

An atlas of the Richelot isogeny graph

Enric Florit, Benjamin Smith

▶ **To cite this version:**

Enric Florit, Benjamin Smith. An atlas of the Richelot isogeny graph. 2021. hal-03094296v1

HAL Id: hal-03094296

https://inria.hal.science/hal-03094296v1

Preprint submitted on 4 Jan 2021 (v1), last revised 4 Jan 2021 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

AN ATLAS OF THE RICHELOT ISOGENY GRAPH

ENRIC FLORIT AND BENJAMIN SMITH

Abstract. We describe and illustrate the local neighbourhoods of vertices and edges in the $(2,2)$-isogeny graph of principally polarized abelian surfaces, considering the action of automorphisms. Our diagrams are intended to build intuition for number theorists and cryptographers investigating isogeny graphs in dimension/genus 2, and the superspecial isogeny graph in particular.

1. Introduction

This article is an illustrated guide to the Richelot isogeny graph. Following Katsura and Takashima [14], we present diagrams of the neighbourhoods of general vertices of each type. Going further, we also compute diagrams of neighbourhoods of general edges, which can be used to glue the vertex neighbourhoods together. Our aim is to build intuition on the various combinatorial structures in the graph, providing concrete examples for some of the more pathological cases. The authors have used the results presented here to verify computations and form conjectures when investigating the behaviour of random walks in superspecial isogeny graphs [8].

We work over a ground field $\Bbbk$ of characteristic not 2, 3, or 5. In our application to superspecial PPASes, $\Bbbk = \mathbb{F}_{p^2}$, though our computations were mostly done over function fields over cyclotomic fields.

Let $\mathcal{A}/\Bbbk$ be a principally polarized abelian surface (PPAS). A $(2,2)$-*isogeny*, or *Richelot isogeny*, is an isogeny $\phi : \mathcal{A} \to \mathcal{A}'$ of PPASes whose kernel is a maximal 2-Weil isotropic subgroup of $\mathcal{A}[2]$. Such a ϕ has kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$; it respects the principal polarizations λ and λ' on $\mathcal{A}$ and $\mathcal{A}'$, respectively, in the sense that $\phi^*(\lambda') = 2\lambda$; and its (Rosati) *dual isogeny* $\phi^\dagger : \mathcal{A}' \to \mathcal{A}$ satisfies $\phi^\dagger \circ \phi = [2]_{\mathcal{A}}$.

The $(2,2)$-*isogeny* or *Richelot isogeny graph* is the directed weighted multigraph defined as follows. The *vertices* are isomorphism classes of PPASes over $\Bbbk$. If $\mathcal{A}$ is a PPAS, then $\big[\mathcal{A}\big]$ denotes the corresponding vertex. The *edges* are isomorphism classes of $(2,2)$-isogenies ($\phi_1 : \mathcal{A}_1 \to \mathcal{A}_1'$ and $\phi_2 : \mathcal{A}_2 \to \mathcal{A}_2'$ are isomorphic if there are isomorphisms of PPASes $\alpha\colon \mathcal{A}_1 \to \mathcal{A}_2$ and $\beta\colon \mathcal{A}_1' \to \mathcal{A}_2'$ such that $\phi_2 \circ \alpha = \beta \circ \phi_1$).

The edges are *weighted* by the number of distinct kernels yielding isogenies in their class. The weight of an edge $\big[\phi\big]$ is denoted by $w(\big[\phi\big])$. If $\big[\phi\big] : \big[\mathcal{A}\big] \to \big[\mathcal{A}'\big]$ is an edge, then $w(\big[\phi\big]) = n$ if and only if there are n kernel subgroups $K \subset \mathcal{A}[2]$ such that $\mathcal{A}' \cong \mathcal{A}/K$ (this is independent of the choice of representative isogeny ϕ).

There are fifteen maximal 2-Weil-istropic subgroups in $\mathcal{A}[2]$, though some (or all) might not be defined over $\Bbbk$. The sum of the weights of the edges leaving any vertex is therefore at most 15.

The isogeny graph breaks up into connected components within isogeny classes. We are particularly interested in the superspecial isogeny class. Recall that a PPAS

Date: December 2020.

The second author was supported by ANR CIAO.

$\mathcal{A}/\overline{\mathbb{F}}_p$ is *superspecial* if its Hasse–Witt matrix vanishes identically. Equivalently, $\mathcal{A}$ is superspecial if it is isomorphic *as an unpolarized abelian variety* to a product of supersingular elliptic curves. For background on superspecial and supersingular abelian varieties in low dimension, we refer to Ibuyiyama, Katsura, and Oort [12] and Brock's thesis [4]. For more general results, we refer to Li and Oort [15].

Definition 1. *The superspecial Richelot isogeny graph is the subgraph $\Gamma_2^{SS}(2;p)$ of the Richelot isogeny graph over $\mathbb{F}_{p^2}$ supported on the superspecial vertices.*

Recall that $\Gamma_2^{SS}(2;p)$ has $p^3/2880 + O(p)$ vertices (see §3.4 for a more precise statement), and is connected [13]. If $\mathcal{A}/\overline{\mathbb{F}}_p$ represents a vertex in $\Gamma_2^{SS}(2;p)$, then the invariants corresponding to $\left[\mathcal{A}\right]$ are defined over $\mathbb{F}_{p^2}$, as are all 15 of the $(2,2)$-isogeny kernels—so $\Gamma_2^{SS}(2;p)$ is a 15-regular graph. It has interesting number-theoretic properties and applications (such as Mestre's *méthode des graphes* [16]), and potential cryptographic applications (including [6, 19, 9, 5, 7]). All of these applications depend on a clear understanding of the structure of $\Gamma_2^{SS}(2;p)$: for example, the local neighbourhoods of vertices with extra automorphisms (and their interrelations) affect the expansion properties and random-walk behaviour of $\Gamma_2^{SS}(2;p)$, as we see in [8].

2. Richelot isogenies and isogeny graphs

There are two kinds of PPASes: products of elliptic curves (with the product polarization) and Jacobians of genus-2 curves. The algorithmic construction of isogenies depends fundamentally on whether the PPASes are Jacobians or elliptic products. We recall the Jacobian case in §2.1, and the elliptic product case in §2.2.

2.1. Richelot isogenies.

Let $\mathcal{C} : y^2 = F(x)$ be a genus-2 curve, with F squarefree of degree 5 or 6. The kernels of $(2,2)$-isogenies from $\mathcal{J}(\mathcal{C})$ correspond to factorizations of F into quadratics (of which one may be linear, if $\deg(F) = 5$):

$$\mathcal{C} : y^2 = F(x) = F_1(x)F_2(x)F_3(x)\,,$$

up to permutation of the F_i and constant multiples. We call such factorizations *quadratic splittings*. The kernel (and isogeny) is defined over $\Bbbk$ if the splitting is.

Fix one such quadratic splitting $\{F_1, F_2, F_3\}$; then the corresponding subgroup $K \subset \mathcal{J}(\mathcal{C})[2]$ is the kernel of a $(2,2)$-isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C})/K$. For each $1 \le i \le 3$, we write $F_i(x) = F_{i,2}x^2 + F_{i,1}x + F_{i,0}$. Now let

$$\delta = \delta(F_1, F_2, F_3) := \begin{vmatrix} F_{1,0} & F_{1,1} & F_{1,2} \\ F_{2,0} & F_{2,1} & F_{2,2} \\ F_{3,0} & F_{3,1} & F_{3,2} \end{vmatrix}.$$

If $\delta(F_1, F_2, F_3) \neq 0$, then $\mathcal{J}(\mathcal{C})/K$ is isomorphic to a Jacobian $\mathcal{J}(\mathcal{C}')$, which we can compute using Richelot's algorithm (see [3] and [18, §8]): $\mathcal{C}'$ is defined by

$$\mathcal{C}' : y^2 = G_1(x)G_2(x)G_3(x) \quad \text{where} \quad G_i(x) := \frac{1}{\delta}(F_j'(x)F_k(x) - F_k'(x)F_j(x))$$

for each cyclic permutation (i,j,k) of $(1,2,3)$. The quadratic splitting $\{G_1, G_2, G_3\}$ corresponds to the kernel of the dual isogeny $\phi^\dagger : \mathcal{J}(\mathcal{C}') \to \mathcal{J}(\mathcal{C})$.

If $\delta(F_1, F_2, F_3) = 0$, then $\mathcal{J}(\mathcal{C})/K$ is isomorphic to an elliptic product $\mathcal{E} \times \mathcal{E}'$. which we can compute as follows. There exist linear polynomials U and V such that $F_1 = \alpha_1 U^2 + \beta_1 V^2$ and $F_2 = \alpha_2 U^2 + \beta_2 V^2$ for some α_1, β_1, α_2, and β_2; and since in

this case F_3 is a linear combination of F_1 and F_2, we must have $F_3 = \alpha_3 U^2 + \beta_3 V^2$ for some α_3 and β_3. The elliptic factors are defined by

$$\mathcal{E} : y^2 = \prod_{i=1}^{3} (\alpha_i x + \beta_i) \qquad \text{and} \qquad \mathcal{E}' : y^2 = \prod_{i=1}^{3} (\beta_i x + \alpha_i)\,,$$

and the isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{E} \times \mathcal{E}'$ is induced by the product of the double covers $\pi : \mathcal{C} \to \mathcal{E}$ resp. $\pi' : \mathcal{C} \to \mathcal{E}'$ mapping (x, y) to $(U^2/V^2, y/V^3)$ resp. $(V^2/U^2, y/U^3)$.

