GENERATORS OF JACOBIANS OF GENUS TWO CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. This paper provides an efficient, probabilistic algorithm to find generators of subgroups of points of prime number order on the Jacobian of a genus two curve.

1. Introduction

In [9], Koblitz described how to use elliptic curves to construct a public key cryptosystem. To get a more general class of curves, and possibly larger group orders, Koblitz [10] then proposed using Jacobians of hyperelliptic curves. After Boneh and Franklin [1] proposed an identity based cryptosystem by using the Weil-pairing on an elliptic curve, pairings have been of great interest to cryptography [5]. The next natural step was to consider pairings on Jacobians of hyperelliptic curves. Galbraith *et al* [6] survey the recent research on pairings on Jacobians of hyperelliptic curves.

Miller [12] uses the Weil-pairing to determine generators of $E(\mathbb{F}_q)$, where E is an elliptic curve defined over a finite field $\mathbb{F}_q$. Let C be a genus two curve defined over $\mathbb{F}_q$. In [14], the author describes an algorithm based on the Tate-pairing to determine generators of the subgroup $\mathcal{J}_C(\mathbb{F}_q)[m]$ of points of order m on the Jacobian, where m is a number dividing $q-1$. The key ingredient of the algorithm is a "diagonalization" of a set of randomly chosen points $\{P_1, \dots, P_4, Q_1, \dots, Q_4\}$ on the Jacobian with respect to a pairing ε; i.e. a modification of the set such that $\varepsilon(P_i, Q_j) \neq 1$ if and only if $i = j$. This procedure is based on solving the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[m]$. Contrary to the special case when m divides $q-1$, this is infeasible in general. Hence, in general the algorithm in [14] does not apply.

In the present paper, we generalize the algorithm in [14] to subgroups of points of prime order ℓ, where ℓ does not divide $q-1$. In order to do so, we must somehow alter the diagonalization step. We exploit the fact that the matrix representation of the Frobenius endomorphism on $\mathcal{J}_C[\ell]$ is particularly simple with respect to an appropriate basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, and that computation of $\mathcal{B}$ is feasible. Hereby, computations of discrete logarithms are avoided, yielding the desired altering of the diagonalization step.

Setup. Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, and with ℓ dividing neither q nor $q-1$. Assume that the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ is cyclic. Let k be the multiplicative order

2000 *Mathematics Subject Classification.* 11G20 (Primary) 11T71, 14G50, 14H45 (Secondary).
Key words and phrases. Jacobians, hyperelliptic genus two curves, pairings, embedding degree.
Research supported in part by a PhD grant from CRYPTOMAThIC.

of q modulo ℓ. Write the characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ as

$$P_k(X) = X^4 + 2\sigma_k X^3 + (2q^k + \sigma_k^2 - \tau_k)X^2 + 2\sigma_k q^k X + q^{2k},$$

where $2\sigma_k, 4\tau_k \in \mathbb{Z}$. Let $\omega_k \in \mathbb{C}$ be a root of $P_k(X)$. Finally, if ℓ divides $4\tau_k$, we assume that ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark. Notice that in most cases relevant to cryptography, the considered genus two curve C fulfills these assumptions. Cf. Remark 7.

The algorithm. First of all, we notice that in the above setup, the q-power Frobenius endomorphism φ on $\mathcal{J}_C$ is represented on $\mathcal{J}_C[\ell]$ by either a diagonal matrix or a matrix of the form

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

with respect to an appropriate basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$; cf. Lemma 8. From this description of the action of φ on $\mathcal{J}_C[\ell]$, it follows that all non-degenerate, bilinear, antisymmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices

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

with respect to $\mathcal{B}$; cf. Theorem 9. By using this description of the pairing, the desired algorithm is given as follows.

