Abelian varieties with prescribed embedding degree

David Freeman[1], Peter Stevenhagen[2], and Marco Streng[2]

[1] University of California, Berkeley[**]
dfreeman@math.berkeley.edu
[2] Mathematisch Instituut, Universiteit Leiden
psh,streng@math.leidenuniv.nl

Abstract. We present an algorithm that, on input of a CM-field K, an integer $k \geq 1$, and a prime $r \equiv 1 \bmod k$, constructs a q-Weil number $\pi \in \mathcal{O}_K$ corresponding to an ordinary, simple abelian variety A over the field $\mathbf{F}$ of q elements that has an $\mathbf{F}$-rational point of order r and embedding degree k with respect to r. We then discuss how CM-methods over K can be used to explicitly construct A.

1 Introduction

Let A be an abelian variety defined over a finite field $\mathbf{F}$, and $r \neq \mathrm{char}(\mathbf{F})$ a prime number dividing the order of the group $A(\mathbf{F})$. Then the *embedding degree* of A with respect to r is the degree of the field extension $\mathbf{F} \subset \mathbf{F}(\zeta_r)$ obtained by adjoining a primitive r-th root of unity ζ_r to $\mathbf{F}$.

The embedding degree is a natural notion in pairing-based cryptography, where A is taken to be the Jacobian of a curve defined over $\mathbf{F}$. In this case, A is principally polarized and we have the non-degenerate *Weil pairing*

$$e_r : A[r] \times A[r] \longrightarrow \mu_r$$

on the subgroup scheme $A[r]$ of r-torsion points of A with values in the r-th roots of unity. If $\mathbf{F}$ contains ζ_r, we also have the non-trivial *Tate pairing*

$$t_r : A[r](\mathbf{F}) \times A(\mathbf{F})/rA(\mathbf{F}) \to \mathbf{F}^*/(\mathbf{F}^*)^r.$$

The Weil and Tate pairings can be used to 'embed' r-torsion subgroups of $A(\mathbf{F})$ into the multiplicative group $\mathbf{F}(\zeta_r)^*$, and thus the discrete logarithm problem in $A(\mathbf{F})[r]$ can be 'reduced' to the same problem in $\mathbf{F}(\zeta_r)^*$ [6, 3]. In pairing-based cryptographic protocols [7], one chooses the prime r and the embedding degree k such that the discrete logarithm problems in $A(\mathbf{F})[r]$ and $\mathbf{F}(\zeta_r)^*$ are computationally infeasible, and of roughly equal difficulty. This means that r is typically large, whereas k is small. Jacobians of curves meeting such requirements are often said to be *pairing-friendly.*

[**] The first author is supported by a National Defense Science and Engineering Graduate Fellowship

If $\mathbf{F}$ has order q, the embedding degree $k = [\mathbf{F}(\zeta_r) : \mathbf{F}]$ is simply the multiplicative order of q in $(\mathbf{Z}/r\mathbf{Z})^*$. As 'most' elements in $(\mathbf{Z}/r\mathbf{Z})^*$ have large order, the embedding degree of A with respect to a large prime divisor r of $\#A(\mathbf{F})$ will usually be of the same size as r, and A will not be pairing-friendly. One is therefore led to the question of how to efficiently construct A and $\mathbf{F}$ such that $A(\mathbf{F})$ has a (large) prime factor r and the embedding degree of A with respect to r has a prescribed (small) value k. The current paper addresses this question on two levels: the *existence* and the actual *construction* of A and $\mathbf{F}$.

Section 2 focuses on the question whether, for given r and k, there exist abelian varieties A that are defined over a finite field $\mathbf{F}$, have an $\mathbf{F}$-rational point of order r, and have embedding degree k with respect to r. We consider only abelian varieties A that are *simple*, that is, not isogenous (over $\mathbf{F}$) to a product of lower-dimensional varieties, as we can always reduce to this case. By Honda-Tate theory [10], isogeny classes of simple abelian varieties A over the field $\mathbf{F}$ of q elements are in one-to-one correspondence with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugacy classes of *$q$-Weil numbers*, which are algebraic integers π with the property that all embeddings of π into $\mathbf{C}$ have absolute value $\sqrt{q}$. This correspondence is given by the map sending A to its q-th power Frobenius endomorphism π inside the number field $\mathbf{Q}(\pi) \subset \mathrm{End}(A) \otimes \mathbf{Q}$. The existence of abelian varieties with the properties we want is thus tantamount to the existence of suitable Weil numbers.

Our main result, Algorithm 2.12, constructs suitable q-Weil numbers π in a given *CM-field K*. It exhibits π as a *type norm* of an element in a *reflex field* of K satisfying certain congruences modulo r. The abelian varieties A in the isogeny classes over $\mathbf{F}$ that correspond to these Weil numbers have an $\mathbf{F}$-rational point of order r and embedding degree k with respect to r. Moreover, they are *ordinary*, i.e., $\#A(\overline{\mathbf{F}})[p] = p^g$, where p is the characteristic of $\mathbf{F}$. Theorem 3.1 shows that for fixed K, the expected run time of our algorithm is heuristically polynomial in $\log r$.

For an abelian variety of dimension g over the field $\mathbf{F}$ of q elements, the group $A(\mathbf{F})$ has roughly q^g elements, and one compares this size to r by setting

$$\rho = \frac{g \log q}{\log r}. \tag{1.1}$$

In cryptographic terms, ρ measures the ratio of a pairing-based system's required bandwidth to its security level, so small ρ-values are desirable. *Supersingular* abelian varieties can achieve ρ-values close to 1, but their embedding degrees are limited to a few values that are too small to be practical [4, 8]. Theorem 3.4 discusses the distribution of the (larger) ρ-values we obtain.

In Section 4, we address the issue of the actual construction of abelian varieties corresponding to the Weil numbers found by our algorithm. This is accomplished via the construction in characteristic zero of the abelian varieties having CM by the ring of integers $\mathcal{O}_K$ of K, a hard problem that is far from being algorithmically solved. We discuss the elliptic case $g = 1$, for which reasonable algorithms exist, and the case $g = 2$, for which such algorithms are still in their infancy. For genus $g \geq 3$, we restrict attention to a few families of curves that we can handle at this point. Our final Section 5 provides numerical examples.

