Isogenies and the Discrete Logarithm Problem on Jacobians of Genus 3 Hyperelliptic Curves

Benjamin Smith

Mathematics Department, Royal Holloway University of London
Egham, Surrey TW20 0EX, UK. Ben.Smith@rhul.ac.uk

Abstract. We describe the use of explicit isogenies to reduce Discrete Logarithm Problems (DLPs) on Jacobians of hyperelliptic genus 3 curves to Jacobians of non-hyperelliptic genus 3 curves, which are vulnerable to faster index calculus attacks. We provide algorithms which compute an isogeny with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ for any hyperelliptic genus 3 curve. These algorithms provide a rational isogeny for a positive fraction of all hyperelliptic genus 3 curves defined over a finite field of characteristic $p > 3$. Subject to reasonable assumptions, our algorithms provide an explicit and efficient reduction from hyperelliptic DLPs to non-hyperelliptic DLPs for around 18.57% of all hyperelliptic genus 3 curves over a given finite field.

1 Introduction

After the great success of elliptic curves in cryptography, researchers have naturally been drawn to their higher-dimensional generalizations: Jacobians of higher-genus curves. Curves of genus 1 (elliptic curves), 2, and 3 are widely believed to offer the best balance of security and efficiency. This article is concerned with the security of curves of genus 3.

There are two classes of curves of genus 3: hyperelliptic and non-hyperelliptic. Each class has a distinct geometry: the canonical morphism of a hyperelliptic curve is a double cover of a curve of genus 0, while the canonical morphism of a non-hyperelliptic curve of genus 3 is an isomorphism to a smooth plane quartic curve. A hyperelliptic curve cannot be isomorphic to a non-hyperelliptic curve. From a cryptological point of view, the Discrete Logarithm Problem (DLP) in Jacobians of hyperelliptic curves of genus 3 over $\mathbb{F}_q$ may be solved in $\widetilde{O}(q^{4/3})$ group operations, using the index calculus algorithm of Gaudry, Thomé, Thériault, and Diem [6]. Jacobians of non-hyperelliptic curves of genus 3 over $\mathbb{F}_q$ are amenable to Diem's index calculus algorithm [3], which requires only $\widetilde{O}(q)$ group operations to solve the DLP (for comparison, Pollard/baby-step-giant-step methods require $\widetilde{O}(q^{3/2})$ group operations to solve the DLP in Jacobians of genus 3 curves over $\mathbb{F}_q$). The security of non-hyperelliptic genus 3 curves is therefore widely held to be lower than that of their hyperelliptic cousins.

Our aim is to provide a means of efficiently translating DLPs from Jacobians of hyperelliptic genus 3 curves to Jacobians of non-hyperelliptic curves, where faster index calculus is available. We do this by constructing an explicit *isogeny* of Jacobians: a surjective homomorphism, with finite kernel, from the hyperelliptic Jacobian to a non-hyperelliptic Jacobian. The kernel of our isogeny will intersect trivially with any subgroup of cryptographic interest, and so the isogeny will restrict to an isomorphism of DLP subgroups.

Specifically, let H be a hyperelliptic curve of genus 3 over a finite field of characteristic $p > 3$. Suppose the Jacobian J_H of H contains a subgroup S isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, generated by differences of Weierstrass points. If the 2-Weil pairing restricts trivially to S, then there exists an isogeny with kernel S from J_H to a principally polarized abelian variety A. Using Recillas' trigonal construction [12], A may be realized as the Jacobian of a genus 3 curve X. This construction appears to be due to Donagi and Livné [5]; our contribution, aside from the cryptological application, is to provide explicit formulae and algorithms to compute the curve X and the isogeny. Naïve moduli space dimension arguments suggest that there is an overwhelming probability that X will be non-hyperelliptic, and thus explicitly isomorphic to a plane quartic curve C. We therefore obtain an explicit isogeny $\phi : J_H \to J_C$ with kernel S. If ϕ is defined over $\mathbb{F}_q$, then it maps $J_H(\mathbb{F}_q)$ into $J_C(\mathbb{F}_q)$, where Diem's $\widetilde{O}(q)$ index calculus is available. Given points P and $Q = [n]P$ of odd order in $J_H(\mathbb{F}_q)$, we can solve the DLP (recovering n from P and Q) in $J_C(\mathbb{F}_q)$, using

$$Q = [n]P \implies \phi(Q) = [n]\phi(P).$$

There are several caveats to our approach, besides the requirement of a subgroup S as described above. First, it does not apply in characteristic 2 or 3. In the case of characteristic 2, the subgroup S is the kernel of a verschiebung, so X is necessarily hyperelliptic. In characteristic 3, we cannot use the trigonal construction. Second, in order to obtain an advantage with index calculus on X over H, the isogeny must be defined over $\mathbb{F}_q$ and X must be non-hyperelliptic. We show in §8 that, subject to some reasonable assumptions, given a hyperelliptic curve H of genus 3 over a sufficiently large finite field, our algorithms succeed in giving an explicit, rational isogeny from J_H to a non-hyperelliptic Jacobian with probability ≈ 0.1857. In particular, the DLP can be solved in $\widetilde{O}(q)$ group operations for around 18.57% of all Jacobians of hyperelliptic curves of genus 3 over a finite field of characteristic $p > 3$.

Our results have a number of interesting implications for curve-based cryptography. First, the difficulty of the DLP in a subgroup G of J_H depends not only on the size of the subgroup G, but upon the existence of other rational subgroups of J_H that can be used to form quotients. Second, the security of a given hyperelliptic genus 3 curve depends upon the factorization of its hyperelliptic polynomial. Neither of these results have any parallel in lower-genus curve cryptography.

After reviewing some standard definitions for hyperelliptic curves in §2, we define the kernels of our isogenies in §3. In §4, §5 and §6, we describe and derive explicit formulae for the trigonal construction, which is our main tool for constructing isogenies. After giving an example in §7, we compute (heuristically) the expectation that the methods of this article will compute a rational isogeny for a randomly chosen curve in §8. Finally, in §9 we briefly describe some of the problems involved in generalizing these methods.

A Note on the Base Field

We will work over $\mathbb{F}_q$ throughout this article, where q is a power of a prime $p > 3$. We let $\mathcal{G}$ denote the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, which is (topologically) generated by the q^{th} power Frobenius map. Some of the theory of this article carries over to fields of characteristic zero: in particular, the contents of §5 and §6 are valid over any field of characteristic not 2 or 3.

Acknowledgements

This work was supported by the EPSRC and ECRYPT. The author gratefully acknowledges Roger Oyono and Christophe Ritzenthaler for discussions which directly inspired this research, and also thanks Steven Galbraith for his advice.

2 Notation and Conventions for Hyperelliptic Curves

We assume that we are given a hyperelliptic curve H of genus 3 over $\mathbb{F}_q$, and that the Jacobian J_H of H is absolutely simple. We will use both an affine model

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

and a weighted projective plane model

$$H : w^2 = \widetilde{F}(u, v)$$

for H (where u, v, and w have weights 1, 1, and 4, respectively). The coordinates of these models are related by $x = u/v$ and $y = w/v^4$. The polynomial $\widetilde{F}$ is squarefree of total degree 8, with $\widetilde{F}(u, v) = v^8 F(u/v)$ and $\widetilde{F}(x, 1) = F(x)$. We emphasize that F need not be monic. By a *randomly chosen hyperelliptic curve*, we mean the hyperelliptic curve defined by $w^2 = \widetilde{F}(u, v)$ where $\widetilde{F}$ is a randomly chosen squarefree homogenous bivariate polynomials of degree 8 over $\mathbb{F}_q$. The canonical *hyperelliptic involution* ι of H is defined by $(x, y) \mapsto (x, -y)$ in the affine model, $(u : v : w) \mapsto (u : v : -w)$ in the projective model, and induces the negation map $[-1]$ on J_H. The quotient $\pi : H \to \mathbb{P}^1 \cong H/\langle\iota\rangle$ sends $(u : v : w)$ to $(u : v)$ in the projective model, and (x, y) to x in the affine model (where it maps onto the affine patch of $\mathbb{P}^1$ where $v \neq 0$).

