Anaël Marit ENS Rennes

ALGORITHME DE BERLEKAMP

- 122, 123, 141, 142, 148 –

—

Lorsque K est un corps, on utilise fréquemment le fait que l'anneau $K[X]$ est factoriel. Malheureusement, calculer la décomposition d'un polynôme en produit d'irréductibles est un problème généralement compliqué. Il se trouve que dans le cas où K est un corps fini, Berlekamp a découvert un algorithme qui permet de calculer cette décomposition pour n'importe quel polynôme (de façon plus intelligente que de simplement tester tous les diviseurs potentiels). Cet algorithme fournit au passage un test efficace d'irréductibilité qui ne nécessite que... le pivot de Gauss !

Dans ce développement, on va donner et étudier l'algorithme de Berlekamp pour des entrées sans facteurs carrés (c'est déjà bien assez long comme ça). En annexe, j'ai ajouté un moyen de traiter le cas général, et je pense qu'il est bon de le connaître pour l'oral, car c'est quand même une question qui se pose tout naturellement.

Tout le développement est extrait de [1].

Soit p un nombre premier et q une puissance de p. On désigne par $\mathbb{F}_q$ un corps à q-éléments. Etant donné $P \in \mathbb{F}_q[X]$, on notera $\langle P \rangle$ l'idéal de $\mathbb{F}_q[X]$ engendré par P. Lorsque Q est un autre polynôme, on notera $\overline{Q}^P$ le projeté de Q dans $\mathbb{F}_q[X]\Big/\langle P\rangle$. Notons qu'à chaque fois qu'on se donnera un élément $\overline{Q}^P \in \mathbb{F}_q[X]\Big/\langle P\rangle$, on fixera implicitement un représentant $Q \in \mathbb{F}_q[X]$.

Un peu de contexte

Dans cette première partie, on va poser un certain nombre de notations et préciser le cadre de travail qui va nous permettre d'étudier l'algorithme.

Soit $P \in \mathbb{F}_q[X]$ un polynôme, qu'on décompose en produit d'irréductibles :

$$P = \prod_{i=1}^{r} P_i^{\nu_i} \tag{1}$$

Le lemme chinois fournit un isomorphisme de $\mathbb{F}_q$-algèbres :

$$\begin{aligned} \Phi : \underbrace{\mathbb{F}_q[X]\Big/\langle P\rangle}_{=:\mathcal{A}} &\xrightarrow{\sim} \prod_{i=1}^{r} \underbrace{\mathbb{F}_q[X]\Big/\langle P_i^{\nu_i}\rangle}_{=:\mathcal{A}_i} \\ \overline{Q}^P &\mapsto \left(\overline{Q}^{P_i^{\nu_i}}\right)_{1\leqslant i\leqslant r} \end{aligned}$$

Remarquons à ce stade qu'une $\mathbb{F}_q$-algèbre est, par définition, un anneau A muni d'un morphisme d'anneaux dit «structural» $\mathfrak{s}_A : \mathbb{F}_q \hookrightarrow A$, injectif puisque $\mathbb{F}_q$ est un corps. Ceci permet d'identifier $\mathbb{F}_q$ à $\mathfrak{s}_A(\mathbb{F}_q)$, qui est un sous-corps de A, identification qui est très couramment faite

dans ce contexte. Le danger ici est que l'on manipule plusieurs $\mathbb{F}_q$-algèbres, et donc $\mathbb{F}_q$ serait assimilé à des parties de différentes algèbres qui n'ont a priori rien à voir entre elles ! Comme on va souvent tirer des éléments de $\mathfrak{s}_A(\mathbb{F}_q)$ dans $\mathbb{F}_q$ par le morphisme structural, de sorte à pouvoir les comparer avec d'autres éléments issus de l'image de $\mathbb{F}_q$ dans d'autres algèbres, on gardera toujours la trace des morphismes structuraux. Cela occasionnera une certaine lourdeur dans les notations, mais qui est justifiée par un gain de clareté non négligeable.