2 Weil numbers yielding prescribed embedding degrees

Let $\mathbf{F}$ be a field of q elements, A a g-dimensional simple abelian variety over $\mathbf{F}$, and $K = \mathbf{Q}(\pi) \subset \mathrm{End}(A) \otimes \mathbf{Q}$ the number field generated by the Frobenius endomorphism π. Then π is a q-*Weil number* in K: an algebraic integer with the property that all of its embeddings in $\overline{\mathbf{Q}}$ have complex absolute value $\sqrt{q}$.

The q-Weil number π determines the group order of $A(\mathbf{F})$: the $\mathbf{F}$-rational points of A form the kernel of the endomorphism $\pi - 1$, and in the case where $K = \mathbf{Q}(\pi)$ is the full endomorphism algebra $\mathrm{End}(A) \otimes \mathbf{Q}$ we have

$$\#A(\mathbf{F}) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1).$$

In the case $K = \mathrm{End}(A) \otimes \mathbf{Q}$ we will focus on, K is a *CM-field* of degree $2g$ as in [10, Section 1], i.e., a totally complex quadratic extension of a totally real subfield $K_0 \subset K$.

Proposition 2.1. *Let A, $\mathbf{F}$ and π be as above, and assume $K = \mathbf{Q}(\pi)$ equals $\mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$. Let k be a positive integer, Φ_k the k-th cyclotomic polynomial, and $r \nmid qk$ a prime number. If we have*

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}, \end{aligned}$$

then A has embedding degree k with respect to r.

Proof. The first condition tells us that r divides $\#A(\mathbf{F})$, the second that the order of $\pi\overline{\pi} = q$ in $(\mathbf{Z}/r\mathbf{Z})^*$, which is the embedding degree of A with respect to r, equals k. □

By Honda-Tate theory [10], all q-Weil numbers arise as Frobenius elements of abelian varieties over $\mathbf{F}$. Thus, we can prove the *existence* of an abelian variety A as in Proposition 2.1 by exhibiting a q-Weil number $\pi \in K$ as in that proposition. The following Lemma states what we need.

Lemma 2.2. *Let π be a q-Weil number and $\mathbf{F}$ be the field of q elements. Then there exists a unique isogeny class of simple abelian varieties $A/\mathbf{F}$ with Frobenius π. If $K = \mathbf{Q}(\pi)$ is totally imaginary of degree $2g$ and q is prime, then such A have dimension g, and K is the full endomorphism algebra $\mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$. If furthermore q is unramified in K, then A is ordinary.*

Proof. The main theorem of [10] yields existence and uniqueness, and shows that $E = \mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$ is a central simple algebra over $K = \mathbf{Q}(\pi)$ satisfying

$$2 \cdot \dim(A) = [E : K]^{\frac{1}{2}}[K : \mathbf{Q}].$$

For K totally imaginary of degree $2g$ and q prime, Waterhouse [12, Theorem 6.1] shows that we have $E = K$ and $\dim(A) = g$. By [12, Prop. 7.1], A is ordinary if and only if $\pi + \overline{\pi}$ is prime to $q = \pi\overline{\pi}$ in $\mathcal{O}_K$. Thus if A is not ordinary, the ideals (π) and $(\overline{\pi})$ have a common divisor $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{p}^2 \mid q$, so q ramifies in K. □

Example 2.3. Our general construction is motivated by the case where K is a Galois CM-field of degree $2g$, with cyclic Galois group generated by σ. Here σ^g is complex conjugation, so we can construct an element $\pi \in \mathcal{O}_K$ satisfying $\pi\sigma^g(\pi) = \pi\overline{\pi} \in \mathbf{Z}$ by choosing any $\xi \in \mathcal{O}_K$ and letting $\pi = \prod_{i=1}^{g} \sigma^i(\xi)$. For such π, we have $\pi\overline{\pi} = N_{K/\mathbf{Q}}(\xi) \in \mathbf{Z}$. If $N_{K/\mathbf{Q}}(\xi)$ is a prime q, then π is a q-Weil number in K.

Now we wish to impose the conditions of Proposition 2.1 on π. Let r be a rational prime that splits completely in K, and $\mathfrak{r}$ a prime of $\mathcal{O}_K$ over r. For $i = 1, \ldots, 2g$, put $\mathfrak{r}_i = \sigma^{-i}(\mathfrak{r})$; then the factorization of r in $\mathcal{O}_K$ is $r\mathcal{O}_K = \prod_{i=1}^{2g} \mathfrak{r}_i$. If $\alpha_i \in \mathbf{F}_r = \mathcal{O}_K/\mathfrak{r}_i$ is the residue class of ξ modulo $\mathfrak{r}_i$, then $\sigma^i(\xi)$ modulo $\mathfrak{r}$ is also α_i, so the residue class of π modulo $\mathfrak{r}$ is $\prod_{i=1}^{g} \alpha_i$. Furthermore, the residue class of $\pi\overline{\pi}$ modulo $\mathfrak{r}$ is $\prod_{i=1}^{2g} \alpha_i$. If we choose ξ to satisfy

$$\textstyle\prod_{i=1}^{g} \alpha_i = 1 \in \mathbf{F}_r, \qquad (2.4)$$

we find $\pi \equiv 1 \pmod{\mathfrak{r}}$ and thus $N_{K/\mathbf{Q}}(\pi - 1) \equiv 0 \pmod{r}$. By choosing ξ such that in addition

$$\zeta = \textstyle\prod_{i=1}^{2g} \alpha_i = \prod_{i=g+1}^{2g} \alpha_i \qquad (2.5)$$

is a primitive k-th root of unity in $\mathbf{F}_r^*$, we guarantee that $\pi\overline{\pi} = q$ is a primitive k-th root of unity modulo r. Thus we can try to find a Weil number as in Proposition 2.1 by picking residue classes $\alpha_i \in \mathbf{F}_r^*$ for $i = 1, \ldots, 2g$ meeting the two conditions above, computing some 'small' lift $\xi \in \mathcal{O}_K$ with $(\xi \bmod \mathfrak{r}_i) = \alpha_i$, and testing whether $\pi = \prod_{i=1}^{g} \sigma^i(\xi)$ has prime norm. As numbers of moderate size have a high probability of being prime by the prime number theorem, a small number of choices $(\alpha_i)_i$ should suffice. There are $(r-1)^{2g-2}\varphi(k)$ possible choices for $(\alpha_i)_{i=1}^{2g}$, where φ is the Euler totient function, so for $g > 1$ and large r we are very likely to succeed. For $g = 1$, there are only a few choices $(\alpha_1, \alpha_2) = (1, \zeta)$, but one can try various lifts and thus recover what is known as the Cocks-Pinch algorithm [2, Theorem 4.1] for finding pairing-friendly elliptic curves. □

