# Expander properties of superspecial isogeny digraphs with level structure

Thomas Decru & Krijn Reijnders

COSIC, KU Leuven

**Abstract.** Charles, Goren and Lauter proved that the supersingular $\ell$-isogeny graph is a Ramanujan graph, which is an optimal expander. Jordan and Zaytman argued that this is no longer true in dimension two, but Florit and Smith showed that those graphs exhibit good expansion properties nonetheless. Castryck, Decru and Smith however have pointed out that the higher-dimensional analogue setting should only consider a subset of all edges, namely the paths corresponding to $(\ell^k, \ell^k)$-isogenies, so-called *good extensions*, instead of all $(\ell^a, \ell^b, \ell^c, \ell^d)$-isogenies in general, which contain bad extensions too. Such bad extensions lead to many small cycles in the graph, which are a cryptographic problem due to collisions and a graph-theoretic nuisance as these superfluous edges counteract part of the expansion properties. Restricting to good extensions makes the resulting graph directed, as outgoing edges now depend on the incoming edge.
We study abelian surfaces with $(\ell, \ell)$-level structure and $(\ell)^g$-isogeny digraphs restricted to good extensions for concrete small dimensions and degrees $\ell$. These graphs exhibit excellent expander properties: by our heuristic evidence, they converge to weakly Ramanujan graphs for all primes $\ell$ in dimension 1, and for $\ell = 2$ in dimension 2. Our main conjecture implies that this would still be the case for $\ell = 3$ in dimension 2, but not for any larger $\ell$ in dimension 2, or any $\ell$ in dimension 3 and up. Furthermore, we generalize the work of Florit and Smith from $\ell = 2$ to general primes $\ell$, by classifying all abelian surfaces with nontrivial automorphism groups and their actions on their maximal isotropic $(\ell, \ell)$-subgroups.

## 1 Introduction

In 2006, Charles Goren and Lauter constructed cryptographic hash functions from expander graphs [CLG09]. One of their constructions relied on computing low-degree isogenies between supersingular elliptic curves over a field of cryptographically large characteristic. Using a trusted setup [BCCF+23, EHLM+18, KLPT14], this hash function is still assumed to be secure and the underlying mathematical structure is used in various other cryptographic protocols

such as SQIsign [FKLP+20] and the - now fallen [CD23, MMPP+23, Rob23] - SIDH [JF11]. Such isogeny graphs are Ramanujan graphs, which are optimal expanders, and Charles, Goren and Lauter have shown in 2009 that they generalize to higher dimensions as well [CGL09]. Unfortunately, this set-up requires using abelian varieties with real multiplication, which is a nontrivial generalization of elliptic curves and a nuisance for cryptographic purposes due to the required overhead.

In 2018, Takashima [Tak18] proposed a leaner - and arguably more natural - version of the two-dimensional hash function, namely abelian surfaces *without* real multiplication, but it was swiftly broken by Flynn and Ti in 2019 [FT19]. Indeed: the composition of two $(\ell, \ell)$-isogenies does not necessarily lead to an $(\ell^2, \ell^2)$-isogeny, but can also compose to an $(\ell^2, \ell, \ell)$-isogeny, leading to many small cycles in the graph, resulting in trivially-found collisions for the hash function. Castryck, Decru and Smith revisited the construction [CDS20], identifying all these cycles and giving a straightforward way to avoid them in all dimensions. In essence, the fix consists of labeling every visited vertex with a so-called level structure referring to the last-traversed edge, and only allowing the walk in the graph to continue along paths which take this into account, namely the *good extensions*. This resulting higher-dimensional hash function is still assumed to be secure, although it has recently been shown that it also requires a trusted setup [CDKL+25], just as in the one-dimensional case. Jordan and Zaytman proved that these graphs are no longer Ramanujan [JZ26], whereas Florit and Smith showed that they exhibit decent expansion properties nonetheless [FS22b]. Unfortunately, neither of these works have taken into account the fact that the small cycles should be avoided, and these indubitably weaken the expander properties. Furthermore, both works do not take into account that these graphs are, by definition, directed.

Using Kani's lemma [Kan97], a lot of the focus in isogeny-based cryptography has shifted towards higher-dimensional variants, including - but not limited to - protocols such as PRISM [BBCS+25], higher-dimensional variants of SQIsign [BDFL+24, DLRW24, DF24, NOCC+24], PEGASIS [DEFM+25] and MIKE [Rob24]. These protocols typically rely on higher-dimensional isogenies as a toolbox to compute one-dimensional isogenies, meaning suboptimal expansion properties in higher dimensions do not necessarily affect their security directly, unlike the hash function. Nonetheless, if expansion properties would be severely lacking in for instance the subgraph consisting of only the elliptic products, this could still lead to a new type of generic attack. Because of this, the expander properties of the underlying graphs in higher dimensions seem interesting metrics, apart from the mathematical curiosity.

As an introductory example, consider $E_0 : y^2 = x^3 + 1$ with automorphism $\zeta^{(3)} : (x, y) \mapsto (\zeta_3 x, y)$. This automorphism acts on $E_0[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as an element of $\mathbb{F}_\ell^{2\times 2}$ with minimal polynomial $x^2+x+1$. If $\ell \equiv 2 \bmod 3$, this polynomial is irreducible so we can find a basis of $E_0[\ell]$ such that $\zeta^{(3)}$ can be represented as $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$. By Burnside's lemma, it follows that there are $(\ell + 1)/3$ orbits of subgroups of order $\ell$. In the corresponding $\ell$-isogeny graph, this node thus only

has $(\ell+1)/3$ outgoing edges. If $\ell \equiv 1 \bmod 3$ however, the automorphism will act as $\left(\begin{smallmatrix} \mu_3 & 0 \\ 0 & \mu_3^2 \end{smallmatrix}\right)$ on some choice of basis $E_0[\ell]$. We then have two one-dimensional $\zeta^{(3)}$-invariant subspaces, leading to $(\ell+5)/3$ orbits of order $\ell$.

### Technical overview

We work in the $(\ell)^2-$isogeny digraph $\mathsf{G}_2(p,\ell)$ where the vertices are pairs $(A,G)$ with $A$ a superspecial abelian surface over $\mathbb{F}_{p^2}$ and $G \subsetneq A[\ell]$ is a maximal isotropic $(\ell,\ell)$-subgroup with $\ell \neq p$ prime. The (directed) edges consist of all isogenies $\Psi$ with domain $A$ such that $\ker\Psi \cap G = 0$ (for a more precise definition, see Definition 3). We start by listing all possible numbers of outgoing edges of principally polarized abelian surfaces in this graph. Generically, there are $\ell^3+\ell^2+\ell+1$ outgoing edges, one for each maximal isotropic subgroup $G \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \subsetneq A[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^4$. Due to nontrivial automorphisms on $A$ however, this is not always the case, which is why in the more well-studied isogeny graphs, one needs to choose between the graph being undirected or regular.

*An example.* Consider the genus-2 curve $C/\overline{\mathbb{F}}_p : y^2 = x^5 - 1$ and let $J$ be its Jacobian. The hyperelliptic involution $(x,y) \mapsto (x,-y)$ is an automorphism on $C$ and induces the automorphism $[-1]$ on $J$. This automorphism exists on every abelian variety and does not impact the number of outgoing edges in the graph since it always maps maximal isotropic subgroups to itself. For this reason, we will work with the reduced automorphism group $\mathrm{RA}(J) = \mathrm{Aut}(J)/[-1]$. In this example, we have that $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$ with generator $\zeta_*^{(5)}$, induced by the automorphism $(x,y) \mapsto (\zeta_5 x, y)$ on $C$, where $\zeta_5$ is a fifth root of unity in $\overline{\mathbb{F}}_p$.

We are now interested in the action of $\zeta_*^{(5)}$ on pairs $(J,G)$, where $G \subsetneq J[\ell]$ is a maximal isotropic subgroup, where we assume $\ell \neq 5$ for the sake of simplicity. Since $\zeta_*^{(5)}$ has order five, its minimal polynomial is $\Phi_5 = x^4+x^3+x^2+x+1$.

If $\ell \equiv 1 \bmod 5$, we have that $\Phi_5 \bmod \ell$ splits into linear factors, hence it must act as the diagonal $4\times4$-matrix $\mathrm{diag}(\mu_5, \mu_5^2, \mu_5^4, \mu_5^3) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ on some symplectic choice of basis $\langle D_1, D_2, D_1', D_2' \rangle = J[\ell]$, where $\mu_5$ is a fifth root of unity in $\overline{\mathbb{F}}_\ell$. One can then argue by eigenspace decomposition that the only $\zeta_*^{(5)}$-invariant maximal isotropic subgroups are $\langle D_1, D_2\rangle, \langle D_1, D_2'\rangle, \langle D_1', D_2\rangle, \langle D_1', D_2'\rangle$. If $\ell \equiv 2,3 \bmod 5$, we have that $\Phi_5 \bmod \ell$ is irreducible and there are no $\zeta_*^{(5)}$-invariant maximal isotropic subgroups of $J[\ell]$. If $\ell \equiv 4 \bmod 5$, we have that $\Phi_5$ factors as

$$\Phi_5 = (x^2 - (\mu_5 + \mu_5^4)\cdot x + 1)\cdot(x^2 - (\mu_5^2 + \mu_5^3)\cdot x + 1) \bmod \ell,$$

and so the action of $\zeta_*^{(5)}$ on $J[\ell]$ can be seen as the $4\times4$-matrix

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & \mu_5+\mu_5^4 & 0 \\ 0 & 1 & 0 & \mu_5^2+\mu_5^3 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

for some symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$. This matrix consists of two "blocks" (rows/columns 1 and 3 and rows/columns 2 and 4), so it decomposes as a direct summand of subspaces. One can show that since the blocks are not similar, the only possible $\zeta_*^{(5)}$-invariant maximal isotropic subgroups are $\langle D_1, D_1' \rangle$ and $\langle D_2, D_2' \rangle$, but these are not symplectic. By Burnside's lemma, we can conclude that the number of $(J, G)$ up to isomorphism for this example is given by

$$\begin{cases} \frac{1}{5}(\ell^3 + \ell^2 + \ell + 17) & \text{if } \ell \equiv 1 \bmod 5, \\ \frac{1}{5}(\ell^3 + \ell^2 + \ell + 1) & \text{if } \ell \not\equiv 1 \bmod 5. \end{cases}$$

This gives us the exact number of abelian surfaces with $(\ell, \ell)$-level structure for this specific Jacobian. In this work, we do the same for all other principally polarized abelian surfaces by a close analysis of their reduced automorphism groups. These results are summarized in Table 1 for Jacobians of genus-2 curves and in Table 2 for products of elliptic curves.

*Isogeny digraphs.* Given the understanding of automorphisms on level structures, we may then explore the *superspecial $(\ell)^g$-isogeny digraph*, whose vertices are isomorphism classes $(A, H)$, where $A$ is a $g$-dimensional superspecial abelian variety, and $H \subseteq A[\ell]$ a maximal isotropic $(\ell)^g$-subgroup. Edges are derived from those $(\ell)^g$-isogenies $\varphi : A \to A'$ whose kernels intersect trivially with $H$.

This directed graph accurately describes the behaviour of isogeny walks with no backtracking: every combination of two edges is a *good extension*, and a walk of length $n$ corresponds to an $(\ell^n)^g$-isogeny, making this digraph fundamentally different from the usual $\ell$-isogeny graphs studied in isogeny-based cryptography. We posit that the expansion properties of this digraph more accurately reflect the behaviour of isogeny walks as used in isogeny-based cryptography.

Surprisingly, the concrete expansion properties of these digraphs has hardly been studied. We provide heuristic data for $g = 1$ for a range of small prime powers $\ell^k$ and for $g = 2$ for $\ell = 2$. This digraph converges to be *weakly Ramanujan*, implying strong expansion properties, in contrast to previous results on the $(2, 2)$-isogeny graph with backtracking. Based on these obeservations, we derive our Main Conjecture. Informally, our conjecture states that the second eigenvalue $\lambda_2$ of the adjacency matrix of such graphs over increasingly larger fields $\mathbb{F}_{p^2}$ converges to

$$\lim_{p \to \infty} \lambda_2 = \ell^{g^2/2}.$$

This agrees with the research on expander properties for $g = 1$, and furthermore implies that these digraphs converge to be weakly Ramanujan for $\ell \in \{2, 3\}$ for $g = 2$. More concretely, our conjecture poses that taking only good extensions strongly improves the expansion properties of isogeny walks, which is a significant result for the fundamental security of higher-dimensional isogeny-based cryptography.

### Our contributions

This work explores the action of automorphisms on abelian surfaces with $(\ell,\ell)$-level structure and the expansion properties of superspecial isogeny digraphs.

(i) We catalog the action of automorphisms on $(\ell,\ell)$-level structure, both for Jacobians and elliptic products. This generalizes previous results for $\ell = 2$ to any prime $\ell$ and provides all data where the digraphs cannot be made undirected.

(ii) We define superspecial isogeny digraphs $\mathsf{G}_g(N,p)$ in full generality, and explore their properties. Our Main Conjecture describes the expansion properties of superspecial isogeny digraphs in dimension $g$.

(iii) We computationally explore these superspecial digraphs $\mathsf{G}_g(\ell,p)$ for a range of small primes for $g = 1$ and for $\ell = 2$ for $g = 2$. This gives us insight into the concrete expansion properties of these graphs, and isogeny walks in general. In particular, the impact of small cycles arising from endomorphisms of small degree is significant when $g = 1$. In higher dimensions, the resulting expansion properties differ significantly from previous work on undirected isogeny graphs.

We verify all propositions and theorems using `Magma` [BCP97]. We generate the superspecial isogeny digraph data for dimension $g = 1$ using `sage` [The24], and for dimension $g = 2$ using `Magma`. Our work can be used more generally to explore automorphisms in dimension 2 and $(\ell,\ell)$-level structures, and isogeny (di)graphs in dimension 1 and 2. The code and full data is available at:

`https://github.com/Krijn-math/good-graphs`

**Table 1.** The number of $(\ell,\ell)$-level structures per Jacobian in function of their reduced automorphism group for primes $\ell > 3$. Clicking the group in the left column brings you to the associated theorem, which also covers $\ell = 2$ and $\ell = 3$.

| $\mathrm{RA}(J)$ | number of $(\ell,\ell)$-level structure per Jacobian |
|---|---|
| 1 | $\ell^3+\ell^2+\ell+1$ |
| $\mathbb{Z}/2\mathbb{Z}$ | $\frac{1}{2}\left(\ell^3+2\ell^2+3\ell+2\right)$ |
| $(\mathbb{Z}/2\mathbb{Z})^2$ | $\frac{1}{4}\left(\ell^3+3\ell^2+6\ell+5+\left(\frac{-1}{\ell}\right)\right)$ |
| $\mathcal{S}_3$ | $\frac{1}{6}\left(\ell^3+4\ell^2+9\ell+8+2\left(\frac{\ell}{3}\right)\right)$ |
| $\mathcal{D}_{2\times 6}$ | $\frac{1}{12}\left(\ell^3+5\ell^2+14\ell+19+3\left(\frac{-1}{\ell}\right)+6\left(\frac{\ell}{3}\right)\right)$ |
| $\mathcal{S}_4$ | $\frac{1}{24}\left(\ell^3+7\ell^2+24\ell+41+9\left(\frac{-1}{\ell}\right)+8\left(\frac{\ell}{3}\right)+6\left(\frac{-2}{\ell}\right)\right)$ |
| $\mathbb{Z}/5\mathbb{Z}$ | $\frac{1}{5}\left(\ell^3+\ell^2+\ell+1+\begin{cases}4 & \text{if } \ell=5\\ 16 & \text{if } \ell\equiv 1 \bmod 5\\ 0 & \text{if } \ell\not\equiv 1 \bmod 5\end{cases}\right)$ |

**Table 2.** The number of $(\ell,\ell)$-level structure per elliptic product in function of their reduced automorphism group for primes $\ell > 3$. Clicking the group in the left column brings you to the associated theorem, which also covers $\ell = 2$ and $\ell = 3$.

| $\mathrm{RA}(E \times E')$ | number of $(\ell,\ell)$-level structures per elliptic product |
|---|---|
| $\mathbb{Z}/2\mathbb{Z}$ | $\frac{1}{2}\left(\ell^3 + 2\ell^2 + \ 3\ell + 2\right)$ |
| $(\mathbb{Z}/2\mathbb{Z})^2$ | $\frac{1}{4}\left(\ell^3 + 3\ell^2 + \ 6\ell + \ 5 + \left(\frac{-1}{\ell}\right)\right)$ |
| $\mathbb{Z}/6\mathbb{Z}$ | $\frac{1}{6}\left(\ell^3 + 2\ell^2 + \ 7\ell + \ 6 + (4\ell+4)\left(\frac{\ell}{3}\right)\right)$ |
| $\mathbb{Z}/4\mathbb{Z}$ | $\frac{1}{4}\left(\ell^3 + 2\ell^2 + \ 5\ell + \ 4 + (2\ell+2)\left(\frac{-1}{\ell}\right)\right)$ |
| $\mathbb{Z}/12\mathbb{Z}$ | $\frac{1}{12}\left(\ell^3 + 2\ell^2 + \ 9\ell + 12 + 2(\ell+3)\left(\frac{-1}{\ell}\right) + 4(\ell+2)\left(\frac{\ell}{3}\right) + 4\left(\frac{3}{\ell}\right)\right)$ |
| $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$ | $\frac{1}{16}\left(\ell^3 + 4\ell^2 + 15\ell + 24 + (4\ell+12)\left(\frac{-1}{\ell}\right) + 4\left(\frac{-2}{\ell}\right)\right)$ |
| $\mathbb{Z}/6\mathbb{Z} \times \mathcal{S}_3$ | $\frac{1}{36}\left(\ell^3 + 5\ell^2 + 24\ell + 59 + (8\ell+38)\left(\frac{\ell}{3}\right) + 9\left(\frac{-1}{\ell}\right)\right)$ |

*Notation and conventions.* All fields are considered to be of positive characteristic $p > 5$, although some results may extend beyond that. We will denote $\ell$ for a (typically small) prime different from the field characteristic $p$. We will require $k$-th roots of unity both in $\mathbb{F}_p$ and $\mathbb{F}_\ell$ and will denote them by $\zeta_k$ and $\mu_k$ respectively. We will denote $\mathrm{diag}(a_1,\ldots,a_n)$ as the $n \times n$ diagonal matrix with entries $a_1,\ldots,a_n$. Bases for (sub)spaces will be denoted by angled brackets $\langle \cdots \rangle$ and will always be assumed to have the order fixed. We will denote $E_0$ and $E_{1728}$ as the elliptic curves with respective $j$-invariants 0 and 1728. The $n$-th cyclotomic polynomial will be denoted by $\Phi_n$ and the dihedral group with $2n$ elements by $\mathcal{D}_{2\times n}$. The notation $\left(\frac{p}{q}\right)$ is used for the Legendre symbol as per usual.


### Acknowledgments

We would like to thank the reviewers from Crypto for their helpful and thorough feedback. Thomas Decru is funded by Fonds voor Wetenschappelijk Onderzoek (FWO) with reference number 1245025N. This work is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02.


## 2 Preliminaries

We provide some of the necessary background regarding abelian varieties and expander (di)graphs. Remark that a large part of this paper specifically focuses on abelian surfaces, i.e. abelian varieties of dimension two, but some parts require the more general framework so we formulate them as such.

