Algorithme de Berlekamp

Notions utilisées : Extensions de corps, PGCD, arithmétique de polynômes

Motivations

Donner une méthode effective (algo) pour trouver la décomposition en facteurs irréductibles de polynômes (d'une certaine classe de polynômes) à coefficients dans un corps fini.

Lemme 1. *Pour tout $P \in \mathbb{F}_q[X]$, l'application* $S_P : \begin{pmatrix} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q(X) mod P & \mapsto & Q(X^q) mod P \end{pmatrix}$ *coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$.*

Théorème 2. *Soit P un polynôme dont la décomposition en facteurs irréductibles $P_1 \dots P_r$ ne contient aucun facteur carré. On note x l'image de X par la projection canonique sur $\mathbb{F}_q[X]/(P)$ et on note $\mathcal{B} = (1, x, \dots, x^{\deg(P)-1})$ la base canonique de $\mathbb{F}_q[X]/(P)$. Alors l'algorithme suivant permet d'obtenir explicitement ces facteurs irréductibles :*

1. *On calcule la matrice de $S_P - id$ dans la base $\mathcal{B}$*
2. *Si le nombre $r = dim(Ker(S_p - id))$ de facteurs irréductibles de P vaut 1, on arrête l'algorithme. Sinon, on passe à l'étape suivante :*
3. *On calcule un $V \in Ker(S_p - id)$ tel que $V mod P$ ne soit pas constant. On applique l'algorithme d'Euclide afin de déterminer $pgcd(P, V - a)$ pour tout $a \in \mathbb{F}_q$. On a alors*

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

4. *On applique l'étape 1 à chaque facteur (non trivial) $pgcd(P, V - a)$.*

Se démontre par propriété universelle.

Preuve. **Etape 1** : Montrer que $r = dim(Ker(S_P - id) = dim(\varphi(Ker(S_P - id))$ en utilisant φ. On décrit le noyau de l'application $\psi := \varphi \circ (S_P - id) \circ \varphi$:

$$(x_1, \dots, x_n) \in Ker(\psi) \iff \forall i, x_i^q = x_i \in \mathbb{F}_q[X]/(P_i)$$

Lemme 3. *Si K est une extension de corps de $\mathbb{F}_q$ alors $\{x \in K, x^q = x\} = \mathbb{F}_q$.*

Peuve du lemme. Le polynôme $X^q - X \in K[X]$ est un polynôme à au plus q racines et est non nul (car $q \neq 1$). Or 0 est racine, et tous les éléments de $\mathbb{F}_q^\times$ sont d'ordre q dans ce groupe multiplicatif donc sont aussi racine de ce polynôme. Ainsi, il ne peut pas y avoir de $y \in K \setminus \mathbb{F}_q$ racine de $X^q - X$ sans quoi celui-ci serait nul. □

Ce lemme permet de montrer que $Ker(\psi) = (\mathbb{F}_q)^r$. On a donc $dim_{\mathbb{F}_q}(Ker(\psi) = r = dim(Ker(S_P - id)$ car φ est un isomorphisme.
Etape 2 : Supposons $r > 1$. But : trouver un bon V et montrer $P = \prod_{a \in \mathbb{F}_q} pgcd(P, V - a)$.
Montrons tout d'abord que l'on peut trouver un tel V. On remarque que l'ensemble $U \in \mathbb{F}_q[X]/(P)$ congrus

à un polynôme constant est la droite engendrée par 1 dans $\mathbb{F}_q[X]/(P)$. Or on a supposé $dim(Ker(S_P - id) = r > 1$ donc il existe $V \in \mathbb{F}_q[X]/(P)$ non constant tel que $V(X^q) = V(X) = V(X)^q$. Par le lemme montré à la première étape, on remarque que $\varphi(VmodP) \in Ker(\psi) = (\mathbb{F}_q)^r$ et donc $\forall i \in [\![1, r]\!], VmodP_i \in \mathbb{F}_q$. Notons $a_i := VmodP_i \in \mathbb{F}_q$.
Soit $a \in \mathbb{F}_q$. Montrons que $pgcd(P, V - a) = \prod_{i, a_i = a} P_i$.
On traduit tout d'abord le fait que $pgcd(P, V - a)$ divise P : il existe un $I_a \subset [\![1, r]\!]$ tel que

$$pgcd(P, V - a) = \prod_{i \in I_a} P_i.$$

En particulier, $\forall i \in I_a, P_i | V - a$. Réciproquement, si on a un indice i tel que P_i divise $V - a$, puisque P_i divise aussi P on a $P_i | pgcd(P, V - a)$ par maximalité du pgcd en tant que diviseur de P et de $V - a$. Ainsi, $I_a = \{i, P_i | V - a\}$.
Or pour $i \in [\![1, r]\!]$, par définition de a_i,

$$a_i = a \iff VmodP_i = a \iff V - a = 0 \text{ dans } \mathbb{F}_q[X]/(P_i) \iff P_i | V - a.$$

On en déduit que $pgcd(P, V - a) = \prod_{i, a_i = a} P_i$. Ainsi, en partitionnant $[\![1, r]\!]$ en $\bigcup_{a \in \mathbb{F}_q} I_a$ il vient

$$P = \prod_{a \in \mathbb{F}_q} \prod_{i \in I_a} pgcd(P, V - a) = \prod_{a \in \mathbb{F}_q} pgcd(P, V - a).$$

Etape 3 : Prouver la terminaison de l'algorithme en montrant que r diminue strictement à chaque étape. Le choix du polynôme $V \in Ker(S_p - id)$ tel que $VmodP$ ne soit pas constant assure qu'il y a au moins deux indices i et j tels que $a_i = VmodP_i \neq VmodP_j = a_j$. En effet, s'ils étaient tous égaux on aurait $V = a_1$ dans tous les $\mathbb{F}_q[X]/(P_i)$ et donc dans $\mathbb{F}_q[X]/(P)$, ce qui contredirait l'hypothèse de non-constance. Autrement dit, on a au moins deux facteurs non triviaux dans le produit, qui ont chacun strictement moins que r facteurs irréductibles. (Garde-fou : ces facteurs sur lequel on répète l'algo sont aussi bien sûr sans facteur carré...) □