CORPS FINIS ET CODES CORRECTEURS D'ERREURS

J. Mellac

Fevrier 2002

Chapitre 1

Anneaux et idéaux.

1.1 Anneaux principaux.

1.1.1 Définitions.

Un anneau est un ensemble A muni de deux lois de composition internes notées $+$ et . et vérifiant

- L'addition est associative, commutative, admet un élément neutre noté 0 et appelé élément nul et chaque élément x admet un symétrique noté $-x$ et appelé opposé de x. On traduit ceci en disant que $(A, +)$ est un groupe commutatif.
- La multiplication est associative, distributive à gauche et à droite par rapport à l'addition et admet un élément neutre noté 1 et appelé unité de l'anneau. Les éléments 0 et 1 sont distincts, le seul cas particulier étant $A = \{0\}$, l'anneau nul, qui ne contient qu'un élément.
- Si la multiplication est commutative, on dit que l'anneau est commutatif. Dans la suite tous les anneaux seront commutatifs.

En général on notera le produit ab et non $a.b$.

Formule du binôme.
$(A, +)$ étant un anneau commutatif, a, b étant deux éléments de A, $n \in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

les C_n^k étant les coefficients du binôme.

Diviseurs de zéros.
A étant un anneau commutatif on dit que $a \in A$ est un diviseur de zéro de A si

- $a \neq 0$.
- $\exists b \in A,\ b \neq 0$ tel que $ab = 0$.

Par exemple dans l'anneau des matrices carrées réelles d'ordre deux

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

Eléments inversibles.
A étant un anneau commutatif, $a \in A$ est inversible s'il admet un symétrique pour la multiplication noté $1/a$ ou a^{-1}.
$a.a^{-1} = a^{-1}.a = 1$.
Un élément a inversible n'est pas diviseur de zéro
$ab = 0 \Rightarrow a^{-1}(ab) = b = 0$.
Un anneau qui n'a pas de diviseurs de zéro est appelé anneau intègre.
Une partie B de A est appelée sous anneau de A si $B \neq \emptyset$ et $(B, +, .)$ est un anneau.
Un anneau A est un corps si tout élément de $A - \{0\}$ est inversible. Dans ce cas A est intègre.

1.1.2 Anneaux Principaux.

Dans la suite $(A, +, .)$ est un anneau commutatif non réduit à zéro.

Définition 1.1 *Un sous ensemble $I \neq \emptyset$ de A est un idéal de A si*
— *$(I, +)$ est un groupe.*
— *$\forall a \in A$, $aI = \{ax | x \in I\} \subset I$.*
Un idéal I de A est appelé idéal principal s'il existe $x \in A$ tel que $I = xA$.
On dit que A est un anneau principal si A est intègre et si tous ses idéaux sont principaux.

Anneaux quotients.

Soit I un idéal de A, on définit une relation d'équivalence sur A par
$x \equiv y$ mod. I si $x - y \in I$. (mod. se lit modulo). On vérifie aisément qu'il s'agit bien d'une relation d'équivalence, l'ensemble des classes d'équivalence est noté A/I et est appelé ensemble quotient de A par I.
La relation d'équivalence est compatible avec l'addition et la multiplication dans A.

$$\left\{ \begin{array}{l} x_1 \equiv y_1 \text{ mod. } I \\ x_2 \equiv y_2 \text{ mod. } I \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x_1 + x_2 \equiv y_1 + y_2 \text{ mod. } I \\ x_1 x_2 \equiv y_1 y_2 \text{ mod. } I \end{array} \right. .$$

En effet
$(x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) \in I$
$x_1 x_2 - y_1 y_2 = x_1(y_1 - y_2) + y_2(x_2 - x_1) \in I$
car $x_1 I \subset I$ et $y_2 I \subset I$.
Ceci permet de définir deux opérations sur A/I, notées également $+$ et $.$ En notant $\overline{x} = x + I$ la classe d'équivalence de x on définit
$\overline{x_1} + \overline{x_2} = \overline{x_1 + x_2}$
$\overline{x_1}.\overline{x_2} = \overline{x_1 x_2}$.
On peut alors vérifier sans difficulté que $(A/I, +, .)$ est un anneau commutatif appelé Anneau Quotient de A par I. L'application

$$p : \left\{ \begin{array}{l} A \to A/I \\ x \to \overline{x} \end{array} \right.$$

vérifie $p(x+y)=p(x)+p(y)$, $p(xy)=p(x)p(y)$, $p(1)=\overline{1}$. On dit que p est un morphisme d'anneau, il est appelé projection canonique de A sur A/I.