Algorithm 13. *On input the considered curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$, the following algorithm outputs a generating set of $\mathcal{J}_C[\ell]$ or "failure".*

(1) *If ℓ does not divide $4\tau_k$, then do the following.*
   (a) *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \backslash \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3' \in U := \mathcal{J}_C[\ell] \backslash \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$; compute $x_3 = x_3' - \varphi^k(x_3')$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
   (b) *Let $i = j = 0$. While $i < n$ do the following*
      (i) *Choose a random point $x_4 \in U$.*
      (ii) *$i := i + 1$.*
      (iii) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
   (c) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*
(2) *If ℓ divides $4\tau_k$, then do the following.*
   (a) *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$*
   (b) *Let $i = j = 0$. While $i < n$ do the following*
      (i) *Choose random points $y_3, y_4 \in \mathcal{J}_C[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
      (ii) *If $\varepsilon(x_3, x_4) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
   (c) *If $j = 0$ then output "failure" and stop.*
   (d) *Let $i = j = 0$. While $i < n$ do the following*
      (i) *Choose a random point $x_2 \in \mathcal{J}_C[\ell]$.*
      (ii) *If $\varepsilon(x_1, x_2) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
   (e) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$ and stop.*

Algorithm 13 finds generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$ and in expected running time $O(\log \ell)$; cf. Theorem 14.

Remark. To implement Algorithm 13, we need to find a q^k-*Weil number* (cf. Definition 2). On Jacobians generated by the *complex multiplication method* [17, 7, 3], we know the Weil numbers in advance. Hence, Algorithm 13 is particularly well suited for such Jacobians.

Assumption. In this paper, a *curve* is an irreducible nonsingular projective variety of dimension one.

2. Genus two curves

A hyperelliptic curve is a projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. It is well known, that any genus two curve is hyperelliptic. Throughout this paper, let C be a 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 $\psi : C \to \mathbb{P}^2$, mapping 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 of degree $\deg(g) \leq 3$ and $\deg(h) \leq 6$; cf. [2, chapter 1].

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

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

The Jacobian is an abelian group. We write the group law additively, and denote the zero element of the Jacobian by $\mathcal{O}$.

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_C[\ell^n] \subseteq \mathcal{J}_C$ of points of order dividing ℓ^n is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank four, i.e.

$$\mathcal{J}_C[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z};$$

cf. [11, Theorem 6, p. 109].

The multiplicative order k of q modulo ℓ plays an important role in cryptography, since the (reduced) Tate-pairing is non-degenerate over $\mathbb{F}_{q^k}$; cf. [8].

Definition 1 (Embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. The embedding degree of $\mathcal{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number k, such that $q^k \equiv 1 \pmod{\ell}$.

3. The Frobenius endomorphism

Since C is defined over $\mathbb{F}_q$, the mapping $(x, y) \mapsto (x^q, y^q)$ is a morphism on C. This morphism induces the q-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. Let $P(X)$ be the characteristic polynomial of φ; cf. [11, pp. 109–110]. $P(X)$ is called the *Weil polynomial* of $\mathcal{J}_C$, and

$$|\mathcal{J}_C(\mathbb{F}_q)| = P(1)$$

by the definition of $P(X)$ (see [11, pp. 109–110]); i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$.

Definition 2 (Weil number)**.** Let notation be as above. Let $P_k(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on $\mathcal{J}_C$. A number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$ is called a q^m-*Weil number* of $\mathcal{J}_C$.

Remark 3. Note that $\mathcal{J}_C$ has four q^m-Weil numbers. If $P_1(X) = \prod_i (X - \omega_i)$, then $P_m(X) = \prod_i (X - \omega_i^m)$. Hence, if ω is a q-Weil number of $\mathcal{J}_C$, then ω^m is a q^m-Weil number of $\mathcal{J}_C$.

4. Non-cyclic subgroups

Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let $P_m(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on the Jacobian $\mathcal{J}_C$. $P_m(X)$ is of the form $P_m(X) = X^4 + sX^3 + tX^2 + sq^mX + q^{2m}$, where $s, t \in \mathbb{Z}$. Let $\sigma = \frac{s}{2}$ and $\tau = 2q^m + \sigma^2 - t$. Then

$$P_m(X) = X^4 + 2\sigma X^3 + (2q^m + \sigma^2 - \tau)X^2 + 2\sigma q^m X + q^{2m},$$

and $2\sigma, 4\tau \in \mathbb{Z}$. In [15], the author proves the following Theorem 4 and 5.