On remarque également que tout $\mathbb{F}_q$-algèbre peut être munie d'un endomorphisme de $\mathbb{F}_q$-algèbre défini par le passe à la puissance q. On notera Frob_q ce morphisme dans le cas de la $\mathbb{F}_q$-algèbre $\mathcal{A}$.

Dans toute la suite, on utilisera les notations introduites ici.

L'algorithme

Je propose de présenter l'algorithme sans plus de contexte, d'une seule traite, afin d'avoir chacune de ses étapes en tête. Tout ceci paraîtra obscure de prime abord, et c'est bien normal, car il est sacrément astucieux ! La suite du développement consistera à en prouver la correction et la terminaison.

Algorithme : Berlekamp
Entrée : $P \in \mathbb{F}_q[X]$ un polynôme sans facteurs carrés [(i)]
Sortie : La liste des facteurs irréductibles de P.

1. Calculer s la dimension du $\mathbb{F}_q$-espace vectoriel $\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}})$
2. Si $s = 1$, retourner P.
3. Sinon, prendre $\overline{V}^P \in \mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}}) \setminus \mathfrak{s}_{\mathcal{A}}(\mathbb{F}_q)$. Retourner :

$$\{\mathrm{Berlekamp}(pgcd(V-\alpha, P)),\ \alpha \in \mathbb{F}_q \mid pgcd(V-\alpha, P) \neq 1\} \tag{2}$$

Etude de l'algorithme

On va prouver d'un seul coup que l'algorithme est correcte est termine en étudiant chacune de ses trois étapes.

Lemme 1. *L'entier s est r le nombre de facteurs irréductibles de P.*

Démonstration. Soit $Q \in \mathbb{F}_q[X]$. On observe la suite d'équivalence suivante :

$$\left[\left(\overline{Q}^P\right)^q = \overline{Q}^P\right] \iff \left[\Phi\left(\overline{Q}^P\right)^q = \Phi\left(\overline{Q}^P\right)\right] \tag{3}$$

$$\iff \left[\forall i \in [\![1, r]\!],\ \left(\overline{Q}^{P_i}\right)^q = \overline{Q}^{P_i}\right] \tag{4}$$

$$\iff \left[\forall i \in [\![1, r]\!],\ \overline{Q}^{P_i} \in \mathfrak{s}_{\mathcal{A}_i}(\mathbb{F}_q)\right] \tag{5}$$

(i). C'est-à-dire que tous ses facteurs irréductibles dans $\mathbb{F}_q[X]$ sont présents avec multiplicité 1.

La dernière équivalence mérite explications. Comme les P_i sont irréductibles, les $\mathbb{F}_q$-algèbres $\mathcal{A}_i := \mathbb{F}_q[X]\Big/\langle P_i \rangle$ sont en réalité des extensions de corps de $\mathbb{F}_q$. $\mathfrak{s}_{\mathcal{A}_i}(\mathbb{F}_q)$ est exactement l'ensemble des points fixes du morphisme de Frobenius $x \mapsto x^q$ (ii), ce qui justifie cette dernière équivalence. Comme Φ est un isomorphisme de $\mathbb{F}_q$-algèbres, c'est en particulier un isomorphisme $\mathbb{F}_q$-linéaire. Il induit donc un isomorphisme entre $\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}})$ et $\Phi(\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}}))$ (ce qui est la traduction de la première équivalence), et les dernières équivalences montrent qu'on a l'isomorphisme de $\mathbb{F}_q$-espaces vectoriels :

$$\Phi(\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}})) = \prod_{i=1}^{r} \mathfrak{s}_{\mathcal{A}_i}(\mathbb{F}_q) \cong \mathbb{F}_q^r \tag{6}$$

D'où l'espace propre $\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}})$ est un $\mathbb{F}_q$-espace vectoriel de dimension r. □

Ainsi, l'étape 2 prend tout sons sens ! Si l'entier s calculé est 1, P a un unique facteur irréductible, donc P est lui-même irréductible. Etudions la troisième étape.

