Logarithme discret dans les corps finis de petite charactéristique

Édouard Rousseau
Université de Versailles

25 mai 2017

TABLE DES MATIÈRES

CONTEXTE

Soit G un groupe cyclique engendré par un élément g, et notons N le cardinal de G. On a alors une *bijection*

$$\begin{array}{rccc} exp_g : & \mathbb{Z}/N\mathbb{Z} & \rightarrow & G \\ & \bar{n} & \mapsto & g^n \end{array}.$$

On note la bijection récriproque log_g.

LE PROBLÈME DU LOGARITHME DISCRET

- En pratique, étant donné un entier n, on dispose d'algorithmes efficaces pour calculer g^n.
- Étant donné $x = g^n \in G$, *on ne dispose pas* d'algorithmes efficaces pour retrouver n.

C'est ce problème, « Comment retrouver n ? », qu'on appelle *Problème du logarithme discret*.

Intérêt en cryptographie

En cryptographie, exp_g est appelée *fonction à sens unique* car

- exp_g est facile à calculer
- sa réciproque, log_g, est difficile à calculer.

Ces fonctions sont très étudiées en cryptographie car elles permettent typiquement de rendre l'opération de cryptage simple et l'opération de décryptage longue et compliquée.

BREF HISTORIQUE DU PROBLÈME

Pour exprimer la difficulté d'un problème, on parle de sa complexité et on utilise la notation

$$L_N(\alpha, c) = \exp((c + o(1))(\log N)^{\alpha}(\log \log N)^{1-\alpha}).$$

On note aussi $L_N(\alpha)$ quand on ne veut pas préciser la constante. On distingue deux types d'algorithmes :

- Les algorithmes *génériques* en $O(\sqrt{N})$
- Les algorithmes de *calcul d'indice*, qui exploitent la structure de groupes issus de corps finis : $\mathbb{F}_q^{\times}$

Bref historique du problème

- Apparition dans “New directions in cryptography” de Diffie et Hellman (1976)
- Premier algorithme sous-exponentiel : Adleman (1979), complexité en $L_N(1/2)$
- Premier algorithme en $L(1/3)$ dans les corps finis binaires : Coppersmith (1984)
- Crible algébrique dans les corps premiers : 1993, $L(1/3)$
- Crible géométrique, utilisable en petite caractéristique : 1994, généralisations en 1999, 2002, 2006 ; $L(1/3)$
- Généralisation du crible algébrique en 2006, on peut dès lors résoudre des logarithmes discret en $L(1/3)$ dans tout type de corps fini

Bref historique du problème

Et plus récemment, dans les corps finis de petite caractéristique :

- Nouvel algorithme dû à Joux (2013) en $L(1/4)$
- Algorithme *quasi-polynomial* dû à Barbulescu, Gaudry, Joux et Thomé en 2014
- Second algorithme quasi-polynomial dû à Granger, Kleinjung et Zumbrägel en 2014

PRINCIPE GÉNÉRAL

Supposons qu'on veuille trouver $log_g(h)$ où $h \in G$. On choisit $F \subset G$ tel que $\langle F \rangle = G$.

1. On trouve des relations entre les éléments de F
2. On résout le système linéaire engendré par ces relations
3. On exprime h en fonction des éléments de F

Les étapes $1, 2$ et 3 dépendent du groupe G et de sa représentation, et donnent lieu à des complexités différentes selon les cas.

Un exemple

Contexte :

- On considère $G = \mathbb{F}_p^\times$ pour un nombre premier p, on a toujours $N = |G|$
- On considère $F = \{f \mid f \leq B,\ f \text{ premier}\}$ pour une certaine borne B
- On suppose que $g \in F$, sinon on rajoute g dans F.

Un exemple

Étape 1 : génération des relations

- On choisi $e \in \mathbb{Z}/N\mathbb{Z}$ aléatoirement
- On calcule g^e
- On teste si g^e, vu comme entier, est B-friable, *i.e.* n'a que des diviseurs premiers inférieurs à B
- Si c'est le cas, on a une relation dans G :

$$g^e = \prod_{f \in F} f^{e_f}, \text{ où } e_f \in \mathbb{N}$$

qui se traduit en

$$e = \sum_{f \in F} e_f \log_g(f).$$

UN EXEMPLE

Étape 2 : algèbre linéaire. Une fois qu'on a assez de relations, *i.e.* au moins $|F|$, on résout le système linéaire obtenu dans $\mathbb{Z}/N\mathbb{Z}$ pour obtenir tous les $\log_g(f)$ pour $f \in F$.

Étape 3 : exprimer h en fonction des éléments de F :

- On choisi $e \in \mathbb{Z}/N\mathbb{Z}$ aléatoirement
- On calcule hg^e
- On teste si hg^e est B-friable
- Si c'est le cas, on a une relation

$$\log_g(h) = \sum_{f \in F} e_f \log_g(f) - e$$

Un exemple

Cet algorithme dépend du choix de B :

- Lorsque B est grand, $\langle F \rangle$ est plus grand donc il est plus simple de trouver des relations
- Mais quand $|F|$ est grand, il faut résoudre un système linéaire plus grand également.

In fine, avec un choix judicieux de B, on trouve une complexité en $L(1/2)$.

