

Abelian varieties with prescribed embedding degree

David Freeman¹, Peter Stevenhagen² and Marco Streng²

¹University of California, Berkeley

Supported by a National Defense
Science and Engineering Graduate Fellowship



²Universiteit Leiden

Supported by the European Commission under
contract MRTN-CT-2006-035495



Universiteit Leiden



MARIE CURIE ACTIONS

ANTS-VIII, Banff, Alberta (Canada)
May 20, 2008

Overview

We construct *Weil numbers* that correspond to abelian varieties with prescribed *embedding degree*.

Overview:

- ▶ What is the embedding degree?
- ▶ What are Weil numbers and how to construct the corresponding abelian varieties?
- ▶ Our actual construction.

The embedding degree

- ▶ Let A be an abelian variety over a finite field $\mathbb{F} = \mathbb{F}_q$ and let $r \nmid q$ be a prime dividing $\#A(\mathbb{F})$.

- ▶ Two pairings:

$$\text{Weil: } A(\mathbb{F})[r] \times \widehat{A}(\mathbb{F})[r] \rightarrow \mu_r(\mathbb{F}),$$

$$\text{Tate: } A(\mathbb{F})[r] \times \widehat{A}(\mathbb{F})/r\widehat{A}(\mathbb{F}) \rightarrow \mathbb{F}^*/(\mathbb{F}^*)^r \cong \mu_r(\mathbb{F}).$$

- ▶ The **embedding degree** k of A with respect to r is the degree of the field extension $\mathbb{F}(\zeta_r)/\mathbb{F}$.
- ▶ For random r and q , the embedding degree grows like r .
- ▶ If k is small and the discrete logarithm problem is hard in both $A(\mathbb{F})[r]$ and $\mathbb{F}(\zeta_r)^*$, then these pairings can be used for pairing-based cryptography.

The embedding degree

The **embedding degree** of A with respect to $r \mid \#A(\mathbb{F})$ is the degree of $\mathbb{F}(\zeta_r)/\mathbb{F}$.

Lemma

*The **embedding degree** of A with respect to r is equal to the order of $(q \bmod r)$ in \mathbb{F}_r^* .*

Proof: The embedding degree is the smallest number k such that $r \mid \#\mathbb{F}_{q^k}^* = q^k - 1$. □

So the embedding degree is k if and only if $(q \bmod r)$ is some primitive k -th root of unity in \mathbb{F}_r .

Weil numbers

- ▶ Let q be a prime power.

A *Weil q -number* is an algebraic integer π such that $\pi\bar{\pi} = q$ for every embedding of π into \mathbb{C} .

- ▶ Honda-Tate theory gives a bijection

$$\frac{\{\text{simple abelian varieties over } \mathbb{F}_q\}}{\text{isogeny}} \leftrightarrow \frac{\{\text{Weil } q\text{-numbers}\}}{\text{conjugation}}$$
$$A \mapsto \text{Frob}_q.$$

If q is prime and $\pi \neq \pm\sqrt{q}$ is a Weil q -number, then

- ▶ $K = \mathbb{Q}(\pi)$ is a *CM field*, i.e. a non-real number field with a unique complex conjugation automorphism,
- ▶ the corresponding abelian variety A has dimension g , where $2g$ is the degree of K and
- ▶ $\#A(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1)$.

The CM method

Given a Weil q -number π , the corresponding abelian variety can be constructed using the *complex multiplication* method:

- ▶ List the isogeny classes of abelian varieties over $\overline{\mathbb{Q}}$ with CM by the ring of integers of $\mathbb{Q}(\pi)$.
- ▶ Reduce them modulo a prime dividing q .
- ▶ Some twist of one of the reduced varieties will have Frobenius π . Select the one of the correct order.

This method is only well-developed for dimensions 1 and 2 and some special cases of higher dimension and takes time exponential in the bit size of the discriminant of $\mathbb{Q}(\pi)$.

About our algorithm

We give an algorithm with

input:

- ▶ a positive integer k ,
- ▶ a CM field K of degree $2g$ with a ‘primitive CM type’ and
- ▶ a prime $r \equiv 1 \pmod{k}$ that splits completely in K .

output:

a prime number q and a Weil q -number $\pi \in K$ corresponding to an abelian variety of dimension g with embedding degree k with respect to r .

Heuristic expected run time polynomial in $\log r$ (for fixed K).

For $g = 1$, we recover the Cocks-Pinch algorithm, so we assume $g \geq 2$ for simplicity.

