Computing endomorphism rings of supersingular elliptic curves

Travis Morrison

Virginia Tech

AGCCT 2023

joint work with Fuselier, Iezzi, Kozek, Namoijam

Computing supersingular endomorphism rings

Problem

Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute $\mathrm{End}(E)$, i.e. give a basis and multiplication table for $\mathrm{End}(E) \otimes \mathbb{Q}$, along with four elements of $\mathrm{End}(E) \otimes \mathbb{Q}$ generating $\mathrm{End}(E)$ as a $\mathbb{Z}$-module.

Computing End(E): ordinary vs supersingular

Let $E/\mathbb{F}_q$ be an elliptic curve. Let $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$.

- If E is ordinary:

Computing End(E): ordinary vs supersingular

Let $E/\mathbb{F}_q$ be an elliptic curve. Let $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$.

- If E is ordinary:
  - $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$ has finite index
  - $\mathrm{End}(E)$ is contained in the unique maximal order in the imaginary quadratic field $\mathrm{End}^0(E) \otimes \mathbb{Q}$, so computing $[\mathrm{End}(E) : \mathbb{Z}[\pi_E]]$ determines $\mathrm{End}(E)$.

Computing End(E): ordinary vs supersingular

Let $E/\mathbb{F}_q$ be an elliptic curve. Let $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$.

- If E is ordinary:
  - $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$ has finite index
  - $\mathrm{End}(E)$ is contained in the unique maximal order in the imaginary quadratic field $\mathrm{End}^0(E) \otimes \mathbb{Q}$, so computing $[\mathrm{End}(E) : \mathbb{Z}[\pi_E]]$ determines $\mathrm{End}(E)$.
- If E is supersingular:
  - Computing one endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ is hard...

Computing End(E): ordinary vs supersingular

Let $E/\mathbb{F}_q$ be an elliptic curve. Let $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$.

- If E is ordinary:
  - $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$ has finite index
  - $\mathrm{End}(E)$ is contained in the unique maximal order in the imaginary quadratic field $\mathrm{End}^0(E) \otimes \mathbb{Q}$, so computing $[\mathrm{End}(E) : \mathbb{Z}[\pi_E]]$ determines $\mathrm{End}(E)$.
- If E is supersingular:
  - Computing one endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ is hard...
  - ... and given an order $\mathcal{O} \subseteq \mathrm{End}(E)$ of finite index, there can be exponentially many (in the size of $\mathcal{O}$!) pairwise nonisomorphic maximal orders containing $\mathcal{O}$, any one of which could be $\mathrm{End}(E)$.

Prior algorithms for computing the endomorphism ring

- If $E/\mathbb{F}_q$ is ordinary: Bisson-Sutherland (2011), Robert (2022) give a subexponential, in $\log q$, algorithm for computing $\mathrm{End}(E)$.
- If E is supersingular: Kohel gives a $O(p^{1+\epsilon})$ algorithm to compute a suborder of $\mathrm{End}(E)$.
- Eisenträger-Hallgren-Leonardi-M.-Park: $\tilde{O}(p^{1/2})$ algorithm, assuming GRH and heuristics, which computes a Bass suborder of $\mathrm{End}(E)$.
- Today: (joint with Fuselier-Iezzi-Kozek-Namoijam): compute $\mathrm{End}(E)$ using *inseparable endomorphisms* in time $\tilde{O}(p^{1/2})$ assuming only GRH.

Computing End(E) with inseparable endomorphisms

- Every inseparable endomorphism $\alpha \in \mathrm{End}(E)$ factors as

$$\alpha = \pi \circ \phi,$$

where $\phi\colon E \to E^{(p)}$ is an isogeny and $\pi\colon E \to E^{(p)}$ is the p-power Frobenius isogeny.

Computing End(E) with inseparable endomorphisms

- Every inseparable endomorphism $\alpha \in \mathrm{End}(E)$ factors as

$$\alpha = \pi \circ \phi,$$

where $\phi\colon E \to E^{(p)}$ is an isogeny and $\pi\colon E \to E^{(p)}$ is the p-power Frobenius isogeny.

