Multiradical isogenies

Wouter Castryck and Thomas Decru

Abstract. We argue that for all integers $N \geq 2$ and $g \geq 1$ there exist "multiradical" isogeny formulae, that can be iteratively applied to compute $(N^k, \ldots, N^k)$-isogenies between principally polarized g-dimensional abelian varieties, for any value of $k \geq 2$. The formulae are complete: each iteration involves the extraction of $g(g+1)/2$ different Nth roots (whence the epithet multiradical) and by varying which roots are chosen one computes all $N^{g(g+1)/2}$ extensions to an $(N^k, \ldots, N^k)$-isogeny of the incoming $(N^{k-1}, \ldots, N^{k-1})$-isogeny. Our argumentation is heuristic, but we provide concrete formulae for several prominent families. As our main application, we illustrate the use of multiradical isogenies by implementing a hash function from $(3,3)$-isogenies between Jacobians of supersingular genus-2 curves, showing that it outperforms its $(2,2)$-counterpart by an asymptotic factor ≈ 9 in terms of speed.

1 Introduction

In a previous joint work with Vercauteren [10], we introduced the concept of *radical isogenies* between elliptic curves, which in low degree allow for a very fast computation of isogeny chains over finite fields, *e.g.,* of the type used in Charles, Goren and Lauter's hash function [12] and in the Couveignes–Rostovtsev–Stolbunov key exchange protocol [14, 37] and its descendant CSIDH [11].

The central observation was that for any integer $N \geq 2$ there exist explicit formulae which, upon input of an elliptic curve E — say given in long Weierstrass form — over a field K with $\operatorname{char} K \nmid N$ and a point $P \in E$ of order N, produce the coordinates of an order-N point $P' \in E' = E/\langle P \rangle$ such that the isogeny $\varphi' : E' \to E'/\langle P' \rangle$ cyclically extends $\varphi : E \to E/\langle P \rangle$. This, of course, assumes that we have a defining equation for E' at hand, such as the one provided by Vélu [40]. Moreover, the formulae can be chosen to enjoy the following properties.

(1) Radicality. The formulae are algebraic expressions in the coefficients of E, the coordinates of P and a radical $\sqrt[N]{\mathfrak{r}_1}$, where $\mathfrak{r}_1$ is itself an algebraic expression in these coefficients and coordinates.

(2) Completeness. By varying the Nth root chosen, *i.e.,* by scaling $\sqrt[N]{\mathfrak{r}_1}$ with powers of a primitive Nth root of unity $\zeta_N \in \overline{K}$, we obtain generators for all N subgroups $G' \subseteq E'$ of order N which are such that $E' \to E'/G'$ cyclically extends φ.

imec-COSIC, Kasteelpark Arenberg 10/2452, 3001 Leuven (Heverlee), Belgium
wouter.castryck@esat.kuleuven.be, thomas.decru@esat.kuleuven.be

(3) Good reduction. The formulae are naturally defined over $\mathbb{Z}[1/N]$, *i.e.,* they work over any field K with $\operatorname{char} K \nmid N$.

(The last property is in fact conjectural [10, Conj. 1].) Concrete versions of our radical isogeny formulae for $N = 2, \ldots, 13$ can be found in the GitHub repository that accompanies [10]. For the sake of illustration, we have included the details of the case $N = 5$ in Section 4.

The current paper studies how radical isogenies generalize to principally polarized (p.p.) abelian varieties of any given dimension $g \geq 1$. That is, we are looking for formulae which, upon input of a g-dimensional p.p. abelian variety A over a field K with $\operatorname{char} K \nmid N$ and points $P_1, \ldots, P_g \in A$ that generate an $(N, \ldots, N)$-subgroup $G \subseteq A$, produce the coordinates of points $P'_1, \ldots, P'_g \in A' = A/G$ generating an $(N, \ldots, N)$-subgroup $G' \subseteq A'$ such that the composition $A \to A' = A/G \to A'/G'$ is an $(N^2, \ldots, N^2)$-isogeny.

When aiming for universally applicable formulae, a major bottleneck is the lack of an analogue of the long Weierstrass form for p.p. abelian varieties of dimension $g \geq 2$. That is, we do not know of a set of defining equations from which every g-dimensional p.p. abelian variety A can be obtained by specializing coefficients. Moreover, in practical applications, we are mostly interested in instances of A that are described in a more implicit form, *e.g.,* as the Jacobian of some genus-g curve, or as a product of Jacobians of lower-genus curves. Things are complicated further by the fact that the isogenous p.p. abelian variety A' may be of a different type, *e.g.,* if A is a Jacobian, then this may not be the case for A'.

We therefore focus on smaller families, parametrized by the points s of some quasi-affine set $\mathcal{S}$, of g-dimensional p.p. abelian varieties A_s together with points $P_{s,1}, \ldots, P_{s,g}$ that generate an $(N, \ldots, N)$-subgroup $G_s \subseteq A_s$. We assume that these families come equipped with Vélu-like formulae providing an explicit description of the isogenous p.p. abelian variety $A'_s = A_s/G_s$. (Several examples of such families can be found in Section 4 and Section 5.) We then argue that there should exist accompanying formulae which, when evaluated at s, produce points $P'_{s,1}, \ldots, P'_{s,g} \in A'_s$ with the desired property. Moreover, we believe that these formulae can be chosen to enjoy the following properties.

(1) Multiradicality. They are algebraic expressions in the coordinates of s and radicals $\sqrt[N]{\mathfrak{r}_1}$, $\ldots$, $\sqrt[N]{\mathfrak{r}_{g(g+1)/2}}$, where in turn the radicands $\mathfrak{r}_i$ are algebraic expressions in the coordinates of s.

(2) Completeness. By varying the Nth roots chosen, *i.e.,* by scaling them with powers of ζ_N, we obtain generating sets for all $N^{g(g+1)/2}$ subgroups $G'_s \subseteq A'_s$ such that $A_s \to A'_s = A_s/G_s \to A'_s/G'_s$ is an $(N^2, \ldots, N^2)$-isogeny.

(3) Good reduction. If the family is defined over $\mathbb{Z}[1/M]$ for some multiple M of N, then so are our formulae, *i.e.,* they work over any field K with $\operatorname{char} K \nmid M$.

We also believe that the radicands $\mathfrak{r}_1, \ldots, \mathfrak{r}_{g(g+1)/2}$ can be taken to be representants of the Tate pairings $t_N(P_{s,i}, P_{s,j})$, $1 \leq i \leq j \leq g$, in the sense of Frey

and Rück [20], as soon as these are well-defined. We call our formulae *multiradical isogeny* formulae. Section 3 provides a group-theoretic heuristic argument in favour of their existence, although each of the above claims remains conjectural.

The main support comes from concrete examples of such formulae, which are discussed in Section 4 and Section 5. For arbitrary N and in arbitrary dimension g, we discuss fully split $(N, \ldots, N)$-isogenies from g-fold products of elliptic curves. Further examples focus on Jacobians of genus-2 curves, where we discuss non-split $(2, 2)$-isogenies (also known as Richelot isogenies) and non-split $(3, 3)$-isogenies as described by Bruin, Flynn and Testa [5]. We also study the multiradical nature of certain $(5, 5)$-isogenies that were described by Flynn [17].

Remark 1. Our eventual goal is the computation of $(N^k, \ldots, N^k)$-isogenies, for arbitrary $k \geq 2$, achieved by an iterated application of our formulae. However, it is possible, and unavoidable in general, that the isogenous p.p. abelian variety A'_s marked with $P'_{s,1}, \ldots, P'_{s,g}$ does not belong to our family. For instance, if $\mathcal{S}$ parametrizes Jacobians of genus-2 curves, we may run into a product of elliptic curves. In such cases, one needs to resort to different sets of multiradical isogeny formulae in order to cover the entire isogeny chain.

We illustrate the use of multiradical isogenies in Section 6, by constructing a Charles–Goren–Lauter style hash function from $(3, 3)$-isogenies between supersingular p.p. abelian surfaces over a large quadratic finite field $\mathbb{F}_{p^2}$, similar to the $(2, 2)$-construction from our joint work with Smith [9]. In short, each message determines a walk in the isogeny graph (which is of size $\approx p^3/2880$), and the hash of the message is the end point of that walk. One should make sure that every two consecutive isogenies compose to a $(9, 9)$-isogeny, to avoid the trivial collisions described in [18, §2.3]. This is automatically taken care of when using multiradical isogeny formulae.

In the Richelot hash function from [9], the cost of a $(2, 2)$-isogeny is about 3 square roots, with very little overhead, which can be used to process 3 bits of the message. In our case, the cost of a $(3, 3)$-isogeny is dominated by the extraction of 3 cube roots, which can now be used to process 3 *trits* of the message. Moreover, if $p \not\equiv \pm 1 \bmod 9$ then $p^2 \not\equiv 1 \bmod 9$ and computing cube roots in $\mathbb{F}_{p^2}$ is faster than computing square roots. Altogether, this leads to an expected speed-up by a factor ≈ 9. However, a noticeable difference with [9] is that chaining multiradical $(3, 3)$-isogenies comes with some non-negligible overhead; our current implementation even involves three small Gröbner basis computations. Despite this overhead, the $(3, 3)$-hash function outperforms the Richelot hash function as soon as the field characteristic p is of cryptographic size (*i.e.,* 86 bits or more). The asymptotic speed-up factor ≈ 9 becomes visible around $p \approx 2^{1024}$.

Acknowledgments. This work was supported by the Research Council KU Leuven grant C14/18/067, by CyberSecurity Research Flanders with reference VR20192203, and by the Research Foundation Flanders (FWO) through the WOG Coding Theory and Cryptography. We thank Marc Houben and Frederik Vercauteren for several helpful remarks and discussions.

2 Background

We discuss some of the material needed for what follows, but we stress that this is not a complete overview. Our main goal is to fix notation and highlight some statements that may be known but that we did not manage to pinpoint in the existing literature, such as Lemma 2, Example 3 and Lemma 4 below. For general background on abelian varieties and isogenies we refer to [29, 31].

2.1 Generalized symplectic bases

We consider abelian varieties A of dimension $g \geq 1$ over a field K with algebraic closure $\overline{K}$, and we always assume that A comes equipped with a principal polarization (p.p.). Important examples of g-dimensional p.p. abelian varieties are Jacobians of smooth projective curves C/K of genus g. Every p.p. abelian variety of dimension ≤ 3 is $\overline{K}$-isomorphic to a product of Jacobians.

For each integer $N \geq 2$ with $\operatorname{char} K \nmid N$, the N-torsion subgroup $A[N]$ can be shown to be free of rank $2g$ over $\mathbb{Z}_N$. The p.p. induces a perfect bilinear and antisymmetric pairing

$$e_N : A[N] \times A[N] \to \mu_N \subseteq \overline{K}^*,$$

known as the Weil pairing. After fixing a primitive Nth root of unity $\zeta_N \in \mu_N$, the Weil pairing turns into a symplectic form:

$$\langle \cdot, \cdot \rangle_N : A[N] \times A[N] \to \mathbb{Z}_N : (P, Q) \mapsto \log_{\zeta_N} e_N(P, Q).$$

Thus $A[N]$ admits a symplectic basis, *i.e.,* a $\mathbb{Z}_N$-basis $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ satisfying $\langle P_i, P_j \rangle_N = \langle Q_i, Q_j \rangle_N = 0$ and $\langle P_i, Q_j \rangle_N = \delta_{ij}$ for all $i, j \in \{1, \ldots, g\}$. This allows us to view $A[N]$ as $\mathbb{Z}_N^{2g}$ equipped with the standard symplectic pairing

$$\langle \cdot, \cdot \rangle : \mathbb{Z}_N^{2g} \times \mathbb{Z}_N^{2g} : (v, w) \mapsto v^T \Omega w, \qquad \Omega = \begin{pmatrix} 0 & \mathbb{I}_g \\ -\mathbb{I}_g & 0 \end{pmatrix}.$$

Changing between symplectic bases is done using matrices from the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z}_N) = \{ M \in \mathrm{GL}_{2g}(\mathbb{Z}_N) \mid M^T \Omega M = \Omega \}$.

Note that the notion of a symplectic basis of $A[N]$ depends on the choice of ζ_N. If a basis is symplectic with respect to *some* choice of ζ_N, then we call it a *generalized symplectic basis*. The matrices of base change between generalized symplectic bases are now taken from the larger group

$$\mathrm{GSp}_{2g}(\mathbb{Z}_N) = \{ M \in \mathrm{GL}_{2g}(\mathbb{Z}_N) \mid M^T \Omega M = d(M)\Omega \text{ for a } d(M) \in \mathbb{Z}_N^* \}, \quad (1)$$

which is known as the generalized symplectic group (its elements are often referred to as symplectic similitudes). An *N-level structure* on A is an isomorphism $\alpha : A[N] \to \mathbb{Z}_N^{2g}$ such that

$$\alpha^{-1}(1, 0, \ldots, 0),\ \alpha^{-1}(0, 1, \ldots, 0),\ \ldots,\ \alpha^{-1}(0, 0, \ldots, 1)$$

is a generalized symplectic basis of $A[N]$.

2.2 Good chains of $(N, \ldots, N)$-isogenies

A subgroup $G \subseteq A[N]$ is called isotropic if $\langle P, Q \rangle_N = 0$ for all $P, Q \in G$. Note that this notion does not depend on the choice of ζ_N. It is called *maximal isotropic* if moreover there is no supergroup $G' \supsetneq G$ that is isotropic. This property ensures that the isogenous abelian variety $A' = A/G$ comes naturally equipped with a p.p. The subgroup is said to be an

$$\underbrace{(N, \ldots, N)}_{g \text{ times}}\text{-subgroup}$$

if it is a (necessarily maximal) isotropic free $\mathbb{Z}_N$-submodule of rank g, *i.e.,* an isotropic subgroup isomorphic to $\mathbb{Z}_N^g$. In that case, we say that the quotient isogeny $\varphi : A \to A'$ is an $(N, \ldots, N)$-*isogeny*.

Given an $(N, \ldots, N)$-isogeny $\varphi : A \to A'$, we say that an $(N, \ldots, N)$-isogeny $\varphi' : A' \to A''$ is a *good* extension of φ if the composition

$$A \xrightarrow{\varphi} A' \xrightarrow{\varphi'} A''$$

is an $(N^2, \ldots, N^2)$-isogeny. According to the lemma below, of which special cases can be found in [18, §2.2], there are $N^{g(g+1)/2}$ subgroups of $A'[N]$ that give rise to good extensions. The group $\varphi(A[N])$ is an $(N, \ldots, N)$-subgroup which is the kernel of the *dual* isogeny $\hat{\varphi} : A' \to A$. All other $(N, \ldots, N)$-subgroups of $A'[N]$ are said to give rise to *bad* extensions. These are precisely the $(N, \ldots, N)$-subgroups that differ from $\varphi(A[N])$ but that intersect it non-trivially.

Lemma 2. *Consider $\mathbb{Z}_N^{2g}$ together with the standard symplectic pairing $\langle \cdot, \cdot \rangle$. Its number of $(N, \ldots, N)$-subgroups is given by*

$$N^{g(g+1)/2} \prod_{\substack{\text{primes} \\ \ell | N}} \prod_{i=1}^{g} \left(1 + \frac{1}{\ell^i}\right).$$

Given an $(N, \ldots, N)$-subgroup $G \subseteq \mathbb{Z}_N^{2g}$, the number of $(N, \ldots, N)$-subgroups that intersect it trivially equals $N^{g(g+1)/2}$.

Proof. As for the second count, consider generators $P_1, \ldots, P_g$ of the given subgroup G and extend to a symplectic basis $P_1, \ldots, P_g, Q_1, \ldots, Q_g$. The free rank-$g$ submodules that intersect G trivially each admit a unique basis of the form

$$\begin{aligned} P_1' &= Q_1 + a_{11}P_1 + \ldots + a_{1g}P_g, \\ &\vdots \\ P_g' &= Q_g + a_{g1}P_1 + \ldots + a_{gg}P_g, \end{aligned} \tag{2}$$

for certain $a_{ij} \in \mathbb{Z}_N$ and, conversely, every such basis generates a rank-g submodule intersecting G trivially. One checks that the maximal isotropy assumption

$\forall i,j : \langle P_i', P_j' \rangle = 0$ translates into $g(g-1)/2$ linear conditions on the a_{ij}'s. These conditions can be used to express the a_{ij}'s with $i > j$ in terms of the other a_{ij}'s. Thus we are left with $g^2 - g(g-1)/2 = g(g+1)/2$ degrees of freedom, as wanted.

