Un algorithme à la Pollard pour le problème du sac à dos

Gaetan Bisson

LORIA, Nancy, France

TU/e, Eindhoven, Pays-Bas

travaux communs avec

Andrew V. Sutherland

Produits courts dans un groupe

Soit une suite finie S d'éléments d'un groupe fini G.
Comment trouver une sous-suite dont le produit vaut un $z \in G$ donné.

Notons $\pi : \mathfrak{P}(S) \to G$ l'application produit et cherchons des préimages.

Produits courts dans un groupe

Soit une suite finie S d'éléments d'un groupe fini G.
Comment trouver une sous-suite dont le produit vaut un $z \in G$ donné.

Notons $\pi : \mathfrak{P}(S) \to G$ l'application produit et cherchons des préimages.

EXEMPLE : pour G engendré par g et $S = \left(g, g^2, g^4, g^8, \ldots, g^{2^{\lfloor \log_2 \#G \rfloor}}\right)$,
écrire z en produit court, c'est calculer son logarithme en base g.

Produits courts dans un groupe

Soit une suite finie S d'éléments d'un groupe fini G.
Comment trouver une sous-suite dont le produit vaut un $z \in G$ donné.

Notons $\pi : \mathfrak{P}(S) \to G$ l'application produit et cherchons des préimages.

Exemple : pour G engendré par g et $S = \left(g, g^2, g^4, g^8, \ldots, g^{2^{\lfloor \log_2 \#G \rfloor}}\right)$,
écrire z en produit court, c'est calculer son logarithme en base g.

Soient des instances avec $\#S \sim d \log_2 \#G$ et $\#G \to \infty$ pour $d > 1$ fixé.

Produits courts dans un groupe

Soit une suite finie S d'éléments d'un groupe fini G.
Comment trouver une sous-suite dont le produit vaut un $z \in G$ donné.

Notons $\pi : \mathfrak{P}(S) \to G$ l'application produit et cherchons des préimages.

EXEMPLE : pour G engendré par g et $S = \left(g, g^2, g^4, g^8, \ldots, g^{2^{\lfloor \log_2 \#G \rfloor}}\right)$,
écrire z en produit court, c'est calculer son logarithme en base g.

Soient des instances avec $\#S \sim d \log_2 \#G$ et $\#G \to \infty$ pour $d > 1$ fixé.

EXEMPLE : pour $G = \mathbb{Z}/n$, solutions en $O(n^{0.3113})$. (Joux et Howgrave-Graham)

Ici, on s'intéresse au case générique.

Pas de bébé, pas de géant

Algorithme (G, S, z) :

1. Découper S en deux suites de même taille A et B.
2. Calculer et stocker les couples $(x, \pi(x))$ pour $x \in \mathfrak{P}(A)$.
3. Pour tout $y \in \mathfrak{P}(B)$:
4. Si $z\pi(y)^{-1} = \pi(x)$ alors $z = \pi(xy)$.

Pas de bébé, pas de géant

Algorithme (G, S, z) :

1. Découper S en deux suites de même taille A et B.
2. Calculer et stocker les couples $(x, \pi(x))$ pour $x \in \mathfrak{P}(A)$.
3. Pour tout $y \in \mathfrak{P}(B)$:
4. Si $z\pi(y)^{-1} = \pi(x)$ alors $z = \pi(xy)$.

Théorème (Impagliazzo et Naor)

Si $d > 2$ les produits courts de A et B sont asymptotiquement équidistribués dans G.

Coût en temps : $O(\sqrt{\#G})$
Coût en mémoire : $O(\sqrt{\#G})$

Méthode à la Pollard

Posons $\mu : (y_1, \ldots, y_m) \mapsto (y_m^{-1}, \ldots, y_1^{-1})$ de sorte que $\pi(\mu(y)) = \pi(y)^{-1}$.

On cherche *une collision* $\pi(x) = \pi(z\mu(y))$ avec $x \in \mathfrak{P}(A), y \in \mathfrak{P}(B)$.

Méthode à la Pollard

Posons $\mu : (y_1, \ldots, y_m) \mapsto (y_m^{-1}, \ldots, y_1^{-1})$ de sorte que $\pi(\mu(y)) = \pi(y)^{-1}$.

On cherche *une collision* $\pi(x) = \pi(z\mu(y))$ avec $x \in \mathfrak{P}(\mathrm{A}), y \in \mathfrak{P}(\mathrm{B})$.

