The Brezing-Weng-Freeman method for certain genus two hyperelliptic curves

Takakazu Satoh

Department of Mathematics,
Tokyo Institute of Technology, Tokyo, 152-8551, Japan
e-mail: satohcgn@mathpc-satoh.math.titech.ac.jp

Abstract

We construct paring friendly curves of the form $Y^2=X^5+uX^3+vX$ over large finite prime fields. The ϱ-value of our family is always less than 4. Our method is based on the fact that, under a certain condition, the Jacobian J of the curve splits to a square of an elliptic curve over the quadratic extension of the base field. However, the generated curves by our method are $\mathbf{F}_p$-simple. A key ingredient is the construction of a pairing non-friendly elliptic curve by the modified Brezing-Weng-Freeman method so that J is pairing-friendly.

1. Introduction

Nowadays, importance of pairing based cryptographic systems does not need explanation. However, generating pairing-friendly curves is still a challenging problem. Let A be an Abelian variety of dimension d, defined over the finite field $\mathbf{F}_q$ with q elements. Assume that we use a cyclic subgroup of $A(\mathbf{F}_q)$ of order l for pairing based cryptosystems. The efficiency of such a system is measured by the ϱ-value defined by $\frac{d\log q}{\log l}$. In Brezing-Weng algorithm[1] and its generalization, we actually generate polynomials whose specialization gives curve parameters. More specifically, we introduce the following notion formulated in Freeman[3, Def. 3.7] with slight modification.

Definition 1.1. Let K be a CM field of degree $2d$. We call a pair of polynomials $(p(x), l(x)) \in \mathbf{Q}[x]\times\mathbf{Q}[x]$ a polynomial parameter for family of d dimensional Abelian variety with embedding degree k if the following conditions hold:

(1.1) There exists $w(x)\in K[x]$ such that $w(x)\overline{w}(x)=p(x)$. (Here $\overline{w}$ is the coefficient-wise complex conjugation of w.)

(1.2) $p(x)$ represents primes in the sense of Freeman[3, Def. 3.6].

(1.3) $l(x)$ is an irreducible, non-constant, integer-valued polynomial.

[1]The work was supported by the Grant-in-Aid for the Scientific Research (B) 18340005.

(1.4) $l(x) \mid N_{K/\mathbf{Q}}(w(x)-1)$.

(1.5) $l(x) \mid \Phi_k(p(x))$ where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

The ϱ-value of the polynomial parameter is defined to be

$$\frac{d \deg p(x)}{\deg l(x)}.$$

An excellent survey article for paring friendly elliptic curve (that is, the case $d=1$) generation is Freeman, Scott and Teske[4]. As to genus two curves, Freeman[2] constructed absolutely simple ordinary curves over large prime fields whose ϱ-value is approximately 8. Later, Freeman[3] constructed the Freeman, Stevenhagen, Streng method[5] analogue of the Brezing-Weng algorithm[1] He gave several polynomial parameters, one of which has ϱ-value 4. Hitt O'Connor et al.[7] gave a construction for curves with p-rank 1 (where p is a characteristic of the definition field), whose ϱ-value is approximately 16. Kawazoe and Takahashi[8] proposed use of the special curve $Y^2=X^5+aX$ to produce curves with ϱ-values (as an individual curve) approximately 4 in general, but one curve attained $\varrho=2.975$. On the other hand, curves defined over binary fields, Hitt[6] gave families with ϱ-values not more than 2 (often close to 1). This motivates us to look for better construction of genus two hyperelliptic curves defined over large prime fields with a smaller ϱ-value.

Our method is as follows. We consider hyperelliptic curves of the form $Y^2=X^5+uX^3+vX$ defined over $\mathbf{F}_p$. Let J be the Jacobian of the curve. Under some assumptions, J splits as E^2 over $\mathbf{F}_{p^2}$ where E is an elliptic curve defined over $\mathbf{F}_p$. This gives rise to an explicit relation between order of $J(\mathbf{F}_p)$ and $E(\mathbf{F}_p)$. We modify the Brezing-Weng method[1] so that we can construct E which makes J pairing-friendly. We can regard our method as the degree four imprimitive CM field version of Freeman[3, Algorithm 3.8]. However, the ϱ-value of our polynomial parameter is always less than 4 and resulting Jacobians are always $\mathbf{F}_p$-simple and ordinary. We also note that $E/\mathbf{F}_p$ is **not** pairing-friendly. (If we regard E as a curve over $\mathbf{F}_{p^4}$, it become a pairing-friendly curve with ϱ-value 8, which is not really pairing-friendly.) As to the difficulty of the discrete log problem on such a Jacobian, we refer to [12, Sect. 8].