Théorème de Bezout.
Soit A un anneau principal. a, b, c, d, e étant des éléments de A on dit que
- $b|a$ s'il existe b_1 tel que $a = bb_1$.
- e est le plus grand commun diviseur de c et d (e =pgcd(c,d)) si $e|c$, $e|d$,et si tout diviseur commun à c et d divise e.
- On dit que c et d sont premiers entre eux si pgcd(c,d)=1.

Remarque : En fait un pgcd est défini à la multiplication par un nombre inversible près.

Théoreme 1.1 (Théorème de Bezout) *Soient a et b éléments de A anneau principal*
$aA + bA = dA$ *où* d= *pgcd*(a,b).

Démonstration.
L'anneau A étant principal et $aA+bA$ étant un idéal de A (vérification immédiate) on a $aA+bA=dA$ pour un élément $d \in A$. Autrement dit $\forall (x,y) \in A^2\ \exists z \in A$ tel que $ax+by=dz$. En prenant $x=1$ (resp. $x=0$), $y=0$ (resp. $y=1$) on obtient $a=da_1$, $b=da_2$, on a donc $d|a$, $d|b$. Il existe x, y éléments de A tels que $d=ax+by$ ce qui monttre que tout diviseur commun à a et à b divise d. On a d=pgcd(a,b).

1.2 Anneaux $\mathbb{Z}$ et $k[X]$.

Théoreme 1.2 *L'anneau $\mathbb{Z}$ est principal*

Démonstration.
Tout sous ensemble $a\mathbb{Z}$, $a \in \mathbb{Z}$, est un idéal de $\mathbb{Z}$ et $\mathbb{Z}$ est intègre.
Réciproquement, soit $I \neq \{0\}$ un idéal de $\mathbb{Z}$ et a le plus petit entier strictement positif de I. Soi $b \in I$. La division euclidienne de b par a s'écrit
$b = aq + r$, $0 \leq r < |b|$, $r = a - bq \in I \Rightarrow r = 0$ d'après la définition de a et on a $I = a\mathbb{Z}$.

La relation d'équivalence
$x \equiv y$ mod. I dans $\mathbb{Z}$ est notée
$x \equiv y$ mod. a avec $I = a\mathbb{Z}$.
C'est équivalent à dire que $a|x-y$.
L'anneau quotient $\mathbb{Z}/a\mathbb{Z}$, $a > 0$ contient a éléments distincts $\overline{0}, \overline{1}, \cdots \overline{a-1}$ correspondants aux restes possibles dans la division euclidienne par a. On vérifie sans difficulté que ces classes d'équivalences sont distinctes deux à deux.
Remarque :
L'anneau $\mathbb{Z}/a\mathbb{Z}$ peut ne pas être intègre, ainsi dans $\mathbb{Z}/6\mathbb{Z}$ $\overline{2}.\overline{3} = \overline{0}$, $\mathbb{Z}/6\mathbb{Z}$ contient donc des diviseurs de zéro.

Caractérisation des éléments inversibles.

Théoreme 1.3 *Les conditions suivantes sont équivalentes*

— $\overline{x}$ *est inversible dans* $\mathbb{Z}/a\mathbb{Z}$.
— $\overline{x}$ *n'est pas diviseur de zéro dans* $\mathbb{Z}/a\mathbb{Z}$.
— x *est premier avec* a.

