$

We call j, the j-invariant of E.

Theorem 2.12. *Over an algebraically closed field, any two elliptic curves with the same j-invariant are isomorphic.*

Genus 2

We would like a way to tell apart isomorphism classes of Hyperelliptic Curves - i.e. an analog to the j-invariant for Genus 2. We will be using the absolute Igusa invariants of Kohel, as built into SageMath, as our invariants of choice in this paper.

Consider H a representative for $[H]$ s.t.

$$H : y^2 = u(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)(x - x_6).$$

Igusa [10] first defined invariants for $[H]$ as follows:

$$J_2 = u^2 \sum_{y_i = \sigma(x_j), \sigma \in \Sigma_2} (y_1 - y_2)^2(y_3 - y_4)^2(y_5 - y_6)^2,$$

$$J_4 = u^4 \sum_{y_i = \sigma(x_j), \sigma \in \Sigma_4} (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2(y_4 - y_5)^2(y_5 - y_6)^2(y_6 - y_4)^2,$$

$$J_6 = u^6 \sum_{y_i = \sigma(x_j), \sigma \in \Sigma_6} (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2(y_4 - y_5)^2(y_5 - y_6)^2(y_6 - y_4)^2 \cdot$$

$$(y_1 - y_4)^2(y_2 - y_5)^2(y_3 - y_6)^2,$$

$$J_{10} = u^{10} \prod_{i<j} (x_i - x_j)^2.$$

A few things to note:

- There is no J_8 invariant as $J_8 = 2^{-2}(J_2 J_6 - J_4^2)$.
- J_{10} is the discriminant.
- These invariants are not 'absolute' as they depend on the given value of u. If we represent the invariants as a 4-tuple:

  $$(J_2, J_4, J_6, J_{10}) \in \mathbb{F}_{p^2}^4,$$

  this implies that we have an equivalence condition defined s.t.

  $$(J_2, J_4, J_6, J_{10}) \equiv (nJ_2, n^2 J_4, n^3 J_6, n^5 J_{10})$$

  for $n \in \mathbb{F}_{p^2}$, $n \neq 0$.

This last bullet point makes Igusa's invariants insufficient for our purposes. However, Kohel [11] would develop a set of absolute invariants based off of Igusa's that do not depend on the value of u.

Definition 2.13. *Kohel's Invariants for a hyperelliptic curve H, are a 3-tuple of invariants in $\mathbb{F}_{p^2}$ s.t. if $H_1, H_2 \in [H]$ the Kohel Invariants of H_1 are equal to the Kohel Invariants of H_2. If (J_2, J_4, J_6, J_{10}) represent the Igusa Invariants of a curve $H \in [H]$. then Kohel's Invariants are defined as*

$$(k_1, k_2, k_3) := (\frac{J_4 J_6}{J_{10}}, \frac{J_2^3 J_4}{J_{10}}, \frac{J_2^2 J_6}{J_{10}}).$$

It is this tuple that we will use to differentiate our isomorphism classes in genus 2

Chapter 3

Supersingularity and Automorphisms

Let k be a field of characteristic $p > 5$. In this chapter we will be looking into what the automorphism groups of the curves look like, and then what it means for a curve to be supersingular or superspecial.

3.1 Automorphisms

First, we note that all Hyperelliptic Curves come equipped with the automorphism

$$\alpha(x, y) = (x, -y).$$

Genus 1

According to Silverman [7], for all elliptic curves with j-invariant, $j \neq 0, 1728$, α is the only nontrivial automorphism. Hence. $\mathrm{Aut(E)} \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem 3.1. *Let E be a supersingular elliptic curve, with $j \neq 0, 1728$. Then the images of E under each of the three 2-isogenies are distinct.*

Proof. Let $K_1, K_2 < E$ be distinct with $K_i \cong \mathbb{Z}/2\mathbb{Z}$. (Generated by a 2-torsion point.) Assume $\exists \phi : E/K_1 \to E/K_2$, an isomorphism. This lifts to an automorphism, ϕ^*, of E where $\phi^*(K_1) = K_2$. The only non-trivial automorphism for elliptic curves with $j \neq 0, 1728$ is $\alpha(x, y) = (x, -y)$. Since the y-coordinate for a 2-torsion point is 0, α acts trivially on the 2-torsion, but ϕ^* does not act trivially on the 2-torsion. $\to\leftarrow$. Hence, $E/K_1 \ncong E/K_2$.

$$\begin{array}{ccc} E & \longrightarrow & E/K_1 \\ \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \phi} \\ E & \longrightarrow & E/K_2 \end{array}$$

Figure 3.1: Our commutative diagram

□

Genus 2

Hyperelliptic curves of genus 2 often have much larger automorphism groups than those in genus 1. We recognize that the automorphism $\alpha(x, y) = (x, -y)$ continues to act trivially on 2-torsion points and hence we define the reduced automorphism group for simplicity:

Definition 3.2.

$$\mathrm{RA(H)} \cong \mathrm{Aut(H)}/\langle\alpha\rangle.$$

Ibukiyama, Katsura, and Oort [6] identified 6 families of hyperelliptic curves with nontrivial $\mathrm{RA(H)}$. [6] They are as follows:

- A *Type 1* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathbb{Z}/2\mathbb{Z}$. There is a 2-dimensional family of these curves, which can be described in RNF form by the equation:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\frac{1-\mu}{1-\lambda}). \tag{3.1}$$

- A *Type 2* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathrm{S}_3$. There is a 1-dimensional family of these curves, which are a specialization of Type 1 curves, and can be described in RNF form by the equation:

$$y^2 = x(x-1)(x-\lambda)(x-\frac{\lambda-1}{\lambda})(x-\frac{1}{1-\lambda}). \tag{3.2}$$

- A *Type 3* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. There is a 1-dimensional family of these curves, which are a specialization of Type 1 curves, and can be described in RNF form by the equation:

$$y^2 = x(x-1)(x+1)(x-\lambda)(x-\frac{1}{\lambda}). \tag{3.3}$$

- A *Type 4* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathrm{D}_{12}$, (order 12.) There is a 0-dimensional family of these curves, i.e. a single isomorphism class. It is a specialization of both Type 2 and Type 3 curves. Two common representations for the curve are

$$y^2 = x(x-1)(x+1)(x-2)(x-\frac{1}{2}), \tag{3.4}$$

$$y^2 = x^6 - 1. \tag{3.5}$$

- A *Type 5* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathrm{PGL}(2,5)$ if $p = 5$ or $\mathrm{RA(H)} \cong \mathrm{S}_4$ if $p \neq 5$. There is a 0-dimensional family of these curves, i.e. a single isomorphism class. It is a specialization of Type 3 curves. A common representation for this curve is

$$y^2 = x(x-1)(x+1)(x-i)(x+i) = x^5 - x. \tag{3.6}$$

- A *Type 6* hyperelliptic curve has $\mathrm{RA(H)} \cong \mathbb{Z}/5\mathbb{Z}$. There is a 0-dimensional family of these curves, i.e. a single isomorphism class. It is a specialization of Type 1 curves. Two common representations for the curve are

$$y^2 = x(x-1)(x-1-\zeta_5)(x-1-\zeta_5-\zeta_5^2)(x-1-\zeta_5-\zeta_5^2-\zeta_5^3), \tag{3.7}$$

$$y^2 = x^5 - 1. \tag{3.8}$$

There is a further family of curves we will call *Type 0*, which is 3-dimensional. It has $\mathrm{RA(H)} \cong 1$, i.e. like most elliptic curves, there are no automorphisms that act-nontrivially on the 2-torsion. Because of this, every isogeny has a unique image. The generic RNF form describes a Type 0 curve:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu). \tag{3.9}$$

Now we consider the products of elliptic curves that can be the image of an isogeny from $\mathrm{Jac}(\mathrm{H})$. There are 7 possibilities for a product of elliptic curves, listed by Florit and Smith [12]:

- *Type* Π*:* This is a product of two, non-identical elliptic curves, neither with $j = 0, 1728$. The family of these products is 2-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/2\mathbb{Z}$.

- *Type* Π_0*:* This is a product of two, non-identical elliptic curves. One has $j = 0$, the other has $j \neq 0, 1728$. The family of these products is 1-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/6\mathbb{Z}$.

- *Type* Π_{1728}*:* This is a product of two, non-identical elliptic curves. One has $j = 1728$, the other has $j \neq 0, 1728$. The family of these products is 1-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/4\mathbb{Z}$.

- *Type* Σ*:* This is a product of two, identical elliptic curves with $j \neq 0, 1728$. The family of these products is 1-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- *Type* $\Pi_{0,1728}$*:* This is a product of two, non-identical elliptic curves. One has $j = 0$, the other has $j = 1728$. The family of these products is 0-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/12\mathbb{Z}$.

- *Type* Σ_0*:* This is a product of two, identical elliptic curves with $j = 0$. The family of these products is 0-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/6\mathbb{Z} \times \mathrm{S}_3$.

- *Type* Σ_{1728}*:* This is a product of two, identical elliptic curves with $j = 1728$. The family of these products is 0-dimensional. Here $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$.

Unfortunately different 'type' notations are used by different sources for these curves. The following is a conversion table between notations. We use Ibukiyama, Katsura, and Oort's notation in this paper[1] for Jacobians of Hyperelliptic Curves and Florit and Smith's notation for products of Elliptic Curves.

[1]Technically, IKO does not mention type 0 at all. We use 0 to maintain a sense of consistency.

Table 3.1: A table of notational differences present in genus 2.

Hyperelliptic Curves: Ibukiyama, Katsura, Oort	0	1	2	3	4	5	6
Florit, Smith	A	I	IV	III	V	VI	II
Elliptic Products:							
Florit, Smith	Π	Π_0	Π_{1728}	Σ	$\Pi_{0,1728}$	Σ_0	Σ_{1728}
My Code	E23	E02	E12	E22	E01	E00	E11

We now discuss the relationship between reduced automorphism groups and kernels of isogenies.

Definition 3.3. *Let K be the kernel of an isogeny, $\phi : A \to A'$. Consider O_K, the orbit of K under $RA(A)$. There are $\#O_K$ distinct kernels of isogenies representing $[\phi]$. Define, $w([\phi]) = \#O_K$.*

As a corollary to the Orbit-Stabilizer theorem, the following theorem tells us information on how the weights of edges in the isogeny graph defined in Chapter 4 are related to the sizes of autmorphism groups.

Theorem 3.4. *Orbit-Stabilizer Theorem for Isogeny Graphs*

Let $\phi : A \to A'$ be an isogeny, and $\phi' : A' \to A$ be the isogeny dual to ϕ. Then,

$$|\mathrm{RA(A)}| \cdot \mathrm{w}([\phi']) = |\mathrm{RA(A')}| \cdot \mathrm{w}([\phi]).$$

With this it is now possible to categorize the isogenies of a superspecial genus 2 curve into what type the image is and how many isogenies have the same images, for all 14 types of curves (the above 7 types of hyperelliptic curves and 7 types of products of ellptic curves). Each curve type has a regular neighborhood, and Florit and Smith [2] have documented what these neighborhoods look like for each type. We will address this in more detail in the next chapter.

3.2 Supersingularity

We will build isogeny graphs in the next chapter using isomorphism classes of supersingular/-superspecial curves. Without these criteria, the graph would not be connected.

Genus 1

Theorem 3.5. *Let k be an algebraically closed field and E/k be an elliptic curve. Then* $\mathrm{End}(\mathrm{E})$ *is either of rank 1,2, or 4. When* $\mathrm{End}(\mathrm{E})$ *has rank 4, it is a maximal order in a quaternion algebra [7].*

Definition 3.6. *When the rank of* $\mathrm{End}(\mathrm{E})$ *is larger than 1, we say the curve has Complex Multiplication (CM). When* $\mathrm{End}(\mathrm{E})$ *is a maximal order in a quaternion algebra we say* E *is a supersingular curve.*

The following result is succinctly stated as Corollary 2.6 in [13], but is derived from statements of Silverman [7].

Theorem 3.7. *If k is a finite field of characteristic p, all supersingular curves can be defined over* $\mathbb{F}_{p^2}$.

As k will be of characteristic p for the remainder of the paper (unless stated otherwise), we will assume we can define all supersingular elliptic curves over $\mathbb{F}_{p^2}$ moving forward.

Genus 2

We now turn our attention back to genus 2. The notion we choose as an analog to a Supersingular Elliptic Curve is a Superspecial Hyperelliptic Curve.

Definition 3.8. *H is called superspecial if* $\mathrm{Jac}(\mathrm{H}) \cong \mathrm{E}_1 \times \mathrm{E}_2$, *a product of two supersingular elliptic curves (ignoring the polarization).*

Recall that a Hyperelliptic curve, H, has equation $y^2 = f(x)$ where $f(x)$ is a degree 5 or 6 polynomial.

Definition 3.9. *Define c_j for $0 \leq j \leq 3(p-1)$ so that,*

$$f(x)^{(p-1)/2} = \sum_{j=0}^{3(p-1)} c_j x^j. \tag{3.10}$$

Then the Cartier-Manin matrix is given by,

$$\begin{bmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{bmatrix}. \tag{3.11}$$

Theorem 3.10. *H is superspecial iff the Cartier-Manin matrix is 0 in every place [6].*

We have an analog to Theorem 3.7 in genus 2 as well, discussed by Florit and Smith in [2], Chapter 1.

Theorem 3.11. *If k is a finite field of characteristic p, all superspecial curves can be defined over $\mathbb{F}_{p^2}$.*

Further, Ibukiyama, Katsura, and Oort [6] tell us exactly when the Type 4,5, and 6 curves should be superspecial.

Theorem 3.12. *Let H be a hyperelliptic curve of genus 2 defined over a finite field k, of characteristic $p > 5$.*

a) A type 4 curve is superspecial if $p \equiv 5 \mod (6)$.

b) A type 5 curve is superspecial if $p \equiv 5, 7 \mod (8)$.

c) A type 6 curve is superspecial if $p \equiv 4 \mod (5)$.

Chapter 4

The Isogeny Graph

4.1 Definition and Nature of the Graph

In this section we will define the graph, $\Gamma_g^{SS}(l,p)$. The vertices of this graph are isomorphism classes of superspecial abelian varieties of dimension g over $\mathbb{F}_{p^2}$. The edges are $(l,\ldots,l)$ isogenies (in this paper l or (l,l) as appropriate).

Genus 1

Definition 4.1. *Let $\Gamma_1^{SS}(2,p)$ be the graph defined in the following way. The vertices are supersingular elliptic curves over $\mathbb{F}_{p^2}$. The edges are 2-isogenies over the same field between the elliptic curves.*

With the possible exception of vertices with j-invariants 0 or 1728, the graph is unweighted as each isogeny has a unique image and is undirected due to the unique dual isogeny. As there are 3 possible 2-isogenies for a given vertex, the graph is 3-regular.

Genus 2

Definition 4.2. *Let $\Gamma_2^{\mathrm{SS}}(2,p)$ be the graph defined in the following way. The vertices are the Jacobians of superspecial hyperelliptic curves of genus 2 and products of two supersingular elliptic curves over $\mathbb{F}_{p^2}$. The edges are $(2,2)$-isogenies over the same field between these varieties.*

The vertices are a mix of the 14 types of curves mentioned in section 3.1. This graph is weighted. For a given isogeny ϕ, representing an edge, the weight of the edge is given by $\mathrm{w}([\phi])$ as described as also described in Definition 3.3. The graph is also directed, as Theorem 3.4 demonstrates that the weight of an isogeny and its dual isogeny need not match. There are 15 possible $(2,2)$-isogenies for (almost) all vertices, thus the graph is 15-regular.

Distance, Local Neighborhoods, and 4-Cycles

We establish, in brief, a metric on our graph for future discussion. First let's classify paths in our graphs:

Definition 4.3. *A path, γ in $\Gamma_2^{\mathrm{SS}}(2,p)$ is a collection of vertices, $\gamma_i \in \mathrm{V}(\Gamma_2^{\mathrm{SS}}(2,\mathrm{p})$, denoted by $\gamma = [[E_0],[E_1],\ldots,[E_n]]$ where $\exists$ a $(2,2)$-isogeny between every pair $[E_i]$ and $[E_{i+1}]$. We denote the set of paths in the graph starting at the vertex $[E_1]$ and ending at $[E_2]$ by $\mathrm{Path}([\mathrm{E}_1],[\mathrm{E}_2])$ and the set of paths without repeat edges from $[E_1]$ to $[E_2]$ by $\overline{\mathrm{Path}}([E_1],[E_2])$. The length of a path is given by the number of edges it passes through, or more formally:*

$$\mathrm{length}([[\mathrm{E}_0],[\mathrm{E}_1],\ldots,[\mathrm{E}_n]]) = \mathrm{n}.$$

With this, we define a notion of distance on our graph:

Definition 4.4. *Let $[E_1],[E_2]$ be two vertices in $\Gamma_2^{\mathrm{SS}}(2,p)$ for some prime p. Define,*

$$d : \mathrm{V}(\Gamma_2^{\mathrm{SS}}(2,\mathrm{p}))^2 \to \mathbb{N} \cup \{0,\infty\}$$

s.t.

$$d([E_1],[E_2]) = \begin{cases} 0 & E_2 \in [E_1], \\ \infty & \overline{\mathrm{Path}}([E_1],[E_2]) = \emptyset, \\ \min\{\mathrm{length}(\gamma) \mid \forall \gamma \in \overline{\mathrm{Path}}([\mathrm{E}_1],[\mathrm{E}_2])\} & \text{otherwise.} \end{cases}$$

It can be shown that this is a metric, but we will not prove that here. Also note, that since the graph is connected, $\overline{\mathrm{Path}}([E_1],[E_2]) \neq \emptyset$. As such, this case is only for dealing with sub-graphs that inherit this metric.

We now define the primary object our code creates.

Definition 4.5. *Define the vertex set*

$$V_n([H]) := \{[C] \in V(\Gamma_2^{\mathrm{SS}}(2,p))\} \mid d([H],[C]) \leq n\},$$

and the edge set

$$E_n([H]) := \{(v_1, v_2) \in E(\Gamma_2^{\mathrm{SS}}(2,p)) \mid v_1, v_2 \in V_n([H])\}$$

We define a 'Neighborhood of Radius n through Starting vertex $[H]$' *as the graph $N_n([H])$ which consists of the vertices in $V_n([H])$ and the edges in $E_n([H])$.*

Note that by this definition, $N_n([H])$ contains self-loops and common edges between vertices at distance n away from $[H]$.

As a warning, our code can construct these neighborhoods, although it likely includes extra information for processing and can be missing information depending on construction parameters.

Finally, we have the tools to define what a 4-cycle is.