### 2.1 Abelian varieties

We work with abelian varieties over finite fields. A *polarization* of an abelian variety is an isogeny $\lambda : A \to \hat{A}$ between $A$ and its dual $\hat{A}$, and such a polarization is *principal* if $\deg \lambda = 1$, i.e., we have an isomorphism $A \xrightarrow{\sim} \hat{A}$. An elliptic curve is naturally equiped with a principal polarization, and in general, the Jacobian of a curve of genus $g$ is a principally polarized abelian variety of dimension $g$. Products of principally polarized abelian varieties $A \times B$ can be equipped with the *product polarization* $\lambda_{A\times B} = \lambda_A \times \lambda_B$. If not stated otherwise, we assume the product polarization on products of elliptic curves. A two-dimensional principally polarized abelian variety over $\overline{\mathbb{F}}_p$ is either (isomorphic to) the product of two elliptic curves, or the Jacobian of a hyperelliptic curve of genus 2. A *divisor* on an abelian variety is a formal finite integer sum of irreducible codimension-one subspaces. The divisors algebraically equivalent to zero (modulo linear equivalences) form the group $\mathrm{Pic}^0(A)$ of an abelian variety. Concretely, for an abelian surface $A$ constructed as the Jacobian of a genus-2 curve $C$, this means we can represent every element of $A$ uniquely as the sum of at most two points of $C$.

*Superspecial abelian varieties.* In higher dimensions, supersingularity of elliptic curves generalizes to several distinct notions. Following [CDS20], we focus on superspecial abelian varieties. We say that an abelian variety $A$ is *superspecial* if $A$ is isomorphic to a product of supersingular curves, as an unpolarized variety. We say that a curve is superspecial when its accompanying Jacobian is superspecial. A one-dimensional principally polarized abelian variety $A$ over $\overline{\mathbb{F}}_p$ is an elliptic curve, and so, superspeciality reduces to supersingularity. All superspecial abelian varieties can be defined over $\mathbb{F}_{p^2}$.

*Weil pairing.* In general, the *Weil pairing of level $n$* on an abelian variety $A$ is an alternating bilinear pairing $e_n : A[n] \times \hat{A}[n] \to \mu_n$. Given a (principal) polarization $\lambda : A \to \hat{A}$, we may define $e_n^\lambda$ as the Weil pairing induced on $A[n] \times A[n]$. On (products of) elliptic curves or Jacobians of hyperelliptic curves, we assume the principal polarization and drop the superscript $\lambda$, to obtain the Weil pairing of level $n$ as

$$e_n : A[n] \times A[n] \to \mu_n.$$

A basis $\langle P_1, \ldots, P_g, Q_1, \ldots, Q_g \rangle$ of $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ is called *symplectic* iff

$$e_n(P_i, P_j) = e_n(Q_i, Q_j) = 1, \qquad e_n(P_i, Q_j) = \zeta_n^{\delta_{ij}},$$

where $\delta_{ij}$ is the Kronecker delta symbol and $\zeta_n$ a fixed $n$th root of unity. For an abelian surface specifically, the basis $\langle P_1, P_2, Q_1, Q_2 \rangle$ is symplectic iff the Weil pairing matrix in block form is

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell),$$

where entries need to be considered as $\log_n(e_n(\cdot,\cdot))$ and where $\mathrm{Sp}_4(\mathbb{F}_\ell)$ denotes the symplectic group of order four over $\mathbb{F}_\ell$.

*Maximal isotropic subgroups.* A subgroup $G \subseteq A[n]$ of a principally polarized abelian variety $A$ is called *isotropic* with respect to the Weil pairing $e_n^\lambda$ when $e_n^\lambda(P,Q) = 1$ for all $P, Q \in G$. If there is no larger isotropic subgroup $G' \subseteq A[n]$ such that $G \subsetneq G'$, then we say that $G$ is a *maximal isotropic subgroup*. When $G$ is maximally isotropic of rank $g$ and has the structure $G \cong (\mathbb{Z}/n\mathbb{Z})^g$ as an abelian group, we call $G$ a maximal isotropic $(n)^g$-subgroup. We refer to a set of points $P_1, \ldots, P_g \in G$ as a *basis* of $G$ whenever $G = \langle P_1, \ldots, P_g \rangle$. An *abelian variety with $(\ell)^g$-level structure* is a pair $(A, G)$, where $G$ is a maximal isotropic $(\ell)^g$-subgroup of $A[\ell]$. For the rest of this work, we consider $(A, G)$ *up to isomorphism*, which includes automorphisms.

*Automorphisms.* An *automorphism* $\alpha$ of a variety $X/k$ is an isomorphism of $X$ to itself as a $k$-scheme. An automorphism $\alpha_*$ of an abelian variety $A/k$ is a variety automorphism of $A/k$ which is also a group homomorphism. The automorphisms of an abelian variety $A$ form a group, which is denoted as $\mathrm{Aut}(A)$. An automorphism $\alpha$ of a curve $C$ induces a natural automorphism $\alpha_*$ on the Jacobian of $C$ by acting on the points of the divisor class. For (products of) elliptic curves, we will often write $\alpha$ instead of $\alpha_*$ due to the natural induced group law. Every abelian variety comes with the order-2 inversion automorphism $[-1]$ which maps $D$ to $-D$. For this reason, we will typically work with the *reduced automorphism group* of $A$, defined by $\mathrm{RA}(A) = \mathrm{Aut}(A)/[-1]$. We refer to Appendix A for a classification of the possible nontrivial automorphisms of p.p. abelian surfaces over finite fields. Automorphisms on abelian varieties preserve the Weil pairing; in particular they map maximal isotropic subgroups to maximal isotropic subgroups. An automorphism $\alpha_*$ acting on the $\ell$-torsion $A[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ can be represented as a matrix $M \in \mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ by its action on a basis of $A[\ell]$.

*Isogenies.* We focus on separable $(\ell, \ldots, \ell)$-isogenies between principally polarized abelian varieties. Similar to dimension one, such isogenies are defined up to isomorphism by their kernel $G = \ker \varphi$. In this case, $G$ must be a maximal isotropic $(\ell)^g$-subgroup of $A[\ell]$, hence isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$. By [CD22, Lemma 2], there are $\ell^{g(g+1)/2} \prod_{i=1}^{g} (1 + \frac{1}{\ell^i})$ maximal isotropic $(\ell)^g$-subgroups.

Given two $(\ell, \ldots, \ell)$-isogenies $\varphi_1 : A \to B$ and $\varphi_2 : B \to C$, we say that $\varphi_2$ is a *good extension* of $\varphi_1$ when $\ker \varphi_2 \cap \ker \hat{\varphi}_1 = 0$, following [CDS20], and for each $\varphi_1$ there exist $\ell^{g(g+1)/2}$ good extensions $\varphi_2$ (up to isomorphism and automorphism). This implies that the composition $\varphi_2 \circ \varphi_1$ is an $(\ell^2, \ldots, \ell^2)$-isogeny. Two cases are important for this work:

(i) In dimension one, any rank-1 subgroup $G \subseteq E[\ell]$ isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ is trivially maximal isotropic, as the Weil pairing will always be trivial on a rank-1 subgroup. When $\ell$ is prime, there are $\ell$ good extensions, as only the dual is eliminated. When $\ell$ is composite, good extensions can be viewed as those isogeny decompositions without backtracking.

(ii) In dimension two, we mostly focus on $\ell = 2$. When $\ell = 2$, we have fifteen $(2,2)$-isogenies given by the fifteen maximal isotropic subgroups of $A[2]$. For a given $(2,2)$-isogeny $A \to B$, only eight out of the fifteen maximal isotropic subgroups of $B[2]$ define a good extension $B \to C$.

Let $A, B, C, D$ be simple abelian varieties. We distinguish four types of isogenies between abelian varieties. The most common is a *generic* isogeny $A \to B$ between simple abelian varieties $A$ and $B$. A *splitting* isogeny is an isogeny $A \to B \times C$, and conversely, a *gluing* isogeny is an isogeny $A \times B \to C$. Lastly, a *diagonal* isogeny $A \times B \to C \times D$ is *de facto* two generic isogenies $A \to C$ and $B \to D$ evaluated simultaneously.

For computations of isogenies in dimension one, Vélu's formulas [Vél71] provide the necessary tools to compute an isogeny given a generator for its kernel. In dimension two, the computation of $(2,2)$-isogenies was given by Richelot [Ric37]; for a more contemporary source, we refer to [Smi05].

### 2.2 Expander (di)graphs

*Graphs.* A *graph* $G = (V, E)$ consists of a set of vertices $V$ and a set of edges $E$, which are unordered pairs of vertices. For our purposes, we will allow the set $E$ to be a multiset, which allows us to define multiple edges between the same two vertices; we will only draw specific attention to it when necessary. A graph is called *$k$-regular* if for each vertex $v$ there are $k$ edges in $E$ which have $v$ as vertex.

A *walk* in a graph is a sequence of edges, where the "ending" vertex of an edge is the "starting" vertex of the subsequent edge. A graph is called *connected* if there exists a walk between any two vertices. The *adjacency matrix* of a graph $G = (V, E)$ is an $n \times n$ matrix $M$, with $n = \#V$, where entry $M_{ij}$ is the number of edges between vertex $i$ and $j$, where we have chosen a fixed ordering for the vertices $V$. The adjacency matrix for a graph is symmetric since $M_{ij} = M_{ji}$.

*Expansion properties.* For cryptographic purposes, we are mostly interested in graphs where random walks are truly random in some sense. This type of behavior is labeled as *expander properties*. There are several notions of these, such as edge expansion, vertex expansion, and spectral expansion. Most types of expansion are related or can be reduced to one another and we will focus on spectral expansion since it is easiest to compute.

Let $G = (V, E)$ be a $k$-regular connected graph with $n = \#V$ and $M$ its adjacency matrix. One can show that the eigenvalues $\lambda_i$ of $M$ satisfy $k = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq -k$. The value $\lambda_1 - \lambda_2$ is called the spectral gap $M$. We call $G$ a *Ramanujan graph* if

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

One may also define the Ramanujan property as a limit property for a family of graphs, which seems more apt for cryptographic purposes since we cannot compute eigenvalues of graphs with an exponential amount of nodes. We then say that a family of graphs $G_1, G_2, G_3, \ldots$ has the Ramanujan property if for $i \to \infty$

it holds that there exists $\epsilon > 0$ such that for $\lambda_2$ of $G_i$ we have $\lambda_2 \leq 2\sqrt{k-1} - \epsilon$. The value $\lambda_2$ also determines the rate of expansion.

**Definition 1.** A $k$-regular connected graph $G$ has *spectral expansion* $\gamma(G)$ if

$$\lambda(G) = |\lambda_2/k| \leq 1 - \gamma(G),$$

where $\lambda_2$ is the eigenvalue of the adjacency matrix of $G$ with second-largest absolute value.

Note that larger values of $\gamma(G)$ (or smaller values of $\lambda(G)$) correspond to better expansion properties.

*Digraphs.* A *directed graph or digraph* $G = (V, E)$ consists of a set of vertices $V$ and a (multi)set of edges $E$, which are ordered pairs of vertices, as opposed to the unordered pairs of vertices for a graph. The *out-degree*, resp. *in-degree*, of a vertex $v \in V$ is the number of edges $(v_1, v_2) \in E$ such that $v = v_1$, resp. $v = v_2$. We will call a digraph $k$-regular if the out-degree for each vertex is $k$.

Most of the properties of graphs translate to digraphs, although subtleties do appear. The adjacency matrix of a digraph for example is no longer symmetric, hence its eigenvalues are not necessarily real. For a $k$-regular connected digraph, however, we still have that the largest eigenvalue $\lambda_1$ of its adjacency matrix equals $k$, which follows from the fact that the sum of the entries of each row is $k$. Given that the second largest eigenvalue $\lambda_2$ can now be complex, we say that a $k$-regular digraph $G$ has spectral expansion $\gamma(G)$ if $\lambda(G) = |\lambda_2/k| \leq 1-\gamma(G)$, where we now take the modulus instead of the absolute value. For digraphs, the notion of Ramanujan seems stricter (see for example [Par20] or [LLP20]), but we will be using a more refined classification (see for example [EFMP26]).

**Definition 2.** Let $G = (V, E)$ be a $k$-regular connected digraph with $\lambda_2$ the eigenvalue of the adjacency matrix with second largest modulus. Assume $G$ is also $k'$-regular regarding the in-degree.

- If $|\lambda_2| \leq \sqrt{k-1}$ then $G$ is *Ramanujan*.
- If $|\lambda_2| \leq \sqrt{k-1} + \sqrt{k'-1}$ then $G$ is *weakly Ramanujan*.
- If $|\lambda_2^2 - k - k' + 2| \leq 2\sqrt{(k-1)(k'-1)}$ then $G$ is *adjacent-Ramanujan*.

It is immediate that Ramanujan implies weakly Ramanujan, and the latter also implies adjacent-Ramanujan, but the other directions do not hold in general. Similarly as in the undirected graph case, a family of directed graphs $G_1, G_2, G_3, \ldots$ is said to have the Ramanujan, weakly Ramanujan or adjacent-Ramanujan property if for $i \to \infty$ the graph $G_i$ converges to one where the respective condition holds.

The spectral expansion $\gamma(G)$ can be interpreted in several ways. The rapid mixing property essentially says that we can approach the uniform distribution using random walks as good as possible based on $\gamma(G)$.

*Property 1.* Let $G = (V, E)$ be a $k$-regular connected (di)graph with spectral expansion $\gamma(G)$ and $\#V = N$. Let $\pi^{(t)}$ be the distribution of the nodes of $G$ after a random walk of length $t$, and let $U_N$ be the uniform distribution on $N$ elements. Then for every $\epsilon > 0$ the statistical distance $\frac{1}{2}||\pi^{(t)} - U_N||_1$ between $\pi^{(t)}$ and $U_N$ is less than or equal to $\epsilon$ for

$$t \geq \frac{\log(\sqrt{N}/\epsilon)}{\log(1/\lambda(G))}.$$

Alternatively, we can also use the spectral expansion $\gamma(G)$ to express quasi-randomness, edge expension, vertex expansion, etc. For all of these and more information about expander graphs and their properties in general, with a focus on directed graphs specifically, we refer to [DM, Vad].

## 3 Automorphisms acting on $(\ell, \ell)$-level surfaces

For a generic p.p. abelian surface $A$, it holds that the only nontrivial automorphism is $[-1]$, leading to $\mathrm{RA}(A) = 1$. Since $[-1]$ maps any maximal isotropic subgroup of $A$ to itself, an abelian surface with trivial $\mathrm{RA}(A)$ gives rise to $\ell^3 + \ell^2 + \ell + 1$ distinct abelian surfaces with $(\ell, \ell)$-level structure.

In this section, we catalog the action of nontrivial automorphisms on abelian surfaces with $(\ell, \ell)$-level structure $(A, G)$. The proofs of the propositions and theorems are all very similar, so we will restrict to elaborating on a couple of Jacobians of genus-2 curves in full detail in section Section 3.2. The remainder of the Jacobians of genus-2 curves is treated in Appendix B and the products of elliptic curves in Appendix C.

Albeit that $[-1]$ acts trivially in $\mathrm{RA}(A)$, we will sometimes use $[-1]$ in our proofs, in particular when there are other automorphisms $\alpha_*$ such that $\alpha_*^k = [-1]$ for some $k > 1$. Nonetheless, we will use the reduced automorphism group to make the comparison with [FS22a] easier.

Throughout the proofs, we will also make use of Burnside's lemma, which we postulate here without proof. Recall that for an action of a group $G$ on a set $X$ we denote $X/G$ as the set of orbits, and for every $g \in G$ the notation $X^g$ corresponds to the set of points of $X$ which are fixed under $g$.

**Lemma 1.** *(Burnside's lemma) Let $G$ be a finite group acting on a finite set $X$. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| .$$

### 3.1 General action on symplectic spaces

Throughout the discussion, we will use the following lemma often.

**Lemma 2.** *Let $\Gamma_1, \Gamma_2 \in \mathrm{Sp}_{2n}(\mathbb{F}_\ell)$ be symplectic matrices. Assume that $\Gamma_1$ and $\Gamma_2$ are similar, and denote by $g(x)$ their common characteristic polynomial. If $(x-1)$ and $(x+1)$ are not factors of $g(x)$, then $\Gamma_1$ and $\Gamma_2$ are symplectically similar; that is, there exists a symplectic matrix $P$ such that $\Gamma_2 = P\Gamma_1 P^{-1}$.*

*Proof.* This follows from the classification of conjugacy classes of symplectic matrices by Wall [Wal63, Page 36, Case (B)(ii)]: all elements in $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$ with $(x \pm 1)$ not dividing the characteristic polynomial are symplectic conjugates. □

To change between fields of definition, we can use the following result.

**Lemma 3.** *Let $M_1$ and $M_2$ be two matrices over a field $K$, and let $L/K$ be a field extension. Then $M_1$ and $M_2$ are similar over $K$ if and only if they are similar over $L$.*

*Proof.* Matrices are similar if and only if they have the same rational canonical form, which in this case is defined over $K$ since the invariant factors are necessarily in $K[x]$. The statement then follows by the rationality of this form, i.e., obtaining it requires no operations which change under field extensions. □

Remark that Lemma 2 is no longer true if $(x \pm 1)$ divides the characteristic polynomial. Indeed: $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{Sp}_2(\mathbb{F}_3)$ are not symplectic conjugates, essentially because $2 \in \mathbb{F}_3$ is not a square, unlike 1. Instead of making general statements about these exceptional cases, we will resolve them as they occur using the following lemma.

**Lemma 4.** *Let $\ell$ be an odd prime and $\Gamma \in \mathrm{Sp}_{2n}(\mathbb{F}_\ell)$. If $\Gamma$ is diagonizable, then $\Gamma$ is symplectically diagonizable; i.e. there exists a $P \in \mathrm{Sp}_{2n}(\mathbb{F}_\ell)$ such that $P\Gamma P^{-1}$ is diagonal.*

*Proof.* Since $\Gamma$ is symplectic, its eigenvalues occur in pairs $\lambda, \lambda^{-1}$ with the same multiplicity. For $\lambda \neq \pm 1$, the eigenspace $E_\lambda$ is isotropic because $\lambda^2\langle v, w\rangle = \langle v, w\rangle$ implies $(\lambda^2 - 1)\langle v, w\rangle = 0$ and $\lambda^2 \neq 1$. The symplectic form pairs $E_\lambda$ nondegenerately with $E_{\lambda^{-1}}$ and we can choose a basis $v_1, \ldots, v_d$ of $E_\lambda$ and a dual basis $w_1, \ldots, w_d$ of $E_{\lambda^{-1}}$ with $\langle v_i, w_j\rangle = \delta_{ij}$ and all other pairings zero. If $\lambda\mu \neq 1$, then $\lambda\mu\langle x, y\rangle = \langle x, y\rangle$ forces $\langle x, y\rangle = 0$, from which it follows that different eigenvalue pairs are orthogonal. For $\lambda = \pm 1$, the eigenspace is symplectic (since $\lambda^{-1} = \lambda$), and we can pick any symplectic basis where $\Gamma$ acts as $[\pm 1]$. Taking the union of these bases over all eigenvalue pairs yields a symplectic basis of the whole space consisting of eigenvectors of $\Gamma$. The change of basis to this eigenbasis is a symplectic matrix, so $\Gamma$ is symplectically diagonalizable. □

Luckily, automorphisms are almost always diagonizable.

**Lemma 5.** *Let $\alpha$ be an automorphism of order $m$ of a principally polarized abelian variety $A/K$. If $m$ is coprime to the characteristic of $K$, then $\alpha$ is diagonizable.*

*Proof.* From $\alpha^m = \mathtt{id}$ it follows that the minimal polynomial of $\alpha$ divides $x^m - 1$. Over $\overline{K}$ this polynomial has $m$ distinct roots, hence the minimal polynomial of $\alpha$ has no repeated roots and is thus diagonizable. □

We will assume that all bases corresponding to an automorphism given in symplectic matrix form are symplectic unless specifically mentioned otherwise. We will also need the following lemmata.