2.2. **Isogenies from elliptic products.** Consider a generic pair of elliptic curves

$$\mathcal{E} : y^2 = (x - s_1)(x - s_2)(x - s_3)\,,$$
$$\mathcal{E}' : y^2 = (x - s'_1)(x - s'_2)(x - s'_3)\,.$$

We have $\mathcal{E}[2] = \{0_{\mathcal{E}}, P_1, P_2, P_3\}$ and $\mathcal{E}'[2] = \{0_{\mathcal{E}'}, P'_1, P'_2, P'_3\}$ where $P_i := (s_i, 0)$ and $P'_i := (s'_i, 0)$. For each $1 \le i \le 3$, we let

$$\psi_i : \mathcal{E} \longrightarrow \mathcal{E}_i := \mathcal{E}/\langle P_i \rangle \quad \text{and} \quad \psi'_i : \mathcal{E}' \to \mathcal{E}'_i := \mathcal{E}'/\langle P'_i \rangle$$

be the quotient 2-isogenies. These can be computed using Vélu's formulæ [21].

Nine of the fifteen kernel subgroups of $(\mathcal{E} \times \mathcal{E}')[2]$ correspond to products of elliptic 2-isogeny kernels. Namely, for each $1 \le i, j \le 3$ we have the kernel

$$K_{i,j} := \langle (P_i, 0_{\mathcal{E}'}), (0_{\mathcal{E}}, P'_i) \rangle \subset (\mathcal{E} \times \mathcal{E}')[2]$$

of the product isogeny

$$\phi_{i,j} := \psi_i \times \psi_j : \mathcal{E} \times \mathcal{E}' \longrightarrow \mathcal{E}_i \times \mathcal{E}'_j \cong (\mathcal{E} \times \mathcal{E}')/K_{i,j}\,.$$

The other six kernels correspond to 2-Weil anti-isometries $\mathcal{E}[2] \cong \mathcal{E}'[2]$: they are

$$K_\pi := \{(0_{\mathcal{E}}, 0_{\mathcal{E}'}), (P_1, P'_{\pi(1)}), (P_2, P'_{\pi(2)}), (P_3, P'_{\pi(3)})\} \quad \text{for } \pi \in \mathrm{Sym}(\{1, 2, 3\})\,,$$

with quotient isogenies

$$\phi_\pi : \mathcal{E} \times \mathcal{E}' \longrightarrow \mathcal{A}_\pi := (\mathcal{E} \times \mathcal{E}')/K_\pi\,.$$

If the anti-isometry $P_i \mapsto P'_{\pi(i)}$ is induced by an isomorphism $\mathcal{E} \cong \mathcal{E}'$, then $\mathcal{A}_\pi \cong \mathcal{E} \times \mathcal{E}'$. Otherwise, following [11, Prop. 4], $\mathcal{A}_\pi$ is the Jacobian of a genus-2 curve

$$\mathcal{C}_\pi : y^2 = -F_1(x)F_2(x)F_3(x)$$

where

$$F_i(x) := A(s_j - s_i)(s_i - s_k)x^2 + B(s'_j - s'_i)(s'_i - s'_k)$$

for each cyclic permutation (i, j, k) of $(1, 2, 3)$, with

$$A := \frac{a_1}{a_2} \prod (s'_i - s'_j)^2 \text{ where } a_1 := \sum \frac{(s_j - s_i)^2}{s'_j - s'_i} \text{ and } a_2 := \sum s_i(s'_k - s'_j)\,,$$
$$B := \frac{b_1}{b_2} \prod (s_i - s_j)^2 \text{ where } b_1 := \sum \frac{(s'_j - s'_i)^2}{s_j - s_i} \text{ and } b_2 := \sum s'_i(s_k - s_j)\,,$$

where the sums and products are over cyclic permutations (i, j, k) of $(1, 2, 3)$. The dual isogeny $\phi^\dagger_\pi : \mathcal{J}(\mathcal{C}_\pi) \to \mathcal{E} \times \mathcal{E}'$ corresponds to the splitting $\{F_1, F_2, F_3\}$.

3. Automorphism groups of abelian surfaces

We now consider the impact of automorphisms on edge weights in the isogeny graph, following Katsura and Takashima [14], and recall the explicit classification of reduced automorphism groups of PPASes. In contrast with elliptic curves, where (up to isomorphism) only two curves have nontrivial reduced automorphism group, with PPASes we see much richer structures involving many more vertices. Proofs for all of the results in this section can be found in [12], [14], and [8].

3.1. **Automorphisms and isogenies.** Let $\phi : \mathcal{A} \to \mathcal{A}/K$ be a $(2,2)$-isogeny with kernel K. Let α be an automorphism of $\mathcal{A}$, and let $\phi' : \mathcal{A} \to \mathcal{A}/\alpha(K)$ be the quotient isogeny; then α induces an isomorphism $\alpha_* : \mathcal{A}/K \to \mathcal{A}/\alpha(K)$ such that $\alpha_* \circ \phi = \phi' \circ \alpha$.

If $\alpha(K) = K$, then $\mathcal{A}/K = \mathcal{A}/\alpha(K)$, so α_* is an automorphism of $\mathcal{A}/K$. Going further, if S is the stabiliser of K in $\mathrm{Aut}(\mathcal{A})$, then S induces an isomorphic subgroup S' of $\mathrm{Aut}(\mathcal{A}/K)$, and in fact S' is the stabiliser of $\ker(\phi^\dagger)$ in $\mathrm{Aut}(\mathcal{A}/K)$.

If $\alpha(K) \neq K$ then the quotients $\mathcal{A}/K$ and $\mathcal{A}/\alpha(K)$ are different, so α_* is an isomorphism but not an automorphism. The isogenies ϕ and $\phi_\alpha := \alpha_*^{-1} \circ \phi'$ have identical domains and codomains, but distinct kernels; thus, they both represent the same edge in the isogeny graph, and $w(\left[\phi\right]) > 1$.

Every PPAS has $[-1]$ in its automorphism group, but $[-1]$ fixes every kernel and commutes with every isogeny—so it has no impact on edges or weights in the isogeny graph. We can therefore simplify by quotienting $[-1]$ out of the picture.

Definition 2. *If $\mathcal{A}$ is a PPAS, then its* ***reduced automorphism group*** *is*

$$\mathrm{RA}(\mathcal{A}) := \mathrm{Aut}(\mathcal{A})/\langle[-1]\rangle\,.$$

Since $\langle[-1]\rangle$ is contained in the centre of $\mathrm{Aut}(\mathcal{A})$, the quotient $\mathrm{RA}(\mathcal{A})$ acts on the set of kernel subgroups of $\mathcal{A}[2]$. We have two useful results for $(2,2)$-isogenies $\phi : \mathcal{A} \to \mathcal{A}/K$. First, if O_K is the orbit of K under $\mathrm{RA}(\mathcal{A})$, then there are $\#O_K$ distinct kernels of isogenies representing $\left[\phi\right]$: that is,

$$w(\left[\phi\right]) = \#O_K\,.$$

Second, we have the "ratio principle" from [8, Lemma 1]:

$$\#\mathrm{RA}(\mathcal{A}) \cdot w(\left[\phi^\dagger\right]) = \#\mathrm{RA}(\mathcal{A}') \cdot w(\left[\phi\right])\,. \tag{1}$$

3.2. **Reduced automorphism groups of Jacobians.** There are seven possible reduced automorphism groups for Jacobian surfaces (provided $p > 5$; see [1]). Figure 1 gives the taxonomy of Jacobian surfaces by reduced automorphism group, using Bolza's names ("types") for the classes of Jacobian surfaces with each of the reduced automorphism groups (we add Type-A for the Jacobians with trivial reduced automorphism group). We will give normal forms for each type in §4.

We can identify the isomorphism class of a Jacobian using the Clebsch invariants:

$$\left[\mathcal{J}(\mathcal{C})\right] \longleftrightarrow (A : B : C : D) \in \mathbb{P}(2,4,6,10)(\Bbbk)\,,$$

where A, B, C, and D are homogeneous polynomials of degree 2, 4, 6, and 10 in the coefficients of the sextic defining $\mathcal{C}$ (see [17, §1]). They should be seen as coordinates on the weighted projective space $\mathbb{P}(2,4,6,10)$: that is,

$$(A : B : C : D) = (\lambda^2 A : \lambda^4 B : \lambda^6 C : \lambda^{10} D) \quad \text{for all } \lambda \neq 0 \in \overline{\Bbbk}\,.$$

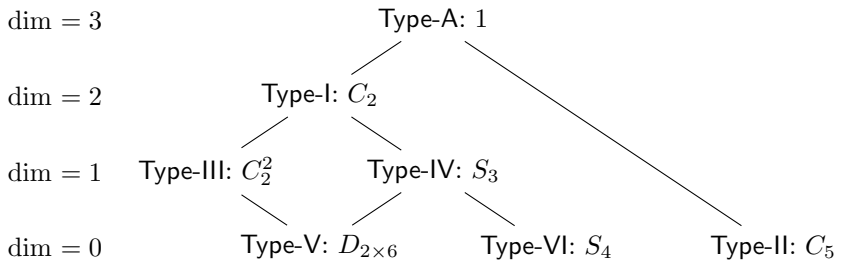


FIGURE 1. Reduced automorphism groups for genus-2 Jacobians. Dimensions are of the corresponding loci in the 3-dimensional moduli space of PPASes. Lines connect sub- and super-types.

We will not define $(A : B : C : D)$ explicitly here; in practice, we compute them using (e.g.) `ClebschInvariants` in Magma [2] or `clebsch_invariants` in Sage [20].

To determine $\mathrm{RA}(\mathcal{J}(\mathcal{C}))$ for a given $\mathcal{C}$, we use Bolza's criteria on Clebsch invariants given in Table 1. We will need some derived invariants (see [17]): let

$$A_{11} = 2C + \frac{1}{3}AB\,, \qquad A_{12} = \frac{2}{3}(B^2 + AC)\,, \qquad A_{23} = \frac{1}{2}B \cdot A_{12} + \frac{1}{3}C \cdot A_{11}\,,$$
$$A_{22} = D\,, \qquad A_{31} = D\,, \qquad A_{33} = \frac{1}{2}B \cdot A_{22} + \frac{1}{3}C \cdot A_{12}\,,$$

and let R be defined by $2R^2 = \det(A_{ij})$ (we will only need to know whether $R = 0$).