Definition 4.6. *If $\exists \gamma \in \overline{\mathrm{Path}}([C],[C])$ s.t. $\mathrm{length}(\gamma) = 4$, we call γ a 4-cycle* [2] *through $[C]$.*

Further, we call a 4-cycle, an Unweighted-Undirected *cycle (UU) if we consider $[E_1, E_2, E_3, E_4, E_1]$ and $[E_1, E_4, E_3, E_2, E_1]$ to be the same cycle and any different isogenies between two vertices (disregarding the weights of edges) to result in the same cycle. Alternatively, if directions and alternate isogenies are considered to result in different cycles, we call them* Weighted-Directed *cycles (WD).*

[2] In genus 1, cryptographic applications rely heavily on the graph being an expander graph and Ramanujan. We do not define these terms here, but note that due to the existence of 4-cycles in the genus 2 graph, it is not Ramanujan. Castryck, Decru, and Smith [14] found a 'fix' for this in cryptographic applications, but it is one of the reasons such a cryptosystem is too slow to be viable. We direct the reader to their paper for further details.

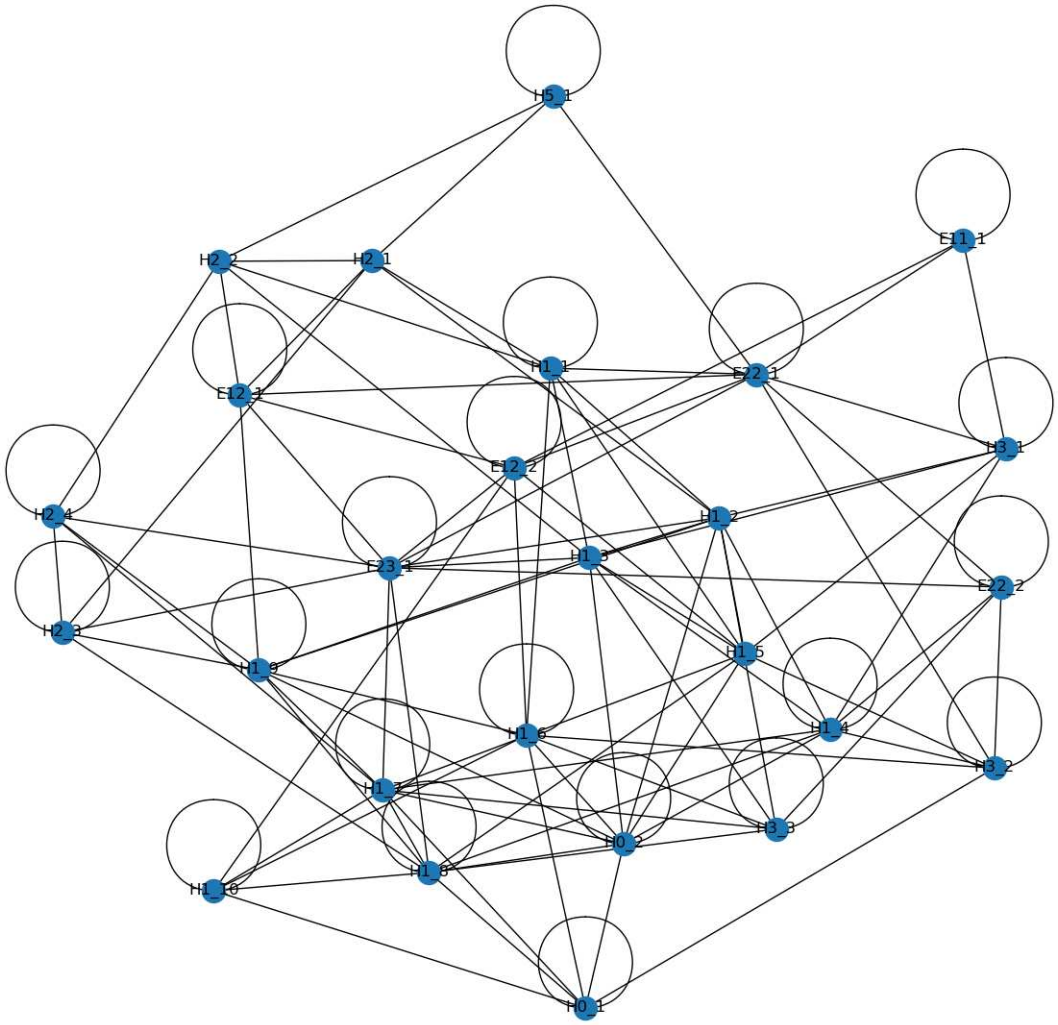

Figure 4.1: A 'small' example: the full $\Gamma_2^{\mathrm{SS}}(2, 31^2)$ graph.

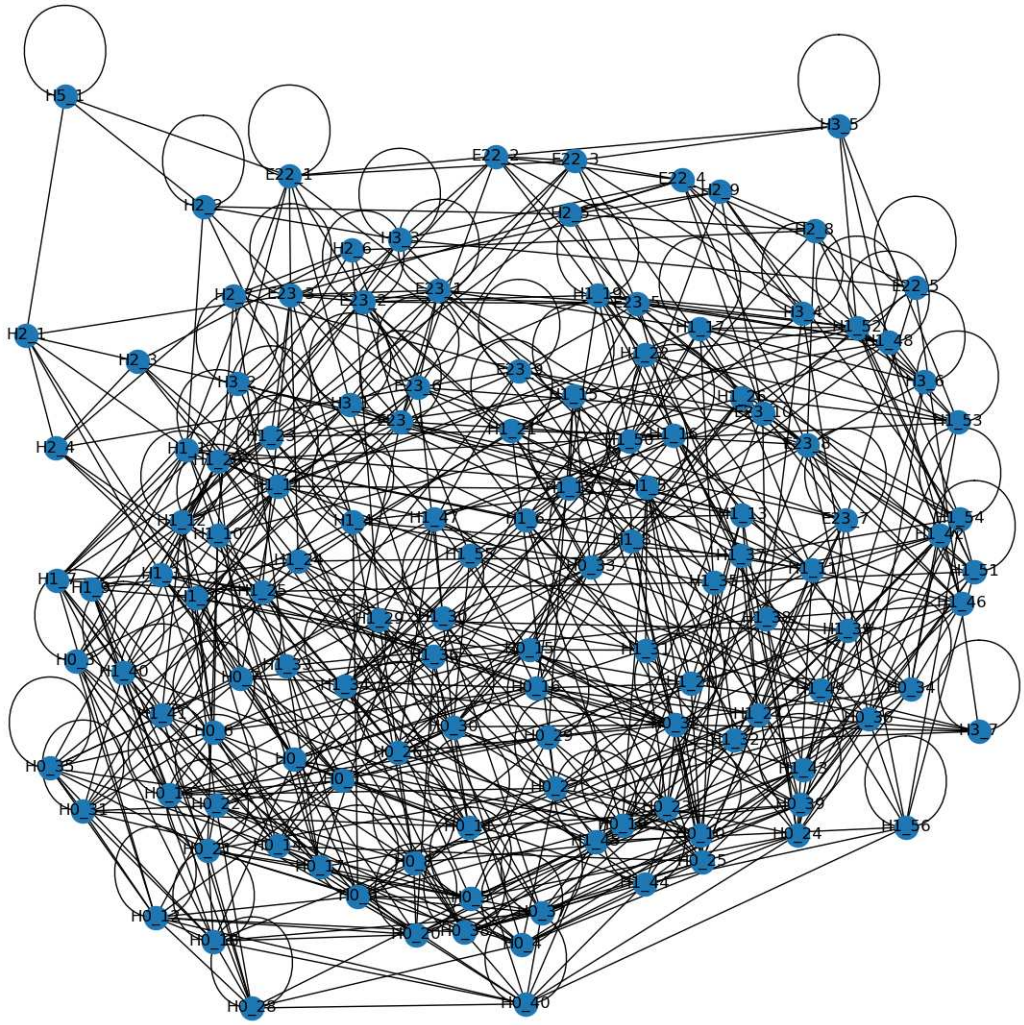

Figure 4.2: A 'much larger' example: the full $\Gamma_2^{\mathrm{SS}}(2, 61^2)$ graph.

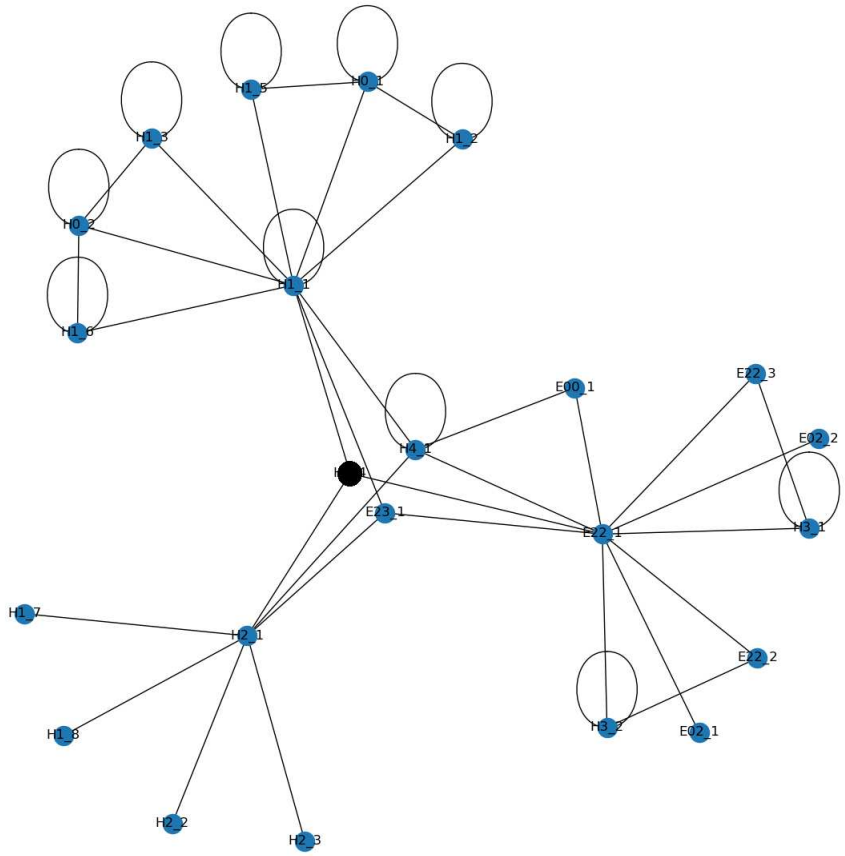

Figure 4.3: An example consisting of only vertices nearby the curve: $y^2 = x^6 - 1$. A portion of the $\Gamma_2^{\mathrm{SS}}(2, 1031^2)$ graph, the radius 2 neighborhood around this vertex: $N_2([\mathrm{Jac}(\mathrm{y}^2 = \mathrm{x}^6 - 1)])$.

4.2 The Florit and Smith Atlas

In this section we will explore the Atlas that Florit and Smith [2] constructed as it pertains to our work. The authors determined, for a general vertex of each type what the types of the neighbors around it should be up to generalization and their associated edge weights. We expand on this, especially as it pertains to 4-cycles, in Chapter 6 of this paper.

Type 0

A type 0 vertex has a trivial reduced automorphism group and hence, each edge has weight 1. For a generalized type 0 vertex we therefore have 15 outgoing edges of weight 1, which go to other

type 0 vertices. Florit and Smith [2] also determined that there would be 12 unweighted-undirected cycles through a general type 0 vertex.

The general type 0 vertex has

- 15, weight 1, isogenies with an image curve of type 0.

Type 1

The general type 1 vertex has

- 4, weight 2, isogenies with an image curve of type 0;
- 6, weight 1, isogenies with an image curve of type 1;
- 1, weight 1, isogeny with an image curve of type Π.

Type 2

The general type 2 vertex has

- 3, weight 3, isogenies with an image curve of type 1;
- 3, weight 1, isogenies with an image curve of type 4;
- 1, weight 1, isogeny with an image curve of type Π.

The type Π vertex here is special, enough so that the authors define it a special subtype: Φ. Here $\Phi = \mathcal{E} \times \mathcal{E}'$ where $\exists$ a 3-isogeny from $\mathcal{E}$ to $\mathcal{E}'$.

Type 3

The general type 3 vertex has

- 1, weight 4, isogeny with an image curve of type 0;
- 4, weight 2, isogenies with an image curve of type 1;
- 2, weight 1, isogenies with an image curve of type Σ;
- 1, weight 1, isogeny with an image curve identical to the domain curve (self-loop).

Type 4

The type 4 vertex has

- 1, weight 6, isogeny with an image curve of type 1;
- 1, weight 2, isogeny with an image curve of type 2;
- 1, weight 3, isogeny with an image curve of type Σ;
- 1, weight 1, isogeny with an image curve of type Σ_0;
- 1, weight 3, isogeny with an image curve identical to the domain curve (self-loop).

Type 5

The type 5 vertex has

- 2, weight 4, isogenies with an image curve of type 2;
- 1, weight 6, isogeny with an image curve of type $\Sigma\Phi$;
- 1, weight 1, isogeny with an image curve identical to the domain curve (self-loop).

Here $\Sigma\Phi$ denotes a special type Σ vertex. When $\Sigma = \mathcal{E}^2$, we have a degree 3 endomorphism for $\mathcal{E}$.

Type 6

The type 6 vertex has

- 3, weight 5, isogenies with an image curve of type 0.

Type Π

The general type Π vertex has

- 6, weight 1, isogenies with an image curve of type 1;
- 9, weight 1, isogenies with an image curve of type Π.

Type Π_0

The general type Π_0 vertex has

- 2, weight 3, isogenies with an image curve of type 1;
- 3, weight 3, isogenies with an image curve of type Π.

Type Π_{1728}

The general type Π_{1728} vertex has

- 3, weight 2, isogenies with an image curve of type 1;
- 3, weight 2, isogenies with an image curve of type Π;
- 3, weight 1, isogenies with an image curve of type Π_{1728}.

Type Σ

The general type Σ vertex has

- 1, weight 2, isogeny with an image curve of type 1;
- 3, weight 1, isogenies with an image curve of type 3;
- 3, weight 2, isogenies with an image curve of type Π;
- 3, weight 1, isogenies with an image curve of type Σ;
- 1, weight 1, isogeny with an image curve identical to the domain curve (self-loop).

Type $\Pi_{0,1728}$

The type $\Pi_{0,1728}$ vertex has

- 1, weight 6, isogeny with an image curve of type 1;
- 1, weight 6, isogeny with an image curve of type Π;
- 1, weight 3, isogeny with an image curve of type Π_{1728}.

Type Σ_0

The type Σ_0 vertex has

- 1, weight 3, isogeny with an image curve of type 4;
- 1, weight 9, isogeny with an image curve of type Σ;
- 1, weight 3, isogeny with an image curve identical to the domain curve (self-loop).

Type Σ_{1728}

The type Σ_{1728} vertex has

- 1, weight 4, isogeny with an image curve of type 3;
- 1, weight 4, isogeny with an image curve of type Σ;
- 1, weight 4, isogeny, with an image curve of type Π_{1728};
- 1, weight 1, isogeny with an image curve identical to the domain curve (self-loop);
- 1, weight 2, isogeny with an image curve identical to the domain curve (self-loop).

We note here that the first self-loop and the second self-loop have different kernels under automorphism.

Chapter 5

Computing Isogeny Graphs

Let $k = \bar{\mathbb{F}}_p$ be a field s.t. $p \neq 2, 3$. Let H be a superspecial hyperelliptic curve of genus 2 of the form $y^2 = f(x)$, for $f(x) \in k[x]$. Finally, let $\Gamma_2^{\mathrm{SS}}(2, p)$ be the genus 2 superspecial $(2, 2)$-isogeny graph over k.

Definition 5.1. *A Richelot Isogeny is a (2,2) isogeny from a superspecial hyperelliptic curve of genus 2 to another such curve or to a product of supersingular elliptic curves.*

In this section we lay the groundwork for calculating Richelot Isogenies and describe the code the author created for generating local neighborhoods of $\Gamma_2^{\mathrm{SS}}(2, p)$.

Definition 5.2. *Let $f(x) \in k[x]$ be of degree 6 and of the form:*

$$(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)(x - \alpha_5)(x - \alpha_6),$$

for distinct $\alpha_i \in \bar{\mathbb{F}}_p$. Consider the set of quadratic equations (where each β_i is one of the α_j),

$$\{(x - \beta_1)(x - \beta_2), (x - \beta_3)(x - \beta_4), (x - \beta_5)(x - \beta_6)\}.$$

We call this set a quadratic splitting of $f(x)$.

We now define the vector space $k[x]_2$ to be space of polynomials of degree at most 2 over x in the field k. This defines a representative of a quadratic splitting as living in $k[x]_2^3$. We endow our vector space with a Lie Algebra structure by defining the Lie Bracket:

$$[f, g] = \frac{df}{dx} \cdot g - \frac{dg}{dx} \cdot f.$$

We also define a map that recovers f from its quadratic splitting:

$$\Pi : k[x]_2^3 \to k[x],$$

$$G = (G_1, G_2, G_3) \mapsto G_1 G_2 G_3.$$

Consider $G = (G_1, G_2, G_3) = (g_{11}x^2 + g_{12}x + g_{13}, g_{21}x^2 + g_{22}x + g_{23}, g_{31}x^2 + g_{32}x + g_{33})$, and the matrix

$$\mathcal{G} := \begin{bmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{bmatrix}.$$

We define a determinant map,

$$\mathrm{Det} : \mathrm{k[x]}_2^3 \to \mathrm{k},$$

$$G \to \det(\mathcal{G}) := \delta.$$

Theorem 5.3. *Quadratic splittings are in a one-to-one correspondence with subgroups of* $\mathrm{Jac(H)}[2]$, *isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *(see [15]).*

$$\{(x - \alpha_1)(x - \alpha_2), (x - \alpha_3)(x - \alpha_4), (x - \alpha_5)(x - \alpha_6)\}$$

$$\Leftrightarrow$$

$$\langle((\alpha_1, 0), (\alpha_2, 0)), ((\alpha_3, 0), (\alpha_4, 0)), ((\alpha_5, 0), (\alpha_6, 0))\rangle.$$

Definition 5.4. *We call a quadratic splitting G, singular if* $\mathrm{Det(G)} = 0$ *and nonsingular otherwise.*

Lemma 5.5. *If a quadratic splitting is nonsingular, taking the quotient of* $\mathrm{Jac(H)}$ *by the corresponding subgroup of* $\mathrm{Jac(H)}[2]$ *results in the Jacobian of another superspecial hyperelliptic curve. If not, the result is a product of two supersingular elliptic curves (see [15].)*

5.1 The Non-Singular Case

Assume $\delta \neq 0$. We define the Richelot Operator as follows, recalling that '[]' is our Lie Bracket:

$$\mathcal{R} : \{G \in k[x]_2^3 : Det(G) \neq 0\} \to k[x]_2^3,$$

$$(G_1, G_2, G_3) \mapsto (\delta^{-1}[G_2, G_3], \delta^{-1}[G_3, G_1], \delta^{-1}[G_1, G_2]).$$

The Richelot Operator defines a well-defined involution on the set of non-singular quadratic splittings according to Smith [15]. We can construct a new degree 6 polynomial by calculating

$$A = \Pi(\mathcal{R}(G)),$$

and a new superspecial hyperelliptic curve

$$H_2 : y^2 = A(x).$$

Smith [15] shows a well-defined homomorphism (isogeny) exists between H and H_2 and hence that this curve is the image of the Richelot Isogeny.