Theorem 4. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$ as $P_m(X) = X^4+2\sigma X^3+(2q^m+\sigma^2-\tau)X^2+2\sigma q^m X+q^{2m}$, where $2\sigma, 4\tau \in \mathbb{Z}$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, and with $\ell \nmid q$ and $\ell \nmid q-1$. If $\ell \nmid 4\tau$, then*

1. *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module, and*
2. *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic if and only if ℓ divides $q^m - 1$.*

Theorem 5. *Let notation be as in Theorem 4. Furthermore, let ω_m be a q^m-Weil number of $\mathcal{J}_C$, and assume that ℓ is unramified in $\mathbb{Q}(\omega_m)$. Now assume that $\ell \mid 4\tau$. Then the following holds.*

1. *If $\omega_m \in \mathbb{Z}$, then $\ell \mid q^m - 1$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^m})$.*
2. *If $\omega_m \notin \mathbb{Z}$, then $\ell \nmid q^m - 1$, $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{mk}})$ if and only if $\ell \mid q^{mk} - 1$.*

Inspired by Theorem 4 and 5 we introduce the following notation.

Definition 6. Consider a curve C. We say that C is a $\mathcal{C}(\ell, q, k, \tau_k)$-curve, and write $C \in \mathcal{C}(\ell, q, k, \tau_k)$, if the following holds.

1. C is of genus two and defined over the finite field $\mathbb{F}_q$.
2. ℓ is an odd prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, and ℓ divides neither q nor $q-1$.
3. $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic.
4. Let k be the multiplicative order of q modulo ℓ. The characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ is given by
$$P_k(X) = X^4 + 2\sigma_k X^3 + (2q^k + \sigma_k^2 - \tau_k)X^2 + 2\sigma_k q^k X + q^{2k},$$
where $2\sigma_k, 4\tau_k \in \mathbb{Z}$.
5. Let ω_k be a q^k-Weil number of $\mathcal{J}_C$. If ℓ divides $4\tau_k$, then ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark 7. In most cases relevant to cryptography, we consider a prime divisor ℓ of size q^2. Assume ℓ is of size q^2. Then ℓ divides neither q nor $q-1$. The number of $\mathbb{F}_q$-rational points on the Jacobian is approximately q^2. Thus, $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic. Since ℓ is ramified in $\mathbb{Q}(\omega_k)$ if and only if ℓ divides the discriminant of $\mathbb{Q}(\omega_k)$, ℓ is unramified in $\mathbb{Q}(\omega_k)$ with probability approximately $1 - 1/\ell$. Hence, in most cases relevant to cryptography the considered genus two curve C is a $\mathcal{C}(\ell, q, k, \tau_k)$-curve.

5. Matrix representation of the Frobenius endomorphism

An endomorphism $\psi : \mathcal{J}_C \to \mathcal{J}_C$ induces a linear map $\bar{\psi} : \mathcal{J}_C[\ell] \to \mathcal{J}_C[\ell]$ by restriction. Hence, ψ is represented by a matrix $M \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ on $\mathcal{J}_C[\ell]$. If ψ can be represented on $\mathcal{J}_C[\ell]$ by a diagonal matrix with respect to an appropriate basis of $\mathcal{J}_C[\ell]$, then we say that ψ is *diagonalizable* or has a *diagonal representation* on $\mathcal{J}_C[\ell]$.

Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ (see [11, pp. 109–110]), and let $\bar{f} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of $\bar{\psi}$. Then f is a monic polynomial of degree four, and by [11, Theorem 3, p. 186],

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

The matrix representation of the q-power Frobenius endomorphism on $\mathcal{J}_C[\ell]$ is given explicitly by the following lemma.

Lemma 8. *Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. If φ is not diagonalizable on $\mathcal{J}_C[\ell]$, then φ is represented on $\mathcal{J}_C[\ell]$ by a matrix of 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 $\mathcal{J}_C[\ell]$.