To compute in J_H, we fix an isomorphism from J_H to the group of degree-zero divisor classes on H, denoted $\mathrm{Pic}^0(H)$. Recall that divisors are formal sums of points on H, and if $D = \sum_{P \in H} n_P(P)$ is a divisor, then $\sum_{P \in H} n_P$ is the *degree* of D. We say D *principal* if $D = \mathrm{div}(f) := \sum_{P \in H} \mathrm{ord}_P(f)(P)$ for some function f on H, where $\mathrm{ord}_P(f)$ denotes the number of zeroes (or the negative of the number of poles) of f at P. Since H is complete, every principal divisor has degree 0. The group $\mathrm{Pic}^0(H)$ is defined to be the group of divisors of degree 0 modulo principal divisors. The equivalence class of a divisor D is denoted by $[D]$.

3 The Kernel of the Isogeny

The eight points of $H(\overline{k})$ where $w = 0$ are called the *Weierstrass points* of H. Each Weierstrass point W corresponds to a linear factor $L_W = v(W)u - u(W)v$ of $\widetilde{F}$. If W_1 and W_2 are Weierstrass points, then $2(W_1)-2(W_2) = \operatorname{div}(L_{W_1}/L_{W_2})$, so $2[(W_1)-(W_2)] = 0$; hence $[(W_1)-(W_2)]$ corresponds to an element of $J_H[2]$. In particular, $[(W_1)-(W_2)] = [(W_2)-(W_1)]$, so the divisor class $[(W_1)-(W_2)]$ corresponds to the pair $\{W_1, W_2\}$ of Weierstrass points, and hence to the quadratic factor $L_{W_1}L_{W_2}$ of $\widetilde{F}$.

Proposition 1. *Every partition of the eight Weierstrass points of H into four disjoint pairs corresponds to a subgroup of $J_H[2]$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. The subgroup is $\mathbb{F}_q$-rational if the partition is stabilized by the Frobenius map.*

Proof. Let $\{\{W_1', W_1''\}, \{W_2', W_2''\}, \{W_3', W_3''\}, \{W_4', W_4''\}\}$ be a partition of the Weierstrass points of H into four disjoint pairs. Each pair $\{W_i', W_i''\}$ corresponds to the two-torsion divisor class $[(W_i') - (W_i'')]$ in $J_H[2]$. Further,

$$\sum_{i=1}^{4}[(W_i') - (W_i'')] = \Big[\operatorname{div}\big(w/\prod_{i=1}^{4} L_{W_i''}\big)\Big] = 0.$$

This is the only relation on the classes $[(W_i') - (W_i'')]$, so

$$\langle[(W_i') - (W_i'')] : 1 \le i \le 4\rangle \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

The action of $\mathcal{G}$ on $J_H[2]$ corresponds to its action on the Weierstrass points, proving the second claim. We emphasize that neither the individual Weierstrass points nor the pairs in the partition need be $\mathbb{F}_q$-rational for the corresponding subgroup to be $\mathbb{F}_q$-rational. □

Definition 1. *We call the subgroups corresponding to partitions of the Weierstrass points of H as in Proposition 1* tractable subgroups*. We let $\mathcal{S}(H)$ denote the set of all $\mathbb{F}_q$-rational tractable subgroups of $J_H[2]$.*

Remark 1. Requiring the pairs to be disjoint ensures that the corresponding subgroup is 2-Weil isotropic. This is necessary for the quotient by the subgroup to be an isogeny of principally polarized abelian varieties (see §9).

Remark 2. Not every subgroup of $J_H[2]$ that is the kernel of an isogeny of Jacobians is a tractable subgroup. For example, if $W_1, \ldots, W_8$ are the Weierstrass points of H, then the subgroup

$$\big\langle[(W_1) - (W_i) + (W_j) - (W_k)] : (i, j, k) \in \{(2, 3, 4), (2, 5, 6), (3, 5, 7)\}\big\rangle$$

is maximally 2-Weil isotropic, and hence is the kernel of an isogeny of Jacobians. However, this subgroup contains no nontrivial differences of Weierstrass points, and so cannot be tractable.

Computing $\mathcal{S}(H)$ is straightforward if we identify each tractable subgroup with the corresponding partition of Weierstrass points. Each pair $\{W_i', W_i''\}$ of Weierstrass points corresponds to a quadratic factor of $\widetilde{F}$. Since the pairs are disjoint, the corresponding quadratic factors are pairwise coprime, and hence form (up scalar multiples) a factorization of the hyperelliptic polynomial $\widetilde{F}$. We therefore have a correspondence of tractable subgroups, partitions of Weierstrass points into pairs, and sets of quadratic polynomials (up to scalar multiples):

$$S \longleftrightarrow \big\{\{W_i', W_i''\} : 1 \leq i \leq 4\big\} \longleftrightarrow \big\{F_i : 1 \leq i \leq 4,\ \widetilde{F} = F_1F_2F_3F_4\big\}.$$

Since the action of $\mathcal{G}$ on $J_H[2]$ corresponds to its action on the set of Weierstrass points, the action of $\mathcal{G}$ on a tractable subgroup S corresponds to its action on the corresponding set $\{F_1, F_2, F_3, F_4\}$. In particular, S is $\mathbb{F}_q$-rational precisely when $\{F_1, F_2, F_3, F_4\}$ is fixed by $\mathcal{G}$. The factors F_i are themselves defined over $\mathbb{F}_q$ precisely when the corresponding points of S are $\mathbb{F}_q$-rational.

We can use this information to compute $\mathcal{S}(H)$. The $\mathcal{G}$-action on pairs of Weierstrass points contains an orbit $\big(\{W_{i_1}', W_{i_1}''\}, \ldots, \{W_{i_n}', W_{i_n}''\}\big)$ if and only if (possibly after exchanging some of the W_{i_k}' with the W_{i_k}'') either $(W_{i_1}', \ldots, W_{i_n}')$ and $(W_{i_1}'', \ldots, W_{i_n}'')$ are both $\mathcal{G}$-orbits or $(W_{i_1}', \ldots, W_{i_n}', W_{i_1}'', \ldots, W_{i_n}'')$ is a $\mathcal{G}$-orbit. Every $\mathcal{G}$-orbit of Weierstrass points corresponds to an $\mathbb{F}_q$-irreducible factor of F. Elementary calculations therefore yield the following useful lemma, as well as algorithms to compute all of the $\mathbb{F}_q$-rational tractable subgroups of $J_H[2]$.

Lemma 1. *Let $H : w^2 = \widetilde{F}(u, v)$ be a hyperelliptic curve of genus 3 over $\mathbb{F}_q$. The cardinality of the set $\mathcal{S}(H)$ depends only on the degrees of the $\mathbb{F}_q$-irreducible factors of $\widetilde{F}$, and is described by the following table:*

Degrees of $\mathbb{F}_q$-irreducible factors of $\widetilde{F}$	$\#\mathcal{S}(H)$
$(8), (6, 2), (6, 1, 1), (4, 2, 1, 1)$	1
$(4, 4)$	5
$(4, 2, 2), (4, 1, 1, 1, 1), (3, 3, 2), (3, 3, 1, 1)$	3
$(2, 2, 2, 1, 1)$	7
$(2, 2, 1, 1, 1, 1)$	9
$(2, 1, 1, 1, 1, 1, 1)$	15
$(2, 2, 2, 2)$	25
$(1, 1, 1, 1, 1, 1, 1, 1)$	105
Other	0

4 The Trigonal Construction

Assume we are given an $\mathbb{F}_q$-rational tractable subgroup S of $J_H[2]$. We will now construct a curve X of genus 3 and an isogeny $\phi : J_H \to J_X$ with kernel S.

Definition 2. *Suppose $S = \langle [(W_i') - (W_i'')] : 1 \leq i \leq 4 \rangle$ is a tractable subgroup. We say that a morphism $g : \mathbb{P}^1 \to \mathbb{P}^1$ is a* trigonal map for S *if g has degree 3 and $g(W_i') = g(W_i'')$ for $1 \leq i \leq 4$.*

Given a trigonal map g, Recillas' trigonal construction [12] specifies a curve X of genus 3 and a map $f : X \to \mathbb{P}^1$ of degree 4. The isomorphism class of X is independent of the choice of g. Theorem 1, due to Donagi and Livné, states that if g is a trigonal map for S, then S is the kernel of an isogeny from J_H to J_X.