Une fonction d'itération ϕ doit :

- aller de $\underbrace{\mathfrak{P}(\mathrm{A})}_{\mathscr{A}} \sqcup \underbrace{\{z\mu(y) : y \in \mathfrak{P}(\mathrm{B})\}}_{\mathscr{B}}$ dans lui-même ;
- être pseudo-aléatoire ;
- préserver les collisions : $\pi(x) = \pi(y) \Rightarrow \pi(\phi(x)) = \pi(\phi(y))$.

Méthode à la Pollard

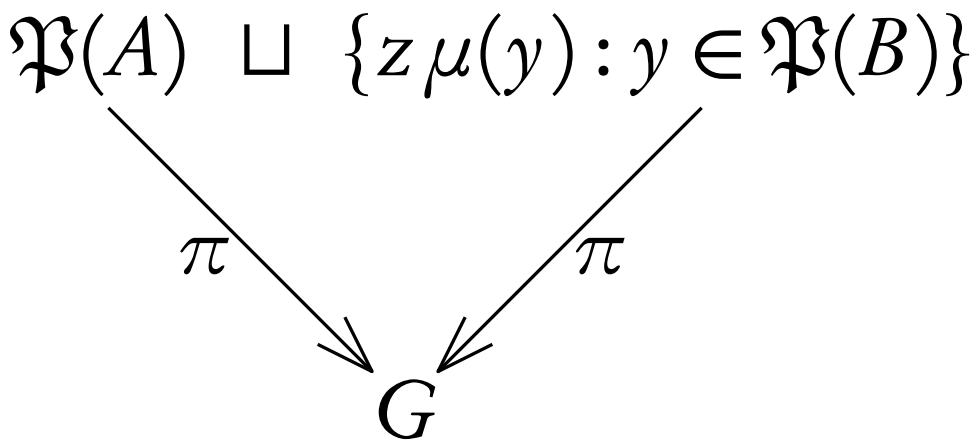
Posons $\mu : (y_1, \ldots, y_m) \mapsto (y_m^{-1}, \ldots, y_1^{-1})$ de sorte que $\pi(\mu(y)) = \pi(y)^{-1}$.

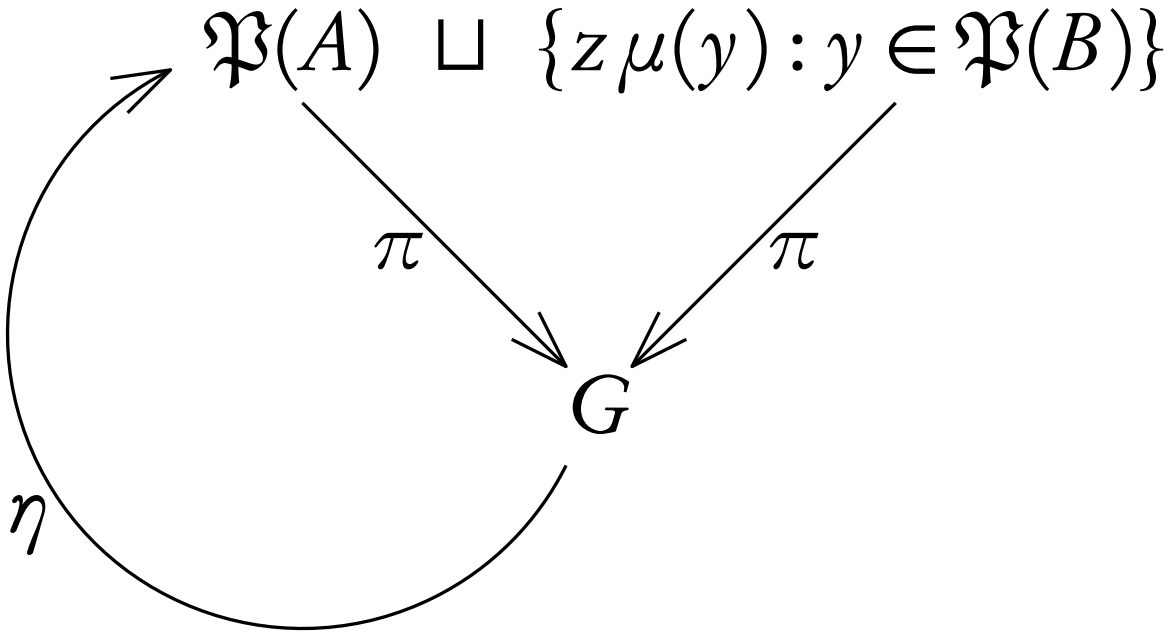
On cherche *une collision* $\pi(x) = \pi(z\mu(y))$ avec $x \in \mathfrak{P}(\mathrm{A}), y \in \mathfrak{P}(\mathrm{B})$.