Proof. Let $\bar{P}_k \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ_k to $\mathcal{J}_C[\ell]$. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of $\bar{P}_k$. Assume that 1 is an root of $\bar{P}_k$ with multiplicity ν. Then

$$\bar{P}_k(X) = (X-1)^\nu \bar{Q}_k(X),$$

where $\bar{Q}_k \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ is a polynomial of degree $4-\nu$, and $\bar{Q}_k(1) \neq 0$. Since the roots of $\bar{P}_k$ occur in pairs $(\alpha, 1/\alpha)$, ν is an even number. Let $U_k = \ker(\varphi_k - 1)^\nu$ and $W_k = \ker(\bar{Q}_k(\varphi_k))$. Then U_k and W_k are φ_k-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\mathrm{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U_k) = \nu$, and $\mathcal{J}_C[\ell] \simeq U_k \oplus W_k$.

Assume at first that ℓ does not divide $4\tau_k$. Then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic and $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ bicyclic; cf. Theorem 4. By [16, Theorem 3.1], $\nu = 2$. Choose points $x_1, x_2 \in \mathcal{J}_C[\ell]$, such that $\varphi(x_1) = x_1$ and $\varphi(x_2) = qx_2$. Then $\{x_1, x_2\}$ is a basis of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Now, let $\{x_3, x_4\}$ be a basis of W_k, and consider the basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. If x_3 and x_4 are eigenvectors of φ_k, then φ_k is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Assume x_3 is not an eigenvector of φ_k. Then $\mathcal{B}' = \{x_1, x_2, x_3, \varphi_k(x_3)\}$ is a basis of $\mathcal{J}_C[\ell]$, and φ_k is represented by a matrix of the form (1).

Now, assume ℓ divides $4\tau_k$. Since ℓ divides $q^k - 1$, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 5. Let $\bar{P} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ to $\mathcal{J}_C[\ell]$. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of $\bar{P}$. Assume that 1 is an root of $\bar{P}$ with multiplicity ν. Since the roots of $\bar{P}$ occur in pairs $(\alpha, q/\alpha)$, it follows that

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

where $\bar{Q} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ is a polynomial of degree $4-2\nu$, $\bar{Q}(1) \neq 0$ and $\bar{Q}(q) \neq 0$. Let $U = \ker(\varphi - 1)^\nu$, $V = \ker(\varphi - q)^\nu$ and $W = \ker(\bar{Q}(\varphi))$. Then U, V and W are φ-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U) = \operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(V) = \nu$, and $\mathcal{J}_C[\ell] \simeq U \oplus V \oplus W$. If $\nu = 1$, then it follows as above that φ is either diagonalizable on $\mathcal{J}_C[\ell]$ or represented by a matrix of the form (1) with respect to some basis of $\mathcal{J}_C[\ell]$. Hence, we may assume that $\nu = 2$. 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 $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$, φ is represented by a matrix of 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

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

Since $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$, we know that $\varphi^k = \varphi_k$ is the identity on $\mathcal{J}_C[\ell]$. Hence, $M^k = I$. So $\alpha \equiv \beta \equiv 0 \pmod{\ell}$, i.e. φ is represented by a diagonal matrix with respect to $\mathcal{B}$.

Finally, we observe that if $c \equiv q + 1 \pmod{\ell}$, then φ_k is diagonalizable. □

6. Anti-symmetric pairings on the Jacobian

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

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times.$$

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

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

for some matrix $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ with respect to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Since ε is Galois-invariant,

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

This is equivalent to

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

where M is the matrix representation of φ on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Since $(Mx)^T \mathcal{E}(My) = x^T M^T \mathcal{E} My$, it follows that

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

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

Now, 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 $\mathcal{J}_C[\ell]$. By Galois-invariance and anti-symmetry we 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. Lemma 8. So

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

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 $\mathcal{J}_C[\ell]$. 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 $\mathcal{J}_C(\mathbb{F}_q)$ is bi-cyclic. Hence the following theorem holds.

Theorem 9. *Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. Now choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix with respect to $\mathcal{B}$. All non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices*

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

with respect to $\mathcal{B}$.