As for the first count, we start with the case where $N = \ell$ is a prime number. The symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ acts transitively on the set of $(\ell, \ldots, \ell)$-subgroups, and our goal is to compute the size of the unique orbit. This can be done via the orbit-stabilizer theorem, which indeed yields

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

as detailed in [23, §1]. Next, to settle the case $N = \ell^n$ for $n > 1$, it suffices to see that the reduction-mod-ℓ map

$$\{\, (\ell^n, \ldots, \ell^n)\text{-subgroups of } \mathbb{Z}_{\ell^n}^{2g} \,\} \to \{\, (\ell, \ldots, \ell)\text{-subgroups of } \mathbb{F}_\ell^{2g} \,\}$$

is $\ell^{(n-1)g(g+1)/2}$-to-1. This works as before: consider generators $Q_1, \ldots, Q_g$ of an $(\ell^n, \ldots, \ell^n)$-subgroup G, and extend to a symplectic basis $Q_1, \ldots, Q_g, P_1, \ldots, P_g$. The $(\ell^n, \ldots, \ell^n)$-subgroups having the same reduction as G admit a unique basis of the form (2), where now each a_{ij} is an element of $\ell\mathbb{Z}_{\ell^n}$. Again, the maximal isotropy translates into expressions for the a_{ij}'s with $i > j$ in terms of the other a_{ij}'s, leaving us with $\ell^{(n-1)g(g+1)/2}$ subgroups, as wanted. The count for arbitrary N then follows from the Chinese remainder theorem. □

2.3 The Tate pairing on (products of) Jacobians

We discuss the Tate pairing on Jacobians, in the sense of Frey and Rück [20, 24], and its natural extension to products of Jacobians. Let C/K be a curve of genus $g \geq 1$ and let $N \geq 2$ be such that $\mathrm{char}\, K \nmid N$. The Tate pairing is a map

$$t_N : \mathrm{Pic}_K^0(C)[N] \times \mathrm{Pic}_K^0(C)/N\,\mathrm{Pic}_K^0(C) \;\to\; K^*/(K^*)^N,$$

where $\mathrm{Pic}_K^0(C)$ denotes the group of K-rational degree zero divisors on C considered modulo divisors of functions in $K(C)^*$, and is defined as follows. Let $\overline{D}_1 \in \mathrm{Pic}_K^0(C)[N]$ be represented by a divisor D_1 and let $\overline{D}_2 \in \mathrm{Pic}_K^0(C)/N\,\mathrm{Pic}_K^0(C)$ be represented by a divisor D_2 with support disjoint from that of D_1. Take a function $f_{N,D_1} \in K(C)^*$ whose divisor is ND_1. We then let

$$t_N(\overline{D}_1, \overline{D}_2) := f_{N,D_1}(D_2) \bmod (K^*)^N.$$

It can be shown that this is a well-defined bilinear pairing. In many cases of interest, the natural inclusion

$$\mathrm{Pic}_K^0(C) \hookrightarrow J_C(K)$$

is surjective, *i.e.,* it is a group isomorphism, and we obtain a pairing

$$J_C(K)[N] \times J_C(K)/NJ_C(K) \to K^*/(K^*)^N$$

that we keep denoting by t_N. Known sufficient conditions for surjectivity are that K has a trivial Brauer group (*e.g.,* this is true if K is finite) [29, Rmk. 1.11], that $C(K) \neq \emptyset$ [21, Thm. 3], or that $g = 2$ [13, Lem. 3.1 and Lem. 3.2].

In this paper we are mainly interested in the case where K is a certain function field over $\mathbb{Q}$, which has a non-trivial Brauer group. To avoid resulting pathologies, we only apply the Tate pairing in cases where $C(K) \neq \emptyset$ or where $g = 2$. We also consider the Tate pairing

$$t_N : A(K)[N] \times A(K)/NA(K) \to K^*/(K^*)^N$$

on abelian varieties A/K that arise as *products* of Jacobians of such curves: this is simply obtained by taking the product of the Tate pairings of the respective components.

Example 3. For use in Section 4.2, let us consider a genus-2 curve

$$C : y^2 = G_1(x)G_2(x)G_3(x)$$

over a field K of odd characteristic, where the G_i's are quadratic polynomials over K whose product is square-free. Each G_i defines an element $\overline{D}_i \in \mathrm{Pic}^0_K(C)$, namely the class of

$$D_i = (\alpha_{i1}, 0) + (\alpha_{i2}, 0) - \infty_1 - \infty_2,$$

with $\alpha_{i1}, \alpha_{i2} \in \overline{K}$ the two roots of G_i and with $\infty_1, \infty_2 \in C(\overline{K})$ the two points at infinity. An analysis of $\mathcal{L}(\infty_1+\infty_2)$ shows that D_i is non-principal, so from $2D_i = \mathrm{div}(G_i)$ we conclude that the $\overline{D}_i$'s have order 2. Let us compute $t_2(\overline{D}_1, \overline{D}_2)$. Replace D_1 by the equivalent divisor

$$D_1' = (\alpha_{11}, 0) + (\alpha_{12}, 0) - \infty_1 - \infty_2 - \mathrm{div}(x - c)$$

for some arbitrary $c \in K$ that is not a root of G_2. Then we can take $f_{2,D_1'} = G_1/(x-c)^2$ so that

$$t_2(\overline{D}_1, \overline{D}_2) \equiv f_{2,D_1'}(D_2) \equiv \frac{G_1(\alpha_{21})G_1(\alpha_{22})}{(\alpha_{21} - c)^2(\alpha_{22} - c)^2 \,\mathrm{lc}(G_1)^2} \equiv \mathrm{res}_x(G_1, G_2)$$

modulo $(K^*)^2$. Here $\mathrm{lc}(G_1)$ denotes the leading coefficient of G_1. By symmetry, it then follows that $t_2(\overline{D}_i, \overline{D}_j) \equiv \mathrm{res}_x(G_i, G_j)$ for all pairs of distinct $i, j \in \{1, 2, 3\}$.

If K is a finite field $\mathbb{F}_q$ containing a primitive Nth root of unity, *i.e.,* $N \mid q-1$, then the Tate pairing can be shown to be perfect. We remark that there is a way of extending Frey and Rück's definition of the Tate pairing to arbitrary abelian varieties over $\mathbb{F}_q$, where it remains perfect [6].

2.4 Multiradical field extensions

We say that a field extension $K \subseteq L$ is *multiradical* if there exist an integer $N \geq 1$ and elements $\alpha_1, \ldots, \alpha_r \in L$ such that $L = K(\alpha_1, \ldots, \alpha_r)$ and $\alpha_i^N \in K^*$

for all i. In this section, we discuss a sufficient Galois-theoretic condition for an extension to be multiradical. While we suspect that this is a well-known fact, we did not manage to find an exact reference, even for the case $r = 1$.

Recall that a group G is the (inner) semi-direct product $G_1 \rtimes G_2$ of a normal subgroup G_1 and a subgroup G_2 if the following three equivalent conditions hold:

- $G = G_1 G_2$ and $G_1 \cap G_2 = \{e_G\}$,
- every $g \in G$ can be written as $g = g_1 g_2$ for unique $g_1 \in G_1$ and $g_2 \in G_2$,
- every $g \in G$ can be written as $g = g_2 g_1$ for unique $g_1 \in G_1$ and $g_2 \in G_2$.

The group structure of G is determined by that of G_1 and G_2 and by how G_2 acts on G_1 through conjugation.

The prototypical example of a multiradical extension is where $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[N]{p_1}, \ldots, \sqrt[N]{p_r})$ for distinct primes p_i, which is a number field of degree N^r [1]. The Galois closure of L over K is $L(\zeta_N)$, with $\zeta_N \in \overline{L}$ a primitive Nth root of unity. Define

$$G_1 = \{\, \sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r} \,|\, 0 \leq i_j < N \text{ for all } j \,\} \;\cong\; \mathbb{Z}_N^r,$$

where $\sigma_j : \sqrt[N]{p_j} \mapsto \zeta_N \sqrt[N]{p_j}$ for $j = 1, \ldots, r$. Letting $G_2 = \{\, \tau_\ell : \zeta_N \mapsto \zeta_N^\ell \,|\, 0 \leq \ell < N, \gcd(\ell, N) = 1 \,\} \cong \mathbb{Z}_N^*$, one then verifies that

$$\mathrm{Gal}(L(\zeta_N)/K) = G_1 \rtimes G_2,$$

where the action is given by $\tau_\ell \circ \sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r} \circ \tau_\ell^{-1} = \sigma_1^{i_1 \ell} \circ \cdots \circ \sigma_r^{i_r \ell}$. Of course, this example generalizes to (the Galois closures of) arbitrary multiradical extensions, as long as $\mathrm{char}\, K \nmid N$ and $[L : K] = N^r$.

Lemma 4 gives a converse statement:

Lemma 4. *Let N, r be positive integers and consider a degree N^r extension $K \subseteq L$ of fields whose characteristic does not divide N. Let $\zeta_N \in \overline{L}$ be a primitive Nth root of unity and assume that $L(\zeta_N)$ is Galois over K with Galois group*

$$\mathrm{Gal}(L(\zeta_N)/K) = \mathrm{Gal}(L(\zeta_N)/K(\zeta_N)) \rtimes \mathrm{Gal}(L(\zeta_N)/L),$$

where the first factor is isomorphic to $\mathbb{Z}_N^r$, say generated by $\sigma_1, \ldots, \sigma_r$, and where the semi-direct product is according to the rule

$$\tau_\ell \circ \sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r} \circ \tau_\ell^{-1} = \sigma_1^{i_1 \ell} \circ \cdots \circ \sigma_r^{i_r \ell} \tag{3}$$

for all $i_1, \ldots, i_r \in \{0, \ldots, N-1\}$ and all $\tau_\ell : \zeta_N \mapsto \zeta_N^\ell \in \mathrm{Gal}(L(\zeta_N)/L)$. Then there exist $\alpha_1, \ldots, \alpha_r \in L$ such that $L = K(\alpha_1, \ldots, \alpha_r)$ and $\alpha_1^N, \ldots, \alpha_r^N \in K^*$.

Proof. First assume that $r = 1$ and write σ instead of σ_1. The restricted maps $\sigma^i|_L : L \to L(\zeta_N)$ are pairwise distinct. Indeed, if $i, i' \in \{0, 1, \ldots, N-1\}$ are such that $\sigma^i|_L = \sigma^{i'}|_L$, then

$$\sigma^{i-i'} \in \mathrm{Gal}(L(\zeta_N)/K(\zeta_N)) \cap \mathrm{Gal}(L(\zeta_N)/L) = \{\mathrm{id}\},$$

which can only be true if $i = i'$. From [36, Lem. 9.13.1] it follows that these restricted maps are linearly independent over $L(\zeta_N)$. In particular there exists some $\beta \in L$ such that

$$\alpha := \sum_{i=0}^{N-1} \zeta_N^i \sigma^i(\beta)$$

is non-zero. From

$$\tau_\ell(\alpha) = \sum_i \zeta_N^{i\ell}(\tau_\ell \circ \sigma^i)(\beta) = \sum_i \zeta_N^{i\ell}(\sigma^{i\ell} \circ \tau_\ell)(\beta) = \sum_i \zeta_N^{i\ell}\sigma^{i\ell}(\beta) = \alpha$$

it follows that $\alpha \in L$. Now observe that α was constructed in such a way that $\sigma^i(\alpha) = \zeta_N^{-i}\alpha$ for $i = 0, 1, \ldots, N-1$, which has two crucial consequences. On the one hand, it implies that $\mathrm{Gal}(L(\zeta_N)/L)$ is the exact group of automorphisms fixing $K(\alpha)$, or in other words $L = K(\alpha)$. On the other hand, it implies that $\sigma(\alpha^N) = \sigma(\alpha)^N = (\zeta_N\alpha)^N = \alpha^N$, so that α^N is fixed by the entire Galois group, i.e., $\alpha^N \in K$ as wanted.

The general case reduces to the case $r = 1$, as follows. Each element of our Galois group $\mathrm{Gal}(L(\zeta_N)/K)$ can be written as

$$\sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r} \circ \tau_\ell$$

for unique $0 \leq i_j, \ell < N$ with $\gcd(\ell, N) = 1$. For each $j = 1, \ldots, r$, let G_j, resp. H_j, be the subgroup obtained by imposing $i_j = 0$, resp. the normal subgroup obtained by imposing $i_j = 0$ and $\ell = 1$. Defining $L_j = L(\zeta_N)^{G_j}$, it is easy to check that $L(\zeta_N)^{H_j} = L_j(\zeta_N)$ and that the chain of inclusions $K \subseteq L_j \subseteq L_j(\zeta_N)$ satisfies the hypotheses of the lemma for $r = 1$. From the first part of our proof, we conclude that there exists an $\alpha_j \in L_j$ such that $L_j = K(\alpha_j)$ and $\alpha_j^N \in K^*$. But from $\cap_j G_j = \mathrm{Gal}(L(\zeta)/L)$ one sees that L is the compositum of the L_j's, from which the lemma follows. □

Note that if $r = 1$ and L contains ζ_N then Lemma 4 specializes to a standard statement from Kummer theory; observe that the factor $\mathrm{Gal}(L(\zeta_N)/L)$ is trivial in this case. In fact, our proof is a tweak of that of [36, Lem. 9.24.1]. In the current paper, we are mostly interested in the other end of the spectrum, where $\langle\zeta_N\rangle \cap L$ is as small as possible, *i.e.,* contained in $\{\pm 1\}$.

2.5 Charles–Goren–Lauter style hash functions

In [12], Charles, Goren and Lauter introduced a hash function based on isogenies between supersingular elliptic curves. This construction was generalized to work for Richelot isogenies between superspecial p.p. abelian surfaces in [9], by fixing an earlier proposal due to Takashima [39], shown to admit trivial collisions by Flynn and Ti [18]. We give a rough outline of the general construction and specify where needed.

Fix distinct primes p and ℓ, a dimension g, and let $G_{p,\ell,g}$ be the directed multigraph with vertex set V and edge set E, which are constructed as follows.

V consists of all superspecial p.p. abelian varieties over $\overline{\mathbb{F}}_p$ of dimension g up to isomorphism, which can always be defined over $\mathbb{F}_{p^2}$ [2]. The edge set E consists of all possible $(\ell, \ldots, \ell)$-isogenies between these p.p. abelian varieties. One can prove that the graph $G_{p,\ell,g}$ is connected [27], and in the case of supersingular elliptic curves, the graph is a Ramanujan graph [12]. Unfortunately, this is no longer the case for dimension $g > 1$ [27], but those graphs seem to exhibit strong expansion properties nonetheless; see [16] for an empiric analysis of the case $\ell = g = 2$. From Lemma 2 we see that it concerns a $\prod_{i=1}^{g}(\ell^i + 1)$-regular multigraph. One can try and turn this graph into an undirected graph by considering dual isogenies, but due to p.p. abelian varieties possibly having non-trivial automorphisms, the multiplicities of the edges and their duals may not coincide. For a more in-depth discussion regarding this phenomenon, we refer to [9, §4].

To turn this graph into a hash function, we must first fix a superspecial p.p. abelian variety and will commence a walk in the graph starting from this vertex. From this initial vertex, we label all outgoing edges in some way (e.g. lexicographical with regards to a fixed choice of representation of $\mathbb{F}_{p^2}$). From these $\prod_{i=1}^{g}(\ell^i + 1)$ edges, we only consider the first $\kappa = \ell^{g(g+1)/2}$ and we walk along the edge that corresponds to the least significant digit of m when expressed in base κ.[1] We have now arrived at a new p.p. abelian variety and want to avoid any possible backtracking while walking in the graph, so for our next edge, we should not consider all possible outgoing edges. For elliptic curves, it suffices to discard the edges corresponding to the dual isogenies [12], but for $g > 1$ we must discard all options that have a kernel which intersects the kernel of the dual isogeny non-trivially [9]. In general, again in view of Lemma 2, this leaves us with κ possible edges to consider, which correspond to good extensions of the isogeny corresponding to the first edge we chose. Once again, we label the κ outgoing edges in some deterministic way and will walk along the one that corresponds to the second least significant digit of m in base κ. We continue this until all the digits of the message have been processed. The output of the hash function is then an invariant of the final p.p. abelian variety we encounter. In the case of elliptic curves, one can choose the j-invariant for example.