Une fonction d'itération ϕ doit :

- aller de $\underbrace{\mathfrak{P}(\mathrm{A})}_{\mathscr{A}} \sqcup \underbrace{\{z\mu(y) : y \in \mathfrak{P}(\mathrm{B})\}}_{\mathscr{B}}$ dans lui-même ;
- être pseudo-aléatoire ;
- préserver les collisions : $\pi(x) = \pi(y) \Rightarrow \pi(\phi(x)) = \pi(\phi(y))$.

Prenons $\phi = \eta \circ \pi$ avec $\eta : \mathrm{G} \to \mathscr{A} \sqcup \mathscr{B}$ fonction de hachage.


$\mathfrak{P}(A) \sqcup \{z\,\mu(y) : y \in \mathfrak{P}(B)\}$
π
π
G


$\mathfrak{P}(A) \sqcup \{z\,\mu(y) : y \in \mathfrak{P}(B)\}$
π
π
G
η

Algorithme à la Pollard

ALGORITHME (G, S, z) :

1. Découper S en AB.
2. Choisir $w \in \mathscr{A} \sqcup \mathscr{B}$ et $\phi = \pi \circ \eta$.

3. Itérer ϕ et ***trouver une collision*** : $\phi^{(i+j)}(w) = \phi^{(i)}(w)$.
4. Poser $s = \phi^{(i+j-1)}(w)$ et $t = \phi^{(i-1)}(w)$.

5. Si $\pi(s) = \pi(t)$:
6. Si $s \in \mathscr{A}$ et $t = z\mu(y) \in \mathscr{B}$ renvoyer $z = \pi(sy)$.
7. Si $t \in \mathscr{A}$ et $s = z\mu(y) \in \mathscr{B}$ renvoyer $z = \pi(ty)$.
8. Retourner en 1.

Algorithme à la Pollard

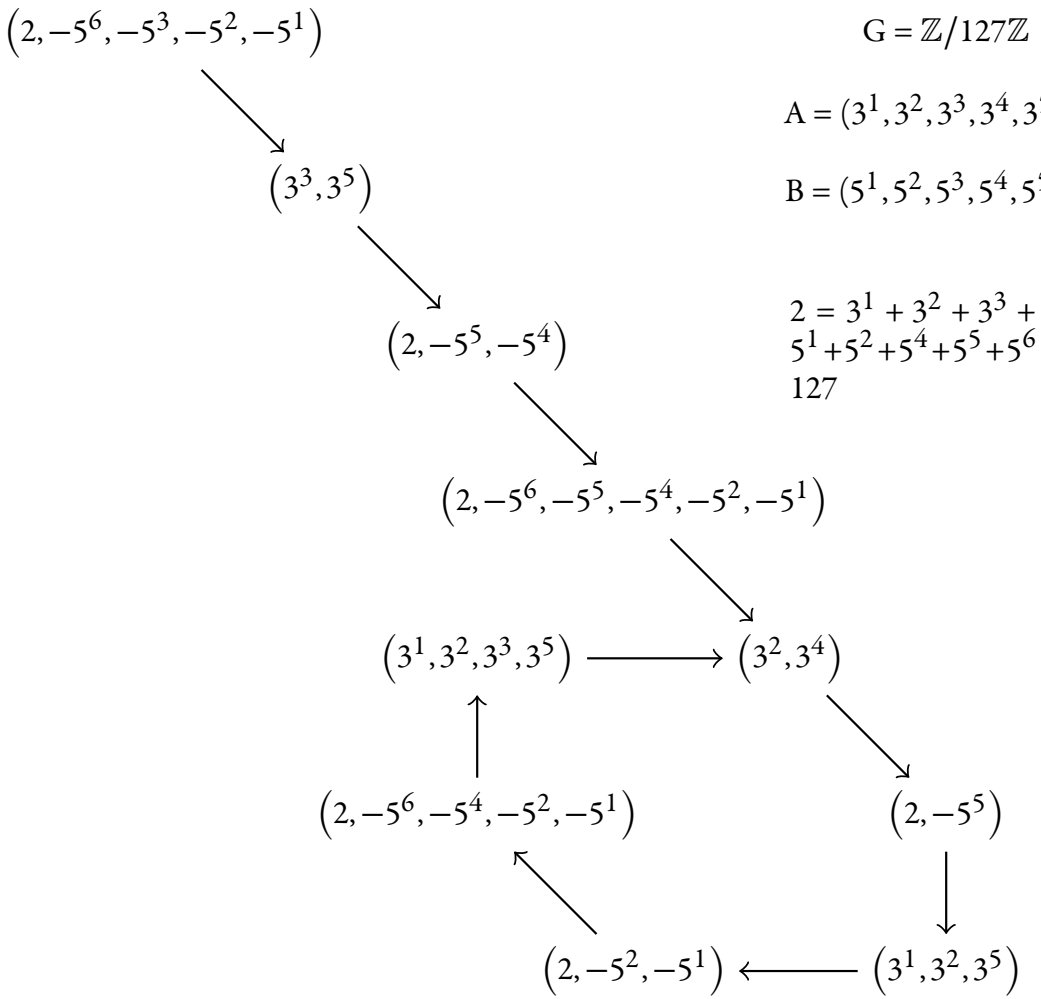
Algorithme (G, S, z) :