Type	Conditions on Clebsch invariants
Type-A	$R \neq 0$, $(A : B : C : D) \neq (0 : 0 : 0 : 1)$
Type-I	$R = 0$, $A_{11}A_{22} \neq A_{12}$
Type-II	$(A : B : C : D) = (0 : 0 : 0 : 1)$
Type-III	$BA_{11} - 2AA_{12} = -6D$, $CA_{11} + 2BA_{12} = AD$, $6C^2 \neq B^3$, $D \neq 0$
Type-IV	$6C^2 = B^3$, $3D = 2BA_{11}$, $2AB \neq 15C$, $D \neq 0$
Type-V	$6B = A^2$, $D = 0$, $A_{11} = 0$, $A \neq 0$
Type-VI	$(A : B : C : D) = (1 : 0 : 0 : 0)$

TABLE 1. Determining the RA-type of $\mathcal{J}(\mathcal{C})$ from its Clebsch invariants.

3.3. **Reduced automorphism groups of elliptic products.** There are seven possible reduced automorphism groups for elliptic product surfaces [8, Prop. 3]. Figure 2 shows the taxonomy of elliptic product surfaces by reduced automorphism group. The names ("types") for the classes of surfaces are taken from [8].

Every elliptic product $\mathcal{E} \times \mathcal{E}'$ has an involution $\sigma = [1] \times [-1]$ in $\mathrm{RA}(\mathcal{E} \times \mathcal{E}')$. If $\mathcal{E} \cong \mathcal{E}'$ then there is also the involution τ exchanging the factors of the product. The situation is more complicated if either or both factors are isomorphic to one of

$$\mathcal{E}_0 : y^2 = x^3 - 1 \qquad \text{with} \qquad \mathrm{Aut}(\mathcal{E}_0) = \langle \zeta : (x, y) \mapsto (\zeta_3 x, -y) \rangle \cong C_6$$

where ζ_3 is a primitive 3rd root of unity, or

$$\mathcal{E}_{12^3} : y^2 = x^3 - x \qquad \text{with} \qquad \mathrm{Aut}(\mathcal{E}_{12^3}) = \langle \iota : (x, y) \mapsto (-x, \sqrt{-1}y) \rangle \cong C_4\,.$$

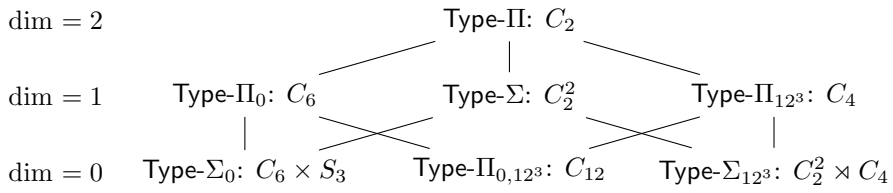


FIGURE 2. Reduced automorphism groups of elliptic products. Dimensions are of the corresponding loci in the 3-dimensional moduli space of PPASes. Lines connect sub- and super-types.

When constructing isogenies, we label the 2-torsion of $\mathcal{E}_0$ and $\mathcal{E}_{12^3}$ as follows:

$$\mathcal{E}_0[2] = \{0, P_1 = (1,0), P_2 = (\zeta_3, 0), P_3 = (\zeta_3^2, 0)\},$$
$$\mathcal{E}_{12^3}[2] = \{0, P_1 = (1,0), P_2 = (-1, 0), P_3 = (0,0)\}.$$

When navigating isogeny graphs, we can identify the isomorphism class of an elliptic product using the pair of j-invariants of the factors:

$$\left[\mathcal{E}_1 \times \mathcal{E}_2\right] \longleftrightarrow \{j(\mathcal{E}_1), j(\mathcal{E}_2)\}.$$

To determine $\mathrm{RA}(\mathcal{E}_1 \times \mathcal{E}_2)$, we can use the criteria on j-invariants given in Table 2.

Type	Conditions	Type	Conditions
Type-Π	$\{j(\mathcal{E}_1), j(\mathcal{E}_2)\} \cap \{0, 1728\} = \emptyset$	Type-Σ	$j(\mathcal{E}_1) = j(\mathcal{E}_2)$, $j(\mathcal{E}_i) \notin \{0, 1728\}$
Type-Π_0	$j(\mathcal{E}_1) = 0$ or $j(\mathcal{E}_2) = 0$		
Type-Π_{12^3}	$j(\mathcal{E}_1) = 1728$ or $j(\mathcal{E}_2) = 1728$	Type-Σ_0	$j(\mathcal{E}_1) = j(\mathcal{E}_2) = 0$
Type-$\Pi_{0,12^3}$	$\{j(\mathcal{E}_1), j(\mathcal{E}_2)\} = \{0, 1728\}$	Type-Σ_{12^3}	$j(\mathcal{E}_1) = j(\mathcal{E}_2) = 1728$

TABLE 2. Determining the RA-type of an elliptic product $\mathcal{E}_1 \times \mathcal{E}_2$.

3.4. **Superspecial vertices.** Ibukiyama, Katsura, and Oort have computed the precise number of superspecial genus-2 Jacobians (up to isomorphism) of each reduced automorphism type [12, Theorem 3.3]. We reproduce their results for $p > 5$, completing them with the number of superspecial elliptic products of each automorphism type (which can be easily derived from the well-known formula for the number of supersingular elliptic curves over $\mathbb{F}_{p^2}$) in Table 3.

Definition 3. *For each prime $p > 5$, we define the following quantities:*

- $\epsilon_{1,p} = 1$ *if* $p \equiv 3 \pmod 4$, *0 otherwise;*
- $\epsilon_{2,p} = 1$ *if* $p \equiv 5, 7 \pmod 8$, *0 otherwise;*
- $\epsilon_{3,p} = 1$ *if* $p \equiv 2 \pmod 3$, *0 otherwise;*
- $\epsilon_{5,p} = 1$ *if* $p \equiv 4 \pmod 5$, *0 otherwise;*
- $N_p = (p-1)/12 - \epsilon_{1,p}/2 - \epsilon_{3,p}/3$.

Note that N_p, $\epsilon_{1,p}$, and $\epsilon_{3,p}$ count the isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with reduced automorphism group of order 1, 2, *and* 3, *respectively.*

If the reader chooses suitable values of p and computes $\Gamma_2^{SS}(2;p)$, then they will find graphs built from overlapping copies of the neighbourhoods described in §4. We will see that $\Gamma_2^{SS}(2;p)$ is much more complicated than the elliptic 2-isogeny graph.

Type	Vertices in $\Gamma_2^{SS}(2;p)$	Type	Vertices in $\Gamma_2^{SS}(2;p)$
Type-I	$\frac{1}{48}(p-1)(p-17)$ $+\frac{1}{4}\epsilon_{1,p}+\epsilon_{2,p}+\epsilon_{3,p}$	Type-Π	$\frac{1}{2}N_p(N_p-1)$
		Type-Π_0	$\epsilon_{3,p}N_p$
Type-II	$\epsilon_{5,p}$	Type-Π_{12^3}	$\epsilon_{1,p}N_p$
Type-III	$\frac{3}{2}N_p+\frac{1}{2}\epsilon_{1,p}-\frac{1}{2}\epsilon_{2,p}-\frac{1}{2}\epsilon_{3,p}$	Type-$\Pi_{0,12^3}$	$\epsilon_{1,p}\cdot\epsilon_{3,p}$
Type-IV	$2N_p+\epsilon_{1,p}-\epsilon_{2,p}$	Type-Σ	N_p
Type-V	$\epsilon_{3,p}$	Type-Σ_0	$\epsilon_{3,p}$
Type-VI	$\epsilon_{2,p}$	Type-Σ_{12^3}	$\epsilon_{1,p}$
Type-A	$\frac{1}{2880}(p-1)(p^2-35p+346)-\frac{1}{16}\epsilon_{1,p}-\frac{1}{4}\epsilon_{2,p}-\frac{2}{9}\epsilon_{3,p}-\frac{1}{5}\epsilon_{5,p}$		

TABLE 3. The number of superspecial vertices of each RA-type.

4. An atlas of the Richelot isogeny graph

We are now ready to compute the neighbourhoods of each type of vertex and edge in the Richelot isogeny graph. We begin with general (Type-A) vertices, before considering each type with an involution, in order of increasing speciality, and ending with Type-II (which has no involution).

4.1. **The algorithm.** We compute each vertex neighbourhood in the same way:

(1) Take the generic curve or product for the RA-type. We use Bolza's normal forms for the curves with special reduced automorphism groups from Bolza [1], reparametrizing to force full rational 2-torsion in the Jacobians.
(2) Enumerate the $(2,2)$-isogeny kernels.
(3) Compute the action of the reduced automorphism group.
(4) For each orbit, choose a representative kernel, compute the codomain using the formulæ of §2.1 and §2.2, and identify the RA-type of the codomain using the criteria of Tables 1 and 2. The orbit sizes give edge weights.

For subsequent isogenies, we repeat Steps (2), (3), and (4) from the current vertex.

4.2. **Diagram notation.** In all of our diagrams, **solid vertices** have definite types, and **solid edges** have definite weights. The **dotted vertices** have an indicative type, but may change type under specialization, acquiring more automorphisms, with the weight of **dotted edges** increasing proportionally according to Eq. (1). For example: in Figure 3, if one of the dotted neighbours specializes to a Type-I vertex, then the returning dotted arrow will become a weight-2 arrow. All edges from solid vertices are shown; some edges from dotted vertices, especially to vertices outside the diagram, are omitted for clarity.

4.3. **General vertices and edges.** Figure 3 shows the neighbourhood of a Type-A vertex: there are weight-1 edges to fifteen neighbouring vertices, generally all Type-A, and a weight-1 dual edge returning from each of them.