On Dependent Representatives

We now discuss a problem that can occur when calculating isogenies between Jacobians of Hyperelliptic Curves.

Definition 5.6. *Let $H \in [H]$, and $\phi : \mathrm{Jac(H)} \to \mathrm{Jac(H_2)}$ be a degree 2 isogeny s.t. $\delta_\phi \neq 0$. Let $\alpha : H \to H'$ for $H' \in [H]$ s.t. $H \neq H'$. If $\delta_{\phi\alpha} = 0$, we call H' a dependent representative of $[H]$.*

Dependent representatives can occur in two cases:

- Multiplicative case:

  $$\alpha_1\alpha_2 = \alpha_3\alpha_4 = \alpha_5\alpha_6$$

  for some selection of roots in f.

- Additive case:

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \alpha_5 + \alpha_6$$

  for some selection of roots in f.

In either of these cases, one of the other columns of our matrix becomes a multiple of the first. This makes calculation of the isogeny impossible, as $\delta = 0$, yet we must divide by this value. As this is a representative of the isomorphism class, the solution is to find a different representative that is not dependant.

In the multiplicative case this is a relatively simple fix. Apply the LFT

$$\phi(z) = z + 1.$$

The only way the problem can persist is if we have a multiple root. This is impossible by definition of our curves. For the additive case, there is no simple fix, but probabilistically, the LFT

$$\phi(z) = \frac{z - m}{z - n}$$

for $m, n \in \mathbb{F}_{p^2}$, $m > n$ and n not a root of f - should produce a better representative within only a few different choices of m, n.

5.2 The Singular Case

We now examine the case where $\mathrm{Det}(\mathrm{G}) = 0$. In this case, the image of the associated isogeny will be a product of two supersingular elliptic curves. This only occurs when G_1, G_2, G_3 are k-linearly dependent. Cassels and Flynn [9] indicate that if this is the case, H is equivalant to a curve of the form

$$y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0$$

and that there exist maps to the elliptic curves

$$E_1 : y^2 = c_3z^3 + c_2z^2 + c_1z + c_0,$$

$$E_2 : v^2 = c_0u^3 + c_1u^2 + c_2u + c_3.$$

Here, $z = x^2, u = z^{-1}, v = yx^{-3}$. These maps extend to the Jacobian, and $E_1 \times E_2$ is isomorphic to the image of the associated isogeny.

Smith [15] outlines a procedure for calculating these curves explicitly. We present this as a constructive proof.

Theorem 5.7. *There exist $s_1, s_2 \in \mathbb{F}_{p^2}$, $s_1 \neq s_2$ so that*

$$G_i = a_{i1}(x - s_1)^2 + a_{i2}(x - s_2)^2$$

where the $a_{ij} \in \mathbb{F}_{p^2}$ completely determine the coefficients of the elliptic curves that form the image of our isogeny. [14]

Proof. First we note that since $G_1, G_2 \in k[x]_2$ they can be written as a linear combination of

$$x_1 = (x - s_1), \qquad x_2 = (x - s_2)$$

as follows, (providing x_1, x_2 exist):

$$G_1 = a_{11}x_1^2 + a_{12}x_2^2,$$

$$G_2 = a_{21}x_1^2 + a_{22}x_2^2,$$

for some $s_1, s_2, a_{11}, a_{12}, a_{21}, a_{22} \in k$. x_1, x_2 can be calculated using the discriminant of the polynomial:

$$g_\alpha = G_1 + \alpha G_2.$$

This must be quadratic in α and hence has two distinct roots α_1, α_2. Up to units, it can be shown that these values satisfy

$$x_1^2 = G_1 + \alpha_1 G_2,$$

$$x_2^2 = G_1 + \alpha_2 G_2.$$

As G_3 is linearly dependent on G_1, G_2 it too can be written as a linear combination of x_1^2, x_2^2 :

$$G_3 = a_{31} x_1^2 + a_{32} x_2^2.$$

With this, we can solve for all the a_{ij}, and it can be shown that E_1, E_2 can be written in the forms:

$$E_1 : y^2 = \prod_{i=1}^{3} (a_{i1} x + a_{i2}),$$

$$E_2 : y^2 = \prod_{i=1}^{3} (a_{i1} + a_{i2} x).$$

□

Thus, these formulas (and the isogeny) can be explicitly calculated by taking the discriminant of g_α, solving for α_1, α_2, using this to calculate x_1^2, x_2^2 and (s_1, s_2), then finally comparing the new system of equations to the original G_1, G_2, G_3 to find the a_{ij} and plug them into the E_i formulas.

5.3 Discussion of Code

At this point, we are able to discuss the code constructed in SageMath by the author. This code will become available on github in May, 2024. This code was run in CoCalc, on SageMath version 9.8 within a Ubuntu 20.04 environment. At the time of writing this paper, the code was in version 1.5.

Overview

General calculation within the author's code is dependent on attaching/loading five '.sage' files. In brief, they are as follows.

- 'LGGClass.sage' This file defines classes to represent our vertices: one for Elliptic product vertices and one for Hyperelliptic Jacobian vertices. It also maintains data in dictionaries and arrays about vertices in the graph for easy recall.
- 'LGGIsog.sage' This file handles the calculation of isogenies between vertices. Using the methodologies discussed in the previous sections, it can construct Richelot Isogenies. It is also able to construct isogenies between elliptic curves, or from a product of elliptic curves to a Jacobian of Hyperelliptic curves. It also maintains code to determine the value of δ from the previous section.
- 'LGGUtilNew.sage' This file contains a variety of functions relevant to the project as whole.
- 'VTools.sage' This file contains a variety of functions that the author considers useful in a broader context.
- 'LGGDataGen.sage' This files contains a variety of functions that allow us to calculate data on the local neighborhood graphs we produce.

The remaining files in the project are used for direct calculation in the form of '.sagews' files.

- 'LGGScript.sagews' This file constructs and saves local neighborhood graphs to a file.
- 'LGGDataCollector.sagews' This file runs data collection tools on saved local neighborhood graphs, then saves the data for processing to file and if requested generates visualizations of the network graphs themselves.
- 'LGGMultiOutput.sagews' and 'LGGDataCollectorMulti.sagews' do the same as above but process many neighborhoods in series.

- 'Type 6 Neighborhood.sagews' This file provides a walkthrough for the proof of the crab graph in Chapter 6 and the number of four cycles through the type 6 vertex.
- 'Type Sigma 1728 Neighborhood.sagews' This file provides a walkthrough for the proof of the nautilus graph in Chapter 6 and the number of four cycles through the type Σ_{1728} vertex.
- 'Type Pi 0 1728 Neighborhood.sagews' This file provides a walkthrough for the proof of the turtle graph in Chapter 6 and the number of four cycles through the type $\Pi_{0,1728}$ vertex.

Constructing Neighborhoods

The first stage of our algorithm begins by constructing local neighborhood graphs. The 'LGGScript' file or equivalent loads the necessary .sage files and packages and then the user inputs the starting curve, prime, and parameters used for limiting program run time.

The algorithm takes the starting curve, builds a class object for it from the 'LGGClass' file and detects nearby neighbors by calculating every possible 2-isogeny and image thereof. It also calculates the curve's invariants for easier storage, and the corresponding automorphism group to then calculate its type. The neighbors are added to an array for processing, and each one has the same process applied to it - adding their neighbors to the same list. This process continues until there are no more vertices in the graph or an arbitrary limit is hit (maximum number, distance away from the starting vertex, etc.)

Every isogeny is calculated by calling upon the 'LGGIsog' file and the appropriate method for the domain and image of the isogeny.

At the end of the process, the data on the neighborhoods is saved to a file using python's 'pickle' package.

Forming Data

We can take our saved neighborhoods, 'unpickle' them, and process data from them. This process is primarily carried out in the 'LGGDataCollection' file or equivalent.

There are a number of things our code can do:

- Split data based on characteristic, so that we can analyze specific things like spinal vertices, or a specific type of vertices.
- Calculate various types of graph theoretic matrices.
- Calculate connectivity of subgraphs.
- Calculate four cycles in the graph.
- Generate a visualization of the neighborhood

Some of these tasks are worth breaking down. Most of the functions run to accomplish these tasks are found in 'LGGDataGen'.

One of the most important tools for splitting data is 'splitSetToolSpinality' which separates spinal and non-spinal vertices into two sets. We could also split our dataset into sets based on how far they are from the starting vertex using 'splitSetToolLayer'.

We can calculate the adjacency matrix, diagonal matrix, and Laplace matrix for a given graph using 'calculateAdjacencyMatrices'. It is simple from here to calculate the connectivity of the data using 'spineComponents' on the Laplace matrix. There is a theorem in graph theory, that the number of components of a network graph is equal to the rank of the kernel of its Laplace matrix. This method calculates and returns the rank. If the number of components is anything other than 1, it isn't connected.

Calculating the number of four-cycles through the starting vertex is more complicated and is addressed at the end of this section.

We generate visualizations of neighborhoods using 'plotNbhd', a method using network graph tools from python's 'networkx' package. By default, the graphs made by this method use the 'circular layout'. But 'kamada kawai' can be called by including the parameter layout = 1 and 'spring layout' by layout = 2. Most of our example graphs are created using spring layout. Networkx is not good at double edges or weights, so those are not included in our visualizations.

Proving Theorems

The files used for proving the theorems in Chapter 6 are formatted as 'Type ___ Neighborhood'. These files attempt to construct the complete radius 2 neighborhood of a vertex in the graph over quadratic extensions of $\mathbb{Q}$. These will walk you through the steps taken to construct the graph, clarifying the proofs in Chapter 6 of this paper. Running the cells in the sage worksheets in order accomplishes this.

The process goes as follows. We construct the starting vertex. Determine if any isogenies require a field extension. If they do, we extend our field to include that. We calculate all isogenies and their images, picking up the outgoing weights along the way. We calculate the invariants and automorphism group of the images and from that get their types. We repeat this process for each of the new vertices at a distance of one away from the starting vertex. Because we calculate invariants, we are able to determine if any vertices have common neighbors. Because we calculate the automorphism group we are able to calculate all reverse edge weights in the graph using Theorem 3.4. This is enough to calculate all relevant details to the proofs.

Algorithm for Detecting 4-Cycles in the Code

Here is the methodology for identifying 4-cycles in the graph in our code.

'fourCyclesData' is called on the vertices and their adjacency matrix. This method does the following:

1. Call the adjacency matrix 'A', find its shape (n, n).

2. Build a new matrix 'P' with shape $(n, (n-1)(n-2)/2)$ where each column contains 0 in every row except two of them, which contain a 1. (The 1 cannot be in the 0th row). There is a column in the matrix for each distinct way to do this.

3. Calculate $B := A \cdot P$. It will have shape $(n, (n-1)(n-2)/2)$.

4. For each column in B, check if the the entry in the zeroth row is 2. If it is, check if any other position in the column has a 2. Record each such column. This can be translated into the number of unweighted-undirected cycles

5. Use edge weights on this data to count the number of weighted-directed cycles.

Proposition 5.8. *There is a 4-cycle between the nodes $0, m, z, n$ if and only if the column of B representing the edge between m and n contains a 2 in the 0'th and z'th rows.*

An Example

A four-cycle in an adjacency matrix appears as a rectangle with 1's in the corner, for example:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Here we see a four cycle is present on vertices 0,1,3 and 4. The associated 'P' matrix looks like this:

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

If we take the product of these two matrices we get

$$B = \begin{bmatrix} 1 & 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 2 & 1 & 2 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The only column that has more than a single 2 is the result of multiplying by the input column $[0, 1, 0, 0, 1]$ and getting the image column $[2, 0, 0, 2, 0]$. We can decode this to get that a 4-cycle through the 0 vertex includes the 1 vertex and 4 vertex as direct neighbors (the position of the 1's in the initial vector are 1 and 4.) and the 3 vertex opposite it in the cycle (the position of the 2's in the final vector are 0 and 3.) Every such cycle we record adds to the count of unweighted-undirected 4-cycles. From here, we can use edge weight data to uncover the exact weighted-directed number of 4-cycles.

Closing Thoughts

A four cycle going through the 0 vertex, a.k.a the starting vertex, must have two neighbors in that cycle. If we multiply the adjacency matrix by the vector that contains a 1 in each of those places but 0's everywhere else, the 0 position will return a 2 as the 0 vertex has 2 neighbors in that vector. But if another 2 appears in the image, that means that there is another vertex that both of those vertices are adjacent to. Therefore, these four vertices must form a 4-cycle. Note that because we want the two vertices that are adjacent to the starting vertex to be something other than the starting vertex, we construct P to have 0's in the first row. Every other combination of two vertices has its own representative column in the P matrix. The number of ways to form such representatives is $(n-1)(n-2)/2$, hence the P matrix's width.

Chapter 6

Results

Follows from Prior Results

The following results can be easily constructed from the work of Florit and Smith [2].

Type 0

The type 0 family is a 3-dimensional space. Each curve, H, has $\mathrm{RA(H)} \cong 1$.

Florit and Smith [2] determined how many unweighted-undirected 4-cycles there should be through a general type 0 vertex. This can easily be extended to the following result.

Lemma 6.1. *A type 0 vertex in the graph has 180 unweighted-undirected cycles or 360 weighted-directed* 4*-cycles. All of these* 4*-cycles are of type* $(0, 0, 0, 0)$.

Type 1

The type 1 family is a 2-dimensional space. Each curve, H, has $\mathrm{RA(H)} \cong \mathbb{Z}/2\mathbb{Z}$.

One can extrapolate the following lemma from the general neighborhood of the type 1 vertex in the atlas.

Lemma 6.2. *A type 1 vertex in the graph has, in total, 12 unweighted-undirected* 4*-cycles or 24 weighted-directed* 4*-cycles.*

There are 6 unweighted-undirected 4*-cycles (12 weighted-directed* 4*-cycles) of type* $(1, 1, \Pi, 1)$.

There are 6 unweighted-undirected 4*-cycles (12 weighted-directed* 4*-cycles) of type* $(1, 1, 1, 1)$.

Type 2

The type 2 family is a 1-dimensional space. Each curve, H, has $\mathrm{RA(H)} \cong \mathrm{S}_3$.

One can extrapolate the following lemma from the general neighborhood of the type 2 vertex in the atlas.

Lemma 6.3. *A type 2 vertex in the graph has, in total, 12 unweighted-undirected* 4*-cycles, or 72 weighted-directed* 4*-cycles.*

There are 3 unweighted-undirected 4*-cycles (18 weighted-directed* 4*-cycles) of type* $(2, 1, 1, \Phi)$.

There are 3 unweighted-undirected 4*-cycles (18 weighted-directed* 4*-cycles) of type* $(2, 1, \Phi, \Phi)$.

There are 3 unweighted-undirected 4*-cycles (18 weighted-directed* 4*-cycles) of type* $(2, 2, 1, \Phi)$.

There are 3 unweighted-undirected 4*-cycles (18 weighted-directed* 4*-cycles) of type* $(2, 2, \Phi, \Phi)$.

Type 3

The type 3 family is a 1-dimensional space. Each curve, H, has $\mathrm{RA(H)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

One can extrapolate the following lemma from the general neighborhood of the type 3 vertex in the atlas.

Lemma 6.4. *A type 3 vertex in the graph has, in total, 6 unweighted-undirected* 4*-cycles, or 24 weighted-directed* 4*-cycles.*

There are 2 unweighted-undirected 4*-cycles (8 weighted-directed* 4*-cycles) of type* $(3, 1, \Pi, 1)$.

There are 4 unweighted-undirected 4*-cycles (16 weighted-directed* 4*-cycles) of type* $(3, 1, \Pi, \Sigma)$.

Type 4

The type 4 family is a 0-dimensional space, and therefore a single curve, $H : y^2 = x^6 - 1$. We note that $\mathrm{RA(H)} \cong \mathrm{D}_{12}$ and that it is superspecial iff $p \equiv 5 \mod (6)$.

One can extrapolate the following lemma from the neighborhood of the type 4 vertex in the atlas.

Lemma 6.5. *The type 4 vertex in the graph has, in total, 6 unweighted-undirected* 4*-cycles, or 72 weighted-directed* 4*-cycles.*

There is 1 unweighted-undirected 4*-cycle (12 weighted-directed* 4*-cycles) of type* $(4, 1, \Phi, 2)$.

There is 1 unweighted-undirected 4*-cycle (12 weighted-directed* 4*-cycles) of type* $(4, 1, 1, 2)$.

There is 1 unweighted-undirected 4*-cycle (15 weighted-directed* 4*-cycles) of type* $(4, 1, 1, \Sigma)$.

There is 1 unweighted-undirected 4*-cycle (12 weighted-directed* 4*-cycles) of type* $(4, 1, \Phi, \Sigma)$.

There is 1 unweighted-undirected 4*-cycle (9 weighted-directed* 4*-cycles) of type* $(4, 2, 1, \Sigma)$.

There is 1 unweighted-undirected 4*-cycle (12 weighted-directed* 4*-cycles) of type* $(4, 2, \Phi, \Sigma)$.

Type 5

The type 5 family is a 0-dimensional space, and therefore a single curve, $H : y^2 = x^5 - x$. Assume $p \neq 5$. We note that $\mathrm{RA(H)} \cong \mathrm{S}_4$ and that it is superspecial iff $p \equiv 5, 7 \mod (8)$.

One can extrapolate the following lemma from the neighborhood of the type 5 vertex in the atlas.

Lemma 6.6. *Let* $p \neq 5$*. The type 5 vertex in the graph has, in total, 6 unweighted-undirected* 4*-cycles, or 144 weighted-directed* 4*-cycles.*

There are 2 unweighted-undirected 4*-cycles (48 weighted-directed* 4*-cycles) of type* $(5, 2, \Phi, \Sigma\Phi)$.

There is 1 unweighted-undirected 4*-cycle (24 weighted-directed* 4*-cycles) of type* $(5, 2, \Phi, 2)$.

There are 2 unweighted-undirected 4*-cycles (48 weighted-directed* 4*-cycles) of type* $(5, 2, 1, \Sigma\Phi)$.

There is 1 unweighted-undirected 4*-cycle (24 weighted-directed* 4*-cycles) of type* $(5, 2, 1, 2)$.

Type Π

The type Π family is a 2-dimensional space constructed from a product of two unique elliptic curves, both with $j \neq 0, 1728$. Each surface, $E_1 \times E_2$, has $\mathrm{RA}(\mathrm{E}_1 \times \mathrm{E}_2) \cong \mathbb{Z}/2\mathbb{Z}$.