Theorem 1 (Donagi and Livné [5, §5]). *Let S be a tractable subgroup of $J_H[2]$, and suppose $g : \mathbb{P}^1 \to \mathbb{P}^1$ is a trigonal map for S. If X is the curve formed from g with Recillas' trigonal construction, then there is an isogeny $\phi : J_H \to J_X$ with kernel S.*

We will give only a brief description of the geometry of X here, concentrating instead on its explicit construction; we refer the reader to Recillas [12], Donagi [4, §2], Birkenhake and Lange [1, §12.7], and Vakil [15] for the geometrical theory (and proofs). The isogeny is analogous to the well-known Richelot isogeny in genus 2 (see Bost and Mestre [2] and Donagi and Livné [5]).

In scheme-theoretic terms, if U is the subset of the codomain of g above which $g \circ \pi$ is unramified, then X is by definition the closure of the curve over U representing the sheaf of sections of $\pi : (g \circ \pi)^{-1}(U) \to g^{-1}(U)$. This means that the points of X over a point P of U represent partitions of the six points of $(g \circ \pi)^{-1}(P)$ into two sets of three exchanged by the hyperelliptic involution. The fibre product of H and X over $\mathbb{P}^1$ (with respect to $g \circ \pi$ and f) is the union of two isomorphic curves, R and R', which are exchanged by the involution on $H \times_{\mathbb{P}^1} X$ induced by the hyperelliptic involution. The natural projections induce coverings $\pi_H : R \to H$ and $\pi_X : R \to X$ of degrees 2 and 3, respectively, so R is a $(3, 2)$-correspondence between H and X. The map $(\pi_X)_* \circ (\pi_H)^*$ on divisor classes — that is, pulling back from H to R, then pushing forward onto X — induces an isogeny $\phi : J_H \to J_X$, with kernel S.[1] If we replace R with R' in the above, we obtain an isogeny isomorphic to $-\phi$. Thus, up to sign, the construction of the isogeny depends only on the subgroup S. The curves and morphisms described above form the commutative diagrams shown in Fig. 1.

The hyperelliptic Jacobians form a codimension-1 subspace of the moduli space of 3-dimensional principally polarized abelian varieties. Naïvely, then, if X is a curve of genus 3 selected at random, then the probability that X is hyperelliptic is inversely proportional to q; for cryptographically relevant sizes of q, this probability should be negligible. This is consistent with our experimental observations.

Hypothesis 1. *The probability that the curve X constructed by the trigonal construction for a randomly chosen H and S in $\mathcal{S}(H)$ is hyperelliptic is negligible.*

5 Computing Trigonal Maps

Suppose we are given a tractable subgroup S of $J_H[2]$, corresponding to a partition $\{\{W_i', W_i''\} : 1 \leq i \leq 4\}$ of the Weierstrass points of H into pairs. In this

[1] Recall that $(\pi_H)^*(\sum_{P \in H} n_P(P)) = \sum_{P \in H} n_P \sum_{Q \in \pi_H^{-1}(P)}(Q)$, with appropriate multiplicities where π_X ramifies, and $(\pi_X)_*(\sum_{Q \in R} m_Q(Q)) = \sum_{Q \in R} n_Q(\pi_X(Q))$.

Fig. 1. The curves, Jacobians, and morphisms of §4

$$\begin{tikzcd}
& R \arrow[dl, "\pi_H"', "2"] \arrow[dr, "\pi_X", "3"'] & \\
H \arrow[d, "\pi"', "2"] & & X \arrow[ddl, "f"', "4"] \\
\mathbb{P}^1 \arrow[dr, "g", "3"'] & & \\
& \mathbb{P}^1 &
\end{tikzcd}$$

$$\begin{tikzcd}
& J_R \arrow[dr, "(\pi_X)_*"] & \\
J_H \arrow[ur, "\pi_H^*"] \arrow[rr, "\phi"'] & & J_X
\end{tikzcd}$$

section, we compute polynomials $N(x) = x^3 + ax + b$ and $D(x) = x^2 + cx + d$ such that the rational map $g : x \mapsto t = N(x)/D(x)$ defines a trigonal map for S. Choosing N and D to have degrees 3 and 2 respectively ensures that g maps the point at infinity to the point at infinity; this will be useful to us in §6.

By definition, $g : \mathbb{P}^1 \to \mathbb{P}^1$ is a degree-3 map with $g(\pi(W_i')) = g(\pi(W_i''))$ for $1 \leq i \leq 4$. We will express g as a composition of maps $g = p \circ e$, where $e : \mathbb{P}^1 \to \mathbb{P}^3$ is the rational normal embedding defined by

$$e : (u : v) \longmapsto (u_0 : u_1 : u_2 : u_3) = (u^3 : u^2v : uv^2 : v^3),$$

and $p : \mathbb{P}^3 \to \mathbb{P}^1$ is the projection defined as follows. For each $1 \leq i \leq 4$, we let L_i denote the line in $\mathbb{P}^3$ passing through $e(\pi(W_i'))$ and $e(\pi(W_i''))$. There exists at least one line L intersecting all four of the L_i (generically, there are two). We take p to be the projection away from L; then $p(e(\pi(W_i'))) = p(e(\pi(W_i'')))$ for $1 \leq i \leq 4$, so $g = p \circ e$ is a trigonal map for S. Given equations for L, we can use linear algebra to compute a, b, c, and d in $\mathbb{F}_q$ such that

$$L = V(u_0 + au_2 + bu_3, u_1 + cu_2 + du_3)\,.$$

The projection $p : \mathbb{P}^3 \to \mathbb{P}^1$ away from L is then defined by

$$p : (u_0 : u_1 : u_2 : u_3) \longmapsto (u_0 + au_2 + bu_3 : u_1 + cu_2 + du_3),$$

and therefore $g = p \circ e$ is defined by

$$g : (u : v) \longmapsto (u^3 + auv^2 + bv^3 : u^2v + cuv^2 + dv^3).$$

Therefore, if we set $N(x) = x^3 + ax + b$ and $D(x) = x^2 + cx + d$, then g will be defined by the rational map $x \longmapsto N(x)/D(x)$.

To compute equations for L, we will use the classical theory of *Grassmannian varieties*. The set of lines in $\mathbb{P}^3$ has the structure of an algebraic variety $\mathrm{Gr}(1, 3)$, called the Grassmannian. There is a convenient model for $\mathrm{Gr}(1,3)$ as a quadric hypersurface in $\mathbb{P}^5$: if $v_0,\ldots,v_5$ are coordinates on $\mathbb{P}^5$, then we may take

$$\mathrm{Gr}(1,3) := V(v_0v_3 + v_1v_4 + v_2v_5)\,.$$

Lemma 2. *There is a bijection between points of* $\mathrm{Gr}(1,3)$ *and lines in* $\mathbb{P}^3$*, defined as follows.*

1. *The point on* $\mathrm{Gr}(1,3)$ *corresponding to the line through* $(p_0 : p_1 : p_2 : p_3)$ *and* $(q_0 : q_1 : q_2 : q_3)$ *in* $\mathbb{P}^3$ *has coordinates*

$$\left(\begin{vmatrix} p_0 & p_1 \\ q_0 & q_1 \end{vmatrix} : \begin{vmatrix} p_0 & p_2 \\ q_0 & q_2 \end{vmatrix} : \begin{vmatrix} p_0 & p_3 \\ q_0 & q_3 \end{vmatrix} : \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix} : \begin{vmatrix} p_3 & p_1 \\ q_3 & q_1 \end{vmatrix} : \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}\right).$$

2. *The line in* $\mathbb{P}^3$ *corresponding to a point* $(\gamma_0 : \cdots : \gamma_5)$ *of* $\mathrm{Gr}(1,3)$ *is defined by*

$$V\begin{pmatrix} 0u_0 - \gamma_3u_1 - \gamma_4u_2 - \gamma_5u_3, \\ \gamma_3u_0 + \ 0u_1 - \gamma_2u_2 + \gamma_1u_3, \\ \gamma_4u_0 + \gamma_2u_1 + \ 0u_2 - \gamma_0u_3, \\ \gamma_5u_0 - \gamma_1u_1 + \gamma_0u_2 + \ \ 0u_3 \end{pmatrix}$$

(two of the equations will be redundant linear combinations of the others).

