PAIRINGS ON JACOBIANS OF HYPERELLIPTIC CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Consider the jacobian of a hyperelliptic genus two curve defined over a finite field. Under certain restrictions on the endomorphism ring of the jacobian we give an explicit description all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on the jacobian. From this description it follows that no such pairing can be computed more efficiently than the Weil pairing.

To establish this result, we need an explicit description of the representation of the Frobenius endomorphism on the ℓ-torsion subgroup of the jacobian. This description is given. In particular, we show that if the characteristic polynomial of the Frobenius endomorphism splits into linear factors modulo ℓ, then the Frobenius is diagonalizable.

Finally, under the restriction that the Frobenius element is an element of a certain subring of the endomorphism ring, we prove that if the characteristic polynomial of the Frobenius endomorphism splits into linear factors modulo ℓ, then the embedding degree and the total embedding degree of the jacobian with respect to ℓ are the same number.

1. Introduction

In [12], Koblitz described how to use elliptic curves to construct a public key cryptosystem. To get a more general class of groups, and possibly larger group orders, Koblitz [13] then proposed using jacobians of hyperelliptic curves. Since Boney and Franklin [2] proposed an identity based cryptosystem by using the Weil pairing on an elliptic curve, pairings have been of great interest to cryptography [8]. The next natural step then was to consider pairings on hyperelliptic curves. Galbraith *et al* [9] survey the recent research on pairings on hyperelliptic curves.

The pairing in question is usually the Weil or the Tate pairing; both pairings can be computed with Miller's algorithm [16]. The Tate pairing is usually preferred because it can be computed more efficiently than the Weil pairing, cf. [7], and it is non-degenerate over a possible smaller field extension than the Weil pairing, cf. [11] and [23]. For elliptic curves, in most cases relevant to cryptography the question of non-degeneracy is not an issue, cf. [1]. This result has been generalized to any abelian variety defined over a finite field by Rubin and Silverberg [20, Theorem 3.1]. The proof in [20] uses intrinsic properties of the Frobenius endomorphism on the abelian variety. This indicates the importance of knowing the representation of the Frobenius endomorphism on torsion subgroups of the abelian variety. This representation has implicitly been given by Rück [21, proof of Lemma 4.2].

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 11G15, 14Q05, 94A60.

Key words and phrases. Jacobians of hyperelliptic curves of genus two, Frobenius endomorphism, pairings, embedding degree, complex multiplication.

Research supported in part by a PhD grant from CRYPTOMAThIC.

Cryptographically, it is essential to know the number of points on the jacobian. Currently, the *complex multiplication method* [24, 10, 4] is the only efficient method to determine the number of points of the jacobian of a genus two curve defined over a large prime field [10]. The complex multiplication method constructs a jacobian with endomorphism ring isomorphic to the ring of integers $\mathcal{O}_K$ in a *quartic CM field* K, i.e. a totally imaginary, quadratic field extension of a quadratic number field. In the present paper we consider the more general situation where $\mathcal{O}_K$ is *embedded* into the endomorphism ring.

1.1. **Notation and assumptions.** Consider a hyperelliptic curve $\mathcal{C}$ of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p. We assume that the jacobian $\mathcal{J}_\mathcal{C}$ of $\mathcal{C}$ is irreducible. Identify the q-power Frobenius endomorphism φ on $\mathcal{J}_\mathcal{C}$ with a root $\omega \in \mathbb{C}$ of the characteristic polynomial $P \in \mathbb{Z}[X]$ of φ; cf. section 4. We then assume that the ring of integers of $\mathbb{Q}(\omega)$ is *embedded* into the endomorphism ring $\mathrm{End}(\mathcal{J}_\mathcal{C})$. Let $\ell \neq p$ be a prime number dividing the order of $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$, and that $\ell \nmid q-1$.

1.2. **Results.** Under these assumptions, in section 5 we give an explicit description of all non-degenerate, bilinear, anti-symmetric, Galois-invariant pairings on the ℓ-torsion subgroup of the jacobian of a hyperelliptic curve of genus two, given by the following theorem.

Theorem 5.1 (Anti-symmetric pairings). *Let notation and assumptions be as above. Choose a basis $\mathcal{B}$ of $\mathcal{J}_\mathcal{C}[\ell]$, such that φ is represented either by a diagonal matrix or a matrix on the form given in theorem 4.2 with respect to $\mathcal{B}$. If $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is cyclic, then all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_\mathcal{C}[\ell]$ are given by the matrices*

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in \mathbb{F}_\ell^\times$$

with respect to $\mathcal{B}$.

This result implies that *the Weil pairing is non-degenerate on the same field extension as the Tate pairing*, and that *no non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_\mathcal{C}[\ell]$ can be computed more effective than the Weil pairing*. To end the description of pairings on $\mathcal{J}_\mathcal{C}$, in section 6 we give an explicit description of the Tate pairing.

The proof of Theorem 5.1 uses an explicit description of the representation of the Frobenius endomorphism on the jacobian of a hyperelliptic curve of genus two, given by the following theorem.

Theorem 4.2 (Matrix representation). *Let notation and assumptions be as above. Then either φ is diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$, or φ is represented on $\mathcal{J}_\mathcal{C}[\ell]$ by a matrix on the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix}$$

with $c \not\equiv q+1 \pmod{\ell}$ with respect to an appropriate basis of $\mathcal{J}_\mathcal{C}[\ell]$.

Perhaps even more interesting, we prove that if the characteristic polynomial of the Frobenius endomorphism splits into linear factors modulo ℓ, then the Frobenius is diagonalizable.

Theorem 4.7 (Diagonal representation). *Let notation and assumptions be as above. Then φ is diagonalizable on $\mathcal{J}_{\mathcal{C}}[\ell]$ if, and only if, the characteristic polynomial of φ splits into linear factors modulo ℓ.*

The proofs are given in section 4. Theorem 4.2 and 4.7 also holds, if $\ell \mid q-1$ and ℓ is uneven. The proofs are similar in this case, but due to the MOV-attack [15] and the attack by Frey-Rück [6], the case $\ell \mid q-1$ is not of cryptographic interest. Therefore, this case is omitted.

Finally, in section 7 we assume that the endomorphism ring of the jacobian is *isomorphic* to the ring of integers in a quartic CM field K. Assuming that the Frobenius endomorphism under this isomorphism is given by an *η-integer* and that the characteristic polynomial of the Frobenius endomorphism splits into linear factors over $\mathbb{F}_\ell$, we prove that if the discriminant of the real subfield of K is not a quadratic residue modulo ℓ, then all ℓ-torsion points are $\mathbb{F}_{q^k}$-rational. Here, k is the multiplicative order of q modulo ℓ.

2. Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $\mathcal{C} \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : \mathcal{C} \to \mathbb{P}^1$. Throughout this paper, let $\mathcal{C}$ be a hyperelliptic curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p. By the Riemann-Roch Theorem there exists a birational map $\psi : \mathcal{C} \to \mathbb{P}^2$, mapping $\mathcal{C}$ to a curve given by an equation of the form

$$y^2 + g(x)y = h(x),$$

where $g, h \in \mathbb{F}_q[x]$ are polynomials of degree at most six [3, chapter 1].