One can extrapolate the following lemma from the general neighborhood of the type Π vertex in the atlas.

Lemma 6.7. *A type* Π *vertex in the graph has, in total, 12 unweighted-undirected* 4*-cycles, or 24 weighted-directed* 4*-cycles.*

There are 6 unweighted-undirected 4*-cycles (12 weighted-directed* 4*-cycles) of type* $(\Pi, \Pi, 1, 1)$.

There are 6 unweighted-undirected 4*-cycles (12 weighted-directed* 4*-cycles) of type* $(\Pi, 1, 1, 1)$.

Type Σ

The type Σ family is a 1-dimensional space constructed from a product of two identical elliptic curves with $j \neq 0, 1728$. Each surface, E^2, has $\mathrm{RA}(\mathrm{E}^2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

One can extrapolate the following lemma from the general neighborhood of the type Σ vertex in the atlas.

Lemma 6.8. *A type Σ vertex in the graph has 6 unweighted-undirected 4-cycles or 24 weighted-directed 4-cycles. All of these 4-cycles are of type $(\Sigma, 3, 1, \Pi)$.*

Type Σ_0

The type Σ_0 family is a 0-dimensional space, and therefore a single surface E_0^2 given by the product of two copies of the elliptic curve with $j = 0$. We note that $\mathrm{RA}(\mathbb{Z}/6\mathbb{Z} \times \mathrm{S}_3)$.

One can extrapolate the following lemma from the neighborhood of the type Σ_0 vertex in the atlas.

Lemma 6.9. *The type Σ_0 vertex in the graph does not contain 4-cycles.*

Constructive Proofs

Type 6

Florit and Smith [2] do not provide enough information for type 6 to extrapolate how many 4-cycles there must be within the neighborhood passing through the type 6 vertex. We have expanded upon their result.

Theorem 6.10. *Consider the type 6 curve $H : y^2 = x^5 - 1$ and let $p \equiv 4 \mod (5)$. Then through $[H]$ there are in total, 10 unweighted-undirected 4-cycles, or 140 weighted-directed 4-cycles, and $N_2([H])$ is represented by Figure* **??**.

Proof. We first note that $[H]$ has $\mathrm{RA} \cong \mathbb{Z}/5\mathbb{Z}$ and that since $p \equiv 4 \mod (5)$, $[H]$ is superspecial. Further,

$$\left(\frac{5}{p}\right) = 1,$$

so $\sqrt{5}, \phi \in \mathbb{F}_p$ where ϕ is the golden ratio. We also note that since

$$\zeta_5 := \frac{\phi - 1 + \sqrt{-\phi - 2}}{2},$$

we know that $\zeta_5 \in \mathbb{F}_{p^2}$.

Florit and Smith [2] provide the Kernels of the three weight-5 isogenies from our type 6 vertex:

$$K_1 = \{x - 1, (x - \zeta_5)(x - \zeta_5^2), (x - \zeta_5^3)(x - \zeta_5^4)\},$$
$$K_2 = \{x - 1, (x - \zeta_5)(x - \zeta_5^3), (x - \zeta_5^2)(x - \zeta_5^4)\},$$
$$K_3 = \{x - 1, (x - \zeta_5)(x - \zeta_5^4), (x - \zeta_5^2)(x - \zeta_5^3)\}.$$

From here, we can construct the image vertices, $H/K_1, H/K_2, H/K_3$. Their Kohel invariants are (respectively) as follows:

$$(k_1, k_2, k_3) = (\tfrac{-2035611}{4}\sqrt{5} + \tfrac{4598775}{4}, \tfrac{-199559376}{5}\sqrt{5} + \tfrac{439744464}{5}, \tfrac{-257829804}{25}\sqrt{5} + \tfrac{113452812}{5}),$$
$$(k_1, k_2, k_3) = (\tfrac{2035611}{4}\sqrt{5} + \tfrac{4598775}{4}, \tfrac{199559376}{5}\sqrt{5} + \tfrac{439744464}{5}, \tfrac{257829804}{25}\sqrt{5} + \tfrac{113452812}{5}),$$
$$(k_1, k_2, k_3) = (\tfrac{2824875}{2}, 656100000, 203391000)$$

We will refer to the first two as $\bar{A}$ vertices and the last as an $\hat{A}$ vertex for reasons that will become clear later. We then calculate all 15-isogenies for each of these three vertices and use Kohel's invariants to determine which vertices share common neighbors, and what our edge weights should be.

We discover that the type $\bar{A}$ vertex has 11 outgoing edges of weight 1 and 2 outgoing edges of weight 2. Also, the type $\hat{A}$ vertex has 15 outgoing edges of weight 1.

Note that one of the weight "1" vertices for each type returns to the Type 6 vertex at the center due to the existence of dual edges.

We observe that two vertices, we will call "σ" vertices, are neighbors to all three of the "A" vertices. They have Kohel invariants

$$(k_1, k_2, k_3) = (56531034\sqrt{5} + 126411030, 13692229632\sqrt{5} + \tfrac{153086920704}{5},$$
$$\tfrac{120920174784}{25}\sqrt{5} + 10815607296),$$
$$(k_1, k_2, k_3) = (-56531034\sqrt{5} + 126411030, -13692229632\sqrt{5} + \tfrac{153086920704}{5},$$
$$\tfrac{-120920174784}{25}\sqrt{5} + 10815607296).$$

The weight of the edges to these vertices is 1. We expect these vertices to be type 0, and indeed, a quick calculation shows that $\mathrm{RA}(\sigma) = 1$ forcing them to be type 0. Further, by Theorem 3.4, the weight of the edges from these vertices back to the $\bar{A}$ and $\hat{A}$ vertices must also be 1.

We also observe a further 4 vertices. Two of these vertices are neighbors to one of the $\bar{A}$ vertices and the other two are neighbors to the other $\bar{A}$ vertex. All four are neighbors to the $\hat{A}$ vertex. The first and last pair of invariants below are both associated with the same $\bar{A}$ vertex. We will call these κ vertices.

We note that $a_1 := \frac{-\phi+\sqrt{\phi-3}}{2}$ is a solution to the equation $x^2+\phi x+1$ where ϕ is the golden ratio, $a_2 := \frac{-(\sqrt{5}+3)+\sqrt{10+6\sqrt{5})}}{2}$ is a solution to the equation $x^2 + (\sqrt{5}+3)x + 1$, and $a_3 := 1 + i\sqrt{\sqrt{5}a_1}$ is a solution to the equation $x^2 - 2x + (\sqrt{5}a_1 + 1)$.

We now list out the invariants for all the type κ vertices.

First Vertex:

$k_1 = (((-\frac{227571687}{2}\sqrt{5} + \frac{508770801}{2})a_1 - 43486065\sqrt{5} + 97113492)a_2 + (-43486065\sqrt{5} + 97113492)a_1 - \frac{33344703}{2}\sqrt{5} + \frac{73910151}{2})a_3 + ((\frac{227571687}{2}\sqrt{5} - \frac{508770801}{2})a_1 + 43486065\sqrt{5} - 97113492)a_2 + (43486065\sqrt{5} - 97113492)a_1 + \frac{403167375}{2}\sqrt{5} - \frac{900212211}{2},$

$k_2 = (((\frac{321021646848}{25}\sqrt{5} - \frac{143574415488}{5})a_1 + \frac{122596431552}{25}\sqrt{5} - \frac{54850799808}{5})a_2 + (\frac{122596431552}{25}\sqrt{5} - \frac{54850799808}{5})a_1 + \frac{46767647808}{25}\sqrt{5} - \frac{20977983936}{5})a_3 + ((\frac{-321021646848}{25}\sqrt{5} + \frac{143574415488}{5})a_1 - \frac{122596431552}{25}\sqrt{5} + \frac{54850799808}{5})a_2 + (-\frac{122596431552}{25}\sqrt{5} + \frac{54850799808}{5})a_1 - \frac{568120454208}{25}\sqrt{5} + 50861711808,$

$k_3 = (((\frac{138527711784}{25}\sqrt{5} - \frac{309785943096}{25})a_1 + \frac{52898596128}{25}\sqrt{5} - \frac{118359635184}{25})a_2 + (\frac{52898596128}{25}\sqrt{5} - \frac{118359635184}{25})a_1 + 806723064\sqrt{5} - \frac{45292962456}{25})a_3 + ((-\frac{138527711784}{25}\sqrt{5} + \frac{309785943096}{25})a_1 - \frac{52898596128}{25}\sqrt{5} + \frac{118359635184}{25})a_2 + (-\frac{52898596128}{25}\sqrt{5} + \frac{118359635184}{25})a_1 - \frac{245161807704}{25}\sqrt{5} + \frac{548700821496}{25}$

Second Vertex:

$k_1 = (((\frac{227571687}{2}\sqrt{5} - \frac{508770801}{2})a_1 + 43486065\sqrt{5} - 97113492)a_2 + (43486065\sqrt{5} - 97113492)a_1 + \frac{33344703}{2}\sqrt{5} - \frac{73910151}{2})a_3 + ((-\frac{227571687}{2}\sqrt{5} + \frac{508770801}{2})a_1 - 43486065\sqrt{5} + 97113492)a_2 + (-43486065\sqrt{5} + 97113492)a_1 + \frac{336477969}{2}\sqrt{5} - \frac{752391909}{2}$,

$k_2 = (((-\frac{321021646848}{25}\sqrt{5} + \frac{143574415488}{5})a_1 - \frac{122596431552}{25}\sqrt{5} + \frac{54850799808}{5})a_2 + (-\frac{122596431552}{25}\sqrt{5} + \frac{54850799808}{5})a_1 - \frac{46767647808}{25}\sqrt{5} + \frac{20977983936}{5})a_3 + ((\frac{321021646848}{25}\sqrt{5} - \frac{143574415488}{5})a_1 + \frac{122596431552}{25}\sqrt{5} - \frac{54850799808}{5})a_2 + (\frac{122596431552}{25}\sqrt{5} - \frac{54850799808}{5})a_1 - \frac{474585158592}{25}\sqrt{5} + \frac{212352591168}{5}$,

$k_3 = (((-\frac{138527711784}{25}\sqrt{5} + \frac{309785943096}{25})a_1 - \frac{52898596128}{25}\sqrt{5} + \frac{118359635184}{25})a_2 + (-\frac{52898596128}{25}\sqrt{5} + \frac{118359635184}{25})a_1 - 806723064\sqrt{5} + \frac{45292962456}{25})a_3 + ((\frac{138527711784}{25}\sqrt{5} - \frac{309785943096}{25})a_1 + \frac{52898596128}{25}\sqrt{5} - \frac{118359635184}{25})a_2 + (\frac{52898596128}{25}\sqrt{5} - \frac{118359635184}{25})a_1 - \frac{204825654504}{25}\sqrt{5} + \frac{458114896584}{25}$

Third Vertex:

$k_1 = (((-\frac{53627427}{2}\sqrt{5} - \frac{120316833}{2})a_1 - \frac{140599557}{2}\sqrt{5} - \frac{314543817}{2})a_2 + (-\frac{140599557}{2}\sqrt{5} - \frac{314543817}{2})a_1 - 184085622\sqrt{5} - 411657309)a_3 + ((\frac{53627427}{2}\sqrt{5} + \frac{120316833}{2})a_1 + \frac{140599557}{2}\sqrt{5} + \frac{314543817}{2})a_2 + (\frac{140599557}{2}\sqrt{5} + \frac{314543817}{2})a_1 - 825714\sqrt{5} - 1493721$,

$k_2 = (((\frac{75828783744}{25}\sqrt{5} + \frac{33872815872}{5})a_1 + \frac{198425215296}{25}\sqrt{5} + 17744723136)a_2 + (\frac{198425215296}{25}\sqrt{5} + 17744723136)a_1 + \frac{519446862144}{25}\sqrt{5} + \frac{232298031168}{5})a_3 + ((-\frac{75828783744}{25}\sqrt{5} - \frac{33872815872}{5})a_1 - \frac{198425215296}{25}\sqrt{5} - 17744723136)a_2 + (-\frac{198425215296}{25}\sqrt{5} - 17744723136)a_1 + \frac{1905944256}{25}\sqrt{5} + \frac{1032543936}{5}$,

$k_3 = (((\frac{32730519528}{25}\sqrt{5} + \frac{73066672728}{25})a_1 + \frac{85629115656}{25}\sqrt{5} + \frac{191426307912}{25})a_2 + (\frac{85629115656}{25}\sqrt{5} + \frac{191426307912}{25})a_1 + \frac{44831365488}{5}\sqrt{5} + \frac{501212251008}{25})a_3 + ((-\frac{32730519528}{25}\sqrt{5} - \frac{73066672728}{25})a_1 - \frac{85629115656}{25}\sqrt{5} - \frac{191426307912}{25})a_2 + (-\frac{85629115656}{25}\sqrt{5} - \frac{191426307912}{25})a_1 + \frac{836903664}{25}\sqrt{5} + \frac{2195608032}{25}$

Fourth Vertex:

$k_1 = (((\frac{53627427}{2}\sqrt{5} + \frac{120316833}{2})a_1 + \frac{140599557}{2}\sqrt{5} + \frac{314543817}{2})a_2 + (\frac{140599557}{2}\sqrt{5} + \frac{314543817}{2})a_1 + 184085622\sqrt{5} + 411657309)a_3 + ((-\frac{53627427}{2}\sqrt{5} - \frac{120316833}{2})a_1 - \frac{140599557}{2}\sqrt{5} - \frac{314543817}{2})a_2 + (-\frac{140599557}{2}\sqrt{5} - \frac{314543817}{2})a_1 - 368996958\sqrt{5} - 824808339$,

$k_2 = (((-\frac{75828783744}{25}\sqrt{5} - \frac{33872815872}{5})a_1 - \frac{198425215296}{25}\sqrt{5} - 17744723136)a_2 + (-\frac{198425215296}{25}\sqrt{5} - 17744723136)a_1 - \frac{519446862144}{25}\sqrt{5} - \frac{232298031168}{5})a_3 + ((\frac{75828783744}{25}\sqrt{5} + \frac{33872815872}{5})a_1 + \frac{198425215296}{25}\sqrt{5} + 17744723136)a_2 + (\frac{198425215296}{25}\sqrt{5} + 17744723136)a_1 + \frac{1040799668544}{25}\sqrt{5} + \frac{465628606272}{5}$,

$k_3 = (((-\frac{32730519528}{25}\sqrt{5} - \frac{73066672728}{25})a_1 - \frac{85629115656}{25}\sqrt{5} - \frac{191426307912}{25})a_2 + (-\frac{85629115656}{25}\sqrt{5} - \frac{191426307912}{25})a_1 - \frac{44831365488}{5}\sqrt{5} - \frac{501212251008}{25})a_3 + ((\frac{32730519528}{25}\sqrt{5} + \frac{73066672728}{25})a_1 + \frac{85629115656}{25}\sqrt{5} + \frac{191426307912}{25})a_2 + (\frac{85629115656}{25}\sqrt{5} + \frac{191426307912}{25})a_1 + \frac{449150558544}{25}\sqrt{5} + \frac{1004620110048}{25}$

These κ vertices are the image of a weight 2 isogeny from one of the $\bar{A}$ vertices, and a weight 1 isogeny from the $\hat{A}$ vertex (hence the difference between the two types of A vertices). Again, we expect the vertices to be type 0, and $\mathrm{RA}(\kappa) = 1$ so this is the case. Again, by Theorem 3.4, the weight of the edge back to $\hat{A}$ is 1 and the weight of the edge back to $\bar{A}$ is 2.

All other isogeny images are unique. Hence, a quick sketch of the graph, makes it clear immediately that there are 10 unweighted-undirected 4-cycles through the type 6 vertex.

Finally, we can list out the cycle types, and calculate their weights:

There are 4 unweighted-undirected 4-cycles (40 weighted-directed 4-cycles) of type $(6, \bar{A}, \sigma, \hat{A})$.

There are 4 unweighted-undirected 4-cycle (80 weighted-directed 4-cycles) of type $(6, \bar{A}, \kappa, \hat{A})$.

There are 2 unweighted-undirected 4-cycles (20 weighted-directed 4-cycles) of type $(6, \bar{A}, \sigma, \bar{A})$.

This leads to a total of 140 weighted-directed cycles, finishing the proof.

□

Finally, due to the new nature of this information, we include a visualization of the neighborhood: the 'crab graph'. Here the red vertex is the type 6 vertex, the two blue vertices are σ vertices, the four purple vertices are κ vertices, the remaining vertices are A vertices with the top two being $\bar{A}$ and the bottom being $\hat{A}$. All edges are weight one except those labeled weight 2 and the edges from the type 6 vertex to the A vertices which are weight 5.

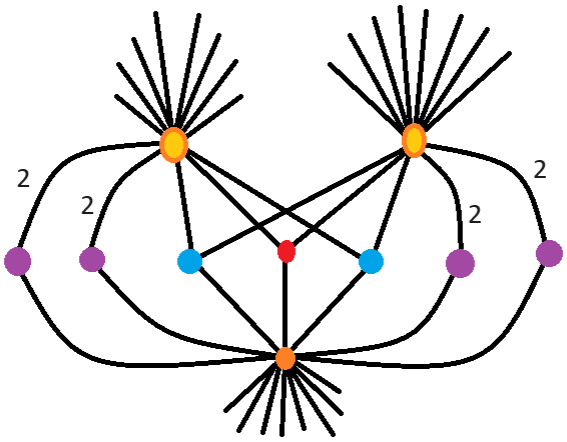

Figure 6.1: The 'Crab' Graph of the Type 6 Curve

Type Σ_{1728}

As was the case for the type 6 vertex, Florit and Smith [2] do not provide enough information for type Σ_{1728} to extrapolate how many 4-cycles there must be within the neighborhood passing through the type Σ_{1728} vertex. We have expanded their result.

Theorem 6.11. *Consider the type* Σ_{1728} *vertex given by a product of two Elliptic curves with* $j = 1728$, *which we will denote* $[E^2]$. *Let* $p \equiv 3 \mod (4)$. *Then through* $[E^2]$ *there are in total, 3 unweighted-undirected 4-cycles, or 48 weighted-directed cycles, and* $N_2([E^2])$ *is represented by Figure* **??**.

Proof. We first note that $[E^2]$ has $\mathrm{RA} \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$. and that since $p \equiv 3 \mod (4)$, $[E]$ is supersingular, and hence $[E^2]$ is in $\Gamma_2^{\mathrm{SS}}(2, p)$.

As a product of two elliptic curves with $j = 1728$, we begin by calculating the images of all 2-isogenies of E. There are two images with $j = 287496$, and one with image $j = 1728$ (a self-loop.)

Hence, the elliptic product neighbors of our Σ_{1728} vertex are as follows:

- a self-loop with invariants: $(1728, 1728)$,
- a type Σ vertex with invariants $(287496, 287496)$,

- a type Π_{1728} vertex with invariants $(1728, 287496)$.