Démonstration.
Supposons $\overline{x}$ inversible dans $\mathbb{Z}/a\mathbb{Z}$.
Soit $\overline{y}$ tel que $\overline{x}.\overline{y} = 0$. On a alors $\overline{x}^{-1}.(\overline{x}.\overline{y}) = 0$ c'est à dire $\overline{y} = 0$, $\overline{x}$ n'est donc pas diviseur de zéro.

Supposons que x ne soit pas premier avec a, soit $d = \text{pgcd}(a, x) \neq 1$
$x = dx_1$, $a = da_1 \Rightarrow \overline{x}.\overline{a_1} = \overline{x_1}.\overline{a} = \overline{0}$ et $\overline{x}$ est diviseur de zéro dans $\mathbb{Z}/a\mathbb{Z}$.

Supposons x premier avec a. En utilisant le théorème de Bezout, il existe des entiers relatifs k et l tels que $kx + la = 1$ ce qui entraîne $\overline{k}.\overline{x} = \overline{1}$, $\overline{x}$ est donc inversible.

Anneau $k[X]$.
k étant un corps, l'ensemble des polynômes à coefficients dans$k$, noté $k[X]$ a une structure d'anneau intègre.
Division euclidienne.
$A, B \in k[X]$, $B \neq 0$. Il existe un couple unique $(Q, R) \in k[X] \times k[X]$ tel que $A = BQ + R$ avec degré(R) <degré(B). R est appelé le reste de la division euclidienne de A par B.

Théoreme 1.4 *L'anneau* $k[X]$ *est principal.*

Démonstration.
Soit $I \neq \{0\}$ un idéal de $k[X]$ et $Q \neq 0$ un polynôme de degré minimal de I.
Soit $P \in I$, $P = QQ_1 + R$, $d^oR < d^oQ$, ceci entraîne $R \in I$ et donc $R = 0$ et $I = (Q(X))$ idéal principal engendré par le polynôme $Q(X)$.

La relation d'équivalence
$A \equiv B$ mod. I dans $k[X]$ est notée
$A \equiv B$ mod. Q
Ceci équivaut à $Q|A-B$ ou encore A et B ont le même reste dans la division par Q. Si $d^oQ = n$, $k[X]/I$ est représenté par l'ensemble des polynômes de degrés strictement inférieurs à n, c'est à dire par les restes potentiels de la division par Q.
Une démonstration analogue à celle faite pour $\mathbb{Z}$ montre le résultat suivant

Théoreme 1.5 *Les conditions suivantes sont équivalentes*
— $\overline{A(X)}$ *est inversible dans* $k[X]/(Q(X))$.
— $\overline{A(X)}$ *n'est pas diviseur de zéro dans* $k[X]/(Q(X))$.
— $A(X)$ *est premier avec* $Q(X)$.

Théoreme 1.6
— $\mathbb{Z}/p\mathbb{Z}$ *est un corps si et seulement si l'entier* p *est premier.*
— $k[X]/(p(X))$ *est un corps si et seulement si* $p(X)$ *est irréductible.*

Dans les deux cas tous les éléments non nuls sont inversibles.

1.3 Exercices.

Exercice 1.

Soit p un entier premier > 2.
Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont leurs propres inverses ?
Montrer le théorème de Wilson : Si p est un entier premier, alors $(p-1)!+1$ est divisible par p. Démontrer la réciproque.

Exercice 2.

Soit p un entier premier supérieur ou égal à 3, $K = \mathbb{Z}/p\mathbb{Z}$ et $q = (p-1)/2$.
1) Montrer que

$$G = \{x \in K^* | \exists a \in K^* \ , \ x = a^2\}$$

est un sous groupe multiplicatif de K^*. Quel est son ordre (c'est à dire son cardinal) ?
2) Montrer que si $k \in G$, alors $k^q = -\overline{(p-1)!}$ et en déduire le théorème de Wilson.
3) Montrer que si $k \in K^* - G$ alors $k^q = \overline{(p-1)!}$.
4) Montrer que

$$G = \{x \in K^* | x^q = 1\} \ , \ K^* - G = \{x \in K^* | x^q = -1\}$$

et en déduire le petit théorème de Fermat
$\forall a \in \mathbb{Z} \ , \ a^p \equiv a \ \text{mod.} p$,
ou $\forall a \in \mathbb{Z}$ non divible par p $\ a^{p-1} \equiv 1$ mod. p.