3 On the existence of multiradical isogeny formulae

In this section we give a group-theoretic argument in favour of the existence of multiradical isogeny formulae. The argument is motivated by Lemma 4.

3.1 A multiradical modular cover

For an integer $n \geq 2$ and a subgroup $H \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_n)$, we consider the moduli problem of parametrizing pairs (A, α) up to H-equivalence, where A is a g-dimensional p.p. abelian variety and α is an n-level structure on it. Two pairs

[1] There is no real reason why one cannot consider all edges in this first step. Restricting to only κ choices however streamlines the algorithm.

(A_1, α_1) and (A_2, α_2) are called H-equivalent if there exists an isomorphism $\varphi : A_1 \to A_2$ and an element $h \in H$ such that $\alpha_1 = h \circ \alpha_2 \circ \varphi$. We write $[(A, \alpha)]_H$ for the H-equivalence class of (A, α), and denote the moduli set of such H-equivalence classes by $\mathcal{A}_g(H)$. Two extremal cases are $\mathcal{A}_g(\mathrm{GSp}_{2g}(\mathbb{Z}_n))$, which just parametrizes g-dimensional p.p. abelian varieties up to isomorphism, and $\mathcal{A}_g(\{\mathrm{id}\})$, which parametrizes g-dimensional p.p. abelian varieties A equipped with a generalized symplectic basis of $A[n]$. Note that if H' is a subgroup of H, then we have a natural map $\mathcal{A}_g(H') \to \mathcal{A}_g(H) : [(A, \alpha)]_{H'} \mapsto [(A, \alpha)]_H$.

We can construct a moduli set of g-dimensional p.p. abelian varieties A together with marked generators $P_1, \ldots, P_g$ of an $(N, \ldots, N)$-subgroup by choosing $n = N$ and letting H be

$$H_N = \left\{ \begin{pmatrix} \mathbb{I}_g & B \\ 0 & d\mathbb{I}_g \end{pmatrix} \;\middle|\; B \in \mathrm{Sym}_g(\mathbb{Z}_N),\, d \in \mathbb{Z}_N^* \right\} \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_N),$$

where $\mathrm{Sym}_g(\mathbb{Z}_N)$ denotes the set of symmetric $g \times g$ matrices with entries in $\mathbb{Z}_N$. Another (overcomplicated) way of arriving at a set with the same moduli interpretation is by instead letting $n = N^2$ and considering the group

$$\Gamma_{1,N} = \left\{ \, M \in \mathrm{GSp}_{2g}(\mathbb{Z}_{N^2}) \;\middle|\; M \bmod N \in H_N \, \right\}.$$

This creates room for defining the subgroup

$$\Gamma'_{1,N} = \left\{ \, M \in \Gamma_{1,N} \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_{N^2}) \;\middle|\; \text{lower-left } g \times g \text{ block of } M \text{ is zero} \, \right\},$$

whose associated moduli set parametrizes p.p. abelian varieties together with marked generators $Q_1, \ldots, Q_g$ of an $(N^2, \ldots, N^2)$-subgroup, considered modulo the following equivalence relation: two such sets of marked generators $Q_1, \ldots, Q_g$ and $R_1, \ldots, R_g$ are identified if and only if $R_i - Q_i \in \langle NQ_1, \ldots, NQ_g \rangle$ for $i = 1, \ldots, g$. Note that the points $P_i := NQ_i$ do not depend on the chosen representants Q_i, and neither do the cosets P'_i of Q_i modulo $\langle P_1, \ldots, P_g \rangle$.

Said differently, the set $\mathcal{A}_g(\Gamma'_{1,N})$ parametrizes g-dimensional p.p. abelian varieties A together with marked generators $P_1, \ldots, P_g$ of some $(N, \ldots, N)$-subgroup $G \subseteq A$, as well as with marked generators $P'_1, \ldots, P'_g$ of an $(N, \ldots, N)$-subgroup $G' \subseteq A/G$ which are such that the chain of quotient maps

$$A \overset{\varphi}{\to} A' = A/G \overset{\varphi'}{\to} A'/G'$$

is good, *i.e.,* it concerns an $(N^2, \ldots, N^2)$-isogeny. The natural map $\mathcal{A}_g(\Gamma'_{1,N}) \to \mathcal{A}_g(\Gamma_{1,N})$ just "forgets" about the points P'_i. Thus, the central question of our paper — given $P_1, \ldots, P_g$, how to find $P'_1, \ldots, P'_g$ — is closely related to understanding the fibers of this map.

Remark 5. In the above moduli interpretation, the marked generators P'_i have the additional property that

$$\hat{\varphi}(P'_i) = P_i \text{ for all } i = 1, \ldots, g, \tag{4}$$

where $\hat{\varphi} : A' \to A$ is the dual of φ. This feature was not explicitly asked for in the introduction. However, every subgroup $G' \subseteq A'$ for which $A' \to A'/G'$ is a good extension of φ admits a unique $\mathbb{Z}_N$-basis satisfying (4); we call this basis *distinguished*. It suffices to concentrate on such bases. Indeed, once we have found formulae for these distinguished generators, formulae for other sets of generators can be found by performing a base change, using arithmetic on A',[2] and this should not affect features like multiradicality, completeness and good reduction. Moreover, it seems reasonable to expect that the formulae for the distinguished generators will stand out in terms of simplicity (although we did not investigate this in detail).

The multiradical nature of the fibers of $\mathcal{A}_g(\Gamma'_{1,N}) \to \mathcal{A}_g(\Gamma_{1,N})$ is hinted at by the following observation, which invokes the notation $d(M)$ from (1), in combination with Lemma 4. Recall that the *normal core* of a subgroup H in a group G is the largest subgroup of H that is normal in G. For use below we remark that, under the Galois correspondence, this notion corresponds to the Galois closure of a separable field extension.

Lemma 6. *The group $\Gamma'_{1,N}$ has index $N^{g(g+1)/2}$ in $\Gamma_{1,N}$. The normal core $\operatorname{Core}(\Gamma'_{1,N})$ can be computed as $\{ M \in \Gamma'_{1,N} \mid d(M) \equiv 1 \bmod N \}$ and has index $\varphi(N)$ in $\Gamma'_{1,N}$. Every element of $\Gamma_{1,N}/\operatorname{Core}(\Gamma'_{1,N})$ admits a unique representant*

$$\sigma_1^{i_1} \cdots \sigma_{g(g+1)/2}^{i_{g(g+1)/2}} \cdot \tau_\ell \tag{5}$$

with $0 \le i_j < N$ for all $j = 1, \ldots, g(g+1)/2$, and $0 \le \ell < N$, $\gcd(N, \ell) = 1$. Here

$$\sigma_j = \begin{pmatrix} \mathbb{I}_g & 0 \\ N S_{k(j)} & \mathbb{I}_g \end{pmatrix}, \qquad \tau_\ell = \begin{pmatrix} \mathbb{I}_g & 0 \\ 0 & \ell \mathbb{I}_g \end{pmatrix},$$

where k denotes any bijection $\{1, \ldots, g(g+1)/2\} \to \{ (k_1, k_2) \mid 1 \le k_1 \le k_2 \le g \}$ and S_{k_1,k_2} is the symmetric $g \times g$ matrix having a 1 at positions (k_1, k_2) and (k_2, k_1) and 0's elsewhere. In particular $\Gamma_{1,N}/\operatorname{Core}(\Gamma'_{1,N})$ can be written as

$$\{ \sigma_j^{i_j} \mid 1 \le j \le g(g+1)/2,\ 0 \le i_j < N \} \rtimes \{ \tau_\ell \mid 0 \le \ell < N,\ \gcd(N, \ell) = 1 \} \cong \mathbb{Z}_N^{g(g+1)/2} \rtimes \mathbb{Z}_N^*,$$

with the semi-direct product according to the rule (3).

Proof. It is not hard to check that all matrices $M \in \Gamma_{1,N}$ have symmetric lower-left $g \times g$ blocks, *i.e.,* these blocks belong to $N \operatorname{Sym}_g(\mathbb{Z}_{N^2})$. A count shows that the resulting map

$$\Gamma_{1,N} \to N \operatorname{Sym}_g(\mathbb{Z}_N)$$

[2] For example, if N is odd, then the formulae for $2P'_1, \ldots, 2P'_g$ are obtained from those for $P'_1, \ldots, P'_g$ by feeding the latter to the formula for doubling on A'.

is uniform, implying that $[\Gamma_{1,N} : \Gamma'_{1,N}] = N^{g(g+1)/2}$. As for the normal core, conjugating $\Gamma'_{1,N}$ with suitable matrices (*e.g.,* one can use the σ_j's from the statement of the lemma) reveals that

$$\mathrm{Core}(\Gamma'_{1,N}) \subseteq \{\, M \in \Gamma'_{1,N} \,|\, d(M) \equiv 1 \bmod N \,\}$$

and since the right-hand side is a normal subgroup of $\Gamma_{1,N}$, equality must hold. Finally, we have $[\Gamma'_{1,N} : \mathrm{Core}(\Gamma'_{1,N})] = \varphi(N)$ because d defines a morphism $\Gamma'_{1,N} \to \mathbb{Z}_N^*$ which is surjective, as can be seen by evaluating it at the τ_ℓ's.

Now assume that some element of $\Gamma_{1,N}/\,\mathrm{Core}(\Gamma'_{1,N})$ admits two distinct decompositions

$$\sigma_1^{i_1} \cdots \sigma_{g(g+1)/2}^{i_{g(g+1)/2}} \cdot \tau_\ell = \sigma_1^{i'_1} \cdots \sigma_{g(g+1)/2}^{i'_{g(g+1)/2}} \cdot \tau_{\ell'}.$$

Applying d shows that $\ell \equiv \ell' \bmod N$, hence we can assume $\ell = \ell' = 1$. We then find

$$\sigma_1^{i_1 - i'_1} \cdots \sigma_{g(g+1)/2}^{i_{g(g+1)/2} - i'_{g(g+1)/2}} = \begin{pmatrix} \mathbb{I}_g & 0 \\ N \sum_{j=1}^{g(g+1)/2} (i_j - i'_j) S_{k(j)} & \mathbb{I}_g \end{pmatrix}. \tag{6}$$

But this is contained in $\Gamma'_{1,N}$ only if $i_j \equiv i'_j \bmod N$ for all j. In particular, the expansion (5) is unique. It must concern a full set of representants of $\Gamma_{1,N}/\,\mathrm{Core}(\Gamma'_{1,N})$ because there are $\varphi(N)N^{g(g+1)/2}$ such expansions.

The statement about the semi-direct product is easy to check using (6). □

We now give more details on how Lemma 6 supports the existence of multiradical isogeny formulae, although we stress that the discussion below is heuristic; the main support comes from the examples discussed in Section 4 and Section 5. A first major assumption is that the sets $\mathcal{A}_g(H)$ are aptly representable by geometric objects,[3] say by varieties[4] over $\mathbb{Q}$. It is then natural to expect that the chain

$$\mathcal{A}_g(\{\mathrm{id}\}) \to \mathcal{A}_g(\Gamma'_{1,N}) \to \mathcal{A}_g(\Gamma_{1,N}) \to \mathcal{A}_g(\mathrm{GSp}_{2g}(\mathbb{Z}_{N^2}))$$

corresponds to an inclusion of function fields of moduli spaces

$$\mathbb{Q}(\mathcal{A}_g(\mathrm{GSp}_{2g}(\mathbb{Z}_{N^2}))) \subseteq \mathbb{Q}(\mathcal{A}_g(\Gamma_{1,N})) \subseteq \mathbb{Q}(\mathcal{A}_g(\Gamma'_{1,N})) \subseteq \mathbb{Q}(\mathcal{A}_g(\{\mathrm{id}\}))$$

where the outer extension is Galois, with Galois group $\mathrm{GSp}_{2g}(\mathbb{Z}_{N^2})$, and where $\mathbb{Q}(\mathcal{A}_g(\Gamma_{1,N}))$, resp. $\mathbb{Q}(\mathcal{A}_g(\Gamma'_{1,N}))$, are the subfields fixed by $\Gamma_{1,N}$, resp. $\Gamma'_{1,N}$. This extrapolates upon known statements from the elliptic curve case, which can be found in [32, 34], for instance.

[3] We refer the interested reader to [30] for general background on moduli spaces of abelian varieties, although we note that we did not manage to pinpoint the precise statements needed for our purposes in the existing literature. It lies beyond our scope to study this in detail, but let us add the disclaimer that this may involve tweaks to our group-theoretic discussion, *e.g.,* in order to obtain a coarse moduli space one may need to work modulo $\{\pm\mathbb{I}_g\}$ to account for the -1-automorphism.

[4] These varieties may be geometrically reducible; more precisely, for $H \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_n)$ we expect $\mathcal{A}_g(H)$ to decompose into $[\mathbb{Z}_n^* : d(H)]$ irreducible components over $\mathbb{Q}(\zeta_n)$.

The middle inclusion has Galois closure

$$\mathbb{Q}(\mathcal{A}_g(\{\mathrm{id}\}))^{\mathrm{Core}(\Gamma'_{1,N})}$$

which, in the same vein, should be obtained from $\mathbb{Q}(\mathcal{A}_g(\Gamma'_{1,N}))$ by adding a primitive Nth root of unity ζ_N. The Galois group of this Galois closure is $\Gamma_{1,N}/\operatorname{Core}(\Gamma'_{1,N})$, so by Lemma 4 and Lemma 6 we have

$$\mathbb{Q}(\mathcal{A}_g(\Gamma'_{1,N})) = \mathbb{Q}(\mathcal{A}_g(\Gamma_{1,N}))(\sqrt[N]{\rho_1}, \ldots, \sqrt[N]{\rho_{g(g+1)/2}})$$

for certain functions $\rho_1, \ldots, \rho_{g(g+1)/2}$ on $\mathcal{A}_g(\Gamma_{1,N})$.

The line of thought behind multiradical isogenies is then that the coordinates of our distinguished generators $P'_1, \ldots, P'_g$ can essentially be viewed as functions on $\mathcal{A}_g(\Gamma'_{1,N})$, therefore they should be expressible in terms of the radicals $\sqrt[N]{\rho_i}$. Since we work over $\mathbb{Q}$, these expressions make sense over any field K, as long as $\operatorname{char} K$ does not divide any denominators; in fact, the idea/hope behind our good reduction assumption **(3)** is that all of this can be set up over $\mathbb{Z}[1/N]$ rather than $\mathbb{Q}$.

3.2 Conjectured existence of multiradical isogeny formulae

As we have discussed in the introduction, it only makes sense to talk about multiradical isogeny formulae at the level of concrete families that come equipped with formulae of Vélu, Richelot, ... type for the codomain p.p. abelian varieties.

Let us therefore repeat, in more detail, our main surmise. For integers $r, g \geq 1, N \geq 2$, we consider a smooth family of g-dimensional p.p. abelian varieties A_s equipped with marked points $P_{s,1}, \ldots, P_{s,g}$ that generate an $(N, \ldots, N)$-subgroup $G_s \subseteq A_s$, where the parameter $s = (s_1, \ldots, s_r)$ ranges over some quasi-affine subset $\mathcal{S} \subseteq \mathbb{A}^r$. We assume that we have algebraic formulae at our disposal, explicitly describing $A'_s = A_s/G_s$ in terms of the s_i. Then we believe that there always exist accompanying multiradical formulae, producing a set of generators $P'_{s,1}, \ldots, P'_{s,g}$ of an $(N, \ldots, N)$-subgroup $G'_s \subseteq A'_s$ which is such that the extension

$$A_s \xrightarrow{\varphi} A'_s = A_s/G_s \xrightarrow{\varphi'} A'_s/G'_s$$

is good. Moreover, we believe that the formulae can be chosen such that they are complete, and such that they work over any field over which the parametrization by $\mathcal{S}$ makes sense.