1. Découper S en AB.
2. Choisir $w \in \mathscr{A} \sqcup \mathscr{B}$ et $\phi = \pi \circ \eta$.

3. Itérer ϕ et ***trouver une collision*** : $\phi^{(i+j)}(w) = \phi^{(i)}(w)$.
4. Poser $s = \phi^{(i+j-1)}(w)$ et $t = \phi^{(i-1)}(w)$.

5. Si $\pi(s) = \pi(t)$:
6. Si $s \in \mathscr{A}$ et $t = z\mu(y) \in \mathscr{B}$ renvoyer $z = \pi(sy)$.
7. Si $t \in \mathscr{A}$ et $s = z\mu(y) \in \mathscr{B}$ renvoyer $z = \pi(ty)$.
8. Retourner en 1.

Prouvé avec η oracle aléatoire pour $d > 4$.
Marche en pratique dès que $d \geq 2$.

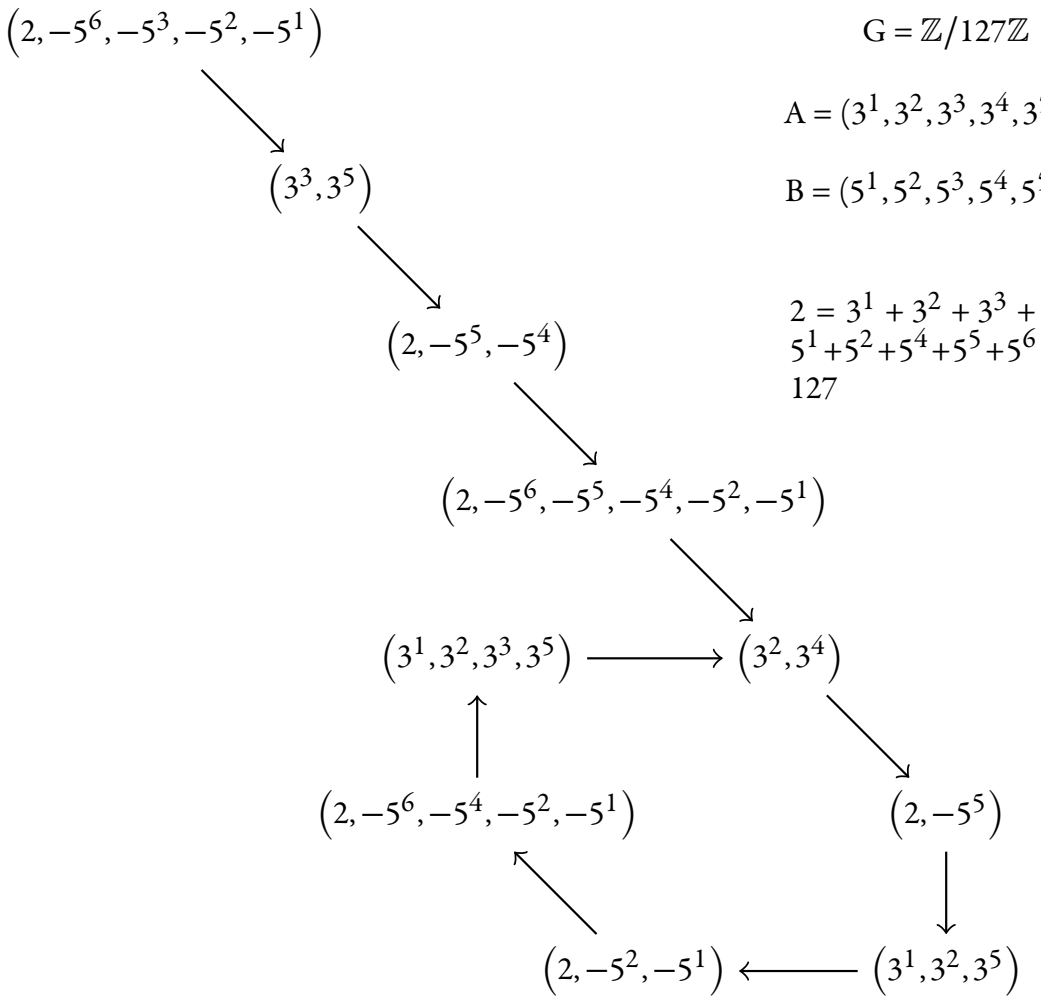


$G = \mathbb{Z}/127\mathbb{Z}$

$A = (3^1, 3^2, 3^3, 3^4, 3^5, 3^6)$

$B = (5^1, 5^2, 5^3, 5^4, 5^5, 5^6)$

$2 = 3^1 + 3^2 + 3^3 + 3^5 + 5^1 + 5^2 + 5^4 + 5^5 + 5^6 \bmod 127$



$G = \mathbb{Z}/127\mathbb{Z}$

$A = (3^1, 3^2, 3^3, 3^4, 3^5, 3^6)$

$B = (5^1, 5^2, 5^3, 5^4, 5^5, 5^6)$

$2 = 3^1 + 3^2 + 3^3 + 3^5 + 5^1 + 5^2 + 5^4 + 5^5 + 5^6 \bmod 127$

Calculs avec $\#G \approx 2^{80}$ pour :

$$\begin{cases} G = GL_2(\mathbb{F}_p) \\ S \text{ aléatoire} \end{cases}$$