Exercice 3.

En utilisant le petit théorème de Fermat, montrer que

$$\forall n \in \mathbb{N} \ , \ 3^{n+3} - 4^{4n+2} \ \text{ est divisible par } 11.$$

Exercice 4.

On appelle $\phi(n)$, $n \in \mathbb{N}^*$, le nombre d'éléments inférieurs à n et premiers avec n, c'est à dire le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On utilise ici une méthode faisant appel au cours de probabilités.
Une urne contient $n \in \mathbb{N}^*$ boules numérotées de 1 à n et indiscernables au toucher. On tire une boule au hasard. $p_1, p_2, \cdots, p_r$ étant les diviseurs premiers de n, on note A_{p_i} l'évenement le numéro porté par la boule tirée est divisible par p_i.
1) Calculer $P(A_{p_i}),\ 1 \leq i \leq r$. Montrer que les évènements A_{p_i} sont indépendants dans leur ensemble.
2) Calculer la probabilité de l'évènement $A =$ "le numéro porté par la boule tirée est premier avec n" (il n'est divisible par aucun p_i). En déduire le nombre $\phi(n)$ des entiers plus petits que n et premiers avec n.

Chapitre 2

Corps finis.

2.1 Caractéristique. Sous corps premier.

Soit K un corps commutatif. Considérons le morphisme d'anneaux

$$\phi : \begin{cases} \mathbb{Z} \to K \\ m \to m.1 = \underbrace{1+1+\cdots 1}_{m\ fois} \end{cases}$$

Deux situations peuvent se présenter

- $\ker \phi = 0$.
  ϕ est alors injectif et peut être étendue à $\mathbb{Q}$ par $\phi(m/n) = m.1/n.1$, dans ce cas on confond $\mathbb{Q}$ et $\phi(\mathbb{Q})$ et on considère $\mathbb{Q}$ comme un sous corps de K.
- $\ker \phi = p\mathbb{Z}$.
  L'entier p est alors un nombre premier, sinon on aurait
  $p.1 = (m.1)(n.1) = 0 \Rightarrow (m.1 = 0)$ ou $(n.1 = 0)$ ce qui est impossible d'après la définition de p qui est le plus petit entier positif vérifiant cette propriété.
  On a alors
  $\phi(x) = \phi(y) \Leftrightarrow x - y \in p\mathbb{Z} \Leftrightarrow x \equiv y \bmod p$. L'application
  $\overline{\phi}\{ \begin{array}{l} \mathbb{Z}/p\mathbb{Z} \to K \\ \overline{m} \to m.1 \end{array}$ est alors injective et $\mathbb{Z}/p\mathbb{Z}$ peut être considéré comme un sous corps de K.

Le nombre p qui est nul ou est premier est appelé caractéristique du corps K.
Si $p = 0$, $\mathbb{Q}$ est appelé sous corps premier de K.
Si p est premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est également appelé sous corps premier de K.
Le sous corps premier est dans les deux cas le plus petit corps contenu dans K.
Un corps fini a donc une caractéristique $p > 0$ et contient $\mathbb{F}_p$ comme sous corps premier. On utilisera par la suite le théorème suivant sans démonstration

Théoreme 2.1 (Théorème de Wederburn) *Tout corps fini est commutatif.*

2.2 Extensions de corps.

Théoreme 2.2 *Soit $f(X)$ un polynôme irréductible sur $\mathbb{F}_p$, de degré n. L'anneau quotient $K = \mathbb{F}_p[X]/((f(X))$ est un corps fini de cardinal p^n.*