The radicands $\mathfrak{r}_i$ appearing in these formulae should be related to the functions ρ_i from the previous section, as follows. As before, assume we are working over $\mathbb{Q}$. By the universal property of moduli spaces, we should have a natural morphism $\sigma : \mathcal{S} \to \mathcal{A}_g(\Gamma_{1,N})$, sending s to the isomorphism class of $(A_s, P_{s,1}, \ldots, P_{s,g})$, which allows us to pull back the functions $\rho_i \in \mathbb{Q}(\mathcal{A}_g(\Gamma_{1,N}))$ to $\mathbb{Q}(\mathcal{S})$. These pull-backs should be our $\mathfrak{r}_i$'s. Explicitly,

$$\mathfrak{r}_1 := \rho_1 \circ \sigma, \quad \ldots, \quad \mathfrak{r}_{g(g+1)/2} := \rho_{g(g+1)/2} \circ \sigma,$$

which can indeed be viewed as algebraic expressions in the coordinates s_i.

For the sake of flexibility, we do not require the map $\mathcal{S} \to \mathcal{A}_g(\Gamma_{1,N})$ to be injective, *i.e.,* up to isomorphism, different s may result in the same p.p. abelian variety and the same generators of an $(N,\dots,N)$-subgroup. This adds another layer of hand-waviness to the discussion: indeed, it makes our way of thinking about the coordinates of $P'_{s,1},\dots,P'_{s,g}$ as functions on $\mathcal{A}_g(\Gamma'_{1,N})$ more frail. Nevertheless, our examples in Section 4 include several families featuring such a redundance.

Remark 7. Our formulae should make sense at every point of $\mathcal{S}$, therefore the functions $\mathfrak{r}_1,\dots,\mathfrak{r}_{g(g+1)/2}$ should be free of poles. In view of the completeness, they should also be free of zeroes.

Remark 8. For small families, the extension

$$\mathbb{Q}(\mathcal{S}) \subseteq \mathbb{Q}(\mathcal{S})(\sqrt[N]{\mathfrak{r}_1},\dots,\sqrt[N]{\mathfrak{r}_{g(g+1)/2}})$$

may not be of degree $N^{g(g+1)/2}$. Indeed, when pulled back along σ, several of the radicands ρ_i may become interrelated. In such cases it is tempting to compress the formulae into versions that use fewer radicals, but then the completeness property gets lost. For instance, in the example in Section 4.3 below, as many as $g(g-1)/2$ radicands collapse to the constant 1; nevertheless one should allow the corresponding occurrences of $\sqrt[N]{1}$ to range independently over the set of Nth roots of unity if one wants to find all $N^{g(g+1)/2}$ good extensions.

If our family of p.p. abelian varieties A_s consists of (products of) Jacobians of curves C_s which, when viewed as a single curve over $\mathbb{Q}(\mathcal{S})$, is either of genus 2 or admits a rational point, then our conjecture comes with the following addendum:

(4) Tate pairings as suitable radicands. The radicands $\mathfrak{r}_1,\dots,\mathfrak{r}_{g(g+1)/2}$ can be taken to be representants of the Tate pairings

$$t_N(P_{s,i},P_{s,j}) \in \mathbb{Q}(\mathcal{S})^*/(\mathbb{Q}(\mathcal{S})^*)^N$$

where $i \le j$ range over $\{1,\dots,g\}$.

This is motivated, again, by our examples below, and by the following observation. For each $1 \le i \le j \le g$, choose a representant $\mathfrak{r}_{i,j}$ of $t_N(P_{s,i},P_{s,j})$. Let $\mathbb{Q}(\mathcal{S})(G'_s)$ denote the field obtained from $\mathbb{Q}(\mathcal{S})$ by adjoining the coordinates of $P'_{s,1},\dots,P'_{s,g}$. As discussed in Remark 5, we can assume that $\hat{\varphi}(P'_{s,i}) = P_{s,i}$ for all i. This implies that

$$\mathfrak{r}_{i,j} = t_N(\hat{\varphi}(P'_{s,i}),\hat{\varphi}(P'_{s,j})) = t_N(P'_{s,i},P'_{s,j})^N$$

when viewed as elements of $\mathbb{Q}(\mathcal{S})(G'_s)^*/(\mathbb{Q}(\mathcal{S})(G'_s)^*)^N$; the second equality follows from the compatibility property of the Tate pairing, see [26, Lem. 5]. Thus $\mathbb{Q}(\mathcal{S})(G'_s)$ contains $\mathbb{Q}(\mathcal{S})(\sqrt[N]{\mathfrak{r}_{i,j}} \mid 1 \le i \le j \le g)$.

We did not manage to prove that these two fields are in fact equal, which would lend further support for our addendum.[5] While for $g = 1$ equality can

[5] Note however that the addendum is an even stronger statement, *e.g.,* in view of Remark 8.

be established using non-degeneracy of the Tate pairing over finite fields containing a primitive Nth root of unity [10, §3], for $g > 1$ non-degeneracy or even perfectness does not seem strong enough to mimic that argument.

4 Examples

In this section, we show how multiradical isogeny formulae manifest themselves for two well-known families: Richelot isogenies, and fully split isogenies from products of elliptic curves. We also discuss the multiradical nature of a certain $(5,5)$-isogeny that was described by Flynn [17]. Our main example, namely non-split $(3,3)$-isogenies from Jacobians of genus-2 curves, will be discussed in Section 5. We begin by recalling an elliptic curve example from [10].

4.1 Elliptic curves

Consider the family of elliptic curves E with a marked point $P \in E$ of order N. For $N \geq 4$ this family is conveniently parametrized by the Tate normal form:

$$E : y^2 + (1-b)xy - by = x^3 - bx^2, \qquad P = (0,0).$$

Concretely, we let $\mathcal{S} \subseteq \mathbb{A}^2$ be the subset of pairs b, c for which E is non-singular and P has exact order N; we refer to [38] for how to obtain a concrete equation for $\mathcal{S}$, which is a model of the modular curve $Y_1(N)$ and which is naturally defined over $\mathbb{Z}[1/N]$. The existence of radical and complete isogeny formulae was discussed in [10], where it was argued that one can take $\mathfrak{r}_1 = f_{N,P}(-P)$, with $f_{N,P}$ the function on E with divisor $N(P) - N(\infty)$, normalized such that its expansion at ∞ with respect to the uniformizer x/y has leading coefficient 1. As mentioned there, $\mathfrak{r}_1$ is a representant of $t_N(P,-P) = t_N(P,P)^{-1}$, so in order to enforce property **(4)**, one should instead work with $\mathfrak{r}_1^{-1}$. This does not cause any issues because $\mathfrak{r}_1$ has no zeroes or poles on $\mathcal{S}$; see also Remark 7.

For the sake of example, let us revisit the case $N = 5$, where we have $\mathfrak{r}_1 = b$ and $\mathcal{S} = \{\, (b,c) \in \mathbb{A}^2 \mid b = c,\, b \neq 0, (11 \pm 5\sqrt{5})/2 \,\}$. Vélu's formulae yield the following defining equation for $E' = E/\langle P \rangle$:

$$y^2 + (1-b)xy - by = x^3 - bx^2 - 5b(b^2+2b-1)x - b(b^4+10b^3-5b^2+15b-1).$$

From [10, §4] we see that the point

$$\begin{aligned} P' = {} & (5\sqrt[5]{\mathfrak{r}_1}^4 + (b-3)\sqrt[5]{\mathfrak{r}_1}^3 + (b+2)\sqrt[5]{\mathfrak{r}_1}^2 + (2b-1)\sqrt[5]{\mathfrak{r}_1} - 2b, \\ & 5\sqrt[5]{\mathfrak{r}_1}^4 + (b-3)\sqrt[5]{\mathfrak{r}_1}^3 + (b^2-10b+1)\sqrt[5]{\mathfrak{r}_1}^2 + (13b-b^2)\sqrt[5]{\mathfrak{r}_1} - b^2 - 11b) \end{aligned} \quad (7)$$

on E' is of the requested kind, *i.e.,* it is the distinguished generator of a subgroup $G' \subseteq E[5]$ such that the composed isogeny $E \to E' \to E'/G'$ is cyclic of degree 25. Varying the choice of $\sqrt[5]{\mathfrak{r}_1}$ produces the five subgroups for which this is true. The formula (7) satisfies good reduction and allows for a very fast computation of chains of 5-isogenies over finite fields; *e.g.,* over $\mathbb{F}_p$ with $p \not\equiv 1 \bmod 5$ we obtain a speed-up by a factor ≈ 40 over more traditional methods [10, Tbl. 4]. We recall that, for general N, the good reduction property is conjectural [10, Conj. 1].

4.2 Richelot isogenies

A convenient reference for Richelot isogenies is [35, Ch. 8]. We consider genus-2 curves C equipped with two generators of a $(2,2)$-subgroup of J_C. Such marked curves can be parametrized by $\mathcal{S} = \mathbb{A}^9 \setminus \Delta$, by letting $s = (s_{ij})_{1\leq i,j\leq 3}$ correspond to the Jacobian of

$$C : y^2 = G_1(x)G_2(x)G_3(x), \qquad G_i(x) = s_{i1}x^2 + s_{i2}x + s_{i3}$$

equipped with the divisor classes $\overline{D}_1, \overline{D}_2$ from Example 3. Here Δ is cut out by the discriminant of $G_1(x)G_2(x)G_3(x)$. The parametrization works over $\mathbb{Z}[1/2]$. We claim that we can take $\mathfrak{r}_1 = \mathrm{res}_x(G_2, G_3)$, $\mathfrak{r}_2 = \mathrm{res}_x(G_1, G_3)$ and $\mathfrak{r}_3 = \mathrm{res}_x(G_1, G_2)$. By Example 3 we know that

$$\begin{aligned} t_2(\overline{D}_1, \overline{D}_1) &\equiv \mathfrak{r}_2\mathfrak{r}_3 \\ t_2(\overline{D}_1, \overline{D}_2) &\equiv \mathfrak{r}_3 \\ t_2(\overline{D}_2, \overline{D}_2) &\equiv \mathfrak{r}_1\mathfrak{r}_2 \end{aligned}$$

modulo squares, so the validity of property **(4)** is not affected by our choice of radicands. Indeed, formulae in terms of $\sqrt{\mathfrak{r}_1}, \sqrt{\mathfrak{r}_2}, \sqrt{\mathfrak{r}_3}$ can easily be rewritten into formulae in terms of $\sqrt{\mathfrak{r}_2\mathfrak{r}_3}, \sqrt{\mathfrak{r}_3}, \sqrt{\mathfrak{r}_1\mathfrak{r}_2}$, and vice versa.

To proceed, we first slightly shrink $\mathcal{S}$ by removing the zero locus of the determinant $\delta = |s_{i,j}|_{1\leq i,j\leq 3}$. This guarantees that the p.p. abelian surface $J_C/\langle \overline{D}_1, \overline{D}_2\rangle$ is again a Jacobian. More precisely, Richelot's formulae show that it is isomorphic to $J_{C'}$ with

$$C' : \delta y^2 = H_1(x) \cdot H_2(x) \cdot H_3(x),$$

where $H_1 := G_2'G_3 - G_2G_3'$, $H_2 := G_3'G_1 - G_3G_1'$ and $H_3 := G_1'G_2 - G_1G_2'$. The reader can verify that $\mathrm{disc}(H_i) = 4\mathfrak{r}_i$, so the two zeroes of H_i are algebraic expressions in $\sqrt{\mathfrak{r}_i}$ and in the s_{ij}'s, and they are obtained from one another by choosing the other square root of $\mathfrak{r}_i$; denote these two zeroes by $\alpha_{\pm i}$. Then according to [9, Prop. 2] the classes of

$$D_1' = (\alpha_1, 0) + (\alpha_2, 0) - \infty_1 - \infty_2, \qquad D_2' = (\alpha_{-1}, 0) + (\alpha_3, 0) - \infty_1 - \infty_2$$

generate a $(2,2)$-subgroup of $J_{C'}$ that defines a $(4,4)$-extension of the incoming isogeny $J_C \to J_{C'}$. Still according to [9, Prop. 2], the sign flips $\pm i$ produce the eight subgroups for which this is true. Thus we have found formulae that are multiradical and complete, and they clearly work in any characteristic different from 2.

Remark 9. One could also try and study the complementary case, namely the restriction $\mathcal{S}_0$ of $\mathcal{S}$ to the zero locus of δ. In this case $J_C/\langle \overline{D}_1, \overline{D}_2\rangle$ geometrically splits as a product of two elliptic curves. Concrete equations for these elliptic curves can be found on [35, p. 119]. The reader can check that they are defined over the field obtained by adding a square root of $\mathrm{disc}_z(\mathrm{disc}_x(G_2 + zG_3))$ which, interestingly, turns out to be $16\mathfrak{r}_1$. However, for a genuine verification of our conjecture, one would need a model of $J_C/\langle \overline{D}_1, \overline{D}_2\rangle$ over $\mathbb{Q}(\mathcal{S}_0)$ rather than $\mathbb{Q}(\mathcal{S}_0)(\sqrt{\mathfrak{r}_1})$. This model concerns the Weil restriction of an elliptic curve over the latter field. Therefore it is not so easily described explicitly; see also [4].

4.3 Fully split $(N, \ldots, N)$-isogenies from products of elliptic curves

In this example we consider g-fold products $E_1 \times \cdots \times E_g$ of elliptic curves, marked with generators $D_1, \ldots, D_g$ of an $(N, \ldots, N)$-subgroup that are of the following kind: each D_i is a g-tuple with ∞_{E_j} at entry j, except when $j = i$ where we then have a point $P_i \in E_i$ of order N. Assuming $N \geq 4$, such marked products are naturally parametrized by $\mathcal{S}^g \subseteq \mathbb{A}^{2g}$, with $\mathcal{S}$ the modular curve $Y_1(N)$ from Section 4.1. Note that the corresponding $(N, \ldots, N)$-isogenies split completely, *i.e.,* they are of the form

$$\Phi : E_1 \times \ldots \times E_g \to E'_1 \times \ldots \times E'_g,$$

decomposing as the product of cyclic N-isogenies $\phi_i : E_i \to E'_i$ with kernel $\langle P_i \rangle$. We assume that the elliptic curves E'_i are given by Vélu's formulae.

For each $i = 1, \ldots, g$, we let $\mathfrak{r}_i$ be the representant of the Tate self-pairing $t_N(P_i, P_i)$ whose inverse was described in Example 4.1. We then choose the following representants of the Tate pairings $t_N(D_i, D_j)$, $1 \leq i \leq j \leq g$: we pick 1 as soon as $i < j$, and we pick $\mathfrak{r}_i$ if $i = j$.

We are interested in identifying all $(N, \ldots, N)$-subgroups of $(E'_1 \times \cdots \times E'_g)[N]$ that have trivial intersection with the kernel of the dual of Φ. Indeed, these are precisely the subgroups that can occur as $\ker \Psi$ for a good extension Ψ of Φ. To get a handle on the kernel of $\hat{\Phi}$, which is just the product of the $\hat{\phi}_i$'s, we rely on Lemma 10 below. When applied over $\mathbb{Q}(\mathcal{S})$, it implies that for each $i = 1, \ldots, g$ we can find a formula $P'_i(\sqrt[N]{1})$ which, when reading $\sqrt[N]{1}$ as ζ_N, produces a generator P'_i of $\ker \hat{\phi}_i$ and which, when reading $\sqrt[N]{1}$ as ζ_N^k, produces the point kP'_i for $0 \leq k \leq N-1$. Then $\ker \hat{\Phi}$ can be written as $\langle C'_1, \ldots, C'_g \rangle$, where each C'_i is a g-tuple with $\infty_{E'_j}$ at each entry, except at $j = i$ where we have P'_i.

Lemma 10. *Let E be an elliptic curve over a field K with $\operatorname{char} K \nmid N$ and let $P \in E(K)$ be a point of order N. Let $\phi : E \to E' = E/\langle P \rangle$ be the corresponding quotient isogeny, where E' is given by Vélu's formulae. Let P' be a generator of the dual isogeny. Then there exist polynomials $F, G, H \in K[z]$ such that*

$$(F(\zeta_N^k) : G(\zeta_N^k) : H(\zeta_N^k)) = kP'$$

for all $0 \leq k \leq N-1$.

