Algorithme de Berlekamp

Leçons 123,141,142,151

Dans tout ce qui suit, $q = p^s$, avec p premier et s un entier naturel non nul et $\mathbb{F}_q$ est le corps à q éléments.

Théorème (Algorithme de Berlekamp)

Soit $P \in \mathbb{F}_q[X]$ dont la décomposition en polynômes irréductibles est sans facteur carré, i.e. on a $P = P_1 \cdots P_r$, où les P_i sont premiers entre eux deux à deux, irréductibles. Soit $x = \overline{X}^P \in \frac{\mathbb{F}_q[X]}{\langle P \rangle}$. L'algorithme suivant s'arrête au bout d'un nombre fini d'étapes et donne la décomposition en produit d'irréductibles de P.

1. On calcule la matrice de $S_P - Id$ dans la base $\left\{1, x, \cdots, x^{\deg(P)-1}\right\}$.
2. Le nombre de facteurs irréductibles est donné par $r = \dim\left(\ker(S_P - Id)\right) = \deg(P) = rg(S_P - Id)$. Si $r = 1$, P est irréductible et l'algorithme s'arrête. Sinon, on passe à l'étape suivante.
3. On calcule $V \in \mathbb{F}_q[X]$ tel que $\overline{V}^P = V \mod P$ ne soit pas un polynôme constante de $\mathbb{F}_q[X]$, avec $V \in \ker(S_P - Id)$. On a alors:

$$P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha) \tag{1}$$

calculé avec l'algorithme d'Euclide. On recommence à la première étape avec chacun des facteurs.

Remarque. *L'application S_P est donnée par:*

$$\begin{array}{rccc} S_P & \frac{\mathbb{F}_q[X]}{\langle P \rangle} & \longrightarrow & \frac{\mathbb{F}_q[X]}{\langle P \rangle} \\ & Q & \longmapsto & Q(X)^q = Q(X^q) \end{array}$$

Il s'agit de l'élévation à la puissance q d'un polynôme. Cette application est linéaire via e morphisme de Frobenius.

Voici le plan de la démonstration:

1. Montrer le second point en utilisant le lemme chinois:

$$\begin{array}{rccc} \varphi : & \frac{\mathbb{F}_q[X]}{\langle P \rangle} & \xrightarrow{\sim} & \mathbb{K}_1 \times \cdots \times \mathbb{K}_r \\ & \overline{Q}^P & \longmapsto & \left(\overline{Q}^{P_1}, \cdots, \overline{Q}^{P_r}\right) \end{array}$$

   avec $\mathbb{K}_i = \frac{\mathbb{F}_q[X]}{\langle P_i \rangle}$ qui est un corps, puisque les P_i sont irréductibles.

2. Justifier l'existence de V dans le troisième point, et montrer la formule (1).

Démonstration. *1. Soit $\widetilde{S_P} = \varphi \circ S_P \circ \varphi^{-1}$, donnée par:*

$$\begin{array}{rccc} \widetilde{S_P}: & \mathbb{K}_1 \times \cdots \times \mathbb{K}_r & \longrightarrow & \mathbb{K}_1 \times \cdots \times \mathbb{K}_r \\ & (Q_1, \cdots, Q_r) & \longmapsto & (Q_1^p, \cdots, Q_r^p) \end{array}$$

ce qui correspond à l'élévation à la puissance q composante par composante. On a:

$$\begin{array}{rcl} (x_1, \cdots, x_r) \in \ker\left(\widetilde{S_P} - Id\right) & \Leftrightarrow & (x_1^q, \cdots, x_r^q) = (x_1, \cdots, x_r) \\ & \Leftrightarrow & \forall i \in [\![1, n]\!], x_i^q = x_i \text{ dans } \mathbb{K}_i \end{array}$$

Or, $\mathbb{F}_q \hookrightarrow \mathbb{K}_i$ est une extension de corps, et, pour tout $x \in \mathbb{F}_q^\times$, $x^{q-1} = 1$, i.e. $x^q = x$ (par le théorème de Lagrange), $0^q = 0$ et tous les éléments de $\mathbb{F}_q$ sont racine de $X^q - X$. Il y en a q.

$$\text{Donc } \quad (x_1, \cdots, x_r) \in \ker\left(\widetilde{S_P} - Id\right) \Leftrightarrow (x_1, \cdots, x_r) \in \mathbb{F}_q^r$$

Or, si u est une application linéaire, φ est un isomorphisme d'espaces vectoriels (c'est le cas ici), alors on a:

$$\begin{array}{rcl} x \in \varphi\left(\ker(u)\right) & \Leftrightarrow & u\left(\varphi^{-1}(x)\right) = 0 \\ & \Leftrightarrow & \left(\varphi \circ u \circ \varphi^{-1}\right)(x) = 0 \\ & \Leftrightarrow & x \in \ker\left(\varphi \circ u \circ \varphi^{-1}\right) \end{array}$$

Donc $\ker(S_P - Id) = \varphi(\ker(\widetilde{S_P} - Id))$ est de dimension r.

