Algorithme de Berlekamp

L'algorithme de Berlekamp est le suivant.
— Calculer la matrice de $S_P - \mathrm{id}$, où $S_P : \overline{Q} \in \mathbb{F}_q[X]/(P) \mapsto \overline{Q}(X^q)$.
— Le nombre de facteurs irréductibles de P est $r = \dim \ker(S_P - \mathrm{id}) = \deg P - \mathrm{rg}(S_P - \mathrm{id})$.
— Si $r = 1$, alors P est irréductible. Sinon, choisir V non constant dans $\mathbb{F}_q[X]/(P)$ tel que $\overline{P} \in \ker(S_P - \mathrm{id})$, et alors :

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

Itérer ensuite l'algorithme sur chacun des termes de ce produit.

Théorème 1. Soit P dans $\mathbb{F}_q[X]$ dont la décomposition en polynômes irréductibles est sans facteur carré. Posons $x = \overline{X}$ dans $\mathbb{F}_q[X]/(P)$. Considérons $B = \{1, x, \dots, x^{\deg P - 1}\}$ base de $\mathbb{F}_q[X]/(P)$. L'algorithme ci-dessus termine en un nombre fini d'étapes.

Démonstration.

Lemme 2. Soient s entier et p premier tels que $q = p^s$. L'application S_P est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$.

Démonstration. Par propriété universelle, il existe un unique morphisme d'anneaux δ tel que $\delta_{|\mathbb{F}_q} = \mathrm{id}$ et $\delta(X) = X^q$, i.e. $\delta : Q \in \mathbb{F}_q[X] \mapsto Q(X^q)$. Puisque l'élévation à la puissance q est un morphisme, et que $a^q = a$ pour tout $a \in \mathbb{F}_q$,

$$\delta(Q) = Q(X^q) = \sum \alpha_k (X^q)^k = \left(\sum \alpha_k X^k\right)^q = Q^q.$$

Notons $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(P)$ la projection canonique et $\overline{\delta} = \pi \circ \delta$. Puisque π est un morphisme, $\overline{\delta}(P) = 0$, donc $\overline{\delta}$ passe au quotient, ce qui donne S_P. Enfin,

$$S_P(\overline{Q}) = S_P(\pi(Q)) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q = \overline{Q}^q.$$

□

Notons $P = P_1 \dots P_r$, où les P_i sont irréductibles et deux à deux premiers entre eux par hypothèse, et $K_i = F_q[X]/(P_i)$ les corps associés. Le théorème chinois donne l'isomorphisme φ entre $\mathbb{F}_q[X]/(P)$ et $K_1 \times \cdots \times K_r$. Notons $\tilde{S}_P = \varphi \circ S_P \circ \varphi^{-1}$, l'élévation à la puissance q dans $K_1 \times \cdots \times K_r$.

$$(x_1, \dots, x_r) \in \ker(\tilde{S}_P - \mathrm{id}) \iff \forall i \in \{1, \dots, r\},\ x_i^q = x_i.$$

Soit K une extension de corps de $\mathbb{F}_q$. L'image de $\mathbb{F}_q$ dans K est l'ensemble des éléments vérifiant $x^q = x$ (car ceux de $\mathbb{F}_q$ le vérifient et il y en a au plus q). Puisque K_i est une extension de $\mathbb{F}_q$, la condition ci-dessus se réécrit $\ker(\tilde{S}_P - \mathrm{id}) = \mathbb{F}_q^r$. Et puisque φ est un isomorphisme de $\mathbb{F}_q$-espace vectoriel et que $\ker(\tilde{S}_P - \mathrm{id}) = \varphi(\ker(S_P - \mathrm{id}))$, on obtient $\dim \ker(S_P - \mathrm{id}) = r$. Supposons $r > 1$. L'ensemble des constantes de $\mathbb{F}_q[X]/(P)$ étant engendré par $1 \pmod P$, il existe $V \in \mathbb{F}_q[X]$ tel que $\overline{V} \in \ker(S_P - \mathrm{id})$ avec $\overline{V}$ non constant dans $\mathbb{F}_q[X]/(P)$. Avec ce qui précède, on a en particulier que :

$$(\alpha_1, \dots, \alpha_r) := (V \mod P_1, \dots, V \mod P_r) \in \mathbb{F}_q^r.$$

De plus, pour $\alpha \in \mathbb{F}_q$, puisque par définition $\mathrm{pgcd}(V - \alpha, P) | P$,

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

Le lemme de Gauss assure que $I_\alpha = \{i \in \{1, \dots, r\},\ P_i | V - \alpha\}$, les P_i étant premiers entre eux. Or,

$$P_i | V - \alpha \iff V - \alpha = 0 \mod P_i \iff \alpha = \alpha_i,$$

donc on obtient la représentation suivante de P, en partitionnant $\{1, \dots, r\}$ par les I_α :

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

Puisque $\overline{V}$ est non constant, il existe i, j tels que $\alpha_i \neq \alpha_j$ (sans quoi, on aurait $P | V - \alpha$, i.e. $\overline{V}$ constant), donc il y a au moins deux facteurs non triviaux dans l'équation (1), ce qui fait diminuer r strictement. □