Algorithme de Berlekamp

Nico

Prérequis : Aisance avec les corps finis, morphisme de Frobenius d'un anneau, Théorème de Bézout et lemme Chinois dans un anneau principal

Notations :

1. $q = p^n$ où $n \in \mathbb{N}^*$ et p est un nombre premier. $\mathbb{F}_q$ le corps à q éléments.
2. Étant donné A un anneau commutatif de caractéristique p, $Fr : A \to A$, $x \mapsto x^p$ désigne le morphisme de Frobenius. Il s'agit d'un automorphisme si A est un corps fini.
3. Pour un polynôme $P \in \mathbb{F}_q[X]$ de degré $N \geq 1$ à facteurs simples, on lui associe pour tout $0 \leq j \leq N-1$ le reste de la division euclidienne de X^{qj} par P, noté $\sum_{i=0}^{N-1} b_{ij} X^i$. On note $B = (b_{ij})_{0 \leq i,j \leq N-1} \in M_n(\mathbb{F}_q)$ la matrice formée des coefficients de ces restes.

Objectif : Déterminer la factorisation en produit d'irréductibles d'un polynôme de $\mathbb{F}_q[X]$ non constant [(1)].

Premier algorithme naïf : Etant donné un polynôme P de degré $N \geq 1$, on divise P par tous les polynômes de degré 1, puis 2,..., jusqu'à $N-1$. $\mathbb{F}_q[X]$ étant fini, l'algorithme se termine, et on est certain que le premier diviseur trouvé est irréductible. Mais un tel algorithme est très (trop) coûteux. On cherche alors un algorithme plus performant. On propose ici d'étudier l'algorithme de Berlekamp.

On considère $P \in \mathbb{F}_q[X]$ unitaire de degré $N \geq 1$. On suppose dans un premier temps que P est à facteurs simples. On justifiera ensuite pourquoi on peut toujours se ramener à l'étude d'un polynôme à facteurs simples.

(1). Une telle factorisation est unique car $\mathbb{F}_q[X]$ est factoriel

Théorème :

i) Soit $H = \sum_{i=0}^{N-1} h_i X^i \in \mathbb{F}_q[X]$. Alors P divise $H^q - H$ si, et seulement si

$$(B - I_N) \begin{pmatrix} h_0 \\ \vdots \\ h_{N-1} \end{pmatrix} = 0$$

Autrement dit, le vecteur colonne des coefficients h_i est dans le noyau de $B - I_N$.

ii) Soit $H \in \mathbb{F}_q[X]$ tel que P divise $H^q - H$, alors $P = \prod_{\lambda \in \mathbb{F}_q} \text{pgcd}(P, H - \lambda)$

iii) Le nombre de facteurs irréductibles de P est $N - \text{rg}(B - I_N)$ [a]

a. valide que dans le cas de P à facteurs simples.

Décription de l'algorithme : Si $B - I_N$ est de rang $N - 1$, alors P est irréductible. Sinon, on choisit un polynôme H non constant tel que P divise $H^q - H$ grâce au calcul de $\text{Ker}(B - I_N)$. Le point ii) nous donne une factorisation de P en facteurs non tous triviaux [(2)] de degrés strictement inférieurs à N. En réitérant l'algorithme sur les facteurs trouvés, on finit par obtenir une décomposition en irréductible de P.

Avant de montrer les trois points, on montre en préliminaire que l'on peut toujours se ramener à l'étude d'un polynôme à facteurs simples.

Lemmes :

1. Si $A = \mathbb{F}_q$, alors $Fr^n = \text{Id}$
2. Si $A = \mathbb{F}_q[X]$, alors Fr est injectif, d'image $\mathbb{F}_q[X^p]$. En conséquence, si $Q \in \mathbb{F}_q[X^p]$, il existe un unique $P \in \mathbb{F}_q[X]$ tel que $Q = P(X)^p$.
3. Si $P \in \mathbb{F}_q[X] \backslash \mathbb{F}_q[X^p]$, alors il existe $R \in \mathbb{F}_q[X^p]$ et $Q \in \mathbb{F}_q[X]$ à facteurs simples tel que $P = \text{pgcd}(P, P')RQ$.

Ainsi, si $P \in \mathbb{F}_q[X^p]$, on réitère le deuxième point jusqu'à à avoir un polynôme $Q = P(X)^{p^k}$, de sorte à ce que $Q \notin \mathbb{F}_q[X^p]$. Le point un nous donne une condition d'arrêt à $k = n$. Ensuite, on est sûr d'avoir un polynôme $P \notin \mathbb{F}_q[X^p]$. On obtient alors un polynôme R à facteurs simples tels que $P = \text{pgcd}(P, P')R$. On recommence

(2). sinon P serait constant

avec $\text{pgcd}(P, P')$ jusqu'à n'avoir que des facteurs simples. A la fin, $P = R_1^{p^{k_1}} \dots R_s^{p^{k_s}}$ où $0 \leq k_i \leq n$, $s \leq N$, et les R_i sont à facteurs simples. On applique ainsi l'algorithme ci-dessus aux R_i.