**Lemma 6.** *Let $V$ be a finite-dimensional $K$-vector space. Assume $M$ is a $K$-linear map with eigenvalues $\lambda_1, \ldots, \lambda_n$ and eigenspace decomposition $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_n}$. Then a subspace $W \subseteq V$ is $M$-invariant iff*

$$W = (W \cap V_{\lambda_1}) \oplus \ldots \oplus (W \cap V_{\lambda_n}).$$

*Proof.* Assume $W$ is $M$-invariant and write $w = v_1 + \ldots + v_n \in W$ with $v_i \in V_{\lambda_i}$. It suffices to show that each $v_i \in W$. Define the polynomial $p_i(x) = \prod_{j \neq i}(x - \lambda_j)$, then $p_i(\lambda_j) = 0$ when $i \neq j$. It then follows that

$$p_i(M)w = p_i(M)v_1 + \ldots + p_i(M)v_n = p_i(M)v_i = p_i(\lambda_i)v_i.$$

Since $W$ is $M$-invariant, it is also $p_i(M)$-invariant thus $p_i(\lambda_i)v_i \in W$ as wanted. The other direction of the proof is immediate. □

**Lemma 7.** *Let $V = V_1 \oplus V_2$ be a finite-dimensional $K$-vector space with $\dim V_1 = \dim V_2 = n$ and let $M \in K^{2n \times 2n}$ be a $K$-linear map given by a square block matrix*

$$\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$$

*such that $M_i V_i = V_i$. If $V_1, V_2$ are irreducible $K[M]$-modules and $M_1$ and $M_2$ have the same characteristic polynomial, then the only $n$-dimensional $M$-invariant subspaces of $V$ are $V_1$, $V_2$ and*

$$\{(v_1, Lv_1) \mid v_1 \in V_1, L : V_1 \xrightarrow{\sim} V_2\},$$

*for some isomorphism $L : V_1 \to V_2$. Furthermore, if $M_1$ and $M_2$ have different characteristic polynomials, then the only $n$-dimensional $M$-invariant subspaces of $V$ are $V_1$ and $V_2$.*

*Proof.* Let $W \subseteq V$ be an $n$-dimensional $M$-invariant subspace and write $W_i = W \cap V_i$. Since $W$ is $M$-invariant, the $W_i$ are $M_i$-invariant and by irreducibility of $V_i$ we have $\dim W_i \in \{0, n\}$. For $(\dim W_1, \dim W_2)$ equal to $(n, 0), (0, n), (n, n)$ we find that $W$ equals $V_1, V_2, V$ respectively, for which we need to discard the latter because its dimension is $2n$. So assume $\dim W_1 = \dim W_2 = 0$.

Since $W \cap V_2 = 0$, the projection $\pi_1 : W \to V_1$ is injective and by dimension argument it must be an isomorphism. The same holds for $\pi_2 : W \to V_2$. For any $v_1 \in V_1$ there is thus a unique $w \in W$ such that $\pi_1(w) = v_1$; define $L : V_1 \to V_2, v_1 \mapsto \pi_2(\pi_1^{-1}(v_1))$. Then any $w$ can be written as $(v_1, Lv_1) \in V_1 \oplus V_2$ and since $\pi_2$ is an isomorphism, so is $L$.

Now assume $M_1$ and $M_2$ have different characteristic polynomials; in particular they are not similar. Since $W$ is $M$-invariant, we have that $(M_1 v_1, M_2 L v_1)$ must also be of the form $(v_1', Lv_1')$ for some $v_1' \in V_1$. Thus $M_2 L v_1 = L v_1' = L M_1 v_1$ for all $v_1 \in V_1$ and consequently $M_2 L = L M_1$ as linear maps. Since $M_1$ and $M_2$ are not similar, no such $L$ can exist. □

### 3.2 Reduced automorphisms on Jacobians

Here, we go over two of the seven possible nontrivial reduced automorphism groups for Jacobians $J$, and discuss the action of these automorphisms on the $(\ell,\ell)$-subgroups of $J[\ell]$. The proofs for the other five cases are very analogous and can be found in Appendix B. For more details about the automorphisms themselves, see Appendix A or [FS22a].

**$\mathbf{RA}(J) = \mathbb{Z}/2\mathbb{Z}$** This case occurs if the Jacobian is $(2,2)$-split; i.e. there exists a $(2,2)$-isogeny $\Psi : J \to E \times E'$. Up to isomorphism, the curve equation giving rise to $J$ can always be written in the form

$$C : y^2 = (x^2-1)(x^2-s^2)(x^2-t^2)$$

for suitable parameters $s,t$; more specifically, $s \neq \pm t$ and $s,t \notin \{0,\pm 1\}$. The automorphism corresponding to $\mathbb{Z}/2\mathbb{Z}$ is given by $\sigma : x \mapsto -x$. We have the following characterization of the action of $\sigma_*$ on abelian surfaces with $(\ell,\ell)$-level structure.

**Proposition 1.** *Let $C : y^2 = (x^2-1)(x^2-s^2)(x^2-t^2)$ be a genus-2 curve over a field of characteristic $p > 5$, with $\sigma : x \mapsto -x$ an automorphism of order 2, and $\ell \neq p$ a prime. Then the induced automorphism $\sigma_*$ acts on the abelian surfaces with $(\ell,\ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 |
|---|---|---|
| $\ell = 2$ | 7 | 8 |
| $\ell \neq 2$ | $(\ell+1)^2$ | $\ell^3 - \ell$ |

*Proof.* (i) For $\ell = 2$, see [FS22a, Section 4.5].

(ii) For $\ell \neq 2$, we know that $\sigma_*^2 = \mathtt{id}$ so its minimal polynomial is $x^2-1$. By Lemma 4, the action on the $\ell$-torsion is thus symplectically diagonizable with eigenvalues $\pm 1$. Since these eigenvalues must both have nonnegative even multiplicities, it follows that $\sigma_*$ can be given as $\mathrm{diag}(1,-1,1,-1) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ for some symplectic basis.* By Lemma 6, the maximal isotropic $\sigma_*$-invariant subspaces are of the form $W = W_+ + W_-$, where $W_\pm$ is a one-dimensional subspace of the eigenspace of eigenvalue $\pm 1$. This yields $(\ell+1)^2$ total options for $W$.

□

This leads to the following result.

*Remark that this is more subtle in higher dimensions, where multiplicities don't automatically follow from having a minimal polynomial $x^2-1$.

**Theorem 1.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $J$ its Jacobian, $\mathrm{RA}(J) = \mathbb{Z}/2\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(J, G)$ is equal to 11 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{2}(\ell^3 + 2\ell^2 + 3\ell + 2).$$

*Proof.* This follows immediately from Proposition 1. □

**$\mathrm{RA}(J) = (\mathbb{Z}/2\mathbb{Z})^2$** This automorphism group comes from a special case of a Jacobian $J$ which is $(2,2)$-split, where it can be shown that any such $J$ must stem from a curve given by the equation

$$C : y^2 = (x^2 - 1)(x^2 - u^2)(x^2 - 1/u^2),$$

for a suitable parameter $u \notin \{0, \pm 1, \pm i\}$. The automorphism corresponding to the additional component $\mathbb{Z}/2\mathbb{Z}$ is then given by $\tau : x \mapsto 1/x$. Remark that $\tau$ has order two in the reduced automorphism group only! Indeed, as a nonreduced automorphism on $C$, it induces $\tau_*$ on $J$ for which it holds that $\tau_*^2 = [-1]$. We have the following characterization of the action of $\tau_*$ on abelian surfaces with $(\ell, \ell)$-level structure.

**Proposition 2.** *Let $C : y^2 = (x^2 - 1)(x^2 - u^2)(x^2 - 1/u^2)$ be a genus-2 curve over a field of characteristic $p > 5$, with $\tau : x \mapsto 1/x$ an automorphism of (reduced) order 2, and $\ell \neq p$ a prime. Then the induced automorphism $\tau_*$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 |
|---|---|---|
| $\ell = 2$ | 3 | 12 |
| $\ell \equiv 1 \bmod 4$ | $\ell + 3$ | $\ell^3 + \ell^2 - 2$ |
| $\ell \equiv 3 \bmod 4$ | $\ell + 1$ | $\ell^3 + \ell^2$ |

*Proof.* Since as a nonreduced automorphism we have that $\tau_*^2 = [-1]$, its minimal polynomial is $\Phi_4 = x^2 + 1$ with eigenvalues $\pm i$. For any symplectic basis of $J[\ell]$, with $\ell$ odd, the linear map that represents the action of $\tau_*$ on this basis is hence diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(i, -i, -i, i) \in \mathrm{Sp}_4(\overline{\mathbb{F}_\ell})$.

(i) For $\ell = 2$, see [FS22a, Section 4.7].

(ii) For $\ell \equiv 1 \bmod 4$, it holds that $\Phi_4 = (x - i)(x + i) \bmod \ell$. Hence, using Lemma 4, we can assume a symplectic basis of $J[\ell]$ such that the action of $\tau_*$ is given by $\mathrm{diag}(i, -i, -i, i) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$. Using Lemma 6, we see that for every line in $V_i$ there is exactly one line in $V_{-i}$ making a maximal isotropic subgroup. Combining with the two maximal isotropic subgroups $V_i$ and $V_{-i}$ themselves, we thus have $\ell + 3$ $\tau_*$-invariant maximal isotropic subgroups.

(iii) For $\ell \equiv 3 \bmod 4$, we have that $\Phi_4$ is irreducible modulo $\ell$ and $\pm i \notin \mathbb{F}_\ell$. By Lemma 2 and Lemma 3, there exists a symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$, such that the action of $\tau_*$ is given by

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

By Lemma 7, there are $\ell + 1$ choices of graphs of isomorphisms $\langle D_1, D_2 \rangle \to \langle D_1', D_2' \rangle$ which are $\tau_*$-invariant two-dimensional subspaces. These are lines corresponding to the subgroups $\langle aD_1 + bD_1', aD_2 + bD_2' \rangle$, where $a$ and $b$ are not simultaneously zero. Since the basis is symplectic, the only nontrivial pairings are $e_\ell(D_1, D_1')$ and $e_\ell(D_2, D_2')$, from which one can easily deduce that all of these $\tau_*$-invariant subgroups are isotropic.

□

Using the action of $\sigma_*$ from Proposition 1, we have the following theorem.

**Theorem 2.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $J$ its Jacobian, $\mathrm{RA}(J) = (\mathbb{Z}/2\mathbb{Z})^2$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(J, G)$ is equal to 8 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{4}\left(\ell^3 + 3\ell^2 + 6\ell + 5 + \left(\frac{-1}{\ell}\right)\right).$$

*Proof.* Burnside's lemma says that the number of abelian surfaces with $(\ell, \ell)$-level structure is equal to

$$\frac{1}{|(\mathbb{Z}/2\mathbb{Z})^2|} \cdot \left(|X^{\mathtt{id}}| + |X^{\sigma_*}| + |X^{\tau_*}| + |X^{\sigma_*\tau_*}|\right),$$

hence by Propositions 1 and 2, it suffices to check $X^{\sigma_*\tau_*}$. One can verify that the minimal polynomial of $\sigma_*\tau_*$ is $x^2 - 1$, so the orbits act exactly the same as $\sigma_*$ from Proposition 1.

□

The remainder of the cases are treated in Appendix B.

### 3.3 Reduced automorphisms on products of elliptic curves

Every product of elliptic curves has $\mathrm{RA}(E \times E') \neq 1$, since $[1] \times [-1]$ is always nontrivial. There are seven possible (reduced) automorphism groups of elliptic curves; see Appendix A or [FS22a]. The six other options all stem from either both factors being isomorphic, which gives the automorphism $(P, Q) \mapsto (Q, P)$, or one of the factors having the automorphism $\iota : E_{1728} \to E_{1728}, (x, y) \mapsto (-x, iy)$ or $\zeta^{(3)} : E_0 \to E_0, (x, y) \mapsto (\zeta_3 x, y)$. The curves $E_{1728}$ and $E_0$ are supersingular if $p \equiv 3 \bmod 4$, respectively $p \equiv 2 \bmod 3$, and can thus make part of a superspecial abelian surface. To not distract from the discussion, we refer to Appendix C for the full details since combining the automorphisms $\iota$ and $\zeta^{(3)}$ is long and technical rather than insightful.

### 3.4 Computational verification

Although the results in Sections 3.2 and 3.3 and Tables 1 and 2 are rigorously proven, we have simultaneously computationally verified these results for all possible reduced automorphism groups for $2 \leq \ell \leq 79$ for a range of primes $p$. This ensures that no minor mistakes or typos have been made in counting arguments. This section briefly describes this verification process, as the computational techniques may be applied more generally when working with $(\ell, \ell)$-subgroups and $(\ell, \ell)$-isogenies.

Assume a supersingular principally polarized abelian surface $A$ over $\mathbb{F}_{p^2}$ with $A(\mathbb{F}_{p^2}) = A[p+1]$ and a prime $\ell \mid p+1$ such that $A[\ell]$ is rational. Furthermore, assume $\alpha_* \in \mathrm{RA}(A)$ is a non-trivial automorphism. Following [KTW22], we construct a symplectic basis $\mathcal{B} := \langle D_1, D_2, D_1', D_2' \rangle$ for $A[\ell]$. Using the echelon form (see Appendix D), we may generate the set $\mathcal{G}$ of all valid maximally isotropic subgroups $G = \langle K_1, K_2 \rangle$ as linear combinations in $\mathcal{B}$, and let $\alpha_*$ act on both $K_i$ to derive $\alpha_*(G)$. However, this procedure is time consuming, and verifying equality of $\alpha_*(G)$ and $\alpha_*(G')$ is non-trivial. Instead, we compute the matrix $M_\alpha$ from the action of $\alpha_*$ on $\mathcal{B}$ and let $M_\alpha$ directly act on the echelon matrix $M_G$ associated to $G$. Verifying equality is now easy using the reduced echelon form of $M_\alpha \cdot M_G$.

This allows us to split $\mathcal{G}$ into its orbits under $\alpha_*$, which allows us to verify the propositions in Sections 3.2 and 3.3. Similarly, to verify the theorems, we split $\mathcal{G}$ into its orbits under the full group $\mathrm{RA}(A)$ such that the number of orbits gives us the number of $(A, G)$ up to isomorphism. The `Magma` code that verifies these results for all Jacobians and products with non-trivial reduced automorphism groups is available in our repository.

## 4 Expansion properties of isogeny digraphs

In this section, we describe the expansion properties of directed isogeny graphs. We first define the general superspecial isogeny *digraph* for any dimension $g$, before discussing the experimental data obtained on the eigenvalues of the adjacency matrix for dimension 1, for several small primes, and dimension 2, for $\ell = 2$. This allows us to state our Main Conjecture on the concrete expansion properties of superspecial isogeny digraphs, which determine the rate at which a random walk approaches the uniform distribution.

### 4.1 The Superspecial $(\ell)^g$-isogeny Digraph

We now define the superspecial $(\ell)^g$-isogeny digraph in its full generality.

**Definition 3.** The *superspecial* $(\ell)^g$*-isogeny digraph* $\mathsf{G}_g(p, \ell) = (V, E)$ is defined as follows.

- The vertex set $V$ consists of all isomorphism classes $(A, H)$, where $A$ is a $g$-dimensional principally polarized superspecial abelian variety over $\overline{\mathbb{F}}_p$ and $H \subseteq A[\ell]$ is a maximal isotropic $(\ell)^g$-subgroup.

– The edge (multi)set $E$ consists of an ordered pair $((A_1, H_1), (A_2, H_2))$ for every maximal isotropic $(\ell)^g$-subgroup $H \subset A_1[\ell]$ such that $H \cap H_1 = 0$ and such that there exists an isogeny $\Psi_1 : A_1 \to A_2$ for which $\ker \Psi_1 = H$ and $\Psi_1(H_1) = H_2$.

For $g = 1$, Charles, Goren and Lauter [CLG09] studied the graphs $\mathsf{G}_1(p, \ell)$ for primes $\ell$, and a significant amount of isogeny-based cryptography is based on these foundations. For $g = 2$, the graph $\mathsf{G}_2(p, 2)$ is similar to the supersingular $(2, 2)$-isogeny graph studied by Castryck, Decru and Smith [CDS20]. Both of these constructions are aware of the fact that the graph is technically directed, but do not elaborate upon that in a significant way. One could hope to turn this graph into an undirected one due to the existence of dual isogenies, but unfortunately this is impossible. The nontrivial automorphisms on certain abelian varieties create multi-edges which only have one dual, such that several edges would need to share the same "dual edge". Only in the case of $g = 1$ and $p \equiv 1 \bmod 12$ are there no nontrivial automorphisms and hence it can be made undirected with ease. Alternatively, one could merge the multi-edges, but this would void the regularity of the graph. We now state some properties of our general digraph.

Consider a walk in this digraph from $((A_1, H_1), (A_2, H_2))$ to $((A_2, H_2), (A_3, H_3))$ to $((A_3, H_3), (A_4, H_4))$. Then $\Psi_1(H_1) = H_2$ and $\ker \Psi_2 \cap H_2 = 0$ imply that $\Psi_2 \circ \Psi_1$ is an $(\ell^2)^g$-isogeny, or, in the terminology of [CDS20], we say that $\Psi_2$ is a *good extension* of $\Psi_1$. Inductively, one can then see that a walk of length $n$ in this digraph corresponds to an $(\ell^n)^g$-isogeny between two $g$-dimensional superspecial abelian varieties with an $(\ell)^g$-level structure. The digraph contains some other nice properties, as can be seen in the following proposition.

**Proposition 3.** *The superspecial $(\ell)^g$-isogeny digraph $\mathsf{G}_g(p, \ell)$ is $\ell^{g(g+1)/2}$-regular digraph with number of vertices equal to*

$$\mathcal{O}\left((\ell p)^{g(g+1)/2}\right).$$

*Proof.* The number of superspecial principally polarized abelian varieties over $\overline{\mathbb{F}}_p$ is $c_g p^{g(g+1)/2}$, with $c_g$ some constant depending on $g$ only [ATY24, §1.1]. By [CD22, Lemma 2], the number of maximal isotropic $(\ell)^g$-subgroups for any given abelian variety is

$$\ell^{g(g+1)/2} \cdot \prod_{i=1}^{g} \left(1 + \frac{1}{\ell^i}\right),$$

which is dominated by $\ell^{g(g+1)/2}$. The number of vertices is thus $\mathcal{O}\left((\ell p)^{g(g+1)/2}\right)$. Lastly, the graph is $\ell^{g(g+1)/2}$-regular as this is the number of good extensions for any given maximal isotropic $(\ell)^g$-subgroup [CD22, Lemma 2]. □

**Remark 1.** Unfortunately, we cannot enforce the in-degree of each vertex to be the same. For fixed $p$ and dimension $g$, the number of superspecial $g$-dimensional

abelian varieties over $\overline{\mathbb{F}}_p$ with nontrivial reduced automorphism group is of density zero relative to the total number of superspecial $g$-dimensional abelian varieties over $\overline{\mathbb{F}}_p$ however. The same thus also holds for the number of vertices which do not have in-degree $\ell^{g(g+1)/2}$.

Our main interest is in the expansion properties of superspecial isogeny digraphs. As detailed in Section 2, the eigenvalues of the adjacency matrix $A$ of $\mathsf{G}_g(p,\ell)$ give us important information on such expansion properties. As we are working with directed graphs, we expect these eigenvalues to be complex numbers $\lambda_i \in \mathbb{C}$. We sort these by their modulus, and, by Proposition 3, we have $\lambda_1 = \ell^{g(g+1)/2} + 0 \cdot i$, where $\ell^{g(g+1)/2}$ is the number of good extensions of degree $\ell$. Our main interest for the expansion properties is the modulus and angle of $\lambda_2$, when $p \to \infty$.

**Definition 4.** Let $A$ be the adjacency matrix of $\mathsf{G}_g(p,\ell)$ and let $\lambda_{2,g}(p,\ell)$ be the second largest eigenvalue of $A$. We define the *general second eigenvalue* $\lambda_{2,g}(\ell)$ as the limit $\lim_{p\to\infty} \lambda_{2,g}(p,\ell)$, if this converges.