Special case: K cyclic

- ▶ Suppose ϕ generates $\text{Gal}(K/\mathbb{Q})$ and τ is a prime of K dividing r . Let $\tau_i = \phi^{-i}(\tau)$, so $r\mathcal{O}_K = \prod_{i=1}^g \tau_i \bar{\tau}_i$.
- ▶ We want $\pi \in \mathcal{O}_K$ with $q = \pi\bar{\pi} \in \mathbb{Z}$ prime such that
 1. $r \mid N_{K/\mathbb{Q}}(\pi - 1)$, e.g. $(\pi \bmod \tau) = 1 \in \mathbb{F}_r$ and
 2. $(q \bmod r) = \zeta_k$ in \mathbb{F}_r .
- ▶ Idea: take $\pi = \prod_{i=1}^g \phi^i(\xi)$ with $\xi \in \mathcal{O}_K$, so $q = \pi\bar{\pi} = N_{K/\mathbb{Q}}(\xi) \in \mathbb{Z}$. Then

$$(\pi \bmod \tau) = \prod_{i=1}^g (\phi^i(\xi) \bmod \tau) = \prod_{i=1}^g (\xi \bmod \tau_i) \quad \text{in } \mathbb{F}_r$$

and similarly $(q \bmod \tau) = \prod_{i=1}^g (\xi \bmod \tau_i)(\xi \bmod \bar{\tau}_i)$ in \mathbb{F}_r .

- ▶ So all we need to do is find $\xi \in \mathcal{O}_K$ with prime norm and
 1. $\prod_{i=1}^g (\xi \bmod \tau_i) = 1$ and
 2. $\prod_{i=1}^g (\xi \bmod \bar{\tau}_i) = \zeta_k$ in \mathbb{F}_r .

Special case: K cyclic

Algorithm

1. Let $\langle \phi \rangle = \text{Gal}(K/\mathbb{Q})$, $\mathfrak{r} \mid r$ a prime of K and $\tau_i = \phi^{-i}(\mathfrak{r})$.
2. Choose α_i and β_i randomly in \mathbb{F}_r^* such that $\prod \alpha_i = 1$ and $\prod \beta_i = \zeta_k$.
3. Compute $\xi \in \mathcal{O}_K$ with $(\xi \bmod \tau_i) = \alpha_i$ and $(\xi \bmod \bar{\tau}_i) = \beta_i$.
4. If $q = N_{K/\mathbb{Q}}(\xi)$ is prime and $\pi = \prod_{i=1}^g \phi^i(\xi)$ generates K , return π and q . Otherwise, go to step (2).

The heuristic expected run time is polynomial in $\log r$ (fixed K).

Proof: As ξ is a lift of a random element modulo $r\mathcal{O}_K$, we expect its norm q to behave like r^{2g} . By the prime number theorem, we thus expect to need $\log(r^{2g})$ iterations before we find a prime q . Moreover, π generates K with probability tending to 1. \square

The type norm

- ▶ The analogue of the map $\xi \mapsto \prod_{i=1}^g \phi^i(\xi)$ for general CM fields is the *type norm*.
- ▶ A *CM type* of a CM field K of degree $2g$ is a set $\Phi = \{\phi_1, \dots, \phi_g\}$ of embeddings of K into a normal closure L such that $\Phi \cup \overline{\Phi}$ is the complete set of embeddings.
 - ▶ We call Φ *primitive* if there is no proper CM subfield K' of K such that $\Phi|_{K'}$ is a CM type of K' .
- ▶ The *type norm* N_Φ with respect to Φ is the map $\xi \mapsto \prod_{i=1}^g \phi_i(\xi)$.
 - ▶ Notice that for $\pi = N_\Phi(\xi)$, we have $\pi\overline{\pi} = N_{K/\mathbb{Q}}(\xi) \in \mathbb{Q}$.
- ▶ The image of N_Φ does not lie in K but in a field called the *reflex field*.

The reflex field

- ▶ Given a pair (K, Φ) of a CM field and a CM type, there is a *reflex* pair (\widehat{K}, Ψ) .
 - ▶ The image of N_Φ lies inside \widehat{K} .
 - ▶ If Φ is primitive, then the reflex of (\widehat{K}, Ψ) is (K, Φ) .
- ▶ We construct π as $N_\Psi(\xi)$ for some $\xi \in \mathcal{O}_{\widehat{K}}$.
- ▶ Remarks about the reflex field: (assume Φ is primitive)
 - ▶ If K is normal, then $\widehat{K} = K$.
 - ▶ In general, K and \widehat{K} don't even have to have the same degree!
 - ▶ Denote the degree of \widehat{K} by $2\widehat{g}$.
 - ▶ If $g = 2$, then $\widehat{g} = 2$. If $g = 3$, then $\widehat{g} \in \{3, 4\}$.