DÉFINITIONS

Avant d'entrer dans le cœur du sujet, revenons sur quelques points de terminologie. Lorsque l'on considère le problème du logarithme discret dans une famille de corps finis $\mathbb{F}_q$, où $q = p^n$ et $q \to \infty$, les algorithmes dépendent de la grandeur relative de p et n, si $p = L_q(\alpha)$:

- Si $\alpha > \frac{2}{3}$, on parle de *grande caractéristique*
- Si $\frac{1}{3} < \alpha < \frac{2}{3}$, on parle de *moyenne caractéristique*
- Si $0 < \alpha < \frac{1}{3}$, on parle de *petite-moyenne caractéristique*
- Si $\alpha = 0$, on parle de *petite caractéristique*

Définitions

Toujours dans le cadre d'une famille de corps finis F_q, un algorithme dont la complexité est $\log q^{O(\log \log q)}$ est dit *quasi-polynomial*. Cette complexité est plus petite que toutes les complexités $L(\varepsilon)$ pour $\varepsilon > 0$ mais plus grande que tout polynôme en $\log q$.

ALGORITHME DE BARBULESCU, GAUDRY, JOUX ET THOMÉ

On note $\mathbb{K}$ le corps fini dans lequel on veut travailler.

- On suppose $\mathbb{K} = \mathbb{F}_{q^{2k}}$ et on on représente $\mathbb{K}$ par $\mathbb{F}_{q^2}[X]/(I_X)$ où I_X est un polynôme irréductible de degré k divisant $h_1 X^q - h_0$ et $\deg h_i \leq 2$ (l'existence des h_i est heuristique).
- L'ensemble F est l'ensemble des polynômes de degré 1.

L'algorithme se base sur une *descente* : on exprime le logarithme d'un polynôme en fonction de $O(q^2 k)$ logarithmes de polynômes de degré deux fois plus petit, jusqu'à n'obtenir que des polynômes dans F.

- Complexité : $(q^2 k)^{O(\log k)}$.

LA DESCENTE

On va utiliser l'équation

$$X^q - X = \prod_{a \in \mathbb{F}_q} (X - a)$$

qu'on transorme en

$$X^q Y - XY^q = \prod_{(\alpha,\beta) \in \mathcal{S}} (\beta X - \alpha Y) \tag{1}$$

où $\mathcal{S}$ est un ensemble de représentants des $q+1$ points de la droite projective $\mathbb{P}^1(\mathbb{F}_q)$ choisi tel que l'équation (1) soit vraie.

LA DESCENTE

Supposons qu'on souhaite appliquer l'algorithme à un élément P. On va générer des relations en substituant $aP+b$ à X et $cP+d$ à Y dans l'équation (1), avec $a,b,c,d \in \mathbb{F}_{q^2}$, on obtient une nouvelle équation $(E_{a,b,c,d})$. Il vient

$$\frac{1}{h_1^D}\mathcal{L}_{a,b,c,d} \quad = \quad \lambda \prod_{(\alpha,\beta)\in\mathcal{S}} (P-\mu_{\alpha,\beta})$$

où $\lambda, \mu_{\alpha,\beta} \in \mathbb{F}_{q^2}$ et $\mathcal{L}_{a,b,c,d}$ est un polynôme de degré $D \leq 3\deg P$, obtenu en utilisant l'égalité $X^q = \frac{h_0}{h_1} \mod I_X$.

La descente

On garde seulement les équations $(E_{a,b,c,d})$ dont le côté gauche $\mathcal{L}_{a,b,c,d}$ est $\left\lceil \frac{\deg P}{2} \right\rceil$-friable et on combine ces équations pour que le côté droit, composé des translatés de P, ne fasse intervenir que P.
La combinaison de ces équations donne alors un côté gauche composé seulement de polynômes $\mathcal{L}_{a,b,c,d}$ de degré au plus $\left\lceil \frac{\deg P}{2} \right\rceil$.

- Certaines hypothèses sont heuristiques !
  - Existence de la combinaison
  - Friabilité des polynômes $\mathcal{L}_{a,b,c,d}$

Algorithme de Granger, Kleinjung et Zumbrägel

Ici $\mathbb{K} = \mathbb{F}_{q^k}$ et on voit $\mathbb{K}$ comme $\mathbb{F}_q[X]/(I_X)$ où I_X est un polynôme de degré k qui divise $h_1 X^q - h_0$. L'algorithme suit le même principe que juste avant mais la phase de descente est différente.

ÉLIMINATION "À LA VOLÉE"

Supposons $Q \in \mathbb{F}_{q^m}[X]$ et $\deg Q = 2$. Cette élimination se base sur le fait que le polynôme $P = X^{q+1} + aX^q + bX + c$ se scinde complètement dans $\mathbb{F}_{q^m}[X]$ pour environ q^{m-3} triplets (a, b, c). Or

$$P = \frac{1}{h_1}((X + a)h_0 + (bX + c)h_1) \mod I_X$$

Donc si $Q|(X + a)h_0 + (bX + c)h_1$ (polynôme de degré 3), on a

$$h_1 P = QL \mod I_X$$

où L est de degré 1 et P se scinde complètement.

DESCENTE

Supposons maintenant $Q \in \mathbb{F}_q[X]$, irreductible et de degré $2d$.

$$Q = \prod_{i=1}^{d} Q_i$$

où les Q_i sont des polynômes irreductibles de degré 2 dans $\mathbb{F}_{q^d}[X]$ et sont tous conjugués. On applique alors l'élimination "à la volée" avec Q_1 pour obtenir $\log Q_1$ en fonction de $O(q)$ $\log P_i$ où les $P_i \in \mathbb{F}_{q^d}[X]$ sont de degré 1.
La norme d'un polynôme linéaire dans $\mathbb{F}_{q^d}[X]$ est un polynôme irréductible de degré d_1 à la puissance d_2, avec $d_1 d_2 = d$. *On a ainsi exprimé* $\log Q$ *en fonction de* $O(q) \log R_i$, *où* $\deg R_i | d$