In light of this definition, we will similarly refer to $\lambda_{1,g}(\ell) = \ell^{g(g+1)/2}$ as the general first eigenvalue.

**Remark 2.** This is in contrast to other isogeny graphs, whose expansion properties can be measured using the *singular values* of the adjacency matrix $A$, which we find by computing $A^\top A$. We cannot take this approach for superspecial isogeny digraphs: transposing $A$ comes down to inverting edges, but inverting the edge $(A_1, H_1) \to (A_2, H_2)$ does not make sense for these graphs, as an edge requires that $A_1 = A_2/H_2$ and, in general, the inverse edge $(A_2, H_2) \to (A_1, H_1)$ will not satisfy $A_2 = A_1/H_1$.

Based on the experimental data for $g = 1$ and $g = 2$, which we detail in Section 4.2, we conjecture the following.

**Main Conjecture.** Let $\lambda_{2,g}(\ell)$ denote the general second eigenvalue of the $(\ell)^g$-isogeny digraph $\mathsf{G}_g(p,\ell)$. Then

$$\lambda_{2,g}(\ell) = \ell^{g^2/2} \in \mathbb{R}.$$

Remark that this implies that the angle of the (complex) second eigenvalue $\lambda_{2,g}(p,\ell)$ converges to zero for $p \to \infty$. Given that $\lambda_{1,g}$ is equal to the number of good extensions $\ell^{g(g+1)/2}$, the conjecture furthermore implies that the spectral expansion $|\lambda_{2,g}|/|\lambda_{1,g}|$ equals $1/\ell^{g/2}$. Finally, as $\ell^{g^2/2} \leq 2\sqrt{\ell^{g(g+1)/2} - 1} \approx 2 \cdot \ell^{g(g+1)/4}$, we claim that the superspecial isogeny digraphs $\mathsf{G}_1(p,\ell)$, $\mathsf{G}_2(p,2)$, $\mathsf{G}_2(p,3)$ converge to have the *weakly Ramanujan* property as $p \to \infty$ in light of Remark 1. Unfortunately, any larger parameter pairs $(g,\ell)$ would fail to even be adjacent-Ramanujan graphs.

### 4.2 Concrete Expansion of Superspecial Isogeny Digraphs

We are interested in concrete expansion properties of superspecial isogeny digraphs in dimension $g = 1$ and $g = 2$ to get an improved understanding of the expansion when considering good extensions.

**Dimension 1** In dimension 1, we not only look at $\ell$-isogeny graphs, but also $N$-isogeny graphs for prime powers $N = \ell^k$. We build the $N$-isogeny digraph $\mathsf{G}_1(p, N)$ by walking around using Vélu's formulas. Although this has the disadvantage of being much slower than working with modular polynomials, our need to identify the correct paths and double edges necessitates the use of torsion bases. In particular, for $N = \ell^k$, we easily identify and compute good extensions for a given node $(E, G)$.

**Lemma 8.** *Let $\ell \neq p$ be a prime, and $N = \ell^k$. Let $(E, G) \in \mathsf{G}_1(p, N)$ with $G = \langle Q \rangle$ for some $Q \in E[N]$ and $P \in E[N] \backslash \langle Q \rangle$. Then, for every $a \in \mathbb{Z}/N\mathbb{Z}$, the isogeny $\varphi : E \to E'$ with $\ker \varphi = \langle P + [a]Q \rangle$ is a good extension from $(E, G)$ to $(E', \varphi(Q))$. Furthermore, all $N$ good extensions of $(E, G)$ are of this form.*

*Proof.* Of the $\ell^k \cdot (\ell+1)$ isogenies of degree $N$ with domain $E$, to ensure non-zero overlap with $\langle Q \rangle$, the kernel must have a generator of the form $P + [a]Q$. We find $N$ such isogenies $\varphi : E \to E'$. The level structure $G'$ on $E'$ is such that $\varphi' : E' \to E'/G$ is the dual of $\varphi$, and is thus given by $G' = \langle \varphi(Q) \rangle$, as this ensures $[N] = \varphi' \circ \varphi$. □

An immediate consequence is that for $N$ prime, every isogeny from $(E, G)$ is a good extension, other than the isogeny with kernel $G$. Thus, for $N$ prime, we may also work with modular polynomials instead of torsion bases to walk around $\mathsf{G}_1(p, N)$.

**Computations.** We have computed $\lambda_2(p, N)$ for all prime powers $N$ up to 32, for primes $p$ up to roughly $2^{14}$.

*Modulus.* We expect $N^{g^2/2} = \sqrt{N}$ as the size of the second eigenvalue. In Figure 1, we show the normalized value $|\lambda_2(p, N)|/\sqrt{N}$ for all prime powers $N \leq 32$, leaving out primes; for primes $N = \ell$, the convergence of the modulus $|\lambda_2(\ell)|$ to $\sqrt{\ell}$ is essentially immediate, hence, it would only be visible as the horizontal line with value 1. For composite $N = \ell^k$, the value $k$ has a large impact on the rate of convergence: we see a far slower convergence for larger $k$.

*Angle.* The angle converges far slower to 0, as is visible in Figure 2. We believe that this is due to the existence of small cycles in the graph, which arise from endomorphisms with a relatively small degree. For example, the action of the class group on the set of $\mathbb{F}_p$-rational supersingular curves creates a cycle of roughly size $h(-p) \approx \sqrt{p}$. The existence of small cycles in isogeny graphs has been studied thoroughly, see [ABCG+26, ACLS+24, BCEM+19, Gha24, LMOS+25, Orv25].

The interpretation for a small angle of $\lambda_2$ is as follows. Normalizing the adjacency matrix of an $m$-regular digraph with a factor $1/m$ yields the transition matrix of a Markov process. The dominant eigenvalue of this normalized matrix is $\lambda_1/m$ and equals one, corresponding to the stationary distribution. The second eigenvalue is $\lambda_2/m = a + bi \in \mathbb{C}$ with accompanying eigenvector $v_2$. The angle

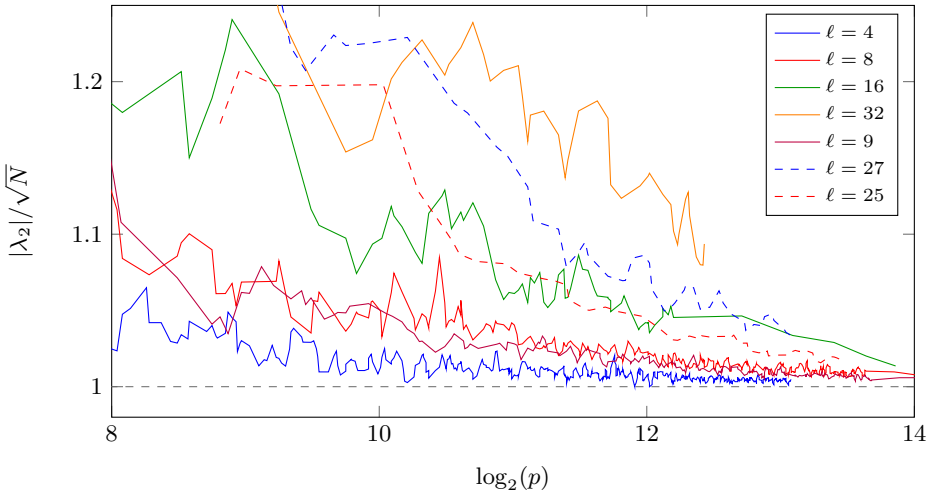



**Fig. 1.** Convergence of normalized $|\lambda_2|$, for prime powers $N \leq 32$

$\theta = \tan^{-1}(b/a)$ measures the strength of directed cyclic motion (i.e. oscillatory behavior) in that eigenmode. If $|b| \ll |a|$, then $|\theta| \approx 0$ and $v_2$'s oscillation in time lacks significant rotational component, hence the directed cycles in the graph responsible for this eigenvalue are almost balanced in forward/backward directions in the support of that eigenvector. The graph thus lacks coherent directed cycles of length related to the phase of this eigenmode (or they exist but are damped heavily by diffusion to other parts). The main dynamic is thus exponential convergence dominated by $a$, with negligible cyclic behavior, similar to an undirected graph.

**Dimension 2.** In dimension 2, we explore the isogeny digraphs $\mathsf{G}_2(\ell, p)$ for $\ell = 2$ using Richelot isogenies [Ric37] and rely heavily on quadratic splittings [Smi05].

*Representing isomorphism classes.* We represent the isomorphism class of a level structure $(A, G)$ using a deterministic quadratic splitting when $A$ is a surface, or by a determinstic pair of elliptic curves and their kernel points when $A$ is a product. When we encounter a level structure $(A, G)$ in the graph, if we have not seen the isomorphism class of $A$ before, we set this level structure as the deterministic representent of $(A, G)$. If we have seen the isomorphism class of $A$ before, represented by some $(A', G')$, we compute all isomorphisms between $A$ and $A'$. If none of these isomorphisms maps $G$ to $G'$, we set $(A, G)$ as the deterministic representant of this isomorphism class of level structures, otherwise, we retrieve $(A', G')$ as the representant. We use the results from Section 3 to verify the number of nodes of $\mathsf{G}_2(p, \ell)$, and Lemmas 9 and 10 to verify the edges.

*The digraph for $\ell = 2$.* When $\ell = 2$, we get $\ell^3 = 8$ good extensions of degree $(\ell, \ell)$. In this subsection, nodes are either Jacobians $J$ or elliptic products $E \times E'$

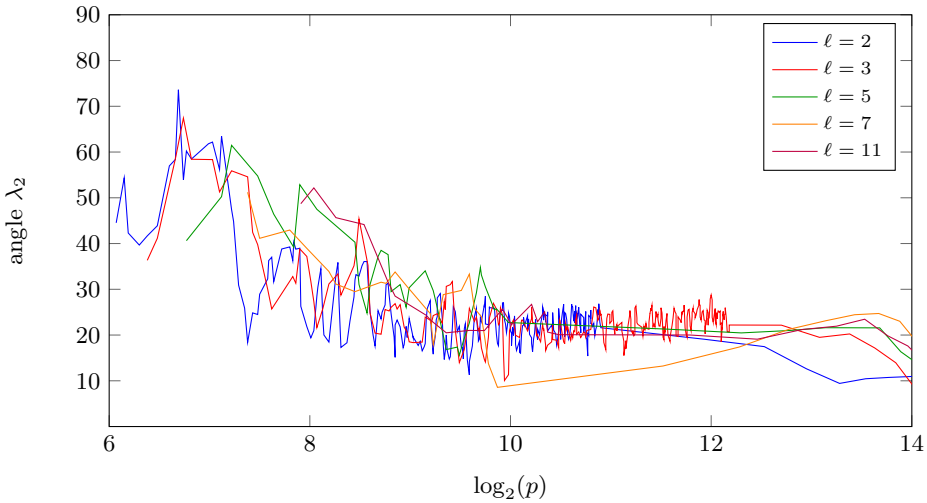



**Fig. 2.** Convergence of angle of $\lambda_2$, for primes $\ell = 2, 3, 5, 7, 11$

with a specified isotropic $(2,2)$-subgroup $G$. By Lemmas 9 and 10 for $\ell = 2$, we can compute these 8 good extensions given $G$ both for Jacobians and products of elliptic curves.

For products of elliptic curves, the fifteen $(2,2)$-isogenies are divided into 9 diagonal isogenies and 6 gluing isogenies. Depending on whether $G$ represents a diagonal or a gluing isogeny $\varphi$, we get:

- if $\varphi$ is a diagonal isogeny, then there are 4 diagonal kernels $G'$ and 4 gluing kernels $G'$ with $G \cap G' = 0$;
- if $\varphi$ is a gluing isogeny, then there are 6 diagonal kernels $G'$ and 2 gluing kernels $G'$ with $G \cap G' = 0$,

We use [EPSV24] to generate a supersingular starting curve $E$, and start walking from $E^2$, keeping track of the level structure.

**Remark 3.** There is one special case for which the normal formulas for diagonal isogenies or gluing isogenies will fail: when $E = E'$, or more generally $E \cong E'$, the $(2,2)$-subgroup $G = \{(P,P) \mid P \in E[2]\}$ is the kernel of the self-dual isogeny[†]

$$\varphi : E \times E \to E \times E, \quad (P,Q) \mapsto (P+Q, P-Q).$$

We count this isogeny as a gluing isogeny because of the shape of its kernel.

**Computations.** We have computed $\mathsf{G}_2(p,\ell)$ for $\ell = 2$ and primes $p < 200$ with $p \equiv 3 \bmod 4$. We find that $\lambda_2 = 4$ for every prime $p$, so that the angle is zero everywhere. Surprisingly, the dimension of the eigenspace associated to $\lambda_2$ grows with $p$, as Figure 3 shows.

[†]One may also derive this $(2,2)$-isogeny from the Kani diagram where all corners are $E$ and all isogenies the identity.

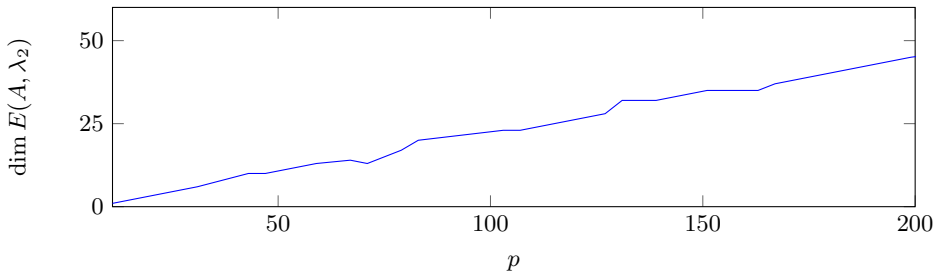



**Fig. 3.** Dimension of the eigenspace of the adjacency matrix of $\mathsf{G}_2(p, \ell)$ for $\lambda_2 = 4$.

*Remark 1.* The dimension of the eigenspace could indicate significant structure in the digraph $\mathsf{G}_2(p, \ell)$, for which we did not find a satisfactory explanation. We leave a full investigation to future work.

## 5 Future work

An evident choice for future work is to see if these heuristic results extend further; i.e. see how the superspecial $(\ell)^g$-isogeny digraph behaves for $g = 2$ and $\ell \geq 3$, for $g > 2$ and any $\ell$. For $g = 2$ and $\ell = 3$, there are significantly more hurdles to compute $\mathsf{G}_2(p, 3)$: the formulas we tried [BFT14, DK23] work for almost all possible isotropic $(3, 3)$-subgroups, apart from some exceptional cases. However, to complete the full graph $\mathsf{G}_2(p, 3)$ these exceptional cases cause a significant issue. The required $(3, 3)$-isogeny computations may be sped up a bit by using the formulas from [CCS25] or [DK26]. The latter would require swapping between level-3 theta structures and isomorphism classes of abelian surfaces, however, and in both cases care would need to be taken to handle the exceptional product surfaces. Furthermore, the large number of edges in combination with the relatively low speed of such isogeny computations make the computation of the full graph at the moment unfeasible. More specifically, we cannot work over small primes $p$, as the proportion of surfaces with non-trivial automorphism group is too large, whereas too large primes $p$ cause infeasibly large adjacency matrices to compute eigenvalues. With the additional restriction $\ell \mid p + 1$ to simplify $(\ell, \ell)$-isogeny computations, this leaves the four primes $p = 41, 47, 53, 59$ as potential candidates to explore $\mathsf{G}_2(p, 3)$. Remark that even for these $p$, the number of abelian surfaces with non-trivial automorphism group still vastly outnumber the ones with $\mathrm{RA}(A) = 1$, potentially skewing the results a lot. Using the exact counts from [CDS20, Proposition 2] and [IKO86, Theorem 3.3], this outnumbering is true for all $p \leq 101$. Note that this plays a lesser role for $\ell = 2$. Indeed: apart from potentially one specific curve, all reduced automorphism groups have an order divisible by two and this seems to make the action on the abelian surfaces with $(\ell, \ell)$-level structure "nicer" in some sense. For instance, generic products $E \times E'$ have zero maximal isotropic $(2, 2)$-subgroups being mapped to one another in the orbit of $[1] \times [-1]$, which is not true for odd $\ell$.

For $\mathsf{G}_2(p,5)$, the work of Cosset and Robert [CR15] is helpful, but these formulas are noticeably more involved than the rather efficient $(2,2)$- and $(3,3)$-isogenies. For $\mathfrak{G}_3(p,2)$, there has been recent work to compute these by means of (multi)radical isogenies in [KMMP+25], although to fully map the graph some nontrivial overhead will come into play, i.e. keeping track of trivially intersecting kernels and swapping from theta structures to isomorphism classes.

Unfortunately, the computational complexity for all these cases quickly explodes due to the fact that there are $\mathcal{O}((\ell p)^{g(g+1)/2})$ vertices in the graph and an increasing amount of edges as well. Besides walking through the entire graph, it also means computing complex eigenvalues of square matrices of dimension $2^{16}$ or larger. Even for sparse matrices for which we only want $\lambda_2$ (which furthermore has a significant gap with $\lambda_1$), more specialized methods start failing. For $g > 2$, it also holds that we have many more potential nontrivial reduced automorphism groups, taking up an exceptional proportion of all superspecial abelian varieties for small $p$. Indeed, the automorphism group of a plane quartic can have an order up to 168. Finally, to actually compute the isogenies, we ideally also have full rational $\ell$-torsion to not have to work over too large extension fields, so specific conditions on $p$ should be met. For these reasons, we expect that a theoretical approach, such as the one from [CGL09], may be more fruitful in further outlining the expander properties of these graphs.

## References


[ATY24] Yusuke Aikawa, Ryokichi Tanaka, and Takuya Yamauchi. "Isogeny graphs on superspecial abelian varieties: eigenvalues and connection to Bruhat–Tits buildings". In: *Canadian Journal of Mathematics* 76.6 (2024), pp. 1891–1916. DOI: 10.4153/S0008414X23000676 (cit. on p. 18).

[ABCG+26] Sarah Arpin, Ross Bowden, James Clements, Wissam Ghantous, Jason T. LeGrow, and Krystal Maughan. "Cycles and cuts in supersingular L-isogeny graphs". In: *Finite Fields and Their Applications* 111 (2026), p. 102768. DOI: 10.1016/j.ffa.2025.102768 (cit. on p. 20).

[ACLS+24] Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, and Ha T. N. Tran. "Orientations and Cycles in Supersingular Isogeny Graphs". In: *Research Directions in Number Theory: Women in Numbers V*. 2024, pp. 25–86. DOI: 10.1007/978-3-031-51677-1_2 (cit. on p. 20).

[BCEM+19] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. "Cycles in the Supersingular $\ell$-Isogeny Graph and Corresponding Endomorphisms". In: *Research Directions in Number Theory*. 2019, pp. 41–66. DOI: 10.1007/978-3-030-19478-9_2 (cit. on p. 20).

[BBCS+25] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. "PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies". In: *PKC 2025 Proceedings, Part III*. Vol. 15676. Lecture Notes in Computer Science. 2025, pp. 300–332. DOI: 10.1007/978-3-031-91826-1_10 (cit. on p. 2).

[BCCF+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. "Supersingular Curves You Can Trust". In: *EUROCRYPT 2023 Proceedings, Part II*. Vol. 14005. Lecture Notes in Computer Science. 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14 (cit. on p. 1).

[BDFL+24] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D-West - The Fast, the Small, and the Safer". In: *ASIACRYPT 2024 Proceedings, Part III*. Vol. 15486. Lecture Notes in Computer Science. 2024, pp. 339–370. DOI: 10.1007/978-981-96-0891-1_11 (cit. on p. 2).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125 (cit. on p. 5).

[BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa. "Descent via (3,3)-isogeny on Jacobians of genus 2 curves". eng. In: *Acta Arithmetica* 165.3 (2014). http://eudml.org/doc/279018, pp. 201–223 (cit. on p. 23).