We notice that although the Kawazoe-Takahashi method can generate only curves given by binomial polynomials of X, their method can be applicable to the case that the splitting field of J is not $\mathbf{F}_{p^2}$.

The rest of paper is organized as follows. In Section 2, we give a explicit relation between the zeta function of J and the zeta function of E. In Section 3, we present our algorithm. In Section 4, we give a polynomial parameter with embedding degree 20 whose ϱ-value is 7/2.

Acknowledgments

The author also would like to thank Gaetan Bisson and Steven Galbraith for their helpful comments on the earlier versions of the paper.

Notation: Throughout the paper, ζ_k stands for $\exp\left(\frac{2\pi i}{k}\right)$. Let p be a prime. In general, we denote the p^2-th power Frobenius endomorphism on an Abelian variety $A/\mathbf{F}_{p^2}$ by Π_A and the p-th power Frobenius endomorphism on an Abelian variety $A/\mathbf{F}_p$ by π_A. The (1-dimensional part) of the zeta function of $A/\mathbf{F}_q$ is denoted as $Z_A(T, \mathbf{F}_q)$ where T is an indeterminate.

2. The Zeta Functions

We reformulate some formulae in Leprévost and Morain[10], or Satoh[12] in our setting to obtain an explicit formula for the zeta function of our curve. Let $p \geq 7$ be a prime. Let $C : Y^2 = X^5 + uX^3 + vX$ be a hyperelliptic curve defined over $\mathbf{F}_p$. Let J be the Jacobian variety of C. We further assume the following conditions:

(2.1) v is a square element of $\mathbf{F}_p^\times$.

(2.2) v is not a fourth power element of $\mathbf{F}_p^\times$.

They impose the condition $p \equiv 1 \bmod 4$. Under the condition (2.1), the Jacobian J splits over $\mathbf{F}_{p^2}$. Then the condition (2.2) is necessary for J to be $\mathbf{F}_p$-simple. There exist α, $\beta \in \mathbf{F}_{p^4}$ such that $X^4 + uX^2 + v = (X^2 - \alpha^2)(X^2 - \beta^2)$. The assumption on v implies that $\alpha\beta$ is a non square element of $\mathbf{F}_p^\times$.

Theorem 2.1. *Let J be as above. Let $E/\mathbf{F}_p$ be the elliptic curve defined by*

$$Y^2 = (X - 1)(X^2 - \gamma X + 1) \tag{2.3}$$

where

$$\gamma := 2(\alpha^2 + 6\alpha\beta + \beta^2)/(\alpha - \beta)^2. \tag{2.4}$$

Assume that E is ordinary and that $\mathrm{End}(E) \otimes \mathbf{Q} \neq \mathbf{Q}(\sqrt{-1})$. Then J is $\mathbf{F}_p$-simple and

$$Z_J(T, \mathbf{F}_p) = (T^2 - p)^2 + (\mathrm{Tr}\,\pi_E)^2 T^2. \tag{2.5}$$

Proof. Let s be one of square roots of $\alpha\beta$. The condition (2.1) ensures that $s \in \mathbf{F}_{p^2}^\times$. Define $E_1/\mathbf{F}_{p^2}$ and $E_2/\mathbf{F}_{p^2}$ by

$$E_1 : Y^2 = \delta(X - 1)(X^2 - \gamma X + 1)$$
$$E_2 : Y^2 = -\delta(X - 1)(X^2 - \gamma X + 1)$$

with

$$\delta := -\frac{(\alpha - \beta)^2}{64 s^3}. \tag{2.6}$$

First we prove that E_1 and E_2 are quadratic twists of E over $\mathbf{F}_{p^2}$. Assume that $s = s_0^2$ with $s_0 \in \mathbf{F}_{p^2}$. Since $s^2 = \alpha\beta \in \mathbf{F}_p$, we see

$$v = s^4 = N_{\mathbf{F}_{p^2}/\mathbf{F}_p}(s^2) = N_{\mathbf{F}_{p^2}/\mathbf{F}_p}(s_0^4) = N_{\mathbf{F}_{p^2}/\mathbf{F}_p}(s_0)^4,$$

which contradicts to (2.2) Therefore s is not a square element in $\mathbf{F}_{p^2}$. Hence δ and $-\delta$ are not square elements in $\mathbf{F}_{p^2}$, which proves the assertion. Put $c := \mathrm{Tr}\,\Pi_{E_1}$ which is equal to $\mathrm{Tr}\,\Pi_{E_2}$ because E_1 and E_2 are isomorphic over $\mathbf{F}_{p^2}$. As a consequence, we have

