Cryptographie II
(Arithmétique des polynômes et Codes cycliques)

A. Bonnecaze

Institut de Mathématiques de Marseille

Polytech Marseille

Polynômes

Soit A un anneau, un polynôme f est une expression de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

n est un entier positif, les coefficients $a_i,\ 0 \leq i \leq n$ sont des éléments de A et x une indeterminée.

Définition

Soit $f = \sum_{i=0}^{n} a_i x^i$ un polynôme tel que $a_n \neq 0$. Alors f est de degré n (on note $\deg(f) = n$), a_0 est le terme constant et a_n le coefficient de plus haut degré (leading coefficient en anglais).

Arithmétique des polynômes

On peut définir la somme et le produit de deux polynômes $f = \sum_{i=0}^{n} a_i x^i$ et $g = \sum_{i=0}^{m} b_i x^i$ $(m \leq n)$:

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

et

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ où } c_k = \sum_{i+j=k} a_i b_j,$$

où $0 \leq i \leq n$ et $0 \leq j \leq m$.
L'ensemble des polynômes sur A muni de ces deux opérations admet une structure d'anneau noté $A[x]$.
Pour tout $f, g \in F[x]$ (F étant un corps)

$$\deg(f + g) \leq max\{\deg(f), \deg(g)\}, \text{ et } \deg(fg) = \deg(f) + \deg(g).$$

Arithmétique des polynômes

Le polynôme g divise le polynôme f si il existe un polynôme h tel que

$$f = gh$$

Pour éviter tout problème, on ne considère ici que des polynômes à coefficients dans un corps.

Exemple :
Dans $\mathbb{F}_2[x]$, considérons les deux polynômes
$f = x^7 + x^6 + x^3 + x^2 + x + 1$ et
$g = x^4 + x^3 + x^2 + 1$.
Le polynôme g divise f car $f = g(x^3 + x + 1)$

PGCD de polynômes

Théorème

Soit g un polynôme non nul dans $F[x]$. Alors pour tout $f \in F[x]$ il existe deux polynômes q et r de $F[x]$ tels que

$$f = qg + r, \text{ où } \deg(r) < \deg(q).$$

Si d (unitaire) divise f et g et si tout polynôme divisant f et g divise aussi d, alors d est le plus grand diviseur commun de f et g. On note

$$d = pgcd(f, g)$$

Si $pgcd(f, g) = 1$, on dit que f et g sont premiers entre eux.
Exercice : Dans $\mathbb{F}_2[x]$
$f = x^2 + x + 1$ et $g = x^5 - 1$ sont-ils premiers entre eux ?

Un polynôme unitaire a son coefficient de plus haut degré égal à 1

Bézout

Théorème

Avec les mêmes notations, il existe $u, v \in F[x]$ tels que

$$d(x) = u(x)f(x) + g(x)v(x), \text{ avec } u, v \in F[x].$$

Exemple : sur $\mathbb{F}_3$
$f := x^6 + x^5 + 2x^4 + 2x^2 + 2$,
$g := x^2 + 2x + 1$
Alors, on a

$$f = q_1 g + r_1 \text{ avec } q_1 = x^4 + 2x^3 + x \text{ et } r_1 = 2x + 2$$
$$g = q_2 r_1 + r_2 \text{ avec } q_2 = 2x + 2 \text{ et } r_2 = 0.$$

On trouve, $d = 2f + q_1 g = x + 1$.

Exercice : Même exercice avec $f = x^5 + x^2 + x + 1$ et $x^4 + x^3 + 1$ dans $\mathbb{F}_2[x]$

Factorisation

Définition

un polynôme non constant $f \in F[x]$ est dit irréductible sur F si les seuls polynômes ($\neq f$) qui le divisent sont constants. Sinon, le polynôme f est réductible.

Exemple : Le polynôme de $\mathbb{F}_2[x]$
$f = x^4 - 1$ est-il irreductible ? même question avec $f = x^3 - 1$.

