DISTORTION MAPS FOR GENUS TWO CURVES

STEVEN D. GALBRAITH, JORDI PUJOLÀS, CHRISTOPHE RITZENTHALER, AND BENJAMIN SMITH

ABSTRACT. Distortion maps are a useful tool for pairing based cryptography. Compared with elliptic curves, the case of hyperelliptic curves of genus $g > 1$ is more complicated since the full torsion subgroup has rank $2g$. In this paper we prove that distortion maps always exist for supersingular curves of genus $g > 1$ and we give several examples in genus 2.
Keywords: hyperelliptic curve cryptography, pairings, supersingular curves, distortion maps.

1. INTRODUCTION

Let q be a power of a prime p. Let C be a non-singular, geometrically irreducible, and projective curve defined over the finite field $\mathbb{F}_q$. The Jacobian variety of C is denoted by $\mathrm{Jac}(C)$, and the q-power Frobenius map is denoted π. Throughout this paper, we identify $\mathrm{Jac}(C)(\mathbb{F}_{q^n})$ with the degree zero divisor class group of C over $\mathbb{F}_{q^n}$. Let r be a prime number dividing $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ and coprime to p. We define the *embedding degree* to be the smallest positive integer k such that r divides $q^k - 1$. Note that $\mathbb{F}_{q^k}$ is then the field generated over $\mathbb{F}_q$ by adjoining the rth roots of unity. If A is an abelian variety, then $\mathrm{End}_K(A)$ denotes the ring of endomorphisms of A defined over a field K, and $\mathrm{End}(A)$ the ring of endomorphisms of A defined over an algebraic closure of K. Unless specified otherwise, all morphisms are defined over the algebraic closure of the field.

An elliptic curve E over $\mathbb{F}_q$ is called *supersingular* if the number of points on E over $\mathbb{F}_q$ is congruent to 1 modulo p. If E is a supersingular elliptic curve, then $\mathrm{End}(E)$ is an order in a quaternion algebra. More generally, an abelian variety A of dimension g over $\mathbb{F}_q$ is called supersingular if A is isogenous over $\overline{\mathbb{F}}_q$ to a product E^g, where E is a supersingular elliptic curve. In this case, it follows that $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra of dimension $(2g)^2$ as a $\mathbb{Q}$-vector space. Finally, a curve C is called supersingular if $\mathrm{Jac}(C)$ is a supersingular abelian variety.

Let $r > 2$ be a prime dividing $q^k - 1$, and coprime to q. The Tate pairing (see Frey and Rück [?]) is a non-degenerate bilinear pairing of the r-torsion in the divisor class group of C over $\mathbb{F}_{q^k}$ with a certain quotient group of the divisor class group over $\mathbb{F}_{q^k}$. Using standard methods (see [?, ?]), we can obtain from the Tate pairing a bilinear pairing (often called the reduced Tate pairing) $e_r(\cdot, \cdot)$ from $\mathrm{Jac}(C)(\mathbb{F}_{q^k})[r]$ to the group μ_r of rth roots of unity in $\mathbb{F}_{q^k}^*$.

When C is supersingular and $r \| \#\mathrm{Jac}(C)(\mathbb{F}_q)$, then $\mathrm{Jac}(C)[r]$ is often contained in $\mathrm{Jac}(C)(\mathbb{F}_{q^k})$ (see [?]). In this case, the Weil pairing is also a non-degenerate bilinear pairing on $\mathrm{Jac}(C)(\mathbb{F}_{q^k})[r]$. If the embedding degree k is small, then either the Weil or Tate pairing may be useful for implementing pairing-based cryptosystems (see [?, ?, ?] for a survey). We use the notation $e_r(\cdot, \cdot)$ to denote any bilinear,

nondegenerate, Galois-invariant pairing on $\mathrm{Jac}(C)[r]$ (such as the Weil or reduced Tate pairings).

When $\mathrm{Jac}(C)$ is supersingular, the embedding degree k is known to be bounded above by a constant $k(g)$ depending only on the genus g of C (see [?, ?]). In cryptographic applications, one tends to be interested in cases where the embedding degree is greater than 1, but not "too large".

Bilinearity is an important property of pairings in cryptography: for all integers a and b and elements D_1 and D_2 of $\mathrm{Jac}(C)[r]$, we have $e_r(aD_1, bD_2) = e_r(D_1, D_2)^{ab}$. For bilinearity to be useful, however, it is necessary that $e_r(D_1, D_2) \neq 1$. It is known that the Weil and Tate pairings are non-degenerate: that is, for each non-zero divisor class D_1 of order r, there is a divisor class D_2 such that $e_r(D_1, D_2) \neq 1$. A problem arises when one wants to pair two specific divisors D_1 and D_2 such that $e_r(D_1, D_2) = 1$ — this can happen, for example, when for efficiency reasons both divisors are defined over $\mathbb{F}_q$, and $k > 1$. In these cases, we need distortion maps.

Definition. A *distortion map* for a non-degenerate pairing e_r and non-zero divisor classes D_1, D_2 of prime order r on C is an endomorphism ψ of $\mathrm{Jac}(C)$ such that $e_r(D_1, \psi(D_2)) \neq 1$.

Distortion maps were introduced by Verheul [?] for elliptic curves in the case where D_1 and D_2 are defined over the ground field. We stress that our definition depends on the choice of divisor classes (and also the pairing). In general, it is not true that there is a single choice of ψ that is a distortion map for all pairs of non-zero divisor classes.

The goal of this paper is to provide, for certain curves, a collection of efficiently computable endomorphisms such that there is a suitable distortion map in the collection for any pair of divisor classes on the curves. Note that the Frobenius or trace maps may be used as distortion maps in many situations, including the case of ordinary curves; but distortion maps for every pair can *only* be obtained for supersingular curves.

The case where C is an elliptic curve is quite simple. If D_1 and D_2 are nonzero divisor classes and $e_r(D_1, D_2) = 1$, then any divisor D_3 of order r which is independent of D_2 (that is, $\langle D_2 \rangle \cap \langle D_3 \rangle = \{0\}$) satisfies $e_r(D_1, D_3) \neq 1$. This follows from the non-degeneracy of the pairing, and the fact that the r-torsion of an elliptic curve has rank 2. For this reason, and others, the problem of finding distortion maps for elliptic curves is relatively easy to handle. An algorithm to find distortion maps for any supersingular elliptic curve has been given by Galbraith and Rotger [?].[1]

For curves C of genus $g > 1$, the r-torsion of the Jacobian has rank $2g$; so independence of divisors is not sufficient to imply non-triviality of their pairing. Indeed, elementary linear algebra implies that for every non-trivial divisor D of order r, there exists a basis for $\mathrm{Jac}(C)[r]$ such that D pairs trivially with all but one of the basis elements. Furthermore, elements of $\mathrm{End}(\mathrm{Jac}(C))$ may be difficult to handle, as they generally do not correspond to maps from C to itself.

In this paper, we discuss this situation, with particular emphasis on curves of genus 2. In Section ??, we prove that distortion maps always exist for supersingular abelian varieties. The rest of the paper is concerned with the question of whether such maps can be easily computed on Jacobians of curves. In Section ??, we

---

[1]Note that there is a missing condition in Lemma 5.1 of [?], namely that $\psi(P) \neq 0$. Since the degree of ψ in [?] is d, which is much smaller than r, this condition is always satisfied.

provide a list of examples of supersingular curves with suitable embedding degree. These examples are explored in depth in the subsequent sections. The results of Section **??**, first presented in [**?**], concern the case $k = 4$ where $p \equiv 2, 3 \pmod 5$. After illustrating our approach on this simple case, we generalize the method to other curves in Section **??**. Section **??** deals with the case $k = 5$ when $p = 5$, and Section **??** deals with the case $k = 6$ when $p \equiv 2 \pmod 3$ (and $p \neq 2$). Finally, Section **??** treats the case $k = 12$ and $p = 2$. We provide non-trivial, efficient, explicit distortion maps for each curve.

Note that there is an important distinction between the cases $k = 4, 12$ and $k = 5, 6$. For the former cases, our result are conditional, since they depend on the assumption (verified in practice) that some denominators can be canceled, which is the case if they are prime to r. In these cases, there seems to be no easy explicit decomposition of $\mathrm{Jac}(C)$: even when we know that the Jacobian splits into a product $E \times E$, the degree of the induced morphisms from C to E is unknown. However, the curves we consider in the cases $k = 5$ and $k = 6$ are both twists of $y^2 = x^6 + 1$, which has two degree-2 maps to an elliptic curve E (see Section **??** for details). This structure is used in a crucial way to remove the assumption on the denominators for the case $k = 6$ (for the case $k = 5$ another argument is used, which is restricted to the case where e_r is the Tate pairing — but the same proof could be adapted).