Proof. The Weil pairing establishes an isomorphism between $\ker \hat{\phi}$ and μ_N that is compatible with the action of $\operatorname{Gal}(\overline{K}/K)$. In particular P' has coordinates in $K(\zeta_N)$. Define $F(z)$ to be the classical Lagrange polynomial that interpolates the x-coordinates of kP' for $0 \leq k \leq N-1$. More precisely,

$$F(z) = \sum_{k=0}^{N-1} x(kP')\ell_k(z), \text{ with } \ell_k(z) = \prod_{\substack{0 \leq m \leq N-1 \\ m \neq k}} \frac{z - \zeta_N^m}{\zeta_N^k - \zeta_N^m}.$$

Then it suffices to show that for any $\sigma \in \mathrm{Gal}(K(\zeta_N)/K)$ it holds that $F(z) = F^\sigma(z)$. Note that $\sigma : \zeta_N \mapsto \zeta_N^a$ for some a coprime to N. One verifies that

$$\ell_k^\sigma(z) = \prod_{\substack{0 \le m \le N-1 \\ m \neq k}} \frac{z - \zeta_N^{am}}{\zeta_N^{ak} - \zeta_N^{am}} = \prod_{\substack{0 \le m \le N-1 \\ m \neq ak}} \frac{z - \zeta_N^{m}}{\zeta_N^{ak} - \zeta_N^{m}} = \ell_{ak}(z).$$

Furthermore, if we assume that the x-coordinates of the points of $\ker \hat{\phi}$ within the same Galois orbit were chosen compatibly, then because of the aforementioned isomorphism we must have $\sigma(x(kP')) = x(akP')$, such that indeed $F(z) = F^\sigma(z)$ as wanted. The polynomials G and H can be argued completely analogously. □

We also know that, for each $i = 1, \ldots, g$, there exists a formula $Q_i'(\sqrt[N]{\mathfrak{r}_i})$ producing a point Q_i' that extends P_i' to a basis of $E_i'[N]$. Furthermore, we know that by scaling $\sqrt[N]{\mathfrak{r}_i}$ with ζ_N^k for $0 \le k \le N-1$, we cycle through all elements $Q_i' + kP_i'$.

We are ready to give multiradical and complete formulae that produce g-tuples $D_1', \ldots, D_g' \in E_1' \times \cdots \times E_g'$ generating the kernel of a good extension Ψ of Φ. Fix

$$D_1' = (Q_1'(\sqrt[N]{\mathfrak{r}_1}), P_2'(\sqrt[N]{1}), \ldots, P_g'(\sqrt[N]{1})),$$

which has g degrees of freedom. Next, choose

$$D_2' = (\infty_{E_1'}, Q_2'(\sqrt[N]{\mathfrak{r}_2}), P_3'(\sqrt[N]{1}), \ldots, P_g'(\sqrt[N]{1})),$$

where we fixed the first coordinate at $\infty_{E_1'}$ in order to avoid repetitions in the subgroups generated by D_1' and D_2'. This results in $g-1$ degrees of freedom. Continuing this inductively, we end up with

$$D_g' = (\infty_{E_1'}, \ldots, \infty_{E_{g-1}'}, Q_g'(\sqrt[N]{\mathfrak{r}_g}))$$

with only 1 degree of freedom left. In total, we have $\sum_{j=1}^{g} j = g(g+1)/2$ degrees of freedom as wanted, and running through all possible interpretations of the radicals (including the $g(g-1)/2$ occurrences of $\sqrt[N]{1}$) results in the kernels of all possible good extensions.

4.4 Flynn's family of (5, 5)-isogenies from genus-2 curve Jacobians

Consider the family of genus-2 curves with given $(5,5)$-subgroup from [17], involving a single parameter r. In this section, we illustrate its multiradical nature. We do not aim at a full analysis including completeness, etc; in fact, for simplicity we will restrict to the curve at $r = 1$. We remark that the absolute Igusa invariants of Flynn's family are in fact parameterless, so up to isomorphism this is the only curve in the family.

In order for the generators of the $(5,5)$-subgroup to be rational (and not just the subgroup), we will fix the base field as $\mathbb{Q}(\zeta_5)$, where ζ_5 is a fifth root of

unity.[6] Writing $\gamma_1 = \sqrt{5} = 2\zeta_5^3 + 2\zeta_5^2 + 1 \in \mathbb{Q}(\zeta_5)$, we have

$$C : y^2 = x^5 + 25x^4 - 200x^3 + 560x^2 - 640x + 256,$$
$$T_1 = (4, 16\gamma_1) - \infty, \qquad T_2 = (0, 16) - \infty,$$

where $T_1, T_2 \in J_C[5]$. Writing $\gamma_2 = \sqrt{2(1/\gamma_1 - 1)} = \frac{2\zeta_5^3 - 6\zeta_5^2 - 4\zeta_5 - 2}{5} \in \mathbb{Q}(\zeta_5)$, the genus-2 curve associated to the isogenous abelian surface obtained by quotienting out $\langle T_1, T_2 \rangle$ can be written as

$$\widetilde{C} : y^2 = x^5 - 125x^4 + 5000x^3 - 175000x^2 + 1250000x - 81250000,$$
$$\widetilde{T_1} = (10\gamma_1, 10000\gamma_2) - \infty, \quad \widetilde{T_2} = (-10\gamma_1, 5000\gamma_2(\gamma_1 + 1)) - \infty,$$

where $\langle \widetilde{T_1}, \widetilde{T_2} \rangle$ is the kernel of the dual isogeny (in particular, $\widetilde{T_1}, \widetilde{T_2} \in J_{\widetilde{C}}[5]$). In order to extend $\langle \widetilde{T_1}, \widetilde{T_2} \rangle$ to a basis for the 5-torsion of the Jacobian of $\widetilde{C}$, with conjectured property **(4)** in mind we compute the following Tate pairings:

$$t_5(T_1, T_1) \equiv \gamma_1, \quad t_5(T_1, T_2) \equiv (\gamma_1 - 1)/2, \quad t_5(T_2, T_2) \equiv 1.$$

Defining $\mathfrak{r}_1 = \gamma_1$ and $\mathfrak{r}_2 = (\gamma_1 - 1)/2$, our conjecture predicts that we can expect to find the 5-torsion of $J_{\widetilde{C}}$ in $\mathbb{Q}(\zeta_5, \sqrt[5]{\mathfrak{r}_1}, \sqrt[5]{\mathfrak{r}_2})$. In order to compute this 5-torsion, we use techniques from [22] that build upon the work of [8].

Concretely, a typical 5-torsion point is expected to be represented by a divisor $D = P_1 + P_2 - 2\infty = (x_1, y_1) + (x_2, y_2) - 2\infty$, for two affine points $(x_1, y_1), (x_2, y_2)$ on $\tilde{C}$. We read the condition $5D \equiv 0$ as $5(P_1 - \infty) \equiv -5(P_2 - \infty)$. In [8], recursive formulae are derived to express $5((x_1, y_1) - \infty)$ in function of x_1, y_1 and the coefficients of our genus-2 curve $\tilde{C}$. The same can be done for $-5((x_2, y_2) - \infty)$ and the aforementioned equality results in a system of equations that can be solved by a Gröbner basis computation. Note that for D to be rational over a certain field, x_1, y_1, x_2, y_2 need not necessarily be defined over that same field. In Mumford coordinates, we can write $D = \left(x^2 - (x_1 + x_2)x + x_1x_2, y_1 + (y_2 - y_1)\frac{x - x_1}{x_2 - x_1}\right)$ and it suffices for the coefficients of these polynomials to be defined over the field. In practice, it is most convenient to simply add an extra variable and corresponding equation to the Gröbner basis computation from before, such as $X - (x_1 + x_2)$, and then compute the minimal polynomial of X (*i.e.,* put it last in the monomial ordering for the Gröbner basis computation). The roots of this polynomial will then correspond to all possible $x_1 + x_2$ such that the class of D is 5-torsion.

There are $5^4 - 1 = 624$ nontrivial elements in $J_{\widetilde{C}}[5]$, but since D and $-D$ correspond to the same $x_1 + x_2$, we expect the minimal polynomial of X to be of degree 312 generically. In this specific case though, we have multiple 5-torsion divisors of the form $(x_1, y_1) - \infty$ rather than $(x_1, y_1) + (x_2, y_2) - 2\infty$ (*e.g.,* this is the case for $\widetilde{T_1}$ and $\widetilde{T_2}$). The techniques of [22] do not capture such points.

[6] Remark that the quadratic extension $\mathbb{Q}(\sqrt{5})$ would suffice, but adding ζ_5 makes for easier notation up ahead.

Nonetheless, all other 5-torsion divisors can be found this way and the minimal polynomial of X turns out to be of degree 305. Factoring this polynomial over $\mathbb{Q}(\zeta_5, \sqrt[5]{\mathfrak{r}_1}, \sqrt[5]{\mathfrak{r}_2})[X]$ we see that it splits completely as expected, thereby lending support to our conjecture.

A similar computation can be done for the other coefficients of the Mumford coordinates, which allows us to define

$$\widetilde{T}_3 = \left(x^2 + 100\left(\frac{\alpha_2^4 - (\zeta_5+1)^2\alpha_2^3 - (\zeta_5^4+1)\alpha_2^2 + (\zeta_5^3 - 2\zeta_5 - 2)\alpha_2}{\gamma_1\zeta_5^3(\zeta_5+1)^2} + 1\right)x + \right.$$
$$\left. 500\left(\frac{10\alpha_2^4 - 2(\zeta_5-1)^2\alpha_2^3 - 2(7\zeta_5^3+11\zeta_5^2+7\zeta_5)\alpha_2^2 + 10(\zeta_5^3-2\zeta_5-2)\alpha_2}{\gamma_1\zeta_5^3(\zeta_5+1)^2} + 1\right),\right.$$
$$100\Big((7\zeta_5^2 - \zeta_5 + 7)\alpha_2^4 - (2\zeta_5^3 + 5\zeta_5^2 + 2\zeta_5)\alpha_2^3 + (7\zeta_5^3 + 5\zeta_5 + 5)\alpha_2^2 -$$
$$(6\zeta_5^3 + 7\zeta_5^2 + 7\zeta_5 + 6)\alpha_2 - 7\Big)x + 5000\Big(-(3\zeta_5^2 + 3\zeta_5 + 3)\alpha_2^4 -$$
$$\left.(2\zeta_5^3 - \zeta_5^2 + 2\zeta_5)\alpha_2^3 + (\zeta_5^3 - \zeta_5 - 1)\alpha_2^2 + (6\zeta_5^3 + 3\zeta_5^2 + 3\zeta_5 + 6)\alpha_2 - 5\Big)\right),$$

where $\alpha_2 = \sqrt[5]{\mathfrak{r}_2}$. One can easily verify that $\widetilde{T}_3 \in J_{\widetilde{C}}[5] \setminus \langle \widetilde{T}_1, \widetilde{T}_2 \rangle$. The expression for a fourth element $\widetilde{T}_4$ that completes a basis for $\mathrm{Jac}(\widetilde{C})[5]$ is too voluminous to reproduce here, but can be found online in our repository at https://github.com/KULeuven-COSIC/Multiradical-Isogenies. From this basis, the 125 maximal isotropic $(5,5)$-subgroups that determine a kernel which intersects the kernel of the dual isogeny trivially can easily be computed.

5 Multiradical (3, 3)-isogenies

5.1 The parametrization by Bruin, Flynn and Testa

Over any field K with $\mathrm{char}\, K \nmid 6$, we consider $\mathbb{A}^3$ with coordinates r, s, t, and we let $\mathcal{S} \subseteq \mathbb{A}^3$ be the joint complement of the zero loci of

$$\begin{aligned}
\delta_1 &= t,\\
\delta_2 &= s,\\
\delta_3 &= st + 1,\\
\delta_4 &= r^3 - 3rt + t^2 + t,\\
\delta_5 &= r^3 s - 3rst + st^2 + st + t,\\
\delta_6 &= r^3 s^2 - 3rs^2 t - 3rs + s^2 t^2 + s^2 t + 2st + s + 1,\\
\delta_7 &= r^3 s^2 t + r^3 s - 3rs^2 t^2 - 3rst + s^2 t^3 + s^2 t^2 + 2st^2 + t,\\
\Delta &= r^6 s^2 - 6r^4 s^2 t - 3r^4 s + 2r^3 s^2 t^2 + 2r^3 s^2 t + 3r^3 st + r^3 s + r^3\\
&\quad + 9r^2 s^2 t^2 + 6r^2 st - 6rs^2 t^3 - 6rs^2 t^2 - 9rst^2 - 3rst - 3rt + s^2 t^4\\
&\quad + 2s^2 t^3 + s^2 t^2 + 2st^3 + 3st^2 + t^2 + t
\end{aligned}$$

and also of $r-1$, r^2-t and $rs-st-1$ (we don't give a name to these last three polynomials since their role is less essential, see Remark 12 below). Following Bruin, Flynn and Testa [5], to r,s,t we then attach the genus-2 curve $C_{rst}: y^2 = F_{rst}(x)$, where

$$F_{rst}(x) = G_1(x)^2 + \lambda_1 H_1(x)^3 = G_2(x)^2 + \lambda_2 H_2(x)^3$$

and

$$\begin{aligned}
H_1(x) &= x^2 + rx + t,\\
\lambda_1 &= 4s,\\
G_1(x) &= (s - st - 1)x^3 + 3s(r-t)x^2 + 3sr(r-t)x - st^2 + sr^3 + t,\\
H_2(x) &= x^2 + x + r,\\
\lambda_2 &= 4st,\\
G_2(x) &= (s - st + 1)x^3 + 3s(r-t)x^2 + 3sr(r-t)x - st^2 + sr^3 - t.
\end{aligned}$$

One can calculate that $\operatorname{disc}(F_{rst}) = -2^{12}3^6\delta_1^3\delta_2^3\delta_3\delta_4^3\delta_5\delta_6^3\delta_7^3 \neq 0$, so it indeed concerns a genus-2 curve. We write J_{rst} for the Jacobian of C_{rst}.

Proposition 11. *For $i = 1, 2$, write $T_i \in J_{rst}(K)$ for the divisor class of*

$$(H_i, G_i) := (\alpha_{i1}, G_i(\alpha_{i1})) + (\alpha_{i2}, G_i(\alpha_{i2})) - \infty_1 - \infty_2,$$

where $\alpha_{i1}, \alpha_{i2} \in \overline{K}$ denote the zeroes of $H_i(x)$. Then $\langle T_1, T_2\rangle$ is a maximal isotropic subgroup of J_{rst}, and the quotient $J_{rst}/\langle T_1, T_2\rangle$ is isomorphic over K to the Jacobian $J^{(-3)}_{r's't'}$ of the genus-2 curve

$$C^{(-3)}_{r's't'} : -3y^2 = F_{r's't'}(x)$$

where $(r', s', t') = \psi_0(r, s, t) :=$

$$\left(\frac{-s(r-1)(r^2-t)(\delta_5 - r)}{(rs - st - 1)^2\delta_4}, \frac{(rs - st - 1)^3\delta_4^2}{st(r-1)^3\Delta}, \frac{s^2(r-1)^3(r^2-t)^3}{(rs - st - 1)^3\delta_4^2}\right).$$

Writing $F_{r',s',t'}(x) = G_1'(x)^2 + \lambda_1' H_1'(x)^3 = G_2'(x)^2 + \lambda_2' H_2'(x)^3$ as above, the kernel of the dual isogeny is generated by the corresponding points T_i', by which we mean the divisor classes of

$$(H_i', G_i'/\sqrt{-3}) = (\alpha_{i1}', G_i'(\alpha_{i1}')/\sqrt{-3}) + (\alpha_{i2}', G_i'(\alpha_{i2}')/\sqrt{-3}) - \infty_1 - \infty_2,$$

with $\alpha_{i1}', \alpha_{i2}' \in \overline{K}$ the zeroes of $H_i'(x)$, for $i = 1, 2$.

Proof. This follows from [5, Thm. 6 & Lem. 10]. □

We call (H_i, G_i) the *Mumford coordinates* of T_i, because of the clear analogy with the Mumford coordinates in the case of hyperelliptic curves with an imaginary Weierstrass model. (For an even better analogy, one should reduce the degree of the second component by writing $(H_i, G_i \bmod H_i)$.)

All sufficiently general triples (C, T_1, T_2) with C a genus-2 curve and T_1, T_2 generating a $(3,3)$-subgroup of J_C are reached by the above parametrization. One exception is where the effective parts of (the natural representants of) the divisor classes corresponding to the generators T_1, T_2 have non-disjoint supports. This is how one should understand the role of $r-1$, r^2-t, $rs-st-1$: if any one of these expressions is zero, then one can still consider C_{rst}, T_1, T_2 as above,[7] but the formalism of [5] will produce generators of the kernel of the dual isogeny that have non-disjoint supports.

