Algorithme de Berlekamp

Leçons concernées

* **122 :** Anneaux principaux. Applications.
* **123 :** Corps finis. Applications.
* **141 :** Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
* **142 :** PGCD et PPCM, algorithmes de calcul. Applications.
* **151 :** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Réference

* *Beck - Objectif Agrégation*

Soit $\mathbb{F}_q$ un corps fini, et soit $P \in \mathbb{F}_q[X]$.
Le but de ce développement consiste à trouver un algorithme nous permettant de trouver la décomposition en produit de facteurs irréductibles de P. En fait, dans ce développement, nous allons plutôt étudier le cas où $P = \prod_{k=1}^{r} P_k$ est sans facteur carré. L'algorithme de Berlekamp permet alors de trouver cette décomposition.

Théorème. *Il existe un polynôme $V \in \mathbb{F}_q[X]$ tel que $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha)$, et cette décomposition est non triviale.*

En d'autres termes, si on trouve ce polynôme V, il existe un $\alpha \in \mathbb{F}_q$ tel que $pgcd(P, V - \alpha)$ (calculable par l'algorithme d'Euclide) soit un facteur non trivial de P.

Démonstration. Le point clé de l'algorithme est de s'intéresser au morphisme :

$$\varphi \quad : \quad \begin{array}{ccc} \dfrac{\mathbb{F}_q[X]}{(P)} & \longrightarrow & \dfrac{\mathbb{F}_q[X]}{(P)} \\ \overline{Q} & \longmapsto & \overline{Q(X^q)} \end{array}$$

Naturellement, rien ne nous dit que cette application est bien définie. Nous allons montrer cela. Soit, pour $Q \in \mathbb{F}_q[X]$, $\overline{\varphi}(Q) = Q(X^q)\ mod\ (P)$. Cette application est un morphisme d'anneau qui vérifie $\overline{\varphi}(Q) = Q(X)^q\ mod\ (P)$ puisque la caractéristique du corps divise q, et que tous les éléments x de $\mathbb{F}_q$ vérifient $x^q = x$. En particulier, $\overline{\varphi}(P) = 0$. Elle passe donc au quotient, ce qui signifie que le morphisme d'anneau φ est bien définie, et coïncide en plus avec l'élévation à la puissance q.

L'idée, maintenant, de l'algorithme, est de s'intéresser aux éléments propres de φ, et plus particulièrement à l'espace propre associé à 1. Comme le quotient sur lequel nous travaillons n'est pas nécessairement un corps (ceci équivaut à dire que P est irréductible, ce qui n'est pas vraiment ce qui nous intéresse), nous allons plutôt utiliser l'isomorphisme $\psi : \dfrac{\mathbb{F}_q[X]}{(P)} \longrightarrow \displaystyle\prod_{k=1}^{r} \dfrac{\mathbb{F}_q[X]}{(P_k)}$ donné par le théorème Chinois, puisque P est sans facteur carré.

On s'intéresse alors plutôt à $\widetilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$, que nous pouvons décrire facilement : $\forall (Q_1, ..., Q_r) \in \displaystyle\prod_{k=1}^{r} \dfrac{\mathbb{F}_q[X]}{(P_k)}, \widetilde{\varphi}(Q_1, ..., Q_r) = (Q_1^q, ..., Q_r^q)$. L'intérêt de cette application, est que, puisque les P_k sont irréductibles et que $\mathbb{F}_q[X]$ est principal, $\widetilde{\varphi}$ est définie sur un produit de corps. Ainsi, les éléments de $\dfrac{\mathbb{F}_q[X]}{(P_k)}$ vérifiant $Q_k^q = Q_k$ sont exactement les éléments de $\mathbb{F}_q$ (par construction des corps finis). Ainsi, $Ker(\widetilde{\varphi} - id) \simeq \mathbb{F}_q^r$. Puisque $\widetilde{\varphi}$ et φ sont semblables, on a alors $dim\ Ker(\varphi - id) = r$.

Si $r = 1$, c'est terminé. Sinon, $\mathbb{F}_q$ corresponds à un espace de vecteurs propres de φ de dimension 1. Puisque $r > 1$, on peut alors trouver un vecteur propre qui ne soit pas un polynôme constant modulo (P). Donc il existe $V \in \mathbb{F}_q[X]$ non constant modulo (P) qui soit un vecteur propre pour φ. C'est ce polynôme qui va nous intéresser.
Puisque V est un vecteur propre pour la valeur propre 1, nous avons $\psi(V) = (\alpha_1, ..., \alpha_r)$ avec, pour tout k, $\alpha_k \in \mathbb{F}_q$ d'après ce qui précède.

