Licence de Mathématiques
Projet d'algorithmique

L'objet du projet est la factorisation de polynômes sur le corps $\mathbb{F}_2$ à deux éléments. Le projet consiste à programmer deux variantes de l'algorithme de Berlekamp.

1 Modalités

Le projet sera écrit en MAPLE et sera réalisé par binômes (2 personnes). Le rapport sera rédigé à l'aide de LaTeX. Un dossier comportant le rapport et un listing commenté des programmes écrits sera rendu avant le lundi 27 avril au secrétariat de la licence. Il sera apporté un soin tout particulier à la lisibilité et à la clarté des programmes. Le projet fera l'objet d'une mini-soutenance.

2 Rappels de mathématiques

Dans toute la suite, le corps sera le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ des entiers modulo 2. L'algèbre des polynômes à coefficients dans $\mathbb{F}_2$ est notée $\mathbb{F}_2[X]$. Le degré d'un polynôme P est noté $\deg(P)$.

On dit qu'un polynôme Q divise un polynôme P s'il existe un polynôme R tel que $P = QR$. Pour deux polynômes P et Q, le *PGCD* de P et Q est le polynôme de plus haut degré qui divise P et Q. Ce polynôme est noté $\mathrm{pgcd}(P, Q)$. Deux polynômes sont dits premiers entre eux si leur PGCD est égal à 1. On dit qu'un polynôme est *sans carré* s'il n'est pas divisible par un carré.

Un polynôme P de $\mathbb{F}_2[X]$ est dit *réductible* s'il existe une factorisation $P = QR$ où les deux polynômes Q ou R sont de degré au moins égal à 1. Il est dit *irréductible* sinon. On rappelle que tout polynôme P de $\mathbb{F}_2[X]$ se factorise $P = P_1^{e_1} \dots P_r^{e_r}$ où les polynômes $P_1, \dots, P_r$ sont irréductibles et distincts deux à deux. Cette factorisation unique à l'ordre des facteurs près est la décomposition de P en polynômes irréductibles. Factoriser un polynôme consiste à calculer cette décomposition en facteurs irréductibles. Si P est un polynôme de $\mathbb{F}_2[X]$, sa dérivée est notée P'. On rappelle que si P s'écrit $P(X) = \sum_{k=0}^{d} a_k X^k$, alors sa dérivée est égale à $P'(X) = \sum_{k=0}^{d} \bar{k} a_k X^{k-1}$ où $\bar{k}$ dénote la classe de l'entier k dans $\mathbb{F}_2$. Pour trois polynômes P, Q et R, on dit que Q est congru à R modulo P, et on note $Q \equiv R \mod P$ si la différence $Q - R$ est divisible par P.

Exemple 1 *Le polynôme* $P = X^8 + X^6 + X^5 + X^3 + X^2 + X + 1$ *sur* $\mathbb{F}_2$ *se factorise* $P = (X^2 + X + 1)^2(X^4 + X + 1)$. *La dérivée de ce polynôme est* $P' = X^4 + X^2 + 1$. *Ce polynôme n'est pas sans carré puisqu'il est divisible par* $(X^2 + X + 1)^2$.

3 Travail demandé

Le travail à effectuer pour le projet se décompose en deux parties. Dans une première partie, il est demandé de rédiger quelques préliminaires nécessaires à la compréhension de l'algorithme de Berlekamp. La seconde partie consiste à programmer en MAPLE deux variantes de cet algorithme de factorisation de polynômes sur $\mathbb{F}_2$.

3.1 Première partie

On admettra le résultat suivant qui est un cas particulier du théorème des restes chinois.

Théorème 1 (Restes chinois) *Pour toute famille* $(P_i)_{1\leq i\leq s}$ *de polynômes premiers deux à deux et pour toute famille* $(Q_i)_{1\leq i\leq s}$ *de polynômes, il existe exactement un polynôme* R *de degré inférieur à* $\deg(P_1)+\cdots+\deg(P_s)$ *tel que* $R \equiv Q_i \mod P_i$ *pour tout* $1 \leq i \leq s$.

1. On commence par montrer que le problème de la factorisation peut se ramener au cas où le polynôme P est sans carré.
   (a) Démontrer que pour toute suite de polynômes $P_1, \ldots, P_n$ de $\mathbb{F}_2[X]$, on a l'égalité $(P_1+\cdots+P_n)^2 = P_1^2+\cdots+P_n^2$.
   (b) Démontrer que P est un carré si et seulement si $P' = 0$.
   (c) Démontrer que tout polynôme non nul P se factorise de façon unique $P = Q^2R$ où le polynôme R est sans carré.
   (d) Démontrer que cette unique factorisation est donnée par la formule $Q^2 = \mathrm{pgcd}(P, P')$.
   (e) Expliquer comment le calcul de la décomposition d'un polynôme P de $\mathbb{F}_2[X]$ en facteurs irréductibles peut se ramener au cas où P est sans carré avec $P(0) = 1$.

2. On suppose maintenant que $P(0) = 1$ et que P est sans carré. La décomposition de P en polynômes irréductibles s'écrit donc $P = P_1 \ldots P_s$. On note $H(P)$ l'ensemble des polynômes Q tels que $\deg(Q) < \deg(P)$ et
$$Q^2 \equiv Q \mod P. \tag{1}$$
   (a) Démontrer qu'un polynôme Q appartient à $H(P)$ s'il existe des éléments $k_1, \ldots, k_s$ de $\mathbb{F}_2$ tel que $Q \equiv k_i \mod P_i$ pour tout $1 \leq i \leq s$.
   (b) En déduire que $H(P)$ est un sous-espace vectoriel de $\mathbb{F}_2[X]$ de dimension s et que pour tout polynôme Q non constant de $H(P)$, on a l'égalité $P = \mathrm{pgcd}(P, Q)\,\mathrm{pgcd}(P, Q-1)$ et que cette factorisation ne peut pas être triviale.