Démonstration.
Le polynôme $(f(X)$ étant irréductible, K est bien un corps. Soit $g(X)$ un polynôme de $\mathbb{F}_p[X]$ et $r(X)$ le reste de la division de ce polynôme par $f(X)$. Posons $x = \overline{X} = X + (f(x))$. On a
$\overline{g(X)} = \overline{r(X)} = a_0 + a_1 x + \cdots a_{n-1}x^{n-1}$, $a_i \in \mathbb{F}_p$, $i = 0, 1, \cdots, n-1$
où $r(X) = a_0 + a_1 X + \cdots a_{n-1}X^{n-1}$. K est un espace vectoriel sur $\mathbb{F}_p$ et on vérifie que $(1, x, x^2, \cdots x^{n-1})$ est une base de cet espace vectoriel qui est donc de dimension n sur $\mathbb{F}_p$ ce qui permet d'obtenir p^n éléments distincts.
Un raisonnement analogue montre que tout corps fini de caractéristique p a un cardinal p^n pour un entier n.

Exemple. $X^2 + 1$ est irréductible sur $\mathbb{F}_3$, 0,1 et 2 n'étant pas zéros de ce polynôme.
$\mathbb{F}_3[X]/(X^2 + 1)$ est un corps à 9 éléments et ils s'écrivent avec les notations précédentes et le fait que $x^2 + 1 = 0$
$0, 1, 2, x, 1 + x, 2 + x, 2x, 1 + 2x, 2 + 2x$. Vérifions de plus que l'élément (1+x) engendre le groupe multiplicatif de ce corps.
$(1 + x)^0 = 1, (1 + x)^1 = 1 + x, (1 + x)^2 = 2x, (1 + x)^3 = 1 + x^3 = 1 + 2x$
$(1 + x)^4 = 4x^2 = 2, (1 + x)^5 = 2 + 2x, (1 + x)^6 = x, (1 + x)^7 = x + 2.$

Théoreme 2.3 *Soit K un corps de caractéristique p, a, b deux éléments de K, $A(X), B(X)$ deux éléments de $K[X]$*

- $(a + b)^p = a^p + b^p$.
- $(A(X) + B(X))^p = (A(X))^p + (B(X))^p$.

Démonstration.
On remarque que

$$1 \leq i \leq p - 1 \Rightarrow C_p^i \text{ est multiple de p}$$

$(a+b)^p = a^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i} + b^p$ et $p.x = 0$ pour tout $x \in K$. La démonstration est analogue pour les polynômes.

Elements algébriques. Soient K et L deux corps, $K \subset L$, on dit que L est une extension de corps de K.
Un élément $x \in L$ est dit algébrique sur K s'il est zéro d'un polynôme P à coefficients dans K. Si ce n'est pas le cas on dit que x est transcendant sur K. Par exemple le réel $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ car il est zéro de $X^2 - 2 \in \mathbb{Q}[X]$. On montre que par contre e et π sont transcendants sur $\mathbb{Q}$.
L'élément $x \in L$ étant algébrique sur K l'ensemble $I = \{P \in K[X] | P(x) = 0\}$ est un idéal de $K[X]$, cet anneau étant principal $I = (f(X))$ où le polynôme $f(X)$ est choisi unitaire, c'est le polynôme unitaire de degré minimum vérifiant $f(x) = 0$, il doit donc être irréductible sinon on aurait $f(x) = f_1(x)f_2(x) = 0$

et $f(X)$ ne serait pas de degré minimum.
Le polynôme $f(X)$ est appelé polynôme minimal de x sur K.

L'élément $x \in L$ étant algébrique sur K, on définit $K[x] = \{P(x)|P \in K[X]\}$. Soit n le degré de son polynôme minimal $f(X)$, en utilisant la division euclidienne des polynômes on vérifie aisément que $K[x]$ est un espace vectoriel de dimension n sur K dont $(1, x,^2, \cdots, x^{n-1})$ est une base. Cet espace vectoriel est aussi un corps, en effet, le morphisme d'anneau

$$\begin{cases} K[X] \to K[x] \\ P \to P(x) \end{cases}$$

est surjectif et son noyau est (fX)), on a donc

$$K[X]/(f(X)) \simeq K[x]$$

, ce qui démontre que $K[x]$ est un corps.

