Equidistribution of elliptic curves with extra structure

j/w/ Benjamin Wesolowski

Reminder $\mathbb{F}$ alg. closed field. $E/\mathbb{F}$ elliptic curve $y^2 = x^3+ax+b$, $a,b \in \mathbb{F}$, disc $\neq 0$. $4a^3+27b^2$

$E(\mathbb{F}) = \{\text{solutions}/\mathbb{F}\} \cup \{\infty\}$ algebraic group. $\infty = 0_E$

morphism $\phi : E \longrightarrow E'$ rational fractions s.t. $\infty \longmapsto \infty \Rightarrow$ group morphism.

- constant : $E \longmapsto \infty$ "zero morphism" $\deg(\phi\circ\psi) = \deg\phi \cdot \deg\psi$.
- isogeny : $\ker\phi$ finite, ϕ surjective $\rightsquigarrow \deg\phi = \#\ker\phi$. (with multiplicity)

dual $\hat\phi$ $\hat\phi\phi = [\deg\phi]$ $E' \to E$

$\exists$ finitely many isogenies of given degree from a given E (up to isom. between targets).

example: $[n] : E \longrightarrow E$ $\deg[n] = n^2$.
$n \in \mathbb{Z}$

$\mathbb{F} = \overline{\mathbb{F}_p}$. $E/\mathbb{F}$.

- ordinary : $E[p](\mathbb{F}) \cong \mathbb{Z}/p\mathbb{Z}$ $\mathrm{End}(E) \underset{gp}{\cong} \mathbb{Z}^2$ commutative
- supersingular : $E[p](\mathbb{F}) = 0$ $\mathrm{End}(E) \underset{gp}{\cong} \mathbb{Z}^4$ $Z(\mathrm{End}\,E) = \mathbb{Z}$.

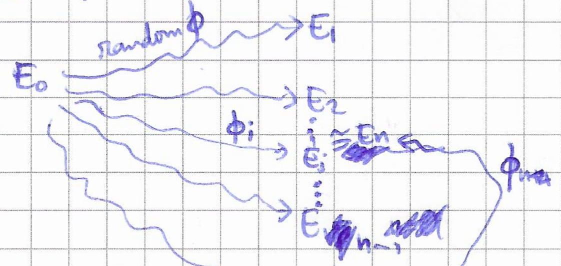
1) Algorithmic problems and random distributions

Problem: Given E, compute $\mathrm{End}(E)$. (End Ring).

When E is supersingular, we don't know any algo faster than exponential.

$\#\{\text{Supersingular } E/\text{isom}\} \approx p$. From now on, all E are supersingular.

Algo: input E_0



$\alpha = \hat\phi_i\,\phi_{n+1} \in \mathrm{End}(E_0)$.

Repeat to get more until generate $\mathrm{End}(E_0)$

Analysis? $n = O(\sqrt{p})$ $E_i \overset{\text{unif.}}{\approx}$ random among all. (birthday paradox)

ex 1: How does ϕ_{n+1} distribute in $\mathrm{Hom}(E_0, E_i)$?

(Easier?) **Problem** Given E, compute some $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$. (OneEnd)

Reduce EndRing to OneEnd: oracle $\mathcal{O}_{\text{oneend}}$ $\rightsquigarrow$ solve EndRing.

(earlier broken heur. red. Eisenträger, Hallgren, Lauter, Morrison, Petit)

Algo: input E_0

$$E_0 \xrightarrow{\text{random } \phi} E \circlearrowleft \alpha := \mathcal{O}_{\text{oneend}}(E) \in \mathrm{End}(E) \setminus \mathbb{Z}$$

get $\beta = \hat{\phi} \alpha \phi \in \mathrm{End}(E_0) \setminus \mathbb{Z}$

repeat to get more until generate $\mathrm{End}(E_0)$.

Analysis? How does β distribute in $\mathrm{End}(E_0)$? ex 2

ex 3: $C \subseteq E$ cyclic group of order N.

$E \xrightarrow{\text{random } \phi} E'$. Distribution of $(E', \phi(C))$?

2) Objects transported by isogenies

To each $E/\mathbb{F}$, attach an object among a set $\mathcal{F}(E)$ of possible ones.

For each isogeny $\phi : E \to E'$, get a map $\left\{ \begin{array}{c} \text{possible objects} \\ \text{for } E \end{array} \right\} \xrightarrow{\mathcal{F}(\phi)} \left\{ \begin{array}{c} \text{possible objects} \\ \text{for } E' \end{array} \right\}$.

category: $SS(\mathbb{F})$:

- objects: supersingular $E/\mathbb{F}$
- morphisms: $\mathrm{Hom}(E, E')$.