Remark 12. While for certain curves the parametrization misses certain pairs T_1, T_2 generating a $(3,3)$-subgroup, any $(3,3)$-subgroup is reached. Indeed, by [5, Lem. 3], at least one choice of basis with generators from $\{T_1, T_2, T_1+T_2, T_1-T_2\}$ will be in sufficiently general form.

The role of Δ is more fundamental: it should not vanish because otherwise $J_{rst}/\langle T_1, T_2\rangle$ is $\overline{K}$-isomorphic to a product of elliptic curves.

We discuss the multiradical isogeny formulae corresponding to the family $\mathcal{S}$ in Section 5.2. First, as an intermezzo, let us elaborate and discuss how to handle the case $\Delta = 0$, as well as how to walk away from products of elliptic curves. None of the material below is new, however, to the best of our knowledge, there is no article containing all these formulae, so we felt it was worth gathering them.

From Jacobians to products If $\Delta = 0$, then any algebraic software package can easily verify that the polynomial $F_{rst}(x)$ factors in two cubic polynomials over the ring $\mathbb{Q}(r,s,t,\zeta_3)[x]/(\Delta)$, where ζ_3 is a primitive cubic root of unity. This factorization induces an isogeny to a product of elliptic curves, and we refer to [28] for the general construction for (ℓ,ℓ)-split Jacobians. In the specific case of a (3,3)-split Jacobian, we mention the complete characterization by [3, Prop. A.2].

Proposition 13. *Let C be a genus-2 curve over a field K with* $\operatorname{char} K \nmid 6$*, and J its Jacobian. If J is $(3,3)$-isogenous to a product of elliptic curves $E_1 \times E_2$, then there exist elements $a, b, c, d, t \in K$ with*

$$12ac + 16bd = 1, \qquad \Delta_1 = a^3 + b^2 \neq 0, \qquad \Delta_2 = c^3 + d^2 \neq 0, \qquad t \neq 0,$$

such that C is isomorphic to $C_{abcdt} : ty^2 = f(x)$ and E_i is isomorphic to $E_{i,abcdt} : ty^2 = f_i(x)$ for $i \in \{1,2\}$, with

$$\begin{aligned} f(x) &= (x^3 + 3ax + 2b)(2dx^3 + 3cx^2 + 1), \\ f_1(x) &= x^3 + 12(2a^2d - bc)x^2 + 12(16ad^2 + 3c^2)\Delta_1 x + 512\Delta_1^2 d^3, \\ f_2(x) &= x^3 + 12(2bc^2 - ad)x^2 + 12(16b^2c + 3a^2)\Delta_2 x + 512\Delta_2^2 b^3. \end{aligned}$$

[7] As long as no δ_i vanishes.

The corresponding morphisms $\varphi_i : C_{abcdt} \to E_{i,abcdt}$ *are given by*

$$\varphi_1(x,y) \mapsto \left(12\Delta_1 \frac{-2dx+c}{x^3+3ax+2b}, y\Delta_1 \frac{16dx^3-12cx^2-1}{(x^3+3ax+2b)^2}\right),$$
$$\varphi_2(x,y) \mapsto \left(12\Delta_2 \frac{x^2(ax-2b)}{2dx^3+3cx^2+1}, y\Delta_2 \frac{x^3+12ax-16b}{(2dx^3+3cx^2+1)^2}\right).$$

As mentioned, the Jacobian of a genus-2 curve is generically not $(3,3)$-split. If it is, however, the curves $E_{1,abcdt}$ and $E_{2,abcdt}$ will typically be unique up to isomorphism, *i.e.,* the Jacobian should not be expected to split in more than one way. Up to isomorphism, there are only two genus-2 curves which are $(3,3)$-isogenous to distinct products of elliptic curves [33].

Ideally, we would like more uniform formulae to identify the curves C_{rst} and C_{abcdt} with one another in the case Δ equals zero. Unfortunately, these formulae would be extremely lengthy and finding an isomorphism from one to the other in practice can be done relatively easily by a Gröbner basis computation since isomorphisms between genus-2 curves are well-understood.

Isogenies from products Let $E_1 \times E_2$ be a product of elliptic curves, both defined over a field K with $\operatorname{char} K \nmid 6$, and $T_1, T_2 \in (E_1 \times E_2)(K)[3]$ such that $\langle T_1, T_2\rangle$ is maximal isotropic with regards to the 3-Weil pairing. Then $(E_1 \times E_2)/\langle T_1, T_2\rangle$ is again a product of elliptic curves in two scenarios. The first scenario is the most common one, where T_1, T_2 correspond to 3-torsion points on the separate elliptic curves E_1, E_2. The codomain of the isogeny can be computed using Vélu's formulae.

Proposition 14. *Let* E_1, E_2 *be elliptic curves over a field* K *with* $\operatorname{char} K \nmid 6$*, with non-trivial* $T_1 \in E_1[3], T_2 \in E_2[3]$*. Then* E_i *can be written as* $E_i : y^2 + a_i xy + b_i y = x^3$ *for* $i \in \{1,2\}$*, where the* T_i *have been translated to* $(0,0)$ *on the respective curves. Write* $G = \langle (T_1, \infty_{E_2}), (\infty_{E_1}, T_2)\rangle$*. Then the codomain of the isogeny with kernel* G *is again a product of elliptic curves* $E_1' \times E_2'$*, where for* $i \in \{1,2\}$ *we can write*

$$E_i' : y^2 + a_i xy + b_i y = x^3 - 5a_i b_i x - a_i^3 b_i - 7b_i^2.$$

The second situation where the codomain of a $(3,3)$-isogeny with domain $E_1 \times E_2$ is again a product of elliptic curves, is the relatively rare occurrence when there exists a 2-isogeny $\theta : E_1 \to E_2$. In this case, the isogeny is the endomorphism

$$\begin{aligned} \phi : E_1 \times E_2 &\to E_1 \times E_2 \\ (P,Q) &\mapsto (P + \hat{\theta}(Q), -Q + \theta(P)), \end{aligned}$$

with kernel the graph of the 2-isogeny $\theta|_{E_1[3]}$, see for example [19].

In all other scenarios, $(E_1 \times E_2)/\langle T_1, T_2\rangle$ is the Jacobian of a genus-2 curve, where the kernel is the graph of an anti-isometry with regards to the 3-Weil pairing. By this we mean that there exists an isomorphism $\psi : E_1[3] \to E_2[3]$

such that $e_3(\psi(P), \psi(Q)) = e_3(P, Q)^{-1}$ for all $P, Q \in E_1[3]$. The formulae in this case are simply the dual isogenies of the split Jacobians in Proposition 13.

Of the 40 $(3, 3)$-isogenies with domain $E_1 \times E_2$, generically there are 16 with codomain a product of elliptic curves, and 24 with codomain the Jacobian of a genus-2 curve. The only exception to this is by means of an aforementioned 2-isogeny $\theta : E_1 \to E_2$.

5.2 Multiradical formulae

We are interested in finding good extensions of our $(3, 3)$-isogeny

$$J_{rst} \longrightarrow J^{(-3)}_{r's't'} = J_{rst}/\langle T_1, T_2 \rangle. \tag{8}$$

In view of the conjectured property **(4)**, let us compute the relevant Tate pairings. The reader might want to compare the following lemma with the Weil pairing computation from [5, Lem. 4].

Lemma 15. *Let*

$$C : y^2 = G_1^2 + \lambda_1 H_1^3 = G_2^2 + \lambda_2 H_2^3$$

be a genus-2 curve over K with $G_1, G_2, H_1, H_2 \in K[x]$ and H_1, H_2 quadratic, and consider the corresponding points $T_1 = (H_1, G_1), T_2 = (H_2, G_2) \in J_C[3]$. Then $t_3(T_1, T_2) \equiv \mathrm{res}_x(G_1 - G_2, H_2)/\lambda_1$.

Proof. Write α_{11}, α_{12}, resp., α_{21}, α_{22}, for the roots of $H_1(x)$, resp., $H_2(x)$. It is easy to check that $G_1(x) - y$ has divisor $3(H_1, G_1)$; however, in order to move away from infinity, as we did in Example 3, we instead work with $(G_1(x) - y)/(x - c)^3$ for some $c \in K$ that is different from α_{21}, α_{22}. Evaluating this function in (H_2, G_2) yields

$$t_3(T_1, T_2) \equiv -\frac{(G_1(\alpha_{21}) - G_2(\alpha_{21})(G_1(\alpha_{22}) - G_2(\alpha_{22}))}{(\alpha_{21} - c)^3(\alpha_{22} - c)^3 \lambda_1 \,\mathrm{lc}(H_1)^3} \equiv \mathrm{res}_x(G_1 - G_2, H_2)/\lambda_1$$

modulo $(K^*)^3$. □

Applying this to our instances of T_1, T_2, one checks that $\mathrm{res}_x(G_1 - G_2, H_2)/\lambda_1$ equals δ_4/δ_2. As for the other pairings: Bruin, Flynn and Testa have also provided an explicit Mumford representation (H_3, G_3) for $T_3 := T_1 + T_2$, see [5, Thm. 6], and the analogous computations yield $t_3(T_1, T_3) \equiv \delta_7^2$ and $t_3(T_3, T_2) \equiv \delta_1 \delta_6^2$. From these outcomes it follows that

$$t_3(T_1, T_1) \equiv \delta_2 \delta_4^2 \delta_7^2, \qquad t_3(T_1, T_2) \equiv \delta_2^2 \delta_4, \qquad t_3(T_2, T_2) \equiv \delta_1 \delta_2 \delta_4^2 \delta_6^2.$$

We will instead work with the radicands

$$\begin{aligned} \mathfrak{r}_1 &= \delta_7 \equiv t_3(T_1, T_1) t_3(T_1, T_2), \\ \mathfrak{r}_2 &= \delta_2 \delta_4^2 \equiv t_3(T_1, T_2)^{-1}, \\ \mathfrak{r}_3 &= \delta_1 \delta_6^2 \equiv t_3(T_1, T_2) \cdot t_3(T_2, T_2), \end{aligned}$$

which does not affect the validity of property **(4)**. Indeed, formulae in terms of $\sqrt[3]{\mathfrak{r}_1}$, $\sqrt[3]{\mathfrak{r}_2}$, $\sqrt[3]{\mathfrak{r}_3}$ can easily be rewritten into formulae in terms of $\sqrt[3]{\mathfrak{r}_1\mathfrak{r}_2} = \sqrt[3]{t_3(T_1,T_1)}$, $\sqrt[3]{1/\mathfrak{r}_2} = \sqrt[3]{t_3(T_1,T_2)}$, $\sqrt[3]{\mathfrak{r}_2\mathfrak{r}_3} = \sqrt[3]{t_3(T_2,T_2)}$, and vice versa.

The good extensions of (8) are characterized by the fact that their kernel intersects the kernel $\langle T_1', T_2'\rangle$ of the dual isogeny trivially. In order to find such kernels, we are first and foremost interested in extending T_1', T_2' to a basis of the 3-torsion. To this end, we try to find all $b_1, \ldots, b_7$ such that

$$F_{r's't'}(x) = (b_4x^3 + b_3x^2 + b_2x + b_1)^2 + b_7(x^2 + b_5x + b_6)^3. \tag{9}$$

Indeed, every such tuple produces a divisor D with Mumford coordinates

$$(x^2 + b_5x + b_6, (b_4x^3 + b_3x^2 + b_2x + b_1)/\sqrt{-3})$$

satisfying $3D = (b_4x^3 + b_3x^2 + b_2x + b_1 - \sqrt{-3}y)$, hence $\overline{D} \in J^{(-3)}_{r's't'}[3]$. Conversely, every 3-torsion point arises in this way, see for example [7]. Over an algebraic closure of the base field, 80 nontrivial 3-torsion elements exist and hence 80 tuples $(b_1, \ldots, b_7)$ that satisfy the above equation. We remark though, that every solution $(b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ immediately results in a second solution $(-b_1, -b_2, -b_3, -b_4, b_5, b_6, b_7)$ due to the square. On the level of Mumford representations, this corresponds with D and $-D$ having the same first component.

The parametrization from Section 5.1 already gives rise to eight solution tuples $(b_1, \ldots, b_7)$ corresponding to the elements in $\{iT_1' + jT_2' : 0 \leq i, j \leq 2\} \setminus \{0\}$. To find the rest of the tuples, one can write out the equation of $F_{r's't'}(x)$ as well as the right-hand side of (9), and equate the found coefficients of the degree-six polynomial. One can then compute a reduced Gröbner basis of these seven expressions to a preferred monomial ordering.[8]

Assuming we put b_4 last in the monomial ordering, the last polynomial of the Gröbner basis will be a degree-80 polynomial in just b_4, of which all the roots correspond to possible solutions for b_4 in (9). Up to some constant factor, this minimal polynomial of b_4 is of the form

$$M(b_4) = \prod_{i=1}^{4}(b_4^2 - \beta_i^2) \prod_{k=1}^{4} f_k(b_4),$$

where the $f_k(b_4)$ are polynomials of degree 18, and the β_i are the (necessarily rational) solutions corresponding to $\{iT_1' + jT_2' : 0 \leq i, j \leq 2\} \setminus \{0\}$. These β_i appear in pairs, which on the level of divisors coincides with the correspondence between D and $-D$, and for the same reason one can see that the polynomials f_k ought to be even. We will write $f_k'(b_4)$ for the polynomial obtained by halving the exponents of the monomials of $f_k(b_4)$.

[8] Performing a straightforward Gröbner basis computation in $\mathbb{Q}[r, s, t, b_1, \ldots, b_7]$ will quickly result in memory issues. Instead, one can first transform $F_{r's't'}$ to the more generic form $x^6 + ax^4 + bx^3 + cx^2 + dx + e$ to suppress the high degrees of r', s', t'. Next, one can compute the Gröbner basis over $\mathbb{F}_p[a, b, c, d, e, b_1, \ldots, b_7]$ for many p, then lift the solution to $\mathbb{Q}[a, b, c, d, e, b_1, \ldots, b_7]$ with the Chinese remainder theorem.

One can verify that the polynomials $f'_k(b_4) \in \mathbb{Q}(r,s,t)[b_4]$ all have Galois group $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3^*$, but the action of $\mathbb{Z}_3^*$ originates from a cubic root of unity, and their Galois groups over $\mathbb{Q}(r,s,t,\zeta_3)$ are thus $\mathbb{Z}_3 \times \mathbb{Z}_3$. Writing $\alpha_1 = \sqrt[3]{\mathfrak{r}_1}$, $\alpha_2 = \sqrt[3]{\mathfrak{r}_2}$, $\alpha_3 = \sqrt[3]{\mathfrak{r}_3}$, it turns out that they split completely when extending the field $\mathbb{Q}(r,s,t,\zeta_3)$ with $\{\alpha_1,\alpha_2\}$, $\{\alpha_1,\alpha_3\}$, $\{\alpha_2,\alpha_3\}$ or $\{\alpha_1\alpha_2,\alpha_1\alpha_3\}$. All roots of one specific $f'_k(b_4)$ can be obtained from a single given root, by scaling the cubic roots with powers of ζ_3. On the level of divisors, these associated roots correspond to adding a linear combination of T'_1 and T'_2. More precisely, one can associate the roots of the polynomials f'_k as follows:

$$\begin{aligned}
x_1(\zeta_3^i\alpha_1, \zeta_3^j\alpha_2) &\longleftrightarrow T'_3 + iT'_1 + jT'_2 \text{ for } 0 \le i,j \le 2,\\
x_2(\zeta_3^i\alpha_1, \zeta_3^j\alpha_3) &\longleftrightarrow T'_4 + iT'_1 + jT'_2 \text{ for } 0 \le i,j \le 2,\\
x_3(\zeta_3^i\alpha_2, \zeta_3^j\alpha_2) &\longleftrightarrow T'_3 + T'_4 + iT'_1 + jT'_2 \text{ for } 0 \le i,j \le 2,\\
x_4(\zeta_3^i\alpha_1\alpha_2, \zeta_3^j\alpha_1\alpha_3) &\longleftrightarrow T'_3 - T'_4 + iT'_1 + jT'_2 \text{ for } 0 \le i,j \le 2,
\end{aligned}$$

for any T'_3, T'_4 that extend $\langle T'_1, T'_2\rangle$ to a basis of $J^{(-3)}_{r's't'}[3]$, where x_k is a single root of $f'_k(b_4)$. This correspondence can be seen from the fact that all $f'_k(b_4)$ split over different fields, yet T'_1 and T'_2 are rational over the ground field. Furthermore, for any fixed choice of $i,j,k \in \{0,1,2\}$, any two distinct divisors from this correspondence coinciding with the choice of $\zeta_3^i\alpha_1, \zeta_3^j\alpha_2, \zeta_3^k\alpha_3$ generate a $(3,3)$-subgroup that intersects $\langle T'_1, T'_2\rangle$ trivially. Hence, to find the 27 (up to sign) distinct b_4 that correspond to a $(3,3)$-subgroup which is the kernel of a good extension relative to the original isogeny, it suffices to scale the radicands with cubic roots of unity.

