L'Algorithme de Berlekamp

Soit $q = p^n$, $\mathbb{K} = \mathbb{F}_q$, P un polynôme dans $\mathbb{K}[X]$.

I. Ecrire P comme un produit de polynômes sans facteur multiple

Si $P \wedge P' \neq P$, alors $P = \frac{P}{P \wedge P'} P \wedge P'$ permet une itération récursive de l'algorithme. Si $P \wedge P' = P$, alors $P \mid P'$ donc $P' = 0$ donc P n'a que des monômes du type X^{pi} donc il existe $Q \in \mathbb{K}[X]$ tel que $P = Q(X^p)$. On écrit $Q = \sum_i a_i X^i$. Si $b_i = a_i^{p^{n-1}}$, alors $b_i^p = a_i^{p^n} = a_i$ ce qui permet d'écrire $P = \left(\sum_i b_i X^i\right)^p$. Donc P est une puissance d'un polynôme de degré plus petit. Itérer : ce processus se terminera un jour car le degré des composantes a baissé strictement.

II. Les acteurs de l'algorithme

P peut donc être supposé à facteurs simples. On pose $A = \mathbb{K}[X]/(P)$ qui est une $\mathbb{K}$-algèbre. L'application $f : \mathbb{K}[X] \to \mathbb{K}[X]$ qui à Q associe Q^q est un morphisme de $\mathbb{K}$-algèbres (pourquoi ?) et passe au quotient (pourquoi ?) en un endomorphisme de la $\mathbb{K}$-algèbre A.

Si $P = P_1 \dots P_r$ est sa décomposition en facteurs irréductibles, alors, par le théorème des restes chinois, il existe un isomorphisme d'anneaux $A \simeq \prod_{i=1}^{r} \mathbb{K}[X]/(P_i)$. Soit $Q \in A$. Alors $Q \in \mathrm{Ker}(f - \mathrm{id}_A)$ équivaut à dire que $Q^q = Q$ ce qui revient à dire que pour tout i, $[Q]^q_{(P_i)} = [Q]_{(P_i)}$ (pourquoi ?). Si i est fixé, on remarque que $\mathbb{K}[X]/(P_i)$ est un corps qui est $\mathbb{K}$-espace vectoriel de dimension finie. C'est donc un corps fini contenant $\mathbb{K}$, et les éléments de $\mathbb{K}$ sont caractérisés par la relation $x^q = x$. On a donc un diagramme commutatif d'applications $\mathbb{K}$-linéaires :

$$\begin{array}{ccc} A = \mathbb{K}[X]/(P) & \xrightarrow{\simeq} & \mathbb{K}[X]/(P_1) \times \cdots \times \mathbb{K}[X]/(P_r) \\ \uparrow & & \uparrow \\ \mathrm{Ker}(f - \mathrm{id}_A) & \xrightarrow{\alpha, \simeq} & \mathbb{K} \times \cdots \times \mathbb{K} \end{array}$$

où l'inclusion de droite est simplement la concaténation des inclusions canoniques $\mathbb{K} \hookrightarrow \mathbb{K}[X]/(P_i)$. pour i entre 1 et r. L'isomorphisme du bas est noté α et est donc la forme coordonnée des éléments de $\mathrm{Ker}(f - \mathrm{id}_A)$. Plus précisément, si $Q \in \mathrm{Ker}(f - \mathrm{id}_A)$, alors en notant $\alpha(Q) = (\alpha_1, \dots, \alpha_r)$, on a, pour tout i, $\boxed{Q \equiv \alpha_i [P_i]}$.

III. L'Algorithme de Berlekamp

Prendre une base $Q_1, \dots, Q_r$ de $\mathrm{Ker}(f - \mathrm{id}_A)$. L'idée est de partir de la décomposition triviale $P = P$ et de la raffiner à chaque étape. Les étapes peuvent paraître obscures mais la section suivante montrera que la liste L vérifiera en permanence $\prod_{F \in L} F = P$ (invariant de boucle), et qu'à a fin la liste L ne contiendra plus que des facteurs irréductibles de P.

1. poser la liste $L = [P]$
2. for Q_i dans la base :
3. poser $L' = [\cdot]$ la liste vide
4. for F dans L :

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr

5. for α dans $\mathbb{F}_q$:
6. calculer $F \wedge (Q_i - \alpha)$ et le mettre dans L'.
7. L prend la valeur de L'
8. renvoyer L

On voit que les lignes 4. à 6. font faire q fois des calculs de $F \wedge (Q_i - \alpha)$ pour une liste de F dont le produit vaut P. Comme $F \wedge (Q_i - \alpha)$ coûte $O(\deg(F)\deg(Q_i))$, ces lignes coûtent (en sommant) : $O(\deg(P)\deg(Q_i))$ soit $O\big(\deg(P)^2\big)$ soit $O\big(q\deg(P)^2\big)$ en comptant pour chaque α. Total : $O\big(q\deg(P)^3\big)$.

