Constructing pairing-friendly hyperelliptic curves using Weil restriction

David Mandell Freeman (Stanford University, USA) and **Takakazu Satoh** (Tokyo Institute of Technology, Japan)

dfreeman@cs.stanford.edu, tkkzsath@math.titech.ac.jp

The problem

A *pairing-friendly curve* is a curve C over a finite field $\mathbb{F}_q$ whose Jacobian $\mathrm{Jac}(C)$ has

- a subgroup of large prime order r
- small *embedding degree* $k := [\mathbb{F}_q(\zeta_r) : \mathbb{F}_q]$ with respect to r.

These curves have numerous applications in cryptography. For these applications to be efficient, we wish to minimize the parameter

$$\rho := \dim(\mathrm{Jac}(C)) \cdot \log q / \log r.$$

Constructing pairing-friendly genus 2 curves C with small ρ-values is a difficult task.
If $\mathrm{Jac}(C)$ is ordinary and absolutely simple, the best known constructions achieve $\rho \approx 8$ generically and $\rho \approx 4$ for some k. If $\mathrm{Jac}(C)$ is supersingular, then we can achieve $\rho \approx 1$, but only for $k \le 12$.
What if we require $\mathrm{Jac}(C)$ to be ordinary and simple, but not absolutely simple?

Weil restriction

Given a field extension L/K, *Weil restriction* interprets a variety over L as a higher-dimensional variety over K. On affine varieties X, we do the following: (For projective varieties we glue affine subsets.)

1. Choose a K-basis $\{\alpha_i\}$ of L.
2. Write the equations for X in terms of the $\{\alpha_i\}$.
3. Collect terms with matching basis elements. These equations define $X' = \mathrm{Res}_{L/K}(X)$.

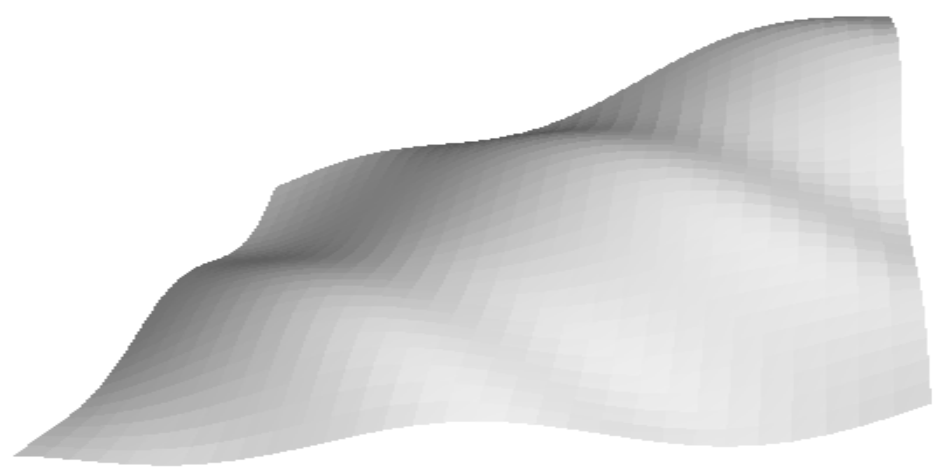
Proposition 1 *Let A/K be a g-dimensional simple abelian variety. Let L/K be a finite, separable extension. Suppose A is isogenous over L to a product of g isomorphic elliptic curves E defined over K. Then A is isogenous over K to a subvariety of the Weil restriction $\mathrm{Res}_{L/K}(E)$.*

For $K = \mathbb{F}_q$, let $f_{X,q}$ be the characteristic polynomial of the q-power Frobenius endomorphism of X.

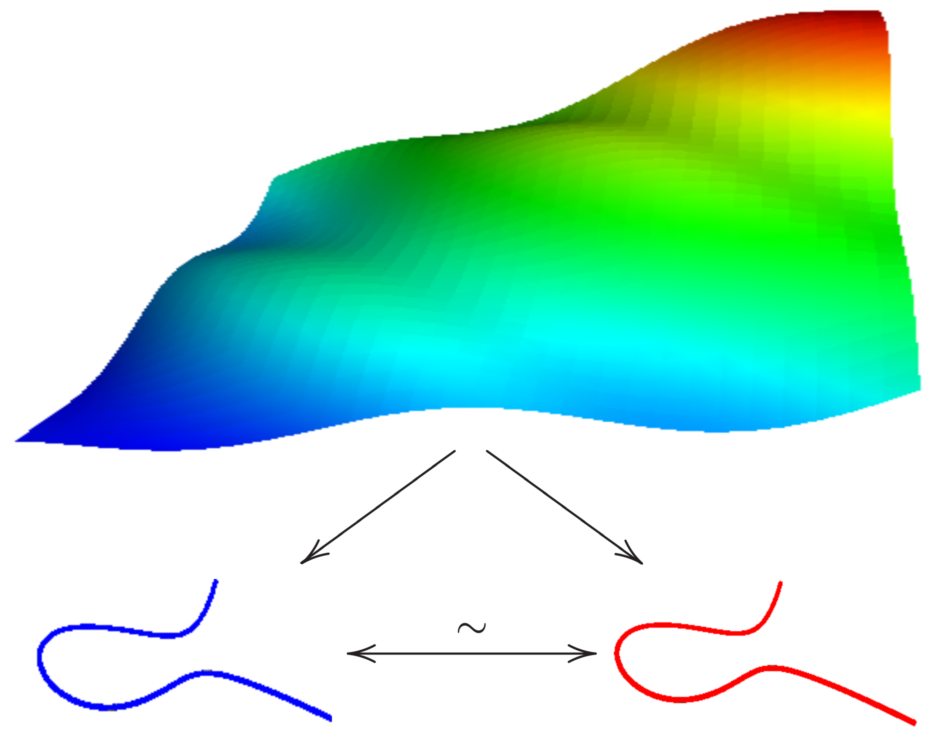
Proposition 2 *Let $A/\mathbb{F}_{q^d}$ be an abelian variety. Let $A' = \mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(A)$. Then $f_{A',q}(x) = f_{A,q^d}(x^d)$.*