The Richelot isogeny graph is 15-regular (counting weights), and it is tempting to imagine that locally, the graph looks like an assembly of copies of the star in Figure 3, with each outer vertex becoming the centre of its own star. However, the reality is more complicated. If we look at a pair of neighbouring Type-A vertices, then six of the neighbours of one are connected to neighbours of the other. Figure 4 shows this configuration.

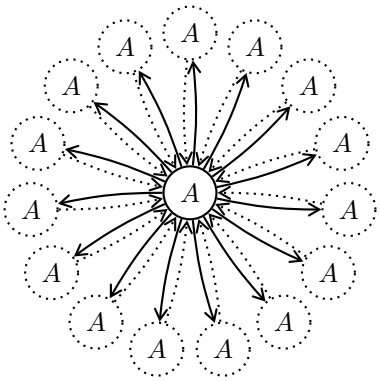


FIGURE 3. The neighbourhood of a Type-A vertex.

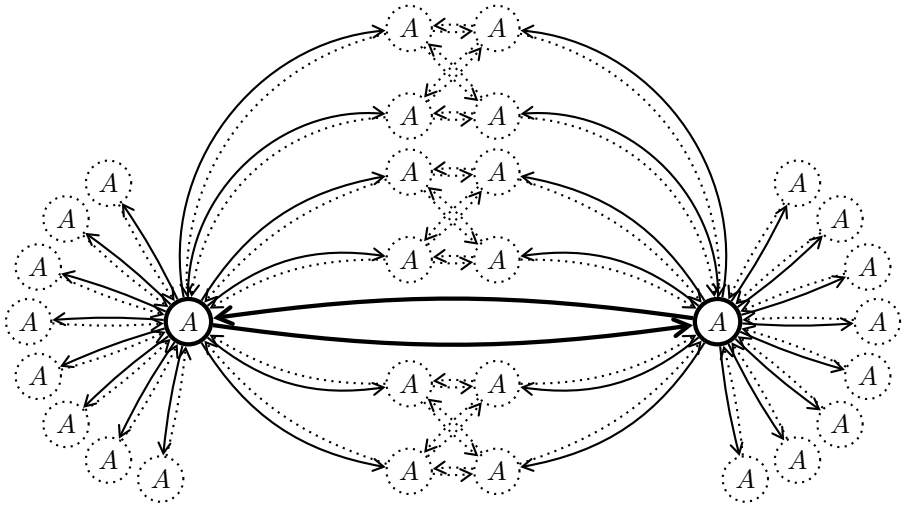


FIGURE 4. The neighbourhood of a general edge and its dual.

The interconnections in Figure 4 are explained as follows. For each $(2,2)$-isogeny $\phi : \mathcal{A}_1 \to \mathcal{A}_2$, there are *twelve* $(4,4,2,2)$-isogenies (each a composition of three $(2,2)$-isogenies) from $\mathcal{A}_1$ to $\mathcal{A}_2$; composing any of these with $\phi^\dagger$ defines a cycle of length 4 in the graph, which is isomorphic to multiplication-by-4 on $\mathcal{A}_1$. These cycles of length 4 are the "small cycles" exploited by Flynn and Ti in [9, §2.3]. In contrast, composing a central isogeny with one of the eight isogenies from the far left or the eight from the far right of Figure 4 yields a $(4,4)$-isogeny, and composing with one of each yields an $(8,8)$-isogeny. In the terminology of [5], the isogenies at the far left and far right are "good" extensions of the central pair, while those forming the adjacent edges of squares are "bad" extensions of each other.

This pattern is replicated throughout the Richelot isogeny graph: each edge is common to twelve of these 4-cycles (counting weights as multiplicities).

4.4. **General elliptic products: Type-Π vertices.** The general Type-Π vertex is an elliptic product vertex $\left[\mathcal{E} \times \mathcal{E}'\right]$ where $\mathcal{E}' \ncong \mathcal{E}$, and neither $\mathcal{E}$ nor $\mathcal{E}'$ has special

automorphisms. In this case $\mathrm{RA}(\mathcal{E}\times\mathcal{E}') = \langle\sigma\rangle \cong C_2$, which fixes every $(2,2)$-isogeny kernel, so we have a subgroup isomorphic to C_2 in the reduced automorphism group of every $(2,2)$-isogeny codomain. The nine elliptic product neighbours are generally Type-Π; the six Jacobian neighbours are generally Type-I, the most general type with a reduced involution. The situation is illustrated at the left of Figure 5.

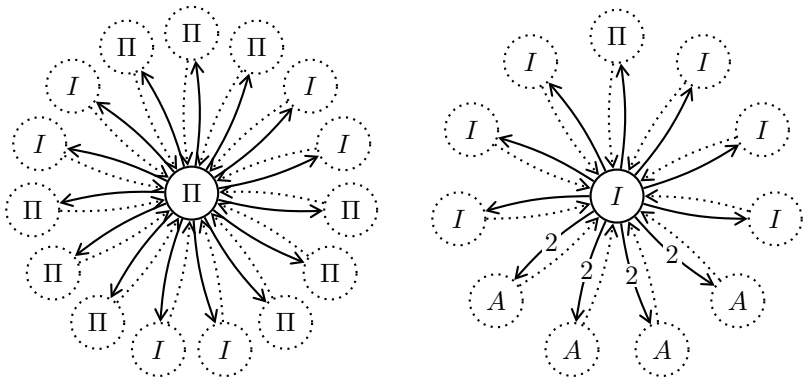


FIGURE 5. Neighbourhoods of the general Type-Π and Type-I vertices.

Remark 1. Looking at Figure 5, we see that Type-Π vertices cannot have Type-A or Type-II neighbours: any walk in the graph from a Type-A vertex to an elliptic product must have already passed through a vertex with an involution in its reduced automorphism group. We will see below that the same applies to any elliptic product or square vertex, as well as to Type-IV, Type-V, and Type-VI vertices.

4.5. **Type-I vertices.** The generic Type-I vertex is $\left[\mathcal{J}(\mathcal{C}_I)\right]$, where $\mathcal{C}_I$ is defined by

$$\mathcal{C}_I : y^2 = F_I(x) := (x^2-1)(x^2-s^2)(x^2-t^2)$$

with parameters s and t. Any Jacobian $\mathcal{A}_0$ with $C_2 \subseteq \mathrm{RA}(\mathcal{A}_0)$ (that is, Type-I, Type-III, Type-IV, Type-V, or Type-VI) is isomorphic to the Jacobian of $\mathcal{J}(\mathcal{C}_I)$ for some (s,t) such that $st(s^2-1)(t^2-1)(s^2-t^2) \neq 0$.

There are maximal 2-Weil isotropic subgroups $K_1, \ldots, K_{15}$ of $\mathcal{J}(\mathcal{C}_I)[2]$; each is the kernel of a $(2,2)$-isogeny $\mathcal{J}(\mathcal{C}_I) = \mathcal{A}_0 \to \mathcal{A}_i = \mathcal{A}_0/K_i$. The kernels K_i correspond to the following quadratic splittings. First:

$$K_1 \leftrightarrow \{x^2-1, x^2-s^2, x^2-t^2\}.$$

These three quadratics are linearly dependent, so $\mathcal{A}_1 \cong \mathcal{E}\times\mathcal{E}'$ with factors $\mathcal{E} : y^2 = (x-1)(x-s^2)(x-t^2)$ and $\mathcal{E}' : y^2 = (x-1)(x-1/s^2)(x-1/t^2)$.

Six of the kernels share a nontrivial element with K_1, namely

$$\begin{aligned}
K_2 &\leftrightarrow \{x^2-1, x^2 \pm (s+t)x + st\}, & K_3 &\leftrightarrow \{x^2-1, x^2 \pm (s-t)x - st\},\\
K_4 &\leftrightarrow \{x^2-s^2, x^2 \pm (t+1)x + t\}, & K_5 &\leftrightarrow \{x^2-s^2, x^2 \pm (t-1)x - t\},\\
K_6 &\leftrightarrow \{x^2-t^2, x^2 \pm (s+1)x + s\}, & K_7 &\leftrightarrow \{x^2-t^2, x^2 \pm (s-1)x - s\}.
\end{aligned}$$

The last eight kernels do not share any nontrivial elements with K_1, namely

$$\begin{aligned}
K_8 &\leftrightarrow \{x^2+(s-1)x-s, x^2-(t-1)x-t, x^2-(s-t)x-st\},\\
K_9 &\leftrightarrow \{x^2-(s-1)x-s, x^2+(t-1)x-t, x^2+(s-t)x-st\},\\
K_{10} &\leftrightarrow \{x^2-(s-1)x-s, x^2-(t+1)x+t, x^2+(s+t)x+st\},\\
K_{11} &\leftrightarrow \{x^2+(s-1)x-s, x^2+(t+1)x+t, x^2-(s+t)x+st\},\\
K_{12} &\leftrightarrow \{x^2+(s+1)x+s, x^2+(t-1)x-t, x^2-(s+t)x+st\},\\
K_{13} &\leftrightarrow \{x^2-(s+1)x+s, x^2-(t-1)x-t, x^2+(s+t)x+st\},\\
K_{14} &\leftrightarrow \{x^2+(s+1)x+s, x^2-(t+1)x+t, x^2-(s-t)x-st\},\\
K_{15} &\leftrightarrow \{x^2-(s+1)x+s, x^2+(t+1)x+t, x^2+(s-t)x-st\}.
\end{aligned}$$

The reduced automorphism group is $\mathrm{RA}(\mathcal{C}_I) = \langle\sigma\rangle \cong C_2$, where σ acts as

$$\sigma_* : x \longleftrightarrow -x$$

on x-coordinates, and on (the indices of) the set of kernels $\{K_1, \ldots, K_{15}\}$ via

$$\sigma_* = (1)(2)(3)(4)(5)(6)(7)(8,9)(10,11)(12,13)(14,15)\,.$$

The orbits of the kernel subgroups under σ and the types of the corresponding neighbours are listed in Table 4. The situation is illustrated on the right of Figure 5.