A présent, pour $\alpha \in \mathbb{F}_q$, intéressons-nous $pgcd(P, V - \alpha)$. Cet élément est un diviseur de P. Mais nous connaissons les diviseurs de P, puisque nous avons sa décomposition en produit de facteurs premiers ! Il existe alors $I_\alpha \subset [\![1; r]\!]$ tel que :

$$pgcd(P, V - \alpha) = \prod_{k \in I_\alpha} P_k$$

Caractérisons I_α : $\forall k \in [\![1; r]\!], k \in I_\alpha$ si et seulement si $V = \alpha\ mod\ (P_k)$ donc si et seulement si $\alpha = \alpha_k$. On en déduit que $I_\alpha = \{k \in [\![1; r]\!] \mid \alpha = \alpha_k\}$. En particulier, si $k \in [\![1; r]\!], k \in I_{\alpha_k}$ par définition.

En conclusion, on a $[\![1; r]\!] = \displaystyle\bigsqcup_{\alpha \in \mathbb{F}_q} I_\alpha$, les I_α étant deux à deux disjoints.

En conséquence, $P = \displaystyle\prod_{k=1}^{r} P_k = \prod_{\alpha \in \mathbb{F}_q} \prod_{k \in I_\alpha} P_k = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha)$.

En particulier, ce produit est non trivial (c'est-à-dire pas uniquement composé de 1 ou de P). En effet, sinon, il existerait $\alpha \in \mathbb{F}_q$ tel que $pgcd(P, V - \alpha) = P$. En particulier, $V = \alpha\ mod\ (P)$, et donc V est constant modulo (P), ce qui est exclut. Donc l'un de ces éléments est un facteur non trivial de P.

$\square$

Détaillons alors un peu le fonctionnement de l'algorithme de Berlekamp, afin de voir sa puissance. Tout d'abord, on vérifie que P est sans facteur carré, ce qui se fait en calculant, grâce à l'algorithme d'Euclide, $pgcd(P, P')$. Si $pgcd(P, P') = 1$, on est dans les hypothèses de Berlekamp.
A présent, on calcule matriciellement $\varphi - id$ et on détermine la dimension de son noyau, par exemple en calculant son rang par la méthode de Gauss, puis en utilisant le théorème du rang. Notons r cette dimension. Si $r = 1$, P est irréductible et c'est terminé. Sinon, on trouve un vecteur propre V non constant modulo (P). On calcule enfin, toujours grâce à l'algorithme d'Euclide, les $pgcd(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$, et on trouve ainsi un facteur non trivial.
On peut aller plus loin et trouver la décomposition de P. Pour cela, on prends tous les facteurs non triviaux qui ont été trouvés, et il suffit alors d'appliquer à nouveau Berlekamp à chacun d'eux pour en déduire, par récurrence, la décomposition de P.
Le développement est terminé.

Remarques : C'est un premier pas pour décomposer un polynôme sur $\mathbb{F}_q[X]$. Mais qu'en est-il si P n'est plus supposé sans facteur carré ? On suppose P non constant. On va alors donner un algorithme qui va permettre de décomposer P. Pour cela, cela va dépendre du polynôme $pgcd(P, P')$. On distingue trois cas :

— Si $pgcd(P, P') = 1$, on applique l'algorithme de Berlekamp.
— Si $pgcd(P, P') \neq 1, P$, alors $pgcd(P, P')$ et $P/pgcd(P, P')$ sont des facteurs non triviaux de P. On applique alors l'algorithme sur ces deux facteurs.
— Si $pgcd(P, P') = P$, on est un peu plus embêté. On remarque tout d'abord que, pour des raisons de degré, cette situation équivaut à dire que $P' = 0$. Le lemme suivant permet de caractériser de tels polynômes :

Lemme. $P' = 0$ *si et seulement si il existe un polynôme* $R \in \mathbb{F}_q[X]$ *tel que* $P = R^p$*, où* p *est la caractéristique du corps.*

Démonstration. Le sens réciproque est évident. Pour le sens direct, il suffit de voir que si $a_k X^k$ est un mônome de P avec $a_k \neq 0$, puisque le polynôme dérivé est nul, on a $k.a_k = 0$. Si r est le reste de k modulo la caractéristique p, alors $r.a_k = 0$. Or, r est un entier entre 0 et $p-1$, et peut alors être considéré comme un élément de $\mathbb{F}_p$, et donc de $\mathbb{F}_q$. Donc $r.a_k = r \times a_k = 0$ et, puisque nous travaillons sur un corps, qui est donc intègre, nous avons $r = 0$ car $a_k \neq 0$.
Ainsi, les seuls monômes présents dans l'écriture de P sont ceux de degré un multiple de p. Il reste à dire qu'il existe $b_k \in \mathbb{F}_q$ tel que $b_k = a_k^p$. En effet, si $q = p^n$, $b_k = a_k^{p^{(n-1)}}$ convient tout à fait. Donc, pour construire R, on prends un monôme $a_k X^{pk}$ et on lui associe $b_k X^k$ qui sera un des monômes de R, qui vérifie $R^p = P$ par construction, la caractéristique du corps étant p.

□

Ainsi, via cette preuve, on peut alors construire explicitement R, et on applique l'algorithme sur R.