2. THE EXISTENCE OF DISTORTION MAPS

Schoof and Verheul [**?**] have shown that distortion maps always exist for supersingular elliptic curves over $\mathbb{F}_q$. In this section, we generalise their result to supersingular abelian varieties.

First, we recall an important theorem of Tate [**?**]. Suppose A is an abelian variety over a finite field K of characteristic p, and let $G = \mathrm{Gal}(\overline{K}/K)$. Let l be a prime not equal to p, and let $T_l(A) := \varprojlim A[l^n]$ be the l-Tate module of A. Let $\mathrm{End}_G(T_l(A))$ denote the ring of endomorphisms of $T_l(A)$ which commute with the action of G. Tate's theorem states that the canonical injection

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow \mathrm{End}_G(T_l(A))$$

is an isomorphism.

Theorem 2.1. *Let A be a supersingular abelian variety of dimension g over $\mathbb{F}_q$, and let r be a prime not equal to the characteristic of $\mathbb{F}_q$. For every two non-trivial elements D_1 and D_2 of $A(\mathbb{F}_q)[r]$, there exists an endomorphism ϕ of A such that $e_r(D_1, \phi(D_2)) \neq 1$.*

Proof. Let d be an integer such that the q^d-power Frobenius map acts as an integer multiplication on A. Let $K = \mathbb{F}_{q^d}$ and $G = \mathrm{Gal}(\overline{K}/K)$. Since A is supersingular, $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$ is a free $\mathbb{Z}_r$-module of rank $(2g)^2$. By definition, $\mathrm{End}_K(A)$ is contained in $\mathrm{End}(A)$, so we may view $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$ as a submodule of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$. By Tate's theorem, $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$ is isomorphic to the $\mathbb{Z}_r$-module $\mathrm{End}_G(T_r(A))$ of endomorphisms which commute with the q^d-power Frobenius — but the q^d-power Frobenius is an integer, so it commutes with every endomorphism of A (and $T_r(A)$). Thus $\mathrm{End}_G(T_r(A)) = \mathrm{End}(T_r(A))$. Since $T_r(A) \cong \mathbb{Z}_r^{2g}$ as a $\mathbb{Z}_r$-module, we have

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r \cong \mathrm{End}_G(T_r(A)) \cong M_{2g}(\mathbb{Z}_r).$$

Hence $\mathrm{End}_K(A) \cong \mathrm{End}(A)$ also has rank $(2g)^2$. By restriction, we have

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}/r\mathbb{Z} \cong M_{2g}(\mathbb{Z}/r\mathbb{Z}).$$

Let D_3 be an element of $A[r]$ such that $e_r(D_1, D_3) \neq 1$ (in fact, D_3 is K-rational). There exists some matrix Φ in $M_{2g}(\mathbb{Z}/r\mathbb{Z})$ corresponding to a mapping of the subspace $\langle D_2 \rangle$ to $\langle D_3 \rangle$. Let ϕ be a preimage in $\mathrm{End}(A)$ of Φ: by construction, $e_r(D_1, \phi(D_2)) \neq 1$. □

The proof of Theorem **??** shows that to have a distortion map for every pair of divisors, we must have a full rank-$(2g)^2$ module of endomorphisms. In other words, if the rank of $\mathrm{End}(\mathrm{Jac}(C))$ is strictly less than $(2g)^2$, then there will exist non-zero elements D_1 and D_2 of $\mathrm{Jac}(C)[r]$ such that $e_r(D_1, \psi(D_2)) = 1$ for every endomorphism ψ of $\mathrm{Jac}(C)$. In particular, if C is not supersingular, then there are pairs (D_1, D_2) for which no distortion maps exist.

Remark. It is important to note that Theorem **??** is not constructive.

3. Embedding degrees of supersingular genus 2 curves

In this section we list some supersingular genus 2 curves which are of potential interest for applications. First, we recall the results of Rubin and Silverberg [**?**] classifying the possible embedding degrees for supersingular abelian varieties of dimension 2. We focus on the case where q is an odd power of p: this gives the largest values for k, and so is usually the most interesting case in practice.

Theorem 3.1 (Rubin–Silverberg [**?**])**.** *Let q be an odd power of a prime p. The precise set of possible embedding degrees for simple supersingular abelian surfaces over $\mathbb{F}_q$ is given in the following table.*

p	*Possible embedding degrees k*
2	$\{1, 3, 6, 12\}$
3	$\{1, 3, 4\}$
5	$\{1, 3, 4, 5, 6\}$
≥ 7	$\{1, 3, 4, 6\}$

We note that other embedding degrees, such as $k = 2$, may be realised using non-simple abelian surfaces. Since large embeddings degrees are of the most interest, we focus on the cases where k is 4, 5, 6 and 12.

$k = 4$**:** The CM curve $y^2 = x^5 + A$ over $\mathbb{F}_p$ where $p > 2$ and $p \equiv 2, 3 \pmod 5$ is supersingular, and has embedding degree 4. More generally, reductions of the CM curves listed by van Wamelen [**?**] have embedding degree 4. These curves are discussed in Sections **??** and **??**.

$k = 5$**:** The curves $y^2 = x^5 - x \pm 1$ where $p = 5$, described by Duursma and Sakurai [**?**], are supersingular and have embedding degree 5. We discuss these curves in Section **??**.

$k = 6$**:** An abelian variety over $\mathbb{F}_q$ has embedding degree 6 if its characteristic polynomial of Frobenius is of the form $T^4 - qT^2 + q^2$. A result of Howe, Maisner, Nart and Ritzenthaler [**?**, Theorem 1] implies that such abelian varieties have a principal polarisation if and only if $p \not\equiv 1 \pmod 3$. Hence, Jacobians of curves of genus 2 can have embedding degree 6 only when $p \not\equiv 1 \pmod 3$. In Section **??**, we give an algorithm to construct supersingular curves with embedding degree 6 when $p \equiv 2 \pmod 3$ and $p \geq 5$, by taking suitable twists of the curve $y^2 = x^6 + 1$.

$k = 12$: The curves $y^2 + y = x^5 + x + b$ over $\mathbb{F}_{2^m}$ where $b = 0, 1$ are supersingular, with embedding degree 12. We consider these curves in Section **??**.

4. CURVES WITH EMBEDDING DEGREE 4: CM INDUCED BY AN AUTOMORPHISM

In this section, we work with $q = p$ such that $p > 2$ and $p \equiv 2, 3 \pmod 5$. Consider the curve $\tilde{C}$ defined over $\mathbb{Q}$ by

$$\tilde{C} \colon y^2 = x^5 + 1.$$

The curve $\tilde{C}$ has an automorphism ρ_5 of order 5 defined by

$$\rho_5 : (x, y) \longmapsto (\zeta_5 x, y),$$

where ζ_5 is a primitive fifth root of unity over $\mathbb{Q}$. The automorphism ρ_5 induces an endomorphism of $\mathrm{Jac}(\tilde{C})$, which we also denote ρ_5. The minimal polynomial of ρ_5 is the same as that of ζ_5, so $\mathrm{End}^0(\mathrm{Jac}(\tilde{C}))$ contains the CM-field $\mathbb{Q}(\zeta_5)$.

Reducing $\tilde{C}$ modulo p, we obtain a curve C defined over $\mathbb{F}_p$. Since $p \not\equiv 1 \pmod 5$, the endomorphism ρ_5 reduces to a non-trivial endomorphism of $\mathrm{Jac}(C)$, also denoted ρ_5. This endomorphism was first used as a distortion map by Choie and Lee [**?**].

Remark. If $p \equiv 1 \pmod 5$, then $\mathrm{Jac}(C)$ is ordinary. If $p \equiv 4 \pmod 5$, then $\mathrm{Jac}(C)$ is supersingular but not simple. This explains our restriction to $p \equiv 2, 3 \pmod 5$.