$$\begin{cases} G = \mathscr{E}/\mathbb{F}_p \\ S = \{\text{points de petite abscisse}\} \end{cases}$$

$$\begin{cases} G = \mathrm{cl}(\mathscr{O}) \\ S = \{\text{petits idéaux premiers}\} \end{cases}$$

Isogénies entre courbes elliptiques

Une *isogénie* est un morphisme de courbes elliptiques.

Calculer une isogénie se fait en temps $\ell^{2+o(1)}$ en son degré ℓ.

Cela *transfère le problème du logarithme discret* d'une courbe à l'autre.

Isogénies entre courbes elliptiques

Une *isogénie* est un morphisme de courbes elliptiques.

Calculer une isogénie se fait en temps $\ell^{2+o(1)}$ en son degré ℓ.

Cela *transfère le problème du logarithme discret* d'une courbe à l'autre.

Isogénies Verticales : degrés restreints (potentiellement grands).
Isogénies Horizontales : degrés très nombreux (dont petits).

Isogénies entre courbes elliptiques

Une *isogénie* est un morphisme de courbes elliptiques.

Calculer une isogénie se fait en temps $\ell^{2+o(1)}$ en son degré ℓ.

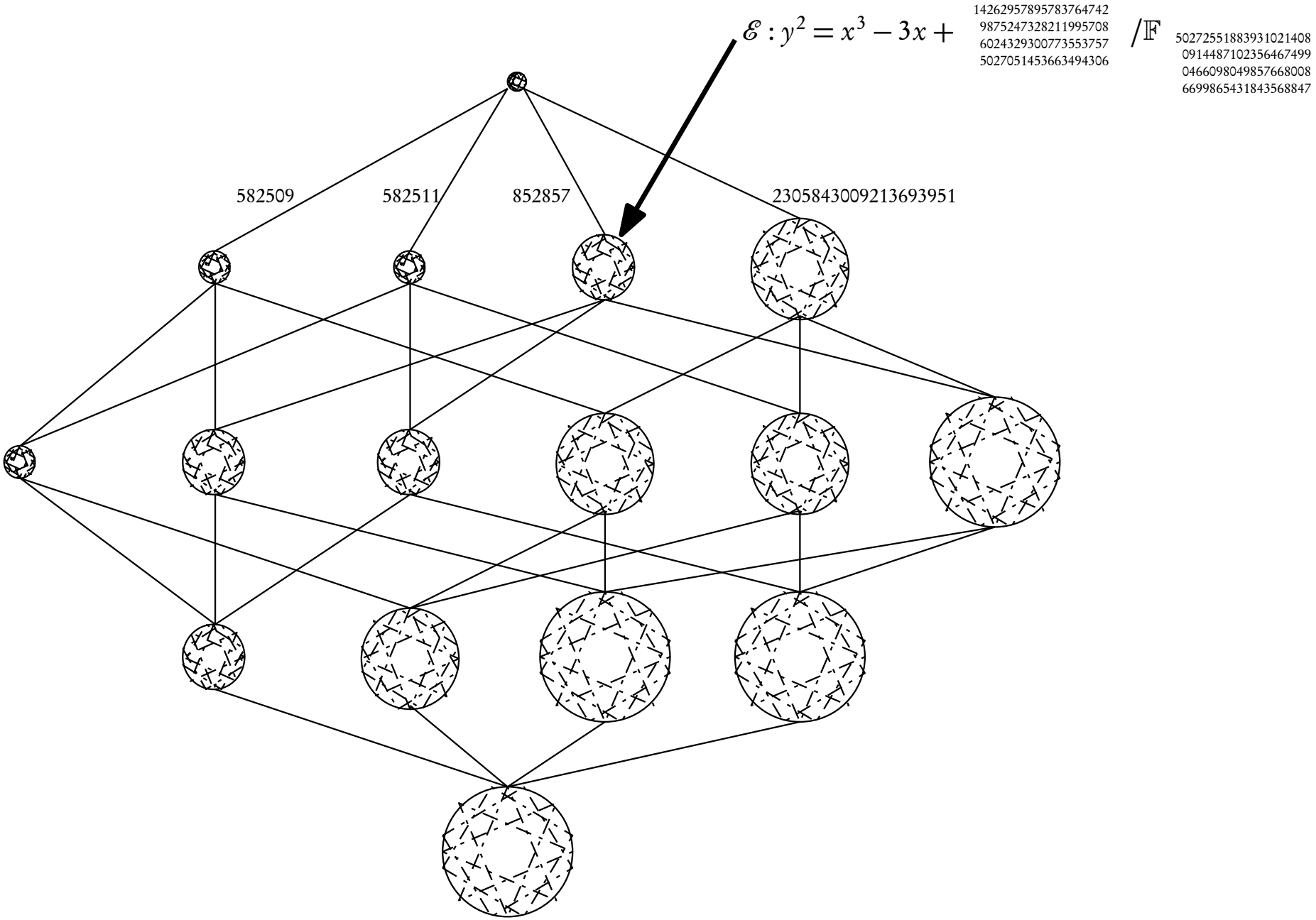
Cela *transfère le problème du logarithme discret* d'une courbe à l'autre.

