L'algorithme de Berlekamp

Rémi Lajugie

4 juin 2017

Soit p premier et $q = p^\beta$. On considère P un polynôme de $\mathbb{F}_q$ sans facteurs carrés, *i.e.,* un polynôme $P = \Pi_{i=1}^r P_i$ où les P_i sont irréductibles et distincts. Rappelons le théorème suivant ainsi que les idées de sa preuve.

Théorème 1 *L'application $A : Q \mapsto Q^q$ est linéaire dans $\mathbb{F}_q[X]/P$.*

Soit $\lambda, \mu \in \mathbb{F}_q, Q, R \in \mathbb{F}_q[X]/P$, alors $A(\lambda Q + \mu R) = \lambda Q^q + \mu R^q$ à cause du morphisme de Frobenius et de la caractéristique du corps.

Théorème 2 *(algorithme de Berlekamp) La procédure suivante permet de décomposer Q en facteurs irréductibles :*

1. *Calculer la matrice A correspondant au polynôme P.*
2. *Soit $\mathcal{A} = Ker(A - Id)$. Calculer $r = dim(\mathcal{A})$.*
3. *Si $r = 1$ alors P est irréductible.*
4. *Sinon, soit Q non constant dans $\mathcal{A}$, alors $P = \Pi_{\alpha \in \mathbb{F}_q}(Q - \alpha) \wedge P$ avec la décomposition non triviale. On retourne à la première étape avec ces facteurs.*

L'analyse de cet algorithme repose sur la proposition suivante

Proposition 1
1. *$\mathcal{A}$ n'est jamais vide..*
2. *$dim(\mathcal{A}) = 1$ si, et seulement si P est irréductible.*
3. *On a, pour $Q \in \mathcal{A}$, $P = \Pi_{\alpha \in \mathbb{F}_q}(Q - \alpha) \wedge P$.*
4. *Si, de plus, Q est un polynôme non constant, l'un des facteurs est non trivial.*

Preuve :

Premier point : C'est évident car $\mathcal{A}$ contient l'ensemble des polynômes constants.

Deuxième point : Par le lemme chinois, on a un isomorphisme d'algèbres Φ entre $\mathbb{F}_q[X]/P$ et $\Pi_{i=1}^r \mathbb{F}_q[X]/P_i$. Comme les P_i sont irréductibles, chacun des $\mathbb{F}_q[X]/P_i$ est un corps, extension de F_q. Appelons $x \mapsto \Phi_i(x)$ l'application qui associe, à un polynôme la ième coordonnée de $\Phi(x)$

Soit $x \in \mathcal{A}$, $\Phi(x^q) = \Phi(x)$ donc $\Phi_i(x)^q = \Phi_i(x)$ donc $\Phi_i(x)$ est dans le sous-corps premier de $\mathbb{F}_q[X]/P_i$ c'est à dire $\mathbb{F}_q$. Ainsi, $\Phi(\mathcal{A})$ (et donc $\mathcal{A}$) est de dimension r.

Troisième point : On se place dans le cas où $\mathcal{A}$ est de dimension au moins 2. Remarquons que Φ envoie les polynômes constants sur les $r-$uplets de la forme $(\alpha, \ldots, \alpha)$ avec $\alpha \in \mathbb{F}^q$, donc ces constantes sont de dimension 1. Il existe par conséquent un polynôme non constant, appelons Q l'un de ceux ci.

Remarquons que $\Phi_i(Q - \alpha) = 0$ si et seulement si $\Phi_i(Q) = \alpha$. Donc $P_i | (Q - alpha)$ si et seulement si $\Phi_i(Q) = \alpha$. Ainsi, $P \wedge Q - \alpha = \Pi_{i, a_i = \alpha} P_i$. Donc $P = \Pi_{\alpha \in \mathbb{F}_q}(Q - \alpha) \wedge P$.

Quatrieme point : Si Q est non constant, alors $\exists i \neq j, \Phi_i(Q) \neq \Phi_j(Q)$ donc par le point précédent $P_i | (Q - \Phi_i(Q))$ mais $P_j \nmid (Q - \Phi_i(Q))$.