Lemma 4.1. *The Jacobian $\mathrm{Jac}(C)$ is $\mathbb{F}_p$-simple, supersingular, and has embedding degree 4.*

Proof. Observe that 5 does not divide $p - 1$, so for each value of y in $\mathbb{F}_p$ there is a unique value $x = (y^2 - 1)^{1/5}$ yielding a point (x, y) in $C(\mathbb{F}_p)$. Since C has a single point at infinity, we have $\#C(\mathbb{F}_p) = p + 1$. Similarly, since 5 does not divide $p^2 - 1$, we obtain $\#C(\mathbb{F}_{p^2}) = p^2 + 1$. It follows that $\#\mathrm{Jac}(C)(\mathbb{F}_p) = p^2 + 1$, and that the characteristic polynomial of the p-power Frobenius endomorphism π on $\mathrm{Jac}(C)$ is $P(T) = T^4 + p^2$. This polynomial is irreducible over $\mathbb{Z}$, so $\mathrm{Jac}(C)$ is simple (but not absolutely simple). We may also deduce from the form of $P(T)$ that C is supersingular (see [**?**, **?**]).

It remains to compute the embedding degree. If r is an odd prime dividing $\#\mathrm{Jac}(C)(\mathbb{F}_p)$, then r divides $p^2 + 1$; hence r divides $p^4 - 1$, and does not divide $p^i - 1$ for any i less than 4. We conclude that $\mathrm{Jac}(C)$ has embedding degree 4. $\square$

Our goal is to show that for any pair of divisor classes on C, there is a suitable distortion map of the form $\pi^i \rho_5^j$ for some i and j. The first step towards establishing this result is to show that the $\mathbb{Q}$-algebra $\mathrm{End}^0(\mathrm{Jac}(C))$ is generated as a $\mathbb{Q}$-module by maps of the form $\pi^i \rho_5^j$.

Consider the non-commutative subring $\mathbb{Z}[\rho_5, \pi]$ of $\mathrm{End}(\mathrm{Jac}(C))$ generated by ρ_5 and π. We let $\mathbb{Q}[\rho_5, \pi]$ denote the non-commutative $\mathbb{Q}$-algebra $\mathbb{Z}[\rho_5, \pi] \otimes_{\mathbb{Z}} \mathbb{Q}$. Since $\mathbb{Z}[\rho_5, \pi]$ is a finitely generated $\mathbb{Z}$-module, $\mathbb{Q}[\rho_5, \pi]$ is a finite dimensional $\mathbb{Q}$-vector space. Note that since the characteristic polynomial of π has nonzero constant term, there exists an element π^{-1} of $\mathbb{Q}[\rho_5, \pi]$ such that $\pi^{-1}\pi = \pi\pi^{-1} = 1$.

Lemma 4.2. *Let π and ρ_5 be as above. Then $\pi^j \rho_5 \pi^{-j} = \rho_5^{(p^j)}$ for all $j \geq 0$.*

Proof. Clearly $\pi^j \rho_5(x, y) = (\zeta_5^{(p^j)} x^{(p^j)}, y^{(p^j)}) = \rho_5^{(p^j)} \pi^j(x, y).$ $\square$

Lemma **??** implies that conjugation by π in the algebra $\mathbb{Q}[\rho_5, \pi]$ is an algebra automorphism of order 4 fixing $\mathbb{Q}(\rho_5)$, and so corresponds to a generator σ of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\rho_5)/\mathbb{Q})$. Let $\rho_5^{\sigma^j}$ denote the map $\sigma^j(\rho_5)$. Since $\mathrm{Gal}(\mathbb{Q}(\rho_5)/\mathbb{Q})$ is cyclic of order 4, the maps $\rho_5^{\sigma^j}$ are distinct for $0 \leq j \leq 3$.

Proposition 4.3. *As a $\mathbb{Q}$-vector space, $\mathbb{Q}[\rho_5, \pi]$ has a direct sum decomposition*

$$\mathbb{Q}[\rho_5, \pi] = \mathbb{Q}(\rho_5) \oplus \pi\mathbb{Q}(\rho_5) \oplus \pi^2\mathbb{Q}(\rho_5) \oplus \pi^3\mathbb{Q}(\rho_5).$$

Proof. We will prove by induction that the sum $\bigoplus_{i=0}^{t} \pi^i \mathbb{Q}(\rho_5)$ is direct for each $0 \leq t \leq 3$. For $t = 0$ there is nothing to prove. For the inductive step, assume $U_n = \bigoplus_{i=0}^{n} \pi^i \mathbb{Q}(\rho_5)$ is direct for $0 \leq n \leq 2$; we will show that $U_n \cap \pi^{n+1}\mathbb{Q}(\rho_5) = \{0\}$. Suppose the contrary: then there is a non-zero z in $\mathbb{Q}(\rho_5)$ such that $\pi^{n+1}z$ is in U_n. Dividing by z, we can write $\pi^{n+1} = z_0 + \pi z_1 + \cdots + \pi^n z_n$, with coefficients z_i in $\mathbb{Q}(\rho_5)$ for $0 \leq i \leq n$, and with at least one of the z_i not zero. Let σ be a generator of $\mathrm{Gal}(\mathbb{Q}(\rho_5)/\mathbb{Q})$ satisfying $\rho_5^\sigma = \rho_5^p$. Lemma **??** implies $\rho_5^{\sigma^j}\pi = \pi\rho_5^{\sigma^{j-1}}$, and thus $\rho_5^{\sigma^{(n+1)}}\pi^{n+1} = \pi^{n+1}\rho_5$. Hence

$$\begin{aligned}
0 &= \rho_5^{\sigma^{n+1}}\pi^{n+1} - \pi^{n+1}\rho_5 \\
&= \rho_5^{\sigma^{n+1}}(z_0 + \pi z_1 + \cdots + \pi^n z_n) - (z_0\rho_5 + \pi z_1\rho_5 + \cdots + \pi^n z_n\rho_5) \\
&= z_0\rho_5^{\sigma^{n+1}} + \pi z_1\rho_5^{\sigma^n} + \cdots + \pi^n z_n\rho_5^{\sigma^1} - z_0\rho_5 - \pi z_1\rho_5 - \cdots - \pi^n z_n\rho_5 \\
&= z_0(\rho_5^{\sigma^{n+1}} - \rho_5) + \pi z_1(\rho_5^{\sigma^n} - \rho_5) + \cdots + \pi^n z_n(\rho_5^{\sigma} - \rho_5).
\end{aligned}$$

But U_n is a direct sum, and $\rho_5^{\sigma^j} \neq \rho_5$ for $1 \leq j \leq 3$; hence $z_0 = z_1 = \cdots = z_t = 0$, which is a contradiction. $\square$

Corollary 4.4. *We have*

$$\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\rho_5, \pi] = \left\{ \sum_{0 \leq i,j \leq 3} \lambda_{i,j}\pi^i\rho_5^j : \lambda_{i,j} \in \mathbb{Q} \right\}.$$

Proof. We know $\mathbb{Q}(\rho_5)$ is a 4-dimensional $\mathbb{Q}$-vector space, so by Proposition **??** $\mathbb{Q}[\rho_5, \pi]$ is a 16-dimensional $\mathbb{Q}$-vector subspace of $\mathrm{End}^0(\mathrm{Jac}(C))$. But $\mathrm{End}^0(\mathrm{Jac}(C))$ is itself 16-dimensional, so $\mathbb{Q}[\rho_5, \pi] = \mathrm{End}^0(\mathrm{Jac}(C))$. The second equality then follows on noting that $\{1, \rho_5, \rho_5^2, \rho_5^3\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\rho_5)$. $\square$

Theorem **??** implies the existence of a distortion map ϕ for every pair (D_1, D_2) of non-trivial points of order r on $\mathrm{Jac}(C)$: that is, an endomorphism ϕ such that $e_r(D_1, \phi(D_2)) \neq 1$. Now $\mathrm{End}(\mathrm{Jac}(C))$ is an order in $\mathbb{Q}[\rho_5, \pi]$ containing $\mathbb{Z}[\rho_5, \pi]$, so by Corollary **??** there exist rational numbers $\lambda_{i,j}$ such that $\phi = \sum_{i,j} \lambda_{i,j}\pi^i\rho_5^j$ in $\mathbb{Q}[\rho_5, \pi]$. Let m denote the least common multiple of the denominators of the $\lambda_{i,j}$; note that the endomorphism $m\phi$ is an element of $\mathbb{Z}[\rho_5, \pi]$.

Assumption 1. We assume that ϕ may be chosen such that $\gcd(m, r) = 1$, where ϕ, m and r are defined as above.