Further, if $(\gamma_0 : \cdots : \gamma_5)$ *is a point on* $\mathrm{Gr}(1,3)$ *corresponding to a line* L*, then the points of* $\mathrm{Gr}(1,3)$ *corresponding to lines meeting* L *are precisely those in the hyperplane defined by* $\sum_{i=0}^{5}\gamma_i v_{i+3}$*, where the subscripts are taken modulo* 6*.*

Assume that S is represented by a set $\{F_i = a_iu^2 + b_iuv + c_iv^2 : 1 \le i \le 4\}$ of quadratics, with each F_i corresponding to the pair $\{W_i', W_i''\}$ of Weierstrass points. With this notation, elementary calculations show that the point on $\mathrm{Gr}(1,3)$ corresponding to the line L_i through $e(W_i')$ and $e(W_i'')$ has coordinates

$$(c_i^2 : -c_ib_i : b_i^2 - a_ic_i : a_i^2 : a_ib_i : a_ic_i).$$

If $(\gamma_0 : \cdots : \gamma_5)$ is a point on $\mathrm{Gr}(1,3)$ corresponding to a candidate for L, then by the second part of Lemma 2 we have $M(\gamma_0,\ldots,\gamma_5)^T = 0$, where

$$M = \begin{pmatrix} a_1^2 & a_1b_1 & a_1c_1 & c_1^2 & -c_1b_1 & (b_1^2 - a_1c_1) \\ a_2^2 & a_2b_2 & a_2c_2 & c_2^2 & -c_2b_2 & (b_2^2 - a_2c_2) \\ a_3^2 & a_3b_3 & a_3c_3 & c_3^2 & -c_3b_3 & (b_3^2 - a_3c_3) \\ a_4^2 & a_4b_4 & a_4c_4 & c_4^2 & -c_4b_4 & (b_4^2 - a_4c_4) \end{pmatrix}. \tag{1}$$

The kernel of M is two-dimensional, corresponding to a line in $\mathbb{P}^5$. Let $\{\underline{\alpha}, \underline{\beta}\}$ be a basis for $\ker M$, writing $\underline{\alpha} = (\alpha_0,\ldots,\alpha_5)$ and $\underline{\beta} = (\beta_0,\ldots,\beta_5)$. If S is $\mathbb{F}_q$-rational, then so is $\ker M$, so we may take the α_i and β_i to be in $\mathbb{F}_q$. We want to find a point $P_L = (\alpha_0 + \lambda\beta_0 : \cdots : \alpha_5 + \lambda\beta_5)$ where the line in $\mathbb{P}^5$ corresponding to $\ker M$ intersects with $\mathrm{Gr}(1,3)$. The points $(u_0 : \ldots : u_3)$ on the line L in $\mathbb{P}^3$ corresponding to P_L satisfy $(M_{\underline{\alpha}} + \lambda M_{\underline{\beta}})(u_0,\ldots,u_3)^T = 0$, where

$$M_{\underline{\alpha}} := \begin{pmatrix} 0 & -\alpha_3 & -\alpha_4 & -\alpha_5 \\ \alpha_3 & 0 & -\alpha_2 & \alpha_1 \\ \alpha_4 & \alpha_2 & 0 & -\alpha_0 \\ \alpha_5 & -\alpha_1 & \alpha_0 & 0 \end{pmatrix} \quad\text{and}\quad M_{\underline{\beta}} := \begin{pmatrix} 0 & -\beta_3 & -\beta_4 & -\beta_5 \\ \beta_3 & 0 & -\beta_2 & \beta_1 \\ \beta_4 & \beta_2 & 0 & -\beta_0 \\ \beta_5 & -\beta_1 & \beta_0 & 0 \end{pmatrix}.$$

By part (2) of Lemma 2, the rank of $M_{\underline{\alpha}} + \lambda M_{\underline{\beta}}$ is 2. Using the expression

$$\det(M_{\underline{\alpha}} + \lambda M_{\underline{\beta}}) = \Big(\frac{1}{2}\big(\sum_{i=0}^{6} \beta_i\beta_{i+3}\big)\lambda^2 + \big(\sum_{i=0}^{6} \alpha_i\beta_{i+3}\big)\lambda + \frac{1}{2}\sum_{i=0}^{6} \alpha_i\alpha_{i+3}\Big)^2$$

(where the subscripts are taken modulo 6), we see that this occurs precisely when $\det(M_{\underline{\alpha}} + \lambda M_{\underline{\beta}}) = 0$. We can therefore solve $\det(M_{\underline{\alpha}} + \lambda M_{\underline{\beta}}) = 0$ to determine a value for λ, and to see that $\mathbb{F}_q(\lambda)$ is at most a quadratic extension of $\mathbb{F}_q$. Considering the discriminant of $\det(M_{\underline{\alpha}} + \lambda M_{\underline{\beta}})$ gives us an explicit criterion for determining whether a given tractable subgroup has a rational trigonal map.

Proposition 2. *Suppose S is a subgroup in $\mathcal{S}(H)$, and let $\{\underline{\alpha} = (\alpha_i), \underline{\beta} = (\beta_i)\}$ be any $\mathbb{F}_q$-rational basis of the nullspace of the matrix M defined in (1). There exists an $\mathbb{F}_q$-rational trigonal map for S if and only if*

$$\Big(\sum_{i=0}^{6} \alpha_i\beta_{i+3}\Big)^2 - \Big(\sum_{i=0}^{6} \alpha_i\alpha_{i+3}\Big)\Big(\sum_{i=0}^{6} \beta_i\beta_{i+3}\Big)$$

is a square in $\mathbb{F}_q$.

Finally, we compute a, b, c, and d in $k(\lambda)$ such that $(1, 0, a, b)$ and $(0, 1, c, d)$ generate the rowspace of $M_{\underline{\alpha}} + \lambda M_{\underline{\beta}}$ (this is easily done by Gaussian elimination). We may then take $L = V(u_0 + au_2 + u_3, u_1 + cu_2 + du_3)$. Both L and the projection $p : \mathbb{P}^3 \to \mathbb{P}^1$ with centre L are defined over $k(\lambda)$. Having computed L, we compute the projection p, the embedding e, and the trigonal map $g = p \circ e$ as above.

Proposition 2 shows that the rationality of a trigonal map for a tractable subgroup S depends only upon whether an element of $\mathbb{F}_q$ depending on S is a square. It seems reasonable to assume that these field elements are uniformly distributed for random choices of H and S, and indeed this is consistent with our experimental observations. Since the probability that a randomly chosen element of $\mathbb{F}_q$ is a square is essentially 1/2, we propose the following hypothesis.

Hypothesis 2. *The probability that there exists an $\mathbb{F}_q$-rational trigonal map for a randomly chosen hyperelliptic curve H over $\mathbb{F}_q$ and subgroup S in $\mathcal{S}(H)$ is 1/2.*

6 Equations for the Isogeny

Suppose we have a tractable subgroup S and a trigonal map g for S. We will now perform an explicit trigonal construction on g to compute a curve X and an isogeny $\phi : J_H \to J_X$ with kernel S. We assume that g has been derived as in §5, and in particular that g maps the point at infinity to the point at infinity.

Let U be the subset of $\mathbb{A}^1 = \mathbb{P}^1 \setminus \{(1 : 0)\}$ above which $g \circ \pi$ is unramified. We denote $f^{-1}(U)$ by $X|_U$, and $(g \circ \pi)^{-1}(U)$ by $H|_U$. By definition, every point P on $X|_U$ corresponds to pair of triples of points on $H|_U$, exchanged by the hyperelliptic involution, with each triple supported on the fibre of $g \circ \pi$ over $f(P)$.