The general case

- ▶ Let $\Psi = \{\psi_1, \dots, \psi_{\hat{g}}\}$ be the reflex type.
- ▶ Let τ be a prime of \mathcal{O}_L dividing r and $\tau_i = \psi_i^{-1}(\tau) \cap \mathcal{O}_{\hat{K}}$.
Then

$$r\mathcal{O}_{\hat{K}} = \prod_{i=1}^{\hat{g}} \tau_i \bar{\tau}_i.$$

Algorithm

1. Choose α_i and β_i randomly in \mathbb{F}_r^* such that $\prod_{i=1}^{\hat{g}} \alpha_i = 1$ and $\prod_{i=1}^{\hat{g}} \beta_i = \zeta_k$ in \mathbb{F}_r .
2. Compute $\xi \in \mathcal{O}_{\hat{K}}$ with $(\xi \bmod \tau_i) = \alpha_i$ and $(\xi \bmod \bar{\tau}_i) = \beta_i$.
3. If $q = N_{\hat{K}/\mathbb{Q}}(\xi)$ is prime and $\pi = N_{\Psi}(\xi)$ generates K , return π and q . Otherwise, go to step (1).

Heuristics

- ▶ Consider the value

$$\rho = \frac{\log q^g}{\log r} \sim \frac{\log \#A(\mathbb{F}_q)}{\log r} \geq 1,$$

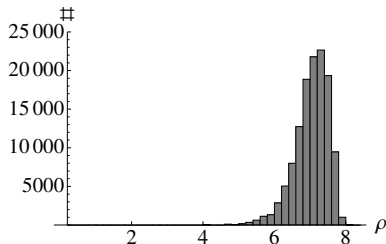
which we want to be small.

- ▶ We expect our output to satisfy $\rho \sim 2g\hat{g}$.
 - ▶ Proof: As ξ is a lift of a random element modulo $r\mathcal{O}_{\hat{K}}$, we expect its norm q to behave like $r^{2\hat{g}}$, so $\log q \sim 2\hat{g} \log r$.
- ▶ For fixed K , k and r , the optimal ξ gives $\rho \sim 2g$.
 - ▶ Proof: We have $(r-1)^{2\hat{g}-2}$ choices for α_i and β_i , so we expect the minimal norm for a ξ to be approximately r^2 .
 - ▶ Open question: can we find it efficiently?
- ▶ A method by Freeman based on our algorithm, in which r is not prescribed, achieves $\rho < 2g\hat{g}$ for some K and k .

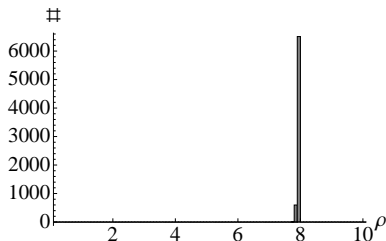
Experimental results

$$K = \mathbb{Q}(\zeta_5)$$

Histograms of ρ -values produced by our algorithm:



$k = 2, r = 1021$
all possible α_1, β_1
minimal ρ : 4.19



$k = 10, r = 2^{160} + 685$
 2^{20} random α_1 and β_1

Notice that $g = \hat{g} = 2$.

Example

$$K = \mathbb{Q}(\zeta_7), k = 17, r = 2^{180} - 7427$$

- ▶ Absolutely simple abelian varieties with CM by K are Jacobians of curves of the form $y^2 = x^7 + a$.
- ▶ Our algorithm found a suitable Weil q -number for

```
q = 1575584138119771535917878020143687930577769468671374639550678761402500812 \  
1759749726349377162542168169176007186988081292604570406371468028127020440 \  
6861277269259077188966205156107806823000096120874915612017184924206843204 \  
6217592329462633576371925169798774026389116897144108553148110927632874029 \  
911153126048408269857121431033499 (1077 bits)
```

in 51 seconds.

- ▶ It has $\rho = 17.95$ and $g = \hat{g} = 3$.
- ▶ The corresponding curve is given by $y^2 = x^7 + 10$.

Summary

- ▶ Our algorithm constructs Weil numbers corresponding to abelian varieties over finite fields with prescribed embedding degree with respect to a subgroup of prescribed order r .
- ▶ We fix our CM field K in advance.
- ▶ The algorithm is polynomial in $\log r$.
- ▶ We get

$$\frac{\log \#A(\mathbb{F})}{\log r} \sim 2g\hat{g}.$$