- The set

$$P := \pi \,\mathrm{Hom}(E, E^{(p)}) \subseteq \mathrm{End}(E)$$

is the unique 2-sided ideal of reduced norm p in End(E)

Computing End(E) with inseparable endomorphisms

- Every inseparable endomorphism $\alpha \in \mathrm{End}(E)$ factors as

$$\alpha = \pi \circ \phi,$$

where $\phi\colon E \to E^{(p)}$ is an isogeny and $\pi\colon E \to E^{(p)}$ is the p-power Frobenius isogeny.

- The set

$$P := \pi \,\mathrm{Hom}(E, E^{(p)}) \subseteq \mathrm{End}(E)$$

is the unique 2-sided ideal of reduced norm p in $\mathrm{End}(E)$

- The order

$$\mathbb{Z} + P \subseteq \mathrm{End}(E)$$

has index p in $\mathrm{End}(E)$, and $\mathrm{End}(E)$ is the unique maximal order containing $\mathbb{Z} + P$.

Supersingular isogeny graphs

Let $p \neq \ell$ be primes. Let $G(p, \ell)$ be the directed graph whose

- vertices are a complete set of representatives of the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$
- (directed) edges are ℓ-isogenies $E_i \to E_j$

$\sigma_p = (x \mapsto x^p) \in Gal(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acts on $G(p, \ell)$ as an automorphism:

- map E_i to $E_i^{(p)}$,
- and map $\phi\colon E_i \to E_j$ to $\phi^{(p)}\colon E_i^{(p)} \to E_j^{(p)}$

Curves close to their Galois conjugate

Cyclic, inseparable endomorphisms with trace zero, i.e. embeddings

$$\mathbb{Z}\left[\sqrt{-dp}\right] \hookrightarrow \mathrm{End}(E).$$

are used in Charles-Goren-Lauter (2011), EHLMP (2020), Chenu-Smith 2022.

Definition (Chenu-Smith)

Let $\epsilon = \pm 1$ and let d be a squarefree positive integer. A *supersingular* (d, ϵ)*-structure* is a pair (E, ψ) where $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve and $\psi\colon E \to E^{(p)}$ satisfies $\psi^{(p)} = \epsilon\widehat{\psi}$.

Chenu and Smith show $\mathbb{Z}[\pi\psi] \simeq \mathbb{Z}[\sqrt{-dp}]$ if d is squarefree and (E, ψ) is a (d, ϵ)-structure.

Inseparable reflections

Definition

Let p be a prime, and let d_1, d be integers with d square-free and with d_1, d, p all pairwise coprime. An **inseparable reflection of degree** dpd_1^2 of a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ is an endomorphism

$$\alpha := \pi \circ \widehat{\phi^{(p)}} \circ \psi \circ \phi$$

such that

1. $\phi\colon E \to E'$ is a cyclic d_1-isogeny,
2. (E', ψ) is a (d, ϵ)-structure,
3. and ϕ does not factor nontrivially through an isogeny $\phi'\colon E \to E''$ such that E'' has a (d, ϵ)-structure.

In our algorithms, we use $d = 1$ or 2 and $d_1 = \ell^t$ for small prime ℓ.

Orders generated by inseparable reflections

Theorem (Fuselier-Iezzi-Kozek-M.-Namoijam)

Let $E/\mathbb{F}_{p^2}$ be supersingular, $p > 3$. For $i = 1, 2$ let d, p, d_i be pairwise coprime, and let

$$\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi\phi_i$$

be inseparable reflections of degree dpd_i^2. Then:

1. $$\mathbb{Z}[\alpha_i] \simeq \mathbb{Z}[\deg(\phi_i)\sqrt{-p}];$$
2. *If $-dp \not\equiv 1 \pmod 4$, then*

$$\Lambda := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2$$

is a Bass suborder of $\mathrm{End}(E)$ with index $\mathrm{disc}(\frac{\alpha_1\alpha_2}{p})$ in $\mathbb{Z} + P$.