[CD22] Wouter Castryck and Thomas Decru. "Multiradical isogenies". In: *Arithmetic, Geometry, Cryptography, and Coding theory 2021*. Vol. 779. Contemporary mathematics. 2022, 57–89. DOI: http://doi.org/10.1090/conm/779 (cit. on pp. 8, 18).

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *EUROCRYPT 2023 Proceedings, Part V*. Vol. 14008. Lecture Notes in Computer Science. 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15 (cit. on p. 2).

[CDKL+25] Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, and Yan Bo Ti. "KLPT$^2$: Algebraic Pathfinding in Dimension Two and Applications". In: *CRYPTO 2025 Proceedings, Part I*. Vol. 16000. Lecture Notes in Computer Science. 2025, pp. 167–200. DOI: 10.1007/978-3-032-01855-7_6 (cit. on p. 2).

[CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith. "Hash functions from superspecial genus-2 curves using Richelot isogenies". In: *J. Math. Cryptol.* 14.1 (2020), pp. 268–292. DOI: 10.1515/JMC-2019-0021 (cit. on pp. 2, 7, 8, 18, 23).

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. "Families of Ramanujan Graphs and Quaternion Algebras". In: *CRM Proceedings and Lecture Notes*. Vol. 47. 2009. DOI: 10.1090/crmp/047 (cit. on pp. 2, 24).

[CLG09] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *J. Cryptol.* 22.1 (2009), pp. 93–113. DOI: 10.1007/S00145-007-9002-X (cit. on pp. 1, 18).

[CCS25] Maria Corte-Real Santos, Craig Costello, and Benjamin Smith. "Efficient (3, 3)-isogenies on fast Kummer surfaces". In: *Research in Number Theory* 11.1 (2025), p. 25. DOI: 10.1007/s40993-024-00600-y (cit. on p. 23).

[CR15] Romain Cosset and Damien Robert. "Computing $(\ell, \ell)$-isogenies in polynomial time on Jacobians of genus 2 curves". In: *Mathematics of Computation* 84.294 (2015), pp. 1953–1975. URL: http://www.jstor.org/stable/24489183 (cit. on p. 24).

[DEFM+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies". In: *CRYPTO 2025 Proceedings, Part I*. Vol. 16000. Lecture Notes in Computer Science. 2025, pp. 67–99. DOI: 10.1007/978-3-032-01855-7_3 (cit. on p. 2).

[DLRW24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. "SQIsignHD: New Dimensions in Cryptography". In: *EUROCRYPT 2024 Proceedings, Part I*. Vol. 14651. Lecture Notes in Computer Science. 2024, pp. 3–32. DOI: 10.1007/978-3-031-58716-0_1 (cit. on p. 2).

[DK23] Thomas Decru and Sabrina Kunzweiler. "Efficient Computation of $(3^n, 3^n)$-Isogenies". In: *AFRICACRYPT 2023 Proceedings*. Vol. 14064. Lecture Notes in Computer Science. 2023, pp. 53–78. DOI: 10.1007/978-3-031-37679-5_3 (cit. on p. 23).

[DK26] Thomas Decru and Sabrina Kunzweiler. *Abelian surfaces in Hesse form and explicit isogeny formulas*. Cryptology ePrint Archive, Paper 2026/039. 2026. URL: https://eprint.iacr.org/2026/039 (cit. on p. 23).

[DM] Holger Dell and Dieter van Melkebeek. *Pseudorandomness and Derandomization, Lecture 9: Expanders*. https://pages.cs.wisc.edu/~dieter/Courses/2013s-CS880/Scribes/PDF/lecture09.pdf (cit. on p. 11).

[DF24] Max Duparc and Tako Boris Fouotsa. "SQIPrime: A Dimension 2 Variant of SQISignHD with Non-smooth Challenge Isogenies". In: *ASIACRYPT 2024 Proceedings, Part III*. Vol. 15486. Lecture Notes in Computer Science. 2024, pp. 396–429. DOI: 10.1007/978-981-96-0891-1_13 (cit. on p. 2).

[EHLM+18] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *EUROCRYPT 2018 Proceedings, Part III*. Vol. 10822. Lecture Notes in Computer Science. 2018, pp. 329–368. DOI: 10.1007/978-3-319-78372-7_11 (cit. on p. 1).

[EPSV24] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. "Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic". In: *LuCaNT: LMFDB, Computation, and Number Theory*. Vol. 796. Contemporary mathematics. 2024, pp. 339–373. DOI: 10.1090/conm/796 (cit. on p. 22).

[EFMP26] Shai Evra, Brooke Feigon, Kathrin Maurischat, and Ori Parzanchevski. *Ramanujan Bigraphs*. 2026. arXiv: 2312.06507 [math.NT]. URL: https://arxiv.org/abs/2312.06507 (cit. on p. 10).

[FKLP+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *ASIACRYPT 2020 Proceedings, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. Lecture Notes in Computer Science. 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3 (cit. on p. 2).

[FS22a] Enric Florit and Benjamin Smith. "An atlas of the Richelot isogeny graph". In: *Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties*. Vol. B90. RIMS Kôkyûroku Bessatsu. Res. Inst. Math. Sci. (RIMS), Kyoto, 2022, pp. 195–219. URL: http://hdl.handle.net/2433/276282 (cit. on pp. 11, 14–16, 31–33, 36, 39, 43, 44, 46).

[FS22b] Enric Florit and Benjamin Smith. "Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph". In: *Arithmetic, Geometry, Cryptography, and Coding theory 2021*. Vol. 779. Contemporary mathematics. 2022, 103–132. DOI: http://doi.org/10.1090/conm/779 (cit. on p. 2).

[FT19] E. Victor Flynn and Yan Bo Ti. "Genus Two Isogeny Cryptography". In: *PQCrypto 2019 Proceedings*. Vol. 11505. Lecture Notes in Computer Science. 2019, pp. 286–306. DOI: 10.1007/978-3-030-25510-7_16 (cit. on p. 2).

[Gha24] Wissam Ghantous. "Loops, multi-edges and collisions in supersingular isogeny graphs". In: *Advances in Mathematics of Com-*

*munications* 18.4 (2024), pp. 935–955. DOI: 10.3934/amc.2022038 (cit. on p. 20).

[IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. "Supersingular curves of genus two and class numbers". In: *Compositio Mathematica* 57.2 (1986), pp. 127–152. URL: http://eudml.org/doc/89752 (cit. on pp. 23, 31, 36, 38, 41).

[JF11] David Jao and Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *PQCrypto 2011 Proceedings*. Vol. 7071. Lecture Notes in Computer Science. 2011, pp. 19–34. DOI: 10.1007/978-3-642-25405-5_2 (cit. on p. 2).

[JZ26] Bruce W. Jordan and Yevgeny Zaytman. "Isogeny graphs of superspecial abelian varieties and Brandt matrices". In: *J. Math. Soc. Japan*. Advance Publication (Mar. 2026), pp. 1–40. DOI: 10.2969/jmsj/91629162 (cit. on p. 2).

[Kan97] Ernst Kani. "The number of curves of genus two with elliptic differentials." In: *Journal für die reine und angewandte Mathematik* 1997.485 (1997), pp. 93–122. DOI: doi:10.1515/crll.1997.485.93 (cit. on p. 2).

[KLPT14] David Kohel, Kristin E. Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion -isogeny path problem". In: *LMS J. Comput. Math.* 17.Theory (2014), pp. 418–432. DOI: 10.1112/S1461157014000151 (cit. on p. 1).

[KMMP+25] Sabrina Kunzweiler, Luciano Maino, Tomoki Moriya, Christophe Petit, Giacomo Pope, Damien Robert, Miha Stopar, and Yan Bo Ti. "Radical 2-Isogenies and Cryptographic Hash Functions in Dimensions 1, 2 and 3". In: *PKC 2025 Proceedings, Part III*. Vol. 15676. Lecture Notes in Computer Science. 2025, pp. 265–299. DOI: 10.1007/978-3-031-91826-1_9 (cit. on p. 24).

[KTW22] Sabrina Kunzweiler, Yan Bo Ti, and Charlotte Weitkämper. "Secret Keys in Genus-2 SIDH". In: *SAC 2021: 28th Annual International Workshop on Selected Areas in Cryptography*. Vol. 13203. Lecture Notes in Computer Science. 2022, pp. 483–507. DOI: 10.1007/978-3-030-99277-4_23 (cit. on pp. 17, 50).

[LMOS+25] Jun Bo Lau, Travis Morrison, Eli Orvis, Gabrielle Scullard, and Lukas Zobernig. *Zeta functions of abstract isogeny graphs and modular curves*. 2025. URL: https://arxiv.org/abs/2509.15214 (cit. on p. 20).

[LLP20] Eyal Lubetzky, Alexander Lubotzky, and Ori Parzanchevski. "Random walks on Ramanujan complexes and digraphs". In: *J. Eur. Math. Soc.* 22.11 (2020), pp. 3441–3466. DOI: 10.4171/JEMS/990 (cit. on p. 10).

[MMPP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *EUROCRYPT 2023 Proceedings, Part V*. Vol. 14008.

Lecture Notes in Computer Science. 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16 (cit. on p. 2).

[NOCC+24] Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. "SQIsign2D-East: A New Signature Scheme Using 2-Dimensional Isogenies". In: *ASIACRYPT 2024 Proceedings, Part III*. Vol. 15486. Lecture Notes in Computer Science. 2024, pp. 272–303. DOI: 10.1007/978-981-96-0891-1_9 (cit. on p. 2).

[Orv25] Eli Orvis. "Distribution of cycles in supersingular $\ell$-isogeny graphs". In: *Journal of Number Theory* 277 (2025), pp. 236–261. DOI: https://doi.org/10.1016/j.jnt.2025.03.013 (cit. on p. 20).

[Par20] Ori Parzanchevski. "Ramanujan Graphs and Digraphs". In: *Analysis and Geometry on Graphs and Manifolds*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2020, pp. 344–367. DOI: 10.1017/9781108615259.014 (cit. on p. 10).

[Ric37] Friedrich Julius Richelot. "De transformatione integralium Abelianorum primi ordinis commentatio. Caput secundum. De computatione integralium Abelianorum primi ordinis." In: *Journal für die reine und angewandte Mathematik* 1837.16 (1837), pp. 285–341. DOI: doi:10.1515/crll.1837.16.285 (cit. on pp. 9, 21).

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time". In: *EUROCRYPT 2023 Proceedings, Part V*. Vol. 14008. Lecture Notes in Computer Science. 2023, pp. 472–503. DOI: 10.1007/978-3-031-30589-4_17 (cit. on p. 2).

[Rob24] Damien Robert. *The module action for isogeny based cryptography*. Cryptology ePrint Archive, Paper 2024/1556. 2024. URL: https://eprint.iacr.org/2024/1556 (cit. on p. 2).

[The24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.4)*. https://www.sagemath.org. 2024 (cit. on p. 5).

[Smi05] Benjamin Smith. "Explicit endomorphisms and correspondences". PhD thesis. University of Sydney, 2005 (cit. on pp. 9, 21).

[Tak18] Katsuyuki Takashima. "Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications". In: *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*. 2018, pp. 97–114. DOI: 10.1007/978-981-10-5065-7_6 (cit. on p. 2).

[Vad] Salil P. Vadhan. *Harvard lecture notes, Pseudorandomness I, Chapter 4: Expander graphs*. https://people.seas.harvard.edu/~salil/cs225/spring09/lecnotes/Chap4.pdf (cit. on p. 11).

[Vél71] Jacques Vélu. “Isogénies entre courbes elliptiques”. In: *Comptes-Rendus de l’Académie des Sciences* 273 (1971), pp. 238–241 (cit. on p. 9).

[Wal63] G. E. Wall. “On the conjugacy classes in the unitary, symplectic and orthogonal groups”. In: *Journal of the Australian Mathematical Society* 3.1 (1963), pp. 1–62. DOI: 10.1017/S1446788700027622 (cit. on p. 12).

## A Automorphisms of Curves and Jacobians

Florit and Smith [FS22a] give a detailed atlas of the nontrivial automorphisms in genus 2, classified by the shape of the hyperelliptic curve. Whereas Florit and Smith mainly use Bolza's names in their classification, we will strictly refer to Jacobians with respect to a certain reduced automorphism group. We mainly do so to avoid confusion: the naming in type system has no relation to the order of the automorphisms, which makes it harder to remember which type refers to which automorphism.

*Jacobians.* Figure 5 shows the 7 possible groups $\mathrm{RA}(J)$. Beyond the 3-dimensional moduli space of generic Jacobians with $\mathrm{RA}(J) = 1$, nontrivial automorphisms only appear in specific situations. All Jacobians where $\mathrm{RA}(J)$ has a $\mathbb{Z}/2\mathbb{Z}$-component are $(2,2)$-isogenous to a product of elliptic curves $E \times E'$, which gives a 2-dimensional subspace. The 1-dimensional moduli subspaces are given by restrictions between $E$ and $E'$. If $E = E'$ and $E$ has no nontrivial automorphisms, the $(2,2)$-isogenous Jacobians have $\mathrm{RA}(J) = (\mathbb{Z}/2\mathbb{Z})^2$, and if $E$ and $E'$ are 3-isogenous by $\varphi$, the Jacobians with $\mathrm{RA}(J) = \mathcal{S}_3$ are given by $J = (E \times E')/\Gamma$ where $\Gamma = \{(P, \varphi(P)) \mid P \in E[2]\}$.[‡]

The 0-dimensional moduli subspaces are all unique up to isomorphism. The only Jacobian $J$ with $\mathrm{RA}(J) \cong \mathcal{D}_{2\times 6}$ is $(2,2)$-isogenous to $E_0 \times E_0$, and is the Jacobian of the curve $C : y^2 = x^6 + 1$. The only Jacobian $J$ with $\mathrm{RA}(J) = \mathcal{S}_4$ is the Jacobian of the curve $C : y^2 = x^5 - x$, and is $(2,2)$-isogenous to the exceptional curve[§] $E \times E$ where $j(E) = 8000$. Lastly, the Jacobian $J$ with $\mathrm{RA}(J) \cong \mathbb{Z}/5\mathbb{Z}$ is *not* $(2,2)$-isogenous to a product of curves; it is the Jacobian of the curve $C : y^2 = x^5 - 1$.

**Remark 4.** The Jacobian of $C : y^2 = x^6 + 1$ is superspecial iff $p \equiv 5 \bmod 6$, the Jacobian of $C : y^2 = x^5 - x$ is superspecial iff $p \equiv 5, 7 \bmod 8$, and the Jacobian of $C : y^2 = x^5 - 1$ is superspecial iff $p \equiv 4 \bmod 5$ (see for example [IKO86, Theorem 3.3]).

These reduced automorphism groups can be described with only a few automorphisms, because subtypes inherit automorphisms from their supertypes. We use the greek letter to denote the automorphism on (the $x$-coordinate of) the curve $C$, and the subscript $*$ to denote the action on elements of the Jacobian $J = \mathrm{Jac}(C)$. We give an overview of Jacobians and their reduced automorphism groups in Table 5, with the specific automorphisms described in Table 4.

[‡]This unique behavior can be explained by the Kani diagram with factorizations $E \xrightarrow{\varphi} E' \to E'$ and $E \to E \xrightarrow{\varphi} E'$, which implies that $E \times E'$ has a $(4,4)$-endomorphism that splits via $J$.

[§]These requirements force $E$ to have a degree-3 endomorphism, making this a specialized case of the two cases above: we have both $E = E'$ and a 3-isogeny $\varphi : E \to E'$.

[‖]The automorphism $\omega$ from Eq. (2) acts on the isomorphic curve $y^2 = (x^2-1)(x^2 - s_v)(x^2 - t_v)$ following Eq. (1) with $v = (\zeta_{12}^2 + \zeta_{12} + 1)/\sqrt{2}$.

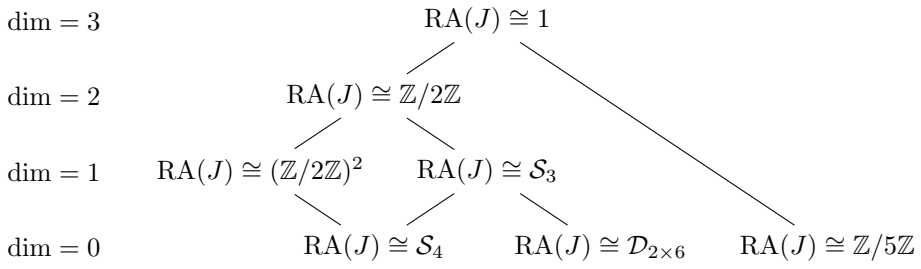



**Fig. 4.** A direct copy of Figure 1 from [FS22a], showing the possible reduced automorphism groups of 2-dimensional Jacobians. Lines indicate subtypes.

**Table 3.** Possible reduced automorphism groups of Jacobians

| RA($J$) | Dimension | $(2,2)$-isogenous $E \times E'$ | Generators |
|---|---|---|---|
| 1 | 3 | - | - |
| $\mathbb{Z}/2\mathbb{Z}$ | 2 | generic $E$, $E'$ | $\sigma_*$ |
| $(\mathbb{Z}/2\mathbb{Z})^2$ | 1 | isomorphic $E \to E'$ | $\sigma_*$, $\tau_*$ |
| $\mathcal{S}_3$ | 1 | 3-isogenous $E \to E'$ | $\sigma_*$, $\rho_*$ |
| $\mathcal{S}_4$ | 0 | $E$ with 3-endomorphism | $\rho_*$, $\omega_*$ |
| $\mathcal{D}_{2\times 6}$ | 0 | $E_0 \times E_0$ | $\tau_*$, $\zeta_*^{(6)}$ |
| $\mathbb{Z}/5\mathbb{Z}$ | 0 | - | $\zeta_*^{(5)}$ |

$$\begin{aligned} \rho : x &\mapsto \frac{(2\zeta_3+1)(v^2-1)x + 3(v+1)^2}{3(v-1)^2 x + (2\zeta_3+1)(v^2-1)}, \\ s_v := \frac{(v+1)(v-\zeta_3)}{(v-1)(v+\zeta_3)}, &\qquad t_v := \frac{(v+1)(v-\zeta_3^2)}{(v-1)(v+\zeta_3^2)} \end{aligned} \tag{1}$$

$$\omega : x \mapsto \frac{x - (\sqrt{2}+1)}{(\sqrt{2}-1)x + 1} \tag{2}$$

*Products of Elliptic Curves.* In the case of elliptic curves, there are seven possible reduced automorphism groups, where most nontrivial automorphisms are derived from the nontrivial automorphisms on $E_0$ and $E_{1728}$.

See Table 6 for the specific automorphisms on elliptic products.

## B Reduced automorphisms on Jacobians of genus-2 curves

We discuss the remaining five cases of the action of nontrivial automorphisms on Jacobians with level structure.