On suppose que la troisième étape est atteinte, c'est-à-dire que $r > 1$. En conséquence, $\mathrm{Ker}(\mathrm{Frob}_q - Id_{\mathcal{A}}) \setminus \mathfrak{s}_{\mathcal{A}}(\mathbb{F}_q)$ est un ensemble non-vide. Soit $\overline{V}^P$ l'un de ses éléments. On pose :

$$\forall i \in [\![1, r]\!],\ \alpha_i := \mathfrak{s}_{\mathcal{A}_i}^{-1}(\overline{V}^{P_i}) \in \mathbb{F}_q \text{ (iii)} \tag{7}$$

Lemme 2.

$$\prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(V - \alpha, P) = P \tag{8}$$

Démonstration. Considérons $i \in [\![1, r]\!]$, $\alpha \in \mathbb{F}_q$ et la suite d'équivalences :

$$\begin{aligned}
[P_i | V - \alpha] &\iff [V \equiv \alpha (mod P_i)] && (9)\\
&\iff \left[\overline{V}^{P_i} = \mathfrak{s}_{\mathcal{A}_i}(\alpha)\right] && (10)\\
&\iff [\alpha = \alpha_i] && (11)
\end{aligned}$$

Ainsi, on a l'égalité :

$$\begin{aligned}
\prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(V - \alpha, P) &= \prod_{\alpha \in \mathbb{F}_q} \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{r} P_i && (12)\\
&= \prod_{i=1}^{r} P_i && (13)\\
&= P && (14)
\end{aligned}$$

(ii). Tous les éléments de $\mathfrak{s}_{\mathcal{A}_i}(\mathbb{F}_q)$ sont de tels points fixes en vertu du théorème de Lagrange, et il ne peut y avoir plus de q tels points fixes puisqu'il s'agit des racines de $X^q - X$, qui est de degré q.

(iii). Par définition de $\overline{V}^P$, on a d'après le travail précédent que $\overline{V}^{p_i}$ est un élément de la copie de $\mathbb{F}_q$ dans $\mathcal{A}_i$. Comme on va vouloir comparer tous ces éléments, on les tire en arrière par le morphisme structural pour récupérer un élément de $\mathbb{F}_q$.

□

On est maintenant en passe de conclure ! Les facteurs $(\text{pgcd}(V-\alpha, P))$ sont soit 1, soit un produit des (P_i). Par ailleurs, pour tout i, P_i est facteur d'un et d'un seul terme de la forme $\text{pgcd}(V-\alpha, P)$. De plus, tous ces termes sont des diviseurs **stricts** de P, car :

$$\text{pgcd}(V-\alpha, P) = P \iff P | V-\alpha \implies \overline{V}^P \in \mathfrak{s}_{\mathcal{A}}(\mathbb{F}_q) \tag{15}$$

donc le choix de V exclue ce cas. En d'autre termes, le nombre de facteurs irréductible de $\text{pgcd}(V-\alpha, P)$ est inférieur strict à r, ce pour tout $\alpha \in \mathbb{F}_q$. Il suit immédiatement que l'algorithme termine, car à chaque appel récursif, le nombre de facteurs irréductibles du polynôme en entrée diminue strictement. L'algorithme est par ailleurs correct : on peut le prouver par récurrence sur r. Lorsque $r = 1$, l'algorithme s'arrête à l'étape 2 et renvoie la décomposition en irréductibles de P. Si on suppose que $r > 1$ et que l'algorithme est correct pour toute entrée ayant au plus $r-1$ facteurs irréductibles, alors par récurrence, l'algorithme renvoie la liste des facteurs irréductibles de tous les $(\text{pgcd}\, V-\alpha, P))$, qui à eux tous contiennent exactement les facteurs irréductibles de P. Ceci achève l'étude de l'algorithme de Berlekamp !

Références

[1] Vincent Beck, Jerôme Malick et Gabriel Peyré. *Objectif agrégation*. H&K, 2005. isbn : 2914010923.