Computing End(E) from a Bass suborder

Given $E/\mathbb{F}_{p^2}$ supersingular:

1. Take random walks of length $O(\log p)$ beginning at E in the 3-isogeny graph until finding a curve E_1 with a $(2, \epsilon)$-structure (E_1, ψ) yielding one inseparable reflection

$$\alpha_1 = \pi \widehat{\phi_1^{(p)}} \psi_1 \phi_1$$

   of degree $2p3^{2e_3}$
2. Repeat the above in the 5-isogeny graph to obtain inseparable reflection α_2 of degree $2p5^{2e_5}$
3. Let $\Lambda = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$.
4. Enumerate maximal orders $\mathcal{O} \subseteq \Lambda$ until $\mathcal{O} = \mathrm{End}(E)$

First two steps take expected $\tilde{O}(\sqrt{p})$ time, assuming GRH. We prove that the final step takes $O(p^\epsilon)$ time for every $\epsilon > 0$, using that Λ is Bass.

Heuristics (re)moved

- With two calls to an algorithm for computing an inseparable reflection, we provably compute a generating set for a Bass suborder of $\mathrm{End}(E)$.
- What is the expected number of calls to such an algorithm until finding a generating set of $\mathbb{Z} + P$?

Heuristic algorithm

Suppose α_{ij} are inseparable reflections for $1 \leq i, j \leq 2$

$$\Lambda_1 = \langle \alpha_{11}, \alpha_{12} \rangle, \quad \Lambda_2 = \langle \alpha_{21}, \alpha_{22} \rangle, \quad \Lambda = \langle \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \rangle$$

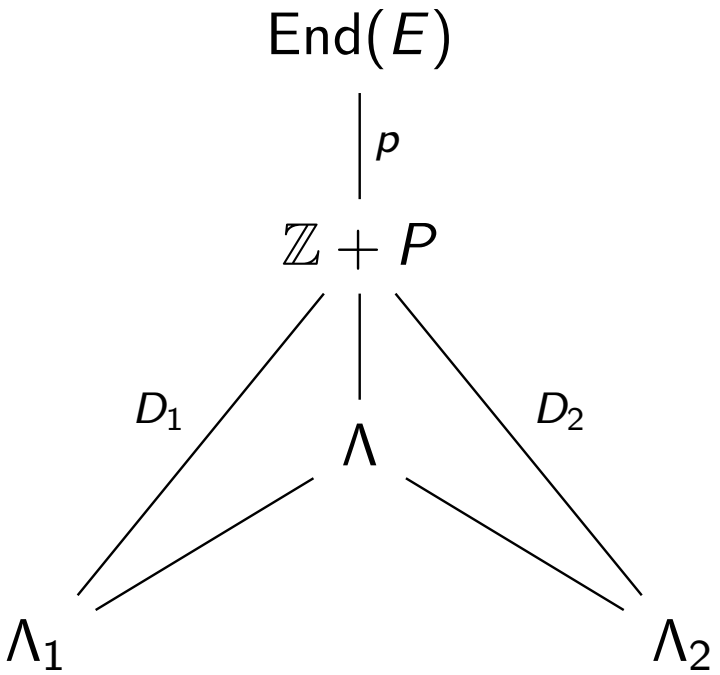
$$\rho_i = \frac{1}{p} \alpha_{i1} \alpha_{i2}, \quad D_i = -\operatorname{disc}(\rho_i)$$

Heuristic algorithm

Suppose α_{ij} are inseparable reflections for $1 \leq i, j \leq 2$

$$\Lambda_1 = \langle \alpha_{11}, \alpha_{12} \rangle, \quad \Lambda_2 = \langle \alpha_{21}, \alpha_{22} \rangle, \quad \Lambda = \langle \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \rangle$$

$$\rho_i = \frac{1}{p} \alpha_{i1} \alpha_{i2}, \quad D_i = -\operatorname{disc}(\rho_i)$$