Théorème

Tout polynôme $f \in F[x]$ peut s'écrire

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

où $a \in F$, les f_i sont des polynômes irréductibles unitaires de $F[x]$ et les exposants e_i des entiers positifs. Cette factorisation est unique.

Rappel : *Un polynôme unitaire a son coefficient de plus haut degré égal à* 1

Racine d'un polynôme

Définition

Un élément a est une racine (ou un zéro) du polynôme f si $f(a) = 0$.

Exercices :

- Calculer la/les racine(s) dans $\mathbb{F}_2$ de $x^3 - 1$
- Calculer les racines de $x^2 + 1$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$ puis $\mathbb{F}_3$
- $x^3 + x^2 + x + 1$ a-t-il une racine dans $\mathbb{F}_3$?
- Soit $P \in \mathbb{F}_2[x]$, montrer que si α est une racine de P, alors α^2 est aussi une racine de P.
- Sachant que $x^3 + x + 1$ est un facteur de $x^7 - 1$, factoriser $x^7 - 1$ dans $\mathbb{F}_2$

Arithmétique modulaire

Exercices : Calculer dans $\mathbb{F}_2$

- $x^5 + x^3 + x + 1 \mod x^4 + x + 1$
- $(x+1)(x^4 + x^3 + 1) \mod x^4 + x + 1$
- $(x^3 + x + 1)(x^7 + x^6 + 1) \mod x^7 - 1$
- $(x^3 + x^2 + 1)(x^4 + x + 1) \mod x^5 + x + 1$
- $xP(x) \mod x^8 + x^4 + x^3 + x^2 + 1$, où P est un polynôme de degré au plus 7
- Ecrire un algorithme permettant de calculer $P(x).Q(x) \mod x^8 + x^4 + x^3 + x^2 + 1$

TP : arithmétique des polynômes binaires

- Ecrire une fonction qui calcule la somme et le produit de deux polynômes
- Ecrire une fonction qui calcule le PGCD de deux polynômes
- Ecrire l'algorithme d'Euclide étendu de P et Q avec P et Q quelconques (voir chapitre 2 du handbook, p.82)
- Ecrire une fonction qui calcule l'inverse de P modulo Q
- Ecrire la fonction *xtimes* qui calcule $xP(x) \mod x^4 + x + 1$, pour tout P tel que $deg(P) < 4$
- Ecrire une fonction qui calcule la somme et le produit de deux polynômes P et Q modulo $x^4 + x + 1$, avec $deg(P) < 4$ et $deg(Q) < 4$. Est-il facile de généraliser à un modulo quelconque ?

Introduction aux codes correcteur d'erreurs

- Voir le fichier CodesIntro.pdf sur
  http ://pages-perso.esil.univmed.fr/ bonnecaze/Math/Math1.html

Corps finis

- On connaît les corps de p éléments : $\mathbb{F}_p$
- Existe-t-il des corps ayant n éléments, n non premier ?
- Si c'est le cas
  - Comment construire ces corps ?
  - Existe-t-il des corps pour tout n ?

Construction de corps

Essayons de construire un corps avec des octets...

- En informatique, on travaille souvent avec des octets (8 bits) plutôt que des bits
- On sait que $\mathbb{F}_2$ est un corps
- Peut-on construire un corps dont les élément sont des octets ?
- L'addition se fait bit à bit ; l'élément neutre est 00000000 et l'opposé d'un octet est lui-même
- L'ensemble des octets muni de l'addition forme un groupe
- Et la multiplication ?

Opérations sur les octets

Il faut définir une multiplication sur les octets, tel que tout octet non nul admette un inverse

- On identifie les octets avec des polynômes en x de degré au plus 7
- On choisit un polynôme f irréductible de degré 8
- Soit α et β deux octets, alors $\alpha \cdot \beta = \gamma$ avec

$$\gamma(x) = \alpha(x)\beta(x) \mod f(x)$$

- Ainsi γ est un octet (un polynôme de degré au plus 7)
- Quel est l'élément neutre multiplicatif ?
- Tous les éléments ont-ils un inverse ? pourquoi f doit-il être irréductible ?
- Cette structure est-elle un corps ? quel est son cardinal ?
- On vient de construire $\mathbb{F}_{2^8}$, le corps à 256 éléments !