Remark. Assumption **??** holds if $\mathbb{Z}[\rho_5, \pi]$ is "most" of $\mathrm{End}(\mathrm{Jac}(C))$, and seems to hold in practical examples. However, we have not proven that it is always satisfied for the curves under consideration. It is instructive to consider Assumption **??** in the case where $\mathrm{Jac}(C)$ is a supersingular elliptic curve E. In this case, $\mathrm{End}(E)$ is a maximal order $\mathcal{O}$ in a quaternion algebra $B = \mathbb{Q}[\pi, \psi]$ where π is the q-power Frobenius and ψ is some other endomorphism. Note that $\alpha\mathcal{O}\alpha^{-1}$ is a maximal order

in B for every α in B; so maximal orders in B can be very far from $\mathbb{Z}[\pi, \psi]$. Thus Assumption **??** may not be true in general. However, following the arguments of [**?**], we may suppose that E has been constructed by the CM method, in which case $\psi^2 = -d$ for some relatively small positive integer d. Hence $\mathbb{Z}[\pi, \psi]$ is contained in $\mathcal{O}$, and Assumption **??** holds when r is larger than d.

Theorem 4.5. *If Assumption* **??** *holds, then for all pairs* (D_1, D_2) *of non-zero divisor classes on C of order r and all non-degenerate pairings e_r there exists a distortion map of the form $\pi^i \rho_5^j$ with $0 \le i, j \le 3$.*

Proof. Theorem **??** shows that there exists an endomorphism ϕ that is a suitable distortion map for (D_1, D_2); Corollary **??** shows that ϕ is in $\mathbb{Q}[\rho_5, \pi]$. Under Assumption **??**, we may take an integer m prime to r such that $m\phi$ is in $\mathbb{Z}[\rho_5, \pi]$ and
$$e_r(D_1, m\phi(D_2)) = e_r(D_1, \phi(D_2))^m \ne 1;$$
so $m\phi$ is also a distortion map for (D_1, D_2). Since $m\phi$ is an integer combination of the $\pi^i \rho_5^j$, we must have $e_r(D_1, \pi^i \rho_5^j(D_2)) \ne 1$ for some $0 \le i, j \le 3$ (otherwise, if all $e_r(D_1, \pi^i \rho_5^j(D_2)) = 1$, then $e_r(D_1, m\phi(D_2)) = 1$ by the linearity of the pairing). $\square$

Remark. Alternatively, one could use maps of the form $\rho_5^i \pi^j$ in Theorem **??**.

Example. Let D_1 be a nonzero element of $\mathrm{Jac}(C)[r]$ defined over $\mathbb{F}_p$; note that $\pi(D_1) = D_1$. It is easy to show that, under Assumption **??**, $e_r(D_1, \rho_5^j(D_1)) \ne 1$ for some $1 \le j \le 3$. This supports the suggestion in [**?**] of using ρ_5 as a distortion map. When implementing pairings, it is desirable to utilise denominator elimination to improve efficiency; to this end, the map ρ_5^j might be combined with a trace operation (see Scott [**?**] for an example of this in the elliptic case).

Remark. The results in this section easily generalise to the twists $y^2 = x^5 + A$ of C (for nonzero A), and even more generally to the curves $y^2 = x^{2n+1} + A$ over $\mathbb{F}_p$, where $2n + 1$ is prime and p is a primitive root modulo $2n + 1$.

5. CURVES WITH EMBEDDING DEGREE 4: OTHER CM CURVES

In [**?**] and [**?**], van Wamelen describes the 19 isomorphism classes of curves of genus 2 over $\mathbb{Q}$ whose Jacobians have CM by the ring of integers of a CM-field. For each isomorphism class, van Wamelen provides a representative curve $\tilde{C}_i$ defined over $\mathbb{Q}$, the CM-field $F_i := \mathrm{End}^0(\mathrm{Jac}(\tilde{C}_i))$, and an explicit partial description of an endomorphism α_i of $\mathrm{Jac}(\tilde{C}_i)$ such that $F_i = \mathbb{Q}(\alpha_i)$, giving the ($x$-coordinates of) the image under α_i of the image of a generic point (x, y) of $\tilde{C}_i$ in $\mathrm{Jac}(\tilde{C}_i)$. One can derive a full description of the endomorphism α_i from this information (see Pujolàs [**?**] for details).

The curve $\tilde{C}$ of Section **??** is a representative of the isomorphism class corresponding to the CM-field $\mathbb{Q}(\zeta_5)$ in van Wamelen's tables. In this section, we generalize our treatment of $\tilde{C}$ to the other CM curves $\tilde{C}_i$. Reducing each $\tilde{C}_i$ modulo suitable inert primes p, we obtain curves C_i over $\mathbb{F}_p$ whose Jacobians are simple, supersingular, and whose characteristic polynomial of Frobenius is equal to $T^4 + p^2$. These Jacobians therefore have a very similar endomorphism structure to that of the Jacobian in Section **??**.

Let $\tilde{\alpha}_i$ be an endomorphism of $\mathrm{Jac}(\tilde{C}_i)$ such that $\mathrm{End}^0(\mathrm{Jac}(\tilde{C}_i)) \cong \mathbb{Q}(\tilde{\alpha}_i)$; the endomorphism supplied by van Wamelen suffices. Note that $\tilde{\alpha}_i$ is defined over the

quartic field F_i, which has cyclic Galois group over $\mathbb{Q}$ for all of the curves in [?]. Let α_i denote the image of $\tilde{\alpha}_i$ in $\mathrm{End}(\mathrm{Jac}(C_i))$. Since p is inert in the cyclic quartic field F_i, it follows that α_i is defined over $\mathbb{F}_{p^4}$.

If π is the p-power Frobenius map then, as before, we have

$$\pi\alpha_i\pi^{-1} = \alpha_i^{(p)}$$

where $\alpha_i^{(p)}$ denotes the map obtained from α_i by applying the p-power Frobenius to the coefficients of α_i. It follows that conjugation by π generates $\mathrm{Gal}(\mathbb{Q}(\alpha_i)/\mathbb{Q})$. We may therefore prove an analogue of Proposition ?? for each curve C_i.

Proposition 5.1. *The non-commutative $\mathbb{Q}$-algebra $\mathbb{Q}[\alpha_i, \pi]$ generated by α_i and π is a 16-dimensional $\mathbb{Q}$-vector space, and (as $\mathbb{Q}$-vector spaces)*

$$\mathbb{Q}[\alpha_i, \pi] = \mathbb{Q}(\alpha_i) \oplus \pi\mathbb{Q}(\alpha_i) \oplus \pi^2\mathbb{Q}(\alpha_i) \oplus \pi^3\mathbb{Q}(\alpha_i).$$

As a result, under the appropriate analogue of Assumption ??, we may choose a distortion map of the form $\pi^u\alpha_i^v$ with $0 \le u, v \le 3$ for any pair of elements of $\mathrm{Jac}(C_i)[r]$. The van Wamelen curves are therefore suitable for cryptography, in the sense that one can easily find a distortion map for every pair of divisors.

Remark. In practice, evaluating the maps α_i of [?] is relatively complicated, making the distortion maps of the curves in this section relatively inefficient compared with those of the CM curve $y^2 = x^5 + 1$ described in Section ??.

Remark. One could also construct curves with distortion maps by reducing CM curves defined over number fields other than $\mathbb{Q}$.

6. Curves with embedding degree 5

The curves $C : y^2 = x^p - x + b$ over $\mathbb{F}_p$ with $b = \pm 1$ have been studied by Duursma and Sakurai [?], and efficient pairing computation on these curves was studied by Duursma and Lee [?]. Our interest is in the genus 2 case, so in this section we consider the curves

$$C : y^2 = x^5 - x + b$$

over $\mathbb{F}_q$, where $q = 5^m$ for some m coprime to 10, and $b = \pm 1$. The distortion map proposed by Duursma and Lee [?] is

$$\psi(x, y) = (\rho - x, 2y),$$

where ρ is an element of $\mathbb{F}_{5^5}$ such that $\rho^5 - \rho + 2b = 0$.