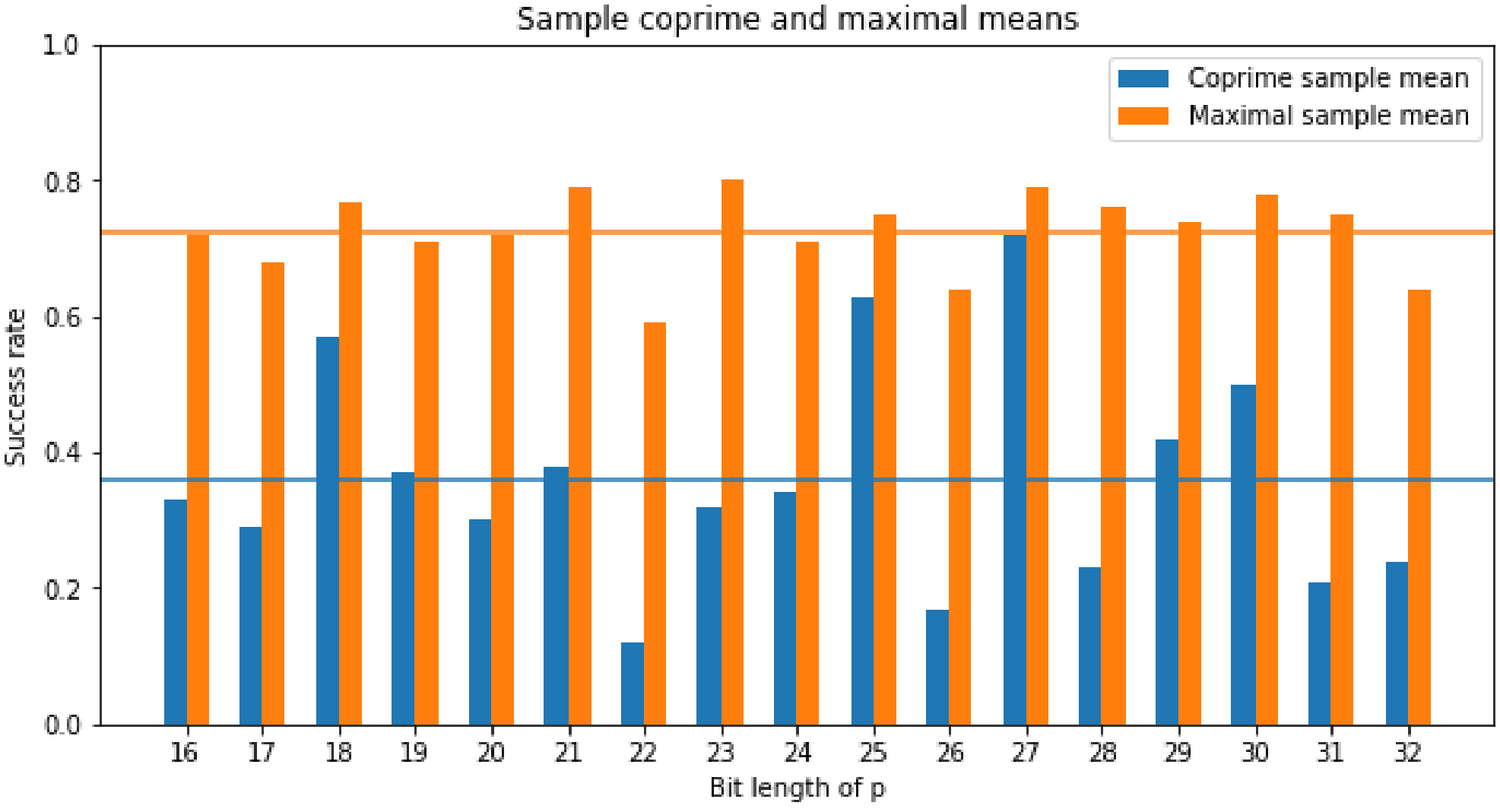
- $[\mathbb{Z} + P : \Lambda]$ divides $[\mathbb{Z} + P : \Lambda_i] = D_i$.
- If $\gcd(D_1, D_2) = 1$, then $\Lambda = \mathbb{Z} + P$.
- Heuristic: for some constant $c > 0$,

$$\Pr[\gcd(\operatorname{disc} \rho_1, \operatorname{disc} \rho_2) = 1] > c$$

Experiment 1

For $b \in [16, 32]$:

- Pick a prime of bit length b. Pick 100 pseudorandom supersingular $E/\mathbb{F}_{p^2}$.
- For each E: compute four inseparable reflections α_{i1}, α_{i2} and let $\rho_i = \alpha_{i1}\alpha_{i2}/p$ for $i = 1, 2$.
- Test if:
  1. $\gcd(\operatorname{disc} \rho_1, \operatorname{disc} \rho_2) = 1$, and
  2. $\langle \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \rangle = \mathbb{Z} + P$