Overview of our technique

$A = \mathrm{Jac}(C)$ is a simple abelian surface over $\mathbb{F}_q$.



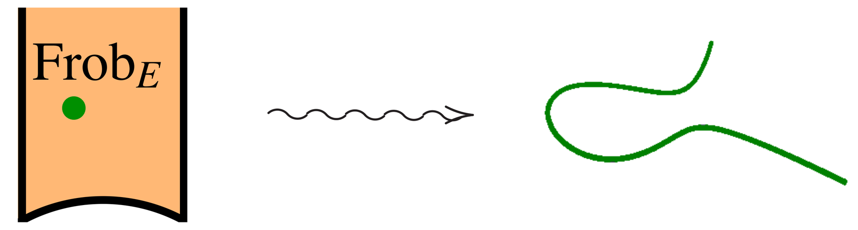
Over the extension field $\mathbb{F}_{q^d}$, A maps to a product of isomorphic elliptic curves E defined over $\mathbb{F}_q$.



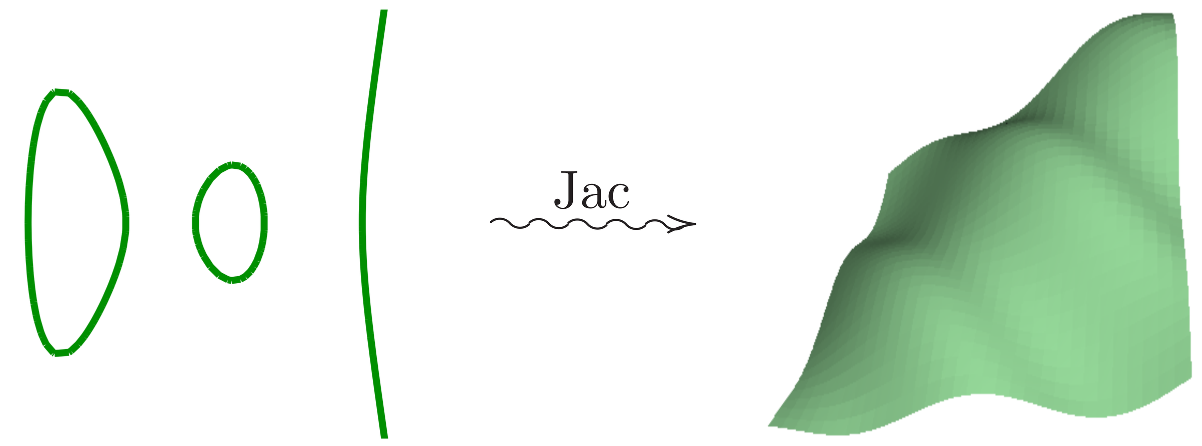
This means that A is isogenous to a ***primitive subgroup*** of the ***Weil restriction*** of E from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$, and thus there is a dth root of unity ζ_d such that

$$\mathrm{Frob}_A = \zeta_d \cdot \mathrm{Frob}_E\,.$$

Using this relationship, we construct a Frob_E so that $\zeta_d \cdot \mathrm{Frob}_E$ has the desired pairing-friendly properties. We use the ***CM method*** to construct E from Frob_E.



From $j(E)$ we can compute a genus 2 curve C such that $A = \mathrm{Jac}(C)$ is pairing-friendly over $\mathbb{F}_q$.