The characteristic polynomial of the (q-power) Frobenius for these curves is

$$P_m^\pm(T) = T^4 \pm 5^{(m+1)/2}T^3 + 3 \cdot 5^m T^2 \pm 5^{(3m+1)/2}T + 5^{2m}.$$

Observe that

$$P_m^+(T)P_m^-(T) = T^8 + qT^6 + q^2T^4 + q^3T^2 + q^4,$$

and hence that $(T^2 - q)P_m^+(T)P_m^-(T) = T^{10} - q^5$. Let $N := \#\mathrm{Jac}(C)(\mathbb{F}_q)$. Since N is equal to either $P_m^+(1)$ or $P_m^-(1)$, it follows that N divides $q^5 - 1$; hence the embedding degree is $k = 5$ for large prime-order subgroups of $\mathrm{Jac}(C)(\mathbb{F}_q)$. Note that the characteristic polynomial of the q^5-power Frobenius is $(T^2 - 5^{5m})^2$, and that the full N-torsion is defined over $\mathbb{F}_{q^{10}}$ but not over $\mathbb{F}_{q^5}$. Since $\mathrm{Jac}(C)(\mathbb{F}_{q^k})[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, this case is as easily handled as the elliptic curve case in Section ??.

Lemma 6.1. *If D_1 and D_2 are non-zero points of prime order r in $\mathrm{Jac}(C)(\mathbb{F}_q)$, then ψ is a suitable distortion map with respect to the Tate pairing.*

Proof. As in the elliptic curve case, the pairing of D_1 with D_2 is defined over $\mathbb{F}_q$, and is therefore trivial. On the other hand, $\psi(D_2)$ is a non-zero r-torsion divisor which is not defined over $\mathbb{F}_q$. Thus $\{D_1, \psi(D_2)\}$ is a basis for $\mathrm{Jac}(C)(\mathbb{F}_{q^k})[r]$, and by non-degeneracy of the Tate pairing we have $e_r(D_1, \psi(D_2)) \neq 1$. □

Remark. Note that Lemma **??** is only stated for the Tate pairing. This is because while the Tate pairing is known to be non-degenerate for points defined over the field $\mathbb{F}_q(\mu_r) = \mathbb{F}_{q^5}$, we are only guaranteed that the Weil pairing is non-degenerate when working over $\mathbb{F}_q(\mathrm{Jac}(C)[r]) = \mathbb{F}_{q^{10}}$.

If C is a curve defined over $\mathbb{F}_q$, then for any integer n there is a natural homomorphism $\mathrm{Tr} : \mathrm{Jac}(C)(\mathbb{F}_q^n) \to \mathrm{Jac}(C)(\mathbb{F}_q)$ defined by

$$\mathrm{Tr}(D) := \sum_{i=0}^{n-1} \pi^n(D).$$

This map is called the *trace* (of Frobenius); its kernel is called the *trace-zero subgroup* of $\mathrm{Jac}(C)(\mathbb{F}_q)$.

Lemma 6.2. *If D is a point in $\mathrm{Jac}(C)(\mathbb{F}_q)$, then $\psi(D)$ lies in the trace-zero subgroup of $\mathrm{Jac}(C)(\mathbb{F}_{q^5})$.*

Proof. We first prove the result for divisors of the form $D = (P) - (\infty)$ where P is a point in $C(\mathbb{F}_q)$. Observe that the y-coordinate of $\psi(P)$ is in $\mathbb{F}_q$. Hence the y-coordinates of $\pi^j(\psi(P))$ for $0 \leq j \leq 4$ are all equal, say to some y_0, while the x-coordinates are all distinct. The function $(y - y_0)$ on C therefore has divisor equal to $(\psi(P)) + (\pi(\psi(P))) + \cdots + (\pi^4(\psi(P))) - 5(\infty)$, which is the trace of $(\psi(P)) - (\infty) = \psi(D)$. Hence, the trace of $\psi(D)$ is zero.

The same argument applies to divisors of the form $(P_1) + (P_2) - 2(\infty)$ where P_1 and P_2 are in $C(\mathbb{F}_q)$. A similar argument applies when P_1 and P_2 are Galois conjugates in $C(\mathbb{F}_{q^2})$: the y-coordinates of the $\pi^j(\psi(P_i))$ take either the same value 10 times, or two different values 5 times each. □

Using Lemmas **??** and **??**, it immediately follows (as in [**?**, **?**]) that ψ and combinations of π^j are sufficient as distortion maps for all pairs of points of order r in $\mathrm{Jac}(C)(\mathbb{F}_{q^5})$. On the other hand, since $\psi^2 = -1$, it is clear that $\mathbb{Q}[\pi, \psi]$ is a $\mathbb{Q}$-algebra of dimension 8; so combinations of π and ψ are not sufficient to act as distortion maps for all pairs of points in $\mathrm{Jac}(C)[r]$.

To obtain generators for the full endomorphism ring we use the fact that C is isomorphic over $\mathbb{F}_{5^5}$ to the curve $C' : Y^2 = X^5 - X$ (the isomorphism is $\eta(x, y) = (x - \alpha, y)$ where $\alpha \in \mathbb{F}_5$ satisfies $\alpha^5 - \alpha + b = 0$). On C' we have the automorphism $\phi'(X, Y) = (2X, \beta Y)$ where $\beta \in \mathbb{F}_{5^2}$ satisfies $\beta^2 = 2$. Defining $\phi = \eta^{-1}\phi'\eta$ gives the automorphism

$$\phi(x, y) = (2x - \alpha, \beta y)$$

on C. Since ϕ is not defined over $\mathbb{F}_{5^5}$ it follows that ϕ does not lie in $\mathbb{Q}[\pi, \psi]$ and hence $\mathbb{Q}[\pi, \psi, \phi] = \mathrm{End}^0(\mathrm{Jac}(C))$. It follows that if the Weil pairing is used then a distortion map of the form $\pi^u \psi^v \phi^w$ with $0 \leq u \leq 3, 0 \leq v, w \leq 1$ may be used.

Remark. Since the embedding degree is odd, the fact that the image of the distortion map is a trace zero divisor does not mean that the usual denominator elimination techniques for pairing implementation may be used. However, the ate pairing approach (see [**?**, **?**]) may be used to obtain a very simple pairing algorithm, with no final exponentiation required. This does not imply that characteristic 5 curves are fast for pairing-based cryptography, since 5 is not a very natural base for computer implementation of finite field arithmetic.

7. Curves with embedding degree 6

Let p be an odd prime such that $p \equiv 2 \pmod{3}$. Let ζ_6 be a primitive sixth root of unity over $\mathbb{F}_p$, and set $\zeta_3 := \zeta_6^2$.

We wish to construct a curve $C'/\mathbb{F}_p$ with embedding degree 6. The characteristic polynomial of Frobenius on $\mathrm{Jac}(C')$ must therefore be $T^4 - pT^2 + p^2$. Following [**?**, p.32], we obtain C' by twisting the curve $C : y^2 = x^6 + 1$ with respect to its automorphism $u : (x, y) \mapsto (\zeta_3/x, y/x^3)$. To find a defining equation for C', we need to find an isomorphism $\phi : C' \to C$ defined over $\overline{\mathbb{F}}_p$ such that $\phi^{(p)} \circ \phi^{-1} = u$. We can assume ϕ is of the form

$$\phi(X, Y) = (x, y) = \left(\frac{aX + b}{cX + d}, \frac{Y}{(cX + d)^3} \right),$$

with $ad - bc \neq 0$; the curve C' will then have a defining equation

$$C' : Y^2 = (aX + b)^6 + (cX + d)^6.$$

We need $\phi^{(p)} = u \circ \phi$ — that is,

$$\left(\frac{a^p X + b^p Z}{c^p X + d^p Z}, \frac{Y}{(c^p X + d^p Z)^3} \right) = \left(\frac{\zeta_3 cX + \zeta_3 dZ}{aX + bZ}, \frac{Y}{(aX + bZ)^3} \right).$$

To find particular solutions for a, b, c and d we begin by setting $a = c^p$ and $b = d^p$. Now $a^p = \zeta_3 c$ and $b^p = \zeta_3 d$, so we need values for c and d such that

$$c^{p^2 - 1} = d^{p^2 - 1} = \zeta_3.$$

Therefore, we choose some γ in $\overline{\mathbb{F}}_p$ satisfying $\gamma^{p^2 - 1} = \zeta_3$, and set $c = \gamma$. One can show that $\gamma \in \mathbb{F}_{p^6}$. Note that $(c/d)^{p^2 - 1} = 1$, so c/d is an element of $\mathbb{F}_{p^2}$. On the other hand, we know $ad \neq bc$, so $c^p d \neq d^p c$: hence c/d is not an element of $\mathbb{F}_p$. Therefore, setting $d = \zeta_3 c$, we obtain a solution

$$a = \gamma^p, \quad b = \zeta_3^{-1} \gamma^p, \quad c = \gamma, \text{ and } d = \zeta_3 \gamma.$$

We want to find suitable distortion maps for $\mathrm{Jac}(C')$. We could proceed as in Section **??**, and obtain a conditional result depending on the final assumption about the denominators. However, since C' is isomorphic to C, we can consider the problem of finding distortion maps for $\mathrm{Jac}(C)$ instead: indeed, if $A \subset \mathrm{End}(\mathrm{Jac}(C))$ is a suitable set of distortion maps for $\mathrm{Jac}(C)$, then $\phi^{-1} A \phi$ will be a suitable set of distortion maps for $\mathrm{Jac}(C')$. This approach allows us to take advantage of the splitting behaviour of $\mathrm{Jac}(C)$, and thus to obtain an unconditional result.