Isogénies Verticales : degrés restreints (potentiellement grands).
Isogénies Horizontales : degrés très nombreux (dont petits).

Théorème (multiplication complexe)

Un idéal de $\mathcal{O} = \mathrm{End}\,\mathcal{E}$ de norme ℓ agit comme une isogénie de degré ℓ.

Cela induit une action fidèle et transitive du groupe des classes d'idéaux de $\mathcal{O}$ sur la classe de $\mathcal{E}$ modulo les isogénies horizontales.


$\mathcal{E} : y^2 = x^3 - 3x +$
14262957895783764742
98752473282119957708
60243293007735537757
50270514536634943306
$/\mathbb{F}$
50272551883931021408
09144871023564674999
04660980498576680008
66998654318435688847
582509
582511
852857
2305843009213693951

Recherche d'isogénie par Pollard

Si $\mathscr{E}$ et $\mathscr{E}'$ ont même anneau d'endomorphismes $\mathscr{O}$,
on cherche un idéal court x de $\mathscr{O}$ qui envoie $\mathscr{E}$ sur $\mathscr{E}'$.

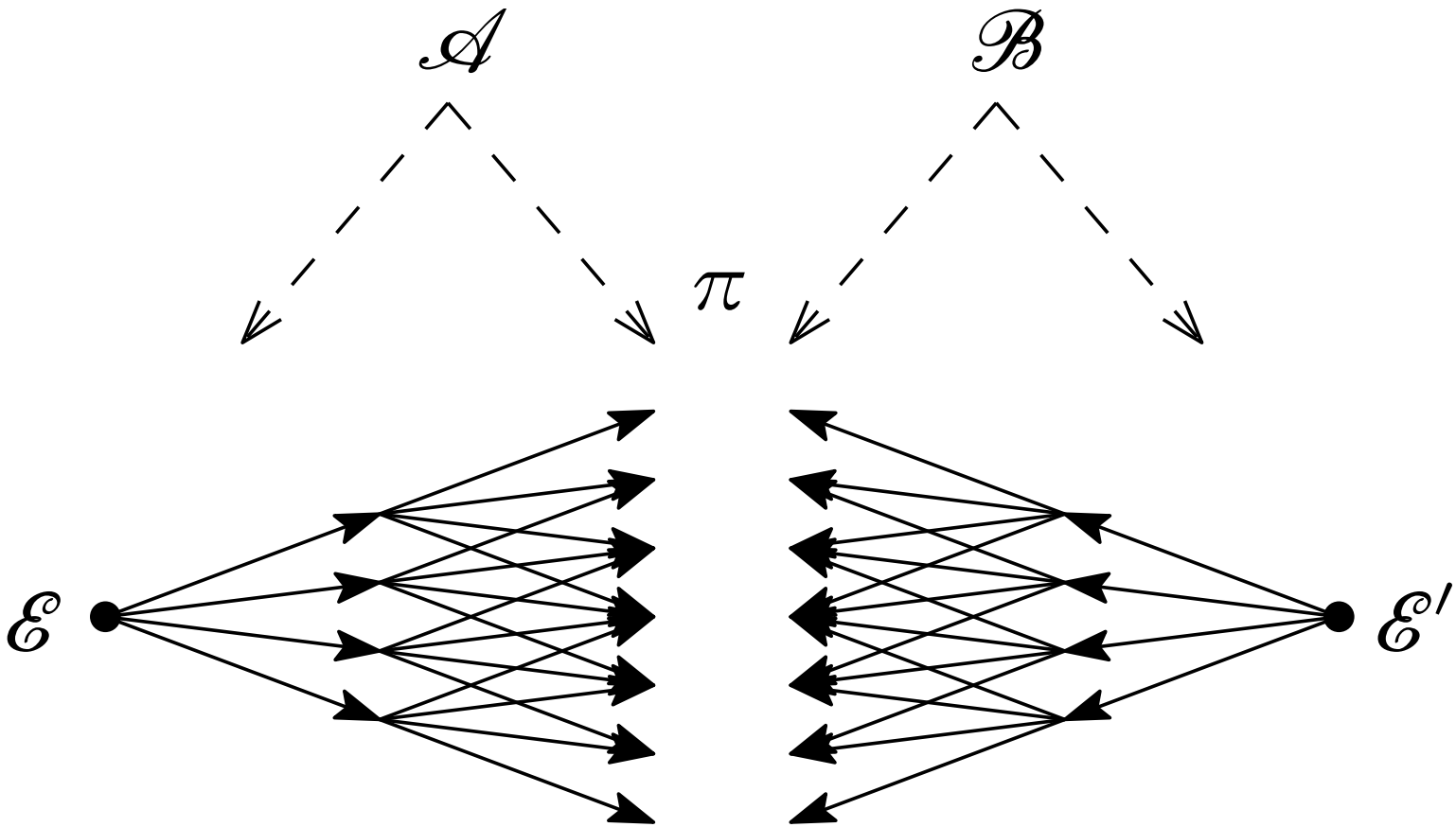
Recherche d'isogénie par Pollard

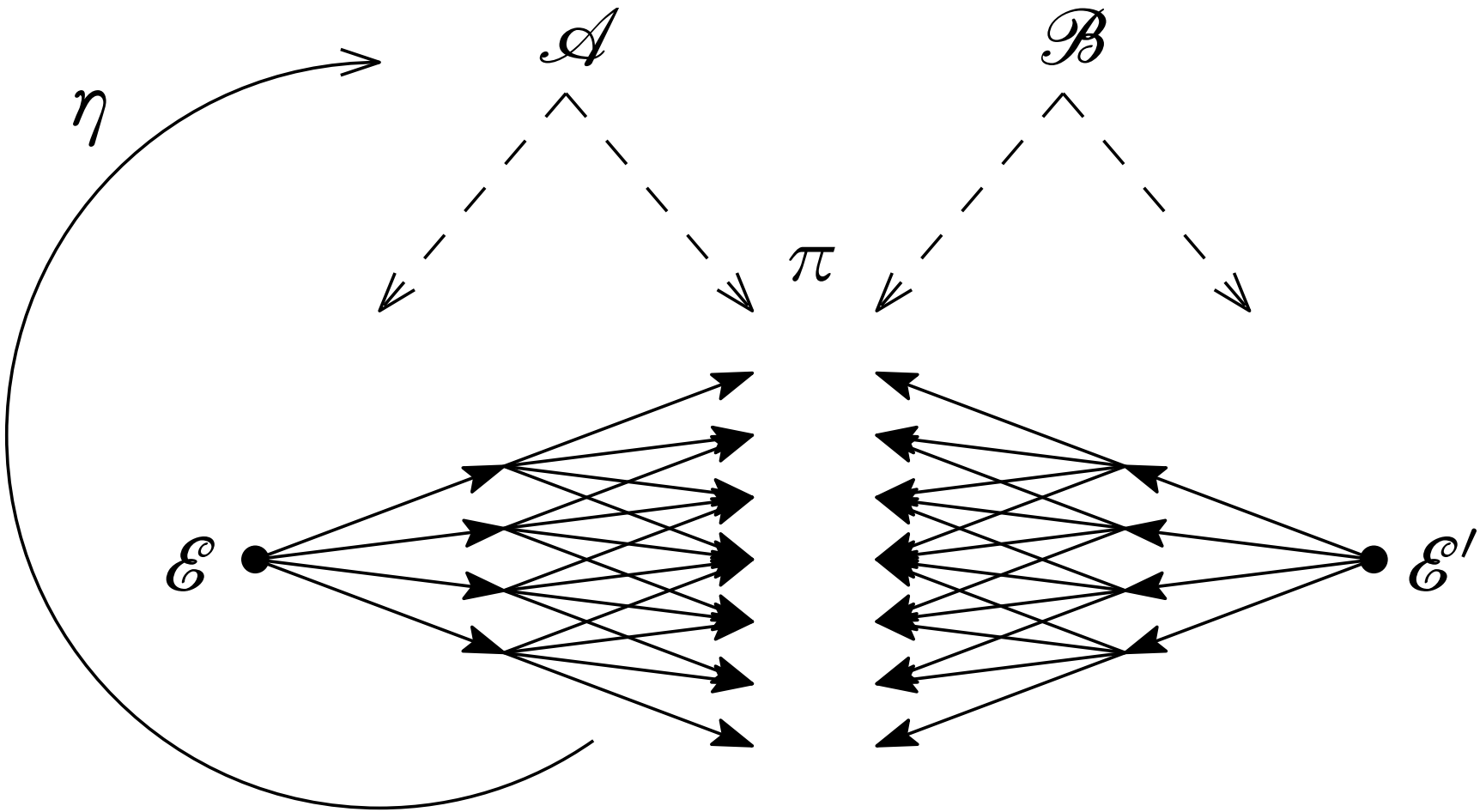
Si $\mathscr{E}$ et $\mathscr{E}'$ ont même anneau d'endomorphismes $\mathscr{O}$,
on cherche un idéal court x de $\mathscr{O}$ qui envoie $\mathscr{E}$ sur $\mathscr{E}'$.

