Algorithme de Berlekamp

V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, 2e édition, H&K. Théorème 5.36 page 245

Recasage : 121, 122, 123, 141

Algorithme : On considère un polynôme $P \in \mathbb{F}_q[X]$ sans facteur carré.

– On note S_P l'endomorphisme d'élévation à la puissance q dans l'anneau $\mathbb{F}_q[X]/(P)$. Calculer $r = \deg(P) - \mathrm{rg}(S_p - \mathrm{Id})$.

– Si $r > 1$
  ⋆ Calculer $V \in \mathbb{F}_q[X]$ tel que $V \bmod P$ n'est pas contant et $V \bmod P \in \mathrm{Ker}(S_P - \mathrm{Id})$.
  ⋆ Calculer $\mathrm{pgcd}(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$.
  ⋆ Appliquer l'algorithme aux $\mathrm{pgcd}(P, V - \alpha)$ non triviaux.

– Si $r = 1$, alors P est irréductible.

▷ Montrons qu'on obtient ainsi la décomposition en facteurs irréductibles de $P \in \mathbb{F}_q[X]$ sans facteur carré. Notons $P = P_1 \cdots P_r$ avec $P_1, \dots, P_r$ irréductibles deux à deux premiers entre eux.

– *Étape 1 : Calcul de r.* D'après le théorème chinois, on dispose d'un isomorphisme

$$\varphi : \mathbb{F}_q[X]/(P) \longrightarrow K_1 \times \cdots \times K_r$$

où $\forall i \in [\![1, r]\!]$, $K_i = \mathbb{F}_q[X]/(P_i)$ est un corps. Posons $\widetilde{S_P} = \varphi \circ S_P \circ \varphi^{-1}$. Alors

$$\widetilde{S_P}(x) = \varphi((\varphi^{-1}(x))^q) = \big(\varphi(\varphi^{-1}(x))\big)^q = x^q$$

et

$$\begin{aligned}(x_1, \dots, x_r) \in \mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) &\iff \forall i \in [\![1, r]\!],\ x_i^q = x_i \text{ dans } K_i \\ &\iff \forall i \in [\![1, r]\!],\ x_i \in \mathbb{F}_q \hookrightarrow K_i.\end{aligned}$$

En effet, les éléments de $\mathbb{F}_q \hookrightarrow K_i$ sont q racines du polynôme $X^q - X$ sur K_i. Comme K_i est un corps et $\deg(X^q - X) = q$, ce sont donc ses seules racines.

Ainsi, $\mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = \mathbb{F}_q^r$. Comme φ est un isomorphisme, $\mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = \varphi(\mathrm{Ker}(S_P - \mathrm{Id}))$ et

$$\dim \mathrm{Ker}(S_P - \mathrm{Id}) = \dim \mathrm{Ker}(\widetilde{S_P} - \mathrm{Id}) = r.$$

– *Étape 2 : Factorisation de P.* On suppose que $r > 1$. La droite vectorielle $\mathbb{F}_q \cdot 1$ de $\mathbb{F}_q[X]/(P)$ étant de dimension 1 et $\mathrm{Ker}(S_P - \mathrm{Id})$ étant de dimension $r > 1$, on peut trouver $V \in \mathbb{F}_q[X]$ tel que $(V \bmod P) \in \mathrm{Ker}(S_P - \mathrm{Id})$ et $(V \bmod P)$ n'est pas contant. Or

$$(V \bmod P) \in \mathrm{Ker}(S_P - \mathrm{Id}) \qquad \iff \qquad \forall i \in [\![1, r]\!],\ (V \bmod P_i) \in \mathbb{F}_q.$$

Notons alors $\alpha_i = (V \bmod P_i) \in \mathbb{F}_q$, $\forall i \in [\![1, r]\!]$.

Montrons que $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$. Comme $\mathrm{pgcd}(P, V - \alpha)$ divise P, on peut écrire $\mathrm{pgcd}(P, V - \alpha) = P_{i_1} \cdot P_{i_k}$ avec $i_1, \dots, i_k \in [\![1, r]\!]$. Or les polynômes $P_{i_1}, \dots, P_{i_k}$ sont deux à deux premiers entre eux donc ils divisent tous $V - \alpha$. Or

$$P_i | V - \alpha \qquad \iff V - \alpha = 0 \bmod P_i \qquad \iff \alpha = \alpha_i$$

donc $\mathrm{pgcd}(P, V - \alpha) = \prod_{\alpha_i = \alpha} P_i$. Alors,

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

– *Étape 3 : L'algorithme se termine.* À partir de cette décomposition de P, on applique l'algorithme aux $\mathrm{pgcd}(P, V - \alpha)$ distincts de 1. Montrons que le nombre de leurs facteurs irréductibles est strictement inférieur à r. Comme $V \bmod P$ n'est pas constant, il existe i, j tels que $\alpha_i \neq \alpha_j$. Alors $\mathrm{pgcd}(P, V - \alpha_i) = \prod_{\alpha_k = \alpha_i} P_k$ et $\mathrm{pgcd}(P, V - \alpha_j) = \prod_{\alpha_k = \alpha_j}$ sont distincts et ont donc strictement moins que r facteurs irréductibles. □