Kernel orbit	Stabilizer	Codomain	Kernel orbit	Stabilizer	Codomain
$\{K_1\}$	$\langle\sigma\rangle$	Type-II	$\{K_7\}$	$\langle\sigma\rangle$	Type-I
$\{K_2\}$	$\langle\sigma\rangle$	Type-I	$\{K_{8,9}\}$	1	Type-A
$\{K_3\}$	$\langle\sigma\rangle$	Type-I	$\{K_{10,11}\}$	1	Type-A
$\{K_4\}$	$\langle\sigma\rangle$	Type-I	$\{K_{12,13}\}$	1	Type-A
$\{K_5\}$	$\langle\sigma\rangle$	Type-I	$\{K_{14,15}\}$	1	Type-A
$\{K_6\}$	$\langle\sigma\rangle$	Type-I			

TABLE 4. Edge data for the generic Type-I vertex.

Computing one isogeny step beyond each Type-I neighbour of $\big[\mathcal{J}(\mathcal{C}_I)\big]$, we find six neighbours of $\big[\mathcal{E}\times\mathcal{E}'\big]$; thus we complete Figure 6, which shows the neighbourhood of the edge $\big[\phi_1\big]$ and its dual, $\big[\phi_1^\dagger\big] = \big[\phi_{Id}\big]$. This should be compared with Figure 4. Note that $\phi_i \circ \phi_1^\dagger$ is a $(4,2,2)$- resp. $(4,4)$-isogeny for $2 \le i \le 7$ resp. $8 \le i \le 15$.

4.6. **General elliptic squares: Type-Σ vertices.** The general Type-Σ vertex is $\big[\mathcal{E}\times\mathcal{E}\big]$ where $\mathcal{E}$ has no special automorphisms, so $\mathrm{RA}(\mathcal{E}^2) = \langle\sigma,\tau\rangle \cong C_2^2$. The orbits of the kernel subgroups under $\mathrm{RA}(\mathcal{E}^2)$ (with respect to an arbitrary labelling of $\mathcal{E}[2]$) and the types of the corresponding neighbours are described by Table 5, and the neighbourhood of the generic Type-Σ vertex is shown on the left of Figure 7.

4.7. **Type-III vertices.** The generic Type-III vertex is $\big[\mathcal{J}(\mathcal{C}_{III})\big]$, where

$$\mathcal{C}_{III} : y^2 = (x^2-1)(x^2-u^2)(x^2-1/u^2)$$

with u a free parameter; note that $\mathcal{C}_{III}(u) = \mathcal{C}_I(s,t)$ with $(s,t) = (u,u^{-1})$. We have $\mathrm{RA}(\mathcal{J}(\mathcal{C})_{III}) = \langle\sigma,\tau\rangle \cong C_2^2$, where σ is inherited from Type-I and τ acts on x-coordinates via

$$\tau_* : x \longmapsto 1/x\,.$$

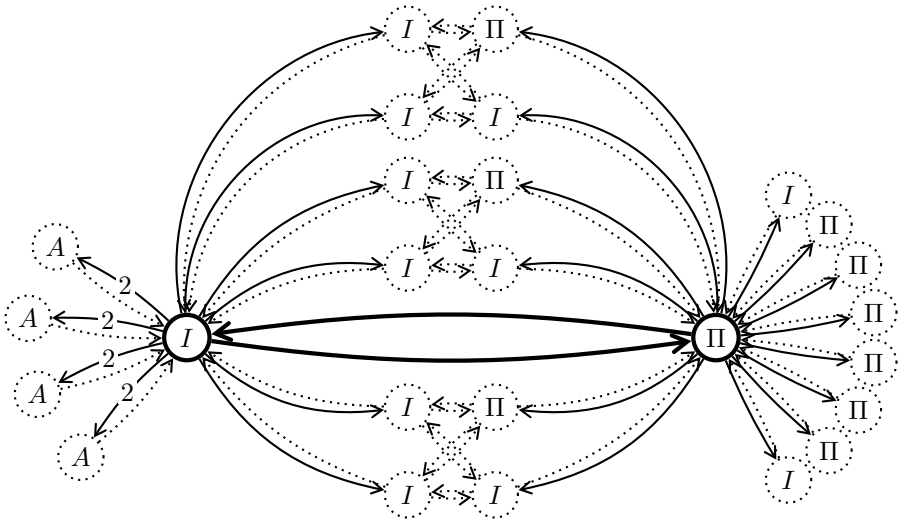


FIGURE 6. The neighbourhood of a general Type-I vertex and its Type-Π neighbour.

Kernel orbit	Stab.	Codomain	Kernel orbit	Stab.	Codomain
$\{K_{1,1}\}$	$\langle\sigma,\tau\rangle$	Type-Σ	$\{K_{\mathrm{Id}}\}$	$\langle\sigma,\tau\rangle$	(loop)
$\{K_{2,2}\}$	$\langle\sigma,\tau\rangle$	Type-Σ	$\{K_{(1,2)(3)}\}$	$\langle\sigma,\tau\rangle$	Type-III
$\{K_{3,3}\}$	$\langle\sigma,\tau\rangle$	Type-Σ	$\{K_{(1,3)(2)}\}$	$\langle\sigma,\tau\rangle$	Type-III
$\{K_{1,2},K_{2,1}\}$	$\langle\sigma\rangle$	Type-Π	$\{K_{(2,3)(1)}\}$	$\langle\sigma,\tau\rangle$	Type-III
$\{K_{1,3},K_{3,1}\}$	$\langle\sigma\rangle$	Type-Π	$\{K_{(1,2,3)},K_{(1,3,2)}\}$	$\langle\sigma\rangle$	Type-I
$\{K_{2,3},K_{3,2}\}$	$\langle\sigma\rangle$	Type-Π			

TABLE 5. Edge data for the generic Type-Σ vertex.

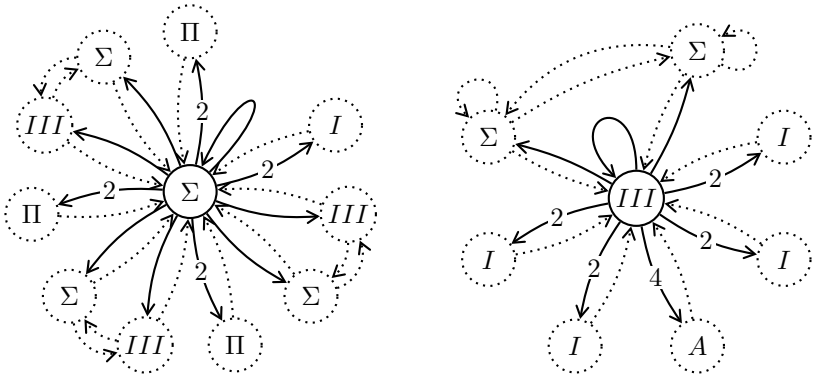


FIGURE 7. Neighbourhoods of the general Type-Σ and Type-III vertices.

Specializing the kernels and quadratic splittings of §4.5 at $(s,t)=(u,u^{-1})$, we see that $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{III}))$ acts on the kernel indices by

$$\sigma_* = (1)(2)(3)(4)(5)(6)(7)(8,9)(10,11)(12,13)(14,15)\,,$$
$$\tau_* = (1)(2)(3)(4,6)(5,7)(8)(9)(10,13)(11,12)(14)(15)\,.$$

The kernel orbits and the edges leaving $\big[\mathcal{J}(\mathcal{C}_{III})\big]$ are described in Table 6.

Orbit	Stab.	Codomain	Orbit	Stab.	Codomain
$\{K_1\}$	$\langle\sigma,\tau\rangle$	Type-Σ	$\{K_5, K_7\}$	$\langle\sigma\rangle$	Type-I
$\{K_2\}$	$\langle\sigma,\tau\rangle$	(loop)	$\{K_8, K_9\}$	$\langle\tau\rangle$	Type-I
$\{K_3\}$	$\langle\sigma,\tau\rangle$	Type-Σ	$\{K_i : 10 \le i \le 13\}$	1	Type-A
$\{K_4, K_6\}$	$\langle\sigma\rangle$	Type-I	$\{K_{14}, K_{15}\}$	$\langle\tau\rangle$	Type-I

TABLE 6. Edge data for the generic Type-III vertex.

We observe that $\mathcal{J}(\mathcal{C}_{III})/K_2 \cong \mathcal{J}(\mathcal{C}_{III})$: that is, ϕ_2 is a $(2,2)$-endomorphism of $\mathcal{J}(\mathcal{C}_{III})$, so $\big[\phi_2\big]$ is a weight-1 loop. The kernels K_1 and K_3 are stabilised by $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{III}))$ and $\delta(K_1) = \delta(K_3) = 0$, so $\big[\phi_1\big]$ and $\big[\phi_2\big]$ are weight-1 edges to Type-Σ vertices $\big[\mathcal{E}^2\big]$ and $\big[(\mathcal{E}')^2\big]$, respectively, where $\mathcal{E}$ and $\mathcal{E}'$ are the elliptic curves

$$\mathcal{E} : y^2 = (x-1)(x-u^2)(x-1/u^2)\,,$$
$$\mathcal{E}' : y^2 = -2\,(x-1)\left(x^2 + 2\frac{u^4-6u^2+1}{(u^2+1)^2}x + 1\right).$$

There is a 2-isogeny $\varphi : \mathcal{E} \to \mathcal{E}'$, as predicted in [10, §4] (in fact $\ker\varphi = \langle(1,0)\rangle$ and $\ker\varphi^\dagger = \langle(1,0)\rangle$), so there are edges $\big[\varphi\times\varphi\big]$ and $\big[\varphi^\dagger\times\varphi^\dagger\big]$ between $\big[\mathcal{E}^2\big]$ and $\big[(\mathcal{E}')^2\big]$. The neighbourhood of the general Type-III vertex is shown on the right of Figure 7. Combining with the Type-Σ neighbourhood and extending to include shared adjacent vertices yields Figure 8.