Functor $\mathcal{F} : SS(\mathbb{F}) \longrightarrow \mathrm{Sets}$

Often convenient to exclude isogenies of "bad" degree. (ex 3)

Σ set of primes.

category: $SS_{\Sigma}(\mathbb{F})$:

- objects: supersingular $E/\mathbb{F}$
- morphisms: $\mathrm{Hom}_{\Sigma}(E, E')$ isogenies of degree $\in \langle \Sigma \rangle$.

Category $\mathcal{C}$, functor $\mathcal{F} : \mathcal{C} \longrightarrow \mathrm{Sets}$

category of "$\mathcal{C}$ + extra structure from $\mathcal{F}$": $\mathrm{El}(\mathcal{F})$ "category of elements".

objects: pairs (c, x) $c \in \mathcal{C}$ $x \in \mathcal{F}(c)$

morphisms: $(c, x) \longrightarrow (c', x')$: $\phi \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ s.t. $\mathcal{F}(\phi)(x) = x'$.

$\mathcal{F} = \cancel{\mathrm{End}}\ \mathrm{Hom}(E_0, -)$

ex1: $SS(\mathbb{F}) \longrightarrow \mathrm{Sets}$

$\mathcal{F}(E) = \mathrm{Hom}(E_0, E)$

$\phi : E \to E' \qquad \underset{\underset{\mathrm{Hom}(E_0,E)}{\cap}}{\mathcal{F}(\phi)(\psi)} = \phi\psi \qquad \in \mathrm{Hom}(E_0, E')$

ex 2: $\mathcal{F} = \mathrm{End} \qquad SS(\mathbb{F}) \longrightarrow \mathrm{Sets}$

$\mathcal{F}(E) = \mathrm{End}(E)$

$\phi : E \to E' \qquad \mathcal{F}(\phi)(\underset{\underset{\mathrm{End}(E)}{\cap}}{\alpha}) = \phi\alpha\hat{\phi} \in \mathrm{End}(E')$

ex 3: $\mathcal{F} = \mathrm{Cyc}_N \qquad SS_\Sigma(\mathbb{F}) \longrightarrow \mathrm{Sets} \qquad \Sigma = \{\ell \nmid N\}$.

$\mathcal{F}(E) = \{$ cyclic subgroups of E of order $N\}$

$\phi : E \to E' \qquad \mathcal{F}(\phi)(C) = \phi(C)$.

problem: ex 1 & 2 $\mathcal{F}(E)$ infinite
- distribution?
- applying isogenies always makes objects bigger.

Hypothesis: $\mathcal{F}(E)$ is finite for all E.

ex. 1: $N \geq 1$. $\Sigma = \{\ell \nmid N\}$

$\mathcal{F} = (\mathrm{Hom}(E_0, -)/N)^\times : SS_\Sigma(\mathbb{F}) \to \mathrm{Sets}$

$\mathcal{F}(E) = \{\psi \in \mathrm{Hom}(E_0,E)/N\mathrm{Hom}(E_0,E) \mid \deg\psi \in (\mathbb{Z}/N\mathbb{Z})^\times\}$

$\phi \in \mathrm{Hom}_\Sigma(E, E'), \qquad \mathcal{F}(\phi)(\psi) = \phi\psi$.

ex 2: $N \geq 1$. $\Sigma = \{\ell \nmid N\}$

$\mathcal{F} = \mathrm{End}/N : SS_\Sigma(\mathbb{F}) \to \mathrm{Sets}$

$\mathcal{F}(E) = \mathrm{End}(E)/N\,\mathrm{End}(E) \qquad (\cong M_2(\mathbb{Z}/N\mathbb{Z})$ if $p \nmid N)$

$\phi : E \to E' \quad \mathcal{F}(\phi)(\alpha) = \phi\alpha\hat{\phi}$

variant: $\mathcal{F}' = (\mathrm{End}/N)' : SS_\Sigma(\mathbb{F}) \longrightarrow \mathrm{Rings}$

$\mathcal{F}'(E) = \mathrm{End}(E)/N\,\mathrm{End}(E)$

$\mathcal{F}'(\phi)(\alpha) = (\deg\phi)^{-1}\phi\alpha\hat{\phi} \mod N$.

Def. $\mathcal{F} : SS_{\Sigma}(\mathbb{F}) \longrightarrow \mathrm{Sets}$ functor, ($\mathcal{F}(E)$ finite).