The set of principal divisors $\mathcal{P}(\mathcal{C})$ on $\mathcal{C}$ constitutes a subgroup of the degree 0 divisors $\mathrm{Div}_0(\mathcal{C})$. The jacobian $\mathcal{J}_{\mathcal{C}}$ of $\mathcal{C}$ is defined as the quotient

$$\mathcal{J}_{\mathcal{C}} = \mathrm{Div}_0(\mathcal{C})/\mathcal{P}(\mathcal{C}).$$

The jacobian is defined over $\mathbb{F}_q$, and the points on $\mathcal{J}_{\mathcal{C}}$ defined over the extension $\mathbb{F}_{q^d}$ is denoted $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^d})$.

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_{\mathcal{C}}[\ell^n] < \mathcal{J}_{\mathcal{C}}$ of elements of order dividing ℓ^n is then isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^4$, i.e. $\mathcal{J}_{\mathcal{C}}[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank four; cf. [14, Theorem 6, p. 109].

The multiplicative order of q modulo ℓ plays an important role in cryptography.

Definition (Embedding degree). Consider a prime number $\ell \neq p$ dividing the order of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$. The embedding degree of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$ with respect to ℓ is the multiplicative order of q modulo ℓ, i.e. the least number k, such that $q^k \equiv 1 \pmod{\ell}$.

Throughout this paper we consider a prime number $\ell \neq p$ dividing the order of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$, and assume that $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$ is of embedding degree $k > 1$ with respect to ℓ.

$$\begin{tikzcd}
\cdots \arrow[r, "{[\ell]}"] & \mathfrak{J}_{\mathcal{C}}[\ell^{n+1}] \arrow[r, "{[\ell]}"] \arrow[d, "\psi"] & \mathfrak{J}_{\mathcal{C}}[\ell^{n}] \arrow[r, "{[\ell]}"] \arrow[d, "\psi"] & \cdots \\
\cdots \arrow[r, "{[\ell]}"] & \mathfrak{J}_{\mathcal{C}}[\ell^{n+1}] \arrow[r, "{[\ell]}"] & \mathfrak{J}_{\mathcal{C}}[\ell^{n}] \arrow[r, "{[\ell]}"] & \cdots
\end{tikzcd}$$

FIGURE 1. Representation of an endomorphism $\psi \in \mathrm{End}(\mathfrak{J}_{\mathcal{C}})$ on the Tate module $\mathrm{T}_\ell(\mathfrak{J}_{\mathcal{C}})$. The horizontal maps $[\ell]$ are the multiplication-by-ℓ map.

Closely related to the embedding degree we have the *total* embedding degree.

Definition (Total embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the order of $\mathfrak{J}_{\mathcal{C}}(\mathbb{F}_q)$. The total embedding degree of $\mathfrak{J}_{\mathcal{C}}(\mathbb{F}_q)$ with respect to ℓ is the least number κ, such that $\mathfrak{J}_{\mathcal{C}}[\ell] \subseteq \mathfrak{J}_{\mathcal{C}}(\mathbb{F}_{q^\kappa})$.

Remark 2.1. If $\mathfrak{J}_{\mathcal{C}}[\ell] \subseteq \mathfrak{J}_{\mathcal{C}}(\mathbb{F}_{q^\kappa})$, then $\ell \mid q^\kappa - 1$; cf. [5, corollary 5.77, p. 111]. Hence, the total embedding degree is a multiple of the embedding degree.

3. The tame Tate pairing

Let $\mathbb{F}$ be an algebraic extension of $\mathbb{F}_q$. Let $x \in \mathfrak{J}_{\mathcal{C}}(\mathbb{F})[\ell]$ and $y = \sum_i a_i P_i \in \mathfrak{J}_{\mathcal{C}}(\mathbb{F})$ be divisors with disjoint support, and let $\bar{y} \in \mathfrak{J}_{\mathcal{C}}(\mathbb{F})/\ell\mathfrak{J}_{\mathcal{C}}(\mathbb{F})$ denote the divisor class containing the divisor y. Furthermore, let $f_x \in \mathbb{F}(\mathcal{C})$ be a rational function on $\mathcal{C}$ with divisor $\mathrm{div}(f_x) = \ell x$. Set $f_x(y) = \prod_i f(P_i)^{a_i}$. Then

$$e_\ell(x, \bar{y}) = f_x(y)$$

is a well-defined pairing $\mathfrak{J}_{\mathcal{C}}(\mathbb{F})[\ell] \times \mathfrak{J}_{\mathcal{C}}(\mathbb{F})/\ell\mathfrak{J}_{\mathcal{C}}(\mathbb{F}) \longrightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^\ell$, the *Tate pairing*; cf. [8].

Theorem 3.1. *If the field $\mathbb{F}$ is finite and contains the ℓ^{th} roots of unity, then the Tate pairing e_ℓ is bilinear and non-degenerate.*

Proof. Hess [11] gives a short and elementary proof of this result. □

Now let $\mathbb{F} = \mathbb{F}_{q^k}$. Raising to the power $\frac{q^k-1}{\ell}$ gives a well-defined element in the subgroup $\mu_\ell < \mathbb{F}_{q^k}^\times$ of the ℓ^{th} roots of unity. This pairing

$$\hat{e}_\ell : \mathfrak{J}_{\mathcal{C}}(\mathbb{F}_{q^k})[\ell] \times \mathfrak{J}_{\mathcal{C}}(\mathbb{F}_{q^k})/\ell\mathfrak{J}_{\mathcal{C}}(\mathbb{F}_{q^k}) \longrightarrow \mu_\ell$$

is called the *tame* Tate pairing.

Corollary. *The tame Tate pairing $\hat{e}_\ell$ is bilinear and non-degenerate.*

4. Tate representation of the Frobenius endomorphism

Let $\mathbb{Z}_\ell$ denote the ring of ℓ-adic integers. An endomorphism $\psi : \mathfrak{J}_{\mathcal{C}} \to \mathfrak{J}_{\mathcal{C}}$ induces a $\mathbb{Z}_\ell$-linear map

$$\psi_\ell : \mathrm{T}_\ell(\mathfrak{J}_{\mathcal{C}}) \to \mathrm{T}_\ell(\mathfrak{J}_{\mathcal{C}})$$

on the ℓ-adic Tate-module $\mathrm{T}_\ell(\mathfrak{J}_{\mathcal{C}})$ of $\mathfrak{J}_{\mathcal{C}}$; cf. [14, chapter VII, §1]. The map ψ_ℓ is given by ψ as described in figure 1. Hence, ψ is represented on $\mathfrak{J}_{\mathcal{C}}[\ell]$ by a matrix $M \in \mathrm{Mat}_4(\mathbb{F}_\ell)$.