4.8. **Elliptic 3-isogenies: Type-IV vertices.** The generic Type-IV vertex is represented by $\mathcal{J}(\mathcal{C}_{IV}(v))$, where $\mathcal{C}_{IV}(v) := \mathcal{C}_I(s_{IV}(v), t_{IV}(v))$ with

$$s_{IV}(v) := \frac{(v+1)(v-\zeta_3)}{(v-1)(v+\zeta_3)} \qquad \text{and} \qquad t_{IV}(v) := \frac{(v+1)(v-\zeta_3^2)}{(v-1)(v+\zeta_3^2)}$$

where ζ_3 is a primitive third root of unity and v is a free parameter. We have $\mathrm{RA}(\mathcal{C}_{IV}(v)) = \langle\sigma,\rho\rangle \cong S_3$, where σ is inherited from Type-I and ρ is the order-3 automorphism acting on x-coordinates via

$$\rho_* : x \longmapsto \big((2\zeta_3+1)(v^2-1)x + 3(v+1)^2\big)/\big(3(v-1)^2x + (2\zeta_3+1)(v^2-1)\big)\,.$$

Specializing the kernels and quadratic splittings from §4.5, we see that the action of $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{IV}))$ on (the indices of) the K_i is given by

$$\rho_* = (1,9,8)(2,15,14)(3)(4,12,13)(5)(6,10,11)(7)\,,$$
$$\sigma_* = (1)(2)(3)(4)(5)(6)(7)(8,9)(10,11)(12,13)(14,15)\,.$$

The kernel orbits and the edges leaving $\big[\mathcal{J}(\mathcal{C})_{IV}\big]$ described in Table 7, and illustrated in Figure 9. We find that $\big[\mathcal{A}_1\big] = \big[\mathcal{A}_8\big] = \big[\mathcal{A}_9\big] = \big[\mathcal{E}\times\mathcal{E}'\big]$, where

$$\mathcal{E} : y^2 = (x-1)(x-s_{IV}(v)^2)(x-t_{IV}(v)^2)$$

and

$$\mathcal{E}' : y^2 = (x-1)(x-1/s_{IV}(v)^2)(x-1/t_{IV}(v)^2)\,.$$

There is a 3-isogeny $\Phi : \mathcal{E} \to \mathcal{E}'$, as predicted in [10, §3]: the kernel of Φ is cut out by $x - (v+1)^2/(v-1)^2$, and the kernel of $\Phi^\dagger$ is cut out by $x - (v-1)^2/(v+1)^2$.

Elliptic products with a 3-isogeny between the factors therefore play a special role in the Richelot isogeny graph; we will represent these special Type-II vertices using

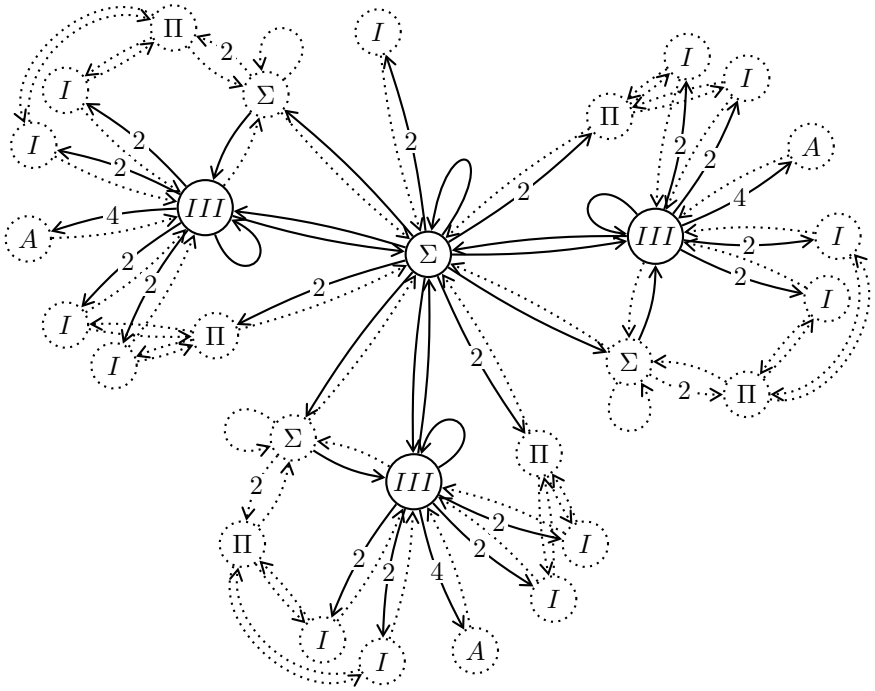


FIGURE 8. The neighbourhood of a generic Type-Σ vertex and its Type-III neighbours.

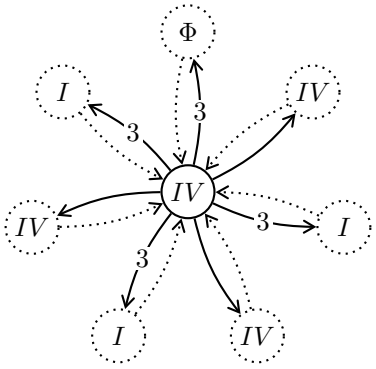


FIGURE 9. The neighbourhood of the general Type-IV vertex.

the symbol Φ. We remark that the presence of the 3-isogeny severely constrains the possible specializations of a Φ-vertex.

Figure 10 shows the neighbourhood of the edges between a general Type-IV vertex and its Φ-neighbour; it should be compared with Figures 4 and 6. Type-IV vertices correspond to Φ-vertices, and edges between Type-IV vertices correspond to edges between Φ-vertices.

Kernel orbit	Stabilizer	Codomain	Kernel orbit	Stabilizer	Codomain
$\{K_1, K_8, K_9\}$	$\langle\sigma\rangle$	Type-Π (Φ)	$\{K_3\}$	$\langle\sigma,\rho\rangle$	Type-IV
$\{K_2, K_{14}, K_{15}\}$	$\langle\sigma\rangle$	Type-I	$\{K_5\}$	$\langle\sigma,\rho\rangle$	Type-IV
$\{K_4, K_{12}, K_{13}\}$	$\langle\sigma\rangle$	Type-I	$\{K_7\}$	$\langle\sigma,\rho\rangle$	Type-IV
$\{K_6, K_{10}, K_{11}\}$	$\langle\sigma\rangle$	Type-I			

TABLE 7. Edge data for the generic Type-IV vertex.

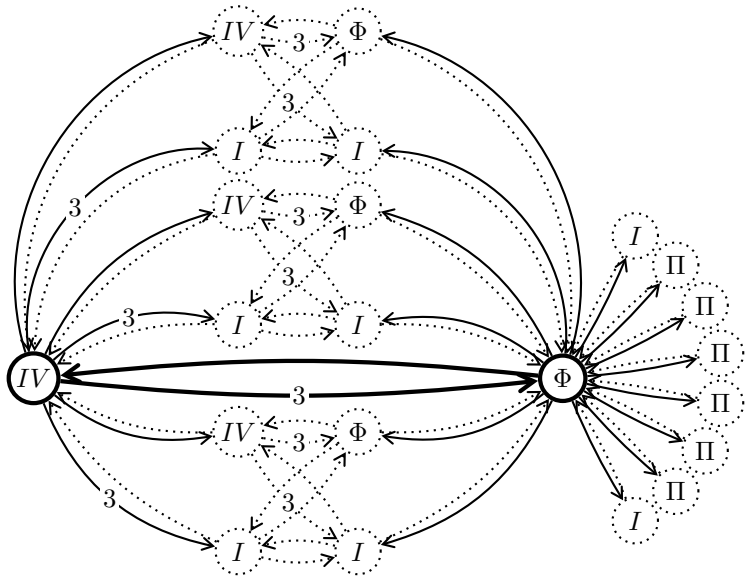


FIGURE 10. The neighbourhood of a Type-IV vertex and its Type-Π neighbour.

4.9. **The Type-Π_0 family.** The Type-Π_0 vertices are $\left[\mathcal{E}\times\mathcal{E}_0\right]$ for elliptic curves $\mathcal{E}\not\cong\mathcal{E}_0$. We have $\mathrm{RA}(\mathcal{E}\times\mathcal{E}_0)=\langle\sigma,[1]\times\zeta\rangle\cong C_6$. The automorphism ζ of $\mathcal{E}_0$ cycles the points of order 2 on $\mathcal{E}_0$, so $[1]\times\zeta$ fixes no $(2,2)$-isogeny kernels. Instead, the kernel subgroups of $\mathcal{E}\times\mathcal{E}_0[2]$ form orbits of three, and so we see the five neighbours with weight-3 edges in Figure 11 (which should be compared with Figure 5).

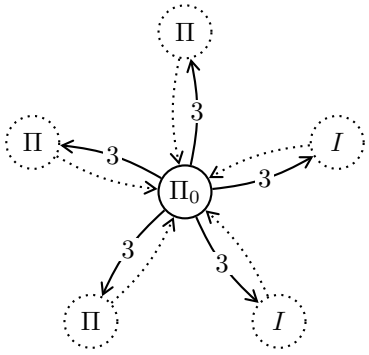


FIGURE 11. The neighbourhood of a generic Type-Π_0 vertex.