For arbitrary CM-fields K, the appropriate generalization of the map

$$\xi \mapsto \textstyle\prod_{i=1}^{g} \sigma^i(\xi)$$

in Example 2.3 is provided by the *type norm*. A *CM-type* of a CM-field K of degree $2g$ is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of embeddings of K into its normal closure L such that $\Phi \cup \overline{\Phi} = \{\phi_1, \ldots, \phi_g, \overline{\phi_1}, \ldots, \overline{\phi_g}\}$ is the complete set of embeddings of K into L. The *type norm* $N_\Phi : K \to L$ with respect to Φ is the map

$$N_\Phi : x \longmapsto \textstyle\prod_{i=1}^{g} \phi_i(x),$$

which clearly satisfies

$$N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbf{Q}}(x) \in \mathbf{Q}. \qquad (2.6)$$

If K is not Galois, the type norm N_Φ does not map K to itself, but to its *reflex field* $\widehat{K}$ with respect to Φ. To end up in K, we can however take the type norm with respect to the *reflex type* Ψ, which we will define now (cf. [9, Section 8]).

Let G be the Galois group of $L/\mathbf{Q}$, and H the subgroup fixing K. Then the $2g$ left cosets of H in G can be viewed as the embeddings of K in L, and this makes the CM-type Φ into a set of g left cosets of H for which we have $G/H = \Phi \cup \overline{\Phi}$. Let S be the union of the left cosets in Φ, and put $\widehat{S} = \{\sigma^{-1} : \sigma \in S\}$. Let $\widehat{H} = \{\gamma \in G : \gamma S = S\}$ be the stabilizer of S in G. Then $\widehat{H}$ defines a subfield $\widehat{K}$ of L, and as we have $\widehat{H} = \{\gamma \in G : \widehat{S}\gamma = \widehat{S}\}$ we can interpret $\widehat{S}$ as a union of left cosets of $\widehat{H}$ inside G. These cosets define a set of embeddings Ψ of $\widehat{K}$ into L. We call $\widehat{K}$ the *reflex field* of (K, Φ) and we call Ψ the *reflex type.*

Lemma 2.7. *The field $\widehat{K}$ is a CM-field. It is generated over $\mathbf{Q}$ by the sums $\sum_{\phi\in\Phi}\phi(x)$ for $x \in K$, and Ψ is a CM-type of $\widehat{K}$. The type norm N_Φ maps K to $\widehat{K}$.*

Proof. The first two statements are proved in [9, Chapter II, Proposition 28] (though the definition of $\widehat{H}$ differs from ours, because Shimura lets G act from the right). For the last statement, notice that for $\gamma \in \widehat{H}$, we have $\gamma S = S$, so $\gamma \prod_{\phi\in\Phi}\phi(x) = \prod_{\phi\in\Phi}\phi(x)$. □

A CM-type Φ of K is *induced* from a CM-subfield $K' \subset K$ if it is of the form $\Phi = \{\phi : \phi|_{K'} \in \Phi'\}$ for some CM-type Φ' of K'. In other words, Φ is induced from K' if and only if S as above is a union of left cosets of $\mathrm{Gal}(L/K')$. We call Φ *primitive* if it is not induced from a strict subfield of K; primitive CM-types correspond to simple abelian varieties [9]. Notice that the reflex type Ψ is primitive by definition of $\widehat{K}$, and that (K, Φ) is induced from the reflex of its reflex. In particular, if Φ is primitive, then the reflex of its reflex is (K, Φ) itself. For K Galois and Φ primitive we have $\widehat{K} = K$, and the reflex type of Φ is $\Psi = \{\phi^{-1} : \phi \in \Phi\}$.

For CM-fields K of degree 2 or 4 with primitive CM-types, the reflex field $\widehat{K}$ has the same degree as K. This fails to be so for $g \geq 3$.

Lemma 2.8. *If K has degree $2g$, then the degree of $\widehat{K}$ divides $2^g g!$.*

Proof. We have $K = K_0(\sqrt{\eta})$, with K_0 totally real and $\eta \in K$ totally negative. The normal closure L of K is obtained by adjoining to the normal closure $\widetilde{K_0}$ of K_0, which has degree dividing $g!$, the square roots of the g conjugates of η. Thus L is of degree dividing $2^g g!$, and $\widehat{K}$ is a subfield of L. □

For a 'generic' CM field K the degree of L is exactly $2^g g!$, and $\widehat{K}$ is a field of degree 2^g generated by $\sum_\sigma \sqrt{\sigma(\eta)}$, with σ ranging over $\mathrm{Gal}(K_0/\mathbf{Q})$.

From (2.6) and Lemma 2.7, we find that for every $\xi \in \mathcal{O}_{\widehat{K}}$, the element $\pi = N_\Psi(\xi)$ is an element of $\mathcal{O}_K$ that satisfies $\pi\overline{\pi} \in \mathbf{Z}$. To make π satisfy the conditions of Proposition 2.1, we need to impose conditions modulo r on ξ in $\widehat{K}$. Suppose r splits completely in K, and therefore in its normal closure L and in the reflex field $\widehat{K}$ with respect to Φ. Pick a prime $\mathfrak{R}$ over r in L, and write $\mathfrak{r}_\psi = \psi^{-1}(\mathfrak{R}) \cap \mathcal{O}_{\widehat{K}}$ for $\psi \in \Psi$. Then the factorization of r in $\mathcal{O}_{\widehat{K}}$ is

$$r\mathcal{O}_{\widehat{K}} = \prod_{\psi\in\Psi} \mathfrak{r}_\psi \overline{\mathfrak{r}_\psi}. \tag{2.9}$$

Theorem 2.10. *Let (K,Φ) be a CM-type and $(\widehat{K},\Psi)$ its reflex. Let $r \equiv 1 \pmod{k}$ be a prime that splits completely in K, and write its factorization in $\mathcal{O}_{\widehat{K}}$ as in* (2.9). *Given $\xi \in \mathcal{O}_{\widehat{K}}$, write $(\xi \bmod \mathfrak{r}_\psi) = \alpha_\psi \in \mathbf{F}_r$ and $(\xi \bmod \overline{\mathfrak{r}_\psi}) = \beta_\psi \in \mathbf{F}_r$ for $\psi \in \Psi$. If we have*

$$\prod\nolimits_{\psi\in\Psi} \alpha_\psi = 1 \qquad \text{and} \qquad \prod\nolimits_{\psi\in\Psi} \beta_\psi = \zeta \tag{2.11}$$

for some primitive k-th root of unity $\zeta \in \mathbf{F}_r^*$, then $\pi = N_\Psi(\xi) \in \mathcal{O}_K$ satisfies $\pi\overline{\pi} \in \mathbf{Z}$ and