Primitive subgroups

When A is an abelian variety over $\mathbb{F}_q$, the Weil restriction of A from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$ is isogenous over $\mathbb{F}_q$ to a product of *primitive subgroups*:

$$\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(A) \sim \bigoplus_{e \mid d} V_e(A).$$

$V_e(A)$ is defined to be the intersection of the kernels of the maps on $\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(A)$ induced by $\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_{q^e}}$.
If $A = E$ is an ordinary elliptic curve over $\mathbb{F}_q$, then:

- $\dim V_d(E) = \varphi(d)$.
- $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quadratic imaginary field K.
- For some primitive $\zeta_d \in \overline{\mathbb{Q}}$, $(\zeta_d)^d = 1$, the q-power Frobenius endomorphisms of $V_d(E)$ and E are related by

$$\mathrm{Frob}_{V_d(E)} = \zeta_d \cdot \mathrm{Frob}_E \in K(\zeta_d).$$

- $V_d(E)$ is simple if and only if $K \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

Non-simple abelian surfaces

Let C, C' be genus 2 curves over $\mathbb{F}_q$ given by

$$C\colon y^2 = x^5 + ax^3 + bx \qquad (1)$$
$$C'\colon y^2 = x^6 + ax^3 + b. \qquad (2)$$

Suppose $b \in (\mathbb{F}_q^*)^2$. Let $c = \frac{a}{\sqrt{b}}$. Define E, E' by $(*)$

$$E\colon Y^2 = (c+2)X^3 - (3c-10)X^2 + (3c-10)X - (c+2)$$
$$E'\colon Y^2 = (c+2)X^3 - (3c-30)X^2 + (3c+30)X - (c-2)$$

Theorem 3 $\mathrm{Jac}(C)$ *is isogenous over* $\mathbb{F}_q(b^{1/8}, i)$ *to* $E \times E$. *If* $\mathrm{Jac}(C)$ *is ordinary,* $b \notin (\mathbb{F}_q^*)^4$, *and* $\mathrm{End}(E) \otimes \mathbb{Q} \ncong \mathbb{Q}(i)$, *then* $\mathrm{Jac}(C)$ *is simple and isogenous over* $\mathbb{F}_q$ *to* $V_4(E)$.

Theorem 4 $\mathrm{Jac}(C')$ *is isogenous over* $\mathbb{F}_q(b^{1/6}, \zeta_3)$ *to* $E' \times E'$. *If* $\mathrm{Jac}(C')$ *is ordinary,* $b \notin (\mathbb{F}_q^*)^6$, *and* $\mathrm{End}(E') \otimes \mathbb{Q} \ncong \mathbb{Q}(\zeta_3)$, *then* $\mathrm{Jac}(C')$ *is simple and isogenous over* $\mathbb{F}_q$ *to* $V_3(E')$.

The algorithm

Data: integers k, d with $d \in \{3, 4\}$ and $d \mid k$;
a quadratic imaginary field $K \not\ni \zeta_d$.
Result: Primes q, r; a genus 2 curve $C/\mathbb{F}_q$.
Thm: $\mathrm{Jac}(C)$ has embedding degree k w.r.t r.

1 Choose a prime $r \equiv 1 \bmod k$ with $r\mathcal{O}_K = \mathfrak{r}\bar{\mathfrak{r}}$.
2 Choose primitive roots of unity $\zeta_k, \zeta_d \in \mathbb{F}_r$.
3 Compute a $\pi \in \mathcal{O}_K$ such that
$$\pi \equiv \zeta_d \pmod{\mathfrak{r}}, \quad \pi \equiv \zeta_k/\zeta_d \pmod{\bar{\mathfrak{r}}},$$
and $q = \pi\bar{\pi}$ is prime.
4 Use the CM method to find the j-invariant j_0 of an elliptic curve $E_0/\mathbb{F}_q$ with $\mathrm{End}(E_0) \cong \mathcal{O}_K$
5 **if** $d = 4$ **then**
  Let E be given by $(*)$ below.
  Compute $c \in \mathbb{F}_q$ such that $j(E) = j_0$.
  Choose $a \in \mathbb{F}_q$ s.t. $\frac{a}{c} \notin (\mathbb{F}_q^*)^2$; set $b := (\frac{a}{c})^2$.
  Output the curve C given by (1).
6 **else if** $d = 3$ **then**
  Let E' be given by $(*)$ below.
  Compute $c \in \mathbb{F}_q$ such that $j(E') = j_0$.
  Choose $a \in \mathbb{F}_q$ s.t. $\frac{a}{c} \notin (\mathbb{F}_q^*)^3$; set $b := (\frac{a}{c})^2$.
  Set $n := \Phi_d(\pi)\Phi_d(\bar{\pi})$.
  if $\#\mathrm{Jac}(C') = n$ **then**
    Output the curve C' given by (2).
  else Output the quadratic twist of C'.

Our results

We ran a Brezing-Weng variant of our algorithm:

- Choose r and π to be *polynomials* in $K[x]$.
- Find x_0 such that $q(x_0)$ and $r(x_0)$ are prime.

We found pairing-friendly genus 2 curves with record ρ-values:

k	d	K	ρ-value
9	3	$\mathbb{Q}(i)$	2.67
12	4	$\mathbb{Q}(\zeta_3)$	3.00
21	3	$\mathbb{Q}(i)$	2.67
24[a]	4	$\mathbb{Q}(\sqrt{-2})$	3.00
27	3	$\mathbb{Q}(i)$	2.22
39	3	$\mathbb{Q}(i)$	2.33
42	3	$\mathbb{Q}(\sqrt{-7})$	3.00
44	4	$\mathbb{Q}(\sqrt{-11})$	3.00
54	3	$\mathbb{Q}(i)$	2.44

[a] The result for $k = 24$ was previously found by Kawazoe and Takahashi; our method properly includes theirs.