The self-loop has weight one, the edge to the type Σ vertex has weight 4, and the edge to the type Π_{1728} edge has weight 4. By Theorem 3.4, we can also conclude that the dual edge from the type Σ vertex has weight 1 and the dual edge from the type Π_{1728} edge also has weight 1.

We can also calculate all the Hyperelliptic neighbors of our starting vertex. 4 such neighbors are valid curves [3], and they all have the same Kohel invariants:

$$(k_1, k_2, k_3) = (\frac{751}{8}, \frac{778688}{27}, \frac{3178232}{81}),$$

and are therefore the same curve, i.e. the outgoing edge is weight 4. Calculating the reduced automorphism group of this curve yields, K_4. Hence it is a type 3 curve, and by Theorem 3.4 the dual edge has weight 1. We have thus calculated $N_1([E^2])$ and determined that there are 3 radius one neighbors to investigate: the Types Σ, Π_{1728}, and 3 vertices.

We begin by investigating the type 3 vertex. Constructing the quadratic splittings and calculating δ for each, we determine that only two neighbors will be elliptic products. One must then be the dual edge back to Σ_{1728} and the other we calculate to be the $(287496, 287496)$ vertex we found earlier of type Σ. This also forces the dual edge to be weight 1 as well, by Theorem 3.4.
The remaining edges are unimportant beyond checking that they do not have any other vertices at distance 1 from Σ_{1728} in common. For completeness we list them here.

- There is an outgoing edge of weight 2 to the curve with invariants:
  $(k_1, k_2, k_3) = (\frac{277864546323}{234256}\sqrt{-2} - \frac{1437440713439}{468512}, \frac{74992314819190916}{1929229929}\sqrt{-2} - \frac{987617438131435438}{5787689787},$
  $\frac{49062146505649193}{5787689787}\sqrt{-2} - \frac{1432983554086604327}{34726138722})$.

- There is an outgoing edge of weight 2 to the curve with invariants:
  $(k_1, k_2, k_3) = -(\frac{277864546323}{234256}\sqrt{-2} - \frac{1437440713439}{468512}, -\frac{74992314819190916}{1929229929}\sqrt{-2} - \frac{987617438131435438}{5787689787},$
  $-\frac{49062146505649193}{5787689787}\sqrt{-2} - \frac{1432983554086604327}{34726138722})$.

[3] Some authors choose to represent the remaining 2 neighbors as a self-loop of weight 2.

- There is an outgoing edge of weight 1 to the curve with invariants:

  $(k_1, k_2, k_3) = (\frac{751}{8}, \frac{778688}{27}, \frac{3178232}{81})$.

  This is a self-loop.

- There is an outgoing edge of weight 4 to the curve with invariants:

  $(\frac{14774210551}{76832}, \frac{12374781614502014}{155649627}, \frac{27205955244928399}{933897762})$.

- There is an outgoing edge of weight 4 to the curve with invariants:

  $(-17197, -\frac{14848000}{27}, -\frac{7590400}{81})$.

One of these two outgoing weight 4 edges is unexpected and is the merging of 2 weight 2 edges in Florit and Smith's [2] graph for the generic type 3 vertex.

Next we will investigate the other two neighbors of the type Σ_{1728} vertex, $(1728, 287496)$ and $(287496, 287496)$. Starting with elliptic neighbors, we recognize a need to calculate the images of all 2-isognies of $j = 287496$ before proceeding.

One of the neighbors must be $j = 1728$, but the other two are new: $29071392966\sqrt{2} + 41113158120$ and $-29071392966\sqrt{2} + 41113158120$.

Hence the elliptic product neighbors of $(287496, 287496)$ are as follows:

- a type Σ_{1728} vertex with invariants $(1728, 1728)$ which is our dual edge back to the origin,
- a type Π_{1728} vertex with invariants $(1728, 29071392966\sqrt{2} + 41113158120)$,
- a type Π_{1728} vertex with invariants $(1728, -29071392966\sqrt{2} + 41113158120)$,
- a type Σ vertex with invariants

  $(29071392966\sqrt{2} + 41113158120, 29071392966\sqrt{2} + 41113158120)$,

- a type Σ vertex with invariants

  $(-29071392966\sqrt{2} + 41113158120, -29071392966\sqrt{2} + 41113158120)$,

- a type Π vertex with invariants

  $(29071392966\sqrt{2} + 41113158120, -29071392966\sqrt{2} + 41113158120)$.

The outgoing weights are 1,2,2,1,1, and 2 respectively and by Theorem 3.4 the dual weights are 4,2,2,1,1, and 1 respectively.

Similarly, the elliptic product neighbors of $(1728, 287496)$ are as follows:

- a type Σ_{1728} vertex with invariants $(1728, 1728)$ which is our dual edge back to the origin,
- a type Π_{1728} vertex with invariants $(1728, 287496)$ which is a self-loop,
- a type Π_{1728} vertex with invariants $(1728, 29071392966\sqrt{2} + 41113158120)$,
- a type Π_{1728} vertex with invariants $(1728, -29071392966\sqrt{2} + 41113158120)$,
- a type Π vertex with invariants $(287496, 29071392966\sqrt{2} + 41113158120)$,
- a type Π vertex with invariants $(287496, -29071392966\sqrt{2} + 41113158120)$.

The outgoing weights are 1,2,1,1,2, and 2 respectively and by Theorem 3.4 the dual weights are 4,2,1,1,1, and 1 respectively.

We note that the vertices: $(1728, 29071392966\sqrt{2} + 41113158120)$, and $(1728, -29071392966\sqrt{2} + 41113158120)$ are common neighbors to both (1728, 287496) and (287496,287496). We will call these type κ vertices for the remainder of this proof. These vertices will allow us to form the only 4-cycles in the graph, but we still need to calculate the hyperelliptic neighbors of $(1728, 287496)$ and $(287496, 287496)$ to verify this.

First, we list the hyperelliptic neighbors of $(287496, 287496)$.

- There is an outgoing edge of weight 1 to the curve with invariants:
  $(k_1, k_2, k_3) = (\frac{6523884707703}{38416}\sqrt{2} + \frac{36905627140531}{153664}, \frac{1504854025601701280}{51883209}\sqrt{2} + \frac{6384680530861497176}{155649627},$
  $\frac{1693972751480432852}{155649627}\sqrt{2} + \frac{7187037942295351235}{466948881})$.
- There is an outgoing edge of weight 1 to the curve with invariants:
  $(k_1, k_2, k_3) = (-\frac{6523884707703}{38416}\sqrt{2} + \frac{36905627140531}{153664}, -\frac{1504854025601701280}{51883209}\sqrt{2} + \frac{6384680530861497176}{155649627},$
  $-\frac{1693972751480432852}{155649627}\sqrt{2} + \frac{7187037942295351235}{466948881})$.

- There is an outgoing edge of weight 2 to the curve with invariants:

  $(k_1, k_2, k_3) = (-\frac{101155}{64}, -\frac{12888615920536}{47832147}, -\frac{13901603081995}{143496441})$.

- There is an outgoing edge of weight 1 to the curve with invariants:

  $(k_1, k_2, k_3) = (\frac{751}{8}, \frac{778688}{27}, \frac{3178232}{81})$, which is the dual to edge to the one we found from the type 3 edge earlier.

- One of the 6 possible isogenies is invalid. [4]

Now, we list the hyperelliptic neighbors of $(1728, 287496)$.

- There is an outgoing edge of weight to the curve with invariants:

  $(k_1, k_2, k_3) = (\frac{3118654011}{76832}\sqrt{2} + \frac{1103115731}{19208}, \frac{291101769555344}{51883209}\sqrt{2} + \frac{1235001447887552}{155649627},$
  $\frac{250932640456322}{155649627}\sqrt{2} + \frac{1064612285857304}{466948881})$.

- There is an outgoing edge of weight to the curve with invariants:

  $(k_1, k_2, k_3) = (-\frac{3118654011}{76832}\sqrt{2} + \frac{1103115731}{19208}, -\frac{291101769555344}{51883209}\sqrt{2} + \frac{1235001447887552}{155649627},$
  $-\frac{250932640456322}{155649627}\sqrt{2} + \frac{1064612285857304}{466948881})$.

- There is an outgoing edge of weight to the curve with invariants:

  $(k_1, k_2, k_3) = (-17197, -\frac{14848000}{27}, -\frac{7590400}{81})$.

We note that $(-17197, -\frac{14848000}{27}, -\frac{7590400}{81})$ appears as a neighbor to both $(1728, 287496)$ and $(\frac{751}{8}, \frac{778688}{27}, \frac{3178232}{81})$. We calculate the reduced automorphism group of this curve and determine it to be $\mathbb{Z}/2\mathbb{Z}$. Thus, this is a type 1 curve, and by Theorem 3.4, the dual edge back to $(1728, 287496)$ must be weight 1 and the dual edge back to $(\frac{751}{8}, \frac{778688}{27}, \frac{3178232}{81})$ must be weight 2.

Finally, we can list out the cycle types, and calculate their weights:

There is 1 unweighted-undirected 4-cycle (16 weighted-directed 4-cycles) of type $(\Sigma_{1728}, 3, 1, \Pi_{1728})$.

There are 2 unweighted-undirected 4-cycles (32 weighted-directed 4-cycles) of type $(\Sigma_{1728}, \Sigma, \kappa, \Pi_{1728})$.

[4] Again, some authors choose to represent this as a self-loop of weight 1.

We thus have 48 weighted-directed cycles in total, finishing the proof.

□

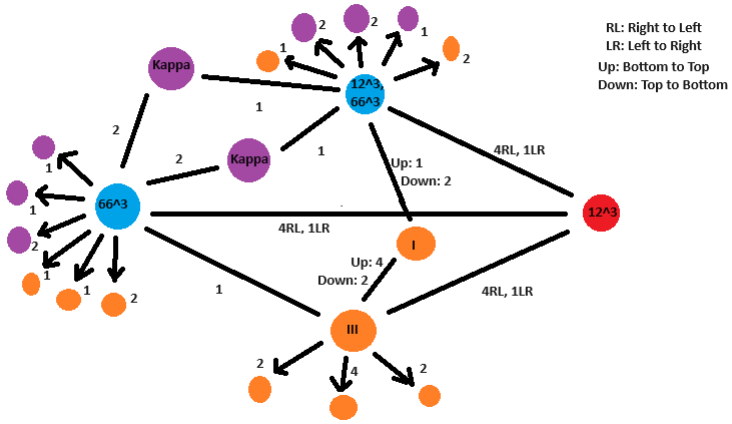

Figure 6.2: The 'Nautilus' Graph of the Type Σ_{1728} Curve

We include a visualization of the neighborhood: the 'nautilus graph' (ignoring self-loops). Here the red vertex is the type Σ_{1728} vertex, the two blue vertices are the elliptic radius 1 neighbors, the large orange vertices are the type 3 and type 1 vertices, the two large purple vertices are the κ vertices, and the remaining vertices are all distinct unimportant radius 2 vertices (purple if elliptic, orange if hyperelliptic).

Type $\Pi_{0,1728}$

Again, we expand on Florit and Smith's [2] results.

Theorem 6.12. *Consider the type* $\Pi_{0,1728}$ *vertex given by a product of two Elliptic curves with* $j = 0$ *and* $j = 1728$*, which we will denote* $[E_0 \times E_{1728}]$*. Let* $p \equiv 11 \mod (12)$*. Then through* $[E_0 \times E_{1728}]$ *there are in total, 5 unweighted-undirected 4-cycles, or 96 weighted-directed cycles, and* $N_2([E_0 \times E_{1728}])$ *is represented by Figure* **??**.

Proof. We first note that $[E_0 \times E_{1728}]$ has RA $\cong (\mathbb{Z}/12\mathbb{Z})$ and that since $p \equiv 11 \mod (12)$, $[E_0]$ and $[E_{1728}]$ are supersingular, and hence $[E_0 \times E_{1728}]$ is in $\Gamma_2^{\mathrm{SS}}(2, p)$.

As mentioned in the previous proof, the curve with $j = 1728$ has 2, 2-isogenies with image $j = 287496$ and a self loop. Further, $j = 287496$ has a dual edge back to $j = 1728$, and two new edges $29071392966\sqrt{2} + 41113158120$, $-29071392966\sqrt{2} + 41113158120$.

We will also need to know the possible isogenies of $[E_0]$ as well. We calculate that E_0 has a weight 3 edge with $j = 54000$. Further, we calculate that $j = 54000$ has a dual edge back to $j = 0$, and two new edges to $818626500\sqrt{3} + 1417905000$, and $-818626500\sqrt{3} + 1417905000$.
Hence we can conclude that the elliptic product neighbors to $[E_0 \times E_{1728}]$ are:

- a type Π_{1728} vertex with invariants $(1728, 54000)$,
- a type Π vertex with invariants $(54000, 287496)$.

The edge to the type Π_{1728} vertex has weight 3 and the edge to the type Π vertex has weight 6. By Theorem 3.4, we can conclude that the dual edge from the former has weight 4 and the dual edge from the later has weight 2.
We now construct all the elliptic product neighbors to $(1728, 54000)$:

- a type $\Pi_{0,1728}$ vertex with invariants $(0, 1728)$,
- a type Π_0 vertex with invariants $(0, 287496)$,
- a type Π_{1728} vertex with invariants $(1728, 818626500\sqrt{3} + 1417905000)$,
- a type Π_{1728} vertex with invariants $(1728, -818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(287496, 818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(287496, -818626500\sqrt{3} + 1417905000)$.

The first of these is representative of the dual edge back to $(0, 1728)$. The second has an outgoing weight of 2 and a dual weight of 3. The third has an outgoing weight of 1 and a dual weight of 1. The fourth has an outgoing weight of 1 and a dual weight of 1. The fifth of these has an outgoing weight of 2 and a dual weight of 1. The sixth of these has an outgoing weight of 2 and a dual weight of 1. All of the dual weights follow from Theorem 3.4.

We now construct all the elliptic product neighbors to $(54000, 287496)$:

- a type $\Pi_{0,1728}$ vertex with invariants $(0, 1728)$,
- a type Π_0 vertex with invariants $(0, 29071392966\sqrt{2} + 41113158120)$,
- a type Π_0 vertex with invariants $(0, -29071392966\sqrt{2} + 41113158120)$,
- a type Π_{1728} vertex with invariants $(1728, 818626500\sqrt{3} + 1417905000)$,
- a type Π_{1728} vertex with invariants $(1728, -818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(29071392966\sqrt{2} + 41113158120,$ $818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(29071392966\sqrt{2} + 41113158120,$ $-818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(-29071392966\sqrt{2} + 41113158120,$ $818626500\sqrt{3} + 1417905000)$,
- a type Π vertex with invariants $(-29071392966\sqrt{2} + 41113158120,$ $-818626500\sqrt{3} + 1417905000)$.

The first of these is representative of the dual edge back to $(0, 1728)$. All of these edges having outgoing weight 1. By Theorem 3.4, we can conclude that the dual edge for the second and third vertices has weight 3, the dual edge for the fourth and fifth vertices has weight 2, and the dual edge for the remaining vertices has weight 1.

We note that $(1728, 818626500\sqrt{3} + 1417905000)$ and $(1728, -818626500\sqrt{3} + 1417905000)$ are common vertices to both $(1728, 54000)$ and $(54000, 287496)$.

We now turn our attention to the Hyperelliptic neighbors of our starting vertex. All 6 are valid, and have the same Kohel invariants:

$$(k_1, k_2, k_3) = (\frac{20565}{4}, 4218240, 1235728),$$

and therefore are the same curve, i.e. the outgoing edge is weight 6. Calculating the reduced autmorphism group of this curve yields, $\mathbb{Z}/2\mathbb{Z}$. Hence, it is a type 1 curve, and by Theorem 3.4 the dual edge has weight 1. We thus have calculated the entirety of $N_1([E_0 \times E_{1728}])$ and have determined that there are 3 radius one neighbors to finish investigating: the adjacent type Π_{1728}, Π, and 1 vertices.

We begin by investigating the type 1 vertex. Constructing the quadratic splittings and calculating δ for each, we determine that only one of these neighbors will be an elliptic product, and it must then be the dual edge back to $\Pi_{0,1728}$. The remaining outgoing edges must all have the Jacobian of a Hyperelliptic curve as their image. We note that $\alpha = \sqrt{-3}\sqrt{1+\sqrt{-3}}$.

- There is an outgoing edge of weight 2 to the curve with invariants:

  (k_1, k_2, k_3) = (104895, 31610880, 9746688).

- There is an outgoing edge of weight 2 to the curve with invariants:

  $(k_1, k_2, k_3) = ((\frac{129828814335}{33856}\sqrt{-3} + \frac{129828814335}{33856})\alpha + \frac{159078548565}{8464},$

  $(\frac{1585204471174230555}{3404825447}\sqrt{-3} + \frac{1585204471174230555}{3404825447})\alpha + \frac{7720638341482384740}{3404825447},$

  $(\frac{1745105126560466561}{13619301788}\sqrt{-3} + \frac{1745105126560466561}{13619301788})\alpha + \frac{2125199950554888987}{3404825447}).$

- There is an outgoing edge of weight 2 to the curve with invariants:

  $(k_1, k_2, k_3) = ((-\frac{129828814335}{33856}\sqrt{-3} - \frac{129828814335}{33856})\alpha + \frac{159078548565}{8464},$

  $(-\frac{1585204471174230555}{3404825447}\sqrt{-3} - \frac{1585204471174230555}{3404825447})\alpha + \frac{7720638341482384740}{3404825447},$

  $(-\frac{1745105126560466561}{13619301788}\sqrt{-3} - \frac{1745105126560466561}{13619301788})\alpha + \frac{2125199950554888987}{3404825447}).$

- There is an outgoing edge of weight 2 to the curve with invariants:

  $(k_1, k_2, k_3) = ((-\frac{686462025}{7744}\sqrt{-3} + \frac{2059386075}{7744})\alpha + \frac{2379103335}{1936},$
  $(\frac{5479060197965485}{526153617}\sqrt{-3} - \frac{5479060197965485}{175384539})\alpha - \frac{5394827265843460}{175384539},$

$(\frac{24676691905900789}{6313843404}\sqrt{-3} - \frac{24676691905900789}{2104614468})\alpha - \frac{3562357300982617}{526153617})$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = ((\frac{686462025}{7744}\sqrt{-3} - \frac{2059386075}{7744})\alpha + \frac{2379103335}{1936},$

$(-\frac{5479060197965485}{526153617}\sqrt{-3} + \frac{5479060197965485}{175384539})\alpha - \frac{5394827265843460}{175384539},$

$(-\frac{24676691905900789}{6313843404}\sqrt{-3} + \frac{24676691905900789}{2104614468})\alpha - \frac{3562357300982617}{526153617})$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = ((-\frac{12050775}{2}\sqrt{-3} - \frac{12050775}{2})\alpha + 29516670,$

$(-578846400\sqrt{-3} - 578846400)\alpha + 2835544320,$

$(-224968172\sqrt{-3} - 224968172)\alpha + 1102050432)$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = ((\frac{12050775}{2}\sqrt{-3} + \frac{12050775}{2})\alpha + 29516670,$

$(578846400\sqrt{-3} + 578846400)\alpha + 2835544320,$

$(224968172\sqrt{-3} + 224968172)\alpha + 1102050432)$.

