Licence de Mathématiques
Projet d'algorithmique

1 Modalités

Le projet sera écrit en MAPLE et sera réalisé par binômes (2 personnes). Le rapport sera rédigé à l'aide de LaTeX (une séance d'initiation est prévue en décembre sur ce traitement de texte). Un dossier comportant le rapport et un listing commenté des programmes écrits sera rendu avant le lundi 8 janvier 1995 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

2.1 Corps finis

Soit $\mathbb{K}$ un corps. On note $\mathbb{K}[X]$ l'algèbre des polynômes à coefficients dans $\mathbb{K}$. Un polynômes est dit *unitaire* si son coefficient de plus haut degré est 1. Un polynôme P de $\mathbb{K}[X]$ est dit *irréductible* si toute factorisation $P = QR$ est triviale : Q ou R appartient au corps $\mathbb{K}$. Par définition, les éléments du corps ne sont pas irréductibles. Quand le polynôme P est irréductible, l'anneau quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ est alors un corps. Deux polynômes Q et R sont dits égaux modulo P si leurs images respectives dans cet anneau quotient sont égales.

On fixe maintenant un nombre premier p. On note $\mathbb{F}_p$ le corps à p éléments constitués des entiers modulo p.

Exemple 1 *Pour $p = 2$, le corps $\mathbb{F}_2$ contient les deux éléments $\{0, 1\}$ et l'addition et la multiplication sont données par les tables suivantes*

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Exemple 2 *Sur $\mathbb{F}_2$, le polynôme $X^2 + 1$ n'est pas irréductible puisque il se factorise $X^2+1 = (X+1)^2$. Par contre le polynôme X^2+X+1 est irréductible sur $\mathbb{F}_2$ puisqu'il est de degré 2 et qu'il n'a pas de racine.*

Exemple 3 (Suite) *Si on pose $P(X) = X^2+X+1$, le corps $\mathbb{K}_2[X]/P\mathbb{K}_2[X]$ contient 4 éléments qui sont 0, 1, X et $1+X$. L'addition et la multiplication sont données par*

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

$\times$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré k. On note $q = p^k$ et $n = q-1$. L'*indice* de P est, par définition, le plus petit entier m tel que X^m soit égal à 1 modulo P. L'indice de P est toujours un diviseur de n. Par définition, le polynôme P est dit *primitif* si son indice est exactement égal à n. Tout les puissances X^i pour $0 \le i \le n-1$ sont alors distinctes et pour tout polynôme Q de degré inférieur à k, il existe un unique entier $0 \le m \le n-1$ tel que $Q = X^m$ modulo P. Cet entier m est alors appelé *logarithme* de Q par rapport à P.

Exemple 4 *Les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 4 et leur indices respectifs sont les suivants*

Polynôme	*Indice*
X^4+X+1	15
X^4+X^3+1	15
$X^4+X^3+X^2+X+1$	5

Seuls les deux premiers sont donc des polynômes primitifs.

2.2 Codes correcteurs

2.2.1 Principe

Les codes correcteurs d'erreurs sont utilisés dans les transmissions de données pour éliminer les effets du bruit. On propose de construire un schéma simple de codes correcteurs.

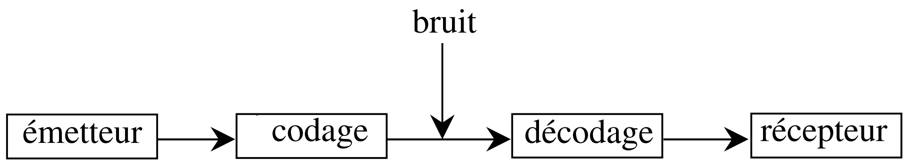

Figure 1: Un canal de communication

Un canal de communication peut être schématisé comme sur la figure 1. Comme toute l'information peut être codée en binaire, on peut suppposer que le message à envoyer est constitué d'une suite de bits. La suite de bits est alors décomposée en blocs de longueur fixe qui sont transmis après codage.

2.2.2 Code de Hamming cyclique

Dans cette partie, le nombre premier p est fixé à $p = 2$. Les bits à valeur 0 ou 1 sont alors considérés comme des éléments du corps $\mathbb{F}_2$. On se propose de décrire maintenant un schéma de codage appelé *Code de Hamming cyclique*. Ce procédé permet de corriger une seule erreur dans un bloc. Il est donc valable pour les faibles taux d'erreurs. On fixe un entier k et on code chaque bloc de longueur $m = 2^k - k - 1$ par un bloc de longueur $n = 2^k - 1$. À un bloc $a = [a_0, \ldots, a_m]$, on associe canoniquement le polynôme $A(X) = a_0 + a_1X + \cdots + a_mX^m$ de $\mathbb{F}_2[X]$. On fixe un polynôme primitif P de degré k. Le codage s'effectue de la façon suivante. Le polynôme $A(X)$, est codé par le polynôme $B(X) = X^kA(X) + R(X)$ où R est le reste de la division euclidienne de $X^kA(X)$ par P. On peut remarquer que B appartient à l'idéal engendré par P. Le décodage s'effectue alors de la manière suivante. Si $C(X)$ est le message reçu, on calcule le reste $S(X)$ de la division euclidienne de C par P. Les deux polynômes $C(X)$ et $S(X)$ sont alors égaux modulo P. Si $S = 0$, on dit qu'il n'y pas eu d'erreur. Sinon, on corrige la composante i de C telle que $S(X) = X^i$ modulo P. L'entier i est donc le logarithme de S par rapport à P.

3 Travail demandé

Les fonctions `Irreduc` et `Primitive` de MAPLE permettent de calculer si un polynôme donné est irréductible ou primitif dans $\mathbb{F}_p[X]$. Ces fonctions seront uniquement utilisées pour vérifier le bon fonctionnement des progammes écrits.

- Écrire une fonction `TableOfIrred` calculant une table de tous les polynômes unitaires et irréductibles de degré inférieur à k sur $\mathbb{F}_p$. On utilisera le crible d'Erathostène. Les polynômes de degré 0 ne sont pas irréductibles et les polynômes irréductibles de degré k s'obtiennent en supprimant des polynômes de degré k ceux qui se factorisent en polynômes de degrés inférieurs. En particulier, les polynômes de degré 1 sont irréductibles.

- Écrire une fonction calculant le produit des polynômes irréductibles de $\mathbb{F}_p[X]$ dont le degré divise un entier k. On vérifiera la formule

$$\prod_{\substack{P \text{ irréductible sur } \mathbb{F}_p[X] \\ \deg(P)|k}} P = X^{p^k-1} - 1$$

- Écrire une fonction `IndexOfIrred` calculant l'indice d'un polynôme irréductible sur $\mathbb{F}_p$.

- Écrire une fonction `TableOfPrim` calculant une table de tous les polynômes primitifs de degré inférieur à k sur $\mathbb{F}_p$.

- Écrire une fonction `DicreteLog` qui, pour un polynôme primitif P, calcule le logarithme d'un polynôme Q par rapport à P.

- Pour un polynôme primitif P, écrire les fonctions de codage et décodage du code de Hamming cyclique associé.