Le but de la partie suivante est de prouver que l'algorithme renverra bien la décomposition de P.

IV. Principe et correction de l'algorithme

Ce lemme est facultatif car on sera dans un cadre factoriel, et je vous conseille même de simplement dire que c'est vrai à l'oral sans le montrer. Je vous le mets en option, notamment si vous voulez encore plus insister sur la beauté des pgcd dans la leçon sur les pgcd. Attention, la preuve dans le cas factoriel est plus facile (il suffit de factoriser et de bien regrouper les facteurs).

Lemme IV.0.1.

Dans un anneau à pgcd, le ppcm d'une famille finie d'objets premiers entre eux deux à deux est leur produit.

Preuve. Soit a, b, c tels que $b \wedge c = 1$. Prouvons que $(a \wedge b)(a \wedge c) = a \wedge bc$.

Il faut calculer à l'aide des propriétés de calcul dans un anneau à pgcd (voir le Rombaldi) qui sont l'homogénéité ($c(a \wedge b) = (ca \wedge cb)$), l'associativité et la commutativité :

$$\begin{aligned}(a \wedge b)(a \wedge c) &= ((a \wedge b)a) \wedge ((a \wedge b)c) = \big(a^2 \wedge ba\big) \wedge (ac \wedge bc) \\ &= a^2 \wedge bc \wedge (ba \wedge ac) = a^2 \wedge bc \wedge (a(b \wedge c)) = a^2 \wedge bc \wedge a = (a^2 \wedge a) \wedge bc = a \wedge bc.\end{aligned}$$

□

Théorème IV.0.2.

Si $Q \in \mathrm{Ker}(f - \mathrm{id}_A)$, alors pour tout L divisant P, on a $L = \prod_{a \in \mathbb{K}} L \wedge (Q - a)$.

Preuve. Soit i tel que P_i divise L. Alors $Q \equiv \alpha(Q)_i [P_i]$ donc $P_i \mid Q - \alpha(Q)_i$ donc il existe bien $a \in \mathbb{K}$ tel que $P_i \mid L \wedge (Q - a)$ donc $P_i \mid \prod_{a \in \mathbb{K}} L \wedge (Q - a)$, ce dernier objet est donc un multiple commun des P_i. Les P_i sont irréductibles et différents donc deux à deux premiers entre eux donc leur ppcm est leur produit (pourquoi ? c'est facile dans un anneau factoriel, et pas très dur dans un anneau à pgcd !). Or, L est à facteurs simples donc $L = P_1 \dots P_r$ d'où $L \mid \prod_{a \in \mathbb{K}} L \wedge (Q - a)$. On utilise le lemme précédent pour obtenir que $L \mid \prod_{a \in \mathbb{K}} L \wedge (Q - a) = L \wedge \prod_{a \in \mathbb{K}} (Q - a) \mid L$ donc ces objets sont donc (à inversible près) égaux. □

Pour prouver que l'algorithme est correct, on prouve qu'il sépare correctement tous les facteurs irréductibles P_i. Le théorème suivant prouve qu'il existe un k tel que l'élément Q_k de la base séparera toujours P_i et P_j, quel que soit le facteur L qui les contient actuellement.

Théorème IV.0.3.

Soit $Q_1, \dots, Q_r$ une base quelconque de $\mathrm{Ker}(f - \mathrm{id}_A)$. Si $i \neq j$, alors il existe k entre 1 et r tel que pour tout L tel que $P_i P_j \mid L \mid P$, le produit $L = \prod_{a \in \mathbb{K}} L \wedge (Q_k - a)$ soit une décomposition de L séparant P_i et P_j (i.e., P_i et P_j divisent chacun un facteur différent de ce produit).

Preuve. L'application α est un isomorphisme, donc $\alpha(Q_1), \dots, \alpha(Q_r)$ est une base de $\mathbb{K}^r$. Il existe donc un Q_k tel que $\alpha(Q_k) = (\alpha_1, \dots, \alpha_r)$ ait des coordonnées différentes en i et en j (sinon cette base

vit dans un hyperplan). Donc $Q_k = \alpha_i[P_i]$ et $Q_k = \alpha_j[P_j]$. Donc $P_i \mid Q_k - \alpha_i$ et $P_j \mid Q_k - \alpha_j$ donc P_i est dans le facteur $(Q_k - \alpha_i) \wedge L$ tandis que P_j est dans le facteur $(Q_k - \alpha_j) \wedge L$.

□