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}. \end{aligned}$$

Proof. This is a straightforward generalization of the argument in Example 2.3. The conditions (2.11) generalize (2.4) and (2.5), and imply in the present context that $\pi - 1 \in \mathcal{O}_K$ and $\Phi_k(\pi\overline{\pi}) \in \mathbf{Z}$ are in the prime $\mathfrak{R} \subset \mathcal{O}_L$ over r that underlies the factorization (2.9). □

If the element π in Theorem 2.10 generates K and $\mathrm{N}_{K/\mathbf{Q}}(\pi)$ is a prime q that is unramified in K, then by Lemma 2.2 π is a q-Weil number corresponding to an ordinary abelian variety A over $\mathbf{F} = \mathbf{F}_q$ with endomorphism algebra K and Frobenius element π. By Proposition 2.1, A has embedding degree k with respect to r. This leads to the following algorithm.

Algorithm 2.12.

Input: a CM-field K of degree $2g \geq 4$, a primitive CM-type Φ of K, a positive integer k, and a prime $r \equiv 1 \pmod{k}$ that splits completely in K.

Output: a prime q and a q-Weil number $\pi \in K$ corresponding to an ordinary, simple abelian variety $A/\mathbf{F}_q$ with embedding degree k with respect to r.

1. Compute a Galois closure L of K and the reflex $(\widehat{K},\Psi)$ of (K,Φ). Set $\widehat{g} \leftarrow \frac{1}{2}\deg \widehat{K}$ and write $\Psi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$.
2. Fix a prime $\mathfrak{R} \mid r$ of $\mathcal{O}_L$, and compute the factorization of r in $\mathcal{O}_{\widehat{K}}$ as in (2.9).
3. Compute a primitive k-th root of unity $\zeta \in \mathbf{F}_r^*$.
4. Choose random $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbf{F}_r^*$.
5. Set $\alpha_{\widehat{g}} \leftarrow \prod_{i=1}^{\widehat{g}-1} \alpha_i^{-1} \in \mathbf{F}_r^*$ and $\beta_{\widehat{g}} \leftarrow \zeta \prod_{i=1}^{\widehat{g}-1} \beta_i^{-1} \in \mathbf{F}_r^*$.
6. Compute $\xi \in \mathcal{O}_{\widehat{K}}$ such that $(\xi \mod \mathfrak{r}_{\psi_i}) = \alpha_i$ and $(\xi \mod \overline{\mathfrak{r}_{\psi_i}}) = \beta_i$ for $i = 1, 2, \ldots, \widehat{g}$.
7. Set $q \leftarrow \mathrm{N}_{\widehat{K}/\mathbf{Q}}(\xi)$. If q is not prime, go to Step (4).
8. Set $\pi \leftarrow N_\Psi(\xi)$. If q is not unramified in K, or π does not generate K, go to Step (4).
9. Return q and π.

Remark 2.13. We require $g \geq 2$ in Algorithm 2.12, as the case $g = 1$ is already covered by Example 2.3, and requires a slight adaptation.

The condition that r be prime is for simplicity of presentation only; the algorithm easily extends to square-free values of r that are given as products of splitting primes. Such r are required, for example, by the cryptosystem of [1].

3 Performance of the algorithm

Theorem 3.1. *If the field K is fixed, then the heuristic expected run time of Algorithm 2.12 is polynomial in* $\log r$.

Proof. The algorithm consists of a precomputation for the field K in Steps (1)–(3), followed by a loop in Steps (4)–(7) that is performed until an element ξ is found that has prime norm $N_{\widehat{K}/\mathbf{Q}}(\xi) = q$, and we also find in Step (8) that q is unramified in K and the type norm $\pi = N_{\Psi}(\xi)$ generates K.

The primality condition in Step (7) is the 'true' condition that becomes harder to achieve with increasing r, whereas the conditions in Step (8), which are necessary to guarantee correctness of the output, are so extremely likely to be fulfilled (especially in cryptographic applications where K is small and r is large) that they will hardly ever fail in practice and only influence the run time by a constant factor.

As ξ is computed in Step (6) as the lift to $\mathcal{O}_{\widehat{K}}$ of an element $\overline{\xi} \in \mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbf{F}_r)^{2\widehat{g}}$, its norm can be bounded by a constant multiple of $r^{2\widehat{g}}$. Heuristically, $q = \mathrm{N}_{\widehat{K}/\mathbf{Q}}(\xi)$ behaves as a random number, so by the prime number theorem it will be prime with probability at least $(2\widehat{g}\log r)^{-1}$, and we expect that we need to repeat the loop in Steps (4)–(7) about $2\widehat{g}\log r$ times before finding ξ of prime norm q. As each of the steps is polynomial in $\log r$, so is the expected run time up to Step (7), and we are done if we show that the conditions in Step (8) are met with some positive probability if K is fixed and r is sufficiently large.

For q being unramified in K, one simply notes that only finitely many primes ramify in the field K (which is fixed) and that q tends to infinity with r, since r divides $\mathrm{N}_{K/\mathbf{Q}}(\pi - 1) \leq (\sqrt{q} + 1)^{2g}$.

Finally, we show that π generates K with probability tending to 1 as r tends to infinity. Suppose that for every vector $v \in \{0,1\}^{\widehat{g}}$ that is not all 0 or 1, we have

$$\textstyle\prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i} \neq 1. \tag{3.2}$$

This set of $2^{\widehat{g}} - 2$ (dependent) conditions on the $2\widehat{g} - 2$ independent random variables α_i, β_i for $1 \leq i < \widehat{g}$ is satisfied with probability at least $1 - (2^{\widehat{g}} - 2)/(r - 1)$. For any automorphism ϕ of L, the set $\phi \circ \Psi$ is a CM-type of $\widehat{K}$ and there is a $v \in \{0,1\}^{\widehat{g}}$ such that $v_i = 0$ if $\phi \circ \Psi$ contains ψ_i and $v_i = 1$ otherwise. Then α_i is $(\psi_i(\xi) \bmod \mathfrak{R})$, while β_i is $(\overline{\psi_i(\xi)} \bmod \mathfrak{R})$, so $(\pi/\phi(\pi) \bmod \mathfrak{R})$ is $\prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i}$. By (3.2), if this expression is 1 then $v = 0$ or $v = 1$, so $\phi \circ \Psi = \Psi$ or $\phi \circ \Psi = \Psi$, which by definition of the reflex is equivalent to ϕ or $\overline{\phi}$ being trivial on K, i.e., to ϕ being trivial on the maximal real subfield K_0. Thus if (3.2) holds, then $\phi(\pi) = \pi$ implies that ϕ is trivial on K_0, hence $K_0 \subset \mathbf{Q}(\pi)$. Since $\pi \in K$ is not real (otherwise, $q = \pi^2$ ramifies in K), this implies that $K = \mathbf{Q}(\pi)$. □

In order to maximize the likelihood of finding prime norms, one should minimize the norm of the lift ξ computed in the Chinese Remainder Step (6). This involves minimizing a norm function of degree $2\widehat{g}$ in $2\widehat{g}$ integral variables, which is already infeasible for $\widehat{g} = 2$.