Graph $\mathcal{G}_{\mathcal{F}}$:

- vertices: isomorphism classes of objects $c \in \mathcal{C}$ in ~~$El(\mathcal{F})$~~ $\mathcal{C}$
- edges: from $\cancel{(E,x)}$ $c \in \mathcal{C}$: isogenies $\cancel{\varphi \in Hom_{\Sigma}(E,E')}$ $\phi \in Hom_{\mathcal{C}}(c,c')$
  modulo automorphisms of $\cancel{(E', \mathcal{F}(\varphi)(x))}$. $Aut_{\mathcal{C}}(c')$

purely from category $El(\mathcal{F})$

$L^2(\mathcal{G}_{\mathcal{F}})$ = space of ($\mathbb{C}$-valued) functions on {vertices of $\mathcal{G}_{\mathcal{F}}$},

$$\langle F, G \rangle = \sum_{(E,x) \in \mathcal{G}_{\mathcal{F}}} \frac{F(E,x)\, G(E,x)}{\# \cancel{Aut}(E,x)} \quad \frac{F(c)G(c)}{\# Aut_{\mathcal{C}}(c)} \quad \text{for } F, G \in L^2(\mathcal{G}_{\mathcal{F}}).$$

Prime $l \in \Sigma$: adjacency operator $A_l \circlearrowright L^2(\mathcal{G}_{\mathcal{F}})$:

$$A_l F(E,x) = \sum_{\substack{(E,x) \longrightarrow (E',x') \\ \uparrow \\ \text{degree } l}} F(E',x').$$

Q: Spectrum of A_l? $\nearrow$ large ev: failure of equidistribution
$\searrow$ small ev: speed of equidistribution

3) Equidistribution theorem

Thm (P.-Weso) $N \geq 1$. Σ set of prime not dividing pN. $\mathcal{F}: SS_{\Sigma}(\mathbb{F}) \longrightarrow \mathrm{Sets}$.

short version

Assume:
- $\langle \Sigma \rangle = (\mathbb{Z}/N\mathbb{Z})^{\times}$ & $\Sigma \neq \emptyset$
- all $\mathcal{F}(E)$ are finite
- $\mathcal{F}$ satisfies the (mod N)-congruence property:
  $\forall E \in SS(\mathbb{F})$, $\forall \varphi, \psi \in End_{\Sigma}(E)$ s.t. $\varphi - \psi \in N\, End(E)$, $\mathcal{F}(\varphi) = \mathcal{F}(\psi)$

Then $\forall\, l \in \Sigma$, A_l is a normal operator on $L^2(\mathcal{G}_{\mathcal{F}})$ stabilising

- $L^2_{deg}(\mathcal{G}_{\mathcal{F}})$ subspace of functions constant on connected components of $\mathcal{G}^1_{\mathcal{F}} \subseteq \mathcal{G}_{\mathcal{F}}$ (same vertices, only edges with degree $\equiv 1$ mod N.)
  $|||A_l||| = l+1$ on $L^2_{deg}(\mathcal{G}_{\mathcal{F}})$.
- $L^2_0(\mathcal{G}_{\mathcal{F}}) = L^2_{deg}(\mathcal{G}_{\mathcal{F}})^{\perp}$. $|||A_l||| \leq 2\sqrt{l}$ on $L^2_0(\mathcal{G}_{\mathcal{F}})$.

Moreover, the A_l, $l \in \Sigma$ pairwise commute.

long version -

In addition, (pick $E_0 \in SS(\mathbb{F})$)

(1) $\forall \phi$ isogeny in $SS_\Sigma(\mathbb{F})$, $\mathcal{F}(\phi)$ is a bijection.

(2) $\forall E, E' \in SS(\mathbb{F})$, $\exists \phi \in \mathrm{Hom}_\Sigma(E,E')$ of degree 1 mod N

(3) $\mathrm{End}_\Sigma(E_0) \longrightarrow \underbrace{(\mathrm{End}(E_0)/N\,\mathrm{End}(E_0))^\times}_{G}$ is surjective

so $G \circlearrowright \mathcal{F}(E_0)$.

Write $\mathcal{F}(E_0) = Gx_1 \sqcup Gx_2 \sqcup \dots \sqcup Gx_n$, $H_i = \mathrm{Stab}_G(x_i)$.

Graph $\mathcal{G}_{\deg}$:

- vertex set : $\bigsqcup_i \underbrace{(\mathbb{Z}/N\mathbb{Z})^\times/\deg H_i}$

- edges : $\begin{matrix} \psi & & \psi \\ a & \xrightarrow{d} & ad \end{matrix}$