Definition (Diagonal representation). An endomorphism $\psi \in \mathrm{End}(\mathcal{J}_{\mathcal{C}})$ is *diagonalizable* or have a *diagonal representation* on $\mathcal{J}_{\mathcal{C}}[\ell]$, if ψ can be represented on $\mathcal{J}_{\mathcal{C}}[\ell]$ by a diagonal matrix $M \in \mathrm{Mat}_4(\mathbb{F}_\ell)$ with respect to an appropriate basis of $\mathcal{J}_{\mathcal{C}}[\ell]$.

Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ, cf. [14, pp. 109–110], and let $\bar{f}(X) \in \mathbb{F}_\ell[X]$ be the characteristic polynomial of the restriction of ψ to $\mathcal{J}_{\mathcal{C}}[\ell]$. Then f is a monic polynomial of degree four, and by [14, Theorem 3, p. 186],

$$f(X) \equiv \bar{f}(X) \pmod{\ell}.$$

Since $\mathcal{C}$ is defined over $\mathbb{F}_q$, the mapping $(x, y) \mapsto (x^q, y^q)$ is a morphism on $\mathcal{C}$. This morphism induces the q-power Frobenius endomorphism φ on the jacobian $\mathcal{J}_{\mathcal{C}}$. Let P be the characteristic polynomial of φ. Consider an algebraic integer $\omega \in \mathbb{C}$ with $P(\omega) = 0$ in $\mathbb{C}$. By the homomorphism $\mathbb{Z}[\omega] \to \mathrm{End}(\mathcal{J}_{\mathcal{C}})$ given by $\omega \mapsto \varphi$ we will identify φ with ω.

Since $\mathrm{End}(\mathcal{J}_{\mathcal{C}})$ is a finitely generated, torsion free $\mathbb{Z}$-module [17, Theorem 1], we may define $\mathrm{End}_{\mathbb{Q}}(\mathcal{J}_{\mathcal{C}}) = \mathrm{End}(\mathcal{J}_{\mathcal{C}}) \otimes \mathbb{Q}$. Notice that $\mathbb{Q}(\omega) \subseteq \mathrm{End}_{\mathbb{Q}}(\mathcal{J}_{\mathcal{C}})$. Throughout this paper we assume that ℓ is unramified in $\mathbb{Q}(\omega)$.

Remark 4.1. It is well-known that ℓ is unramified in $\mathbb{Q}(\omega)$ if, and only if, ℓ divides the discriminant of the field extension $\mathbb{Q}(\omega)/\mathbb{Q}$; see e.g. [19, Theorem 2.6, p. 199]. Hence, almost any prime number ℓ is unramified in $\mathbb{Q}(\omega)$. In particular, if ℓ is large, then ℓ is unramified in $\mathbb{Q}(\omega)$.

We prove the following theorem.

Theorem 4.2 (Matrix representation). *Let $\mathcal{C}$ be a hyperelliptic curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p with irreducible jacobian. Identify the q-power Frobenius endomorphism φ on $\mathcal{J}_{\mathcal{C}}$ with a root $\omega \in \mathbb{C}$ of the characteristic polynomial $P \in \mathbb{Z}[X]$ of φ. Assume that the ring of integers of $\mathbb{Q}(\omega)$ under this identification is embedded in $\mathrm{End}(\mathcal{J}_{\mathcal{C}})$. Consider a prime number $\ell \neq p$ dividing the order of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$, and that $\ell \nmid q - 1$. If φ is not diagonalizable on $\mathcal{J}_{\mathcal{C}}[\ell]$, then φ is represented on $\mathcal{J}_{\mathcal{C}}[\ell]$ by a matrix on the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} \tag{1}$$

with $c \not\equiv q + 1 \pmod{\ell}$ with respect to an appropriate basis of $\mathcal{J}_{\mathcal{C}}[\ell]$.

The proof of theorem 4.2 uses a number of lemmas. At first we notice that if a power of an endomorphism is trivial on the ℓ-torsion subgroup of $\mathcal{J}_{\mathcal{C}}$, then so is also the endomorphism.

Lemma 4.3. *Let notation and assumptions be as in theorem 4.2. Consider an endomorphism $\alpha \in \mathbb{Q}(\omega)$. If $\ker[\ell] \subseteq \ker(\alpha^n)$ for some number $n \in \mathbb{N}$, then $\ker[\ell] \subseteq \ker(\alpha)$.*

Proof. Since $\ker[\ell] \subseteq \ker(\alpha^n)$, it follows that $\alpha^n = \ell\beta$ for some endomorphism $\beta \in \mathrm{End}(\mathcal{J}_{\mathcal{C}})$; see e.g. [18, Remark 7.12, p. 37]. Notice that $\beta = \frac{\alpha^n}{\ell} \in \mathbb{Q}(\omega)$. Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of β. Since $f(\beta) = 0$ and f is monic, β is an algebraic integer. So $\beta \in \mathfrak{O}_{\mathbb{Q}(\omega)}$, whence $\alpha^n \in \ell\mathfrak{O}_{\mathbb{Q}(\omega)}$. Since ℓ is unramified in $\mathbb{Q}(\omega)$ by assumption, it follows that $\alpha \in \ell\mathfrak{O}_{\mathbb{Q}(\omega)}$, i.e. $\ker[\ell] \subseteq \ker(\alpha)$. $\square$

We will examine the representation of φ on $\mathcal{J}_{\mathcal{C}}[\ell]$. A first, basic observation is given by the following lemma.

Lemma 4.4. *Let notation and assumptions be as in theorem 4.2. Then either $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^k})[\ell]$ is of dimension two as a $\mathbb{F}_\ell$-vectorspace, or all ℓ-torsion points of $\mathcal{J}_{\mathcal{C}}$ are $\mathbb{F}_{q^k}$-rational.*

Proof. By the non-degeneracy of the Tate pairing on $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^k})[\ell]$, the dimension over $\mathbb{F}_\ell$ is at least two. If $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^k})[\ell]$ is of dimension at least three over $\mathbb{F}_\ell$, then the restriction of the q^k-power Frobenius endomorphism φ^k to $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^k})[\ell]$ is represented by a matrix on the form

$$M = \begin{bmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \\ 0 & 0 & 0 & m_4 \end{bmatrix}.$$

Notice that $m_4 = \det M \equiv \deg(\varphi^k) = q^{2k} \equiv 1 \pmod{\ell}$. Thus, the characteristic polynomial of φ^k satisfies $P(X) \equiv (X-1)^4 \pmod{\ell}$, i.e. $\ker[\ell] \subseteq \ker(\varphi^k - 1)^4$. By Lemma 4.3 it follows that $\ker[\ell] \subseteq \ker(\varphi^k - 1)$. But then $\mathcal{J}_{\mathcal{C}}[\ell] \subseteq \mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^k})$, i.e. all ℓ-torsion points of $\mathcal{J}_{\mathcal{C}}$ are $\mathbb{F}_{q^k}$-rational. □

By [20, proof of Theorem 3.1] we know that $\mathcal{J}_{\mathcal{C}}[\ell]$ as a vector space over $\mathbb{F}_\ell$ is isomorphic to a direct sum of φ-invariant subspaces. From this we get a partial description of the representation of φ on $\mathcal{J}_{\mathcal{C}}[\ell]$.