3.2 Algorithme de Berlekamp

L'algorithme de Berlekamp de factorisation de polynômes sur un corps fini est basé sur la résolution de l'équation (1). D'après ce qui a été vu, tout polynôme non constant et solution de l'équation (1) fournit une factorisation non triviale du polynôme P.

On remarquera que pour calculer la décomposition en polynômes irréductibles de tout polynône P, il suffit de savoir calculer une factorisation non triviale de tout polynône réductible. On part de la factorisation triviale de P et on remplace chaque facteur réductible par une factorisation non triviale de ce facteur. L'algorithme s'arrête quand tous les facteurs sont irréductibles et on a alors trouvé la décomposition de P en facteurs irréductibles.

3.2.1 Première variante

La première méthode consiste à résoudre directement l'équation (1). On remarque que la fonction $\varphi : Q \mapsto Q^2$ qui à un polynôme Q associe son carré est une application linéaire de $\mathbb{F}_2[X]$ dans $\mathbb{F}_2[X]$. On considère alors l'anneau quotient $\mathbb{F}_2[X]/(P)$ des polynômes sur $\mathbb{F}_2$ modulo P. Soit $\hat{\varphi}$ l'application linéaire induite par φ sur le quotient $\mathbb{F}_2[X]/(P)$. L'équation (1) devient alors équivalente à $\hat{\varphi}(Q) = Q$. Un polynôme Q est solution de l'équation (1) si et seulement si il appartient au noyau de l'application linéaire $\hat{\varphi} - \mathrm{Id}$. On considère alors alors la matrice M_P de $\hat{\varphi}$ dans la base canonique $(1, \ldots, X^{n-1})$ de $\mathbb{F}_2[X]/(P)$ où n désigne le degré de P. La matrice $M_P = (m_{i,j})_{0 \leq i,j \leq n-1}$ est donnée par les relations

$$X^{2k} \equiv m_{0,k} + m_{1,k}X + \cdots + m_{n-1,k}X^{n-1} \mod P.$$

Résoudre l'équation consiste alors à calculer le noyau de la matrice $M_P - I_n$. Il n'est pas nécessaire de calculer complètement le noyau. Puisqu'on cherche une factorisation non triviale, il suffit de calculer un polynôme non constant de ce noyau.

Exemple 2 *Soit le polynôme $P(X) = X^5 + X^4 + 1$. La matrice M_P est égale à*

$$M_P = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

3.2.2 Deuxième variante

Soit k un entier strictement positif. On admettra que pour tout polynôme P, il existe un plus petit entier α_k tel que

$$X^{k2^{\alpha_k}} - X^k \equiv 0 \mod P.$$

On considère alors le polynôme R_k qui est l'unique polynôme tel que $\deg(R_k) < \deg(P)$ et

$$R_k \equiv \sum_{i=0}^{\alpha_k - 1} X^{k2^i} \mod P.$$

On admettra que pour tout entier k le polynôme R_k appartient à l'espace vectoriel $H(P)$. Si R_k n'est pas constant, il fournit alors une factorisation du polynôme P.

3.3 Programmation

Le but du projet est de programmer les deux variantes de l'algorithme de Berlekamp dans le langage MAPLE. Les primitives de MAPLE seront bien sûr utilisées pour l'implémentation du calcul polynomial sur le corps $\mathbb{F}_2$ (addition, multiplication et division euclidienne). Par contre, on s'efforcera au maximum de programmer directement les autres opérations. Pour le calcul du PGCD, on pourra utiliser l'algorithme d'Euclide. Les fonctions élaborées de MAPLE comme `Gcd` et `Factor` pourront être utilisées pour valider ce qui a été programmé.

- Ecrire une fonction `PgcdPoly` qui calcule le PGCD de deux polynômes sur $\mathbb{F}_2$.
- Ecrire une fonction `DecoPoly` qui calcule la factorisation $P = Q^2 R$ d'un polynôme.
- Ecrire une fonction `MatOfPoly` qui calcule la matrice $M_P - I_n$ associée à un polynôme.
- Ecrire une fonction `KernelOfMat` qui calcule un vecteur du noyau d'une matrice à coefficients dans $\mathbb{F}_2$.
- Ecrire une fonction `FactOfPolyH` qui calcule la factorisation d'un polynôme P associée à un polynôme Q de $H(P)$.
- Utiliser ces fonctions pour programmer une fonction `Berlekamp1` qui décompose un polynôme en facteur irréductibles en suivant la première variante de l'algorithme de Berlekamp.
- Ecrire une fonction `PolyR` qui pour un entier k et un polynôme P calcule les polynômes R_k utilisés dans la seconde variante de l'algorithme de Berlekamp.
- Utiliser ces fonctions pour programmer une fonction `Berlekamp2` qui décompose un polynôme en suivant la seconde variante de l'algorithme de Berlekamp.

On testera les programmes sur les polynômes de la forme $P_n = 1 + X + \cdots + X^n$ et $P_{n,k} = X^n + X^k + 1$ avec $1 \leq k \leq n/2$ et n inférieur à une constante `Nmax` choisie au moins égale à 100.