2. On suppose que $r > 1$. $\left\{\overline{U}^P : \exists a \in \mathbb{F}_q : \overline{U}^P = a\right\} = Vect_{\mathbb{F}_q}\{1\}$ dans $\frac{\mathbb{F}_q[X]}{\langle P \rangle}$, et est de dimension 1. $\ker(S_P - Id)$ est de dimension $r > 1$, donc il existe $V \in \mathbb{F}_q[X]$ tel que $\overline{V}^P$ ne soit pas un polynôme constant et $\overline{V}^P \in \ker(S_P - Id)$.

Montrons l'égalité (1). On a:

$$\overline{V}^P \in \ker(S_P - Id) \overset{\varphi \text{ isomorphisme}}{\Leftrightarrow} \left(\overline{V}^{P_1}, \cdots, \overline{V}^{P_r}\right) \in \mathbb{F}_q^r$$

On pose, pour tout $i \in [\![1, r]\!]$, $\alpha_i = \overline{V}^{P_i}$. On a donc $\alpha_i \in \mathbb{F}_q \subset \mathbb{K}_i$. Soit $\alpha \in \mathbb{F}_q$. Montrons que:

$$pgcd(P, V - \alpha) = \prod_{\{i:\alpha_i = \alpha\}} P_i$$

Comme $pgcd(P, V - \alpha) | P$, on obtient alors:

$$pgcd(P, V-\alpha) = \prod_{i\in I_\alpha} P_i$$

avec $I_\alpha \subset [\![1,r]\!]$. Les P_i sont premiers entre eux deux à deux, donc, par le lemme de Gauss, on a $I_\alpha = \{i \in [\![1,r]\!] : P_i | V-\alpha\}$. Or, pour tout $i \in [\![1,r]\!]$,

$$\alpha_i = \alpha \Leftrightarrow \overline{V}^{P_i} = \alpha \Leftrightarrow P_i | V-\alpha$$

donc $I_\alpha = \{i \in [\![1,r]\!] : \alpha_i = \alpha\}$ et on a:

$$pgcd(P, V-\alpha) = \prod_{\{i:\alpha_i=\alpha\}} P_i$$

$$Donc \quad P = \prod_{i=1}^{r} P_i = \prod_{\alpha\in\mathbb{F}_q} \left(\prod_{\{i:\alpha_i=\alpha\}} P_i \right) = \prod_{\alpha\in\mathbb{F}_q} pgcd(P, V-\alpha)$$

et on réitère l'algorithme sur les $pgcd(P, V-\alpha)$.

Montrons que r diminue à chaque itération. Si $\overline{V}^P$ n'est pas un polynôme constant, alors les facteurs de (1) ont tous strictement moins de r facteurs irréductibles, puisque sinon il existerait $\alpha \in \mathbb{F}_q$ tel que $pgcd(P, V-\alpha) = P$, i.e. $P | V-\alpha$ et $\overline{V}^P = \alpha$, constant, ce qui est absurde. De plus, $pgcd(P, V-\alpha) | P$, donc est sans facteur carré.

■

Application (Un exemple tout bête)

$P = X^2 + X \in \mathbb{F}_2[X]$ admet pour décomposition en produit d'irréductibles le produit $P = X(X+1)$.

Remarque. *Cet exemple d'application est présent à titre d'illustration, en réalité, je ne pense pas que l'on applique l'algorithme de Berlekamp pour donner la décomposition en produit d'irréductibles de $X^2 + X$...*

Démonstration. *$P = X^2 + X \in \mathbb{F}_2[X]$, et $\deg(P) = 2$. De plus, on a $S_P(1) = 1$ et $S_P(X) = X^2 = X$ modulo P ($X^2 = X$ dans $\frac{\mathbb{F}_2[X]}{\langle P \rangle}$). Donc on a:*

$$Mat_{\{\overline{1},\overline{X}\}}(S_P - Id)$$

Cette matrice est de rang nul, donc P admet 2 facteurs irréductibles.

*X est non constant modulo P, et $X \in \ker(S_P - Id)$. Donc on calcule $pgcd(P, X)$ et $pgcd(P, X+1)$ ($-1 = 1$ dans $\mathbb{F}_2$). Une **division euclidienne** assure que $P = X^2 + X =$*

$X(X+1)$, *donc* $pgcd(P,X) = X$ *et* $pgcd(P,X+1) = X+1$.

On recommence avec les polynômes $P_1 = X$ *et* $P_2 = X+1$. $\deg(P_1) = \deg(P_2) = 1$, *et* $S_{P_1}(1) = S_{P_2}(1) = 1$, *donc on a:*

$$Mat_{\{\overline{1}\}}(S_{P_1} - Id) = Mat_{\{\overline{1}\}}(S_{P_2} - Id) = [0]$$

Cette matrice est de rang nul, donc P_1 *et* P_2 *ont* 1 *facteur irréductible, i.e. sont irréductibles, donnant ainsi la décomposition souhaitée.*

■

Reférence. *V.Beck, J.Malick, G.Peyré, Objectif Agrégation*