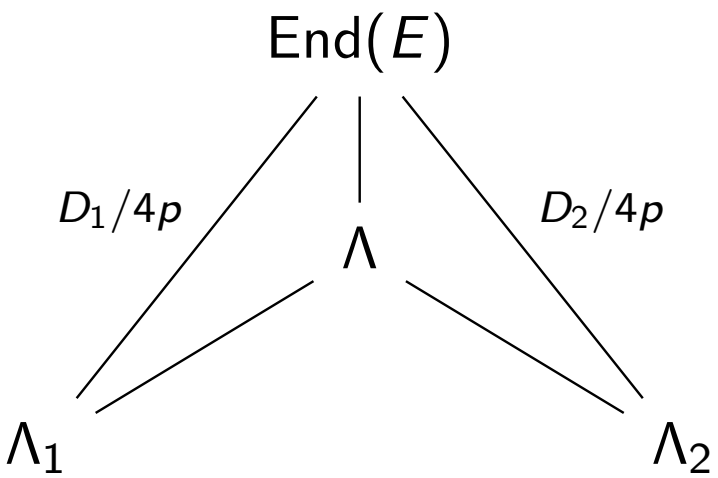

Sample coprime and maximal means
Coprime sample mean
Maximal sample mean
Success rate
1.0
0.8
0.6
0.4
0.2
0.0
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
Bit length of p

What is the truth?

Suppose α_{ij} are arbitrary in $\mathrm{End}(E)$ (of degree up to some bound X) for $1 \le i, j \le 2$

$$\Lambda_1 = \langle \alpha_{11}, \alpha_{12} \rangle, \quad \Lambda_2 = \langle \alpha_{21}, \alpha_{22} \rangle, \quad \Lambda = \langle \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \rangle$$

$$\rho_i = (\mathrm{Trd}\,\alpha_1)\alpha_2 + (\mathrm{Trd}\,\alpha_2)\alpha_1 - 2\alpha_1\alpha_2, \quad \mathrm{disc}(\Lambda_i) = \left(\frac{1}{4}\,\mathrm{disc}\,\rho_i\right)^2.$$



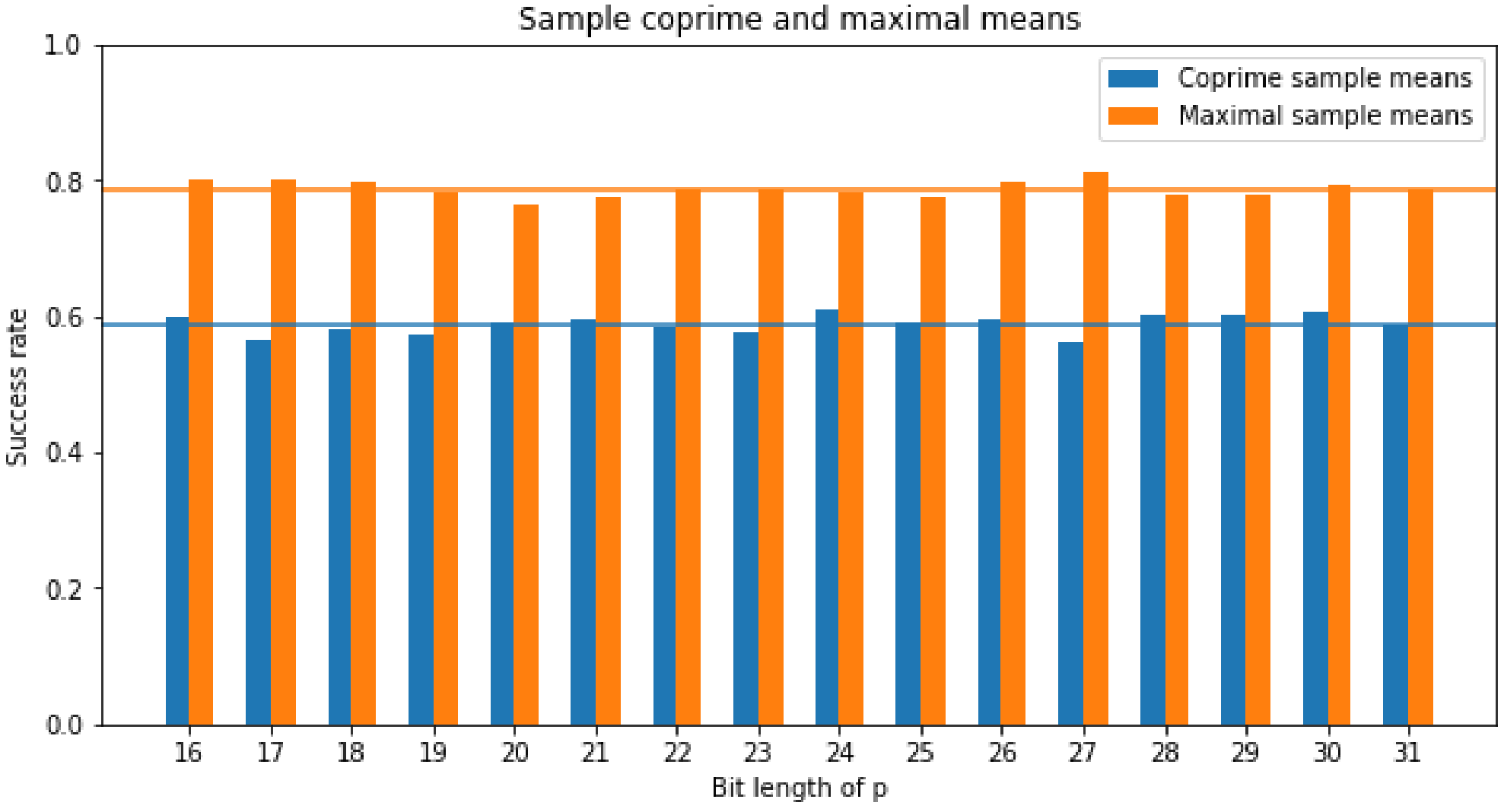
- $[\mathrm{End}(E) : \Lambda]$ divides $[\mathrm{End}(E) : \Lambda_i] = \frac{1}{4p} D_i$.
- If $\gcd(D_1, D_2) = 4p$, then $\Lambda = \mathrm{End}(E)$.
- Heuristic: for some constant $c > 0$,