We now calculate the hyperelliptic neighbors of $(1728, 54000)$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = (-\frac{361426185}{234256}\sqrt{3} + \frac{315725715}{117128}, -\frac{68030963040}{214358881}\sqrt{3} - \frac{165244524480}{214358881}, -\frac{23470237060}{214358881}\sqrt{3} + \frac{30198334488}{214358881})$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = (\frac{361426185}{234256}\sqrt{3} + \frac{315725715}{117128}, \frac{68030963040}{214358881}\sqrt{3} - \frac{165244524480}{214358881}, \frac{23470237060}{214358881}\sqrt{3} + \frac{30198334488}{214358881})$.

- There is an outgoing edge of weight 2 to the curve with invariants:

$(k_1, k_2, k_3) = (104895, 31610880, 9746688)$.

We note that the vertex $(104895, 31610880, 9746688)$ is common to both $(1728, 54000)$ and the type 1 curve. Calculating the reduced automorphism group of this curve yields, $\mathbb{Z}/2\mathbb{Z}$. Hence, it is also a type 1 curve. By Theorem 3.4 we can conclude that the dual edge back to the other type 1 vertex has weight 2 and the dual edge back to $(1728, 54000)$ has weight 1.

We now calculate the hyperelliptic neighbors of $(54000, 287496)$.

- There is an outgoing edge of weight 1 to the curve with invariants:

$$k_1 = ((-\frac{31832054036460038809305}{174788455772288}\sqrt{3} + \frac{27567450345666893369895}{87394227886144})i + \frac{9189150115222297789965}{87394227886144}\sqrt{3}$$
$$- \frac{31832054036460038809305}{174788455772288})\alpha - \frac{11254331242621088425485}{21848556971536}\sqrt{3} + \frac{9746564533047070429815}{10924278485768},$$

$$k_2 = ((-\frac{474469050172383087790429739021937006 0}{1864685319290837296539841}\sqrt{3} + \frac{821804522902225058815292648937775 4280}{1864685319290837296539841})i$$
$$+ \frac{27393484096740835293843088297925847 60}{1864685319290837296539841}\sqrt{3} - \frac{474469050172383087790429739021937006 0}{1864685319290837296539841})\alpha$$
$$- \frac{13420011315278688770081606313933777 60}{1864685319290837296539841}\sqrt{3} + \frac{232441419738938775274591894025231644 80}{1864685319290837296539841},$$

$$k_3 = ((-\frac{31170846091181231097932188866674782 01}{3729370638581674593079682}\sqrt{3} + \frac{26994745250050018244956383594482992 95}{1864685319290837296539841})i$$
$$+ \frac{89982484166833394149854611981609976 5}{1864685319290837296539841}\sqrt{3} - \frac{31170846091181231097932188866674782 01}{3729370638581674593079682})\alpha$$
$$- \frac{44082233413959476978827078845385520 20}{1864685319290837296539841}\sqrt{3} + \frac{76352669583988039781638760701042966 32}{1864685319290837296539841}).$$

- There is an outgoing edge of weight 1 to the curve with invariants:

$$k_1 = ((\frac{31832054036460038809305}{174788455772288}\sqrt{3} + \frac{27567450345666893369895}{87394227886144})i + \frac{9189150115222297789965}{87394227886144}\sqrt{3}$$
$$+ \frac{31832054036460038809305}{174788455772288})\alpha + \frac{11254331242621088425485}{21848556971536}\sqrt{3} + \frac{9746564533047070429815}{10924278485768},$$

$$k_2 = ((\frac{474469050172383087790429739021937006 0}{1864685319290837296539841}\sqrt{3} + \frac{821804522902225058815292648937775 4280}{1864685319290837296539841})i$$
$$+ \frac{27393484096740835293843088297925847 60}{1864685319290837296539841}\sqrt{3} + \frac{474469050172383087790429739021937006 0}{1864685319290837296539841})\alpha$$
$$+ \frac{13420011315278688770081606313933777 60}{1864685319290837296539841}\sqrt{3} + \frac{232441419738938775274591894025231644 80}{1864685319290837296539841},$$

$$k_3 = ((\frac{31170846091181231097932188866674782 01}{3729370638581674593079682}\sqrt{3} + \frac{26994745250050018244956383594482992 95}{1864685319290837296539841})i$$
$$+ \frac{89982484166833394149854611981609976 5}{1864685319290837296539841}\sqrt{3} + \frac{31170846091181231097932188866674782 01}{3729370638581674593079682})\alpha$$
$$+ \frac{44082233413959476978827078845385520 20}{1864685319290837296539841}\sqrt{3} + \frac{76352669583988039781638760701042966 32}{1864685319290837296539841}).$$

- There is an outgoing edge of weight 1 to the curve with invariants:

$$k_1 = ((\frac{31832054036460038809305}{174788455772288}\sqrt{3} - \frac{27567450345666893369895}{87394227886144})i - \frac{9189150115222297789965}{87394227886144}\sqrt{3}$$
$$+ \frac{31832054036460038809305}{174788455772288})\alpha - \frac{11254331242621088425485}{21848556971536}\sqrt{3} + \frac{9746564533047070429815}{10924278485768},$$
$$k_2 = ((\frac{474469050172383087790429739021937006 0}{1864685319290837296539841}\sqrt{3} - \frac{821804522902225058815292648937775 4280}{1864685319290837296539841})i$$
$$- \frac{27393484096740835293843088297925847 60}{1864685319290837296539841}\sqrt{3} + \frac{474469050172383087790429739021937006 0}{1864685319290837296539841})\alpha$$
$$- \frac{13420011315278688770081606313933777 60}{1864685319290837296539841}\sqrt{3} + \frac{232441419738938775274591894025231644 80}{1864685319290837296539841},$$
$$k_3 = ((\frac{31170846091181231097932188866674782 01}{3729370638581674593079682}\sqrt{3} - \frac{26994745250050018244956383594482992 95}{1864685319290837296539841})i$$
$$- \frac{89982484166833394149854611981609976 5}{1864685319290837296539841}\sqrt{3} + \frac{31170846091181231097932188866674782 01}{3729370638581674593079682})\alpha$$

$$-\frac{4408223341395947697882707884538552020}{186468531929083729653984 1}\sqrt{3}+\frac{7635266958398803978163876070104296632}{186468531929083729653984 1}).$$

- There is an outgoing edge of weight 1 to the curve with invariants:

$$k_1=((-\frac{31832054036460038809305}{174788455772288}\sqrt{3}-\frac{27567450345666893369895}{87394227886144})i-\frac{9189150115222297789965}{87394227886144}\sqrt{3}$$

$$-\frac{31832054036460038809305}{174788455772288})\alpha+\frac{11254331242621088425485}{21848556971536}\sqrt{3}+\frac{9746564533047070429815}{10924278485768},$$

$$k_2=((-\frac{474469050172383087790429739021937 0060}{186468531929083729653984 1}\sqrt{3}-\frac{821804522902225058815292648937 7754280}{186468531929083729653984 1})i$$

$$-\frac{27393484096740835293843088297925847 60}{186468531929083729653984 1}\sqrt{3}-\frac{474469050172383087790429739021937 0060}{186468531929083729653984 1})\alpha$$

$$+\frac{13420011315278688770081606313933377760}{186468531929083729653984 1}\sqrt{3}+\frac{23244141973893877527459189402523164480}{186468531929083729653984 1},$$

$$k_3=((-\frac{31170846091181231097932188866667478201}{37293706385816745930796 82}\sqrt{3}-\frac{26994745250050018244956383594482992 95}{186468531929083729653984 1})i$$

$$-\frac{89982484166833394149854611981609976 5}{186468531929083729653984 1}\sqrt{3}-\frac{31170846091181231097932188866667478201}{37293706385816745930796 82})\alpha$$

$$+\frac{4408223341395947697882707884538552020}{186468531929083729653984 1}\sqrt{3}+\frac{7635266958398803978163876070104296632}{186468531929083729653984 1}).$$

- There is an outgoing edge of weight 1 to the curve with invariants:

$$(k_1,k_2,k_3)=((\frac{12050775}{2}\sqrt{-3}+\frac{12050775}{2})\alpha+29516670,(578846400\sqrt{-3}+578846400)\alpha+2835544320,$$

$$(224968172\sqrt{-3}+224968172)\alpha+1102050432).$$

- There is an outgoing edge of weight 1 to the curve with invariants:

$$(k_1,k_2,k_3)=((-\frac{12050775}{2}\sqrt{-3}-\frac{12050775}{2})\alpha+29516670,(-578846400\sqrt{-3}-578846400)\alpha+2835544320,$$

$$(-224968172\sqrt{-3}-224968172)\alpha+1102050432).$$

We note that these last two vertices are common to both $(54000, 287496)$ and the original type 1 curve. Calculating the reduced automorphism group of these curves yields, $\mathbb{Z}/2\mathbb{Z}$ for both. Hence, they are both also type 1 curves. By Theorem 3.4 we can conclude that the dual edges back to the other type 1 vertex have weight 2 and the dual edges back to $(54000, 287496)$ have weight 1.

Finally, we can list out the cycle types, and calculate their weights:

There are 2 unweighted-undirected 4-cycles (24 weighted-directed 4-cycles) of type $(\Pi_{0,1728}, \Pi_{1728}, \Pi_{1728}, \Pi)$.

There are 2 unweighted-undirected 4-cycles (48 weighted-directed 4-cycles) of type $(\Pi_{0,1728}, \Pi, 1, 1)$.

There is 1 unweighted-undirected 4-cycle (24 weighted-directed 4-cycles) of type $(\Pi_{0,1728}, \Pi_{1728}, 1, 1)$.

This leads to a total of 96 weighted-directed cycles, finishing the proof. □

Finally, we include a visualization of the neighborhood: the 'turtle' graph (ignoring self-loops). Here the red vertex is the type $\Pi_{0,1728}$ vertex, the blue vertices are elliptic vertices and the orange vertices are Hyperelliptic vertices.

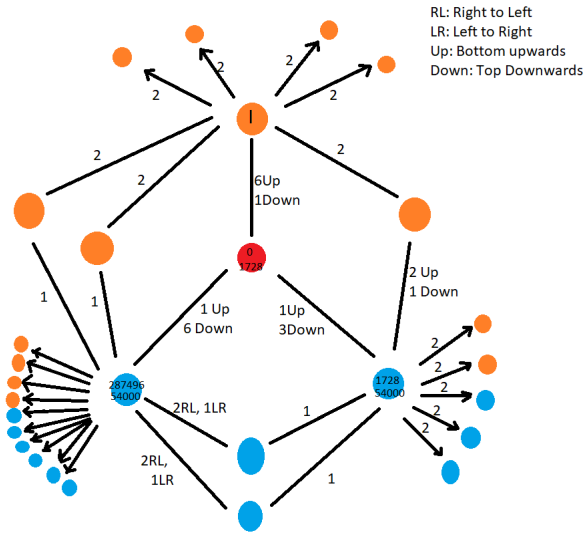

Figure 6.3: The 'Turtle' Graph of the Type $\Pi_{0,1728}$ Curve

Other Matters of Note

On Π_0 and Π_{1728}

Like types 6, Σ_{1728}, and $\Pi_{0,1728}$, Florit and Smith [2] do not provide enough information to calculate the number of 4-cycles in the graphs of type Π_0 or Π_{1728}. However, unlike the aforementioned types - these are not 0-dimensional families and therefore calculating $N_2([C])$ is more resource intensive. Additionally, the Kohel invariants will depend on the parameter of the family. Calculating these is a reasonable, but time-consuming, next step for this project.

On Special Cases

In section 7 we conjecture that $N_2([C])$ will have 23 vertices for C the type 4 curve for sufficiently large prime p. We note that this does not hold true for the prime $p = 101$. Here there are 22 vertices. Here we investigate what causes this behavior.

We start by, in part, mimicking the methodology of the previous sections and calculating (part) of $N_2([C])$ over extensions of $\mathbb{Q}$.

The type 4 curve has invariants, $(k_1, k_2, k_3) = (8325/2, 480000, 148000)$ and has 4 neighbors. We care about the type 1 neighbor - which we calculate has the invariants: $(k_1, k_2, k_3) = (\frac{402129}{16}, -\frac{4500941172}{15625}, -\frac{907209407}{15625})$.

We care about 4 of this curve's neighbors, which are all hyperelliptic curves with outgoing edge weight 1. Let's define the following coefficients:

$$A_0 = \frac{16004780521425763771}{180848704}, \quad A_1 = \frac{5658544410385411611}{45212176}, \quad A_2 = \frac{289277927528706567}{11303044}, \quad A_3 = \frac{3272805789888501829}{90424352},$$

$$B_0 = \frac{751561297818376692412960622824087866 09}{8131078842655033695192187 5}, \quad B_1 = \frac{7466358067775863003060264579688554458 8}{9034532047394481883546875},$$

$$B_2 = \frac{1871967574642846150978627292445109323 2}{9034532047394481883546875}, \quad B_3 = \frac{2382625329530960142319215639740595763 94}{8131078842655033695192187 5},$$

$$C_0 = \frac{1433148186324216390955905075897858961771}{97572946111860404342306250 0}, \quad C_1 = \frac{1125987507471131018742791105791399108 3}{5420719228436689130128125},$$

$$C_2 = \frac{1468147139681785414800217056700558725 2}{2710359614218344565064062 5}, \quad C_3 = \frac{7474583527362394921702844778300912353 3}{9757294611186040434230625 0}.$$

Define H_i over $\mathbb{Q}(\sqrt{2}, i)$, to be the four neighboring curves. We then calculate their Kohel invariants to be:

$$(k_1, k_2, k_3)_{H_0} = (-A_0\sqrt{-2} - A_1\sqrt{-1} - A_2\sqrt{2} - A_3, -B_0\sqrt{-2} - B_1\sqrt{-1} - B_2\sqrt{2} - B_3, -C_0\sqrt{-2} - C_1\sqrt{-1} - C_2\sqrt{2} - C_3),$$

$$(k_1, k_2, k_3)_{H_1} = (A_0\sqrt{-2} + A_1\sqrt{-1} - A_2\sqrt{2} - A_3, B_0\sqrt{-2} + B_1\sqrt{-1} - B_2\sqrt{2} - B_3, C_0\sqrt{-2} + C_1\sqrt{-1} - C_2\sqrt{2} - C_3),$$

$$(k_1, k_2, k_3)_{H_2} = (-A_0\sqrt{-2} + A_1\sqrt{-1} + A_2\sqrt{2} - A_3, -B_0\sqrt{-2} + B_1\sqrt{-1} + B_2\sqrt{2} - B_3, -C_0\sqrt{-2} + C_1\sqrt{-1} + C_2\sqrt{2} - C_3),$$

$$(k_1, k_2, k_3)_{H_3} = (A_0\sqrt{-2} - A_1\sqrt{-1} + A_2\sqrt{2} - A_3, B_0\sqrt{-2} - B_1\sqrt{-1} + B_2\sqrt{2} - B_3, C_0\sqrt{-2} - C_1\sqrt{-1} + C_2\sqrt{2} - C_3).$$

We now take these curves to be over $k = \mathbb{F}_{101^2}$. Note that over this field, $\sqrt{-1} = 10$, but $\sqrt{2} \notin \mathbb{F}_p$. Our coefficients reduce as follows:

$$k(A_0) = 95, \quad k(A_1) = 76, \quad k(A_2) = 41, \quad k(A_3) = 39, \quad k(B_0) = 56, \quad k(B_1) = 76,$$

$$k(B_2) = 55, \quad k(B_3) = 83, \quad k(C_0) = 43, \quad k(C_1) = 78, \quad k(C_2) = 26, \quad k(C_3) = 98.$$

Thus our invariants reduce as follows:

$$(k_1, k_2, k_3)_{H_0} = (60\sqrt{2} + 48 + 60\sqrt{2} + 62, 46\sqrt{2} + 48 + 46\sqrt{2} + 18, 75\sqrt{2} + 28 + 75\sqrt{2} + 3)$$

$$= (19\sqrt{2} + 9, 92\sqrt{2} + 66, 49\sqrt{2} + 31),$$

$$(k_1, k_2, k_3)_{H_1} = (41\sqrt{2} + 53 + 60\sqrt{2} + 62, 55\sqrt{2} + 53 + 46\sqrt{2} + 18, 26\sqrt{2} + 73 + 75\sqrt{2} + 3)$$

$$= (14, 71, 76),$$

$$(k_1, k_2, k_3)_{H_2} = (60\sqrt{2} + 53 + 41\sqrt{2} + 62, 46\sqrt{2} + 53 + 55\sqrt{2} + 18, 75\sqrt{2} + 73 + 26\sqrt{2} + 3)$$

$$= (14, 71, 76),$$

$$(k_1, k_2, k_3)_{H_3} = (41\sqrt{2} + 48 + 41\sqrt{2} + 62, 55\sqrt{2} + 48 + 55\sqrt{2} + 18, 26\sqrt{2} + 28 + 26\sqrt{2} + 3)$$

$$= (82\sqrt{2} + 9, 9\sqrt{2} + 66, 52\sqrt{2} + 31).$$

From this we can see what happened to the missing vertex in the graph for $p = 101$. H_1 and H_2 have the same Kohel invariants in k. This is certainly more likely for for smaller values of p, and further there should only be finitely many values of p for which this can even happen as we require

$$k_{1,1} \equiv k_{1,2}, \quad k_{2,1} \equiv k_{2,2}, \quad k_{3,1} \equiv k_{3,2}.$$

Chapter 7

The Spine

Graphs over $\mathbb{F}_p$

Let $g = 1$. Recall that all supersingular (and superspecial) curves are defined over $\mathbb{F}_{p^2}$. However, many curves can be defined over $\mathbb{F}_p$. This introduces two new graphs for consideration.

Definition 7.1. *The Spine, $\mathcal{S}$, is the full subgraph of $\Gamma_1^{SS}(2,p)$ whose vertices are defined by geometric isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$, and whose edges are all the edges between them regardless of the field of definition.*

Definition 7.2. *$\mathcal{G}_l(\mathbb{F}_p)$ is the graph whose vertices are supersingular curves defined over $\mathbb{F}_p$ and whose edges are only isogenies defined over $\mathbb{F}_p$ between them.*

We believe that the title 'Spine' is an excellent shorthand for the first graph. In an attempt to provide a similar brevity for the second graph, we will refer to it as the 'Ribs', and denote it as $\mathcal{R}$.