Opérations sur les octets

Focus sur les racines de f

- Choisissons $f(x) = x^8 + x^4 + x^3 + x^2 + 1$
- Soit α une racine de f. Alors $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$
- Donc $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$
- α^8 peut s'écrire 00011101 dans la base $(\alpha^7, \alpha^6, \alpha^5, \alpha^4, \alpha^3, \alpha^2, \alpha, 1)$
- Dans cette base, comment s'écrit α^9 ? α^{10} ?
  Les combinaisons linéaires des α^i se représentent aussi comme des octets
- Soit $F := \{a_0 + a_1\alpha + \cdots + a_7\alpha^7 \mid a_i \in \mathbb{F}_2\}$
- $(F, +, 0)$ est un groupe commutatif
- Montrer que tout élément de F^* admet un inverse multiplicatif
- $(F^*, \cdot, 1)$ est un groupe
- Donc $(F, +, \cdot)$ est un corps de 2^8 éléments

Construction de $\mathbb{F}_{p^m}$

Soit m un entier positif et $f(x)$ un polynôme irréductible sur $\mathbb{F}_p$ de degré m. On considère un élément α satisfaisant $f(\alpha) = 0$. Posons

$$\mathbb{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbb{F}_p\},$$

l'ensemble de tous les polynômes en α de degrés inférieurs à m et à coefficients dans F_p.
On peut alors munir cet ensemble des opérations " $+$ " et " $\cdot$ "
L'opération " $+$ " est définie comme l'addition de polynômes dans $\mathbb{F}_p$.
L'opération " $\cdot$ " est définie comme la multiplication de deux polynômes modulo f.

Proposition

La structure construite forme un corps de caractéristique p. Tout corps fini peut être construit comme précédemment.
Tout corps fini F de caractéristique p admet p^m éléments $(m > 0)$

Construction de $\mathbb{F}_{p^m}$

Remarque

Puisque f est irréductible sur F_p, la racine α n'est pas un élément de F_p

α peut être représenté par un $m-$uplet d'éléments de F_p

- Les élément du corps peuvent être représentés par des vecteurs ou des polynômes
- $\mathbb{F}_{p^m}$ est appelé une extension de F_p de degré m
- F_p est appelé le corps de base
- $\mathbb{F}_{p^m}$ se note aussi $\mathbb{F}_p[x]/(f(x))$, avec f irréductible
- Comment trouver un polynôme irréductible de degré m ?
- Que se passe-t-il si f est réductible ?

Exercice : Soit $p = 2$ et $f(x) = x^3 + x + 1$ un polynôme irréductible sur $\mathbb{F}_2$. Quel corps peut-on construire ? Comment peut-on représenter les éléments du corps ?

Construction de $\mathbb{F}_4$

- Le corps de base est $\mathbb{F}_2$
- Trouver un polynôme irréductible f de degré 2 dans $\mathbb{F}_2$
- Soit α une racine de f, calculer α^3 et α^4
- Ecrire les tables d'addition et de multiplication
- Quelle est la caractéristique du corps $\mathbb{F}_4$?
- Quel est le plus petit corps de caractéristique 2 contenant α ?

Eléments primitifs

Soit $\beta \in \mathbb{F}_{p^m}^*$
Alors toute puissance de β appartient aussi à $\mathbb{F}_{p^m}^*$ et comme $\mathbb{F}_{p^m}$ est fini, il existe un k et un l tel que $\beta^k = \beta^l$. Cela signifie que $\beta^{k-l} = 1$.

Exemple

$F = \mathbb{Z}_{11}$, $\beta = 2$. $F^\star$ s'écrit

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	5	10	9	7	3	6	1	2

Donc $\beta^{10} = 1$: β est une racine dixième de l'unité.

Définition

L'**ordre** d'un élément β non nul dans un corps fini est le plus petit entier $r \geq 1$ tel que $\beta^r = 1$.