$$c = -\mathrm{Tr}\,\Pi_E = -((\mathrm{Tr}\,\pi_E)^2 - 2p). \tag{2.7}$$

Next we determine $Z_J(T, \mathbf{F}_p)$. There exist two covering maps $\varphi_m : C \to E_m$ defined over $\mathbf{F}_{p^2}$ by

$$\varphi_1(x, y) := \left(\left(\frac{x+s}{x-s}\right)^2, \frac{y}{(x-s)^3} \right),$$
$$\varphi_2(x, y) := \left(\left(\frac{x-s}{x+s}\right)^2, \frac{y}{(x+s)^3} \right).$$

(For details, see [12, Sect. 3].) Then φ_m induces a group homomorphism $\varphi_{m*} : J \to E_m$ for $m = 1, 2$ and $(\varphi_{1*}, \varphi_{2*}) : J \to E_1 \times E_2$ is an isogeny defined over $\mathbf{F}_{p^2}$. As is well known, $\Pi_{E_m}^2 - c\Pi_{E_m} + p^2 = 0$ in $\mathrm{End}(E_m)$. Observe that

$$(\varphi_{1*}, \varphi_{2*}) \circ (\Pi_J^2 - c\Pi_J + p^2) = ((\Pi_{E_1}^2 - c\Pi_{E_1} + p^2) \circ \varphi_{1*}, (\Pi_{E_2}^2 - c\Pi_{E_2} + p^2) \circ \varphi_{2*}) = 0.$$

Since an isogeny is of finite type, $\Pi_J^2 - c\Pi_J + p^2 = 0$. On the other hand, J is already defined over $\mathbf{F}_p$ and $\Pi_J = \pi_J^2$. Thus

$$\pi_J^4 - c\pi_J^2 + p^2 = 0.$$

Put $f(T) := T^4 - cT^2 + p^2 = T^4 + (t^2 - 2p)T^2 + p^2$. Because E is ordinary, $t \neq 0$. Moreover, $\pi_E \in \mathrm{End}(\mathbf{Q}) \otimes \mathbf{Q} \neq \mathbf{Q}(\sqrt{-1})$ implies that $4p - t^2$ is not a square. Thus $f(T)$ is irreducible over $\mathbf{Q}$ by Rück[11, Lemma 3.1]. Assume that J splits to $\mathscr{E}_1 \times \mathscr{E}_2$ over $\mathbf{F}_p$ where $\mathscr{E}_1$ and $\mathscr{E}_2$ are elliptic curves defined over $\mathbf{F}_p$. Let $\psi : J \to \mathscr{E}_1 \times \mathscr{E}_2$ be an isogeny over $\mathbf{F}_p$ and let $\mathrm{pr}_m : \mathscr{E}_1 \times \mathscr{E}_2 \to \mathscr{E}_m$ be a projection for $m = 1, 2$. Since $\mathrm{pr}_m \circ \psi$ is defined over $\mathbf{F}_p$, we have

$$f(\pi_{\mathscr{E}_m}) \circ \mathrm{pr}_m \circ \psi = \mathrm{pr}_m \circ \psi \circ f(\pi_J) = 0.$$

However, $\mathrm{pr}_m \circ \psi$ is an epimorphism and $\mathrm{End}(\mathscr{E}_m)$ is an integral domain. Hence $f(T)$ is divisible by the minimal polynomial of $\pi_{\mathscr{E}_m}$ which is $Z_{\mathscr{E}_m}(T, \mathbf{F}_p)$. This contradicts to the irreducibility of $f(T)$. Thus J is $\mathbf{F}_p$-simple. By Waterhouse and Milne[13, Theorem 8], $Z_J(T, \mathbf{F}_p)$ is either an irreducible polynomial of degree four or a square of an irreducible polynomial of degree two. Using the irreducibility of $f(T)$ again, we see $Z_J(T, \mathbf{F}_p) = f(T)$. □

Remark 2.2. We can paraphrase (2.5) as $Z_J(T, \mathbf{F}_p) = Z_E(iT, \mathbf{F}_p)Z_E(-iT, \mathbf{F}_p)$ (where $i = \sqrt{-1}$).

Remark 2.3. Under the condition $\gamma \in \mathbf{F}_p$, not every elliptic curve is isomorphic (over the algebraic closure of $\mathbf{F}_p$) to the elliptic curve of the form (2.3). Indeed, we see

$$j(E) = 2^8 \frac{(\gamma+1)^3}{\gamma+2}. \tag{2.8}$$

Thus only an elliptic curve whose j-invariant is represented as the right hand side of (2.8) is isomorphic to the elliptic curve of the form (2.3).