Remark 10. Let notation and assumptions be as in Theorem 9. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_C[\ell]$, and let ε be given by $\mathcal{E}_{a,b}$ with respect to a basis $\{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Then ε is given by $\mathcal{E}_{1,1}$ with respect to $\{a^{-1}x_1, x_2, b^{-1}x_3, x_4\}$.

7. Finding generators of $\mathcal{J}_C[\ell]$

Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times;$$

We consider the cases $\ell \nmid 4\tau_k$ and $\ell \mid 4\tau_k$ seperately.

7.1. **The case $\ell \nmid 4\tau_k$.** If ℓ does not divide $4\tau_k$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic and $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 4. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and expand $\{x_1\}$ to a basis $\{x_1, y_2\}$ of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$, where $\varphi(y_2) = qy_2$. Let $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$ be a random point. Write $x_2' = \alpha_1 x_1 + \alpha_2 y_2$. Then

$$x_2 = x_2' - \varphi(x_2') = \alpha_2(1-q)y_2 \in \langle y_2 \rangle,$$

i.e. $\varphi(x_2) = qx_2$. Now, let $\mathcal{J}_C[\ell] \simeq \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \oplus W$, where W is a φ-invariant submodule of rank two. Choose a random point $x_3' \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Then

$$x_3 = x_3' - \varphi^k(x_3') \in W$$

as above. Notice that

$$\mathcal{J}_C[\ell] = \langle x_1, x_2, x_3, \varphi(x_3) \rangle \quad \text{if and only if} \quad \varepsilon(x_3, \varphi(x_3)) \neq 1;$$

cf. Theorem 9.

Assume $\varepsilon(x_3, \varphi(x_3)) = 1$. Then x_3 is an eigenvector of φ. Let $\varphi(x_3) = \alpha x_3$. Then

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell},$$

where $P(X)$ is the Weil polynomial of $\mathcal{J}_C$. If $\alpha \not\equiv q/\alpha \pmod{\ell}$, then φ is diagonalizable on $\mathcal{J}_C[\ell]$. Assume $\alpha \equiv q/\alpha \pmod{\ell}$; then $\alpha^2 \equiv q \pmod{\ell}$, i.e.

$$\bar{P}_k(X) = (X-1)^2(X \pm 1)^2,$$

where $\bar{P}_k(X)$ is the characteristic polynomial of the restriction of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ to $\mathcal{J}_C[\ell]$. But then ℓ divides $4\tau_k$. Hence, $\{x_1, x_2, x_3\}$ can be expanded to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 10.

Now, choose a random point $x \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Write $x = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4$. Then $\varepsilon(x_3, x) = \zeta^{\alpha_4}$. So $\varepsilon(x_3, x) \neq 1$ if and only if ℓ does not divide α_4. On the other hand, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only ℓ does not divide α_4. Hence, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only if ℓ does not divide α_4. Thus, if ℓ does not divide $4\tau_k$, then the following Algorithm 11 outputs generators of $\mathcal{J}_C[\ell]$ with probability $1 - {}^1/_{\ell^n}$.

Algorithm 11. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

(1) *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3' \in U := \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$; compute $x_3 = x_3' - \varphi^k(x_3')$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
(2) *Let $i = j = 0$. While $i < n$ do the following*
   (a) *Choose a random point $x_4 \in U$.*
   (b) *$i := i + 1$.*
   (c) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
(3) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

7.2. **The case $\ell \mid 4\tau_k$.** Assume ℓ divides $4\tau_k$. Then $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 5. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and let $y_2 \in \mathcal{J}_C[\ell]$ be a point with $\varphi(y_2) = qy_2$. Write $\mathcal{J}_C[\ell] = \langle x_1, y_2 \rangle \oplus W$, where W is a φ-invariant submodule of rank two; cf. the proof of Lemma 8. Let $\{y_3, y_4\}$ be a basis of W, such that φ is represented on $\mathcal{J}_C[\ell]$ by either a diagonal matrix or a matrix of the form (1) with respect to the basis