Lemma 4.5. *Let notation and assumptions be as in theorem 4.2. We may choose a basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_{\mathcal{C}}[\ell]$, where $\varphi(x_1) = x_1$, $\varphi(x_2) = qx_2$ and $\varphi(x_3) \in \langle x_3, x_4 \rangle$. If $\varphi(x_3) \notin \langle x_3 \rangle$, then φ can be represented on $\mathcal{J}_{\mathcal{C}}[\ell]$ by a matrix on the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix}.$$

If $c \equiv q+1 \pmod{\ell}$, then φ is diagonalizable.

Proof. Let $\bar{P} \in \mathbb{F}_\ell[X]$ be the characteristic polynomial of the restriction of φ to $\mathcal{J}_{\mathcal{C}}[\ell]$. Since $\ell \mid |\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)|$, 1 is a root of $\bar{P}$. Assume that 1 is an root of $\bar{P}$ with multiplicity d. Since the roots of $\bar{P}$ occur in pairs $(\alpha, q/\alpha)$, also q is a root of $\bar{P}$ with multiplicity d. Hence, we may write

$$\bar{P}(X) = (X-1)^d (X-q)^d \bar{Q}(X),$$

where $\bar{Q} \in \mathbb{F}_\ell[X]$ is a polynomial of degree $4-2d$, and $\bar{Q}(1) \cdot \bar{Q}(q) \not\equiv 0 \pmod{\ell}$. Let $U = \ker(\varphi - 1)^d$, $V = \ker(\varphi - q)^d$ and $W = \ker(\bar{Q}(\varphi))$. Then U, V and W are φ-invariant subspaces of the $\mathbb{F}_\ell$-vectorspace $\mathcal{J}_{\mathcal{C}}[\ell]$, $\dim_{\mathbb{F}_\ell}(U) = \dim_{\mathbb{F}_\ell}(V) = d$, and $\mathcal{J}_{\mathcal{C}}[\ell] \simeq U \oplus V \oplus W$.

If $d = 1$, then choose $x_i \in \mathcal{J}_{\mathcal{C}}[\ell]$, such that $U = \langle x_1 \rangle$, $V = \langle x_2 \rangle$ and $W = \langle x_3, x_4 \rangle$. Then (x_1, x_2, x_3, x_4) establishes the first part of the lemma. Hence, we may assume that $d = 2$. Now choose $x_1 \in U$, such that $\varphi(x_1) = x_1$, and expand this to a basis (x_1, x_2) of U. Similarly, choose a basis (x_3, x_4) of V with $\varphi(x_3) = qx_3$. With respect to the basis (x_1, x_2, x_3, x_4), φ is then represented by a matrix on the form

$$M = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & \beta \\ 0 & 0 & 0 & q \end{bmatrix}.$$

Notice that

$$M^k = \begin{bmatrix} 1 & k\alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & kq^{k-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Hence, the restriction of φ^k to $\mathfrak{J}_\mathcal{C}[\ell]$ has the characteristic polynomial $(X-1)^4$, i.e. $\mathfrak{J}_\mathcal{C}[\ell] \subseteq \mathfrak{J}_\mathcal{C}(\mathbb{F}_{q^k})$. But then $M^k = I$, whence $\alpha \equiv \beta \equiv 0 \pmod{\ell}$. So if $d = 2$, then the first part of the lemma is established by (x_1, x_3, x_2, x_4). Thus, the first part of the lemma is proved.

Now choose a basis (x_1, x_2, x_3, x_4) of $\mathfrak{J}_\mathcal{C}[\ell]$ accordingly to the first part of the lemma. Assume that $\varphi(x_3) \notin \langle x_3 \rangle$. Then the set $(x_1, x_2, x_3, \varphi(x_3))$ is a basis of $\mathfrak{J}_\mathcal{C}[\ell]$. With respect to this basis, φ is represented by a matrix on the given form. If $c \equiv q+1 \pmod{\ell}$, then φ is diagonalizable. □

Remark 4.6. Notice that if $\bar{P}(X) = (X-1)^2(X-q)^2$, then φ is represented by the diagonal matrix $\operatorname{diag}(1, 1, q, q)$ with respect to an appropriate basis of $\mathfrak{J}_\mathcal{C}[\ell]$, $\mathfrak{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is bi-cyclic and $\mathfrak{J}_\mathcal{C}[\ell] \subseteq \mathfrak{J}_\mathcal{C}(\mathbb{F}_{q^k})$.

With lemma 4.5 we can finally prove theorem 4.2.

Proof of theorem 4.2. If $\varphi(x_3) \in \langle x_3 \rangle$, then φ is represented by a matrix on the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & 0 & q\alpha^{-1} \end{bmatrix}$$

with respect to (x_1, x_2, x_3, x_4). If $\alpha^2 \not\equiv q \pmod{\ell}$, then M is diagonalizable, i.e. φ can be represented by a diagonal matrix on $\mathfrak{J}_\mathcal{C}[\ell]$. So assume that $\alpha^2 \equiv q \pmod{\ell}$. Then

$$M^{2k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2k\alpha^{-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

i.e. the restriction of φ^{2k} to $\mathfrak{J}_\mathcal{C}[\ell]$ has the characteristic polynomial $(X-1)^4$. But then $\mathfrak{J}_\mathcal{C}[\ell] \subseteq \mathfrak{J}_\mathcal{C}(\mathbb{F}_{q^{2k}})$ by Lemma 4.3, i.e. $M^{2k} = I$. So $\beta \equiv 0 \pmod{\ell}$, and φ is diagonalizable.

Thus, if φ is not diagonalizable on $\mathfrak{J}_\mathcal{C}[\ell]$, then $\varphi(x_3) \notin \langle x_3 \rangle$, whence φ is represented on $\mathfrak{J}_\mathcal{C}[\ell]$ by a matrix on the form (1) with respect to an appropriate basis of $\mathfrak{J}_\mathcal{C}[\ell]$. □

Since the roots of the characteristic polynomial P of the Frobenius φ are all of absolute value $\sqrt{q}$, we can determine whether the Frobenius is diagonalizable on $\mathfrak{J}_\mathcal{C}[\ell]$ directly from the roots of P modulo ℓ. From this it follows that if P splits into linear factors modulo ℓ, then the Frobenius is diagonalizable.

Theorem 4.7 (Diagonal representation)**.** *Let notation and assumptions be as in theorem 4.2. Then φ is diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$ if, and only if, the characteristic polynomial of φ splits into linear factors modulo ℓ.*

Proof. The "only if" part is trivial. We prove the "if" part.