To be more explicit, suppose Q is a generic point of U. Since $g\circ\pi$ is unramified above Q, we may choose preimages P_1, P_2 and P_3 of Q such that

$$(g\circ\pi)^{-1}(Q) = \{P_1, P_2, P_3, \iota(P_1), \iota(P_2), \iota(P_3)\}. \qquad (2)$$

The four points on X in the preimage $f^{-1}(Q)$ correspond to partitions of the six points in $(g\circ\pi)^{-1}(Q)$ into two unordered triples exchanged by the hyperelliptic involution:

$$f^{-1}(Q) = \left\{ \begin{array}{l} Q_1 \leftrightarrow \big\{\{P_1, P_2, P_3\},\ \{\iota(P_1), \iota(P_2), \iota(P_3)\}\big\}, \\ Q_2 \leftrightarrow \big\{\{P_1, \iota(P_2), \iota(P_3)\},\ \{\iota(P_1), P_2, P_3\}\big\}, \\ Q_3 \leftrightarrow \big\{\{\iota(P_1), P_2, \iota(P_3)\},\ \{P_1, \iota(P_2), P_3\}\big\}, \\ Q_4 \leftrightarrow \big\{\{\iota(P_1), \iota(P_2), P_3\},\ \{P_1, P_2, \iota(P_3)\}\big\} \end{array} \right\}. \qquad (3)$$

Every triple is cut out by an ideal $(a(x), y-b(x))$, where a is a cubic polynomial, b is a quadratic, and $b^2 \equiv F \pmod{a}$. If we require a to be monic, then there is a one-to-one correspondence between such ideals and triples; this is the well-known *Mumford representation.* For example, the triple $\{P_1, P_2, P_3\}$ corresponds to the ideal $(a(x), y-b(x))$ where $a(x) = \prod_i (x - x(P_i))$ and b satisfies $y(P_i) = b(x(P_i))$ for $1 \leq i \leq 3$; the Lagrange interpolation formula may be used to compute b. If $(a(x), y-b(x))$ corresponds to one triple in a partition, then $(a(x), y+b(x))$ corresponds to the other triple. The union of the triples equals the whole fibre $(g\circ\pi)^{-1}(Q)$, and since the union of the triples is cut out by the product of the corresponding ideals, we know that $a(x)$ must cut out the fibre of $g\circ\pi$ over Q. Therefore, we have $a(x) = N(x) - t(Q)D(x)$. We may thus define a bijection between points P on $X|_U$ and pairs $\{(N(x) - t(f(P))D(x), y \pm b(x))\}$ of ideals, where b is a quadratic such that $b^2 \equiv F \pmod{N(x) - t(f(P))D(x)}$.

The polynomials of the form $N(x) - tD(x)$ are parametrized by $\mathbb{A}^1$, via the map $t \leftrightarrow N(x) - tD(x)$. The space of quadratic polynomials $b(x)$ may be viewed naturally as the affine space $\mathbb{A}^3$ via the identification

$$b(x) = b_0x^2 + b_1x + b_0 \longleftrightarrow (b_0, b_1, b_2) \in \mathbb{A}^3.$$

We will therefore construct a model of the abstract curve $X|_U$ in $\mathbb{A}^1 \times \mathbb{A}^3$; the isomorphism will be defined by

$$p : (t, b_0, b_1, b_2) \longleftrightarrow \{(G(t,x), y \pm (b_0 + b_1x + b_2x^2))\},$$

where

$$G(t,x) = x^3 + g_2(t)x^2 + g_1(t)x + g_0(t) := N(x) - tD(x).$$

If (t, b_0, b_1, b_2) is a point on $p^{-1}(X|_U)$, then we have $(\sum_i b_ix^i)^2 \equiv F(x) \pmod{G(t,x)}$. Expanding $(b_2x^2 + b_1x + b_0)^2 - F(x)$ modulo $G(t,x)$, we obtain polynomials c_0, c_1, and c_2 in $k[t, b_0, b_1, b_2]$ such that

$$\sum_{i=0}^{2} c_i(t, b_0, b_1, b_2)x^i \equiv \big(\sum_{i=0}^{2} b_ix^i\big)^2 - F(x) \pmod{G(t,x)}.$$

Set $Z := V(c_0, c_1, c_2)$. By definition, c_0, c_1, and c_2 all vanish on $p^{-1}(X|_U)$, so $p^{-1}(X|_U) \subset Z$. Define polynomials f_0, f_1, and f_2 in $k[t]$ by

$$f_2(t)x^2 + f_1(t)x + f_0(t) \equiv F(x) \pmod{G(t,x)}.$$

The polynomials c_0, c_1, and c_2 are given explicitly by the equations

$$\begin{aligned} c_0(t,b_0,b_1,b_2) &= g_2(t)g_0(t)b_2^2 - 2g_0(t)b_2b_1 + b_0^2 - f_0(t), \\ c_1(t,b_0,b_1,b_2) &= (g_2(t)g_1(t) - g_0(t))b_2^2 - 2g_1(t)b_2b_1 + 2b_1b_0 - f_1(t), \text{ and} \\ c_2(t,b_0,b_1,b_2) &= (g_2(t)^2 - g_1(t))b_2^2 - 2g_2(t)b_2b_1 + 2b_2b_0 + b_1^2 - f_2(t). \end{aligned} \tag{4}$$

The map $p : Z \to X$ is a double cover, whose sheets are exchanged by the involution $\iota_* : (t, b_0, b_1, b_2) \mapsto (t, -b_0, -b_1, -b_2)$ of Z induced by the hyperelliptic involution ι. We will see that Z is the union of two curves, each isomorphic to (an open subset of) X; the involution ι_* maps each curve onto the other.

Remark 3. What follows is essentially a derivation of the primary decomposition of the ideal (c_0, c_1, c_2). In practice, the reader equipped with a computational algebra system may avoid using the formulae below by computing the primary decomposition using Gröbner basis methods. This approach is quite efficient if (c_0, c_1, c_2) is viewed as a zero-dimensional ideal in $k(t)[b_0, b_1, b_2]$.

Consider again the fibre of $f : X \to \mathbb{P}^1$ over the generic point $Q = (t)$ of U (as in (3)). If $\{P_1, P_2, P_3\}$ is one of the triples in a pair in the fibre, then by the Lagrange interpolation formula the value of b_2 at the corresponding point of Z is

$$b_2 = \sum y(P_i)/((x(P_i) - x(P_j))(x(P_i) - x(P_k))),$$

where the sum is taken over the cyclic permutations (i, j, k) of $(1, 2, 3)$. Interpolating for all triples in the pairs in the fibre, an elementary but involved symbolic calculation shows that if we define Δ_1, Δ_2, and Δ_3 by

$$\Delta_i := (x(P_j) - x(P_k))^2$$

and Γ_1, Γ_2, and Γ_3 by

$$\Gamma_i := \left(f_2(t)x(P_i)^2 + f_1(t)x(P_i) + f_0(t)\right)\Delta_i = F(x(P_i))\Delta_i$$

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

$$\Delta := \Delta_1\Delta_2\Delta_3,$$

then b_2 satisfies

$$\Big(\Delta b_2^4 - 2\big(\sum_i \Gamma_i\big)b_2^2 + \frac{1}{\Delta}\Big(2\big(\sum_i \Gamma_i^2\big) - \big(\sum_i \Gamma_i\big)^2\Big)\Big)^2 - 64\big(\prod_i \Gamma_i\big)b_2^2 = 0. \tag{5}$$