$\mathcal{R}$ is not a subgraph of $\Gamma_1^{SS}(2,p)$. To understand this, we briefly explore the concept of twisting. Consider an algebraic curve $A/\mathbb{F}_p$. Consider also, a second curve $A'/\mathbb{F}_p$ s.t. $A/\mathbb{F}_p \cong A'/\mathbb{F}_p$ over $\overline{\mathbb{F}}_p$. If they are also isomorphic over $\mathbb{F}_p$ we consider the curves to be equivalent.

Definition 7.3. *Any curve A' not equivalent to A is called a twist of A. We denote the group of twists of A by* $\mathrm{Twist(A/\mathbb{F}_p)}$.

Silverman [7] also demonstrates that

$$\mathrm{Twist(A/\mathbb{F}_p)} \cong \mathrm{H^1(Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p), Aut(A))}.$$

It can be shown that, for $p \neq 2$, and an elliptic curve, $j \neq 0, 1728$ (equivalent conditions exist for these cases),

$$\mathrm{Twist(E/\mathbb{F}_p)} \cong (\mathbb{F}_p^*)/(\mathbb{F}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

Thus, (almost) every elliptic curve has a single twist. As these curves are isomorphic over $\overline{\mathbb{F}_p}$, there will be two vertices with the same j-invariant in $\mathcal{R}$. We will revisit the Ribs in section 9.

The Spine in Genus 2

Arpin, et al. [3] studied the genus 1 Spine extensively. We are interested in extending this definition to genus 2 for further study. Determining whether there is a representative with coefficients in $\mathbb{F}_p$ for genus 2 is quite difficult. Instead we consider the following lemma about the genus 1 graph that will serve as inspiration for an alternative definition (see Silverman [7] Proposition 1.4c).

Lemma 7.4. *$[E]$ is in $\mathcal{S}$ in genus 1, iff the j-invariant of $[E]$ is in $\mathbb{F}_p$.*

Hyperelliptic curves do not have j-invariants, but as discussed earlier, we have a 3-tuple of invariants developed by Kohel that serves this role. We will use Kohel's invariants to form an analog in genus 2.

Definition 7.5. *The Kohel Spine, denoted $\mathcal{S}_\mathcal{K}$, of $\Gamma_2^{\mathrm{SS}}(2,p)$, is a subgraph consisting of all vertices $[H]$ where the Kohel invariants, (a_H, b_H, c_H), are in $\mathbb{F}_p^3$. The edges are all those between these vertices regardless of the field of definition.*

For the radial vertex, edge, and neighborhood sets defined in Chapter 4, we notate analogs in the Spine with $V_n^{\mathcal{S}}([H])$, $E_n^{\mathcal{S}}([H])$, and $N_n^{\mathcal{S}}([H])$ respectively.

Another distinction we make is between Hyperelliptic spinal vertices, and elliptic product spinal vertices. We will utilize this in discussing connectivity below.

Definition 7.6. *Define the Kohel Cervical Spine, $\mathcal{CS}_\mathcal{K}$, to be the full subgraph of $\Gamma_2^{\mathrm{SS}}(2,p)$ whose vertices and whose edges are defined by isomorphism classes of the Jacobians of superspecial hyperelliptic curves defined over $\mathbb{F}_p$ and all edges between them.*

Also, define the Kohel Lumbar Spine, $\mathcal{LS}_\mathcal{K}$, to be the full subgraph of $\Gamma_2^{\mathrm{SS}}(2,p)$ whose vertices and whose edges are defined by isomorphism classes of products of supersingular elliptic curves curves defined over $\mathbb{F}_p$ and all edges between them.

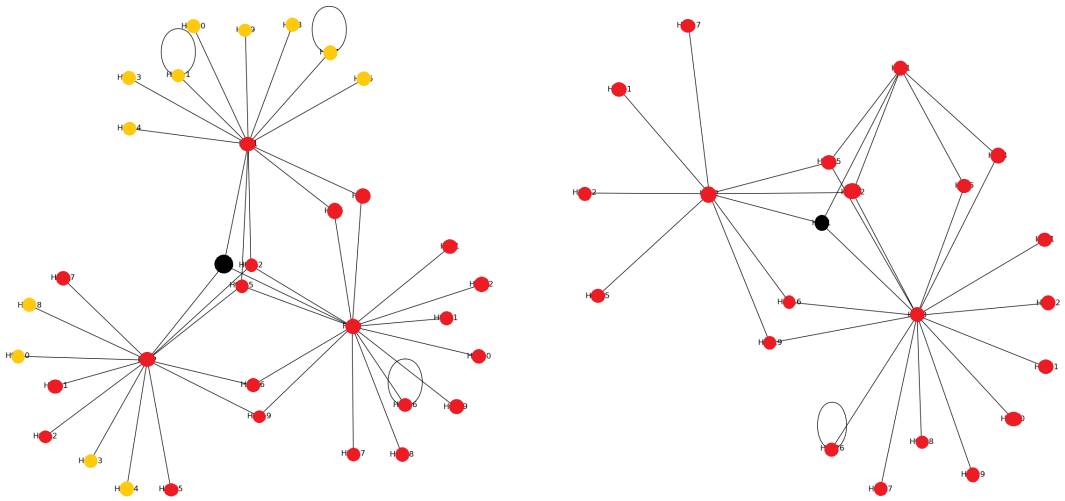

Figure 7.1: Left: The radius 2 neighborhood of the type 6 curve for $p = 839$, and Right: the same neighborhood for the Spine. The black vertex is the starting vertex, the red vertices are Spinal vertices and the yellow vertices are those that are non-Spinal.

Connectivity

Here we demonstrate a simple, yet important result. Arpin, et al [3] discovered the genus 1 Spine need not be connected. This remains true in genus 2, as we see in the graph below. (Note in each of the following graphs, red vertices are elliptic and blue vertices are hyperelliptic.)

This is the full graph for $\mathbb{F}_{31^2}$. We observe that neither $\mathcal{S}$ nor $\mathcal{CS}$ need to be connected.

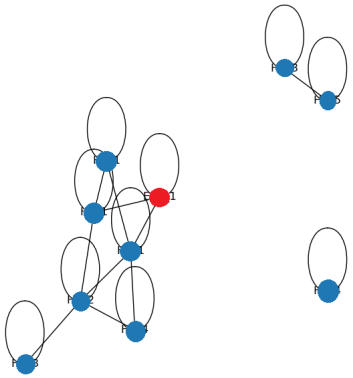

Figure 7.2: The full graph for $p = 31$.

This is the full graph for $\mathbb{F}_{53^2}$. We can see that $\mathcal{LS}$ does not need to be connected either.

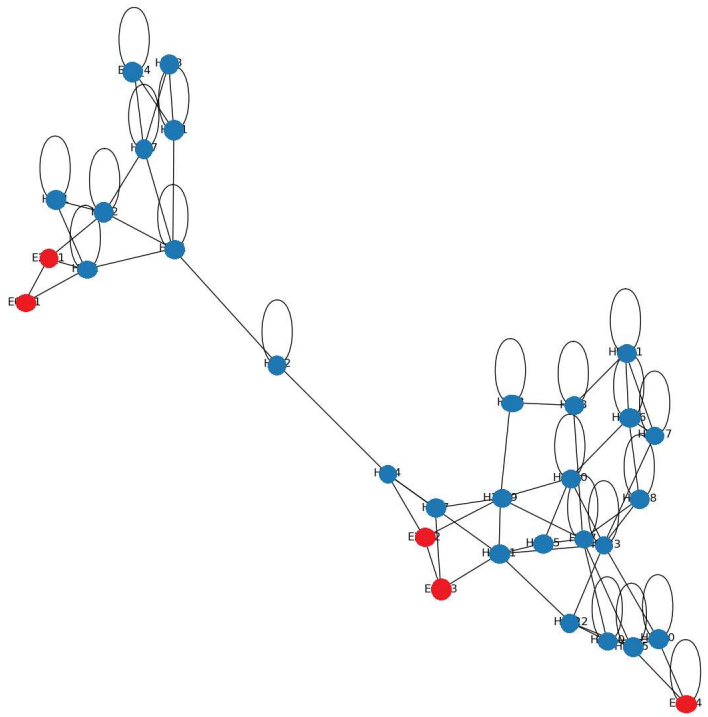

Figure 7.3: The full graph for $p = 53$.

We constructed the full graphs and their spines for the primes $p = 31, 37, 47, 53, 61, 71, 83, 101$. The number of vertices in a graph can be approximated by $p^3/2880$ [2], so the difficulty of producing full graphs grows very quickly. Within the graphs provided, $p = 37, 101$ are not connected, whereas everything else is. In both cases, only a very small proportion of the vertices can be found in the other components of the spine. It would be interesting to determine if this pattern continues.

Data and Conjectures

The following three sections cover findings and conjectures determined from data generated with the author's code for 0 dimensional families of curves.

The goal of this project was to determine what similarities exist in the data for small neighborhoods. Primarily, this relates to vertex count and the number of 4-cycles through the starting vertex.

Due to the unusual behavior of primes below 100, and the difficulty of calculation for larger primes, our dataset covers primes $100 < p < 1100$. Regardless, some unusual behavior appears.

Type 4

The type 4 curve is given by, $H_4 : y^2 = x^6 - 1$. We note that $\mathrm{RA(H)} \cong \mathrm{D}_{12}$ and that it is superspecial iff $p \equiv 5 \mod (6)$.

There are 81 primes, p, s.t. $100 < p < 1100$ where H_4 is defined over $\mathbb{F}_{p^2}$ and superspecial.

In a neighborhood of radius 2 about the type 4 curve, there are 23 vertices for 80 of these primes. Only the prime '101' differs, with 22 vertices.

When considering just the spine, we see the following interesting pattern emerge.

$$|V_2^{\mathcal{S}}([H_4])| = \begin{cases} 12 & p \equiv 1 \mod (8) \\ 15 & p \equiv 3 \mod (8) \\ 10 & p \equiv 5 \mod (8) \\ 17 & p \equiv 7 \mod (8) \end{cases}.$$

The only prime for which this pattern fails is once again '101,' which has 11 vertices, but $101 \equiv 5 \mod (8)$.

We also see a pattern emerge with the number of 4-cycles through H_4 in the spine.

$$\#\mathrm{Unweighted} - \mathrm{Undirected} = \begin{cases} 3 & p \equiv 1 \mod (4) \\ 6 & p \equiv 3 \mod (4) \end{cases},$$

$$\#\text{Weighted} - \text{Directed} = \begin{cases} 36 & p \equiv 1 \mod (4) \\ 72 & p \equiv 3 \mod (4) \end{cases}.$$

If we consider the radius 1 neighborhood instead, all 81 primes result in a neighborhood with 5 vertices. This is true for the entire graph (as expected) and the spine.

All neighborhoods, spinal or otherwise were connected for all primes in this dataset.

We now package all of this data as a conjecture:

Conjecture 7.7 (Nature of H_4)**.** *Let $H_4 : y^2 = x^6 - 1$ be defined over $\mathbb{F}_{p^2}$, for $p \equiv 5 \mod (6)$. For all but finitely many primes we claim the following:*

a) $N_2(H_4)$ *contains 23 vertices.*

b) $N_1^{\mathcal{S}}(H_4)$ *contains 5 vertices.*

c) $N_2^{\mathcal{S}}(H_4)$ *contains 12 vertices if $p \equiv 1 \mod (8)$, 15 vertices if $p \equiv 3 \mod (8)$, 10 vertices if $p \equiv 5 \mod (8)$, and 17 vertices if $p \equiv 7 \mod (8)$.*

d) $\mathcal{S}$ *contains 3 unweighted-undirected* 4*-cycles (36 weighted-directed* 4*-cycles) through* H_4 *if $p \equiv 1 \mod (4)$ and it contains 6 unweighted-undirected* 4*-cycles (72 weighted-directed* 4*-cycles) through* H_4 *if $p \equiv 3 \mod (4)$.*

e) $N_2^{\mathcal{S}}(H_4)$ *is connected.*

We note that *b)* implies *e)*, but not necessarily the reverse.

Type 5

The type 5 curve is given by, $H_5 : y^2 = x^5 - x$. We note that (assuming $p \neq 5$), $\mathrm{RA(H)} \cong \mathrm{S}_4$ and that it is superspecial iff $p \equiv 5, 7 \mod (8)$.

There are 83 primes, p, s.t. $100 < p < 1100$ where H_5 is defined over $\mathbb{F}_{p^2}$ and superspecial.

In a neighborhood of radius 2 about the type 5 curve, there are 20 vertices for 82 of these primes. Only the prime '101' differs, with 19 vertices.

When considering just the spine, we see the following interesting pattern emerge.

$$|V_2^{\mathcal{S}}([H_4])| = \begin{cases} 9 & p \equiv 1 \mod (4) \\ 10 & p \equiv 3 \mod (4) \end{cases}.$$

The only prime for which this pattern fails is once again '101,' which has 10 vertices, but $101 \equiv 1 \mod (4)$.

We also see a pattern emerge with the number of 4-cycles through H_5 in the spine.

$$\#\text{Unweighted} - \text{Undirected} = \begin{cases} 3 & p \equiv 1 \mod (4) \\ 0 & p \equiv 3 \mod (4) \end{cases},$$

$$\#\text{Weighted} - \text{Directed} = \begin{cases} 72 & p \equiv 1 \mod (4) \\ 0 & p \equiv 3 \mod (4) \end{cases}.$$

If we consider the radius 1 neighborhood instead, all 83 primes result in a neighborhood with 4 vertices (as expected). For the spine, all of these vertices persist if $p \equiv 1 \mod (4)$ and 2 vertices persist if $p \equiv 3 \mod (4)$.

All neighborhoods, spinal or otherwise were connected for all primes in this dataset.

We now package all of this data as a conjecture:

Conjecture 7.8 (Nature of H_5)**.** *Let $H_5 : y^2 = x^5 - x$ be defined over $\mathbb{F}_{p^2}$, for $p \equiv 5, 7 \mod (8)$, $p > 5$. For all but finitely many primes we claim the following:*

a) $N_2(H_5)$ contains 20 vertices.

b) $N_1^{\mathcal{S}}(H_5)$ contains 4 vertices if $p \equiv 1 \mod (4)$ and 2 vertices if $p \equiv 3 \mod (4)$.

c) $N_2^{\mathcal{S}}(H_5)$ contains 9 vertices if $p \equiv 1 \mod (4)$ and 10 vertices if $p \equiv 3 \mod (4)$.

d) $\mathcal{S}$ contains 3 unweighted-undirected 4-cycles (72 weighted-directed 4-cycles) through H_5 if $p \equiv 1 \mod (4)$ and it contains 0 unweighted-undirected 4-cycles (0 weighted-directed 4-cycles) through H_5 if $p \equiv 3 \mod (4)$.

e) $N_2^{\mathcal{S}}(H_5)$ is connected.

We note that *b)* implies *e)* but not necessarily the reverse.

Type 6

The type 6 curve is given by, $H_6 : y^2 = x^5 - 1$. We note that $\mathrm{RA(H)} \cong \mathbb{Z}/5\mathbb{Z}$ and that it is superspecial iff $p \equiv 4 \mod (5)$.

There are 38 primes, p, s.t. $100 < p < 1100$ where H_6 is defined over $\mathbb{F}_{p^2}$ and superspecial.

In a neighborhood of radius 2 about the type 6 curve, there are 34 vertices for 31 of these primes. Exceptions exist as follows: 33 vertices for the primes $179, 199, 239, 349, 379$ and 32 vertices for the primes $139, 229$.

When considering just the spine, we see the following interesting pattern emerge.

$$|V_2^{\mathcal{S}}([H_4])| = \begin{cases} 6 \ OR \ 12 & p \equiv 1 \mod (4) \\ 22 & p \equiv 3 \mod (4) \end{cases}.$$

This pattern fails for the same primes as above: $139, 179, 199, 229, 239, 349, 379$. Which primes $p \equiv 1 \mod (3)$ - where there are 6 vertices vs those where there are 12 vertices - are evenly distributed over our interval. Having tried every reasonable prime congruence condition, it is clear something else controls this discrepancy. What that is, remains an open question.

We also see a pattern emerge with the number of 4-cycles through H_6 in the spine.

$$\#\mathrm{Unweighted} - \mathrm{Undirected} = \begin{cases} 6 & p \equiv 1 \mod (4) \\ 10 & p \equiv 3 \mod (4) \end{cases},$$

$$\#\text{Weighted} - \text{Directed} = \begin{cases} 60 & p \equiv 1 \mod (4) \\ 140 & p \equiv 3 \mod (4) \end{cases}.$$

If we consider the radius 1 neighborhood instead, all 38 primes result in a neighborhood with 4 vertices. This is true for the entire graph (as expected) and the spine.

All neighborhoods, spinal or otherwise were connected for all primes in this dataset.

We now package all of this data as a conjecture:

Conjecture 7.9 (Nature of H_6)**.** *Let $H_6 : y^2 = x^5 - 1$ be defined over $\mathbb{F}_{p^2}$, for $p \equiv 4 \mod (5)$. For all but finitely many primes we claim the following:*

a) $N_2(H_6)$ *contains 34 vertices.*

b) $N_1^{\mathcal{S}}(H_6)$ *contains 4 vertices.*

c) $N_2^{\mathcal{S}}(H_6)$ *contains 6 or 12 vertices if* $p \equiv 1 \mod (4)$ *and 22 vertices if* $p \equiv 3 \mod (4)$.

d) $\mathcal{S}$ *contains 6 unweighted-undirected* 4*-cycles (60 weighted-directed* 4*-cycles) through* H_6 *if* $p \equiv 1 \mod (4)$ *and it contains 10 unweighted-undirected* 4*-cycles (140 weighted-directed* 4*-cycles) through* H_6 *if* $p \equiv 3 \mod (4)$.

e) $N_2^{\mathcal{S}}(H_6)$ *is connected.*

We note that *b)* implies *e)*, but not necessarily the reverse.

Chapter 8

Further Directions

Before we conclude this paper, we wish to provide some examples of further directions that can be explored at this point using the tools and groundwork we have established.

The Ribs Problem

We open by discussing the Ribs graph in genus 2.

Definition 8.1. *The ribs of* $\Gamma_2^{\mathrm{SS}}(2,p)$ *denoted* $\mathcal{R}$ *is the graph whose vertices are curves defined over* $\mathbb{F}_p$ *and whose edges are only isogenies defined over* $\mathbb{F}_p$ *between them.*

In short, studying $\mathcal{R}$ in genus 2 to the extent it was studied in genus 1 via Arpin, et al [3] is simply not possible at the moment.

What we do know comes primarily from two papers by Karemaker and Pries [16], and Cardona [17].

We first note the structure of the set of twists of a genus 2 surface.