(Cayley graph) } easy spectrum of A_ℓ

(4) $\exists!$ morphism of graphs

$$\mathcal{G}_{\mathcal{F}} \xrightarrow{\mathrm{Deg}} \mathcal{G}_{\deg}$$

s.t. $\mathrm{Deg}(E_0, x_i) = 1 \in (\mathbb{Z}/N\mathbb{Z})^\times/\deg H_i$

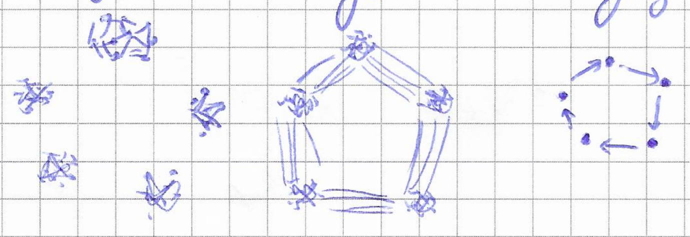
for ϕ edge in $\mathcal{G}_{\mathcal{F}}$, $\mathrm{Deg}(\phi)$ is labelled by $\deg\phi$ mod N

} disconnectedness + multipartition

(5) Deg is surjective

(6) $L^2_{\deg}(\mathcal{G}_{\mathcal{F}}) =$ space of functions that factor through Deg.

$$\mathcal{G}^1_{\mathcal{F}} \longrightarrow \mathcal{G}_{\mathcal{F}} \longrightarrow \mathcal{G}_{\deg}$$



ex 3: $p \nmid N$, $\Sigma = \{\ell \nmid pN\}$. $\mathcal{F} = \mathrm{Cyc}_N$

$G \cong GL_2(\mathbb{Z}/N\mathbb{Z})$

$\mathcal{F}(E_0) \cong \{\mathbb{Z}/N\mathbb{Z} - \text{lines in } (\mathbb{Z}/N\mathbb{Z})^2\}$

$n=1$ $\quad x_1 \longleftrightarrow \mathbb{Z}/N\mathbb{Z} \cdot \begin{pmatrix}1\\0\end{pmatrix}$

$H = H_1 \longleftrightarrow \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

$\deg H = (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow L^2_{\deg}(\mathcal{G}_{\mathrm{Cyc}_N}) = \mathbb{C}\cdot 1$.

random walks converge to almost uniform.

ex 1: $\mathcal{F} = (\mathrm{Hom}(E_0,-)/N)^\times$.

$$G = (\mathrm{End}(E_0)/N\mathrm{End}(E_0))^\times$$

$\circlearrowleft$ $\circlearrowleft$ left regular.

$$\mathcal{F}(E_0) = (\mathrm{End}(E_0)/N\mathrm{End}(E_0))^\times$$

$n=1$ $x_1 = \mathrm{id}$ $H_1 = \{1\}$.

$\Rightarrow$ $\mathcal{G}_{deg}$ = Cayley graph of $(\mathbb{Z}/N\mathbb{Z})^\times$.

$$\mathrm{Deg}: \mathcal{G}_{\mathcal{F}} \longrightarrow \mathcal{G}_{deg}$$
$$(E,\psi) \longmapsto (\deg\psi) \bmod N$$

$\Rightarrow$ * equidistribution up to degree constraint.

Cor (P.-Weso) Algo to compute End(E) in time $\tilde{O}(\sqrt{p})$ (unconditional)

previous ↗ GRH ↘ $\tilde{O}(p)$

ex2: $\mathcal{F} = (\mathrm{End}/N)'$. $p \nmid N$.

$$G \cong GL_2(\mathbb{Z}/N\mathbb{Z})$$

$\circlearrowleft$ $\circlearrowleft$ conjugation.

$$\mathcal{F}(E_0) \cong M_2(\mathbb{Z}/N\mathbb{Z})$$

- connected components $\longleftrightarrow$ orbits: conjugacy classes
- mostly $(\mathbb{Z}/N\mathbb{Z})^\times = \deg H$.

$\Rightarrow$ equidistribution up to "obvious constraints".

$\Rightarrow$ + work Thm (P.-Weso) EndRing $\xleftrightarrow{\text{Poly}}$ OneEnd.

4) Ideas of proof

① Deuring correspondence: SS E.C $\longleftrightarrow$ maximal orders in quat alg.

Kohel: categorical version: equivalence

$$\begin{array}{ccc} SS(\bar{\mathbb{F}}) & \cong & \mathrm{Mod}(\mathcal{O}) \\ \downarrow \mathcal{F} & & \downarrow \mathcal{F}' \\ \text{Sets} & & \text{Sets} \end{array}$$

② $\mathrm{Mod}(\mathcal{O}) \xrightarrow{\mathcal{F}'}$ Sets + (mod N)-cong prop

$\longrightarrow$ $\mathcal{F}' \cong \bigsqcup_i \mathcal{F}_{U_i}$ $U_i \subseteq \hat{\mathcal{O}}^\times$ compact open, level N.

$L^2(\mathcal{G}_{\mathcal{F}_{U_i}})$ = space of quaternionic automorphic forms.

(Eichler) $A_\ell \longleftrightarrow$ Hecke ops.

③ JL + (Shimura) Deligne.