In practice, for given r, one lifts a standard basis of $\mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbf{F}_r)^{2\widehat{g}}$ to $\mathcal{O}_{\widehat{K}}$. Multiplying those lifts by integer representatives for the elements α_i and β_i of $\mathbf{F}_r$, one quickly obtains lifts ξ. We also choose, independently of r, a $\mathbf{Z}$-basis of $\mathcal{O}_{\widehat{K}}$ consisting of elements that are 'small' with respect to all absolute values of $\widehat{K}$. We translate ξ by multiples of r to lie in rF, where F is the fundamental parallelotope in $\widehat{K} \otimes \mathbf{R}$ consisting of those elements that have coordinates in $(-\frac{1}{2}, \frac{1}{2}]$ with respect to our chosen basis.

If we denote the maximum on $F \cap \widehat{K}$ of all complex absolute values of $\widehat{K}$ by $M_{\widehat{K}}$, we have $q = N_{\widehat{K}/\mathbf{Q}}(\xi) \leq (rM_{\widehat{K}})^{2\widehat{g}}$. For the ρ-value (1.1) we find

$$\rho \leq 2g\widehat{g}(1 + \log M_{\widehat{K}}/\log r), \tag{3.3}$$

which is approximately $2g\widehat{g}$ if r gets large with respect to $M_{\widehat{K}}$. We would like ρ to be small, but this is not what one obtains by lifting random admissible choices of $\overline{\xi}$.

Theorem 3.4. *If the field K is fixed and r is large, we expect that (1) the output q of Algorithm 2.12 yields $\rho \approx 2g\widehat{g}$, and (2) an optimal choice of $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 2.10 yields $\rho \approx 2g$.*

Open problem 3.5. *Find an efficient algorithm to compute an element $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 2.10 for which $\rho \approx 2g$.*

We will prove Theorem 3.4 via a series of lemmas. Let $H_{r,k}$ be the subset of the parallelotope $rF \subset \widehat{K} \otimes \mathbf{R}$ consisting of those $\xi \in rF \cap \mathcal{O}_{\widehat{K}}$ that satisfy the two congruence conditions (2.11) for a given embedding degree k. Heuristically, we will treat the elements of $H_{r,k}$ as random elements of rF with respect to the distributions of complex absolute values and norm functions. We will also use the fact that, as $\widehat{K}$ is totally complex of degree $2\widehat{g}$, the $\mathbf{R}$-algebra $\widehat{K} \otimes \mathbf{R}$ is naturally isomorphic to $\mathbf{C}^{\widehat{g}}$. We assume throughout that $g \geq 2$.

Lemma 3.6. *Fix the field K. Under our heuristic assumption, there exists a constant $c_1 > 0$ such that for all $\varepsilon > 0$, the probability that a random $\xi \in H_{r,k}$ satisfies $q < r^{2(\widehat{g}-\varepsilon)}$ is less than $c_1 r^{-\varepsilon}$.*

Proof. The probability that a random ξ lies in the set $V = \{z \in \mathbf{C}^{\widehat{g}} : \prod |z_i|^2 \leq r^{2(\widehat{g}-\varepsilon)}\} \cap rF$ is the quotient of the volume of V by the volume $2^{-\widehat{g}}\sqrt{|\Delta_{\widehat{K}}|}r^{2\widehat{g}}$ of rF, where $\Delta_{\widehat{K}}$ is the discriminant of $\widehat{K}$. Now V is contained inside $W = \{z \in \mathbf{C}^{\widehat{g}} : \prod |z_i|^2 \leq r^{2(\widehat{g}-\varepsilon)}, |z_i| \leq rM_{\widehat{K}}\}$, which has volume

$$(2\pi)^{\widehat{g}} \int\limits_{\substack{x \in [0, rM_{\widehat{K}}]^{\widehat{g}} \\ \prod |x_i|^2 \leq r^{2(\widehat{g}-\varepsilon)}}} \prod |x_i| dx \quad < \quad (2\pi)^{\widehat{g}} \int\limits_{x \in [0, rM_{\widehat{K}}]^{\widehat{g}}} r^{\widehat{g}-\varepsilon} dx \quad = \quad (2\pi M_{\widehat{K}})^{\widehat{g}} r^{2\widehat{g}-\varepsilon},$$

so a random ξ lies in V with probability less than $(4\pi M_{\widehat{K}})^{\widehat{g}} |\Delta_{\widehat{K}}|^{-1/2} r^{-\varepsilon}$. □

Lemma 3.7. *There exists a number $Q_{\widehat{K}}$, depending only on $\widehat{K}$, such that for any positive real number $X < rQ_{\widehat{K}}$, the expected number of $\xi \in H_{r,k}$ with all absolute values below X is*

$$\frac{\varphi(k)(2\pi)^{\widehat{g}}}{|\Delta_{\widehat{K}}|}\frac{X^{2\widehat{g}}}{r^2}.$$

Proof. Let $Q_{\widehat{K}} > 0$ be a lower bound on $\widehat{K} \setminus F$ for the maximum of all complex absolute values, so the box $V_X \subset \widehat{K} \otimes \mathbf{R}$ consisting of those elements that have all absolute values below X lies completely inside $(X/Q_{\widehat{K}})F \subset rF$. The volume of V_X in $\widehat{K} \otimes \mathbf{R}$ is $(\pi X^2)^{\widehat{g}}$, while rF has volume $2^{-\widehat{g}}\sqrt{|\Delta_{\widehat{K}}|}r^{2\widehat{g}}$. The expected number of $\xi \in H_{r,k}$ satisfying $|\xi| < X$ for all absolute values is $\#H_{r,k} = r^{2\widehat{g}-2}\varphi(k)$ times the quotient of these volumes. □