**Table 4.** Automorphisms on specific types of Jacobians

| **Autom.** | On $C$ | Order | Conditions on Curve Eq. |
|---|---|---|---|
| $\sigma$ | $x \mapsto -x$ | 2 | $y^2 = (x^2-1)(x^2-s)(x^2-t)$ |
| $\tau$ | $x \mapsto 1/x$ | 2 | $y^2 = (x^2-1)(x^2-u^2)(x^2-\frac{1}{u^2})$ |
| $\rho$ | See Eq. (1) | 3 | $y^2 = (x^2-1)(x^2-s_v)(x^2-t_v)$ |
| $\zeta^{(6)}$ | $x \mapsto \zeta_6 x$ | 6 | $y^2 = x^6+1$ |
| $\omega$ | See Eq. (2) | 4 | $y^2 = x^5 - x$[¶] |
| $\zeta^{(5)}$ | $x \mapsto \zeta_5 x$ | 5 | $y^2 = x^5 - 1$ |

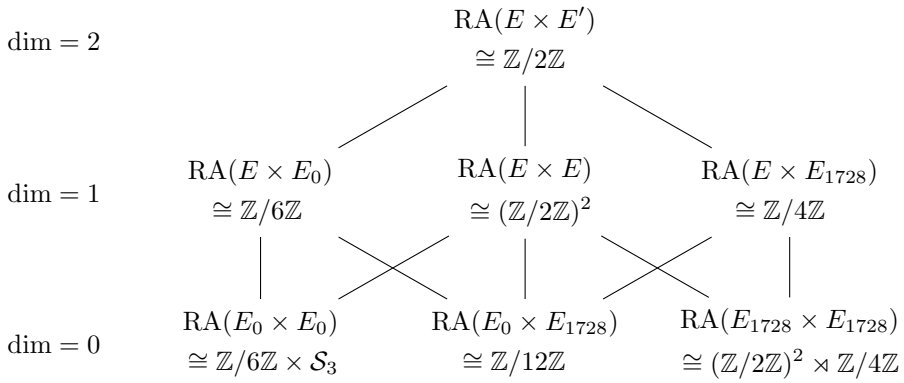



**Fig. 5.** A direct copy of Figure 2 from [FS22a], showing the possible reduced automorphism groups of products of elliptic curves. Lines indicate subtypes.

**$\mathrm{RA}(J) = \mathcal{S}_3$** This is a one-parameter family of curves $C$ which are a specialization of the case for which the reduced automorphism group is $\mathbb{Z}/2\mathbb{Z}$. More specifically, define

$$C : y^2 = (x^2-1)(x^2-s^2)(x^2-t^2),$$

with

$$s = \frac{(v+1)(v-\zeta_3)}{(v-1)(v+\zeta_3)}, \quad t = \frac{(v+1)(v-\zeta_3^2)}{(v-1)(v+\zeta_3^2)},$$

where $v$ is a free parameter and $\zeta_3$ a cubic root of unity. The extra automorphism of order 3 is given by

$$\rho : x \mapsto \frac{(2\zeta_3+1)(v^2-1)x + 3(v+1)^2}{3(v-1)^2 x + (2\zeta_3+1)(v^2-1)}.$$

We have the following characterization of the action of $\rho_*$ on abelian surfaces with $(\ell,\ell)$-level structure.

**Proposition 4.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $\mathrm{RA}(C) = \mathcal{S}_3$, with $\rho$ an automorphism of order 3 (given as above), and*

**Table 5.** Possible reduced automorphism groups of products of elliptic curves

| $\mathrm{RA}(E \times E')$ | Dimension | Properties | Generators |
|---|---|---|---|
| $\mathbb{Z}/2\mathbb{Z}$ | 2 | generic $E, E'$ | $\kappa$ |
| $(\mathbb{Z}/2\mathbb{Z})^2$ | 1 | isomorphic $E \cong E'$ | $\kappa$, $\chi$ |
| $\mathbb{Z}/6\mathbb{Z}$ | 1 | $E' \cong E_0$ | $[1] \times -\zeta^{(3)}$ |
| $\mathbb{Z}/4\mathbb{Z}$ | 1 | $E' \cong E_{1728}$ | $[1] \times \iota$ |
| $\mathbb{Z}/12\mathbb{Z}$ | 0 | $E \cong E_{1728}$, $E' \cong E_0$ | $\iota \times \zeta^{(3)}$ |
| $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$ | 0 | $E \cong E' \cong E_{1728}$ | $\chi$, $[1] \times \iota$ |
| $\mathbb{Z}/6\mathbb{Z} \times \mathcal{S}_3$ | 0 | $E \cong E' \cong E_0$ | $\chi$, $[1] \times -\zeta^{(3)}$ |

**Table 6.** Automorphisms on products of elliptic curves

| **Autom.** | Action on $E \times E'$ | Order | Types |
|---|---|---|---|
| $\kappa$ | $(P, Q) \mapsto (P,\ -Q)$ | 2 | - |
| $\chi$ | $(P, Q) \mapsto (Q,\ P)$ | 2 | $E \cong E'$ |
| $[1] \times \zeta^{(3)}$ | $(P, Q) \mapsto (P,\ (\zeta_3 x_Q, y_Q))$ | 3 | $E' \cong E_0$ |
| $[1] \times \iota$ | $(P, Q) \mapsto (P,\ (-x_Q, i y_Q))$ | 4 | $E' \cong E_{1728}$ |

*$\ell \neq p$ a prime. Then the induced automorphism $\rho_*$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 3 |
|---|---|---|
| $\ell = 3$ | 7 | 33 |
| $\ell \equiv 1 \bmod 3$ | $\ell + 3$ | $\ell^3 + \ell^2 - 2$ |
| $\ell \equiv 2 \bmod 3$ | $\ell + 1$ | $\ell^3 + \ell^2$ |

*Proof.* Since $\rho_*^3 = \mathtt{id}$, its minimal polynomial is $\Phi_3 = x^2 + x + 1$ with eigenvalues the two primitive cubic roots of unity. For any symplectic basis of $J[\ell]$, with $\ell \neq 3$, the linear map that represents the action of $\rho_*$ on this basis is hence diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(\mu_3, \mu_3, \mu_3^2, \mu_3^2) \in \mathrm{Sp}(\overline{\mathbb{F}_\ell})$.

(i) For $\ell = 3$, the $\rho$-invariant points of $C$ are

$$Q_{\pm,\pm} = \left( \pm \frac{v+1}{v-1}, \pm 8 \cdot \frac{v\sqrt{v}(v+1)^2}{(v-1)^3(v+\zeta_3)(v+\zeta_3^2)} \right).$$

One can verify that the $\rho^2$-invariant points on $C$ are also just $Q_{\pm,\pm}$, since the map $\rho^2$ is the same as $\rho$ apart from the factors $(2\zeta_3 + 1)$ now having a minus sign in front. From these we can build exactly two one-dimensional

$\rho_*$-invariant subspaces, say

$$H_+ = \langle Q_{+,+} - Q_{+,-} \rangle, \qquad H_- = \langle Q_{-,+} - Q_{-,-} \rangle.$$

One can verify that these have trivial 3-Weil pairing, hence $\rho_*$ is given by

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

for some symplectic basis. We immediately see that $\langle H_+, H_- \rangle$ as well as the upper left block and the bottom right block create three maximal isotropic $\rho_*$-invariant subspaces. Remark that the blocks are *not* irreducible, hence Lemma 7 does not hold. However, following the proof of Lemma 7, it is clear we only need to consider the 1-dimensional subspace case separately (which we have by means of $H_+$ and $H_-$), so the other subspaces are created by isomorphisms between the blocks. These correspond to lines so there are $\ell+1$ of them and the isotropy condition follows from the symplectic basis.

(ii) For $\ell \equiv 1 \bmod 3$, a primitive cubic root of unity $\mu_3 \in \mathbb{F}_\ell$ exists such that $\Phi_3$ splits completely modulo $\ell$. Hence, $\rho_*$ can be given by $\mathrm{diag}(\mu_3, \mu_3, \mu_3^2, \mu_3^2) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ for some symplectic basis. We thus have $\ell + 3$ maximal isotropic subgroups which are $\rho_*$-invariant just as in Proposition 2(ii).

(iii) For $\ell \equiv 2 \bmod 3$, $\Phi_3$ is irreducible modulo $\ell$ and for a suitable choice of basis $\langle D_1, D_2, D_1', D_2' \rangle$, by Lemma 2 and Lemma 3, we may assume that $\rho_*$ acts as

$$\Gamma = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

Remark that $\Gamma$ is in "blocks" acting on $\langle D_1, D_1' \rangle$ and $\langle D_2, D_2' \rangle$. By Lemma 7, the only possible $\rho_*$-invariant maximal isotropic subspaces are $\langle D_1, D_1' \rangle$, $\langle D_2, D_2' \rangle$ (which are not isotropic) and all graphs consisting of isomorphisms $\langle D_1, D_1' \rangle \to \langle D_2, D_2' \rangle$. There are $\ell + 1$ of those just as in Proposition 2(iii).

□

Since $\mathrm{RA}(J) = \langle \sigma_*, \rho_* \rangle$, we have the following result.

**Theorem 3.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $J$ its Jacobian, $\mathrm{RA}(J) = \mathcal{S}_3$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(J, G)$ is equal to 7 if $\ell = 2$, equal to 17 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{6}\left(\ell^3 + 4\ell^2 + 9\ell + 8 + 2\left(\frac{\ell}{3}\right)\right).$$

*Proof.* Burnside's lemma says that the number of abelian surfaces with $(\ell,\ell)$-level structure is equal to

$$\frac{1}{|\mathcal{S}_3|}\cdot\left(|X^{\mathtt{id}}|+|X^{\sigma_*}|+|X^{\rho_*}|+|X^{\rho_*^2}|+|X^{\rho_*\sigma_*}|+|X^{\rho_*^2\sigma_*}|\right).$$

By Propositions 1 and 4 and it suffices to check $X^{\rho_*\sigma_*}$ and $X^{\rho_*^2\sigma_*}$. One can verify that the minimal polynomial of both $\rho_*\sigma_*$ and $\rho_*^2\sigma_*$ is $x^2-1$, so the orbits act exactly the same as $\sigma_*$ from Proposition 1.

□

**$\mathrm{RA}(J)=\mathcal{D}_{2\times 6}$** This case only occurs if the Jacobian stems from the genus-2 curve defined by $C: y^2=x^6+1$, and the automorphism is given by $\zeta^{(6)}: x\mapsto \zeta_6 x$, where $\zeta_6$ is a primitive sixth root of unity in $\overline{\mathbb{F}}_p$. This is a special case of $\mathrm{RA}(C)=(\mathbb{Z}/2\mathbb{Z})^2$, where $(\zeta^{(6)})^3=\sigma: x\mapsto -x$, such that $\mathrm{RA}(C)=\langle\tau,\zeta^{(6)}\rangle$. The curve is superspecial iff $p\equiv 5 \bmod 6$, see [IKO86, Proposition 1.11]. We have the following characterization of the action of $\zeta_*^{(6)}$ on abelian surfaces with $(\ell,\ell)$-level structure.

**Proposition 5.** *Let $C: y^2=x^6+1$ be a genus-2 curve over a field of characteristic $p>5$, with $\zeta^{(6)}: x\mapsto\zeta_6 x$ an automorphism of order 6, and $\ell\neq p$ a prime. Then the induced automorphism $\zeta_*^{(6)}$ acts on the abelian surfaces with $(\ell,\ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 | surfaces in orbits of size 3 | surfaces in orbits of size 6 |
|---|---|---|---|---|
| $\ell=2$ | 1 | 2 | 6 | 6 |
| $\ell=3$ | 1 | 6 | 15 | 18 |
| $\ell\equiv 1 \bmod 3$ | 4 | $\ell-1$ | $(\ell+1)^2-4$ | $\ell^3-2\ell+1$ |
| $\ell\equiv 2 \bmod 3$ | 0 | $\ell+1$ | $(\ell+1)^2$ | $\ell^3-2\ell-1$ |

*Proof.* Since $\zeta_*^{(6)}=\mathtt{id}$, its minimal polynomial must divide $x^6-1$ and one can verify that it equals $x^4+x^2+1=(x^2-x+1)(x^2+x+1)=\Phi_6\Phi_3$, with eigenvalues the third and sixth primitive roots of unity. For any symplectic basis of $J[\ell]$, with $\ell>3$, the linear map that represents the action of $\zeta_*^{(6)}$ on this basis is hence diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(\mu_3,-\mu_3,\mu_3^2,-\mu_3^2)\in\mathrm{Sp}(\overline{\mathbb{F}_\ell})$.

(i) For $\ell=2$, see [FS22a, Section 4.11].

(ii) For $\ell=3$, the minimal polynomial reduces to $(x-1)^2(x+1)^2 \bmod 3$. Given that this concerns one specific $\ell$ for one specific curve (up to isomorphism), the count is a direct computation. For the sake of completeness, the sym-

plectic matrices of $\zeta_*^{(6)}$, $(\zeta_*^{(6)})^2$ and $(\zeta_*^{(6)})^3$ are given by respectively

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Remark that the last one equals the one of Proposition 1 since $(\zeta_*^{(6)})^3 = \sigma_*$.

(iii) For $\ell \equiv 1 \bmod 3$, a primitive cubic root of unity $\mu_3 \in \mathbb{F}_\ell$ exists such that the minimal polynomial splits completely modulo $\ell$ and $\zeta_*^{(6)}$ acts as $\operatorname{diag}(\mu_3, -\mu_3, \mu_3^2, -\mu_3^2) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ on some symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$. By Lemma 6, the $\zeta_*^{(6)}$-invariant maximal isotropic subspaces are direct sums of two one-dimensional eigenspaces. We thus have four $\zeta_*^{(6)}$-invariant maximal isotropic subspaces:

$$\langle D_1, D_2 \rangle, \langle D_1, D_2' \rangle, \langle D_1', D_2 \rangle, \langle D_1', D_2' \rangle.$$

Squaring this matrix results in $\operatorname{diag}(\mu_3^2, \mu_3^2, \mu_3, \mu_3) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$. By checking the $e_\ell$-pairing, one can readily verify that any two-dimensional subspace consisting of a line in the eigenspace with eigenvalue $\mu_3^2$ has exactly one line in the eigenspace with eigenvalue $\mu_3$ which creates a maximal isotropic subgroup. There are thus $\ell - 1$ $(\zeta_*^{(6)})^2$-invariant subspaces (since we already counted $\langle D_1, D_2' \rangle$ and $\langle D_2, D_1' \rangle$). We also know that $(\zeta_*^{(6)})^3 = \sigma_*$, which has $(\ell+1)^2$ invariant maximal isotropic subspaces. Remark that we need to subtract the $\zeta_*^{(6)}$-invariant ones from this count, but not the $(\zeta_*^{(6)})^2$-invariant ones since these do not overlap.

(iv) For $\ell \equiv 2 \bmod 3$, the minimal polynomial is irreducible modulo $\ell$ and for a suitable choice of basis $\langle D_1, D_2, D_1', D_2' \rangle$ we can write that $\zeta_*^{(6)}$ acts as

$$\Gamma = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

by Lemma 2 and Lemma 3. This decomposes as a direct summand as it acts in "blocks" on $\langle D_1, D_1' \rangle$ and $\langle D_2, D_2' \rangle$. Since they are not similar, it follows from Lemma 7 that the only $\zeta_*^{(6)}$-invariant subspaces are $\langle D_1, D_1' \rangle$ and $\langle D_2, D_2' \rangle$ but those are not isotropic. The action of $(\zeta_*^{(6)})^2$ is then given by

$$\Gamma^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell),$$

where the "blocks" are now similar, hence by Lemma 7 the $\ell+1$ isomorphisms between them provide the $(\zeta_*^{(6)})^2$-invariant maximal isotropic subgroups. The case $(\zeta_*^{(6)})^3 = \sigma_*$ is as before.

□

Combining this proposition with Proposition 2 we get the following result.

**Theorem 4.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $J$ its Jacobian, $\mathrm{RA}(J) = \mathcal{D}_{2\times 6}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell,\ell)$-level structure $(J, G)$ is equal to 5 if $\ell = 2$, equal to 11 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{12}\left(\ell^3 + 5\ell^2 + 14\ell + 19 + 3\left(\frac{-1}{\ell}\right) + 6\left(\frac{\ell}{3}\right)\right).$$

*Proof.* Burnside's lemma says that the number of abelian surfaces with $(\ell,\ell)$-level structure is equal to

$$\frac{1}{|\mathcal{D}_{2\times 6}|}\cdot\left(|X^{\mathtt{id}}| + \sum_{k=1}^{5}|X^{(\zeta_*^{(6)})^k}| + |X^{\tau_*}| + \sum_{i=1}^{5}|X^{\tau_*(\zeta_*^{(6)})^k}|\right).$$

By Propositions 2 and 5 we need only verify the $X^{\tau_*(\zeta^{(6)})_*^k}$ for $1 \leq k \leq 5$. For $k = 3$ we have that $\tau_*(\zeta^{(6)})_*^k = \tau_*\sigma_*$, which has the same number of fixed points as $\sigma_*$ as we have shown in the proof of Theorem 2. One can verify that the minimal polynomial of $\tau_*\zeta_*^{(6)}$ and $\tau_*(\zeta_*^{(6)})^5$ is $x^2-1$, so the orbits act exactly the same as $\sigma_*$ from Proposition 1. Similarly, the minimal polynomial of $\tau_*(\zeta_*^{(6)})^2$ and $\tau_*(\zeta_*^{(6)})^4$ is $x^2+1$, so the orbits act exactly the same as $\tau_*$ from Proposition 2. □

**$\mathrm{RA}(J) = \mathcal{S}_4$** This is a special case of $\mathrm{RA}(C) = \mathcal{S}_3$ where we need to choose

$$v = \frac{1}{\sqrt{2}}(\zeta_{12}^2 + \zeta_{12} + 1).$$

Remark that there exists a $(2,2)$-isogeny from the Jacobian of $C$ to $E^2$, with $j(E) = 8000$. The extra automorphism to generate $\mathcal{S}_4$ is given by

$$\omega : x \mapsto \frac{x - (\sqrt{2}+1)}{(\sqrt{2}-1)x + 1}.$$

Since this is a specialization of a previous case, we have that $\mathrm{RA}(C) = \mathcal{S}_4 = \langle\sigma,\rho,\omega\rangle = \langle\rho,\omega\rangle$, where $\omega$ has order four. The curve is superspecial iff $p \equiv 5, 7 \bmod 8$, see [IKO86, Proposition 1.12]. Note that as a nonreduced automorphism, $\omega$ has order eight![‖] We have the following characterization of the action of $\omega_*$ on abelian surfaces with $(\ell,\ell)$-level structure.

[‖] The curve in question is isomorphic to $C : y^2 = x^5 - x$, with the new automorphism given by $(x, y) \mapsto (ix, \sqrt{i}y)$. In a vacuum, it would be easier to work with this defining equation, but we will use the other automorphisms up ahead as well so we stick with the choice of $v$. Remark that over a field of characteristic five, this curve actually has $\mathrm{RA}(C) = \mathrm{PGL}(2,5) \cong \mathcal{S}_5$ [IKO86].

**Proposition 6.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$, with $\omega$ an automorphism of order 8, and $\ell \neq p$ a prime. Then the induced automorphism $\omega_*$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 | surfaces in orbits of size 4 |
|---|---|---|---|
| $\ell = 2$ | 1 | 2 | 12 |
| $\ell \equiv 1 \bmod 8$ | 4 | $\ell - 1$ | $\ell^3 + \ell^2 - 2$ |
| $\ell \equiv 3 \bmod 8$ | 2 | $\ell - 1$ | $\ell^3 + \ell^2$ |
| $\ell \equiv 5 \bmod 8$ | 2 | $\ell + 1$ | $\ell^3 + \ell^2 - 2$ |
| $\ell \equiv 7 \bmod 8$ | 0 | $\ell + 1$ | $\ell^3 + \ell^2$ |

*Proof.* Since $\omega_*^4 = [-1]$, its minimal polynomial is $\Phi_8 = x^4 + 1$ with eigenvalues the four primitive eighth roots of unity. For any symplectic basis of $J[\ell]$, with $\ell$ odd, the linear map that represents the action of $\omega_*$ on this basis is thus diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(\mu_8, \mu_8^3, \mu_8^7, \mu_8^5) \in \mathrm{Sp}(\overline{\mathbb{F}_\ell})$.

(i) For $\ell = 2$, see [FS22a, Section 4.14].