Theorem 8.2. *If X is a hyperelliptic curve, then* $\mathrm{Aut_k}(\mathrm{Jac(X)}) \cong \mathrm{Aut_k(X)}$. *Further, this implies that* $\mathrm{Twist(Jac(X)/k)} = \mathrm{Twist(X/k)}$. *If instead, X is not a hyperelliptic curve, then* $\mathrm{Aut_k}(\mathrm{Jac(X)}) \cong \langle \mathrm{i} \rangle \times \mathrm{Aut_k(X)}$. *[18]*

This implies that when looking at the twists of Jacobians of hyperelliptic curves, it is sufficient to look at the twists of the hyperelliptic curves themselves. We must first quantify the number of twists.

Let $q = p^r$ the size of the field of definition.

By [17], Proposition 9, the Type 0 curve has 2 twists.

By [17], Proposition 10 and [16], Proposition 7.5, the Type 1 curve has 4 twists.

By [17], Proposition 13 and [16], Proposition 7.5, the Type 2 curve can be expressed as $y^2 = x^6 + x^3 + a$ for $p \neq 3, a \neq 0, 1/4, -1/50$. If $q \equiv 2 \mod (3)$ and a is a perfect square then the Type 2 curve has 6 twists - otherwise it has 4 twists.

By [17], Proposition 12 and [16], Proposition 7.5, the Type 3 curve can be expressed as $y^2 = x^5 + x^3 + ax$ for $a \neq 0, 1/4, 9/100$. If r is odd and a is a perfect square then the Type 3 curve has 5 twists - otherwise it has 3 twists.

By [17], Proposition 16 and [16], Proposition 7.4, the Type 4 curve has 7 twists if $p \equiv 2 \mod (3)$.

By [17], Proposition 17 and [16], Proposition 7.4, the Type 5 curve has 6 twists if $p \equiv 5, 7 \mod (8)$.

By [17], Proposition 11 and [16], Proposition 7.4, the Type 6 curve has 2 twists if $p \not\equiv 1 \mod (5)$.

Further details can be found in the above articles, but unfortunately, we are left without a way to directly calculate most of these twists. Until such an algorithm is developed we are unable to proceed with this project. However, with so many twists present in the graph - we can expect a rich structure from $\mathcal{R}$ when this is fully realized.

Open Questions

1. In Chapter 7, we discuss many conjectures regarding the number of vertices and 4-cycles in radius 2 neighborhoods in the graph. A natural next project would be to prove these conjectures. It is worth mentioning, as is easily visible from the invariants present in the proofs of the types 6, Σ_{1728}, and $\Pi_{0,1728}$ vertices in Chapter 6, that this would be dependent on which extensions are required over $\mathbb{Q}$ that are trivial for a given $\mathbb{F}_p$.

   One could also attempt to establish a theorem for when the number of vertices in both the graph itself and the spine is smaller than expected. Determining why there exists an uncertainty in the number of spinal vertices for the graph centered on the type 6 vertex when $p \equiv 1$ mod(4) is also a good question.

Finally, one could also seek to find similar results to those we present here for other curve types.

2. Continuing work on constructing the general neighborhood of radius 2 for every type of curve is a must. This still needs to be started for types Π_0 and Π_{1728}. If the remaining curve types are completed, one could approximate the exact number of 4-cycles in the entire graph.

3. Arpin, et al [3] produce a lot of statistical results on the Spine and Ribs. Attempting to recreate these results in genus 2 is a natural step to take.

4. With higher computing power we could extend our exploration of radius 2 neighborhoods to radius 3 neighborhoods. Looking at the overlap of neighborhoods given multiple starting vertices could also prove interesting. Perhaps even looking into persistence homology may prove interesting if calculating entire graphs becomes easier.

5. When further research allows for the easy calculation of twists in genus 2, there should be a rich area of exploration in building Ribs graphs. Constructing code to actively and accurately calculate these would also be of immense benefit and a natural extension of the current SageMath code.

6. There are plenty of places to extend the code, potential speed-ups, and better coding practices to be implemented in future versions. The author has learned more than half their knowledge in coding during this project so there are sure to be plenty of reasonable alterations.

Bibliography

[1] E. V. Flynn and Yan Bo Ti. Genus two isogeny cryptography. Cryptology ePrint Archive, Paper 2019/177, 2019. https://eprint.iacr.org/2019/177.

[2] Enrico Florit and Benjamin Smith. An atlas of the Richelot isogeny graph. 2021. 2021.

[3] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland, 2019.

[4] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999.

[5] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). 2022.

[6] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57(2):127–152, 1986.

[7] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[8] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[9] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[10] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[11] David Kohel. ECHIDNA: Databases for elliptic curves and higher dimensional analogues. http://echidna.maths.usyd.edu.au/~kohel/dbs/.

[12] Enrico Florit and Benjamin Smith. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. *Arithmetic, Geometry, Cryptography, and Coding Theory*, 2021.

[13] Marzio Mula, Nadir Murru, and Federico Pintore. On random sampling of supersingular elliptic curves. Cryptology ePrint Archive, Paper 2022/528, 2022. https://eprint.iacr.org/2022/528.

[14] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *J. Math. Cryptol.*, 14(1):268–292, 2020.

[15] Benjamin Smith. *Explicit Endomorphisms and Correspondences*. PhD thesis, 2005.

[16] Valentijn Karemaker and Rachel Pries. Fully maximal and fully minimal abelian varieties. *J. Pure Appl. Algebra*, 223(7):3031–3056, 2019.

[17] Gabriel Cardona. On the number of curves of genus 2 over a finite field. *Finite Fields Appl.*, 9(4):505–526, 2003.

[18] Kristin Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *Algebraic Geometry*, 10(1):19–36, 2001.

[19] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

Appendix A

Post-Quantum Cryptography and the Isogeny Graph

We begin by reviewing the motivating concern for our field of study.

A.1 Diffie-Hellman Key Exchange and the Discrete Logarithm Problem

Cryptographic methods are used to encrypt messages amongst many other security concerns. One of the most prevalent such methods is that of the Diffie-Hellman Key Exchange.

Let (*A*)lice and (*B*)ob be two individuals with an interest in communication, and (*E*)ve an eavesdropper. The goal is for *A* and *B* to share a secret without *E* being able to decipher it.

Algorithm A.1.

- *Initalization: A large prime p is chosen at random so that $p-1$ has only large prime factors. A generator $g \in G = \mathbb{Z}/p\mathbb{Z}$ is also chosen to give an environment for computation. This information is public. A,B and E all have access to it.*
- *Selection: A chooses $a \in (0, p-1)$ and calculates $\mathfrak{A} = g^a$. B chooses $b \in (0, p-1)$ and calculates $\mathfrak{B} = g^b$.*
- *Publication: A publishes $\mathfrak{A}$ and B publishes $\mathfrak{B}$. Now A, B, E all have access to $\mathfrak{A}$ and $\mathfrak{B}$.*
- *Calculation of the Shared Secret: A calculates $\mathfrak{B}^a = (g^b)^a = g^{ab}$ and B calculates $\mathfrak{A}^b = (g^a)^b = g^{ab}$. This serves as the shared secret.*

Thus Alice and Bob have a shared secret. Eve knows $G, g, \mathfrak{A}$ and $\mathfrak{B}$. In order for Eve to learn the shared secret, she needs to know either a or b. Solving for 'a' requires solving $\log_g(\mathfrak{A})$ or solving $\log_g(\mathfrak{B})$. As G is a finite group, this problem translates to the discrete logarithm problem, which for substantially large p is computationally infeasible.

Elliptic Curve Diffie-Hellman (ECDH) replaces G with a subgroup of $E(k)$. This method is even more secure, but also relies on the notion that the discrete logarithm problem is hard.

With modern computers this is indeed the case, requiring $O\sqrt{|G|}$ time to solve the discrete logarithm problem over $E(k)$. However, with the advent of quantum computers on the horizon this will not remain the case. Solving the discrete logarithm problem reduces to finding orders of elements within the group in question. This is a job that Shor's Algorithm does quite quickly. Quantum computers are able to run Shor's Algorithm, thus meaning we require a new algorithm that is quantum-resistant. NIST has sent out a call for potential post-quantum cryptographic methodologies. One of which was built around our isogeny graphs. Recently, Castryck and Decru [5] found a break in this methodology. In this section we review the cryptosystem. Details on how it was broken can be found in the second appendix.

A.2 Supersingular Elliptic Curve Diffie-Hellman

We now establish a variant of the Diffie-Hellman Key Exchange involving Supersingular Elliptic Curves.

Algorithm A.2.

- *Initialization: Pick E a supersingular elliptic curve over $E_{\mathbb{F}_{p^2}}$ of order $(p \pm 1)^2$. Pick two primes l_A, l_B (usually 2 and 3) and values e_A, e_B, f so that $E_{\mathbb{F}_{p^2}}$ contains the full subgroups $E[l_A^{e_A}], E[l_B^{e_B}]$ and moreover $p = l_A^{e_A} l_B^{e_B} f \mp 1$. Lastly pick a basis $\langle P_A, Q_A \rangle$ for $E[l_A^{e_A}]$, and a basis $\langle P_B, Q_B \rangle$ for $E[l_B^{e_B}]$. All of this information is public.*

- *Selection: A picks a torsion point in $E[l_A^{e_A}]$: $\mathfrak{A} = [m_A]P_A + [n_A]Q_A$. B picks a torsion point in $E[l_B^{e_B}]$: $\mathfrak{B} = [m_B]P_B + [n_B]Q_B$.*

- *Publication: Using Velu's Formulas (see [19]) for the calculation of elliptic curve isogenies, A calculates the curve $E_A = E/\langle \mathfrak{A} \rangle$ from the quotient map $\alpha : E \to E_A$. A then also calculates $\alpha(P_B), \alpha(Q_B)$ and publishes $E_A, \alpha(P_B)$, and $\alpha(Q_B)$. Similarly B calculates the curve $E_B = E/\langle \mathfrak{B} \rangle$ from the quotient map $\beta : E \to E_B$. B then also calculates $\beta(P_A), \beta(Q_A)$ and*

publishes $E_B, \beta(P_A)$, and $\beta(Q_A)$. Now A, B and E all have access to both resulting covers and all of the resulting basis points.

- *Calculation of the Shared Secret: A calculates*

$$E/\langle \mathfrak{A}, \mathfrak{B} \rangle = E_B/\langle \beta(\mathfrak{A}) \rangle = E_B/\langle [m_A]\beta(P_A) + [n_A]\beta(Q_A) \rangle.$$

B calculates

$$E/\langle \mathfrak{A}, \mathfrak{B} \rangle = E_A/\langle \beta(\mathfrak{B}) \rangle = E_B/\langle [m_B]\alpha(P_B) + [n_B]\beta(Q_B) \rangle.$$

This serves as the shared secret.

Eve needs to be able to solve the isogeny path problem. Given two elliptic curves, E, E' over a finite field of the same size, find an isogeny $\phi : E \to E'$ of smooth degree. Recently an attack using classical computers was constructed, which we discuss in the second appendix.

A natural generalization is to switch elliptic curves to our genus 2 setting. However, finding $(3, 3)$-isogenies is currently difficult, and all calculations in the genus 2 setting are computationally taxing, making this an unlikely alternative for a cryptosystem.

Appendix B

The Castryck-Decru Attack

This appendix is adapted from a talk presented at the Colorado State University Number Theory Lab by the author in Fall of 2022. It is a brief overview of the basic ideas and is by no means a full exploration of the topic. It is relatively informal, and thus relegated to this appendix. The reader is encouraged to read the original paper by Castryck and Decru [5] for more details. We will be attempting to break SIKE by finding Bob's secret, $\mathfrak{B}$.

Since P_B and Q_B are public, and it can be shown that finding the pair (P_B, Q_B) is equivalent to finding $(1, \mu)$ for μ an integer - we merely need to find the μ so that

$$\ker(\beta) = \langle P_B + \mu Q_B \rangle.$$

Recall from Appendix A that Bob calculates on the 3-isogeny graph, so we expand μ as

$$\mu = k_1 + k_2 3^{\beta_1} + \cdots + k_\tau 3^{\beta_{\tau-1}}$$

for $k_i \in [0, 3^{\beta_i - \beta_{i-1}} - 1)$. The isogeny β will be a $\beta_\tau = b$-isogeny.

In order to calculate μ we will need to calculate each of the k_i. The idea in general is to guess the value of each k_i in order. Knowing k_{i-1} can be used to reduce the number of possibilities for k_i to $3^{\beta_i - \beta_{i-1}}$. For all but very small values of i, it is overwhelmingly likely that $\beta_i - \beta_{i-1} = 2$ and hence there are 9 options for k_i.

We now develop a check as to when an option for k_i is (highly) likely to be correct. Our decision process is based on whether or not we can construct a chain of isogenies in the $(2, 2)$ isogeny graph of the following form:

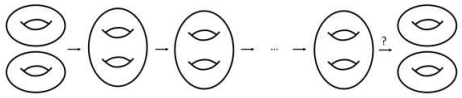

Figure B.1: A visualization of ‘Gluing and Splitting’

This process is referred to as “Gluing and Splitting." It takes in a product of Supersingular Elliptic Curves and “glues" them to form the Jacobian of a Superspecial Hyperelliptic Curve.

Next it passes through a series of Richelot Isogenies until at the end it “splits" again into a product of Supersingular Elliptic Curves. If this happens, the test succeeds. We can test this by calculating δ for the final isogeny. We want $\delta = 0$, or in other words, for the isogeny to be singular. If this holds, we say there exists a 3^b-isogeny

$$\phi : E_0 \to E,$$

$$\text{s.t.} \quad \phi(\mathrm{P}_0) = \mathrm{P}, \quad \phi(\mathrm{Q}_0) = \mathrm{Q}.$$

We now must find the initial product of our Supersingular Elliptic Curves. We begin by making two assumptions:

- $2^a > 3^b$ (there is a workaround if not).
- Let $c = 2^a - 3^b > 0$. There is an arbitrary cyclic c-isogeny,

$$\gamma : E_0 \to C,$$

  where E_0 is the initial curve in the cryptosystem and C is an arbitrary codomain curve. We are able to calculate

$$P_C = \gamma(P_0), \quad Q_C = \gamma(Q_0).$$

  (This is non-trivial but beyond the scope of this discussion.)

Consider the map $\psi : C \to E$ that completes the diagram:

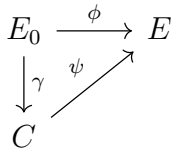

Figure B.2: Our commutative diagram

We define $\psi = [-1] \circ \phi \circ \hat{\gamma}$. Hence,

$$\psi(P_C) = -cP, \quad \psi(Q_C) = -cQ.$$

Let $x \equiv 3^{-b} \mod (2^a)$. Then the Weil Pairing,

$$e_{2^a}(x\psi(R), x\psi(S)) = e_{2^a}(R, S)^{-1},$$

$\forall R, S \in C[2^a]$. The map below has a special name, an “anti-isometry" of the 2^a-Weil Pairing:

$$[x] \circ \psi|_{C[2^a]} : C[2^a] \to E[2^a].$$

We call the group

$$\langle (P_C, x\psi(P_C)), (Q_C, x\psi(Q_C)) \rangle = \langle (P_C, P), (Q_C, Q) \rangle$$

maximally isotropic with respect to the 2^a-Weil Pairing on $C \times E$ (a product of supersingular elliptic curves). This is an alternative condition for a subgroup of a Genus 2 Superspecial Abelian Surface's 2^a torsion to be a $(2^a, 2^a)$ Richelot Isogeny. Such an isogeny is a walk in the $(2, 2)$-isogeny graph. With overwhelming likelihood, the first $(2, 2)$-isogeny in the walk is a “gluing" step.

As the result of a theorem by Kani discussed in Castryck and Decru's paper [5], the γ map is used to "split" the $(2^a, 2^a)$-isogeny in the last step, resulting in a product of super-singular elliptic curves, once more.

SIKE is commonly taken to start with one of the initial curves:

$$E_{\text{Start}} : y^2 = x^3 + x$$

or

$$E_{\text{Start}} : y^2 = x^3 + 6x^2 + x.$$

This however need not be the case. Castryck and Decru [5] provide workarounds for other cases - but we assume $E_0 = E_{\text{Start}}$. As an attacker, we are expected to know E_0 as well as the generators P_B, Q_B. We define the intermediate maps:

$$\kappa_i : E_{i-1} \to E_i,$$

$$\phi_i : E_i \to E,$$

where

$$\phi = \phi_0.$$

The maps κ_i are all 3^{β_i}-isogenies. We note that determining the maps κ_i is in essence equivalent to determining the k_i. We can construct the kernals of the κ_i as follows:

$$\ker(\kappa_1) = \langle 3^{b-\beta_1} P_B + k_1 3^{b-\beta_1} Q_B \rangle,$$

$$\ker(\kappa_2) = \langle 3^{b-\beta_2} P_B + (k_1 + k_2 3^{\beta_1}) 3^{b-\beta_2} Q_B \rangle,$$

and so on. We now discuss the Algorithm for actually breaking SIKE.

Algorithm B.1. *Initial Step:*

- *Make a guess at the value of* k_1.
- *Choose an appropriate intermediate* $c_1 = 2^{a-\alpha_1} - 3^{b-\beta_1}$ *so that its only prime factors are* $p \equiv 1 \mod (4)$.
- *Construct* C_1 *as above using* $\ker(\kappa_1)$*, and then* $P_{C_1}, Q_{C_1} \in C_1$.
- *Determine whether the codomain of the isogeny of* $E_0 \times C_1$ *by* $\langle (P_{C_1}, 2^{\alpha_1}P), (Q_{C_1}, 2^{\alpha_1}Q) \rangle$ *is a product of elliptic curves by calculating the walk of Richelot Isogenies in the* $(2,2)$*-graph.*
- *If so, our guess for* k_1 *is correct and we record it. If not, we make another guess at the value of* k_1*. This should be easily exhaustible.*

Iterative Step:

- *Make a guess at the value of* k_2.
- *Choose appropriate* c_i*, then construct* C_i *using* $\ker(\kappa_i)$*, and then* $P_{C_i}, Q_{C_i} \in C_i$.
- *Determine whether the codomain of the isogeny* $E_{i-1} \times C_i$ *by* $\langle (P_{C_1}, 2^{\alpha_i}P), (Q_{C_1}, 2^{\alpha_i}Q) \rangle$ *is a product of elliptic curves by calculating the walk of Richelot Isogenies in the* $(2,2)$*-graph.*
- *If so, we record* k_i*. Once all* k_i *are recorded, we have successfully found the value for Bob's secret key, and broken SIKE.*

Ran on a single core, the authors were able to break the Microsoft SIKE challenges SIKEp182 and SIKEp217 in 4 and 6 minutes respectively.

On SIKEp715, which is considered to be level 5 quantum resistant, it took 20 hours and 37 minutes.

Changing the starting curve, the prime, or the size of the torsion group does not solve this problem. The authors have workarounds for these scenarios.