Now Δ, $\sum_i \Gamma_i$, $\sum_i \Gamma_i^2$, and $\prod_i \Gamma_i$ are symmetric functions with respect to permutations of the points in the fibre $g^{-1}(Q) = g^{-1}((t))$. They are therefore polynomials in the homogeneous elementary symmetric functions

$$e_1 = \sum x(P_i), \quad e_2 = \sum x(P_i)x(P_j), \quad \text{and} \quad e_3 = \prod x(P_i),$$

which are polynomials in t. Indeed, the e_i are given by the coefficients of $G(t,x)$:

$$e_1 = -g_2(t), \quad e_2 = g_1(t), \quad \text{and} \quad e_3 = -g_0(t).$$

Expressing $\varDelta$, $\sum_i \varGamma_i$, $\sum_i \varGamma_i^2$, and $\prod_i \varGamma_i$ in terms of f_0, f_1, f_2, g_0, g_1, g_2, and g_3, and then simplying, we define δ_4, δ_2, and δ_0 by

$$\begin{aligned}\delta_4 &:= -27g_0^2 + 18g_0g_1g_2 - 4g_0g_2^3 - 4g_1^3 + g_1^2g_2^2,\\ \delta_2 &:= 12f_0g_1 - 4f_0g_2^2 - 18f_1g_0 + 2f_1g_1g_2 + 12f_2g_0g_2 - 4f_2g_1^2,\\ \delta_0 &:= -4f_0f_2 + f_1^2,\end{aligned} \tag{6}$$

and s by

$$\begin{aligned}s := {}& f_0^3 - f_0^2f_1g_2 - 2f_0^2f_2g_1 + f_0^2f_2g_2^2 + f_0f_1^2g_1 + 3f_0f_1f_2g_0 - f_0f_1f_2g_1g_2\\ &- 2f_0f_2^2g_0g_2 + f_0f_2^2g_1^2 - f_1^3g_0 + f_1^2f_2g_0g_2 - f_1f_2^2g_0g_1 + f_2^3g_0^2.\end{aligned} \tag{7}$$

With this notation, (5) becomes

$$\big(\delta_4(t)b_2^4 + \delta_2(t)b_2^2 + \delta_0(t)\big)^2 - 64s(t)b_2^2 = 0. \tag{8}$$

Since $s(t) = F(x(P_1))F(x(P_2))F(x(P_3)) = (y(P_1)y(P_2)y(P_3))^2$, there is a square root of $s(t)$ in $\overline{\mathbb{F}_q}[t]$. Indeed, if $s(0)$ is a square in $\mathbb{F}_q$, then the square root is an element of $\mathbb{F}_q[t]$, and we define

$$\delta_1 := 8\sqrt{s}. \tag{9}$$

We define polynomials d_2 and d_2^- in $\mathbb{F}_q[t, b_0, b_1, b_2]$ by

$$d_2 := \delta_4(t)b_2^4 + \delta_2(t)b_2^2 + \delta_1(t)b_2 + \delta_0(t) \quad \text{and} \quad d_2^- := d_2(t, -b_0, -b_1, -b_2). \tag{10}$$

It follows from (5) that $d_2d_2^-$ vanishes on every fibre of $(f \circ p) : Z \to U$, so it must vanish everywhere on Z. Hence $Z = V\big(c_0, c_1, c_2, d_2d_2^-\big)$, from which it follows that

$$Z = V(c_0, c_1, c_2, d_2) \cup V\big(c_0, c_1, c_2, d_2^-\big).$$

The scheme $Z^+ := V(c_0, c_1, c_2, d_2)$ is singular: it has some embedded points supported on the fibres where δ_1 vanishes. To remove these singularities, we derive two more defining equations.

When $b_2 \neq 0$, the equation $c_2 = 0$ becomes

$$b_0 = ((g_1 - g_2^2)b_2^2 + (2g_2)b_2b_1 - b_1^2 + f_2)/(2b_2). \tag{11}$$

Substituting (11) into the definitions of c_0 and c_1, we obtain functions

$$c_0'(t, b_1, b_2) := c_0\big(t, ((g_1 - g_2^2)b_2^2 + (2g_2)b_2b_1 - b_1^2 + f_2)/(2b_2), b_1, b_2\big)$$

and

$$c_1'(t, b_1, b_2) := c_1\big(t, ((g_1 - g_2^2)b_2^2 + (2g_2)b_2b_1 - b_1^2 + f_2)/(2b_2), b_1, b_2\big).$$

Considered as polynomials in $(k(t)[b_2]/(d_2))[b_1]$, we see that c_0' and c_1' have degree 4 and 3, respectively. Since both c_0' and c_1' vanish on Z^+, so must their greatest common divisor, which is a linear polynomial in b_1 over $k(t)[b_2]/(d_2)$. Hence, there are polynomials $n_{1,1}$, $d_{1,1}$, $n_{1,0}$, and $d_{1,0}$ in $k[t, b_2]$ such that

$$\gcd(c_0', c_1') = \frac{n_{1,1}(t,b_2)}{d_{1,1}(t,b_2)} b_1 + \frac{n_{1,0}(t,b_2)}{d_{1,0}(t,b_2)}. \tag{12}$$

Since $\gcd(c_0', c_1') = 0$ on Z^+, the polynomial

$$d_1(t, b_1, b_2) := n_{1,1}(t,b_2) d_{1,0}(t,b_2) b_1 + n_{1,0}(t,b_2) d_{1,1}(t,b_2) \tag{13}$$

vanishes on Z^+. Substituting $b_1 = -(n_{1,0}d_{1,1})/(n_{1,1}d_{1,0})$ into $c_1 = 0$, we obtain an equation $d_0(t, b_1, b_2) = 0$, where

$$d_0(t, b_1, b_2) := n_{0,1}(t,b_2) d_{0,0}(t,b_2) b_0 + n_{0,0}(t,b_2) d_{0,1}(t,b_2) \tag{14}$$

for some polynomials $n_{0,1}$, $n_{0,0}$, $d_{0,1}$, and $d_{0,0}$ in $k[t, b_2]$.

The curve $Y = V(c_0, c_1, c_2, d_0, d_1, d_2)$ in $\mathbb{A}^1 \times \mathbb{A}^3$ is nonsingular, and agrees with Z^+ on an open subset; the double cover $p : Z|_U \to X|_U$ restricts to an isomorphism from an open subset of Y to an open subset of $X|_U$. By Corollary I.6.12 of Hartshorne [7], Y itself is isomorphic to an open subset of X, and we may view Y as an affine model of X. Hence, in the sequel, we will take X to be (a projective closure of the curve) defined by

$$X : V(c_0, c_1, c_2, d_0, d_1, d_2) \subset \mathbb{A}^1 \times \mathbb{A}^3.$$

Next, we compute the Recillas correspondence R. The fibre product $H \times_{\mathbb{A}^1} X$ with respect to $g \circ \pi$ and f is defined by $H \times_{\mathbb{A}^1} X = V(G(t,x)) \subset \mathbb{A}^2 \times (\mathbb{A}^1 \times \mathbb{A}^3)$, and has two components:

$$V(G(t,x)) = V\Big(G(t,x),\ y - \Big(\textstyle\sum_i b_i x^i\Big)\Big) \cup V\Big(G(t,x),\ y + \Big(\textstyle\sum_i b_i x^i\Big)\Big).$$

We set

$$R = V\big(G(t,x),\ y - (b_0 + b_1 x + b_2 x^2)\big).$$

The natural projections $\pi_X : R \to X$ and $\pi_H : R \to H$ send (x, y, t, b_0, b_1, b_2) to (t, b_0, b_1, b_2) and (x, y), respectively. On the level of divisor classes, the isogeny $\phi : J_H \to J_X$ is made explicit by the map

$$\phi = (\pi_X)_* \circ (\pi_H)^*.$$

In terms of ideals cutting out effective divisors, ϕ is realized by the map

$$I_D \longmapsto \big(I_D + (G(t,x), y - (b_0 z^2 + b_1 x z + b_2 x^2))\big) \cap k[s, t, b_0, b_1, b_2].$$

Taking $V\big(G(t,x), y + (b_2 x^2 + b_1 x + b_0)\big)$ in place of R above gives an isogeny equal to $-\phi$. Similarly, the isogeny from H to X' induced by R' is isomorphic to the isogeny ϕ from H to X.

Considering the formulae above, we see that X and the isogeny are both defined over $\mathbb{F}_q$ if a certain element of $\mathbb{F}_q$ depending only on F and g — namely $s(0)$ — is a square in $\mathbb{F}_q$. This gives us a useful criterion for when an $\mathbb{F}_q$-rational S and g leads to an $\mathbb{F}_q$-rational X.

Proposition 3. *If S is a subgroup in $\mathcal{S}(H)$ with an $\mathbb{F}_q$-rational trigonal map g, then the trigonal construction on g yields a curve X defined over $\mathbb{F}_q$ if and only if $s(0)$ is a square in $\mathbb{F}_q$, where s is defined in* (7).