Lemma 3.8. *Fix the field K. Under our heuristic assumption, there exists a constant c_2 such that for all positive $\varepsilon < 2\widehat{g} - 2$, if r is sufficiently large, then we expect the number of $\xi \in H_{r,k}$ satisfying $N_{\widehat{K}/\mathbf{Q}}(\xi) < r^{2+\varepsilon}$ to be at least $c_2 r^{\varepsilon}$.*

Proof. Any ξ as in Lemma 3.7 satisfies $N_{\widehat{K}/\mathbf{Q}}(\xi) < X^{2\widehat{g}}$, so we apply the lemma to $X = r^{(1/\widehat{g}+\varepsilon/2\widehat{g})}$, which is less than $rQ_{\widehat{K}}$ for large enough r and $\epsilon < 2\widehat{g}-2$. □

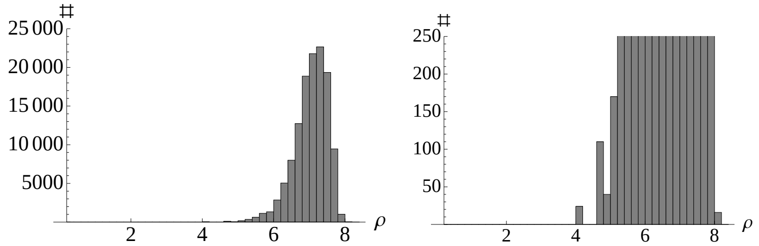
Lemma 3.9. *Fix the field K. Under our heuristic assumption, for all $\varepsilon > 0$, if r is large enough, we expect there to be no $\xi \in H_{r,k}$ satisfying $N_{\widehat{K}/\mathbf{Q}}(\xi) < r^{2-\varepsilon}$.*

Proof. Let $\widehat{\mathcal{O}}$ be the ring of integers of the maximal real subfield of $\widehat{K}$. Let U be the subgroup of norm one elements of $\widehat{\mathcal{O}}^*$. We embed U into $\mathbf{R}^{\widehat{g}}$ by mapping $u \in U$ to the vector $l(u)$ of logarithms of absolute values of u. The image is a complete lattice in the $(\widehat{g}-1)$-dimensional space of vectors with coordinate sum 0. Fix a fundamental parallelotope F' for this lattice. Let ξ_0 be the element of $H_{r,k}$ of smallest norm. Since the conditions (2.11), as well as the norm of ξ_0, are invariant under multiplication by elements of U, we may assume without loss of generality that $l(\xi_0)$ is inside $F' + \mathbf{C}(1,\ldots,1)$. Then every difference of two entries of $l(\xi_0)$ is bounded, and hence every quotient of absolute values of ξ_0 is bounded from below by a positive constant c_3 depending only on K. In particular, if m is the maximum of all absolute values of ξ_0, then $N_{\widehat{K}/\mathbf{Q}}(\xi) > (c_3 m)^{2\widehat{g}}$. Now suppose ξ_0 has norm below $r^{2-\varepsilon}$. Then all absolute values of ξ_0 are below $X = r^{(1/\widehat{g}-\varepsilon/2\widehat{g})}/c_3$, and $X < rQ_{\widehat{K}}$ for r sufficiently large. Now Lemma 3.7 implies that the expected number of $\xi \in H_{r,k}$ with all absolute values below X is a constant times $r^{-\varepsilon}$, so for any sufficiently large r we expect there to be no such ξ, a contradiction. □

Proof *(of Theorem 3.4)*. The upper bound $\rho \lesssim 2g\widehat{g}$ follows from (3.3). Lemma 3.6 shows that for any $\varepsilon > 0$, the probability that ρ is smaller than $2g\widehat{g}-\varepsilon$ tends to zero as r tends to infinity, thus proving the lower bound $\rho \gtrsim 2g\widehat{g}$. Lemma 3.8 shows that for any $\varepsilon > 0$, if r is sufficiently large then we expect there to exist a ξ with ρ-value at most $2g+\varepsilon$, thus proving the bound $\rho \lesssim 2g$. Lemma 3.9 shows that we expect $\rho > 2g-\varepsilon$ for the optimal ξ, which proves the bound $\rho \gtrsim 2g$. □

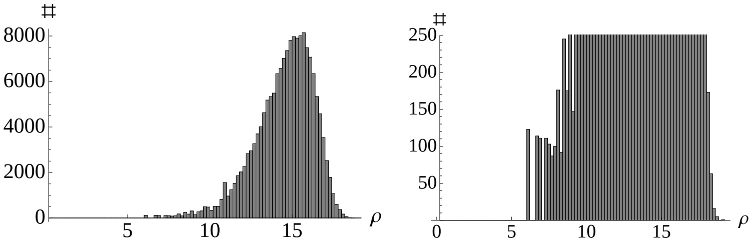
For very small values of r we are able to do a brute-force search for the smallest q by testing all possible values of $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1}$ in Step 4 of Algorithm 2.12. We performed two such searches, one in dimension 2 and one in dimension 3. The experimental results support our heuristic evidence that $\rho \approx 2g$ is possible with a smart choice in the algorithm, and that $\rho \approx 2g\widehat{g}$ is achieved with a randomized algorithm.

Example 3.10. Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of K defined by $\phi_n(\zeta_5) = e^{2\pi i n/5}$. We ran Algorithm 2.12 with $r = 1021$ and $k = 2$, and tested all possible values of α_1, β_1. The total number of primes q found was 125578, and the corresponding ρ-values were distributed as follows:



The smallest q found was 2023621, giving a ρ-value of 4.19. The curve over $\mathbf{F} = F_q$ for which the Jacobian has this ρ-value is $y^2 = x^5 + 18$, and the number of points on its Jacobian is 4092747290896.

Example 3.11. Take $K = \mathbf{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM-type of K defined by $\phi_i(\zeta_7) = e^{2\pi i/7}$. We ran Algorithm 2.12 with $r = 29$ and $k = 4$, and tested all possible values of $\alpha_1, \alpha_2, \beta_1, \beta_2$. The total number of primes q found was 162643, and the corresponding ρ-values were distributed as follows:



The smallest q found was 911, giving a ρ-value of 6.07. The curve over $\mathbf{F} = F_q$ for which the Jacobian has this ρ-value is $y^2 = x^7 + 34$, and the number of points on its Jacobian is 778417333.