$G = \{\text{classes d'isomorphismes de courbes d'anneau d'endomorphismes } \mathscr{O}\}$

$S = \{\text{idéaux de petite norme de } \mathscr{O}\} = AB \qquad \mathscr{A} = \mathfrak{P}(A) \qquad \mathscr{B} = \mu(\mathfrak{P}(B))$

$\pi : \mathscr{A} \sqcup \mathscr{B} \to G$ envoie un idéal de $\mathscr{A}$ sur l'image de l'isogénie partant de $\mathscr{E}$.
$\pi : \mathscr{A} \sqcup \mathscr{B} \to G$ envoie un idéal de $\mathscr{B}$ sur l'image de l'isogénie partant de $\mathscr{E}'$.


$\mathscr{A}$
$\mathscr{B}$
π
$\mathscr{E}$
$\mathscr{E}'$


$\mathscr{A}$
$\mathscr{B}$
η
π
$\mathscr{E}$
$\mathscr{E}'$

Résultats

Heuristiquement, on trouve une $\mathscr{E} \to \mathscr{E}'$ en temps $(\operatorname{disc} \mathscr{O})^{1/4+o(1)}$.

Pareil sous GRH via (Jao, Miller et Venkatesan) en prenant plus d'idéaux premiers.

Résultats

Heuristiquement, on trouve une $\mathscr{E} \to \mathscr{E}'$ en temps $(\mathrm{disc}\,\mathscr{O})^{1/4+o(1)}$.

Pareil sous GRH via (Jao, Miller et Venkatesan) en prenant plus d'idéaux premiers.

Auparavant :

Galbraith (1999) utilisait l'approche «pas de bébés...» (mémoire exponentielle)

Galbraith, Hess et Smart (2002) itéraient une fonction, obtenaient une énorme isogénie, puis la friabilisaient $\Rightarrow$ idéal de taille $L[1/2]$.

Résultats

Heuristiquement, on trouve une $\mathscr{E} \to \mathscr{E}'$ en temps $(\operatorname{disc} \mathscr{O})^{1/4+o(1)}$.

Pareil sous GRH via (Jao, Miller et Venkatesan) en prenant plus d'idéaux premiers.

Auparavant :

Galbraith (1999) utilisait l'approche «pas de bébés...» (mémoire exponentielle)

Galbraith, Hess et Smart (2002) itéraient une fonction, obtenaient une énorme isogénie, puis la friabilisaient $\Rightarrow$ idéal de taille $L[1/2]$.

Ici, l'isogénie est courte et obtenue avec peu de mémoire.

FIN

http://arxiv.org/abs/1101.0564
http://eprint.iacr.org/2011/004