$$\mathcal{B} = \{x_1, y_2, y_3, y_4\}.$$

Now, choose a random point $z \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$. Since $z - \varphi(z) \in \langle y_2, y_3, y_4 \rangle$, we may assume that $z \in \langle y_2, y_3, y_4 \rangle$. Write $z = \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. If φ is not diagonalizable on $\mathcal{J}_C[\ell]$, then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 y_4 + \alpha_4(-q y_3 + c y_4)) \\ &= (\alpha_3 + \alpha_4) y_3 + (\alpha_4 q - \alpha_3 - \alpha_4 c) y_4, \end{aligned}$$

i.e. $qz - \varphi(z) \in \langle y_3, y_4 \rangle = W$. If $qz - \varphi(z) = 0$, then it follows that $c \equiv q+1 \pmod{\ell}$. This is a contradiction; cf. Lemma 8. So $qz - \varphi(z)$ is a non-trivial element of W. On the other hand, if φ is represented by a diagonal matrix $M = \operatorname{diag}(1, q, \alpha, q/\alpha)$ on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$, then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 \alpha y_3 + \alpha_4 (q/\alpha) y_4) \\ &= \alpha_3 (q - \alpha) y_3 + \alpha_4 (q - q/\alpha) y_4; \end{aligned}$$

so $qz - \varphi(z) \in \langle y_3, y_4 \rangle$. If $qz - \varphi(z) = 0$, then it follows that $q \equiv 1 \pmod{\ell}$. This contradicts the choice of the curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$.

Choose two random points $w_1, w_2 \in W$. Write $w_i = \alpha_{i3} y_3 + \alpha_{i4} y_4$ for $i = 1, 2$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 10. But then

$$\varepsilon(w_1, w_2) = \zeta^{\alpha_{13}\alpha_{24} - \alpha_{14}\alpha_{23}}.$$

Hence, $\varepsilon(w_1, w_2) = 1$ if and only if $\alpha_{13}\alpha_{24} \equiv \alpha_{14}\alpha_{23} \pmod{\ell}$. If $\alpha_{13} \not\equiv 0 \pmod{\ell}$, then $\varepsilon(w_1, w_2) = 1$ if and only if $\alpha_{24} \equiv \frac{\alpha_{14}\alpha_{23}}{\alpha_{13}} \pmod{\ell}$. So $\varepsilon(w_1, w_2) \neq 1$ with probability $1 - 1/\ell$. Hence, we have a procedure to find a basis of W.

Until now, we have found points $x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $w_3, w_4 \in W$, such that $W = \langle w_3, w_4 \rangle$. Now, choose a random point $x_2 \in \mathcal{J}_C[\ell]$. Write $x_2 = \alpha_1 x_1 + \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Then $\varepsilon(x_1, x_2) = \zeta^{\alpha_2}$, i.e. $\varepsilon(x_1, x_2) = 1$ if and only if $\alpha_2 \equiv 0 \pmod{\ell}$. Thus, with probability $1 - \ell^3/\ell^4 = 1 - 1/\ell$, the set $\{x_1, x_2, w_3, w_4\}$ is a basis of $\mathcal{J}_C[\ell]$.

Summing up, if ℓ divides $4\tau_k$, then the following Algorithm 12 outputs generators of $\mathcal{J}_C[\ell]$ with probability $(1 - 1/\ell^n)^2$.

Algorithm 12. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

(1) *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$*
(2) *Let $i = j = 0$. While $i < n$ do the following*
  (a) *Choose random points $y_3, y_4 \in \mathcal{J}_C[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
  (b) *If $\varepsilon(x_3, x_4) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
(3) *If $j = 0$ then output "failure" and stop.*
(4) *Let $i = j = 0$. While $i < n$ do the following*
  (a) *Choose a random point $x_2 \in \mathcal{J}_C[\ell]$.*
  (b) *If $\varepsilon(x_1, x_2) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
(5) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

7.3. **The complete algorithm.** Combining Algorithm 11 and 12 yields the desired algorithm to find generators of $\mathcal{J}_C[\ell]$.