Example 3.12. Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of K defined by $\phi_i(\zeta_5) = e^{2\pi i/5}$. We ran Algorithm 2.12 with $r = 2^{160} + 685$ and $k = 10$, and tested 2^{20} random values of α_1, β_1. The total number of primes q found was 7108. Of these primes, 6509 (91.6%) produced ρ-values between 7.9 and 8.0, while 592 (8.3%) had ρ-values between 7.8 and 7.9. The smallest q found had 623 binary digits, giving a ρ-value of 7.78.

4 Constructing abelian varieties with given Weil numbers

Our Algorithm 2.12 yields q-Weil numbers $\pi \in K$ that correspond, in the sense of Honda and Tate [10], to isogeny classes of ordinary, simple abelian varieties over prime fields that have a point of order r and embedding degree k with respect to r. It does not give a method to explicitly construct an abelian variety A with Frobenius $\pi \in K$. In this section we focus on the problem of explicitly constructing such varieties using complex multiplication techniques.

The key point of the complex multiplication construction is the fact that every ordinary, simple abelian variety over $\mathbf{F} = \mathbf{F}_q$ with Frobenius $\pi \in K$ arises as the reduction at a prime over q of some abelian variety A_0 in characteristic zero that has CM by the ring of integers of K. Thus if we have fixed our K as in Algorithm 2.12, we can solve the construction problem for all ordinary Weil numbers coming out of the algorithm by compiling the finite list of $\overline{\mathbf{Q}}$-isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$. There will be one $\overline{\mathbf{Q}}$-isogeny class for each equivalence class of primitive CM-types of K, where Φ and Φ' are said to be equivalent if we have $\Phi = \Phi' \circ \sigma$ for an automorphism σ of K. As we can choose our favorite field K of degree $2g$ to produce abelian varieties of dimension g, we can pick fields K for which such lists already occur in the literature.

From representatives of our list of isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$, we obtain a list $\mathcal{A}$ of abelian varieties over $\mathbf{F}$ with CM by $\mathcal{O}_K$ by reducing at some fixed prime $\mathfrak{q}$ over q. Changing the choice of the prime $\mathfrak{q}$ amounts to taking the reduction at $\mathfrak{q}$ of a conjugate abelian variety, which also has CM by $\mathcal{O}_K$ and hence is $\overline{\mathbf{F}}$-isogenous to one already in the list.

For every abelian variety $A \in \mathcal{A}$, we compute the set of its twists, i.e., all the varieties up to $\mathbf{F}$-isomorphism that become isomorphic to A over $\overline{\mathbf{F}}$. There is at least one twist B of an element $A \in \mathcal{A}$ satisfying $\#B(\mathbf{F}) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1)$, and this B has a point of order r and the desired embedding degree.

Note that while efficient point-counting algorithms do not exist for varieties of dimension $g > 1$, we can determine probabilistically whether an abelian variety has a given order by choosing a random point, multiplying by the expected order, and seeing if the result is the identity.

The complexity of the construction problem rapidly increases with the genus $g = [K : \mathbf{Q}]/2$, and it is fair to say that we only have satisfactory general methods at our disposal in very small genus.

In genus one, we are dealing with elliptic curves. The j-invariants of elliptic curves over $\mathbf{C}$ with CM by $\mathcal{O}_K$ are the roots of the *Hilbert class polynomial* of K, which lies in $\mathbf{Z}[X]$. The degree of this polynomial is the class number h_K of K, and it can be computed in time $\widetilde{O}(|\Delta_K|)$.

For genus 2, we have to construct abelian surfaces. Any principally polarized abelian surface is the Jacobian of a genus 2 curve, and all genus 2 curves are hyperelliptic. There is a theory of class polynomials analogous to that for elliptic curves, as well as several algorithms to compute these polynomials, which lie in $\mathbf{Q}[X]$. The genus 2 algorithms are not as well-developed as those for elliptic curves; at present they can handle only very small quartic CM-fields, and there exists no rigorous run time estimate. From the roots in $\mathbf{F}$ of these polynomials, we can compute the genus 2 curves using Mestre's algorithm.

Any three-dimensional principally polarized abelian variety is isogenous to the Jacobian of a genus 3 curve. There are two known families of genus 3 curves over $\mathbf{C}$ whose Jacobians have CM by an order of dimension 6. The first family, due to Weng [14], gives hyperelliptic curves whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(i)$. The second family, due to Koike and Weng [5], gives Picard curves (curves of the form $y^3 = f(x)$ with $\deg f = 4$) whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(\zeta_3)$.

Explicit CM-theory is mostly undeveloped for dimension ≥ 3. Moreover, most principally polarized abelian varieties of dimension ≥ 4 are not Jacobians, as the moduli space of Jacobians has dimension $3g - 3$, while the moduli space of abelian varieties has dimension $g(g+1)/2$. For implementation purposes we prefer Jacobians or even hyperelliptic Jacobians, as these are the only abelian varieties for which group operations can be computed efficiently.

In cases where we cannot compute every abelian variety in characteristic zero with CM by $\mathcal{O}_K$, we use a single such variety A and run Algorithm 2.12 for each different CM-type of K until it yields a prime q for which the reduction of A mod q is in the correct isogeny class. An example for $K = \mathbf{Q}(\zeta_{2p})$ with p prime is given by the Jacobian of $y^2 = x^p + a$, which has dimension $g = (p-1)/2$.

5 Numerical examples

We implemented Algorithm 2.12 in MAGMA and used it to compute examples of hyperelliptic curves of genus 2 and 3 over fields of cryptographic size for which the Jacobians are pairing-friendly. The subgroup size r is chosen so that the discrete logarithm problem in $A[r]$ is expected to take roughly 2^{80} steps. The embedding degree k is chosen so that $r^{k/g} \approx 1024$; this would be the ideal embedding degree for the 80-bit security level if we could construct varieties over $\mathbf{F} = \mathbf{F}_q$ with $\#A(\mathbf{F}) \approx r$. Space constraints prevent us from giving the group orders for each Jacobian, but we note that a set of all possible q-Weil numbers in K, and hence all possible group orders, can be computed from the factorization of q in K.