Corollary 2.4. *Let* $t_0 + y_0\sqrt{-D}$ *with* $t_0, y_0 \in \frac{1}{2}\mathbf{Z}$, $D \in \mathbf{N}$ *be one of the roots of* $Z_E(T, \mathbf{F}_p) = 0$. *Put* $y := 2y_0$. *Then,*

$$Z_J(T, \mathbf{F}_p) = (p+T^2)^2 - y^2DT^2. \tag{2.9}$$

Proof. This is an immediate consequence of (2.5), $\mathrm{Tr}\,\pi_E = 2t_0$ and $t_0^2 + y_0^2 D = p$. □

Lemma 2.5. *For any* $v_0 \in \mathbf{F}_p^\times$ *and* $\gamma \in \mathbf{F}_p$ *with* $\gamma \neq 2$, *There exists* $\alpha, \beta \in \mathbf{F}_{p^4}$ *satisfying the relation (2.4) among* α, β, γ, *and* $\alpha^2 + \beta^2 \in \mathbf{F}_p$ *and* $\alpha\beta = v_0$.

Proof. By the change of variable $w := \alpha/\beta$, Eq. (2.4) becomes

$$(\gamma - 2)w^2 - (2\gamma + 12)w + (\gamma - 2) = 0.$$

By the assumption $\gamma \neq 2$, this is a reciprocal quadratic equation on w. Hence its solution satisfies $w + \frac{1}{w} = \frac{2\gamma+12}{\gamma-2} \in \mathbf{F}_p$. Therefore,

$$\alpha^2 + \beta^2 = v_0 w + \frac{v_0}{w} = v_0\left(w + \frac{1}{w}\right) \in \mathbf{F}_p.$$

□

3. The algorithm

In this section, we present our modification to Brezing-Weng-Freeman algorithm and prove its correctness. We keep notations in Section 2. We denote $\mathrm{Tr}\,\pi_E$ by t for simplicity. In order to specify an embedding $\mathbf{Q}(\sqrt{-D}) \to \mathbf{C}$ explicitly, we use $i\sqrt{D}$ rather than $\sqrt{-D}$.

Let $k \in \mathbf{N}$ be a given embedding degree. Let D be a positive integer such that $-D$ is a discriminant of an order of an imaginary quadratic field and that $\sqrt{D} \notin \mathbf{Q}$ and that $D \neq 3$. We are going to construct a pairing-friendly hyperelliptic curve with help of E satisfying $\mathrm{End}(E) \otimes \mathbf{Q} = \mathbf{Q}(\sqrt{-D})$. Note that if $\frac{t}{2} + \frac{y}{2} i\sqrt{D}$ with $y \in \mathbf{Z}$ is a root of $Z_E(T, \mathbf{F}_p)$, it holds that

$$t^2 + y^2 D = 4p. \tag{3.1}$$

By (2.9),

$$^{\#}J(\mathbf{F}_p) = Z_J(1, \mathbf{F}_p) = (1 - y\sqrt{D} + p)(1 + y\sqrt{D} + p).$$

Now assume that $^{\#}J(\mathbf{F}_p)$ is divisible by a prime l which satisfies the following conditions:

(3.2) The prime l splits to principal prime ideals generated by λ_1 and λ_2 in $\mathbf{Q}(\sqrt{D})$.

(3.3) $\lambda_1 \mid 1 - y\sqrt{D} + p$ and $\lambda_2 \mid 1 + y\sqrt{D} + p$. (Changing the sign of y if necessary, we see that these conditions always hold in case of $l > \sqrt{^{\#}J(\mathbf{F}_p)}$. Indeed, if $l \mid 1 - y\sqrt{D} + p$, then $l^2 \le \left| N_{\mathbf{Q}(\sqrt{D})/\mathbf{Q}}(1 - y\sqrt{D} + p) \right| = {}^{\#}J(\mathbf{F}_p)$.)

By Freeman[2, Prop. 2.3], the embedding degree for the group $J(\mathbf{F}_p)[l]$ is k if and only if $l \mid \Phi_k(p)$, which is equivalent to

$$\lambda_1 \mid \Phi_k(p) \text{ and } \lambda_2 \mid \Phi_k(p)$$

under the condition (3.2). Using (3.3), we see that the embedding degree is k if and only if

$$\lambda_1 \mid \Phi_k(y\sqrt{D} - 1) \text{ and } \lambda_2 \mid \Phi_k(-y\sqrt{D} - 1). \tag{3.4}$$

Our task is to find rational integers t, y and l for given k and D which satisfy (3.1), (3.3) and (3.4).