$$\Pr[\gcd(\mathrm{disc}\,\rho_1, \mathrm{disc}\,\rho_2) = 4p] > c$$

Experiment 2

For $b \in [16, 32]$:

- Pick a prime of bit length b. Pick 100 pseudorandom maximal orders $\mathcal{O}$ in the quaternion algebra ramified at p, ∞.
- For each $\mathcal{O}$: compute four random elements $\alpha_{i1}, \alpha_{i2} \in \mathcal{O}$ and $\rho_i = (\mathrm{Trd}\,\alpha_1)\alpha_2 + (\mathrm{Trd}\,\alpha_2)\alpha_1 - 2\alpha_1\alpha_2$ for $i = 1, 2$.
- Test if:
  1. $\gcd(\mathrm{disc}\,\rho_1, \mathrm{disc}\,\rho_2) = 4p$, and
  2. $\langle \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \rangle = \mathcal{O}$


Sample coprime and maximal means
Coprime sample means
Maximal sample means
Success rate
1.0
0.8
0.6
0.4
0.2
0.0
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
Bit length of p

Thank you!

From a lattice to a quaternion algebra: Schoof's algorithm

- Suppose we have a finitely generated subgroup

$$\Lambda := \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3 + \mathbb{Z}\alpha_4 \subseteq \mathbb{Z} + P.$$

  How can we tell if $\Lambda = \mathbb{Z} + P$?

- Compute $G = (\mathit{trace}(\alpha_i\alpha_j))_{1\leq i,j\leq 4}$.

$$\det(G) = p^4 \iff \Lambda = \mathbb{Z} + P.$$

  Here, $\mathit{trace}(\alpha)$ is the integer t such that $[t] = \alpha + \widehat{\alpha}$.

- We can compute $\mathit{trace}(\alpha)$ efficiently with Schoof's algorithm (efficiently: polynomial in the length of a compact representation of the endomorphism α).

Computing $\mathrm{End}(E) \otimes \mathbb{Q}$ with inseparable endomorphisms

Compute $\mathrm{End}(E) \otimes \mathbb{Q}$...