Prouvons que les lemmes sont vrais :

Démonstration.

1. On considère le morphisme de Frobenius sur $\mathbb{F}_q$. Soit $x \in \mathbb{F}_q$, $Fr^n(x) = (\dots(x^p)^p \dots)^p = x^{p^n} = x^q = x$. D'où $Fr^n = \text{Id}$.

2. On considère le morphisme de Frobenius sur $\mathbb{F}_q[X]$. Soit $P \in \text{Ker}(Fr)$. Notons $P = \sum_{i=0}^{N} a_i X^i$. Alors $Fr(P) = 0_{\mathbb{F}_q[X]}$. En identifiant les coefficients, il vient que $a_0^p = \dots = a_N^p = 0_{\mathbb{F}_q}$. D'où $a_0 = \dots = a_N = 0$. D'où $P = 0$. D'où Fr est injectif.

   Il est clair que $Fr(\mathbb{F}_q[X]) \subseteq \mathbb{F}_q[X^p]$ par propriété de morphisme de Frobenius sur $\mathbb{F}_q$. Montrons l'inclusion réciproque. Soit $Q = \sum_{i=0}^{N} b_i X^{pi} \in \mathbb{F}_q[X^p]$. Par surjectivité du morphisme de Frobenius sur $\mathbb{F}_q$, il existe $(a_0, \dots, a_N) \in \mathbb{F}_q^{N+1}$ tels que $a_i^p = b_i \ \forall i$. D'où $Fr(\sum_{i}^{N} a_i X^i) = Q$. D'où l'égalité souhaitée.

   Il vient que Fr réalise une bijection de $\mathbb{F}_q[X]$ dans $\mathbb{F}_q[X^p]$. D'où pour tout $Q \in \mathbb{F}_q[X^p]$, il existe un unique $P \in \mathbb{F}_q[X]$ tel que $Q = P(X)^p$.

3. Notons $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ sa décomposition en facteurs d'irréductibles. Alors :

$$P' = \sum_{i=1}^{r} \alpha_i P_i^{\alpha_i - 1} P_i' \prod_{j \neq i} P_j^{\alpha_i}$$

   Soit $1 \leq i \leq r$

   (a) Si $p \nmid \alpha_i$, $P_i^{\alpha_i - 1} \mid P'$ et $P_i^{\alpha_i} \nmid P'$. Donc $P_i^{\alpha_i - 1} \mid \text{pgcd}(P, P')$.

   (b) Si $p \mid \alpha_i$, $\alpha_i = 0$ dans $\mathbb{F}_q$, donc $P_i \nmid \alpha_i$.

   D'où $\text{pgcd}(P, P') = \prod_{\substack{1 \leq i \leq r \\ p \nmid \alpha_i}} P_i^{\alpha_i - 1}$. Soit $R = \prod_{p \mid \alpha_i} P_i^{\alpha_i}$. On a que $R \in \mathbb{F}_q[X^p]$,

   Finalement, $Q = \dfrac{P}{R \,\text{pgcd}(P, P')}$ convient.

□

On peut maintenant supposer, sans perdre en généralité, que $P \in \mathbb{F}_q[X]$ est à facteurs simples. Notons $N \geq 1$ son degré. Montrons le théorème. On commence par le premier point. **Début de la preuve de Berlekamp :**

Démonstration. Soit $H = \sum_{i=0}^{N-1} h_i X^i$.
Notons $A = \mathbb{F}_q[X]/(P)$. Il s'agit d'une F_q-Algèbre de dimension N [3].
On considère $\mathcal{B} = (1, \overline{X}, \dots, \overline{X}^{N-1})$ une base du $\mathbb{F}_q$-espace vectoriel A. On prend le morphisme de Frobenius Fr sur A.

Notons $\psi = Fr^n$. Par le premier lemme, ψ est $\mathbb{F}_q$-linéaire. Donc il vient que pour tout $x, y \in A$, pour tout $\lambda \in \mathbb{F}_q$, $\psi(\lambda x) = \lambda\psi(x)$ et $\psi(x+y) = \psi(x) + \psi(y)$. D'où $\psi \in \mathcal{L}(A)$. Pour tout $j \in [\![0, N-1]\!]$, $\psi(\overline{X}^j) = \overline{X}^{qj} = \sum_{i=0}^{N-1} b_{ij}\overline{X}^i$. D'où la matrice de ψ dans $\mathcal{B}$ est la matrice B introduite dans les notations.