In order to find such integers, we modify the Brezing-Weng method[1] so that it works with prime elements of the quadratic field $\mathbf{Q}(\sqrt{D})$. Let K be a finite Galois extension of $\mathbf{Q}$ containing i, $\sqrt{D}$, $\zeta_k \in K$. Let θ be an algebraic integer which generates K over $\mathbf{Q}$. Let $F(x) \in \mathbf{Z}[x]$ be the monic minimal polynomial of θ over $\mathbf{Q}$. Further, assume that the polynomial $F(x)$ factors as $F(x) = u_1(x)u_2(x)$ over $\mathbf{Q}(\sqrt{D})$. Replacing θ with its suitable conjugate, we may assume that $u_1(x)$ is the minimal polynomial of θ over $\mathbf{Q}(\sqrt{D})$. We look for polynomials satisfying

(3.5) $4p(x) = t(x)^2 + Dy(x)^2$

(3.6) $u_1(x) \mid 1 - \sqrt{D}y(x) + p(x)$ and $u_2(x) \mid 1 + \sqrt{D}y(x) + p(x)$.

(3.7) $u_1(x) \mid \Phi_k(\sqrt{D}y(x) - 1)$ and $u_2(x) \mid \Phi_k(-\sqrt{D}y(x) - 1)$.

Here we consider divisibility in $\mathbf{Q}(\sqrt{D})[x]$. Note that (3.6) and (3.5) imply $F(x) \mid (p(x) - 1)^2 + t(x)^2$. Then we search $n \in \mathbf{N}$ satisfying the following conditions:

(3.8) $p(n)$ is prime and $p(n) \equiv 1 \bmod 4$.

(3.9) $\dfrac{t(n)}{2} + \dfrac{y(n)}{2} i\sqrt{D} \in \mathbf{Z}\left[\dfrac{-D + i\sqrt{D}}{2}\right]$.

(3.10) $F(n)$ has a large prime factor.

Then, we use the CM-method to compute the j-invariant of an ordinary elliptic curve whose endomorphism ring is isomorphic to $\mathbf{Z}\left[\dfrac{-D + i\sqrt{D}}{2}\right]$. By the definition (2.3) of E, we extract γ from (2.8). Note that $(\mathrm{Tr}\,\pi_E)^2 = t^2$ since $D \neq 1, 3$. Since what we really need is t^2, the choice of a correct twist class does not matter to us. If $\gamma \notin \mathbf{F}_p$ or $\gamma = 2$,

we try another value of n. Otherwise, we choose a non-square element $v_0 \in \mathbf{F}_p^\times$ and use Lemma 2.5 to obtain u (and set $v := v_0^2$).

Our modified Brezing-Weng-Freeman algorithm is as follows.

Algorithm 3.1.
Input: $D \in \mathbf{N}$ such that $\sqrt{D} \notin \mathbf{N}$ and that $D \neq 3$,
$k \in \mathbf{N}$,
K: the finite Galois extension of $\mathbf{Q}$ containing ζ_k, $\sqrt{D}$ and i,
θ: a primitive element of K which is an algebraic integer,
$F(x) \in \mathbf{Z}[x]$: the monic minimal polynomial of θ over $\mathbf{Q}$.
Output: Polynomials $y(x)$, $t(x)$ and $p(x) \in \mathbf{Q}[x]$ satisfying (3.5), (3.6) and (3.7).
Procedure:
1: factorize $F(x)$ over $\mathbf{Q}(\sqrt{D})$ to obtain $u_1(x)$ and $u_2(x)$.
2: determine $z(x) \in \mathbf{Q}[x]$ by $z(\theta) = \zeta_k$ and $\deg z < \deg F$.
3: find $v_1(x)$ and $v_2(x)$ s.t. $u_1(x)v_1(x) + u_2(x)v_2(x) = 1$ and $\deg v_1 < \deg F$, $\deg v_2 < \deg F$.
4: $y(x) := \frac{1}{\sqrt{D}}(1 + z(x))(u_2(x)v_2(x) - u_1(x)v_1(x)) \bmod F(x)$.
5: determine $t(x) \in \mathbf{Q}[x]$ by $t(\theta) = i(\sqrt{D}y(\theta) - 2)$ and $\deg t < \deg F$.
6: $p(x) := \frac{1}{4}(t(x)^2 + Dy(x)^2)$.
7: return $y(x)$, $t(x)$, $p(x)$.