1. ...as a **vector space**: compute three isogenies $\phi_i \colon E \to E^{(p)}$ to get three (linearly independent, over $\mathbb{Q}$) endomorphisms $\gamma_i := \pi \circ \phi_i$ generating a lattice Λ. Then $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ span $\mathrm{End}(E) \otimes \mathbb{Q}$

Computing $\mathrm{End}(E) \otimes \mathbb{Q}$ with inseparable endomorphisms

Compute $\mathrm{End}(E) \otimes \mathbb{Q}$...

1. ...as a **vector space**: compute three isogenies $\phi_i \colon E \to E^{(p)}$ to get three (linearly independent, over $\mathbb{Q}$) endomorphisms $\gamma_i := \pi \circ \phi_i$ generating a lattice Λ. Then $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ span $\mathrm{End}(E) \otimes \mathbb{Q}$
2. ...as a **quadratic space**: use a generalization of Schoof's algorithm to compute the Gram matrix $(\mathit{trace}(\gamma_i \gamma_j))$ of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$

Computing $\mathrm{End}(E) \otimes \mathbb{Q}$ with inseparable endomorphisms

Compute $\mathrm{End}(E) \otimes \mathbb{Q}$...

1. ...as a **vector space**: compute three isogenies $\phi_i \colon E \to E^{(p)}$ to get three (linearly independent, over $\mathbb{Q}$) endomorphisms $\gamma_i := \pi \circ \phi_i$ generating a lattice Λ. Then $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ span $\mathrm{End}(E) \otimes \mathbb{Q}$
2. ...as a **quadratic space**: use a generalization of Schoof's algorithm to compute the Gram matrix $(\mathit{trace}(\gamma_i \gamma_j))$ of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$
3. ...as a **quaternion algebra**: recover a multiplication table for $\mathrm{End}(E) \otimes \mathbb{Q}$ from the Gram matrix using the Gram-Schmidt process, yielding $a, b \in \mathbb{Q}^*$ and $f \colon \Lambda \hookrightarrow \left(\frac{a,b}{\mathbb{Q}}\right)$

Computing $\mathrm{End}(E) \otimes \mathbb{Q}$ with inseparable endomorphisms

Compute $\mathrm{End}(E) \otimes \mathbb{Q}$...

1. ...as a **vector space**: compute three isogenies $\phi_i \colon E \to E^{(p)}$ to get three (linearly independent, over $\mathbb{Q}$) endomorphisms $\gamma_i := \pi \circ \phi_i$ generating a lattice Λ. Then $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ span $\mathrm{End}(E) \otimes \mathbb{Q}$
2. ...as a **quadratic space**: use a generalization of Schoof's algorithm to compute the Gram matrix $(\mathit{trace}(\gamma_i \gamma_j))$ of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$
3. ...as a **quaternion algebra**: recover a multiplication table for $\mathrm{End}(E) \otimes \mathbb{Q}$ from the Gram matrix using the Gram-Schmidt process, yielding $a, b \in \mathbb{Q}^*$ and $f \colon \Lambda \hookrightarrow \left(\frac{a,b}{\mathbb{Q}}\right)$

Computing $\mathrm{End}(E) \otimes \mathbb{Q}$ with inseparable endomorphisms

Compute $\mathrm{End}(E) \otimes \mathbb{Q}$...

1. ...as a **vector space**: compute three isogenies $\phi_i \colon E \to E^{(p)}$ to get three (linearly independent, over $\mathbb{Q}$) endomorphisms $\gamma_i := \pi \circ \phi_i$ generating a lattice Λ. Then $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ span $\mathrm{End}(E) \otimes \mathbb{Q}$
2. ...as a **quadratic space**: use a generalization of Schoof's algorithm to compute the Gram matrix $(\mathit{trace}(\gamma_i \gamma_j))$ of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$
3. ...as a **quaternion algebra**: recover a multiplication table for $\mathrm{End}(E) \otimes \mathbb{Q}$ from the Gram matrix using the Gram-Schmidt process, yielding $a, b \in \mathbb{Q}^*$ and $f \colon \Lambda \hookrightarrow \left(\frac{a,b}{\mathbb{Q}}\right)$

Next, compute more $\pi\gamma$ until we've generated $\mathbb{Z} + P$ and compute $\mathrm{End}(E)$ with Voight's algorithm.