Algorithm 13. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

(1) *If $\ell \nmid \tau_k$, run Algorithm 11 on input $(C, \ell, q, k, \tau_k, n)$.*
(2) *If $\ell \mid \tau_k$, run Algorithm 12 on input $(C, \ell, q, k, \tau_k, n)$.*

Theorem 14. *Let C be a $\mathcal{C}(\ell, q, k, \tau_k)$-curve. On input (C, ℓ, τ_k, n), Algorithm 13 finds generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$ and in expected running time $O(\log \ell)$.*

Proof. We may assume that the time necessary to perform an addition of two points on the Jacobian, to multiply a point with a number or to evaluate the q-power Frobenius endomorphism on the Jacobian is small compared to the time necessary to compute the (Weil-) pairing of two points on the Jacobian. By [4], the pairing can be evaluated in time $O(\log \ell)$. Hence, the expected running time of Algorithm 13 is of size $O(\log \ell)$. □

8. Implementation issues

To implement Algorithm 13, we need to find a q^k-*Weil number* (cf. Definition 2). On Jacobians generated by the *complex multiplication method* [17, 7, 3], we know the Weil numbers in advance. Hence, Algorithm 13 is particularly well suited for such Jacobians.

If ℓ divides $4\tau_k$, then we have to check if ℓ ramifies in $L = \mathbb{Q}(\omega_k)$, where ω_k is a q^k-Weil number. Notice that $L \subseteq K = \mathbb{Q}(\omega)$, where ω is a q-Weil number. Thus, if ℓ ramifies in L, then ℓ ramifies in K; cf. e.g. [13, Corollary 2.10, p. 202]. Hence, if ℓ does not ramify in K, then we do not have to find a q^k-Weil number. This may reduce computing time.

Assume ℓ divides $4\tau_k$ and is unramified in L. Then $\omega_k \in \mathbb{Z}$; cf. Theorem 5. So $\omega^k \in \mathbb{Z}$, i.e. $\omega = \sqrt{q} e^{\frac{in\pi}{k}}$ for some $n \in \mathbb{Z}$ with $0 < n < k$. Assume k divides mn for some $m < k$. Then $\omega^{2m} = q^m \in \mathbb{Z}$. Since the q-power Frobenius endomorphism is the identity on the $\mathbb{F}_q$-rational points on the Jacobian, it follows that $\omega^{2m} \equiv 1 \pmod{\ell}$. Hence, $q^m \equiv 1 \pmod{\ell}$, i.e. k divides m. This is a contradiction. So n and k has no common divisors. Let $\xi = \omega^2/q = e^{\frac{in2\pi}{k}}$. Then ξ is a primitive k^{th} root of unity, and $\mathbb{Q}(\xi) \subseteq K$. Since $[K : \mathbb{Q}] \leq 4$ and $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(k)$, where ϕ is the Euler phi function, it follows that $k \leq 12$. Hence, if q is of multiplicative order $k > 12$ modulo ℓ, then ℓ does not divide $4\tau_k$, and we may skip this check. On the other hand, if $k \leq 12$, then both $\omega_k = \omega^k$ and the characteristic polynomial of the q^k-power Frobenius endomorphism are easy to compute, and we can check if ℓ divides $4\tau_k$ directly.

References

[1] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Computing*, 32(3):586–615, 2003.

[2] 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.

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

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

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

[6] S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing 2007*, Lecture Notes in Computer Science, pages 108–131. Springer, 2007.

[7] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic cm-method for genus 2, 2005.

[8] F. Hess. A note on the tate pairing of curves over finite fields. *Arch. Math.*, 82:28–32, 2004.

[9] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[10] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.

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

[12] V.S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17:235–261, 2004.

[13] J. Neukirch. *Algebraic Number Theory.* Springer, 1999.

[14] C.R. Ravnshøj. Generators of Jacobians of hyperelliptic curves, 2007. Preprint, available at `http://arxiv.org`. Submitted to *Math. Comp.*

[15] C.R. Ravnshøj. Non-cyclic subgroups of Jacobians of genus two curves, 2007. Preprint, available at `http://arxiv.org`. Submitted to *Design, Codes and Cryptography.*

[16] K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In M. Yung, editor, *CRYPTO 2002*, Lecture Notes in Computer Science, pages 336–353. Springer, 2002.

[17] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72:435–458, 2003.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

E-mail address: `cr@imf.au.dk`