Eléments primitifs

Théorème de l'élément primitif

Tout corps fini F de taille p^m contient un élément β d'ordre $p^m - 1$, appelé **élément primitif** de F.

Corollaire

Tout corps fini de taille p^m est de la forme

$$F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}, \ \beta \in F.$$

Exemple : $F = \mathbb{Z}_{11} = \{0\} \cup \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$

- Un polynôme primitif est un polynôme qui contient une racine primitive. Il faut noter que tous les polynômes irréductibles ne sont pas primitifs.

Polynôme minimal

Théorème

Tout élément β d'un corps F d'ordre p^m satisfait $\beta^{p^m} = \beta$.
Ainsi, β est racine de $x^{p^m} = x$ et

$$x^{p^m} - x = \prod_{\beta \in F} (x - \beta).$$

Définition

Le polynôme minimal sur $\mathbb{F}_p$ de β est le polynôme unitaire de plus bas degré $M(x)$ dont les coefficients sont dans $\mathbb{F}_p$ tel que $M(\beta) = 0$.

Exercices

- Construire le corps $\mathbb{F}_{16}$ en utilisant $f(x) = x^4 + x + 1$
- Soit α une racine de f, calculer la fonction $Zech(r)$ définie par

$$\alpha^{Zech(r)} = \alpha^r + 1$$

- Montrer que si α est une racine de f, alors α^2 est aussi une racine de f
- Déterminer toutes les racines de f

Classes cyclotomiques

Les classes cyclotomiques (cyclotomic cosets en anglais) permettent de déterminer le nombre de facteurs irréductibles de $x^{p^m-1} - 1$ sur $\mathbb{F}_p$

Théorème

$\beta \in F_{p^m}$ et β^p ont le même polynôme minimal.

Définition

Soit $\beta \in F_{p^m}$. Alors les éléments $\beta,\ \beta^p, \ldots,\ \beta^{p^{m-1}}$ sont appelés les conjugués de β pour le corps F_p.

Exemple

On considère le corps F_{16} avec $p = 2$, $m = 4$ et β admettant pour polynôme minimal $\beta^4 + \beta + 1$. Alors

$$\left.\begin{array}{ll} \beta & \text{est un zéro de } x^4 + x + 1 \\ \beta^2 & \text{idem} \\ \beta^4 & \text{idem} \\ \beta^8 & \text{idem} \\ \beta^{16} = \beta & \end{array}\right\} \text{4 racines distinctes}$$

Finalement, on peut vérifier par le calcul que

$$x^4 + x + 1 = (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8).$$

Trouver l'ensemble des conjugués de toutes les racines revient à partitionner l'ensemble des puissances de β. Le corps F s'écrit $F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}$ et l'ensemble des puissances de β est tout simplement Z_{p^m-1}.

Classes cyclotomiques

Définition

Soit $a,\ b \in Z_{p^m-1}$
a et b sont dits equivalents (notés $a \equiv b$) si

$$b = p^i a \mod (p^m - 1)$$

La relation d'equivalence est reflexive, symétrique et transitive. C_s représente une classe cyclotomique où s est le plus petit entier de la classe :

$$\{s,\ sp,\ sp^2, \ldots,\ sp^{m_s-1}\},$$

où m_s est l'entier le plus petit tel que $p^{m_s} = s \pmod{p^m - 1}$. L'entier s est quelquefois appelé le chef de classe ou en anglais coset leader.

Classes cyclotomiques

Exemple

Quelles sont les classes cyclotomiques modulo 15 pour $p = 2$?

Théorème

Soit $\alpha \in \mathbb{F}_{p^m}$ un élément primitif.

$$M(\alpha^s)(x) = \prod_{i \in C_s} (x - \alpha^i)$$

Exercice

Soit α une racine primitive de $x^4 + x + 1$ sur $\mathbb{F}_{16}$.
Déterminer les polynômes minimaux de $1, 3, 5, 7$.