Let E be the elliptic curve defined over $\mathbb{F}_p$ by $E : y^2 = x^3 + 1$, and let π_E denote the p-power Frobenius on E. The curve E has an automorphism ρ_3 defined over $\mathbb{F}_{p^2}$ by $(x, y) \mapsto (\zeta_3 x, y)$.

Lemma 7.1. *With E, ρ_3 and π_E as above,*

    (1) *E is supersingular,*

(2) *the characteristic polynomial of π_E is $X^2 + p$, and*
(3) $\mathbb{Z}[\pi_E, \rho_3]$ *is an order of index 3 in* $\mathrm{End}(E)$.

Proof. One easily checks that $\pi_E \circ \rho_3 \neq \rho_3 \circ \pi_E$ when $p \equiv 2 \pmod 3$, so $\mathrm{End}(E)$ is non-commutative; it follows that E is supersingular. The characteristic polynomial of π_E has the form $T^2 - tT + p$, where $-2\sqrt{p} \leq t \leq 2\sqrt{p}$; but since E is supersingular, p divides t [**?**, Theorem V.3.1], and the only such t is 0. Hence the characteristic polynomial of Frobenius is $T^2 + p$. Since E is supersingular, $\mathrm{End}(E)$ is isomorphic to a maximal order of the quaternion algebra ramified at p and ∞; its discriminant is therefore p [**?**, Corollary 5.3]. Explicit calculation shows that $\mathbb{Z}[\pi_E, \rho_3]$ is an order of discriminant $3p$, and thus an order of index 3 in $\mathrm{End}(E)$. $\square$

Let $f : C \to E$ (resp. $f' : C \to E$) be the morphism defined by $f(x, y) = (x^2, y)$ (resp. $f'(x, y) = (1/x^2, y/x^3)$). Since $f^*(dx/y) = 2x \, dx/y$ and $f'^*(dx/y) = -2dx/y$, the morphism

$$\mu = (f^* + f'^*) : E \times E \to \mathrm{Jac}(C)$$

is a $(2, 2)$-isogeny. Let $\tilde{\mu} = (f_*, f'_*) : \mathrm{Jac}(C) \to E \times E$. We have $\tilde{\mu} \circ \mu = [2]_{E \times E}$ and $\mu \circ \tilde{\mu} = [2]_{\mathrm{Jac}(C)}$. We can define an injective (group) homomorphism

$$T : \mathrm{End}(\mathrm{Jac}(C)) \longrightarrow \mathrm{End}(E \times E)$$
$$\psi \longmapsto \tilde{\mu} \circ \psi \circ \mu.$$

While T is not a ring homomorphism, one easily checks that

$$T(\psi)T(\psi') = 2T(\psi\psi')$$

for all endomorphisms ψ and ψ' of $\mathrm{Jac}(C)$.

Let χ and ρ_6 be the automorphisms of C defined by

$$\chi(x, y) = (1/x, y/x^3) \quad \text{and} \quad \rho_6(x, y) = (\zeta_6 x, y);$$

we use the same notations for the induced endomorphisms of $\mathrm{Jac}(C)$. Let π_C denote the p-power Frobenius on C, and let $A = \mathbb{Z}[\pi_C, \chi, \rho_6]$ be the subring of $\mathrm{End}(\mathrm{Jac}(C))$ generated by π_C, χ, and ρ_6. We will compute an upper bound for the index of $T(A)$ in $\mathrm{End}(E \times E) = M_2(\mathrm{End}(E))$. It suffices to compute the images of π_C, χ, and ρ_6.

Lemma 7.2. *The images of π_C, χ, and ρ_6 in $\mathrm{End}(E \times E)$ are given by*

$$T(\pi_C) = 2 \begin{pmatrix} \pi_E & 0 \\ 0 & \pi_E \end{pmatrix}, \quad T(\chi) = 2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad and \quad T(\rho_6) = 2 \begin{pmatrix} \rho_3 & 0 \\ 0 & -\rho_3^2 \end{pmatrix}.$$

Proof. We show this for ρ_6, the other computations being similar. Consider a point (x^2, y) on E. We have $f^*(x^2, y) = (x, y) + (-x, y)$ in $\mathrm{Jac}(C)$, so

$$\rho_6 \circ f^*(x^2, y) = (\zeta_6 x, y) + (-\zeta_6 x, y).$$

Now

$$\begin{aligned}
f_* \circ \rho_6 \circ f^*(x^2, y) &= ((\zeta_6 x)^2, y) + ((-\zeta_6 x)^2, y) \\
&= 2(\zeta_3 x^2, y) \\
&= ([2] \circ \rho_3)(x^2, y)
\end{aligned}$$

whereas

$$\begin{aligned}
(f'_* \circ \rho_6 \circ f^*)(x^2, y) &= \left(1/(\zeta_6 x)^2, y/(\zeta_6 x)^3\right) + \left(1/(-\zeta_6 x)^2, y/(-\zeta_6 x)^3\right) \\
&= \left(1/(\zeta_3 x), -y/x^3\right) + \left(1/(\zeta_3 x), y/x^3\right) \\
&= 0.
\end{aligned}$$

In the same way , $f'^* \left(1/x^2, y/x^3 \right) = (x,y) + (-x,-y)$, so

$$
\begin{aligned}
(f'_* \circ \rho_6 \circ f'^*) \left(1/x^2, y/x^3 \right) &= \left(1/(\zeta_6 x)^2, y/(\zeta^6 x)^3 \right) + \left(1/(-\zeta_6 x)^2, -y/(-\zeta^6 x)^3 \right) \\
&= \left(1/(\zeta_3 x), -y/x^3 \right) + \left(1/(\zeta_3 x), -y/x^3 \right) \\
&= ([-2] \circ \rho_3^2) \left(1/x^2, y/x^3 \right)
\end{aligned}
$$

whereas $(f_* \circ \rho_6 \circ f'^*) \left(1/x^2, y/x^3 \right) = 0$. $\hfill\square$

Using Lemma **??**, we see that the images of $1 + \rho_6^3$, $1 - \rho_6^3$, $\chi + \chi\rho_6^3$ and $\chi - \chi\rho_6^3$ in $\mathrm{End}(E \times E)$ are the "projectors"

$$
4 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ 4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \ 4 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ \text{and} \ 4 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.
$$

Composing with the images of π_C and ρ_6, we get

$$
M_2(4\mathbb{Z}[\pi_E, \rho_3]) \subset T(A) \subset (M_2(\mathrm{End}(E)).
$$

Since $\mathbb{Z}[\pi_E, \rho_3]$ has index 3 in $\mathrm{End}(E)$, the index of $T(A)$ in $M_2(\mathrm{End}(E))$ divides $2^8 \cdot 3^4$. Now, suppose r is a prime different from p, 2 and 3. Following the proof of Theorem **??**, by tensoring with $\mathbb{Z}/r\mathbb{Z}$ we get an isomorphism

$$
T_r : \mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} M_2(\mathrm{End}(E)) \otimes \mathbb{Z}/r\mathbb{Z} \simeq M_4(\mathbb{Z}/r\mathbb{Z})
$$

and $T_r(A)$ is of index dividing $2^8 \cdot 3^4$ in $M_4(\mathbb{Z}/r\mathbb{Z})$. Thus, if D_1 and D_2 are non-zero elements of $\mathrm{Jac}(C)[r]$, we can find a map Φ in $M_4(\mathbb{Z}/r\mathbb{Z})$ such that $e_r(D_1, \Phi(D_2)) \neq 1$. Then $2^8 \cdot 3^4 \Phi = T_r(\psi)$ for some ψ in A, and

$$
e_r(D_1, \psi(D_2)) = e_r(D_1, [2^8 \cdot 3^4]\Phi(D_2)) = e_r(D_1, \Phi(D_2))^{2^8 \cdot 3^4} \neq 1.
$$

We have proven the following theorem.