In the appendix, we have included two expressions for b_4 which we believe are the easiest amongst the b_4 in terms of arithmetic. Alternatively, the formulae can also be extracted from the code of our hash function from Section 6, which can be found in our online repository at `https://github.com/KULeuven-COSIC/Multiradical-Isogenies`. One can derive closed algebraic expressions for b_i in function of b_4 for $i \in \{1,2,3,5,6,7\}$. However, in practice, it is more efficient to only partially do this for the easier expressions, and the remainder by means of a small Gröbner basis computation. Finding the 27 distinct pairs of tuples $(b_1,\ldots,b_7)$ corresponding to good extensions is done by simply scaling the radicands in the expressions of the b_4 with cubic roots of unity before computing the rest of the b_i.

Remark 16. Observe that our formulae involve a factor $\sqrt{-3}$ (called `twist`), but this factor disappears when considering the corresponding Mumford coordinates.

Iterated application Using this new $(3,3)$-subgroup $\langle T'_3, T'_4\rangle$ as kernel for a new isogeny is easiest if we first transform $C_{r's't'}$ into an isomorphic curve C_{RST}, where T'_3 and T'_4 have now taken the role of the T_1 and T_2 from Section 5.1 again. This isomorphism allows us to only need to perform the rational transformation $\psi_0(R,S,T)$ to compute the next isogenous curve. To find this isomorphism, one

can use the construction of [5] that has been implemented in Magma in [18]. This construction makes use of somewhat expensive field extensions though, and in practice, a Gröbner basis computation is more efficient.

6 Hash function from (3, 3)-isogenies

We can use the $(3,3)$-isogenies from the previous section to construct a hash function similar to the hash function from [9]. We will start by describing a general outline, followed by some more in-depth discussion regarding choices that must be made.

6.1 The graph $\mathcal{G}_p$

For a large prime p we construct the (directed multi-)graph $\mathcal{G}_p$ as follows. The vertices are all the $\overline{\mathbb{F}}_{p^2}$-isomorphism classes of superspecial p.p. abelian surfaces, which can always be defined over $\mathbb{F}_{p^2}$. In practice we assume $p \equiv 2 \bmod 3$ and work with representants $A/\mathbb{F}_{p^2}$ on which Frobenius acts as multiplication with $-p$; see [2]. A consequence of this choice is that $A[3] \subseteq A(\mathbb{F}_{p^2})$; indeed, on 3-torsion points Frobenius acts as multiplication by $-p \equiv 1 \bmod 3$. The edges are all possible $(3,3)$-isogenies between these p.p. abelian surfaces, where multiplicities need to be taken into account. Given that only the superspecial surfaces are considered, the graph $\mathcal{G}_p$ is a directed 40-regular finite multigraph. In order to hash a given message in this graph, we first choose an arbitrary — yet fixed — starting vertex. Next, we order the 40 outgoing edges from this vertex according to some fixed order (*e.g.,* lexicographic), and choose the first 27 to continue with. The message that needs to be hashed is then converted into trits, and we choose to walk along the edge that corresponds to the three least significant trits of the message towards the next vertex. At this vertex, we consider the 27 outgoing edges that correspond to $(3,3)$-isogenies that intersect the dual of the previous isogeny trivially. Now we follow the edge that corresponds to the next three trits of the message. By excluding the other 13 $(3,3)$-isogenies, we avoid trivial cycles in our path by not (partially or fully) backtracking. This process is repeated until the entire message has been hashed. As output, an invariant of the resulting p.p. abelian surface is then returned.

Given that we will have to compute cubic roots in the computations, p should ideally be chosen such that the valuation of $p^2 - 1$ at 3 is 1 in order to speed up the computations. In combination with our assumption $p \equiv 2 \bmod 3$, this means we want $p \equiv 2, 5 \bmod 9$. Of course, we want p large enough to provide ample security. The graph $\mathcal{G}_p$ was proven to be connected, see for example [27]. Even though the graph is not Ramanujan, in the $(2,2)$-case it still exhibits strong expander properties so we assume this to be the case for $(3,3)$-isogenies as well. The set of edges of the graph is of size $\mathcal{O}(p^3)$, of which the majority consists of p.p. abelian surfaces corresponding to Jacobians of genus-2 curves, and only $\mathcal{O}(p^2)$ corresponding to products of elliptic curves.

Remark 17. Since $p^2 \equiv 1 \bmod 3$ we have $\sqrt{-3} \in \mathbb{F}_{p^2}$. Consequently, we can ignore the twisting factor -3 from Proposition 11 and identify $J_{rst}/\langle T_1, T_2 \rangle$ with $J_{r's't'}$. This comes at the (negligible) expense of carrying an extra factor $\sqrt{-3}$ in our multiradical isogeny formulae (called `twist` in our code); see Remark 16.

6.2 Starting p.p. abelian surface

It is still an open problem whether one can generate a supersingular elliptic curve over a large prime field in reasonable time without knowing its endomorphism ring. This knowledge can in fact compromise the security of the associated cryptographic protocols, see for example [15]. Even though this has not been explicitly written down yet for superspecial p.p. abelian surfaces, it is not too far-fetched to assume the knowledge of its endomorphism ring can provide similar security risks. On the same note, it is not known how to construct a genus-2 curve of which the Jacobian is superspecial. Some exceptional curves are known however, see for example [25]. Note that all of these are curves with many automorphisms, possibly leading to small collisions at the start of the hash function. Ergo, the best starting vertex in our graph should be obtained by taking a random walk in the graph starting from one of these exceptional cases. Given that the isomorphism classes corresponding to products of elliptic curves have negligible occurrence for cryptographically large p, we can assume our starting vertex to be the Jacobian of a genus-2 curve. Furthermore, we are interested in only 27 of the 40 $(3,3)$-subgroups of this Jacobian. Hence our starting point can be chosen as an (r,s,t)-parametrization from Section 5.1, where the 27 $(3,3)$-subgroups correspond precisely to those that intersect the $(3,3)$-subgroup determined by the (r,s,t)-parametrization trivially. This choice can be seen as having performed a step 0 in the hash function, where the kernel of the dual isogeny is determined by this (r,s,t)-parametrization.

6.3 Genus-2 curves versus products of elliptic curves

The cases of vertices corresponding to the Jacobians of genus-2 curves or the product of two elliptic curves will of course need to be handled differently with regards to computing the next edge in our graph. Apart from this internal code distinction, it is preferred that a hash function has a fixed size as output. The isomorphism class of the Jacobians of genus-2 curves can be classified by their absolute Igusa invariants, which are ordered triplets, whereas products of elliptic curves are completely determined by an unordered pair of j-invariants. In order to unify these two types of invariants in one output, we first note that the entropy of the output is only $3 \log p$, and not $6 \log p$ as the absolute Igusa invariants may suggest. If one is okay with the hash function having a set that is sparse in a much larger set as output, one can apply the following method during the hashing. Whenever we arrive in a vertex corresponding to a product of elliptic curves, we (deterministically) take one more step in the graph without processing information, to a vertex corresponding to the Jacobian of a genus-2 curve again. Alternatively, if one only wants an output of the same length as there is entropy,

one needs to choose a function to reduce both the absolute Igusa invariants as well as the pair of j-invariants to something of size $3 \log p$.

6.4 Implementation

We implemented our $(3,3)$-hash function in Magma (version 2.26-1) and ran it on an Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz with 128 GB memory. For every prime size we averaged the speed over 100 random inputs of 1000 bits. A summary of our timed results can be found in the following table, where we included the timings of the $(2,2)$-hash function from [9] for comparison.

	$p \approx 2^{86}$	$p \approx 2^{128}$	$p \approx 2^{171}$	$p \approx 2^{256}$
bits of classical security	128	192	256	384
bits of quantum security	86	128	170	256
output bits	516	768	1026	1536
time per bit processed $(2,2)$	5.01ms	6.52ms	9.33ms	15.70ms
time per bit processed $(3,3)$ (this work)	4.70ms	4.87ms	5.54ms	6.36ms

To understand why the $(3,3)$-hash function scales much better than the $(2,2)$-hash function, we take a look at the breakdown of the computation cost in the following table.

	$p \approx 2^{86}$	$p \approx 2^{128}$	$p \approx 2^{171}$	$p \approx 2^{256}$
Tate pairings (cubic roots)	7.0%	8.5%	11.2%	14.3%
Compute b_4's (arithmetic)	20.5%	18.9%	18.9%	17.0%
Find other b_i's (two GCD's)	16.4%	15.9%	15.8%	15.2%
Reparametrize r, s, t (Gröbner basis)	54.6%	55.3%	52.7%	52.2%
Isogenous curve (arithmetic)	1.5%	1.4%	1.4%	1.3%

As p grows, the degrees involved in the polynomials of step 3 and 4 in this table don't change, hence the complexity of these steps is only dependent on the arithmetic of the associated field $\mathbb{F}_{p^2}$. Asymptotically, root finding over finite fields $\mathbb{F}_{p^2}$ for large p scales a lot worse than addition and multiplication, such that in the $(3,3)$-hash function step 1 in the table takes up a larger relative amount of work as p grows. For p large enough, this part of the computation will dominate the total cost. In the $(2,2)$-hash function on the other hand, the computation is already heavily dominated by the three (square) roots for small p, with only a handful of basic arithmetic operations.

Furthermore, the valuation of $p^2 - 1$ at N determines the complexity of finding an Nth root of an element in $\mathbb{F}_{p^2}$. One can choose p such that $9 \nmid p^2 - 1$ but at the very least we always have $8 \mid p^2 - 1$, which means cubic roots can be found significantly cheaper than square roots. In practice, Magma can compute cubic roots over $\mathbb{F}_{p^2}$ faster than square roots with a factor of about 2.7 for large enough p.

Additionally, for every three computed roots, the $(3,3)$-hash function can process 3 trits, whereas the $(2,2)$-hash function can only process 3 bits. Asymptotically we can thus expect the $(3,3)$-hash function to outperform the $(2,2)$-hash

function by a total factor of $2.7 \cdot (3/2)^3 \approx 9$. For $\mathbb{F}_{p^2}$ with $p = 2^{1024} + 643$ for example, we see that $(2,2)$-hashing a 100-bit message takes about 20.4 seconds, whereas $(3,3)$-hashing a 100-bit message takes about 2.26 seconds.

References

[1] Iurie Boreico. My favorite problem – linear independence of radicals. In *The Harvard College Mathematics Review*, volume 2, pages 87–92. 2008.

[2] Bradley W. Brock. *Superspecial curves of genera two and three.* PhD thesis, Princeton University, 1994.

[3] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen. Genus-2 curves and jacobians with a given number of points. *LMS Journal of Computation and Mathematics*, 18(1):170–197, 2015.

[4] Nils Bruin and Kevin Doerksen. The arithmetic of genus two curves with $(4,4)$-split Jacobians. *Canadian Journal of Mathematics*, 63(5):992–1021, 2011.

[5] Nils Bruin, E. Victor Flynn, and Damiano Testa. Descent via (3, 3)-isogeny on jacobians of genus 2 curves. *Acta Arithmetica*, 165(3):201–223, 2014.

[6] Peter Bruin. The Tate pairing for abelian varieties over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 23(2):323–328, 2011.

[7] Frank Calegari, Shiva Chidambaram, and David P Roberts. Abelian surfaces with fixed 3-torsion. In *Proceedings of ANTS-XIV*, volume 4 of *Open Book Series*, pages 91–108. Mathematical Sciences Publishers, 2020.

[8] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal für die reine und angewandte Mathematik*, 1994(447):91–146, 1994.

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

[10] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *Proceedings of Asiacrypt 2020 Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519. Springer, 2020.

[11] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Proceedings of Asiacrypt 2018 Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

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

[13] Daniel Coray and Constantin Manoil. On large Picard groups and the Hasse principle for curves and K3 surfaces. *Acta Arithmetica*, 76:165–189, 1996.

[14] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, available at https://eprint.iacr.org/2006/291, 2006.

[15] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Proceedings of Eurocrypt 2018*, volume 10822 of *Lecture Notes in Computer Science*, pages 329–368. Springer, 2018.

[16] Enric Florit and Benjamin Smith. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. Cornell University arXiv, available at https://arxiv.org/abs/2101.00919, 2020.

[17] E. Victor Flynn. Descent via (5, 5)-isogeny on jacobians of genus 2 curves. *Journal of Number Theory*, 153:270–282, 2015.

[18] E. Victor Flynn and Yan Bo Ti. Genus two isogeny cryptography. In *Proceedings of PQCrypto 2019*, volume 11505 of *Lecture Notes in Computer Science*, pages 286–306. Springer, 2019.

[19] Gerhard Frey and Ernst Kani. Curves of genus 2 covering elliptic curves and an arithmetical application. In *Proceedings of Arithmetic Algebraic Geometry*, volume 89 of *Progress in Mathematics*, pages 153–176. Springer, 1991.

[20] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.

[21] Steven D. Galbraith, Sachar Paulus, and Nigel P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002. (The cited theorem refers to a preliminary version of this paper, published as Hewlett-Packard Labs technical report HPL-98-179, available at https://www.hpl.hp.com/techreports/98/HPL-98-179.pdf).

[22] Pierrick Gaudry and Éric Schost. Modular equations for hyperelliptic curves. *Mathematics of Computation*, 74(249):429–454, 2005.

[23] Genevieve Hanlon. Counting points in $\mathrm{Sp}(2n, \mathbb{F}_q)$/maximal parabolic subgroup. Course notes available at http://www-math.mit.edu/~dav/symplectic_parabolic.pdf, 2005.

[24] Florian Hess. A note on the Tate pairing of curves over finite fields. *Archiv der Mathematik*, 82:28–32, 2004.

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

[26] Sorina Ionica. Pairing-based methods for jacobians of genus 2 curves with maximal endomorphism ring. *Journal of Number Theory*, 133(11):3755–3770, 2013.

[27] Bruce W. Jordan and Yevgeni Zaytman. Isogeny graphs of superspecial abelian varieties and Brandt matrices. Cornell University arXiv:2005.09031, 2021.

[28] Robert M. Kuhn. Curves of genus 2 with split Jacobian. *Transactions of the American Mathematical Society*, 307(1):41–49, 1988.

[29] James Milne. Abelian varieties. Course notes, version 2.0, available at https://www.jmilne.org/math/CourseNotes/av.html, 2008.

[30] James Milne. Introduction to Shimura varieties. Course notes, available at https://www.jmilne.org/math/xnotes/svi.pdf, 2017.

[31] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[32] David E. Rohrlich. Modular curves, Hecke correspondence, and L-functions. In *Modular forms and Fermat's last theorem*, pages 41–100. Springer, 1997.

[33] Tony Shaska. Genus 2 fields with degree 3 elliptic subfields. *Forum Mathematicum*, 16:263–280, 2004.

[34] Samir Siksek. Explicit arithmetic of modular curves. Summer school notes, available at https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf, 2019.

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

[36] The Stacks project authors. The stacks project. Available at https://stacks.math.columbia.edu, 2021.

[37] Anton Stolbunov. Public-key encryption based on cycles of isogenous elliptic curves. Master's thesis, Saint-Petersburg State Polytechnical University, 2004. In Russian.

[38] Marco Streng. Generators of the group of modular units for $\Gamma_1(N)$ over the rationals. Cornell University arXiv, available at https://arxiv.org/abs/1503.08127v2, 2015.

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

[40] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, 1971.

Appendix: code for 3-torsion

The following is the Magma code that accompanies Section 5.2. The essence can be found hard-coded in the hash function of our online repository at https://github.com/KULeuven-COSIC/Multiradical-Isogenies, but these formulae are deemed important enough to add them in an appendix.