(ii) For $\ell \equiv 1 \bmod 8$ we have that $\Phi_8$ splits completely modulo $\ell$, hence the action of $\omega_*$ is given by $\mathrm{diag}(\mu_8, \mu_8^3, \mu_8^7, \mu_8^5) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ for some symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$ by Lemma 4. Using Lemma 6, the $\omega_*$-invariant maximal isotropic subgroups are thus given by

$$\langle D_1, D_2 \rangle, \langle D_1, D_2' \rangle, \langle D_1', D_2 \rangle, \langle D_1', D_2' \rangle.$$

For $\omega_*^2$ we have that the action is given by $\mathrm{diag}(i, -i, -i, i) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$. Any line in the eigenspace corresponding to $i$ pairs with exactly one line in the eigenspace corresponding to $-i$, as well as the two eigenspaces themselves. We already counted four of them as $\omega_*$-invariant, so there are $\ell - 1$ remaining.

(iii) For $\ell \equiv 3 \bmod 8$ we have that $\sqrt{-2}$ is $\mathbb{F}_\ell$-rational so that $\Phi_8$ factors as $(x^2 + \sqrt{-2}x - 1)(x^2 - \sqrt{-2}x - 1) \bmod \ell$. By Lemma 2 and Lemma 3, the actions of $\omega_*$ and $\omega_*^2$ are thus given by the respective matrices

$$\begin{pmatrix} -\sqrt{-2} & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & \sqrt{-2} \end{pmatrix}, \quad \begin{pmatrix} -1 & -\sqrt{-2} & 0 & 0 \\ -\sqrt{-2} & 1 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{-2} \\ 0 & 0 & \sqrt{-2} & -1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

for some basis $\langle D_1, D_2, D_1', D_2' \rangle$. Since the blocks for $\omega_*$ are *not* similar but those for $\omega_*^2$ are, by Lemma 7 we know that there are $\ell + 1$ $\omega_*^2$-invariant maximal isotropic subspaces; the blocks themselves give $\omega_*$-invariant maximal isotropic subspaces $\langle D_1, D_2 \rangle$, $\langle D_1', D_2' \rangle$.

(iv) For $\ell \equiv 5 \bmod 8$ we have that $\Phi_8 = (x^2+i)(x^2-i) \bmod \ell$ such that $\omega_*$ is given by

$$\begin{pmatrix} 0 & -i & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

for some basis $\langle D_1, D_2, D_1', D_2' \rangle$, following Lemma 2 and Lemma 3. Given how the blocks are not similar, we have that $\langle D_1, D_2 \rangle$ and $\langle D_1', D_2' \rangle$ are the only $\omega_*$-invariant maximal isotropic subspaces by Lemma 7. For $\omega_*^2$ we immediately see that the action is given by $\mathrm{diag}(-i,-i,i,i) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$, and by Lemma 6 we can combine any line corresponding to the eigenspace with eigenvalue $-i$ with any line corresponding to the eigenspace with eigenvalue $i$, keeping in mind we need to discard the two that were already $\omega_*$-invariant.

(v) For $\ell \equiv 7 \bmod 8$ we have that $\sqrt{2}$ is $\mathbb{F}_\ell$-rational so that $\Phi_8$ factors as $(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) \bmod \ell$. Hence, by Lemma 2 and Lemma 3, $\omega_*$ and $\omega_*^2$ are given by

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -\sqrt{2} & 0 \\ 0 & -1 & 0 & \sqrt{2} \end{pmatrix}, \begin{pmatrix} -1 & 0 & -\sqrt{2} & 0 \\ 0 & -1 & 0 & \sqrt{2} \\ \sqrt{2} & 0 & 1 & 0 \\ 0 & -\sqrt{2} & 0 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

The argument is the same as for $\ell \equiv 3 \bmod 8$, except now the blocks themselves are only $\omega_*^2$-invariant and not $\omega_*$-invariant.

□

We have that $\mathrm{RA}(J) = \langle \rho_*, \omega_* \rangle$, resulting in the following theorem.

**Theorem 5.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$ with $J$ its Jacobian, $\mathrm{RA}(J) = \mathcal{S}_4$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell,\ell)$-level structure $(J,G)$ is equal to 4 if $\ell = 2$, equal to 9 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{24}\left(\ell^3 + 7\ell^2 + 24\ell + 41 + 9\left(\frac{-1}{\ell}\right) + 8\left(\frac{\ell}{3}\right) + 6\left(\frac{-2}{\ell}\right)\right).$$

*Proof.* One can verify that the group $\mathcal{S}_4$ contains

- one identity element `id`;
- six elements of order two (the transpositions) with minimal polynomial $x^2-1$ acting as $\sigma_*$ from Proposition 1;
- three elements of order two (two disjoint transpositions) with minimal polynomial $x^2+1$ acting as $\tau_*$ from Proposition 2;
- eight elements of order three with minimal polynomial $x^2+x+1$ acting as $\rho_*$ from Proposition 4;
- six elements of order four with minimal polynomial $x^4+1$ acting as $\omega_*$ from Proposition 6.

We thus have that the number of abelian surfaces with $(\ell,\ell)$-level structure is given by

$$\frac{1}{24}\cdot\left(|X^{\mathtt{id}}|+6|X^{\sigma_*}|+3|X^{\tau_*}|+8|X^{\rho_*}|+6|X^{\omega_*}|\right).$$

□

**$\mathbf{RA}(J)=\mathbb{Z}/5\mathbb{Z}$** This case only occurs if the Jacobian stems from the genus-2 curve defined by $C: y^2=x^5-1$, and the automorphism is given by $\zeta^{(5)}: x\mapsto \zeta_5 x$, where $\zeta_5$ is a primitive fifth root of unity in $\overline{\mathbb{F}}_p$. The curve is superspecial iff $p\equiv 4 \bmod 5$, see [IKO86, Proposition 1.13]. We have the following characterization of the action of $\zeta_*^{(5)}$ on abelian surfaces with $(\ell,\ell)$-level structure.

**Proposition 7.** *Let $C: y^2=x^5-1$ be a genus-2 curve over a field of characteristic $p>5$, with $\zeta^{(5)}: x\mapsto\zeta_5 x$ an automorphism of order 5, and $\ell\neq p$ a prime. Then the induced automorphism $\zeta_*^{(5)}$ acts on the abelian surfaces with $(\ell,\ell)$-level structure of $C$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 5 |
|---|---|---|
| $\ell=5$ | 1 | 155 |
| $\ell\equiv 1 \bmod 5$ | 4 | $\ell^3+\ell^2+\ell-3$ |
| $\ell\not\equiv 1 \bmod 5$ | 0 | $\ell^3+\ell^2+\ell+1$ |

*Proof.* Since $\zeta_*^{(5)}=\mathtt{id}$, its minimal polynomial is $\Phi_5=x^4+x^3+x^2+x+1$ and its eigenvalues are the four primitive fifth roots of unity. For any symplectic basis of $J[\ell]$, the linear map that represents the action of $\zeta_*^{(5)}$ on this basis is hence diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(\mu_5,\mu_5^2,\mu_5^4,\mu_5^3)\in \mathrm{Sp}(\overline{\mathbb{F}_\ell})$, assuming $\ell\neq 5$.

(i) If $\ell=5$ then $\Phi_5=(x-1)^4 \bmod 5$ and the only $\zeta_*^{(5)}$-invariant subspaces are those in the kernel of $(\zeta_*^{(5)}-1)^k$ for some $k\in\{1,2,3,4\}$. The only points on the curve invariant under $\zeta^{(5)}$ are given by $Q=(0,i)$ and $Q'=(0,-i)$, giving rise to the $\zeta_*^{(5)}$-invariant one-dimensional subspace

$$\langle[Q-\infty]\rangle=\{0,[Q-\infty],[2Q-2\infty],[2Q'-2\infty],[Q'-\infty]\}\subseteq J[5].$$

Any other divisor $[P+Q-2\infty]$ cannot be invariant under $\zeta_*^{(5)}$ as this requires either $\zeta^{(5)}(P)=P$, as we had before, or $\zeta^{(5)}(P)=Q$ and vice versa, which implies $x_P=\zeta_5^2 x_P$ hence $x_P=0$. As we only have a single eigenvector for $\lambda=1$, we can thus assume that $\zeta_*^{(5)}$ is given by

$$\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\0&0&0&1\end{pmatrix}\in \mathrm{Sp}_4(\mathbb{F}_\ell).$$

By Lemma 6, the only $\zeta_*^{(5)}$-invariant two-dimensional subspace stems from $(\zeta_*^{(5)} - 1)^2$, which is maximal isotropic since $\zeta_*^{(5)}$ is symplectic.

(ii) If $\ell \equiv 1 \bmod 5$, then a primitive fifth root of unity exists in $\mathbb{F}_\ell$, such that $\Phi_5 = \prod_{i=1}^4 (x - \mu_5^i)$ splits completely modulo $\ell$. By Lemma 4, we can thus assume that $\zeta_*^{(5)}$ is given by $\mathrm{diag}(\mu_5, \mu_5^2, \mu_5^4, \mu_5^3) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ for some symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$. By Lemma 6, the $\zeta_*^{(5)}$-invariant maximal isotropic subgroups are thus given by

$$\langle D_1, D_2 \rangle, \langle D_1, D_2' \rangle, \langle D_1', D_2 \rangle, \langle D_1', D_2' \rangle.$$

(iii) If $\ell \equiv 2, 3 \bmod 5$ then $\Phi_5$ is irreducible modulo $\ell$ and no $\zeta_*^{(5)}$-invariant two-dimensional subspace of $J[\ell]$ exists. If $\ell \equiv 4 \bmod 5$, a fifth root of unity exists modulo $\ell^2$, and we can write

$$\Phi_5 = (x^2 - (\mu_5 + \mu_5^4)x + 1) \cdot (x^2 - (\mu_5^2 + \mu_5^3)x + 1) \bmod \ell.$$

By Lemma 2 and Lemma 3, we can thus assume that $\zeta_*^{(5)}$ is given by the matrix

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & \mu_5 + \mu_5^4 & 0 \\ 0 & 1 & 0 & \mu_5^2 + \mu_5^3 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

for some symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$. Thus it decomposes as a direct summand of the two irreducible subspaces $\langle D_1, D_1' \rangle$ and $\langle D_2, D_2' \rangle$. Since the "blocks" are not similar, it follows from Lemma 7 that these irreducible spaces are the only ones to consider, but they are not symplectic.

□

This immediately results in the following proposition.

**Theorem 6.** *Let $C$ be a genus-2 curve over a field of characteristic $p > 5$, $J$ its Jacobian, with $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(J, G)$ is equal to 32 if $\ell = 5$ and*

- $\frac{1}{5}(\ell^3 + \ell^2 + \ell + 17)$ *if* $\ell \equiv 1 \bmod 5$;
- $\frac{1}{5}(\ell^3 + \ell^2 + \ell + 1)$ *if* $\ell \not\equiv 1 \bmod 5$.

*Proof.* This follows from Proposition 7 and Burnside's lemma. □

## C Reduced automorphisms on products of elliptic curves

Remark that in the standard notation, a symplectic basis for $(E \times E')[\ell]$ is of the form $((P, \infty), (\infty, P'), (Q, \infty), (\infty, Q'))$. Ergo, when discussing matrix representations of automorphisms, the upper-left $2 \times 2$ block does *not* represent the $E[\ell]$ component nor does the lower-right $2 \times 2$ block represent the $E'[\ell]$ component.

### C.1 $\mathbf{RA}(E \times E') = \mathbb{Z}/2\mathbb{Z}$

This is the generic case stemming from the automorphism $\kappa = [1] \times [-1]$, where $E \not\cong E'$ and neither $E$ nor $E'$ having $j$-invariant 0 or 1728.

**Proposition 8.** *Let $E \times E'$ be a product of elliptic curves over a field of characteristic $p > 5$, with the automorphism $\kappa = [1] \times [-1]$ of order 2, and $\ell \neq p$ a prime. Then $\kappa$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $E \times E'$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 |
|---|---|---|
| $\ell = 2$ | 15 | 0 |
| $\ell \neq 2$ | $(\ell+1)^2$ | $\ell^3 - \ell$ |

*Proof.* (i) For $\ell = 2$, see [FS22a, Subsection 4.4].
(ii) For $\ell \neq 2$, it is easy to see that $\kappa$ acts as $\mathrm{diag}(1, -1, 1, -1) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ and the result from Proposition 1(ii) also holds.

□

This immediately leads to the following result.

**Theorem 7.** *Let $E \times E'$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E \times E') = \mathbb{Z}/2\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E \times E', G)$ is equal to 15 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{2}(\ell^3 + 2\ell^2 + 3\ell + 2).$$

*Proof.* This is a direct consequence of Proposition 8. □

### C.2 $\mathbf{RA}(E \times E') = (\mathbb{Z}/2\mathbb{Z})^2$

This is the case when $E \cong E'$, and $j(E) \notin \{0, 1728\}$. The additional automorphism of order two is given by $\chi : (P, Q) \mapsto (Q, P)$, assuming $E' = E$.

**Proposition 9.** *Let $E \times E$ be a product of elliptic curves over a field of characteristic $p > 5$, with the automorphism $\chi : (P, Q) \mapsto (Q, P)$ of order 2, and $\ell \neq p$ a prime. Then $\chi$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $E \times E$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 |
|---|---|---|
| $\ell = 2$ | 7 | 8 |
| $\ell \neq 2$ | $(\ell+1)^2$ | $\ell^3 - \ell$ |

*Proof.* (i) For $\ell = 2$, see [FS22a, Subsection 4.6].
(ii) For $\ell \neq 2$, it is easy to see that $\chi$ acts as

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell),$$

but with a symplectic change of basis to $((P,P),(P,-P),(Q,Q),(Q,-Q))$ we see that it is symplectically similar to $\mathrm{diag}(1,-1,1,-1) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ and the same result as Proposition 8(ii) holds.

□

Combining Propositions 8 and 9, we get the following result.

**Theorem 8.** *Let $E \times E$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E \times E) = (\mathbb{Z}/2\mathbb{Z})^2$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell,\ell)$-level structure $(E \times E, G)$ is equal to 11 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{4}\left(\ell^3 + 3\ell^2 + 6\ell + 5 + \left(\frac{-1}{\ell}\right)\right).$$

*Proof.* Burnside's lemma says that the number of abelian surfaces with $(\ell,\ell)$-level structure is equal to

$$\frac{1}{|(\mathbb{Z}/2\mathbb{Z})^2|} \cdot \left(|X^{\mathtt{id}}| + |X^{\kappa}| + |X^{\chi}| + |X^{\kappa\chi}|\right),$$

hence by Propositions 8 and 9, it suffices to check $X^{\kappa\chi}$. One can verify that the minimal polynomial of $\kappa\chi$ is $x^2+1$, so the orbits act exactly the same as $\tau_*$ from Proposition 2. □

### C.3 $\mathrm{RA}(E \times E') = \mathbb{Z}/6\mathbb{Z}$

This is the case when $j(E) \notin \{0, 1728\}$ and $E' \cong E_0$. The additional automorphism of order three is given by $[1] \times \zeta^{(3)}$, where $\zeta^{(3)} : x \mapsto \zeta_3 x$ on $E_0$.

**Proposition 10.** *Let $E \times E_0$ be a product of elliptic curves over a field of characteristic $p > 5$, with $[1] \times \zeta^{(3)}$ an automorphism of order 3, and $\ell \neq p$ a prime. Then $[1] \times \zeta^{(3)}$ acts on the abelian surfaces with $(\ell,\ell)$-level structure of $E \times E_0$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 3 |
|---|---|---|
| $\ell = 3$ | 4 | 36 |
| $\ell \equiv 1 \bmod 3$ | $2\ell + 2$ | $(\ell+1)^2(\ell-1)$ |
| $\ell \equiv 2 \bmod 3$ | 0 | $\ell^3 + \ell^2 + \ell + 1$ |

*Proof.* (i) For $\ell = 3$, $\zeta^{(3)}$ is unipotent of order 3 and $[1] \times \zeta^{(3)}$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

Any line from $E[3]$ can thus be combined with one specific $\langle (P, 0) \rangle \subseteq E_0[3]$ to create a maximal isotropic $[1] \times \zeta^{(3)}$-invariant subspace.

(ii) For $\ell \equiv 1 \bmod 3$, $\zeta^{(3)}$ is diagonizable so the action of $[1] \times \zeta^{(3)}$ is given by $\mathrm{diag}(1, \mu_3, 1, \mu_3^2) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ by Lemma 4. By Lemma 6, we can combine any line from $E[\ell]$ with the one-dimensional subspaces belonging to $\mu_3$ or $\mu_3^2$. There are thus $2\ell + 2$ maximal isotropic $[1] \times \zeta^{(3)}$-invariant subspaces.

(iii) For $\ell \equiv 2 \bmod 3$, $\zeta^{(3)}$ is not diagonizable so, by Lemma 2 and Lemma 3, there exists a symplectic basis such that he action of $[1] \times \zeta^{(3)}$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)\,.$$

The only $[1] \times \zeta^{(3)}$-invariant two-dimensional subspaces are clearly $E[\ell]$ and $E_0[\ell]$, but those are not maximal isotropic.

□

Using $\kappa$ from Proposition 8, we can conclude with the following.

**Theorem 9.** *Let $E \times E_0$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E \times E_0) = \mathbb{Z}/6\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E \times E_0, G)$ is equal to 5 if $\ell = 2$, equal to 12 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{6}\left(\ell^3 + 2\ell^2 + 7\ell + 6 + (4\ell + 4)\left(\frac{\ell}{3}\right)\right).$$

*Proof.* Burnside's lemma says that the number of abelian surfaces with $(\ell, \ell)$-level structure is equal to

$$\frac{1}{|\mathbb{Z}/6\mathbb{Z}|} \cdot \left(|X^{\mathtt{id}}| + 2|X^{[1]\times\zeta^{(3)}}| + |X^{\kappa}| + 2|X^{[1]\times-\zeta^{(3)}}|\right).$$

The behaviour of $[1] \times -\zeta^{(3)}$ is easily determined from Proposition 10 since $[-1]$ is explicit. In particular we have that $|X^{[1]\times\zeta^{(3)}}| = |X^{[1]\times-\zeta^{(6)}}|$. The rest follows from Propositions 8 and 10. □

### C.4 $\mathrm{RA}(E \times E') = \mathbb{Z}/4\mathbb{Z}$

This is the case when $j(E) \notin \{0, 1728\}$ and $E' \cong E_{1728}$. The additional automorphism of order four is given by $[1] \times \iota$, where $\iota : (x, y) \mapsto (-x, iy)$ on $E_{1728}$, with $i^2 = -1$.

**Proposition 11.** *Let $E \times E_{1728}$ be a product of elliptic curves over a field of characteristic $p > 5$, with $[1] \times \iota$ an automorphism of order 4, and $\ell \neq p$ a prime. Then $[1] \times \iota$ acts on the abelian surfaces with $(\ell, \ell)$-level structure of $E \times E_{1728}$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 | surfaces in orbits of size 4 |
|---|---|---|---|
| $\ell = 2$ | 3 | 12 | 0 |
| $\ell \equiv 1 \bmod 4$ | $2\ell + 2$ | $\ell^2 - 1$ | $\ell^3 - \ell$ |
| $\ell \equiv 3 \bmod 4$ | 0 | $(\ell + 1)^2$ | $\ell^3 - \ell$ |

*Proof.* Note that $\iota^2 = \kappa$ so that distinction goes back to Proposition 8. The minimal polynomial of $[1] \times \iota$ is the product of the separate minimal polynomials and hence $(x - 1)(x^2 + 1)$.

(i) For $\ell = 2$, see [FS22a, Subsection 4.10].

(ii) For $\ell \equiv 1 \bmod 4$, the minimal polynomial of $\iota$ splits in linear factors such that the action of $[1] \times \iota$ is given by $\mathrm{diag}(1, i, 1, -i) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ by Lemma 4. By Lemma 6, we can thus choose any line on $E[\ell]$ with the one-dimensional subspaces belonging to $i$ or $-i$. There are $2\ell + 2$ maximal isotropic $[1] \times \iota$-invariant subspaces.