Si l'on note π la projection canonique de $\mathbb{F}_q[X]$ dans A, on obtient que :

$P \mid H^q - H$ si, et seulement si $\pi(H^q - H) = 0$. D'où :

$$P \mid H^q - H \iff \pi(H)^q = \pi(H) \iff \psi(\pi(H)) = \pi(H) \iff (\psi - \mathrm{Id})(\pi(H)) = 0$$

Or $\pi(H) = \sum_{i=0}^{N-1} h_i \overline{X}^i$ car H est de degré strictement inférieur à P. D'où matriciellement, si l'on note $h = \begin{pmatrix} h_0 \\ \vdots \\ h_{N-1} \end{pmatrix}$, on obtient l'équivalence souhaitée :

$$P \mid H^q - H \iff \sum_{i=0}^{N-1} h_i(\psi - \mathrm{Id})(\overline{X}^i) = 0 \iff (B - I_N)h = 0$$

□

Montrons le deuxième point.

Démonstration. Soit $H \in \mathbb{F}_q[X]$.

Pour tout $\lambda \neq \mu \in \mathbb{F}_q$, $\frac{1}{\lambda - \mu}(H + \lambda - (H + \mu)) = 1$. D'où par Bézout, $H - \lambda$ et $H - \mu$ sont premier entre eux. Or on sait que :

$$\prod_{\lambda \in \mathbb{F}_q} X - \lambda = X^q - X$$

D'où en évaluant en H :

$$\prod_{\lambda \in \mathbb{F}_q} H - \lambda = H^q - H$$

[3]. comme $\mathbb{F}_q$-espace vectoriel

Or $P \mid H^q - H$, donc

$$P = \operatorname{pgcd}(P, H^q - H) = \operatorname{pgcd}(P, \prod_{\lambda \in \mathbb{F}_q} H - \lambda) = \prod_{\lambda \in \mathbb{F}_q} \operatorname{pgcd}(P, H - \lambda)$$

car si $U \wedge V = 1$, alors $\operatorname{pgcd}(Q, U) \operatorname{pgcd}(Q, V) = \operatorname{pgcd}(Q, UV)$ pour tout Q [4]. □

Terminons avec le dernier point.

Démonstration. Notons $P = P_1 \dots P_r$ la décomposition en facteurs irréductibles de P. Puisque P est à facteurs simples, les P_i sont deux à deux premiers entre eux. Montrons que $r = N - \operatorname{rg}(B - I_n)$.

Le théorème des restes chinois nous donne que :

$$A = \mathbb{F}_q[X]/(P) \simeq \mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_r) =: \mathbb{K}_1 \times \cdots \times \mathbb{K}_r$$

Où tous les $\mathbb{K}_i$ sont des corps finis par irréductiblités des P_i, extensions de $\mathbb{F}_q$

Notons $E = \operatorname{Ker}(B - I_N)$, et pour chaque $\mathbb{K}_i$ on note E_i le sous espace $\{x \in \mathbb{K}_i : x^q = x\}$. Or puisque $\mathbb{K}_i$ est une extension de $\mathbb{F}_q$, il existe $n_i \in \mathbb{N}^*$ tel que $\mathbb{K}_i = \mathbb{F}_{q^{n_i}}$. Dans ce corps, $X^q - X$ possède exactement q racines, et ce sont exactement les éléments de $\mathbb{F}_q$. Donc $E_i = \mathbb{F}_q$, qui est donc de dimension 1. Par suite, $E_1 \times \cdots \times E_r = \mathbb{F}_q^r$ est de dimensions r.

Or $h \in E \iff P \mid H^q - H \iff \forall i \in [\![1, r]\!],\ P_i \mid H^q - H \iff \forall i \in [\![1, r]\!],\ h \in E_i$. D'où $\dim E = \dim \mathbb{F}_q^r = r$. D'où par le théorème du rang, $r = N - \operatorname{rg}(B - I_N)$ □

Question 1. *Expliquer l'algorithme de Berlekamp. Comparer sa complexité avec un algorithme "naïf".*

Question 2. *Justifier que Fr sur $\mathbb{F}_q$ est surjectif.*

Question 3. *Expliquer pourquoi on doit dissocier les cas $P \in \mathbb{F}_q[X^p]$ et $P \notin \mathbb{F}_q[X^p]$ pour écrire sa factorisation en facteurs simples.*

Question 4. *Déterminer une manière de trouver tous les polynômes irréductibles de $\mathbb{F}_q[X]$ de degré fixe.*

Question 5. *Justifier que $\mathbb{F}_q[X]$ est un anneau principal.*

Question 6. *Appliquer Berlekamp à $X^4 + 1 \in \mathbb{F}_p[X]$, $p \geq 3$.*

Question 7. *Que dire de la preuve de Berlekamp en terme de réduction ?*

[4]. $A \mid UV \implies A \mid U$ ou $A \mid V$. D'où $\operatorname{pgcd}(Q, UV) \mid \operatorname{pgcd}(Q, U) \operatorname{pgcd}(Q, V)$

Référence

Odile Fleury Loic Foissy, Alain Ninet (2023). *Algèbre et calcul formel*. 2eme edition. ellipses, p. 212.

Recasages

Leçon 122 : Anneaux principaux. Exemples et applications.

Leçon 123 : Corps finis. Applications.

Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Leçon 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.