The variables `r,s,t` in the code represent the domain of the $(3,3)$-isogeny, whereas `R,S,T` coincide with the parameters of the codomain.[9] The variables `a,b,c` represent cubic roots of factors of the Tate pairings. The variables `b4ab` and `b4bc` represent solutions for b_4 in (9). Note that we work with b_4 instead of b_5 since in practice we want to be able to distinguish between a divisor and its inverse. From these two solutions for b_4, we compute a Gröbner basis to find solutions for the other b_i. Note that the formulae are general, but Magma struggles to work over a degree 54 extension of a function field in 3 variables. Hence, to make the code work standalone, we opted to work with a concrete example where $(R,S,T) = (2,5,-3)$. To verify the formulae in their generality, one can work over $\mathbb{Q}(R,S,T)$ where you adjoin only the cubic roots corresponding to for example `a,b`, and then assert that one of the degree 18 factors from the minimal polynomial of b_4 coincides with the product $\prod_{i=1}^{3}\prod_{j=1}^{3}(x^2 - b_4(\zeta_3^i a, \zeta_3^j b))$, where the product ranges over all possible cubic roots `a,b`.

```
clear;
Q := Rationals();
R := 2; S := 5; T := -3;
Qx<x> := PolynomialRing(Q);
Q<twist> := ext<Q | x^2 + 3>;
Qx<x> := PolynomialRing(Q);

D1 := T;
D2 := S;
D3 := S*T + 1;
D4 := R^3 - 3*R*T + T^2 + T;
D5 := R^3*S - 3*R*S*T + S*T^2 + S*T + T;
D8 := R^2 - T;
```

[9] Remark that we want the codomain curve to have small integer parameters, so in the code these are defined first, after which we use the dual isogeny to compute the more elaborate rational parameters of the domain curve.

```
D9 := R - 1;
D10 := R*S - S*T - 1;
D11 := S*T - S + 1;
DELTA := R^6*S^2 - 6*R^4*S^2*T - 3*R^4*S + 2*R^3*S^2*T^2 + 2*R^3*S^2*T
+ 3*R^3*S*T + R^3*S + R^3 + 9*R^2*S^2*T^2 + 6*R^2*S*T
- 6*R*S^2*T^3 - 6*R*S^2*T^2 - 9*R*S*T^2 - 3*R*S*T - 3*R*T + S^2*T^4
+ 2*S^2*T^3 + S^2*T^2 + 2*S*T^3 + 3*S*T^2 + T^2 + T;

r := -D2*D9*D8*(D5-R)/(D10^2*D4);
s := D10^3*D4^2/(D1*D2*D9^3*DELTA);
t := D2^2*D9^3*D8^3/(D10^3*D4^2);

d1 := t;
d2 := s;
d4 := r^3 - 3*r*t + t^2 + t;
d6 := r^3*s^2 - 3*r*s^2*t - 3*r*s + s^2*t^2 + s^2*t + 2*s*t + s + 1;
d7 := r^3*s^2*t + r^3*s - 3*r*s^2*t^2 - 3*r*s*t + s^2*t^3 + s^2*t^2 + 2*s*t^2 + t;

Q<a> := ext<Q | x^3 - d7>;
Q<b> := ext<Q | x^3 - d2*d4^2>;
Q<c> := ext<Q | x^3 - d1*d6^2>;

cofab1 := D1^2     *D4^4     *D10^8 /(D2^3*D8^6*D9^2*DELTA^2);
cofab2 := D1^2     *D4^4*D8  *D10^7      *D11 /(D2^2*D8^6*D9^2*DELTA^2);
cofab3 := D1       *D4^4*D8^2*D10^6 /(D2  *D8^6*D9^2*DELTA^2);
cofab4 := D1^2     *D4^2*     D10^5      *D11 /(D2^2*D8^4*D9  *DELTA);
cofab5 := D1       *D4^2*D8*  D10^4 /(D2  *D8^4*D9  *DELTA);
cofab6 := D1  *D3  *D4^2*D8^2*D10^3 /(     D8^4*D9  *DELTA);
cofab7 := D1^2                      *D10^2 /      D8^2;
cofab8 := D1                        *D10 /      D8;
cofab9 :=                                 D11;

cofab1 *:= -6*S*T-2;
cofab2 *:= -2;
cofab3 *:= 6*S*T+4;
cofab4 *:= 2;
cofab5 *:= -6*S*T-2;
cofab6 *:= -6;
cofab7 *:= 6;
cofab8 *:= 6*S*T+4;
cofab9 *:= 2*S*T+1;

b4ab := twist* ((cofab9 + cofab8*a + cofab7*a^2) + (cofab6 + cofab5*a + cofab4*a^2)*b
+ (cofab3 + cofab2*a + cofab1*a^2)*b^2);

cofbc1 := 1 /(D2  *D4^3);
cofbc2 := D1^2   *D9  *D10 /(D2  *D4^3     *D8);
cofbc3 := D1^3   *D9^2*D10^2 /(D2  *D4^3*D5  *D8^2);
cofbc4 := D1           *D10^3 /(D2^2*D4       *D8^2*D9  *DELTA);
cofbc5 := D1^2         *D10^4 /(D2^2*D4       *D8^3     *DELTA);
cofbc6 := D1^3   *D9   *D10^5 /(D2^2*D4  *D5  *D8^4     *DELTA);
cofbc7 := D1  *D4      *D10^6 /(D2^3           *D8^4*D9^2*DELTA^2);
cofbc8 := D1^2*D4      *D10^7 /(D2^3           *D8^5*D9  *DELTA^2);
cofbc9 := D1^4*D4      *D10^8 /(D2^3     *D5   *D8^6     *DELTA^2);

cofbc1 *:= R^9*S^2*T + R^9*S^2 - R^9*S - 6*R^8*S^2*T - 3*R^7*S^2*T^2 - 3*R^7*S^2*T
- 5*R^7*S*T + R^6*S^2*T^3 + 40*R^6*S^2*T^2 + R^6*S^2*T + 13*R^6*S*T^2 + 13*R^6*S*T
- 2*R^6*T - 21*R^5*S^2*T^3 - 21*R^5*S^2*T^2 + 3*R^5*S*T^2 + 6*R^4*S^2*T^4 - 54*R^4*S^2*T^3
+ 6*R^4*S^2*T^2 - 52*R^4*S*T^3 - 52*R^4*S*T^2 - 6*R^4*T^2 - R^3*S^2*T^5 + 64*R^3*S^2*T^4
+ 64*R^3*S^2*T^3 - R^3*S^2*T^2 + 11*R^3*S*T^4 + 103*R^3*S*T^3 + 11*R^3*S*T^2 + 14*R^3*T^3
+ 14*R^3*T^2 - 33*R^2*S^2*T^5 - 48*R^2*S^2*T^4 - 33*R^2*S^2*T^3 - 15*R^2*S*T^4 - 15*R^2*S*T^3
- 18*R^2*T^3 + 9*R*S^2*T^6 + 15*R*S^2*T^5 + 15*R*S^2*T^4 + 9*R*S^2*T^3 + 7*R*S*T^5
- 40*R*S*T^4 + 7*R*S*T^3 - 6*R*T^4 - 6*R*T^3 - S^2*T^7 - 2*S^2*T^6 - 2*S^2*T^5
- 2*S^2*T^4 - S^2*T^3 - 3*S*T^6 + 9*S*T^5 + 9*S*T^4 - 3*S*T^3 - 2*T^5 + 14*T^4 - 2*T^3;
cofbc2 *:= -2*R^7*S + 8*R^6*S - 6*R^5*S + 6*R^5 + 2*R^4*S*T^2 - 22*R^4*S*T - 12*R^4*T
+ 22*R^3*S*T^2 + 28*R^3*S*T + 6*R^3*T - 18*R^2*S*T^3 - 24*R^2*S*T^2 - 6*R^2*S*T
+ 6*R^2*T^2 - 12*R^2*T + 4*R*S*T^4 + 20*R*S*T^3 - 2*R*S*T^2 + 6*R*T^3 + 6*R*T^2 -
4*S*T^4 - 2*S*T^3 + 2*S*T^2 - 12*T^3 + 6*T^2;
```

```
cofbc3 *:= 2*R^8*S - 6*R^7*S + 4*R^6*S*T - 8*R^5*S*T^2 + 16*R^5*S*T + 6*R^5*T
- 30*R^4*S*T^2 - 12*R^4*T + 44*R^3*S*T^3 + 14*R^3*S*T^2 + 6*R^3*T^2 - 10*R^2*S*T^4
- 32*R^2*S*T^3 - 22*R^2*S*T^2 - 12*R^2*T^3 + 6*R^2*T^2 - 6*R*S*T^4 + 36*R*S*T^3
+ 6*R*S*T^2 + 6*R*T^3 + 6*R*T^2 + 4*S*T^5 - 4*S*T^4 - 8*S*T^3 + 6*T^4 - 12*T^3;
cofbc4 *:= 2*R^9*S^2 - 2*R^8*S^2*T - 4*R^8*S^2 + 4*R^8*S - 8*R^7*S^2*T + 2*R^7*S^2
- 10*R^7*S + 16*R^6*S^2*T^2 + 26*R^6*S^2*T - 4*R^5*S^2*T^3 - 18*R^5*S^2*T^2 - 20*R^5*S^2*T
- 10*R^5*S*T^2 + 32*R^5*S*T + 6*R^5*T - 22*R^4*S^2*T^3 - 24*R^4*S^2*T^2 + 4*R^4*S^2*T
- 38*R^4*S*T^2 - 2*R^4*S*T - 12*R^4*T + 14*R^3*S^2*T^4 + 72*R^3*S^2*T^3 + 40*R^3*S^2*T^2
+ 60*R^3*S*T^3 + 6*R^3*S*T^2 + 6*R^3*T^2 - 2*R^2*S^2*T^5 - 32*R^2*S^2*T^4 - 64*R^2*S^2*T^3
- 16*R^2*S^2*T^2 - 14*R^2*S*T^4 - 40*R^2*S*T^3 - 26*R^2*S*T^2 - 12*R^2*T^3 + 6*R^2*T^2
+ 4*R*S^2*T^5 + 22*R*S^2*T^4 + 20*R*S^2*T^3 + 2*R*S^2*T^2 - 10*R*S*T^4 + 52*R*S*T^3
+ 8*R*S*T^2 + 6*R*T^3 + 6*R*T^2 - 2*S^2*T^5 - 4*S^2*T^4 - 2*S^2*T^3 + 6*S*T^5
- 6*S*T^4 - 12*S*T^3 + 6*T^4 - 12*T^3;
cofbc5 *:= -2*R^7*S + 4*R^6*S*T + 4*R^6*S - 2*R^6 - 6*R^5*S*T - 10*R^4*S*T^2 - 10*R^4*S*T
- 6*R^4*T + 2*R^3*S*T^3 + 46*R^3*S*T^2 + 2*R^3*S*T + 14*R^3*T^2 + 14*R^3*T - 24*R^2*S*T^3
- 24*R^2*S*T^2 - 18*R^2*T^2 + 10*R*S*T^4 + 2*R*S*T^3 + 10*R*S*T^2 - 6*R*T^3 - 6*R*T^2
- 2*S*T^5 - 2*S*T^2 - 2*T^4 + 14*T^3 - 2*T^2;
cofbc6 *:= 2*R^8*S - 6*R^7*S*T + 4*R^6*S*T + 16*R^5*S*T^2 - 8*R^5*S*T + 6*R^5*T
- 30*R^4*S*T^2 - 12*R^4*T^2 + 14*R^3*S*T^3 + 44*R^3*S*T^2 + 6*R^3*T^2 - 22*R^2*S*T^4
- 32*R^2*S*T^3 - 10*R^2*S*T^2 + 6*R^2*T^3 - 12*R^2*T^2 + 6*R*S*T^5 + 36*R*S*T^4
- 6*R*S*T^3 + 6*R*T^4 + 6*R*T^3 - 8*S*T^5 - 4*S*T^4 + 4*S*T^3 - 12*T^4 + 6*T^3;
cofbc7 *:= 2*R^9*S^2 - 4*R^8*S^2*T - 2*R^8*S^2 + 4*R^8*S + 2*R^7*S^2*T^2 - 8*R^7*S^2*T
- 10*R^7*S*T + 26*R^6*S^2*T^2 + 16*R^6*S^2*T - 20*R^5*S^2*T^3 - 18*R^5*S^2*T^2 - 4*R^5*S^2*T
+ 32*R^5*S*T^2 - 10*R^5*S*T + 6*R^5*T + 4*R^4*S^2*T^4 - 24*R^4*S^2*T^3 - 22*R^4*S^2*T^2
- 2*R^4*S*T^3 - 38*R^4*S*T^2 - 12*R^4*T^2 + 40*R^3*S^2*T^4 + 72*R^3*S^2*T^3 + 14*R^3*S^2*T^2
+ 6*R^3*S*T^3 + 60*R^3*S*T^2 + 6*R^3*T^2 - 16*R^2*S^2*T^5 - 64*R^2*S^2*T^4 - 32*R^2*S^2*T^3
- 2*R^2*S^2*T^2 - 26*R^2*S*T^4 - 40*R^2*S*T^3 - 14*R^2*S*T^2 + 6*R^2*T^3 - 12*R^2*T^2
+ 2*R*S^2*T^6 + 20*R*S^2*T^5 + 22*R*S^2*T^4 + 4*R*S^2*T^3 + 8*R*S*T^5 + 52*R*S*T^4
- 10*R*S*T^3 + 6*R*T^4 + 6*R*T^3 - 2*S^2*T^6 - 4*S^2*T^5 - 2*S^2*T^4 - 12*S*T^5
- 6*S*T^4 + 6*S*T^3 - 12*T^4 + 6*T^3;
cofbc8 *:= -2*R^7*S + 8*R^6*S*T - 6*R^5*S*T^2 + 6*R^5*T - 22*R^4*S*T^2 + 2*R^4*S*T
- 12*R^4*T + 28*R^3*S*T^3 + 22*R^3*S*T^2 + 6*R^3*T^2 - 6*R^2*S*T^4 - 24*R^2*S*T^3
- 18*R^2*S*T^2 - 12*R^2*T^3 + 6*R^2*T^2 - 2*R*S*T^4 + 20*R*S*T^3 + 4*R*S*T^2 + 6*R*T^3
+ 6*R*T^2 + 2*S*T^5 - 2*S*T^4 - 4*S*T^3 + 6*T^4 - 12*T^3;
cofbc9 *:= -8*R^7*S + 10*R^6*S*T + 10*R^6*S - 2*R^6 + 12*R^5*S*T - 40*R^4*S*T^2 - 40*R^4*S*T
- 6*R^4*T + 8*R^3*S*T^3 + 64*R^3*S*T^2 + 8*R^3*S*T + 14*R^3*T^2 + 14*R^3*T - 6*R^2*S*T^3
- 6*R^2*S*T^2 - 18*R^2*T^2 + 4*R*S*T^4 - 28*R*S*T^3 + 4*R*S*T^2 - 6*R*T^3 - 6*R*T^2
- 2*S*T^5 + 6*S*T^4 + 6*S*T^3 - 2*S*T^2 - 2*T^4 + 14*T^3 - 2*T^2;

b4bc := twist* ((cofbc1 + cofbc2*c + cofbc3*c^2) + (cofbc4 + cofbc5*c + cofbc6*c^2)*b
+ (cofbc7 + cofbc8*c + cofbc9*c^2)*b^2);

Qbi<b1,b2,b3,b5,b6,b7> := PolynomialRing(Q,6);
Qx<x> := PolynomialRing(Qbi);

H1 := x^2 + R*x + T;
lambda1 := 4*S;
G1 := (S - S*T - 1)*x^3 + 3*S*(R - T)*x^2 + 3*S*R*(R - T)*x - S*T^2 + S*R^3 + T;
F := G1^2 + lambda1*H1^3;

bis := [];
for b4 in [b4ab,b4bc] do
  Fbi := (b4*x^3 + b3*x^2 + b2*x + b1)^2 + b7*(x^2 + b6*x + b5)^3;
  I := {Eltseq(F)[i] - Eltseq(Fbi)[i] : i in [1..7]};
  GB := GroebnerBasis(I);
  roots := [Roots(UnivariatePolynomial(GB[i]))[1][1] : i in [1..6]];
  bi := roots[1..3] cat [b4] cat roots[4..6];
  Append(~bis, bi);
end for;

C := HyperellipticCurve(F);
J := Jacobian(C);

for bi in bis do
  T := J ! [Qx ! (bi[5..6] cat [1]), Qx ! bi[1..4]];
  assert 3*T eq J ! 0;
end for;
```