Let $\bar{P} \in \mathbb{F}_\ell[X]$ be the characteristic polynomial of the restriction of φ to $\mathcal{J}_\mathcal{C}[\ell]$. Assume at first that $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is cyclic. If $\bar{P}(X) = (X-1)^2(X-q)^2$, then $\mathcal{J}_\mathcal{C}[\ell]$ is bi-cyclic by Remark 4.6. So $\bar{P}(X) \neq (X-1)^2(X-q)^2$. If $\bar{P}$ has only simple roots, then φ is diagonalizable. Hence, we may assume that $\bar{P}$ has a double root $\bar{\alpha} \in \mathbb{F}_\ell$. The roots of $\bar{P}$ occur in pairs $(\bar{\alpha}, q/\bar{\alpha})$. Thus, if $\bar{\alpha} \in \{1, q\}$, then $\bar{P}(X) = (X-1)^2(X-q)^2$. So $\bar{\alpha} \notin \{1, q\}$, and it follows that φ can be represented on $\mathcal{J}_\mathcal{C}[\ell]$ by a matrix on the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & 0 & \alpha \end{bmatrix},$$

where $\alpha \equiv \bar{\alpha} \pmod{\ell}$. Let $\alpha^\kappa \equiv 1 \pmod{\ell}$. Then

$$M^\kappa = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \kappa\alpha^{\kappa-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

i.e. the restriction of φ^κ to $\mathcal{J}_\mathcal{C}[\ell]$ has the characteristic polynomial $(X-1)^4$. But then $\mathcal{J}_\mathcal{C}[\ell] \subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^\kappa})$ by Lemma 4.3, i.e. $M^\kappa = I$. So $\beta \equiv 0 \pmod{\ell}$, and φ is diagonalizable.

Then assume that $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is bi-cyclic. Then $\mathcal{J}_\mathcal{C}[\ell] \subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_q)$ by Lemma 4.4, and it follows that φ can be represented on $\mathcal{J}_\mathcal{C}[\ell]$ by a matrix on the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & \alpha \\ 0 & 0 & 0 & q \end{bmatrix}.$$

As above, it follows that $\alpha \equiv 0 \pmod{\ell}$, whence φ is diagonalizable. □

Remark 4.8. Assume that P splits into linear factors modulo ℓ. If $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is cyclic, then φ is diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$, and the the total embedding degree κ of $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)$ with respect to ℓ is given by the multiplicative order of a root $\alpha \in \mathbb{F}_\ell$ of $\bar{P}$. If $\mathcal{J}_\mathcal{C}[\ell]$ is not cyclic, then $\mathcal{J}_\mathcal{C}[\ell] \subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})$ by Lemma 4.4, i.e. $\kappa = k$. Hence, κ is easy to determine.

5. Anti-symmetric pairings on the jacobian

On $\mathcal{J}_\mathcal{C}[\ell]$, a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell] \to \mu_\ell < \mathbb{F}_{q^k}^\times$$

exists, e.g. the Weil pairing. Since ε is bilinear, it is given by

$$\varepsilon(x, y) = x^T \mathcal{E} y$$

for some matrix $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{F}_\ell)$ with respect to a basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_\mathcal{C}[\ell]$. Since ε is Galois–invariant,

$$\forall x, y \in \mathcal{J}_\mathcal{C}[\ell] : \varepsilon(x, y)^q = \varepsilon(\varphi(x), \varphi(y)).$$

This is equivalent to

$$\forall x, y \in \mathcal{J}_{\mathcal{C}}[\ell] : q(x^T \mathcal{E} y) = (Mx)^T \mathcal{E}(My),$$

where M is the representation of φ on $\mathcal{J}_{\mathcal{C}}[\ell]$ with respect to (x_1, x_2, x_3, x_4). Since $(Mx)^T \mathcal{E}(My) = x^T M^T \mathcal{E} M y$, from the Galois-invarians of ε it follows that

$$\forall x, y \in \mathcal{J}_{\mathcal{C}}[\ell] : x^T q \mathcal{E} y = x^T M^T \mathcal{E} M y,$$

or equivalently, that $q\mathcal{E} = M^T \mathcal{E} M$.

Now let ζ be a primitive ℓ^{th} root of unity. Let

$$\varepsilon(x_1, x_2) = \zeta^{a_1}, \quad \varepsilon(x_1, x_3) = \zeta^{a_2}, \quad \varepsilon(x_2, x_3) = \zeta^{a_4} \quad \text{and} \quad \varepsilon(x_3, x_4) = \zeta^{a_6}.$$

Assume at first that φ is not diagonalizable on $\mathcal{J}_{\mathcal{C}}[\ell]$. By Galois-invarians and anti-symmetry we then see that

$$\mathcal{E} = \begin{bmatrix} 0 & a_1 & a_2 & qa_2 \\ -a_1 & 0 & a_4 & a_4 \\ -a_2 & -a_4 & 0 & a_6 \\ -qa_2 & -a_4 & -a_6 & 0 \end{bmatrix}.$$

Since $M^T \mathcal{E} M = q\mathcal{E}$, it follows that

$$a_2 q(c - (1+q)) \equiv a_4 q(c - (1+q)) \equiv 0 \pmod{\ell}.$$

Thus, $a_2 \equiv a_4 \equiv 0 \pmod{\ell}$, cf. Theorem 4.2. So

$$\mathcal{E} = \begin{bmatrix} 0 & a_1 & 0 & 0 \\ -a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_6 \\ 0 & 0 & -a_6 & 0 \end{bmatrix}. \tag{2}$$

Since ε is non-degenerate, $a_1^2 a_6^2 = \det \mathcal{E} \not\equiv 0 \pmod{\ell}$.

Now assume that φ is represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to an appropriate basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_{\mathcal{C}}[\ell]$. Let $\varepsilon(x_1, x_4) = \zeta^{a_3}$ and $\varepsilon(x_1, x_4) = \zeta^{a_5}$. Then it follows from $M^T \mathcal{E} M = q\mathcal{E}$ that

$$a_2(\alpha - q) \equiv a_3(\alpha - 1) \equiv a_4(\alpha - 1) \equiv a_5(\alpha - q) \equiv 0 \pmod{\ell}.$$

If $\alpha \equiv 1, q \pmod{\ell}$, then $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$ is bi-cyclic. Hence the following theorem holds.

Theorem 5.1 (Anti-symmetric pairings). *Let $\mathcal{C}$ be a hyperelliptic curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p with irreducible jacobian. Identify the q-power Frobenius endomorphism φ on $\mathcal{J}_{\mathcal{C}}$ with a root $\omega \in \mathbb{C}$ of the characteristic polynomial $P \in \mathbb{Z}[X]$ of φ. Assume that the ring of integers of $\mathbb{Q}(\omega)$ under this identification is embedded in $\operatorname{End}(\mathcal{J}_{\mathcal{C}})$. Choose a basis $\mathcal{B}$ of $\mathcal{J}_{\mathcal{C}}[\ell]$, such that φ is represented either by a diagonal matrix or a matrix on the form given in theorem 4.2 with respect to $\mathcal{B}$. Consider a prime number $\ell \neq p$ dividing the order of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$, and that $\ell \nmid q-1$. If $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)[\ell]$ is cyclic, then all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_{\mathcal{C}}[\ell]$ are given by the matrices*

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in \mathbb{F}_\ell^\times$$

with respect to $\mathcal{B}$.