4.10. **The Type-Π_{12^3} family.** The Type-Π_{12^3} vertices are $\left[\mathcal{E} \times \mathcal{E}_{12^3}\right]$ for elliptic curves $\mathcal{E} \ncong \mathcal{E}_{12^3}$. The curve $\mathcal{E}_{12^3}$ has an order-4 automorphism ι which fixes one point P_3 of order 2, and exchanges P_1 and P_2. We therefore have an order-4 element $\alpha = [1] \times \iota$ generating $\mathrm{RA}(\mathcal{E} \times \mathcal{E}_{12^3}) \cong C_4$, and $\alpha^2 = [1] \times [-1] = \sigma$ (which fixes all the kernels). Hence, with respect to $\langle \alpha \rangle$, the isometries form three orbits of size two, as do the six product kernels not involving P_3; on the other hand, the kernels $\langle P \rangle \times \langle P_3 \rangle$ are fixed by α, and since $\mathcal{E}_{12^3}/\langle P_1 \rangle \cong \mathcal{E}_{12^3}$ we get three weight-1 edges to Type-Π_{12^3} vertices. The situation is illustrated in Figure 12 (which should be compared with Figure 5).

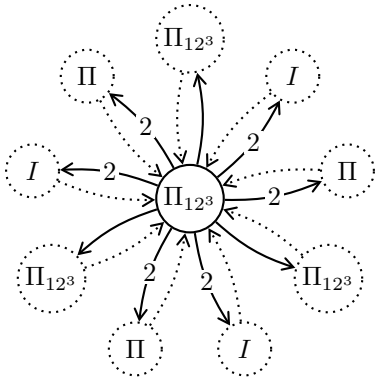


FIGURE 12. The neighbourhoods of the generic Type-Π_{12^3} vertex.

4.11. **The Type-$\Pi_{0,12^3}$ vertex.** The unique Type-$\Pi_{0,12^3}$ vertex is $\left[\mathcal{E}_0 \times \mathcal{E}_{12^3}\right]$. Its reduced automorphism group is $\mathrm{RA}(\mathcal{E}_0 \times \mathcal{E}_{12^3}) = \langle \zeta \times [1], [1] \times \iota \rangle \cong C_{12}$. The kernel orbits and edges can be derived using a combination of the analyses in §4.9 and §4.10; the results are described in Table 8. The neighbourhood of the Type-$\Pi_{0,12^3}$ vertex, illustrated in Figure 13, is a combination of the Type-Π_0 and Type-Π_{12^3} neighbourhoods of Figures 11 and 12.

Kernel orbit	Stabilizer (conjugate)	Codomain type		
		General p	$p = 7$	$p = 11$
$\{K_{1,3}, K_{2,3}, K_{3,3}\}$	$\langle [1] \times \iota \rangle$	Type-Π_{12^3}	Type-Π_{12^3}	Type-Σ_{12^3}
$\{K_{i,j} : 1 \le i \le 3, 1 \le j \le 2\}$	$\langle \sigma \rangle$	Type-Π	Type-Π_{12^3}	(loops)
$\{K_\pi : \pi \in S_3\}$	$\langle \sigma \rangle$	Type-I	Type-I	Type-IV

TABLE 8. Edge data for the unique Type-$\Pi_{0,12^3}$ vertex.

4.12. **The Type-Σ_{12^3} vertex.** The unique Type-Σ_{12^3} vertex is $\left[\mathcal{E}_{12^3}^2\right]$. We have $\mathrm{RA}(\mathcal{E}_{12^3}^2) = \langle \sigma, \tau, [1] \times \iota \rangle \cong C_2^2 \rtimes C_4$. The kernel orbits and edges are described in Table 9. Figure 14, illustrating the neighbourhood of $\left[\mathcal{E}_{12^3}^2\right]$, should be compared with Figure 7.

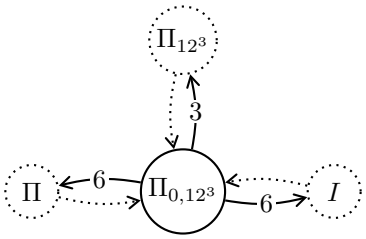


FIGURE 13. The neighbourhood of the Type-$\Pi_{0,12^3}$ vertex.

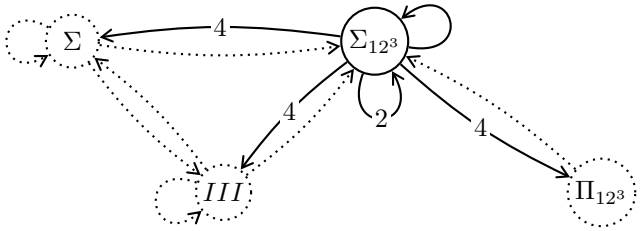


FIGURE 14. The neighbourhood of the Type-Σ_{12^3} vertex. The dotted neighbour types change for $p = 7$ and 11 (see Table 9).

Kernel orbit	Stabilizer (conjugate)	Codomain type General p	$p = 7$	$p = 11$
$\{K_{1,1}, K_{1,2}, K_{2,1}, K_{2,2}\}$	$\langle \sigma, \tau \rangle$	Type-Σ	(loops)	Type-Σ_0
$\{K_{1,3}, K_{2,3}, K_{3,1}, K_{3,2}\}$	$\langle [1] \times \iota \rangle$	Type-Π_{12^3}	(loops)	Type-$\Pi_{0,12^3}$
$\{K_{3,3}\}$	$\mathrm{RA}(\mathcal{E}_{12^3})$	(loop)	(loop)	(loop)
$\{K_{\mathrm{Id}}, K_{(1,2)(3)}\}$	$\langle \tau, \iota \times \iota \rangle$	(loops)	(loops)	(loops)
$\left\{\begin{matrix} K_{(1,2,3)}, K_{(1,3,2)}, \\ K_{(1,3)(2)}, K_{(1)(2,3)} \end{matrix}\right\}$	$\langle \sigma, \tau \rangle$	Type-III	Type-III	Type-V

TABLE 9. Edge data for the unique Type-Σ_{12^3} vertex.

Kernel orbit	Stabilizer (conjugate)	Codomain type General p	$p = 11$
$\{K_{i,j} : 1 \leq i, j \leq 3\}$	$\langle \sigma, \tau \rangle$	Type-Σ	Type-Σ_{12^3}
$\{K_{\mathrm{Id}}, K_{(1,2,3)}, K_{(1,3,2)}\}$	$\langle \tau, \zeta \times (-\zeta) \rangle$	(loop)	(loop)
$\{K_{(1,2)(3)}, K_{(1,3)(2)}, K_{(2,3)(1)}\}$	$\langle \tau, \zeta \times \zeta^2 \rangle$	Type-V	Type-V

TABLE 10. Edge data for the unique Type-Σ_0 vertex.

4.13. **The Type-V and Type-Σ_0 vertices.** The Type-V and Type-Σ_0 vertices are always neighbours, so we treat them simultaneously.

The unique Type-Σ_0 vertex is $\left[\mathcal{E}_0^2\right]$, and $\mathrm{RA}(\mathcal{E}_0^2) = \langle \tau, [1] \times \zeta, \zeta \times [1] \rangle / \langle -1 \rangle \cong C_6 \times S_3$. The kernel orbits and edges are described in Table 10.

The unique Type-V vertex is $\left[\mathcal{J}(\mathcal{C}_V)\right]$, where $\mathcal{C}_V : y^2 = x^6 + 1$; note that $\mathcal{C}_V = \mathcal{C}_{III}(\zeta_6) = \mathcal{C}_I(\zeta_6, 1/\zeta_6)$, where ζ_6 is a primitive sixth root of unity. We

have $\mathrm{RA}(\mathcal{C}_V) = \langle \sigma, \tau, \zeta \rangle$, where σ and τ are inherited from $\mathcal{C}_{III}$, and ζ is a new automorphism of order 6 such that $\zeta^3 = \sigma$. Specializing the kernels and quadratic splittings from §4.5, these automorphisms act on (the indices of) the K_i via

$$\begin{aligned} \tau_* &= (1)(2)(3)(4,6)(5,7)(8,9)(10,13)(11,12)(14,15)\,, \\ \zeta_* &= (1)(2,4,6)(3,5,7)(8,9)(10,14,12,11,15,13)\,, \\ \sigma_* = \zeta_*^3 &= (1)(2)(3)(4)(5)(6)(7)(8,9)(10,11)(12,13)(14,15)\,. \end{aligned}$$

The kernel orbits and edges are described in Table 11.

Figure 15 illustrates the shared neighbourhood of the Type-V and Type-Σ_0 vertices for general p; it should be compared with Figure 7. The Type-I neighbour of the Type-V vertex always has four $(2,2)$-endomorphisms, and they are included here for completeness, as well as the Type-I and Type-II neighbours of the Type-IV vertex, since these are also connected to the Type-Σ and Type-I neighbours. Dashed neighbour types may change for $p = 11$, 17, 29, and 41 (see Table 11).

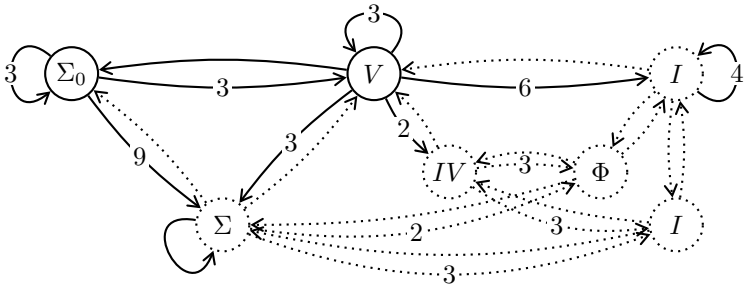


FIGURE 15. The neighbourhood of the Type-V and Type-Σ_0 vertices.