TP

1. Ecrire une fonction qui additionne deux éléments de $\mathbb{F}_{16}$
2. Ecrire une fonction qui multiplie deux éléments de $\mathbb{F}_{16}$
3. Ecrire la fonction *LogZech* : $LogZech(r) = \alpha^r + 1$
4. Ecrire une fonction qui calcule l'inverse d'un élément de $\mathbb{F}_{16}$
5. Ecrire une fonction qui détermine les classes cyclotomique modulo n (pour p quelconque)

Définition

Les codes cycliques représentent la famille de codes la plus importante. D'un point de vue pratique ce sont les codes les plus utilisés car leur mise en œuvre est facile et ils admettent souvent de bons algorithmes de décodage

Définition

Un code linéaire en bloc C de longueur n sur $F[x]$ est dit cyclique si l'ensemble de ses mots est invariant par décalage circulaire :

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Exemple

i) Le code binaire $C = \{000,\ 101,\ 011,\ 110\}$ est un code cyclique.

ii) Le code binaire $C = \{0000,\ 1001,\ 0110,\ 1111\}$ n'est pas cyclique. Il est cependant équivalent à un code cyclique (il faut échanger les troisième et quatrième coordonnées).

Structure algébrique

Tout mot $c = (c_0, c_1, \cdots, , c_{n-1})$ d'un code C sur F peut être identifié à un polynôme $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ de $F[x]$.
Pour pouvoir construire des codes cycliques, l'anneau à considérer est $R_n = F[x]/(x^n - 1)$.
Dans R_n, on peut réduire tout polynôme modulo $x^n - 1$ en remplaçant simplement x^n par 1, x^{n+1} par x et ainsi de suite.

$$\begin{aligned} x \,.\, c(x) &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}. \end{aligned}$$

La multiplication par x correspond à un décalage circulaire.
La multiplication par x^m correspond à m décalages circulaires.

Polynôme générateur

Définition

Le polynôme générateur $g(x)$ d'un code cyclique C est un polynôme non nul unitaire de plus bas degré de C.

Proposition

Le polynôme générateur est unique (Preuve : par contradiction)

Proposition

Tout mot d'un code cyclique est un multiple du polynôme générateur. On note $C = \langle g \rangle$.
Preuve : par contradiction en effectuant la division euclidienne de c par g

Proposition

Le polynôme générateur divise $x^n - 1$.
Preuve : On a $x^n - 1 = ag + r$ avec $\deg(r) < \deg(g)$ et on conclut

Représentation matricielle

$c(x) = a(x)g(x)$. Puisque $\deg(c(x)) < n$ et $\deg(g(x)) = r$, on obtient $\deg(a(x)) < n - r$.
En notation matricielle, on a

$$c = aG$$

où $c = (c_0, \ldots, c_{n-1})$, $a = (a_0, \ldots, a_{n-r})$ et G est une matrice circulante $(n-r) \times n$ dont la $i$ème ligne ligne contient le mot $x^{i-1}g$

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & & 0 \\ & g_0 & g_1 & \cdots & g_{r-1} & g_r & \\ & & & \cdots & \cdots & & \\ 0 & & g_0 & \cdots & \cdots & & g_r \end{bmatrix}.$$

Son rang est $n - r$. G est une matrice génératrice du code qui a $dim(C)$ lignes. Ainsi $\deg(g) = n - dim(C)$.

Procédure de codage systématique

On veut coder la séquence de longueur k $u_1, u_2, \ldots, u_k$ avec $u_i \in F$:

u_1	$u_2 \ldots$	u_k

L'idée est de rajouter $n-k$ symboles de manière à obtenir un mot de longueur n qui appartienne au code cyclique C engendré par le polynôme générateur g.

1. On forme le polynôme

$$u(x) = u_1 x^{n-k} + u_2 x^{n-k+1} + \cdots + u_k x^{n-1}$$

La séquence est ainsi décalée de k positions vers la droite :

$0 \ldots 0$	u_1	$u_2 \ldots$	u_k

2. puis on effectue la division euclidienne par le polynôme générateur g du code
$$u(x) = g(x)q(x) + r(x)$$
avec $\deg(r) < \deg(g) = n - k$
3. le polynôme $c(x) = u(x) - r(x)$ est un multiple de $g(x)$. Le mot c appartient donc au code. Si le code est binaire, on ne prend pas en compte les signes et on obtient :

$r_1 \dots r_{n-k}$	$u_1 \quad u_2 \dots \quad u_k$

Il s'agit d'un codage systématique car les symboles de parité (coefficients de $r(x)$) sont séparés des symboles d'information.