Corollary. *Under the assumptions of theorem 5.1,*

1. *the Weil-pairing is non-degenerate on $\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})[\ell]$, and*
2. *no non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell]$ can be computed more than eight times as effective as the Weil-pairing.*

Proof. By a precomputation, a basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_\mathcal{C}[\ell]$ can be found, such that the Weil-pairing is given by the matrix $\mathcal{E}_{1,1}$; cf. the notation of theorem 5.1. To compute the Weil-pairing of $A, B \in \mathcal{J}_\mathcal{C}[\ell]$, we only need to find the coordinates of A and B in this basis. Now assume a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing ε on $\mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell]$ exists, such that ε can be computed more than eight times as effective the Weil-pairing. By a precomputation we can find the matrix representation $\mathcal{E}_{a,b}$ of ε. Write $A = \sum_i \alpha_i x_i$. Then

$$\alpha_1 = -a^{-1}\varepsilon(x_2, A), \qquad \alpha_2 = a^{-1}\varepsilon(x_1, A),$$
$$\alpha_3 = -b^{-1}\varepsilon(x_4, A), \qquad \alpha_4 = b^{-1}\varepsilon(x_3, A).$$

Similarly we find the coordinates of B. Hence, the Weil-pairing of A and B can be computed by at most eight pairing computations with ε, a contradiction. □

6. Matrix representation of the tame Tate pairing

The tame Tate pairing induces a pairing $\tau_\ell : \mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell] \to \mu_\ell$ by

$$\tau_\ell(x, y) = \hat{e}_\ell(x, \bar{y}).$$

In this section we will examine the matrix representation of this pairing.

Let $x, y \in \mathcal{J}_\mathcal{C}[\ell] = \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^\kappa})[\ell]$ be divisors with disjoint support, and choose functions $f_x, f_y \in \mathbb{F}_{q^\kappa}(\mathcal{C})$ with $\mathrm{div}(f_x) = \ell x$ and $\mathrm{div}(f_y) = \ell y$. The Weil pairing $e_\ell : \mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell] \to \mu_\ell$ is then defined by

$$e_\ell(x, y) = \frac{f_x(y)}{f_y(x)}$$

Notice that

$$e_\ell(x, y) = \frac{\tau_\ell(x, y)}{\tau_\ell(y, x)} \tag{3}$$

Now choose an appropriate basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_\mathcal{C}[\ell]$, such that the Weil pairing is represented by the matrix

$$\mathcal{W} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

with respect to this basis. Notice that $x_1 \in \mathcal{J}_\mathcal{C}(\mathbb{F}_q)$, so $\tau_\ell(x_1, x_1) = 1$.

By (3) it follows that τ_ℓ is represented by a matrix on the form

$$\mathcal{T} = \begin{bmatrix} 0 & a_1 & a_2 & a_3 \\ a_1 - 1 & d_2 & a_4 & a_5 \\ a_2 & a_4 & d_3 & a_6 \\ a_3 & a_5 & a_6 - 1 & d_4 \end{bmatrix}$$

with respect to the basis (x_1, x_2, x_3, x_4). Since τ_ℓ is Galois-invariant, it follows that $M^T \mathcal{T} M = q\mathcal{T}$, where M is the representation of φ on $\mathcal{J}_\mathcal{C}[\ell]$ with respect to (x_1, x_2, x_3, x_4).

Assume at first that the Frobenius φ is not diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$. Then φ is represented by a matrix M on the form given in theorem 4.2, and it follows from $M^T \mathcal{T} M = q\mathcal{T}$, that

$$\mathcal{T} = \begin{bmatrix} 0 & a_1 & 0 & 0 \\ a_1 - 1 & 0 & 0 & 0 \\ 0 & 0 & d_3 & a_6 \\ 0 & 0 & a_6 - 1 & qd_3 \end{bmatrix},$$

where $2a_6 \equiv d_3 c + 1 \pmod{\ell}$.

Now assume that φ is represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to an appropriate basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_\mathcal{C}[\ell]$. It then follows that

$$a_i(\alpha - q) \equiv a_j(\alpha - 1) \equiv d_2(q-1) \equiv d_j(\alpha^2 - q) \equiv 0 \pmod{\ell}$$

for $i \in \{2, 5\}$ and $j \in \{3, 4\}$. Hence the following theorem is established.

Theorem 6.1. *Let $\mathcal{C}$ be a hyperelliptic curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p with irreducible jacobian. Identify the q-power Frobenius endomorphism φ on $\mathcal{J}_\mathcal{C}$ with a root $\omega \in \mathbb{C}$ of the characteristic polynomial $P \in \mathbb{Z}[X]$ of φ. Assume that the ring of integers of $\mathbb{Q}(\omega)$ under this identification is embedded in $\operatorname{End}(\mathcal{J}_\mathcal{C})$. Consider a prime number $\ell \neq p$ dividing the order of $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$, and that $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)$ is of embedding degree $k > 1$ with respect to ℓ. If $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell]$ is cyclic, then the tame Tate pairing is represented on $\mathcal{J}_\mathcal{C}[\ell] \times \mathcal{J}_\mathcal{C}[\ell]$ by a matrix on the form*

$$\mathcal{T} = \begin{bmatrix} 0 & a_1 & 0 & 0 \\ a_1 - 1 & 0 & 0 & 0 \\ 0 & 0 & d_3 & a_6 \\ 0 & 0 & a_6 - 1 & d_4 \end{bmatrix}$$

with respect to an appropriate basis of $\mathcal{J}_\mathcal{C}[\ell]$. Furthermore, the following holds.

1. *If the q-power Frobenius endomorphism is not diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$, then $d_4 \equiv qd_3 \pmod{\ell}$ and $2a_6 \equiv d_3 c + 1 \pmod{\ell}$.*
2. *If the q-power Frobenius endomorphism is diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$, and $\mathcal{J}_\mathcal{C}[\ell] \not\subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^{2k}})$, then $d_3 \equiv d_4 \equiv 0 \pmod{\ell}$.*
3. *Assume $\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})[\ell]$ is bi-cyclic.*
   (a) *If $\ell^3 \nmid |\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})|$, then $a_1 \not\equiv 0, 1 \pmod{\ell}$.*
   (b) *If $\ell^3 \mid |\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})|$ and $\ell^2 \nmid |\mathcal{J}_\mathcal{C}(\mathbb{F}_q)|$, then $a_1 \equiv 0 \pmod{\ell}$.*