If we assume that the values $s(0)$ are uniformly distributed for randomly chosen H, S and g, then the probability that $s(0)$ is a square in $\mathbb{F}_q$ is $1/2$. Indeed, it is easily seen that $s(0)$ is a square for H if and only if it is not a square for the quadratic twist of H. This suggests that the probability that we can compute an $\mathbb{F}_q$-rational X and ϕ given an $\mathbb{F}_q$-rational g for a randomly chosen H and S in $\mathcal{S}(H)$ is $1/2$. This is consistent with our experimental observations, so we propose Hypothesis 3.

Hypothesis 3. *Given a randomly chosen hyperelliptic curve H over $\mathbb{F}_q$ and tractable subgroup S in $\mathcal{S}(H)$ with an $\mathbb{F}_q$-rational trigonal map g, the probability that we can compute an $\mathbb{F}_q$-rational curve X is* $1/2$.

7 Computing Isogenies

Suppose we are given a hyperelliptic curve H of genus 3, defined over $\mathbb{F}_q$, and a DLP in $J_H(\mathbb{F}_q)$. Our goal is to compute a plane quartic curve C and an isogeny $J_H \to J_C$ so that we can reduce to a DLP in $J_C(\mathbb{F}_q)$.

First, we compute the set $\mathcal{S}(H)$ of $\mathbb{F}_q$-rational tractable subgroups of $J_H[2]$. For each S in $\mathcal{S}(H)$, we apply Proposition 2 to determine whether there exists an $\mathbb{F}_q$-rational trigonal map g for S. If so, we use the formulae of §5 to compute g; if not, we move on to the next S. Having computed g, we apply Proposition 3 to determine whether we can compute an X over $\mathbb{F}_q$. If so, we use the formulae of §6 to compute equations for X and the isogeny $J_H \to J_X$; if not, we move on to the next S.

The formulae of §6 give an affine model of X in in $\mathbb{A}^1 \times \mathbb{A}^3$. In order to apply Diem's algorithm to the DLP in J_X, we need a plane quartic model of X: that is, a nonsingular curve $C \subset \mathbb{P}^2$ isomorphic to X, cut out by a quartic form. Such a model exists if and only if X is not hyperelliptic. To find C, we compute a basis $\mathcal{B}$ of the Riemann–Roch space of a canonical divisor of X. This is a routine geometrical calculation; some of the various approaches are listed in Hess [8]. In practice, the algorithms implemented in Magma [9] compute $\mathcal{B}$ very quickly. The functions in $\mathcal{B}$ define a rational map $\psi : X \to \mathbb{P}^2$. If the image of ψ is a conic or a line, then X is hyperelliptic, and we move on to the next S. Otherwise, the image of ψ is a smooth plane quartic model C of X, and ψ restricts to an isomorphism $\psi : X \to C$.

If the procedure outlined above succeeds for some S in $\mathcal{S}(H)$, then we have computed an explicit $\mathbb{F}_q$-rational isogeny $\psi_* \circ \phi : J_H \to J_C$. We can then map our DLP from $J_H(\mathbb{F}_q)$ into $J_C(\mathbb{F}_q)$, and solve using Diem's algorithm.

We emphasize that the entire procedure is very fast: as we saw above, the curve X and the isogeny can be constructed using only low-degree polynomial arithmetic and low-dimensional linear algebra. For a rough idea of the computational effort involved, given a random H over a 150-bit prime field, an unoptimized implementation of our algorithms in Magma [9] computes the trigonal map g, the curve X, the plane quartic C, and the isogeny $\phi : J_H \to J_C$ in around six seconds on a 1.2GHz laptop. Since the difficulty of the construction depends only upon the size of $\mathbb{F}_q$ (and *not* upon the size of the DLP subgroup of $J_H(\mathbb{F}_q)$), we may conclude that DLPs in 150-bit Jacobians chosen for cryptography may also be reduced to DLPs in non-hyperelliptic Jacobians in around six seconds.

We will give an example over a small field. For the sake of space, we will not display the equations for the intermediate curve X or the isogeny.

Example 1. Let H be the hyperelliptic curve over $\mathbb{F}_{37}$ defined by

$$H : y^2 = x^7 + 28x^6 + 15x^5 + 20x^4 + 33x^3 + 12x^2 + 29x + 2.$$

Using the ideas in §3, we see that J_H has one $\mathbb{F}_{37}$-rational tractable subgroup:

$$\mathcal{S}(H) = \left\{ \left\{ \begin{matrix} u^2 + \xi_1 uv + \xi_2 v^2,\ u^2 + \xi_1^{37} uv + \xi_2^{37} v^2, \\ u^2 + \xi_1^{37^2} uv + \xi_2^{37^2} v^2,\ uv + 20v^2 \end{matrix} \right\} \right\},$$

where $\xi_2 = \xi_1^{50100}$ and $\xi_1^3 + 29\xi_1^2 + 9\xi_1 + 13 = 0$. We compute an $\mathbb{F}_{37}$-rational trigonal map $g : x \longmapsto N(x)/D(x)$ for S, with

$$N(x) = x^3 + 16x + 22, \quad \text{and} \quad D(x) = x^2 + 32x + 18.$$

Using the formulae of §6, we compute a curve X of genus 3 and a map on divisors inducing an isogeny from J_H to J_X with kernel S. Computing the canonical morphism of X, we find that X is non-hyperelliptic, and isomorphic to the plane quartic

$$C = V\begin{pmatrix} x^4 + 28x^3y + 2x^3z + 8x^2y^2 + 11x^2yz + 32x^2z^2 + 16xy^3 + 4xy^2z \\ + 18xyz^2 + 14xz^3 + 18y^4 + 26y^3z + 25y^2z^2 + 3yz^3 + 35z^4 \end{pmatrix}.$$

Composing the isomorphism with the isogeny, we obtain an isogeny $\phi : J_H \to J_C$. The characteristic polynomial of Frobenius on both J_H and J_C is $T^6 + 4T^5 - 6T^4 - 240T^3 - 6{\cdot}37T^2 + 4{\cdot}37^2T + 37^3$. If D and D' are the divisor classes on H with Mumford representatives $(x^2+13x+29, y-10x-2)$ and $(x^2+3x+26, y-10x-23)$, respectively, then $D' = [5719]D$. Applying ϕ, we have

$$\begin{aligned} \phi(D) &= [(20:22:1) + (3:22:1) - (20:1:0) - (11:6:1)] \quad \text{and} \\ \phi(D') &= [(25:3:1) + (27:36:1) - (34:14:1) - (21:32:1)]\,; \end{aligned}$$

direct calculation shows that $\phi(D') = [5719]\phi(D)$, as expected.

8 Expectation of Existence of Computable Isogenies

We conclude by estimating the proportion of genus 3 hyperelliptic Jacobians over $\mathbb{F}_q$ for which the methods of this article produce a rational isogeny — and thus the proportion of hyperelliptic curves for which the DLP may be solved using Diem's algorithm — as q tends to infinity. We will assume that if we are given a selection of $\mathbb{F}_q$-rational tractable subgroups, then it is equally probable that any one of them will yield a rational isogeny. This is consistent with our experimental observations.

Hypothesis 4. If S_1 and S_2 are distinct subgroups in $\mathcal{S}(H)$, then the probability that we can compute an $\mathbb{F}_q$-rational isogeny with kernel S_1 is independent of the probability that we can compute an $\mathbb{F}_q$-rational isogeny with kernel S_2.