Remark 3.2. Our algorithm does not involve choosing polynomials as in Freeman[3, Algorithm 3.8, Step 4]. This is because we use the algorithm to generate curve parameters for the elliptic curve CM method.

Provided $p(x)$ represents primes, $(p(x), F(x))$ is a polynomial parameter for 2 dimensional Abelian varieties with embedding degree k. (For (1.1), take $w(x) := it(x) + \sqrt{D}y(x)$.) The ϱ-value of our polynomial parameter $(p(x), F(x))$ is clearly not greater than $\frac{4(\deg F - 1)}{\deg F}$.

A proof of correctness of Algorithm 3.1 is quite similar to those of Freeman, Stevenhagen and Streng[5, Algorithm 2.12] and Freeman[3, Algorithm 3.8]. However we include our proof here for completeness. We need some more notation. Put $G := \mathrm{Gal}(K/\mathbf{Q})$, $G_r := \mathrm{Gal}(K/\mathbf{Q}(\sqrt{D}))$, $G_i := \mathrm{Gal}(K/\mathbf{Q}(i))$, and $G_0 := \mathrm{Gal}(K/\mathbf{Q}(\sqrt{D}, i)) = G_r \cap G_i$. We choose (and fix) $g_r \in G_i - G_r$, $g_i \in G_r - G_i$ (but usually g_i is the complex conjugation). Then $G = G_r \amalg g_r G_r = G_i \amalg g_i G_i$, $G_r = G_0 \amalg g_i G_0$, $G_i = G_0 \amalg g_r G_0$. Put

$$u_{1+}(x) := \prod_{\sigma \in G_0} (x - \sigma(\theta)), \qquad u_{2+}(x) := \prod_{\sigma \in G_0} (x - g_r\sigma(\theta)),$$
$$u_{1-}(x) := \prod_{\sigma \in G_0} (x - g_i\sigma(\theta)), \qquad u_{2-}(x) := \prod_{\sigma \in G_0} (x - g_i g_r\sigma(\theta)).$$

Since G_0 is a normal subgroup of G, they are irreducible polynomials of degree $\deg(F)/4$ belonging to $\mathbf{Q}(\sqrt{D}, i)$. We see that

$$u_1(x) = \prod_{\sigma \in G_r} (x - \sigma(\theta)) = u_{1+}(x)u_{1-}(x),$$
$$u_2(x) = (g_r(u_1))(x) = \prod_{\sigma \in G_r} (x - g_r(\sigma(\theta))) = u_{2+}(x)u_{2-}(x).$$

Note that $u_{1+}(x)$ is the minimal polynomial of θ over $\mathbf{Q}(\sqrt{D}, i)$. We define two embeddings $\iota_1 : \mathbf{Q}(\sqrt{D})[x]/\langle u_1(x)\rangle \to K$ and $\iota_2 : \mathbf{Q}(\sqrt{D})[x]/\langle u_2(x)\rangle \to K$ by $\iota_1(x) = \theta$ and $\iota_2(x) = g_r(\theta)$, respectively.

Lemma 3.3. *The polynomial $y(x)$ obtained in Step 4 satisfies $y(x) \in \mathbf{Q}[x]$ and (3.7).*

Proof. Note that the conditions $\deg u_1 < \deg F$ and $\deg u_2 < \deg F$ and

$$u_1 v_1 + u_2 v_2 = 1 \tag{3.11}$$

uniquely determine $v_1(x)$, $v_2(x) \in \mathbf{Q}(\sqrt{D})[x]$. On the other hand, letting g_r act on (3.11), we obtain

$$u_1 g_r(v_2) + u_2 g_r(v_1) = 1.$$

(Recall that $u_2 = g_r(u_1)$.) Since the action of G does not change a degree of a polynomial, the above uniqueness implies $g_r(v_1) = v_2$ and therefore

$$g_r(u_1 v_1) = u_2 v_2. \tag{3.12}$$

It is obvious that $y(x) \in \mathbf{Q}(\sqrt{D})[x]$. However,

$$g_r(y) = -\frac{1}{\sqrt{D}} g_r(z+1) g_r(u_2 v_2 - u_1 v_1) = y$$

by (3.12). This proves that in fact $y(x) \in \mathbf{Q}[x]$. By construction, $\iota_1(\sqrt{D}y(x) - 1) = \zeta_k$ and $\iota_2(-\sqrt{D}y(x) - 1) = g_r(\zeta_k)$. Since ι_1 and ι_2 are field embeddings over $\mathbf{Q}(\sqrt{D})$, we obtain

$$\iota_1(\Phi_k(\sqrt{D}y(x) - 1)) = \iota_2(\Phi_k(\sqrt{D}y(x) - 1)) = 0.$$

This proves (3.7) since $u_1(x)$ and $u_2(x)$ are the minimal polynomials of θ and $g_r(\theta)$) over $\mathbf{Q}(\sqrt{D})$, respectively. □