Kernel orbit	Stabilizer (conj.)	Codomain type				
		General p	$p = 11$	$p = 17$	$p = 29$	$p = 41$
$\{K_1\}$	$\langle \tau, \zeta \rangle$	Type-Σ_0	Type-Σ_0	Type-Σ_0	Type-Σ_0	Type-Σ_0
$\{K_2, K_4, K_6\}$	$\langle \sigma, \tau \rangle$	(loops)	(loops)	(loops)	(loops)	(loops)
$\{K_3, K_5, K_7\}$	$\langle \sigma, \tau \rangle$	Type-Σ	Type-Σ_{12^3}	Type-Σ	Type-Σ	Type-Σ
$\{K_8, K_9\}$	$\langle \tau\zeta, \zeta^2 \rangle$	Type-IV	Type-IV	Type-IV	Type-VI	Type-IV
$\{K_i : 10 \le i \le 15\}$	$\langle \sigma\tau \rangle$	Type-I	Type-IV	(loops)	Type-I	Type-III

TABLE 11. Edge data for the Type-V vertex

Remark 2. To see the Type-V neighbourhood in Figure 15 as a specialization of the Type-IV diagram (Figure 9):

- the Type-II neighbour specializes to $[\mathcal{E}]^2$, where $\mathcal{E}$ has j-invariant 54000 and an endomorphism of degree 3;
- one of the Type-IV neighbours degenerates to Type-Σ_0;
- the other two Type-IV neighbours merge, yielding a weight-2 edge;
- one of the Type-I neighbours specializes to Type-V, yielding a loop;
- the other two Type-I neighbours merge, yielding a weight-6 edge.

4.14. **The Type-VI vertex.** The unique Type-VI vertex is $\big[\mathcal{J}(\mathcal{C}_{VI})\big]$, where $\mathcal{C}_{VI} = \mathcal{C}_{IV}(v_{VI})$ with $v_{VI} = (\zeta_{12}^2+\zeta_{12}+1)/\sqrt{2}$ where $\zeta_{12}^2 = \zeta_6$. This curve is isomorphic to Bolza's Type-VI normal form $y^2 = x(x^4+1)$. We have $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{VI})) = \langle\sigma,\rho,\omega\rangle \cong S_4$, where σ and ρ are inherited from $\mathcal{C}_{III}$ and ω is an order-4 automorphism acting as

$$\omega_* : x \longmapsto (x-(\sqrt{2}+1))/((\sqrt{2}-1)x+1)$$

on x-coordinates. Specializing the splittings of §4.5 at $s = s_{IV}(v_{VI}) = -\zeta_{12}^3\sqrt{2}-\zeta_{12}^3$ and $t = t_{IV}(v_{VI}) = 2\sqrt{2}+3$, we see that $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{VI}))$ acts as

$$\begin{aligned}\sigma_* &= (1)(2)(3)(4)(5)(6)(7)(8,9)(10,11)(12,13)(14,15)\,,\\ \rho_* &= (1,9,8)(2,15,14)(3)(4,12,13)(5)(6,10,11)(7)\,,\\ \omega_* &= (1,4)(2,14,7,15)(3,10,6,11)(5)(8,9,13,12)\end{aligned}$$

on kernel indices. Table 12 describes the kernel orbits and edges. It is interesting to compare this with Table 7, to see how the various neighbours degenerate, specialize, and merge. The Type-Σ neighbour is special: it is $\big[\mathcal{E}^2\big]$ where $\mathcal{E}$ is an elliptic curve of j-invariant 8000; it is Φ, because $\mathcal{E}$ has a degree-3 endomorphism. Pushing one step beyond the Type-IV neighbours, we find new Type-I and Φ vertices connected to $\big[\mathcal{E}^2\big]$, and we thus complete the neighbourhood shown in Figure 16.

Kernel orbit	Stabilizer (conjugate)	Codomain type		
		General p	$p=7$	$p=13,29$
$\{K_1,K_4,K_8,K_9,K_{12},K_{13}\}$	$\langle\sigma,\omega^2\rangle$	Type-Σ	Type-Σ_{12^3}	Type-Σ
$\{K_3,K_6,K_{10},K_{11}\}$	$\langle\sigma,\rho\rangle$	Type-IV	(loops)	Type-IV/V
$\{K_2,K_7,K_{14},K_{15}\}$	$\langle\sigma,\rho\rangle$	Type-IV	(loops)	Type-V/IV
$\{K_5\}$	$\mathrm{RA}(\mathcal{J}(\mathcal{C}_{VI}))$	(loop)	(loop)	(loop)

TABLE 12. Edge data for the Type-VI vertex. For $p = 13$ and $p = 29$, one of the two Type-IV neighbours specializes to Type-V, depending on the choice of ζ_{12}.

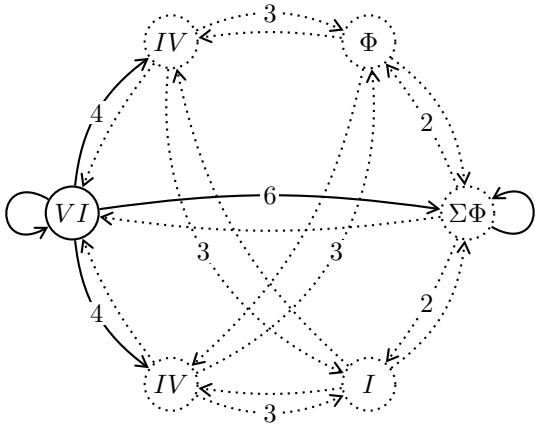


FIGURE 16. The neighbourhood of the Type-VI vertex. The dotted neighbours change type for $p = 7$, 13, and 29 (see Table 12).

4.15. **The Type-II vertex.** The unique Type-II vertex is $\left[\mathcal{J}(\mathcal{C}_{II})\right]$ where $\mathcal{C}_{II}$ is defined by $y^2 = x^5 - 1$; we have $\mathrm{RA}(\mathcal{J}(\mathcal{C}_{II})) = \langle\zeta\rangle \cong C_5$, where ζ acts as

$$\zeta_* : x \longmapsto \zeta_5 x\,.$$

The 15 kernel subgroups of $\mathcal{J}(\mathcal{C}_{II})[2]$ form three orbits of five under the action of ζ. We fix orbit representatives

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

and let $\phi_i : \mathcal{J}(\mathcal{C}_{II}) \to \mathcal{A}_i := \mathcal{J}(\mathcal{C}_{II})/K_i$ be the quotient isogenies for $1 \le i \le 3$. Equation (1) tells us that $w(\left[\phi_i\right]) = 5$ for each i.

The neighbourhood of $\left[\mathcal{J}(\mathcal{C}_{II})\right]$ is shown in Figure 17. Generally, the $\left[\mathcal{A}_i\right]$ are Type-A (because the stabilizer of each orbit is trivial), but for $p = 19$, 29, 59, 79, and 89 the codomain types change (see Table 13). Note that at $p = 19$, the codomain $\mathcal{A}_2$ becomes isomorphic to $\mathcal{A}_0$, so $\left[\phi_2\right]$ becomes a weight-5 loop.

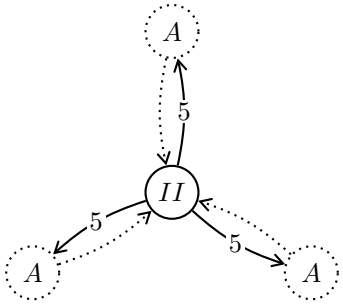


FIGURE 17. The neighbourhood of the (unique) Type-II vertex.

Characteristic p	19	29	59	79	89	Other
Type of $\left[\mathcal{A}_1\right]$	Type-I	Type-I	Type-I	Type-I	Type-A	Type-A
Type of $\left[\mathcal{A}_2\right]$	Type-II	Type-I	Type-A	Type-A	Type-I	Type-A
Type of $\left[\mathcal{A}_3\right]$	Type-III	Type-A	Type-I	Type-A	Type-A	Type-A

TABLE 13. Types of neighbours of the Type-II vertex.

REFERENCES

[1] Oskar Bolza. On binary sextics with linear transformations into themselves. *American Journal of Mathematics*, 10(1):47–70, 1887.

[2] Wieb Bosma, John J. Cannon, Claus Fieker, and Allan Steel. *Handboook of Magma functions*, 2.25 edition, January 2020.

[3] Jean-Benoît Bost and Jean-François Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math. Soc. France*, 38:36–64, 1988.

[4] Bradley W. Brock. *Superspecial curves of genera two and three*. PhD thesis, Princeton University, 1993.

[5] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, 2020. Proceedings of NuTMiC 2019.

[6] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Families of Ramanujan graphs and quaternion algebras. *Groups and symmetries: from Neolithic Scots to John McKay*, 47:53–63, 2009.

[7] Craig Costello and Benjamin Smith. The supersingular isogeny problem in genus 2 and beyond. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, volume 12100 of *Lecture Notes in Computer Science*, pages 151–168. Springer, 2020.

[8] Enric Florit and Benjamin Smith. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. 2020.

[9] E. Victor Flynn and Yan Bo Ti. Genus two isogeny cryptography. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 286–306. Springer, 2019.

[10] Pierrick Gaudry and Éric Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 373–386. Springer, 2001.

[11] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12(3):315–364, 2000.

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

[13] Bruce W. Jordan and Yevgeny Zaytman. Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices, 2020.

[14] Toshiyuki Katsura and Katsuyuki Takashima. Counting richelot isogenies between superspecial abelian surfaces. In Steven D. Galbraith, editor, *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *The Open Book Series*, pages 283–300. MSP, 2020.

[15] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[16] Jean-François Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata)*, pages 217–242, 1986.

[17] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, pages 313–334. Springer, 1991.

[18] Benjamin Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005.

[19] Katsuyuki Takashima. Efficient algorithms for isogeny sequences and their cryptographic applications. In T. Takagi et al., editor, *Mathematical Modelling for Next-Generation Cryptography. Mathematics for Industry*, volume 29, pages 97–114, Singapore, 2018. Springer.

[20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.1)*, 2020. `https://www.sagemath.org`.

[21] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Série A*, 273:238–241, juillet 1971. `https://gallica.bnf.fr/ark:/12148/cb34416987n/date`.

IMUB - Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

Email address: `efz1005@gmail.com`

Inria and Laboratoire d'Informatique de l'École polytechnique (LIX), Institut Polytechnique de Paris, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France

Email address: `smith@lix.polytechnique.fr`