Proof. Write $\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})[\ell] = \langle x_1 \rangle \oplus \langle x_2 \rangle$, where $\mathcal{J}_\mathcal{C}(\mathbb{F}_q)[\ell] = \langle x_1 \rangle$. If $\ell^2 \nmid |\mathcal{J}_\mathcal{C}(\mathbb{F}_q)|$ and $\ell^3 \nmid |\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})|$, then $\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})/\ell\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k}) \simeq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})[\ell]$. By Theorem 3.1 it then follows that $a_1 \not\equiv 0, 1 \pmod{\ell}$. On the other hand, if $\ell^3 \mid |\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})|$, then $x_2 \in \ell\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})$, i.e. $a_1 \equiv 0 \pmod{\ell}$. □

Corollary. *Assume $\ell^3 \nmid |\mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})|$. If the Frobenius is not diagonalizable on $\mathcal{J}_\mathcal{C}[\ell]$, then either*

1. *a point $x \in \mathcal{J}_\mathcal{C}[\ell]$ with $\tau_\ell(x, x) \neq 1$ exists, or*
2. *τ_ℓ is non-degenerate on $\mathcal{J}_\mathcal{C}[\ell]$.*

Proof. Choose an appropriate basis (x_1, x_2, x_3, x_4) of $\mathcal{J}_\mathcal{C}[\ell]$, such that the Frobenius is represented by a matrix M on the form given in theorem 4.2, and τ_ℓ is represented by a matrix $\mathcal{T}$ on the form given in Theorem 6.1 with respect to this basis. Since $M^T\mathcal{T}M = q\mathcal{T}$, it follows that $d_3 c \equiv 2a_6 - 1 \pmod{\ell}$. Hence, if $2a_6 \not\equiv 1 \pmod{\ell}$, then $d_3 \not\equiv 0 \pmod{\ell}$, and τ is a self-pairing on $\mathcal{J}_\mathcal{C}[\ell]$. If $2a_6 \equiv 1 \pmod{\ell}$ and $d_3 \equiv 0 \pmod{\ell}$, then τ_ℓ is non-degenerate on $\mathcal{J}_\mathcal{C}[\ell]$. □

7. Complex multiplication curves

In this section we assume that the endomorphism ring of the jacobian is isomorphic to the ring of integers in a *quartic CM field* K, i.e. a totally imaginary, quadratic field extension of a quadratic number field. Assuming that the Frobenius endomorphism under this isomorphism is given by an *η-integer* and that the characteristic polynomial of the Frobenius endomorphism splits into linear factors over $\mathbb{F}_\ell$, we prove that if the discriminant of the real subfield of K is not a quadratic residue modulo ℓ, then all ℓ-torsion points are $\mathbb{F}_{q^k}$-rational.

7.1. Complex multiplication.

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *complex multiplication*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field*, and if $\mathrm{End}(E) \simeq \mathfrak{O}_K$, then E is said to have *CM by* $\mathfrak{O}_K$. More generally a CM field is defined as follows.

Definition (CM field)**.** A number field K is a CM field, if K is a totally imaginary, quadratic extension of a totally real number field K_0.

We only consider *quartic* CM field, i.e. CM fields of degree $[K:\mathbb{Q}] = 4$.

Remark 7.1. Consider a quartic CM field K. Let $K_0 = K \cap \mathbb{R}$ be the real subfield of K. Then K_0 is a real, quadratic number field, $K_0 = \mathbb{Q}(\sqrt{D})$. By a basic result on quadratic number fields, the ring of integers of K_0 is given by $\mathfrak{O}_{K_0} = \mathbb{Z} + \xi\mathbb{Z}$, where

$$\xi = \begin{cases} \sqrt{D}, & \text{if } D \not\equiv 1 \pmod 4, \\ \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Since K is a totally imaginary, quadratic extension of K_0, a number $\eta \in K$ exists, such that $K = K_0(\eta)$, $\eta^2 \in K_0$. The number η is totally imaginary, and we may assume that $\eta = i\eta_0$, $\eta_0 \in \mathbb{R}$. Furthermore we may assume that $-\eta^2 \in \mathfrak{O}_{K_0}$; so $\eta = i\sqrt{a + b\xi}$, where $a, b \in \mathbb{Z}$.

Let $\mathcal{C}$ be a hyperelliptic curve of genus two. Then $\mathcal{C}$ is said to have CM by $\mathfrak{O}_K$, if $\mathrm{End}(\mathcal{J}_\mathcal{C}) \simeq \mathfrak{O}_K$. The structure of K determines whether $\mathcal{J}_\mathcal{C}$ is irreducible. More precisely, the following theorem holds.

Theorem 7.2. *Let $\mathcal{C}$ be a hyperelliptic curve of genus two with $\mathrm{End}(\mathcal{J}_\mathcal{C}) \simeq \mathfrak{O}_K$, where K is a quartic CM field. Then $\mathcal{J}_\mathcal{C}$ is reducible if, and only if, $K/\mathbb{Q}$ is Galois with bi-cyclic Galois group.*

Proof. [22, proposition 26, p. 61]. □

Theorem 7.2 motivates the following definition.

Definition (Primitive, quartic CM field)**.** A quartic CM field K is called primitive if either $K/\mathbb{Q}$ is not Galois, or $K/\mathbb{Q}$ is Galois with cyclic Galois group.

7.2. **Jacobians with complex multiplication.** The CM method for constructing curves of genus two with prescribed endomorphism ring is described in detail by Weng [24], Gaudry *et al* [10] and Eisenträger and Lauter [4]. In short, the CM method is based on the construction of the class polynomials of a primitive, quartic CM field K with real subfield K_0 of class number $h(K_0) = 1$. The prime power q has to be chosen such that $q = x\bar{x}$ for a number $x \in \mathfrak{O}_K$. By [24] we will restrict ourselves to the case $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$.

Now assume that $\mathcal{J}_\mathcal{C}$ has CM by a primitive, quartic CM field $K = \mathbb{Q}(\eta)$, where $\eta = i\sqrt{a + b\xi}$ and

$$\xi = \begin{cases} \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \end{cases} \tag{4}$$

Here, D is a square-free integer, and $K_0 = \mathbb{Q}(\sqrt{D})$.

Definition (η-integer)**.** An integer $\alpha \in \mathfrak{O}_K$ is an η-integer, if $\alpha \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$.

If the q-power Frobenius endomorphism φ under the isomorphism $\mathrm{End}(\mathcal{J}_\mathcal{C}) \simeq \mathfrak{O}_K$ is given by an η-integer ω, then we can express the characteristic polynomial P of φ in terms ω. Together with Remark 4.6 it follows from this that if P splits into linear factors over $\mathbb{F}_\ell$ and D is not a quadratic residue modulo ℓ, then all ℓ-torsion points are $\mathbb{F}_{q^k}$-rational. This result is given by the following theorem.