Lemma 3.4. *The polynomials $t(x)$ and $p(x)$ belong to $\mathbf{Q}(x)$ and they satisfy (3.6) and (3.5).*

Proof. It is obvious that $t(x) \in \mathbf{Q}[x]$ and that (3.5) holds. Since $y(x) \in \mathbf{Q}[x]$, Step 6 ensures $p(x) \in \mathbf{Q}[x]$. Recall that u_{1+} is the minimal polynomial of θ over $\mathbf{Q}(\sqrt{D}, i)$. Since $t(\theta) - i(\sqrt{D}y(\theta) - 2) = 0$ and $t(x) - i(\sqrt{D}y(x) - 2) \in \mathbf{Q}(\sqrt{D}, i)[x]$,

$$u_{1+}(x) \mid t(x) - i(\sqrt{D}y(x) - 2).$$

Letting g_i act on the formula, we obtain $u_{1-}(x) \mid t(x) + i(\sqrt{D}y(x) - 2)$. Therefore

$$u_{1+}(x)u_{1-}(x) \mid t(x)^2 + (\sqrt{D}y(x) - 2))^2 = t(x)^2 + Dy(x)^2 - 4\sqrt{D}y(x) + 4$$
$$u_1(x) \mid 4(p(x) - \sqrt{D}y(x) + 1).$$

Letting g_r act on the formula, we obtain $u_2(x) \mid p(x) + \sqrt{D}y(x) + 1$. □

Remark 3.5. This explains why our method gives a better ϱ-value, or in other words, smaller degree $p(x)$. Note that the Galois group of the degree four primitive CM fields over $\mathbf{Q}$ is $\mathbf{Z}/4\mathbf{Z}$ while the Galois group of the degree four imprimitive CM fields is $(\mathbf{Z}/2\mathbf{Z})^2$. In Freeman[3, Algorithm 3.8], $p(x)$ is represented by a norm between a degree four extension while in our method $p(x)$ is represented by a norm between quadratic extensions in three ways.

4. Examples

We give an illustrative example here. The ϱ-value as a polynomial parameter of the example is 7/2.

Example 4.1. We take $k := 20$, $K := \mathbf{Q}(\zeta_{20}) \cong \mathbf{Q}[x]/\langle F(x) \rangle$ with

$$F(x) := \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1.$$

In this case, $\theta = \zeta_{20}$ and $i = \zeta_{20}^5$. Using the Gauss sum (see e.g. Lang[9, Sect. IV.3]), we see

$$\begin{aligned}\sqrt{5} &= \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \\ &= -2\zeta_{20}^6 + 2\zeta_{20}^4 + 1.\end{aligned}$$

We have $u_1(x) = x^4 - \frac{1+\sqrt{5}}{2}x^2 + 1$, $u_2(x) = x^4 - \frac{1-\sqrt{5}}{2}x^2 + 1$, $v_1(x) = \frac{\sqrt{5}}{5}x^2 - \frac{5-\sqrt{5}}{10}$, $v_2(x) = -\frac{\sqrt{5}}{5}x^2 - \frac{5+\sqrt{5}}{10}$. Then we obtain

$$y(x) = \frac{1}{5}(-2x^7 - 2x^6 + 2x^5 + 2x^4 + x + 1).$$

The value $t(\theta)$ should be

$$\zeta_{20}^5(\sqrt{5}y(\zeta_{20}) - 2) = \zeta_{20}^6 - \zeta_{20}^5.$$

Thus, $t(x) = x^6 - x^5$ and

$$p(x) = \frac{1}{20}(4x^{14} + 8x^{13} + x^{12} - 26x^{11} + x^{10} + 8x^9 - 8x^7 + 8x^5 + 4x^4 + x^2 + 2x + 1).$$

Hence, the ϱ-value for the polynomials is $2 \cdot 14/8 = 7/2$. We can verify that $p := p(197) = 267883778632337179848138866670001$ is a 105 bit prime. Since $t(197) = 58155019028372$, the resulting Jacobian has the order

$$7176171885433902981502012076269327727827000883530297678299703 84$$

which is divisible by $l := 11065339871837941$ which is a 54 bit prime. The class polynomial for the discriminant -20 is $j^2 - 1264000j - 681472000 = 0$. In $\mathbf{F}_p$, it has two solutions. We take a solution $j = 158221751668403689497580562168 11$. Then, (2.8) has one $\mathbf{F}_p$ solution $\gamma = 196815646063749775607294871025 94$. The resulting curve is

$$Y^2 = X^5 + 181776933479446653019947360596 31X^3 + 4X$$

The ϱ-value for the curve is approximately 3.88.