Theorem 2. *Assume Hypotheses 1, 2, 3, and 4. Let $\mathcal{T}$ be the set of integer partitions of* 8*; for each T in $\mathcal{T}$ we define $\nu_T(n)$ to be the multiplicity of n in T, and define $s(T) = \#\mathcal{S}(H)$, where H is* any *hyperelliptic curve over $\mathbb{F}_q$ such that the multiset of degrees of the $\mathbb{F}_q$-irreducible factors of its hyperelliptic polynomial coincides with T. As q tends to infinity, the expectation that the algorithms in this article will give a reduction of the DLP in a subgroup of $J_H(\mathbb{F}_q)$ for a randomly chosen hyperelliptic curve H of genus* 3 *over $\mathbb{F}_q$ to a subgroup of $J_C(\mathbb{F}_q)$ for some plane quartic curve C is*

$$\sum_{T\in\mathcal{T}} \Big((1-(1-1/4)^{s(T)}) / \prod_{n\in T} \left(\nu_T(n)! \cdot n^{\nu_T(n)}\right) \Big) \approx 0.1857.$$

Proof. Hypotheses 1, 2, 3, and 4 together imply that if H is a randomly chosen hyperelliptic curve of genus 3 over $\mathbb{F}_q$, then the probability that we will succeed in computing a rational isogeny from J_H is

$$1-(1-(1/2\cdot 1/2))^{\#\mathcal{S}(H)}. \qquad (15)$$

Lemma 1 implies that $\mathcal{S}(H)$ depends only on the degrees of the irreducible factors of $\widetilde{F}$. For each T in $\mathcal{T}$, let $N_q(T)$ denote the number of homogeneous squarefree polynomials over $\mathbb{F}_q$ whose multiset of degrees of irreducible factors coincides with T. By (15), the expectation that we can compute an $\mathbb{F}_q$-rational isogeny from the Jacobian a randomly chosen hyperelliptic curve to the Jacobian of a non-hyperelliptic curve using the methods in this article is

$$E_q := \frac{\sum_{T\in\mathcal{T}}(1-(1-1/4)^{s(T)})N_q(T)}{\sum_{T\in\mathcal{T}} N_q(T)}. \qquad (16)$$

Let $N_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$; clearly $N_q(T) = (q-1)\prod_{n\in T}\binom{N_q(n)}{\nu_T(n)}$. Computing $N_q(T)$ is a straightforward combinatorial exercise: we find that $N_q(n) = q^n/n + O(q^{n-1})$, so

$$N_q(T) = \Big(\prod_{n\in T}(\nu_T(n)!\cdot n^{\nu_T(n)})^{-1}\Big)q^9 + O(q^8),$$

and $\sum_{T\in\mathcal{T}} N_q(T) = q^9 + O(q^8)$. Therefore, as q tends to infinity, we have

$$\lim_{q\to\infty} E_q = \sum_{T\in\mathcal{T}} \Big((1-(1-1/4)^{s(T)}) / \prod_{n\in T} (\nu_T(n)!\cdot n^{\nu_T(n)}) \Big).$$

The result follows upon explicitly computing this sum using the values for $s(T)$ derived in Lemma 1. □

Theorem 2 gives the expectation that we can construct an explicit isogeny for a randomly selected hyperelliptic curve. However, looking at the table in Lemma 1, we see that we can ensure that a particular curve has no rational isogenies if its hyperelliptic polynomial has an irreducible factor of degree 5 or 7 (or a single irreducible factor of degree 3). It may be difficult to construct a curve in this form if we are using the CM construction, for example, to ensure that the Jacobian has a large prime-order subgroup. In any case, it is interesting to note that the security of genus three hyperelliptic Jacobians depends upon the factorization of their hyperelliptic polynomials. This observation has no analogue for elliptic curves and Jacobians of genus 2 curves.

Remark 4. We noted in §4 that the isomorphism class of the curve X in the trigonal construction is independent of the choice of trigonal map. If there is no rational trigonal map for a given subgroup S, then the methods of §5 construct a pair of Galois-conjugate trigonal maps g_1 and g_2 instead. If the trigonal constructions on g_1 and g_2 require no further base extension, then we obtain a pair of curves X_1 and X_2, which must be twists. If the isomorphism between these two curves was made explicit, then Galois descent could be used to compute a curve X in their isomorphism class defined over $\mathbb{F}_q$, and hence a plane quartic C and isogeny $J_H \to J_C$ over $\mathbb{F}_q$. This approach would allow us to replace the $1/4$ in (15) and (16) with $1/2$, raising the expectation of success to over 30%.

9 Other Isogenies

In this article, we have used a special kind of $(2,2,2)$-isogeny for moving DLPs from hyperelliptic to non-hyperelliptic Jacobians. More generally, we can consider using other types of isogenies. There are two important issues to consider here: the first is a theoretical restriction on the types of subgroups S of J_H that can be kernels of isogenies of Jacobians, and the second is a practical restriction on the isogenies that we can currently compute.

Suppose J_H is a hyperelliptic Jacobian, and S a (finite) $\mathbb{F}_q$-rational subgroup of J_H. The quotient $J_H \to J_H/S$ exists as an isogeny of abelian varieties (see Serre [14, §III.3.12], for example). For the quotient to be an isogeny of Jacobians, there must be an integer m such that S is a maximal isotropic subgroup with respect to the m-Weil pairing (see Proposition 16.8 of Milne [10]): this ensures that the canonical polarization on J_H induces a principal polarization on the quotient. The simplest such subgroups have the form $(\mathbb{Z}/l\mathbb{Z})^3$ where l is prime. The theorem of Oort and Ueno [11] then guarantees that there will be an isomorphism over $\overline{\mathbb{F}}_q$ from J_H/S to the Jacobian J_X of some (possibly reducible) curve X. Standard arguments from Galois cohomology (see Serre [13, §III.1], for example) show that the isomorphism is defined over $\mathbb{F}_{q^2}$. We can expect X to be isomorphic to a non-hyperelliptic curve C. To compute an isogeny from J_H to a non-hyperelliptic Jacobian, therefore, the minimum requirement is an $\mathbb{F}_q$-rational subgroup of J_H isomorphic to $(\mathbb{Z}/l\mathbb{Z})^3$ for some prime l.

The second and more serious problem is the lack of general constructions for isogenies in genus 3. Apart from integer and Frobenius endomorphisms, we know of no constructions for explicit isogenies of general Jacobians of genus 3 hyperelliptic curves other than the one presented here. This situation stands in marked contrast to the case of isogenies of elliptic curves, which has been made completely explicit by Vélu [16]. Deriving general formulae for explicit isogenies in genus 3 (and 2) remains a significant problem in computational number theory.

References

1. C. Birkenhake and H. Lange, *Complex abelian varieties* (2e). Grundlehren der mathematischen Wissenschaften **302**, Springer 2004.
2. J.-B. Bost and J.-F. Mestre, Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math. Soc. France* **38** (1988), 36–64.
3. C. Diem, An index calculus algorithm for plane curves of small degree, *Algorithmic Number Theory - ANTS VII*, LNCS **4076**, Springer 2006.
4. R. Donagi, The fibres of the Prym map, *Curves, Jacobians, and abelian varieties (Amherst, MA, 1990)*, *Contemp. Math.* **136** (1992), 55–125.
5. R. Donagi and R. Livné, The arithmetic-geometric mean and isogenies for curves of higher genus, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **28** (1999), no. 2, 323–339.
6. P. Gaudry, E. Thomé, N. Thériault, and C. Diem, A double large prime variation for small genus hyperelliptic index calculus, *Math. Comp.* **76** (2007), 475–492.
7. R. Hartshorne, *Algebraic Geometry*, GTM **52**, Springer (1977).
8. F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics, *J. Symbolic Computation* **33** v.4 (2002), 425–445.
9. The Magma computational algebra system. `http://magma.maths.usyd.edu.au/`
10. J. S. Milne, Abelian varieties, *Arithmetic geometry (Storrs, Conn., 1984)*, Springer (1986), 103–150.
11. F. Oort and K. Ueno, Principally polarized abelian varieties of dimension two or three are Jacobian varieties, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **20** (1973), 377–381.
12. S. Recillas, Jacobians of curves with g^1_4's are the Prym's of trigonal curves, *Bol. Soc. Mat. Mexicana (2)* **19** (1974), no. 1, 9–13.
13. J.-P. Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Springer (2002).
14. J.-P. Serre, *Algebraic Curves and Class Fields*, GTM **117**, Springer (1988).
15. R. Vakil, Twelve points on the projective line, branched covers, and rational elliptic fibrations, *Math. Ann.* **320** (2001), no. 1, 33–54.
16. J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris, Séries A* **273** (1971), 305–347.