(iii) For $\ell \equiv 3 \bmod 4$, the minimal polynomial of $\iota$ does not factor such that the action of $[1] \times \iota$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell)$$

for some symplectic basis, following Lemma 2 and Lemma 3. The subspace $E_0[\ell]$ is clearly irreducible but it's not isotropic, nor is complement $E[\ell]$, so there are no maximal isotropic $[1] \times \iota$-invariant subspaces.

□

This immediately leads to the following result.

**Theorem 10.** *Let $E \times E_{1728}$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E \times E_{1728}) = \mathbb{Z}/4\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E \times E_{1728}, G)$ is equal to 9 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{4}\left(\ell^3 + 2\ell^2 + 5\ell + 4 + (2\ell + 2)\left(\frac{-1}{\ell}\right)\right).$$

*Proof.* It is clear that $\iota^3$ acts the same as $\iota$, so the statement follows from Burnside's lemma and Propositions 8 and 11. □

### C.5 $\mathrm{RA}(E \times E') = \mathbb{Z}/12\mathbb{Z}$

This is the case when $E \cong E_{1728}$ and $E' \cong E_0$. No additional automorphisms are needed apart from the already discussed $\iota \times [1]$ and $[1] \times \zeta^{(3)}$.

**Theorem 11.** *Let $E_0 \times E_{1728}$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E_0 \times E_{1728}) = \mathbb{Z}/12\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E_0 \times E_{1728}, G)$ is equal to 3 if $\ell = 2$, is equal to 6 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{12}\left(\ell^3 + 2\ell^2 + 9\ell + 12 + 2(\ell+3)\left(\frac{-1}{\ell}\right) + 4(\ell+2)\left(\frac{\ell}{3}\right) + 4\left(\frac{3}{\ell}\right)\right).$$

*Proof.* We have that the number is given by

$$\frac{1}{12} \cdot \left(|X^{\mathtt{id}}| + |X^{\kappa}| + 2|X^{[1]\times\zeta^{(3)}}| + 2|X^{\iota\times[1]}| + 2|X^{[1]\times-\zeta^{(3)}}| + 4|X^{\iota\times\zeta^{(3)}}|\right),$$

since the choice of a root of unity should not change the outcome. By Propositions 8, 10 and 11, it suffices to verify the fixed elements of the action of $\iota \times \zeta^{(3)}$, which has order 12. For $\ell \equiv 1 \bmod 12$ this means the action is diagonizable as $\mathrm{diag}(i, \mu_3, -i, \mu_3^2) \in \mathrm{Sp}_4(\mathbb{F}_\ell)$ and by Lemma 6 we can create 4 maximal isotropic $\iota \times \zeta^{(3)}$-invariant subspaces from this. For $\ell \equiv 5, 7, 11 \bmod 12$, either $\iota$ or $\zeta^{(3)}$ is not diagonizable and it yields no fixed subspaces. □

### C.6 $\mathrm{RA}(E \times E') = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$

This is the case when $E \cong E' \cong E_{1728}$. No additional automorphisms are needed and the group is generated by $\langle \chi, [1] \times \iota \rangle$.

**Theorem 12.** *Let $E_{1728} \times E_{1728}$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E_{1728} \times E_{1728}) = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E_{1728} \times E_{1728}, G)$ is equal to 5 if $\ell = 2$ and for $\ell > 2$ it is*

$$\frac{1}{16}\left(\ell^3 + 4\ell^2 + 15\ell + 24 + (4\ell+12)\left(\frac{-1}{\ell}\right) + 4\left(\frac{-2}{\ell}\right)\right).$$

*Proof.* All automorphisms of $E_{1728} \times E_{1728}$ are given by $(P, Q) \mapsto (\iota^a(P), \iota^b(Q))$ or $(P, Q) \mapsto (\iota^c(P), \iota^d(Q))$, where $b, d \in \{0, 1\}$ and $a, c \in \{0, 1, 2, 3\}$ cover all options up to equivalence. One can verify that this group contains

- one identity element $\mathtt{id}$;
- three elements of order two with minimal polynomial $x^2 - 1$ acting as $\kappa$ from Proposition 8;
- four elements of order two with minimal polynomial $x^2 + 1$ acting as $\tau_*$ from Proposition 2;
- four elements of order four with minimal polynomial $(x-1)(x^2+1)$ acting as $[1] \times \iota$ from Proposition 11;

– four elements of order four with minimal polynomial $x^4+1$ acting as $\omega_*$ from Proposition 6.

We thus have that the number of abelian surfaces with $(\ell,\ell)$-level structure is given by

$$\frac{1}{16}\cdot\left(|X^{\mathtt{id}}|+3|X^{\kappa}|+4|X^{\tau_*}|+4|X^{[1]\times\iota}|+4|X^{\omega_*}|\right).$$

□

### C.7 $\mathbf{RA}(E\times E')=\mathbb{Z}/6\mathbb{Z}\times\mathcal{S}_3$

This is the case when $E\cong E'\cong E_0$. No additional automorphisms are needed and the group is generated by $\langle\chi,[1]\times-\zeta^{(3)}\rangle$. Some of these automorphisms - such as $\chi\circ([1]\times-\zeta^{(3)})$ have nonreduced order twelve however, which we have not had to discuss previously.

**Proposition 12.** *Let $E_0\times E_0$ be a product of elliptic curves over a field of odd characteristic $p>5$, with $\chi\circ([1]\times-\zeta^{(3)})$ an automorphism of nonreduced order 12, and $\ell\neq p$ a prime. Then $\chi\circ([1]\times-\zeta^{(3)})$ acts on the abelian surfaces with $(\ell,\ell)$-level structure of $E_0\times E_0$ as follows:*

| | surfaces in orbits of size 1 | surfaces in orbits of size 2 | surfaces in orbits of size 3 | surfaces in orbits of size 6 |
|---|---|---|---|---|
| $\ell=2$ | 1 | 2 | 6 | 6 |
| $\ell=3$ | 1 | 0 | 3 | 36 |
| $\ell\equiv 1 \bmod 12$ | 4 | $\ell-1$ | $\ell-1$ | $\ell^3+\ell^2-\ell-1$ |
| $\ell\equiv 5 \bmod 12$ | 2 | $\ell-1$ | $\ell+1$ | $\ell^3+\ell^2-\ell-1$ |
| $\ell\equiv 7 \bmod 12$ | 2 | $\ell+1$ | $\ell-1$ | $\ell^3+\ell^2-\ell-1$ |
| $\ell\equiv 11 \bmod 12$ | 0 | $\ell+1$ | $\ell+1$ | $\ell^3+\ell^2-\ell-1$ |

*Proof.* Since $(\chi\circ([1]\times-\zeta^{(3)}))^6=[-1]$, its minimal polynomial is $\Phi_{12}=x^4-x^2+1$ with eigenvalues the four primitive twelfth roots of unity. For any symplectic basis, the linear map representing the action of this automorphism on this basis is thus diagonizable over $\overline{\mathbb{F}_\ell}$ as $\mathrm{diag}(\mu_{12},\mu_{12}^5,\mu_{12}^{11},\mu_{12}^7)\in\mathrm{Sp}(\overline{\mathbb{F}_\ell})$. Note that the minimal polynomial of its square and its cube are respectively $x^2-x+1$ and $x^2+1$ such that we can apply the results from $\rho_*$ and $\tau_*$ to determine the orbits of size three and two.

(i) For $\ell=2,3$ this is a direct computation.
(ii) For $\ell\equiv 1 \bmod 12$, we have that $\Phi_{12}$ splits completely and for some symplectic basis, the automorphism is given by $\mathrm{diag}(\mu_{12},\mu_{12}^5,\mu_{12}^{11},\mu_{12}^7)\in\mathrm{Sp}_4(\mathbb{F}_\ell)$, which follows from Lemma 4. This yields 4 invariant maximal isotropic subspaces by Lemma 6.

(iii) For $\ell \equiv 5, 7, 11 \bmod 12$, we have that $\Phi_{12}$ factors as respectively $(x^2+ix-1)(x^2-ix-1)$, $(x^2+\mu_3)(x^2+\mu_3^2)$ and $(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)$, resulting in the action given by the respective matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ \mu_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -\mu_3 & 0 \end{pmatrix}, \begin{pmatrix} \sqrt{3} & 0 & -1 & 0 \\ 0 & -\sqrt{3} & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{F}_\ell),$$

which follows from Lemma 2 and Lemma 3. None of these cases yield similar $2 \times 2$ blocks, so by Lemma 7, only the subspaces corresponding to the two blocks can be potential invariant maximal isotropic subspaces. This is the case for $\ell \equiv 5, 7 \bmod 12$ but for $\ell \equiv 11 \bmod 12$ they are not isotropic.

□

This yields the following result.

**Theorem 13.** *Let $E_0 \times E_0$ be a product of elliptic curves over a field of characteristic $p > 5$, with $\mathrm{RA}(E_0 \times E_0) = \mathbb{Z}/6\mathbb{Z} \times \mathcal{S}_3$, and $\ell \neq p$ a prime. Then the number of abelian surfaces with $(\ell, \ell)$-level structure $(E_0 \times E_0, G)$ is equal to 3 if $\ell = 2$, equal to 5 if $\ell = 3$, and for $\ell > 3$ it is*

$$\frac{1}{36}\left(\ell^3 + 5\ell^2 + 24\ell + 59 + (8\ell + 38)\left(\frac{\ell}{3}\right) + 9\left(\frac{-1}{\ell}\right)\right).$$

*Proof.* All automorphisms of $E_0 \times E_0$ are given by $(P, Q) \mapsto ((-\zeta)^a(P), (-\zeta)^b(Q))$ or $(P, Q) \mapsto ((-\zeta)^c(P), (-\zeta)^d(Q))$, where $b, d \in \{0, 1, 2\}$ and $a, c \in \{0, 1, 2, 3, 4, 5\}$ cover all options up to equivalence. One can verify that this group contains

- one identity element $\mathtt{id}$;
- seven elements of order two: four with minimal polynomial $x^2 - 1$ acting as $\kappa$ from Proposition 8 and three elements with minimal polynomial $x^2 + 1$ acting as $\tau_*$ from Proposition 2;
- eight elements of order three: two with minimal polynomial $x^2 + x + 1$ and two with minimal polynomial $(x + 1)(x^2 + x + 1)$ which act as $\rho_*$ from Proposition 4, four with minimal polynomial $(x - 1)(x^2 + x + 1)$ which act as $[1] \times \zeta^{(3)}$ from Proposition 10;
- twenty elements of order six: two with minimal polynomial $x^2 - x + 1$ and two with minimal polynomial $(x-1)(x^2-x-1)$ which act as $[1] \times \zeta^{(3)}$ from Proposition 10, ten with minimal polynomial $(x^2+x+1)(x^2-x+1)$ which act as $\zeta_*^{(6)}$ from Proposition 5, six with minimal polynomial $x^4-x^2+1$ which act as $\chi \circ ([1] \times -\zeta^{(3)})$ from Proposition 12.

We thus have that the number of abelian surfaces with $(\ell, \ell)$-level structure is given by

$$\frac{1}{36} \cdot \left(|X^{\mathtt{id}}| + 4|X^{\kappa}| + 3|X^{\tau_*}| + 4|X^{\rho_*}| + 8|X^{[1]\times\zeta^{(3)}}| + 10|X^{\zeta_*^{(6)}}| + 6|X^{\chi\circ([1]\times-\zeta^{(3)})}|\right).$$

□

## D Representation of $(\ell, \ell)$-isogenies

In this section, we give a compact description of all maximal isotropic $(\ell, \ell)$-subgroups, including a unique representation for such a subgroup, given a symplectic basis of $J[\ell]$. This representation is very similar to one given by Kunzweiler, Ti, and Weitkämper [KTW22], although we adapt their representation to our purpose of computing $(\ell, \ell)$-isogenies, for which we require a specific representation of maximal isotropic subgroups. This representation has two advantages: on the theoretical side, they simplify our later exposition of the action of automorphisms on such subgroups. On the practical side, they allow us to quickly compute all such subgroups and speed up the computation of orbits under the automorphism.

*The echelon form.* We assume a symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$ of $J[\ell]$, i.e., a basis such that

$$e_\ell(D_1, D_2) = 1, \quad e_\ell(D_1', D_2') = 1, \quad e_\ell(D_i, D_i') = \mu_\ell,$$

where $e_\ell$ is the $\ell$-Weil pairing and $\mu_\ell$ some fixed $\ell$-th root of unity. Any maximal isotropic $(\ell, \ell)$-subgroup $G$ is then generated by two elements

$$K_1 = [a_1]D_1 + [a_2]D_2 + [a_3]D_1' + [a_4]D_2', \qquad K_2 = [b_1]D_1 + [b_2]D_2 + [b_3]D_1' + [b_4]D_2'$$

such that $e_\ell(K_1, K_2) = 1$. Written additively, these coefficients must satisfy the following equation in order for $G$ to be maximal isotropic:

$$\Delta(G) := a_1 \cdot b_3 + a_2 \cdot b_4 - a_3 \cdot b_1 - a_4 \cdot b_2 \equiv 0 \mod \ell. \tag{3}$$

By representing (the generators $K_1$ and $K_2$ of) a maximal isotropic subgroup $G$ as a matrix

$$M_G = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}, \qquad \text{with } \Delta(G) \equiv 0 \mod \ell,$$

we find a simple way to compute all $\ell^3 + \ell^2 + \ell + 1$ maximal isotropic subgroups, together with a canonical representation, by simple row reductions on $M_G$. We refer to such a row-reduced representation $\overline{M_G}$ as the *echelon form* of $G$, with respect to a symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$.

*When $a_1$ is non-zero.* If $a_1$ is non-zero, we may normalize the first row, and clear the second row with the first row. Depending on the number of leading zeroes in the second row, this gives us three options after normalizing to the first non-zero value.

(i) If the resulting $b_2$ is non-zero, we get

$$\overline{M_G} = \begin{pmatrix} 1 & 0 & a_3 & a_4 \\ 0 & 1 & b_3 & b_4 \end{pmatrix}, \qquad \text{with } \Delta(G) = b_3 - a_4 \equiv 0 \mod \ell. \tag{4}$$

This gives us $\ell^3$ subgroups by choosing $a_3, a_4, b_4 \in \mathbb{Z}/\ell\mathbb{Z}$, and are required to set $b_3 = a_4$.

(ii) If the resulting $b_2$ is zero, but $b_3$ is non-zero, we get

$$\overline{M_G} = \begin{pmatrix} 1 & a_2 & 0 & a_4 \\ 0 & 0 & 1 & b_4 \end{pmatrix}, \qquad \text{with } \Delta(G) = 1 + a_2 \cdot b_4 \equiv 0 \mod \ell. \tag{5}$$

This gives us $\ell \cdot (\ell - 1)$ options by choosing $a_2 \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ and $a_4 \in \mathbb{Z}/\ell\mathbb{Z}$, and are required to set $b_4 = -a_2^{-1}$.

(iii) If the resulting $b_2$ and $b_3$ are zero, but $b_4$ is non-zero, we get

$$\overline{M_G} = \begin{pmatrix} 1 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{with } \Delta(G) = a_2 \equiv 0 \mod \ell. \tag{6}$$

This gives us $\ell$ options, as we may only choose $a_3 \in \mathbb{Z}/\ell\mathbb{Z}$ freely.

*When $a_1$ is zero.* We may do similar derivations assuming both $a_1$ and $b_1$ are zero, as we simply swap rows. This gives us three other options for canonical representations.

(i) If $b_3$ is non-zero after clearing row two, we get

$$\overline{M_G} = \begin{pmatrix} 0 & 1 & 0 & a_4 \\ 0 & 0 & 1 & b_4 \end{pmatrix}, \qquad \text{with } \Delta(G) = b_4 \equiv 0 \mod \ell. \tag{7}$$

This gives us another $\ell$ options, as we may only choose $a_4 \in \mathbb{Z}/\ell\mathbb{Z}$ freely.

(ii) If $b_3$ is zero after clearing row two, we get

$$\overline{M_G} = \begin{pmatrix} 0 & 1 & a_3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{with } \Delta(G) = 1 \equiv 0 \mod \ell. \tag{8}$$

As the requirement on $\Delta(G)$ is impossible, none of these subgroups are maximal isotropic.

(iii) Lastly, the only remaining option is the maximal isotropic subgroup given by

$$\overline{M_G} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{with } \Delta(G) = 0 \mod \ell. \tag{9}$$

*The action of $\alpha$ on the echelon form.* When $\alpha$ is a (reduced) automorphism of a curve $C$, with $\alpha_*$ the associated automorphism on its Jacobian $J$, we may write the action of $\alpha_*$ on the symplectic basis $\langle D_1, D_2, D_1', D_2' \rangle$ as some matrix $M_\alpha \in \mathbb{F}_\ell^{4\times 4}$. We then easily compute the action of $\alpha_*$ on $G$ by $\overline{M_{\alpha_*(G)}} = \text{Echelon}(M_\alpha \cdot M_G^T)$.

The echelon form allows us to deduce results on the size of orbits of subgroups under automorphisms, by identifying those echelon forms with orbits of certain orders. In particular, for computational purposes, the echelon form allows us to easily compute all maximal isotropic subgroups, given a symplectic basis. Furthermore, as the echelon form $\overline{M_G}$ is a unique representation of $G$, this allows us to easily verify equality of subgroups $G$ and $G'$ by comparing $\overline{M_G} = \overline{M_{G'}}$, simplifying an otherwise tedious comparison.

### D.1 Good extensions for the echelon form

The categorization using echelon form makes it simple to compute the good extensions to a given isogeny $\varphi : J' \to J$ which we may represent as $(J, G)$ where $G = \ker \hat{\varphi}$.

**Lemma 9.** *Let $(J, G)$ be a level structure of a p.p. abelian surface with $G = \langle T_1, T_2 \rangle$ for $T_1, T_2 \in J[\ell]$. Let $S_1, S_2 \in J[\ell]$ be such that $S_1, S_2, T_1, T_2$ is a symplectic basis. Then the $\ell^3$ good extensions of $(J, G)$ are given by the kernels $\langle K_1, K_2 \rangle$, where*

$$K_1 = S_1 + [a]T_1 + [b]T_2, \quad K_2 = S_2 + [b]T_1 + [c]T_2, \quad a, b, c \in \mathbb{Z}/\ell\mathbb{Z}.$$

*Proof.* This follows directly from Eq. (4). □

It is similarly straightforward to compute the good extensions on products of elliptic curves.

**Lemma 10.** *For an elliptic product $(E \times E', G)$ with $(\ell, \ell)$-level structure, with associated isogeny $\varphi : E \times E' \to (E \times E')/G$, we have:*

- *if $\varphi$ is a diagonal isogeny, then there are $\ell^2$ diagonal kernels $G'$ and $\ell^3 - \ell^2$ gluing kernels $G'$ with $G \cap G' = 0$;*
- *if $\varphi$ is a gluing isogeny, then there are $\ell^2 + \ell$ diagonal kernels $G'$ and $\ell^3 - \ell^2 - \ell$ gluing kernels $G'$ with $G \cap G' = 0$.*

*Proof.* When $\varphi$ is diagonal, we may choose a basis $(Q, \infty), (\infty, Q')$ for $G$, which we may extend to a symplectic basis $\langle (P, \infty), (\infty, P'), (Q, \infty), (\infty, Q') \rangle$ for $(E \times E')[\ell]$. Similar to Lemma 9, we can associate a good extension to a triple $(a, b, c) \in (\mathbb{Z}/\ell\mathbb{Z})^3$. Diagonal kernels are those with $b = 0$.

When $\varphi$ is a gluing, we may assume $\ell^2 - 1$ points $(K_1, K_2)$ of order $\ell$ in its kernel. Each of these overlaps with the diagonal isogeny generated by $(K_1, \infty), (\infty, K_2)$. Dividing by the projective factor $\ell - 1$ to remove scalars, this gives us $\ell + 1$ bad diagonal kernels out of $(\ell + 1)^2$ total diagonal kernels, leaving $\ell^2 + \ell$ good ones. □