Example 5.1. Let $\eta = \sqrt{-2 + \sqrt{2}}$ and let K be the degree-4 Galois CM field $\mathbf{Q}(\eta)$. Let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of K such that $\operatorname{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.12 with CM type (K, Φ), $r = 2^{160} - 1679$, and $k = 13$. The algorithm output the following field size:

$$\begin{aligned} q = {} & 3134605780829315791376234453100527571554468021964133849744950023887230035061 7165 \ \backslash \\ & 40892530853973205578151445285706963588204818794198739264123849002104890399459807 \ \backslash \\ & 4631327324771546515176667557 02167 \quad \text{(640 bits)} \end{aligned}$$

There is a single $\overline{\mathbf{F}}_q$-isomorphism class of curves over $\mathbf{F}_q$ whose Jacobians have CM by $\mathcal{O}_K$ and it has been computed in [11]; the desired twist turns out to be $C : y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$. The ρ-value of $\operatorname{Jac}(C)$ is 7.99.

Example 5.2. Let $\eta = \sqrt{-30 + 2\sqrt{5}}$ and let K be the degree-4 non-Galois CM field $\mathbf{Q}(\eta)$. The reflex field $\widehat{K}$ is $\mathbf{Q}(\omega)$ where $\omega = \sqrt{-15 + 2\sqrt{55}}$. Let Ψ be the CM type of K such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.12 with the CM type (K, Φ), subgroup size $r = 2^{160} - 1445$, and embedding degree $k = 13$. The algorithm output the following field size:

$$\begin{aligned} q = {} & 1109165488716951297136540704029359957997637815897340518163508137915707830213092 7 \backslash \\ & 516520036237861925310771273889444533035840913344924527526930940891929865415338 19 \backslash \\ & 35518866167783400231181308345981461 \quad (645 \text{ bits}) \end{aligned}$$

The class polynomials for K can be found in the preprint version of [13]. We used the roots of the class polynomials mod q to construct curves over $\mathbf{F}_q$ with CM by $\mathcal{O}_K$. As K is non-Galois with class number 4, there are 8 isomorphism classes of curves in 2 isogeny classes. We found a curve C in the correct isogeny class with equation $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$$\begin{aligned} a_3 = {} & 37909827361040902434390338072754918705969566622865244598340785379492062293493023 \backslash \\ & 07887220632471591953460261515915189503199574055791975955834407879578484212700263 \backslash \\ & 26004014371084570321085865481897 69 \\ a_2 = {} & 18960350992731066141619447121681062843951822341216980089632110294900985267348927 \backslash \\ & 56700435114431697785479098782721806327279074708206429263751983109351250831853735 \backslash \\ & 19012820004210701825726715060564 32 \\ a_1 = {} & 69337488142924022910219499907432470174331183248226721112535199929650663260487281 \backslash \\ & 50177351432967251207037416196614255668796808046612641767922273749125366541534440 \backslash \\ & 58824657313765233049070410064645 04 \\ a_0 = {} & 31678142561939596895646021753607012342277658384169880961095701825776704126204818 \backslash \\ & 48230687778916790603969757571449880417861689471274167016388608712966941178120424 \backslash \\ & 38133326172720384940201785611195 64 \end{aligned}$$

The ρ-value of $\mathrm{Jac}(C)$ is 8.06.

Example 5.3. Let K be the degree-6 Galois CM field $\mathbf{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM type of K such that $\phi_n(\zeta_7) = e^{2\pi in/7}$. We used the CM type (K, Φ) to construct a curve C whose Jacobian has embedding degree 17 with respect to $r = 2^{180} - 7427$. Since K has class number 1 and one equivalence class of primitive CM types, there is a unique isomorphism class of curves in characteristic zero whose Jacobians are simple and have CM by K; these curves are given by $y^2 = x^7 + a$. Algorithm 2.12 output the following field size:

$$\begin{aligned} q = {} & 15755841381197715359178780201436879305777694686713746395506787614025008121759749 \backslash \\ & 72634937716254216816917600718698808129260457040637146802812702044068612772692590 \backslash \\ & 77188966205156107806823000096120874915612017184924206843204621759232946263357637 \backslash \\ & 19251697987740263891168971441085531481109276328740299111531260484082698571214310 \backslash \\ & 33499 \quad (1077 \text{ bits}) \end{aligned}$$

The equation of the curve C is $y^2 = x^7 + 10$. The ρ-value of $\mathrm{Jac}(C)$ is 17.95.

We conclude with an example of an 8-dimensional abelian variety found using our algorithms. We started with a single CM abelian variety A in characteristic zero and applied our algorithm to different CM-types until we found a prime q for which the reduction has the given embedding degree.

Example 5.4. Let $K = \mathbf{Q}(\zeta_{17})$. We set $r = 1021$ and $k = 10$ and ran Algorithm 2.12 repeatedly with different CM types for K. Given the output, we tested the Jacobians of twists of $y^2 = x^{17} + 1$ for the specified number of points. We found that the curve $y^2 = x^{17} + 30$ has embedding degree 10 with respect to r over the field $\mathbf{F}$ of order

$$q = 68696035083224346148549085355452089780388 19437.$$

The CM type was

$$\Phi = \{\phi_1, \phi_3, \phi_5, \phi_6, \phi_8, \phi_{10}, \phi_{13}, \phi_{15}\},$$

where $\phi_n(\zeta_{17}) = e^{2\pi i n/17}$. The ρ-value of $\mathrm{Jac}(C)$ is 121.9.

References

1. D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *TCC '05*, Springer LNCS **3378**, 2005, 325–341.
2. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Cryptology eprint 2006/371, available at `http://eprint.iacr.org`.
3. G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," *Math. Comp.* **62** (1994), 865–874.
4. S. Galbraith, "Supersingular curves in cryptography," in *ASIACRYPT '01*, Springer LNCS **2248**, 2001, 495–513.
5. K. Koike and A. Weng, "Construction of CM Picard curves," *Math. Comp.* **74** (2004), 499–518.
6. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory* **39** (1993) 1639–1646.
7. K. Paterson, "Cryptography from pairings," in *Advances in Elliptic Curve Cryptography*, ed. I. F. Blake, G. Seroussi, and N. P. Smart, Cambridge University Press, 2005, 215–251.
8. K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology," in *CRYPTO '02*, Springer LNCS **2442**, 2002, 336–353.
9. G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.
10. J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)," Séminaire Bourbaki 1968/69, Springer Lect. Notes in Math. **179** (1971) exposé 352, 95–110.
11. P. van Wamelen, "Examples of genus two CM curves defined over the rationals," *Math. Comp.* **68** (1999), 307–320.
12. W. C. Waterhouse, "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup.* (4) **2** (1969) 521–560.
13. A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography," *Math. Comp.* **72** (2003), 435–458.
14. A. Weng, "Hyperelliptic CM-curves of genus 3," *Journal of the Ramanujan Mathematical Society* **16**:4 (2001), 339–372.