Theorem 7.3. *Let r be a prime different from 2, 3 and p. For all pairs D_1, D_2 of non-zero elements of $\mathrm{Jac}(C')[r]$, there exists a suitable distortion map in the ring $\phi^{-1}\mathbb{Z}[\pi_C, \chi, \rho_6]\phi$.*

Remark. Using the construction of [**?**, p. 12] with the group-scheme isomorphism $\eta : E[2] \to E[2]$ mapping $(-1, 0)$ to itself and $(\zeta_6, 0)$ to $(1/\zeta_6, 0)$, we have $\mathrm{Jac}(C) \simeq (E \times E)/\mathrm{Graph}(\eta)$. Moreover, if λ is the canonical polarization on $\mathrm{Jac}(C)$ and $\lambda_{E \times E}$ the split polarization on $E \times E$, then $\lambda_{E \times E} = \hat{\mu}(2\lambda)\mu$. Thus if D_1 and D_2 are elements of $\mathrm{Jac}(C)[r]$, then

$$
\begin{aligned}
e_r^\lambda(D_1, D_2)^8 &= e_r^{2\lambda}(2D_1, 2D_2) = e_r^{2\lambda}(\mu\tilde{\mu}D_1, \mu\tilde{\mu}D_2) \\
&= e_r^{\lambda_{E \times E}}(\tilde{\mu}D_1, \tilde{\mu}D_2) \\
&= e_r^{\lambda_E}(f_*(D_1), f_*(D_2)) \cdot e_r^{\lambda_E}(f'_*(D_1), f'_*(D_2)).
\end{aligned}
$$

In particular, pulling back two divisors on $\mathrm{Jac}(C')$ first to $\mathrm{Jac}(C)$ and then to $E \times E$, we see that the computation of the pairing on $\mathrm{Jac}(C')$ is in fact equivalent to the computation of twice the pairing on the elliptic curve E.

8. Curves with embedding degree 12

The curves $C : y^2 + y = x^5 + x^3 + b$ over $\mathbb{F}_{2^m}$ with $b = 0, 1$ were studied by van der Geer and van der Vlugt in [**?**] and [**?**], in view of their applications to coding theory. Throughout this section, the ground field is $\mathbb{F}_{2^m}$, where $m \equiv \pm 1 \pmod 6$.

The characteristic polynomial of the Frobenius endomorphism π over $\mathbb{F}_{2^m}$ is

$$
P_m^\pm(T) = T^4 \pm 2^{(m+1)/2}T^3 + 2^m T^2 \pm 2^{(3m+1)/2}T + 2^{2m},
$$

so $\mathrm{Jac}(C)$ is supersingular and simple over $\mathbb{F}_{2^m}$. We have

$$P_m^+(T)P_m^-(T) = T^8 - 2^{2m}T^4 + 2^{4m}$$

and

$$(T^8 - 2^{4m})(T^8 + 2^{2m}T^4 + 2^{4m})P_m^+(T)P_m^-(T) = T^{24} - 2^{12m},$$

so the embedding degree is $k = 12$.

Theorem **??** shows that a distortion map ϕ exists for every pair (D_1, D_2) of points in $\mathrm{Jac}(C)[r]$. We will now give a set of maps that contains a distortion map for any pair of divisors in $\mathrm{Jac}(C)(\mathbb{F}_{2^{12m}})[r]$, by exhibiting a basis of $\mathrm{End}^0(\mathrm{Jac}(C))$.

The automorphisms of C are of the form

$$\sigma_\omega : (x, y) \longmapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$$

where ω is any root of the polynomial

$$\begin{aligned}
&x^{16} + x^8 + x^2 + x \\
&= (x^6 + x^5 + x^3 + x^2 + 1)(x^3 + x^2 + 1)(x^3 + x + 1)(x^2 + x + 1)(x + 1)x,
\end{aligned}$$

and where $s_2 = \omega^8 + \omega^4 + \omega$, $s_1 = \omega^4 + \omega^2$, and s_0 is a root of $y^2 + y = \omega^5 + \omega^3$ (note that $s_0 + 1$ is the other root). For each ω, we arbitrarily fix one of the corresponding s_0, and denote the resulting automorphism σ_ω. We interpret these automorphisms as elements of $\mathrm{End}(\mathrm{Jac}(C))$. One can verify that they satisfy the relations

$$\sigma_\omega \sigma_{\omega'} = \sigma_{\omega'} \sigma_\omega = \pm \sigma_{\omega + \omega'}.$$

Fix a root τ in $\mathbb{F}_{2^6}$ of $x^6 + x^5 + x^3 + x^2 + 1$, and set $\xi = \tau^4 + \tau^2$, $\rho = \tau^2 + \tau + 1$, and $\theta = \tau^4 + \tau^2 + \tau$. Note that ξ, ρ and θ are roots of the cubic and quadratic factors above. We have $\theta^2 = \theta + 1$, $\tau^8 = \tau + 1$, and $\theta + \tau = \xi$. As before, we let $\mathbb{Z}[\pi, \sigma_\tau, \sigma_\theta]$ denote the non-commutative ring generated by π and σ_τ, and write $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = \mathbb{Z}[\pi, \sigma_\tau, \sigma_\theta] \otimes \mathbb{Q}$ for the algebra generated by π, σ_τ and σ_θ.

Proposition 8.1. *The $\mathbb{Q}$-algebra $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$ is a 16-dimensional $\mathbb{Q}$-vector space with a direct sum decomposition*

$$\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = \mathbb{Q}(\pi) \oplus \sigma_\tau \mathbb{Q}(\pi) \oplus \sigma_\theta \mathbb{Q}(\pi) \oplus \sigma_\xi \mathbb{Q}(\pi).$$

Furthermore, $\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$.

Proof. Let $F = \mathbb{Q}(\pi)$; note that F is a 4-dimensional $\mathbb{Q}$-vector space. One easily checks that the relations

$$\begin{aligned}
&\pi \sigma_\omega = \pm \sigma_{\omega^{2m}} \pi, \\
&\sigma_\tau^2 = -1, \\
&\pi^3 \sigma_\tau \pi^{-3} = \sigma_{\tau^{2^3}} = \sigma_{\tau+1} = \pm \sigma_\tau \sigma_1, \text{ and} \\
&\pi \sigma_\theta \pi^{-1} = \pm \sigma_{\theta^2} = \pm \sigma_{\theta+1} = \pm \sigma_1 \sigma_\theta
\end{aligned}$$

hold, where σ_1 is the automorphism $(x, y) \mapsto (x + 1, y + x^2)$.

Let $A := F \oplus \sigma_\tau F$; the sum is direct, because σ_τ is not in F. We see that A is an 8-dimensional $\mathbb{Q}$-vector space. Note that A is not an algebra.

We now show that $A \oplus \sigma_\xi F$ is direct. Assume the contrary: that is, that there is some non-zero z in F such that $\sigma_\xi z$ lies in A. Dividing by z, we must have

$$\sigma_\xi = z_1 + \sigma_\tau z_2$$

for some z_1 and z_2 in F. Now, since $\xi \in \mathbb{F}_{2^3}$ we have $\sigma_\xi = \pi^3 \sigma_\xi \pi^{-3}$. Using the relations above, we see

$$
\begin{aligned}
z_1 + \sigma_\tau z_2 &= \pi^3 \sigma_\xi \pi^{-3} \\
&= \pi^3 (z_1 + \sigma_\tau z_2) \pi^{-3} \\
&= z_1 + \sigma_{\tau^{2^3}} z_2 \\
&= z_1 \pm \sigma_\tau \sigma_1 z_2.
\end{aligned}
$$

Since A is a direct sum and $\sigma_1 \neq \pm 1$, we have $z_2 = 0$: that is, σ_ξ must lie in F, which is a contradiction since σ_ξ does not commute with π.