As to cryptographic size examples, we give two values of x here. In the case $x = 1053959$, we see $\Phi_{20}(x)$ is a 161 bit prime and $p(x)$ is a 278 bit pime, hence the ϱ-value is 3.45. In the case $x = 20005259$, we see $\Phi_{20}(x)$ is a 195 bit prime and $p(x)$ is a 338 bit pime, hence the ϱ-value is 3.47.

Remark 4.2. Freeman[3, Table 1] reports the ϱ-value 6 for the embedding degree 20, a primitive CM filed $\mathbf{Q}(\zeta_5)$ and $F(x) = \Phi_{20}(x)$.

Remark 4.3. Unlike the original Brezing-Weng algorithm, the parameters $k = 4$, $K = \mathbf{Q}(\zeta_8)$, $D = 2$ do not seem to work. In this case, we obtain

$$p(x) = \frac{1}{8}(3x^6 - 6x^5 + x^4 + 3x^2 + 2x + 1)$$

which does not take an integral value at any integer.

References

1. Brezing, F. and Weng, A.: Elliptic curves suitable for pairing based cryptography. Des. Codes Crypt., **37**, 133-141 (2005). doi: 10.1007/s10623-004-3808-4
2. Freeman, D.: Constructing pairing-friendly genus 2 curves with ordinary Jacobians, Pairing-Based Cryptography - Pairing 2007, Lect. Notes in Comput. Sci., **4575**, 152-176, ed. Takagi, T., Okamoto, T., Okamoto, E. and Okamoto, T., Berlin, Heidelberg: Springer, 2007. doi: 10.1007/978-3-540-73489-5_9
3. Freeman, D.: A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary Abelian varieties, Pairing-Based Cryptography - Pairing 2008, Lect. Notes in Comput. Sci., **5209**, 146-163, ed. Galbraith, S.D. and Paterson, K.G., Berlin, Heidelberg: Springer, 2008. doi: 10.1007/978-3-540-85538-5_11
4. Freeman, D., Scott, M. and Teske, E.: A taxonomy of pairing-friendly elliptic curves, (2006) IACR e-print 2006/372.
5. Freeman, D., Stevenhagen, P. and Streng, M.: Abelian varieties with prescribed embedding degree, Algorithmic number theory, ANTS-VIII, Lect. Notes in Comput. Sci., **5011**, 60-73, Berlin, Heidelberg: Springer, 2008. doi: 10.1007/978-3-540-79456-1_3
6. Hitt, L.: Families of genus 2 curves with small embedding degree, (2007) IACR e-print 2007/001.
7. Hitt O'Connor, L., McGuire, G., Naehrig, M. and Streng, M.: CM construction of genus 2 curves with p-rank 1, (2008) IACR e-print 2008/491.
8. Kawazoe, M. and Takahashi, T.: Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$, Pairing-based cryptgraphy - Pairing 2008, Lect. Notes in Comput. Sci., **5209**, 164-177, Berlin, Heidelberg: Springer, 2008. doi: 10.1007/978-3-540-85538-5_12

9. Lang, S.: Algebraic number theory. Reading, Mass.: Addison-Wesley Pub. 1970.

10. Leprévost, F. and Morain, F.: Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. J. Number Theory, **64**, 165-182 (1997). doi: 10.1006/jnth.1997.2070

11. Rück, H.G.: Abelian surfaces and Jacobian varieties over finite fields. Compositio Math., **76**, 351-366 (1990).

12. Satoh, T.: Generating genus two hyperelliptic curves over large characteristic finite fields, Advances in Cryptology - Eurocrypt 2009, Lect. Notes in Comput. Sci, **5479**, 536-553(provisional), ed. Joux, A., Heidelberg: Springer, 2009.

13. Waterhouse, W.C. and Milne, J.S.: Abelian varieties over finite fields, 1969 Number Theory Institute (State Univ. New York, Stony Brook, N.Y.), Proc. Sympos. Pure Math., **20**, 53-64, Providence, RI: AMS, 1971.