Exercice

Construire un code de longueur 7 sur $\mathbb{F}_2$ de dimension 4, sachant que $x^7 - 1 = \left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)(x + 1)$
Puis coder la séquence 1011.

Dual d'un code cyclique

Théorème

Soit g le polynôme générateur de $C = [n, k]$ et $h := (x^n - 1)/g$. Alors le polynôme générateur de $C^\perp$ est $x^k h(x^{-1})$

Construction du code de Hamming $[7, 4]$

Soit $C = \langle g \rangle$ avec $g = x^3 + x + 1$.

- Ecrire une matrice génératrice G du code
- Quel est le polynôme générateur de $C^\perp$?
- Ecrire une matrice génératrice H du code dual

Construction d'un code cyclique

Pour construire un code cyclique de longueur n, il est utile de connaître la décomposition de $x^n - 1$ en polynômes irréductibles sur le corps de base F :

$$x^n - 1 = \prod_i f_i(x).$$

- On détermine les classes cyclotomiques modulo n
- La donnée d'un facteur irréductible primitif permet d'obtenir tous les autres facteurs
- Le polynôme générateur du code est un produit de facteurs

Exercice Combien peut-on construire de codes cycliques $[31, 21]$ sur $\mathbb{F}_2$?

Les codes de Hamming

Il s'agit d'une famille de codes de paramètres

$$[n = 2^m - 1, k = n - m, d = 3]$$

Un code de Hamming H_m peut être défini par sa matrice de contrôle dont les colonnes sont tous les $m-$tuples distincts non nuls.

Soit α une racine primitive de $\mathbb{F}_{2^m}$, alors $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$ sont tous distincts et peuvent être représentés par tous les $m-$tuples non nuls. Ainsi, la matrice de contrôle d'un code de Hamming peut s'écrire

$$H = [1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}].$$

Les codes de Hamming

$$c = (c_0, c_1, \ldots, c_{n-1}) \in H_m$$
$$\Leftrightarrow$$
$$Hc^T = 0$$
$$\Leftrightarrow$$
$$\sum_{i=0}^{n-1} c_i \alpha^i = 0$$
$$\Leftrightarrow$$
$$c(\alpha) = 0 \text{ où } c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Donc $c \in H_m \Leftrightarrow M^{(1)}(x) \mid c(x)$ et H_m consiste en tous les multiples de $M^{(1)}(x)$.
On vient de montrer que H_m est un code cyclique de polynôme générateur $g(x) = M^{(1)}(x)$.

Les codes BCH

Définition

Un code BCH sur $\mathbb{F}_q$ de longueur n et distance construite δ est le plus grand code possible ayant comme zéros

$$\beta^b, \beta^{b+1}, \ldots, \beta^{b+\delta-2},$$

où $\beta \in \mathbb{F}_{q^m}$ est une racine primitive de l'unité, b un entier positif et m l'ordre multiplicatif de q modulo n.

Il existe deux cas importants :

1. $b = 1$ appelé en anglais *narrow-sense BCH code*.
2. Si $n = q^m - 1$ on parle de code BCH primitif.

Proposition

La distance construite δ est une borne inférieure de la distance minimale d.

TP

Programmer les fonctions suivantes (les codes sont binaires)

1. Input : un vecteur x de longueur n. Output : le poids de Hamming de x
2. Input : un polynôme générateur, une longueur n. Output : k et d
3. Input : matrice de contrôle d'un code $[n, k]$, un vecteur de longueur n. Output : le syndrome
4. Input : matrice de contrôle du code de Hamming, un vecteur. Output : position de l'erreur éventuelle
5. Input : distance construite δ. Output : degré du polynôme générateur et la dimension du code de longueur 15