Finally, we show that $(A \oplus \sigma_\xi F) \oplus \sigma_\theta F$ is direct. Assuming the contrary, we have

$$
\sigma_\theta = z_1 + \sigma_\tau z_2 + \sigma_\xi z_3
$$

for some z_1, z_2 and z_3 in F. Again using the above relations, we have

$$
\begin{aligned}
0 &= \sigma_1 \sigma_\theta \pi^3 - \pi^3 \sigma_\theta \\
&= \sigma_1 \sigma_\theta \pi^3 - \pi^3 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \\
&= \sigma_1 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \pi^3 - (z_1 + \sigma_{\tau^{2^3}} z_2 + \sigma_{\xi^{2^3}} z_3) \pi^3 \\
&= (\sigma_1 - 1) z_1 \pi^3 + (\sigma_1 - \sigma_1) \sigma_\tau z_2 \pi^3 + (\sigma_1 - 1) \sigma_\xi z_3 \pi^3.
\end{aligned}
$$

Since $A \oplus \sigma_\xi F$ is direct, we must have $z_1 = z_3 = 0$. Therefore, $\sigma_\theta = \sigma_\tau z$ for some z in F; but this is a contradiction, since σ_θ is defined over $\mathbb{F}_{2^2}$, while σ_τ is defined over $\mathbb{F}_{2^6}$. We conclude that $(A \oplus \sigma_\xi F) \oplus \sigma_\theta F$ is direct.

Thus $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = F \oplus \sigma_\tau F \oplus \sigma_\xi F \oplus \sigma_\theta F$, and is therefore a 16-dimensional $\mathbb{Q}$-vector space. Since $\mathrm{End}^0(\mathrm{Jac}(C))$ is 16-dimensional and contains $\mathbb{Q}(\pi, \sigma_\tau, \sigma_\theta)$, we have $\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$. $\qquad\square$

Our claim that a distortion map for any pair of divisors may be chosen from the maps π, σ_τ, and σ_θ follows. Indeed, for any pair of points (D_1, D_2) in $\mathrm{Jac}(C)[r]$, we may choose a distortion map ϕ as a $\mathbb{Q}$-linear combination of the endomorphisms π^i, $\pi^j \sigma_\tau$, $\pi^k \sigma_\theta$ and $\pi^l \sigma \xi$. If we assume that we may choose coefficients such that the least common multiple m of their denominators is coprime to r, then $m\phi$ lies in $\mathbb{Z}[\pi, \sigma_\tau, \sigma_\theta]$, and is a suitable distortion map.

9. Conclusions and future work

We have given several examples of distortion maps for supersingular Jacobians of genus 2 curves with embedding degree 4, 5, 6 and 12. We have proven, subject to a reasonable assumption, that these maps are sufficient for all applications.

One natural problem for future study is to show that the assumption holds for the curves considered in this paper. Another problem is to consider similar problems in the genus 3 case, although Rubin and Silverberg [?] have shown that there is little motivation for using high genus curves in pairing applications.

Acknowledgements

References

[BSS05] I. Blake, G. Seroussi and N. Smart (eds.), *Advanced topics in elliptic curve cryptography*, Cambridge (2005).

[CL04] Y.-J. Choie and E. Lee, Implementation of tate pairing on hyperelliptic curves of genus 2, in J. I. Lim and D. H. Lee (eds.), ICISC 2003, Springer LNCS 2971 (2004) 97–111.

[DS00] I. M. Duursma and K. Sakurai, Efficient algorithms for the Jacobian variety of hyperelliptic curves $y^2 = x^p - x + 1$ over a finite field of odd characteristic p, in *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 73–89. Springer-Verlag, 2000.

[DL03] I. M. Duursma and H. S. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, in C.-S. Laih (ed.), ASIACRYPT 2003, Springer LNCS 2894 (2003) 111–123.

[FR94] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.*, **52** (1994) 865–874.

[Gag03] M. Gagné, Identity-based encryption: a survey, CryptoBytes 6(1), RSA Laboratories (2003) 10–19.

[Gal01] S. D. Galbraith, Supersingular curves in cryptography, in C. Boyd (ed.) ASIACRYPT 2001, Springer LNCS 2248 (2001) 495–513.

[GR04] S. D. Galbraith and V. Rotger, Easy decision Diffie-Hellman groups, *LMS J. Comput. Math.*, **7** (2004) 201–218.

[GP05] S. D. Galbraith and J. Pujolàs, Distortion maps for genus two curves, in R. Cramer and T. Okamoto (eds.), Proceedings of a workshop on Mathematical Problems and Techniques in Cryptology, CRM Barcelona (2005) 46–58.

[Gor97] E. Z. Goren, "*On certain reduction problems concerning abelian surfaces*" Manuscripta Mathematica, **94** (1997) 33–43.

[GHOTV] R. Granger, F. Hess, R. Oyono, N. Thériault and F. Vercauteren, Ate pairing on hyperelliptic curves, in preparation.

[HSV] F. Hess, N. P. Smart and F. Vercauteren, The eta pairing revisited, *IEEE Trans. Inf. Theory.*, **52**, No. 10 (2006) 4595–4602.

[HLP00] E. W. Howe, F. Leprvost & B. Poonen, large torsion subgroups of split Jacobian if curves if genus two or three, Forum Math. **12**, (2000), 315-364.

[HMNR06] E. W. Howe, D. Maisner, E. Nart and C. Ritzenthaler, Principally polarizable isogeny classes of abelian surfaces over finite fields, preprint available on `http://front.math.ucdavis.edu/math.NT/0602650`, (2006).

[HNR06] E. W. Howe, E. Nart and C. Ritzenthaler, Jacobians in isogeny classes of abelian surfaces over finite fields, `arxiv.org` math.NT/0607515 (2006).

[Lan83] S. Lang, "*Complex Multiplication*", Die Grundlehren der matematischen Wissenchaften in Einzeldarstellungen, vol. **255**, Springer-Verlag, Berlin- Heidelberg (1983).

[Pat02] K. G. Paterson, Cryptography from pairings: a snapshot of current research, Information Security Technical Report 7(3) (2002) 41–54.

[Pat05] K. Paterson, Pairing based cryptography, Chapter 10 of [**?**].

[Puj06] J. Pujolàs, On the decisional Diffie-Hellman problem in genus 2, PhD thesis, Universitat Politècnica de Catalunya 2006.

[RS02] K. Rubin and A. Silverberg, Supersingular abelian varieties in cryptology, in M. Yung (ed.), CRYPTO 2002, Springer LNCS 2442 (2002) 336–353.

[Sco04] M. Scott, Faster identity based encryption, *Elec. Letters*, Vol. 40, No. 14 (2004) 861.

[Sil86] J. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.

[SX95] H. Stichtenoth and C. Xing, On the structure of the divisor class group of a class of curves over finite fields, *Arch. Math.*, **65** (1995) 141–150.

[Tat66] J. Tate, Endomorphisms of abelian varieties over finite fields, *Inv. Math.*, **2** (1966) 134–144.

[vdGvdV92] G. van der Geer and M. van der Vlugt, "*Supersingular Curves of Genus 2 over finite fields of Characteristic 2*" , Math. Nachr. **159** (1992), 73–81.

[vdGvdV92b] G. van der Geer and M. van der Vlugt, "*Reed-Muller codes and supersingular curves. I*" , Compositio Math. **84** (1992), 333–367.

[vWam99] P. van Wamelen, Examples of genus two CM curves defined over the rationals, *Math. Comp.*, vol. 68, no. 225 (1999) 307–320.

[vWam99b] P. van Wamelen, Proving that a genus 2 curve has complex multiplication, *Math. Comp.*, vol. 68, no. 228 (1999) 1663–1677.

[Ver01] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, in B. Pfitzmann (ed.), EUROCRYPT 2001, Springer LNCS 2045 (2001) 195–210.

[Ver04] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *J. Crypt.*, 17, No. 4 (2004) 277–296.

[Vig80] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics 800. Springer, Berlin, 1980.

MATHEMATICS DEPARTMENT, ROYAL HOLLOWAY UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, UNITED KINGDOM.

E-mail address: `Steven.Galbraith@rhul.ac.uk`

URL: `http://www.isg.rhul.ac.uk/ sdg/`

DEPARTAMENT DE MATEMÀTICA APLICADA 4, UNIVERSITAT POLITÈCNICA DE CATALUNYA, JORDI GIRONA 1-3, 08034 BARCELONA, SPAIN.

E-mail address: `jpujolas@matematica.udl.es`

INSTITUT DE MATHÉMATIQUES DE LUMINY, UMR 6206 DU CNRS, LUMINY, CASE 907, 13288 MARSEILLE, FRANCE.

E-mail address: `ritzenth@iml.univ-mrs.fr`

URL: `http://iml.univ-mrs.fr/ ritzenth/`

MATHEMATICS DEPARTMENT, ROYAL HOLLOWAY UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, UNITED KINGDOM.

E-mail address: `Ben.Smith@rhul.ac.uk`

URL: `http://www.ma.rhul.ac.uk/ bensmith/`