Theorem 7.3. *Let $\mathcal{C}$ be a hyperelliptic curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p and with $\mathrm{End}(\mathcal{J}_\mathcal{C}) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field with real subfield $\mathbb{Q}(\sqrt{D})$. Assume that the q-power Frobenius endomorphism φ under this isomorphism is given by an η-integer ω. Consider a prime number $\ell \neq p$ dividing $|\mathcal{J}_\mathcal{C}(\mathbb{F}_q)|$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$, and that the characteristic polynomial $\bar{P}$ of the restriction of φ to $\mathcal{J}_\mathcal{C}[\ell]$ splits into linear factors over $\mathbb{F}_\ell$. Let k be the multiplicative order of q modulo ℓ. If D is not a quadratic residue modulo ℓ, then all the ℓ-torsion points of $\mathcal{J}_\mathcal{C}$ are $\mathbb{F}_{q^k}$-rational.*

Proof. Write

$$\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta, \qquad c_i \in \mathbb{Z}.$$

Since D is not a quadratic residue modulo ℓ, it follows by lemma 7.4 that $c_2 \equiv 0 \pmod \ell$ and $\bar{P}(X) = (X-1)^2(X-q)^2$. By theorem 4.7 it then follows that if $q \not\equiv 1 \pmod \ell$, then the q-power Frobenius endomorphism is represented by the diagonal matrix $\mathrm{diag}(1, 1, q, q)$ on $\mathcal{J}_\mathcal{C}[\ell]$ with respect to an appropriate basis, whence $\mathcal{J}_\mathcal{C}[\ell] \subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})$. On the other hand, if $q \equiv 1 \pmod \ell$, then $\bar{P}(X) = (X-1)^4$, i.e. also in this case $\mathcal{J}_\mathcal{C}[\ell] \subseteq \mathcal{J}_\mathcal{C}(\mathbb{F}_{q^k})$. □

Lemma 7.4. *Let notation and assumptions be as in theorem 7.3. Write*

$$\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta, \qquad c_i \in \mathbb{Z}.$$

(1) *If $c_2 \not\equiv 0 \pmod \ell$, then D is a quadratic residue modulo ℓ.*
(2) *If $c_2 \equiv 0 \pmod \ell$, then $\bar{P}(X) = (X-1)^2(X-q)^2$.*

Proof. At first, assume that $D \not\equiv 1 \pmod 4$. Since the conjugates of ω are given by $\omega_1 = \omega$, $\omega_2 = \bar{\omega}_1$, ω_3 and $\omega_4 = \bar{\omega}_3$, where

$$\omega_3 = c_1 - c_2\sqrt{D} + i(c_3 - c_4\sqrt{D})\sqrt{a - b\sqrt{D}},$$

it follows that the characteristic polynomial of φ is given by

$$P(X) = \prod_{i=1}^{4}(X-\omega_i) = X^4 - 4c_1X^3 + (2q + 4(c_1^2 - c_2^2D))X^2 - 4c_1qX + q^2.$$

Dividing $P(X)$ by $(X-1)(X-q)$ it then follows that $\alpha X + \beta \equiv 0 \pmod{\ell}$, where

$$\beta \equiv q(-q^2 + (4c_1 - 2)q + (-1 + 4c_2^2D - 4c_1^2 + 4c_1)) \pmod{\ell}$$

Since $\beta \equiv 0 \pmod{\ell}$, it follows that $4c_2^2D \equiv (2c_1 - q - 1)^2 \pmod{\ell}$. So if $c_2 \equiv 0 \pmod{\ell}$, then $2c_1 \equiv q + 1 \pmod{\ell}$, and it follows that $\bar{P}(X) = (X-1)^2(X-q)^2$.

If $D \equiv 1 \pmod 4$, then

$$\omega_3 = c_1 + c_2\frac{1-\sqrt{D}}{2} + i\left(c_3 + c_4\frac{1-\sqrt{D}}{2}\right)\sqrt{a + b\frac{1-\sqrt{D}}{2}},$$

and it follows that the characteristic polynomial of φ is given by

$$P(X) = X^4 - 2cX^3 + (2q + c^2 - c_2^2d)X^2 - 2qcX + q^2,$$

where $c = 2c_1 + c_2$. Dividing $P(X)$ by $(X-1)(X-q)$ it then follows that $\alpha X + \beta \equiv 0 \pmod{\ell}$, where

$$\beta \equiv -q(q^2 + (2-2c)q + (1 - 2c + c^2 - c_2^2D)) \pmod{\ell}.$$

Since $\beta \equiv 0 \pmod{\ell}$, it follows that $c_2^2D \equiv (c - q - 1)^2 \pmod{\ell}$. As before it then follows that if $c_2 \equiv 0 \pmod{\ell}$, then $\bar{P}(X) = (X-1)^2(X-q)^2$. □

References

[1] R. Balasubramanian and N. Koblitz. The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm, *J. Cryptology*, vol. 11, pp.141–145, 1998.

[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[3] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

[4] K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. To appear in *Proceedings of AGCT-10*. 2007. `http://arxiv.org`.

[5] G. Frey and T. Lange. Varieties over Special Fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 87–113. Chapman & Hall/CRC, 2006.

[6] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, vol. 62, pp. 865–874, 1994.

[7] S. Galbraith. Supersingular curves in cryptography. Asiacrypt 2001, *Lecture Notes in Computer Science*, vol. 2248, pp. 495–513, Springer, 2001.

[8] S. Galbraith. Pairings. In I.F. Blake, G. Seroussi and N.P. Smart, editors, *Advances in Elliptic Curve Cryptography*. London Mathematical Society Lecture Note Series, vol. 317, pp. 183–213. Cambridge University Press, 2005.

[9] S. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In T. Takagi *et al*, editors, *Pairing 2007*, pp. 108–131. Springer, 2007.

[10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng. The p-adic CM-Method for Genus 2. 2005. `http://arxiv.org`.

[11] F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, no. 82, pp. 28–32, 2004.

[12] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, vol. 48, pp. 203–209, 1987.

[13] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1, pp. 139–150, 1989.

[14] S. Lang. *Abelian Varieties*. Interscience, 1959.

[15] A.J. Menezes, T. Okamoto and S.A. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions on Information Theory*, vol. 39, nr. 5, pp. 1639–1646, 1993.
[16] V. Miller. *Short Programs for Functions on Curves.* Unpublished manuscript, 1986. Available at `http://crypto.stanford.edu/miller/miller.pdf`.
[17] J.S. Milne and W.C. Waterhouse. Abelian varieties over finite fields. *Proc. Symp. Pure Math.*, vol. 20, pp. 53–64, 1971.
[18] J.S. Milne. *Abelian Varieties.* 1998. Available at `http://www.jmilne.org`.
[19] J. Neukirch. *Algebraic Number Theory.* Springer, 1999.
[20] K. Rubin and A. Silverberg. *Using Abelian Varieties to Improve Pairing-Based Cryptography.* Preprint, 2007. Available at `http://www.math.uci.edu/~asilverb/bibliography/`
[21] H.-G. Rück. Abelian surfaces and jacobian varieties over finite fields. *Compositio Mathematica*, vol. 76, no. 3, pp. 351–366, 1990.
[22] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, 1998.
[23] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.
[24] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, vol. 72, pp. 435–458, 2003.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C
E-mail address: `cr@imf.au.dk`