Remarque :
Soit K un corps et $f(X)$ un polynôme irréductible sur K de degré > 1, il existe un plus petit corps L (à un isomorphisme près), extension de K, dans lequel $f(X)$ admet un zéro. Définissons $L = K[X]/(f(X))$ et on pose $x = \overline{X} = X + (f(X))$, on a $f(x) = 0$. Un corps vérifiant cette propriété est appelé corps de rupture de $f(X)$. En répétant cette opération on obtient un corps extension de K contenant toutes les racines de $f(X)$. Ce corps est aussi unique à un isomorphisme près.

2.3 Propriétés des corps finis.

Propriété.
Pour un corps fini K de cardinal $q = p^n$, tous les éléments x de K vérifient l'équation $X^q - X = 0$.
C'est vérifié pour $x = 0$, si $x \neq 0$, le groupe multiplicatif K^* est de cardinal $q - 1$, le théorème de Lagrange entraîne alors que $x^{q-1} = 1$ pour tout $x \in K^*$.

Théoreme 2.4 *Pour tout nombre premier p et tout entier n strictement positif, il existe un corps fini K de cardinal $q = p^n$. Il est noté $\mathbb{F}_q$. Ce corps est unique à un isomorphisme près.*

Démonstration.
Définissons par K le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. Ce polynôme a q racines distinctes car son polynôme dérivé $qX^{q-1} - 1 = -1$ est non nul (remarquer que l'on multiplie par q et que les corps sont de cactéristique p).
Posons $S = \{a \in K|a^q = a\}$. On vérifie que S est un sous corps de K. Il contient 0 et 1 et si $a, b \in S$
$(a - b)^q = a^q - b^q = a - b$, $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$.
Le polynôme $X^q - X$ est scindé dans S qui contient toutes ses racines, on a donc $K = S$ et Card$S = q$. L'unicité provient de l'unicité du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Théoreme 2.5 *Le groupe multiplicatif d'un corps fini est cyclique.*

Démonstration.
On utilise le résultat suivant que l'on laisse au lecteur le soin de vérifier. Soient x, y éléments de K^* d'ordres respectifs e et f premiers entre eux, l'ordre de xy est ef. Il existe donc un élément $x \in I\!F_q^*$ dont l'ordre est le plus petit commun multiple α des ordres de tous les éléments.
D'une part $\forall u \in I\!F_q^*\ ,\ u^\alpha = 1$, d'autre part $\forall u \in I\!F_q^*\ ,\ u^{q-1} = 1$, α étant d'après sa définition le plus petit entier vérifiant cette propriété, on a $\alpha \leq q-1$. Le polynôme $X^\alpha - 1$ ayant au plus α racines distinctes dans le corps $I\!F_q^*$, on a $q-1 \leq \alpha$ ce qui entraîne l'égalité entre ces deux nombres. Ceci démontre que x engendre le groupe multiplicatif $I\!F_q^*$, tout élément de ce groupe est donc une puissance de x qui est appelé élément primitif du corps $I\!F_q$. On peut remarquer que $I\!F_q = I\!F_p[x]$.

Théoreme 2.6 *Pour tout entier n et tout nombre premier p il existe un polynôme irréductible de degré n sur $I\!F_p$.*

Démonstration.
Soit $q = p^n$ et ξ un élément primitif de $I\!F_q$. $I\!F_q = I\!F_p[\xi]$.
Soit $f(X)$ le polynôme minimal de ξ sur $I\!F_p$.

$$I\!F_q = I\!F_p[\xi] \simeq I\!F_p[X]/(fX)) \text{ et } [I\!F_q : I\!F_p] = n$$

entraîne $d^o f = n$ et le polynôme $f(X)$ est irréductible sur $I\!F_p$ en tant que polynôme minimal d'un élément.

Exemple.
Soit $f(X) = X^2 + X + 2$ polynôme à coefficients dans $I\!F_3$. Ce polynôme est irréductible sur $I\!F_3$ car il n'admet aucun zéro, $f(0) = 2,\ f(1) = 1,\ f(2) = 2$.
$I\!F_9 \simeq I\!F_3[X]/(f(X))$.
Soit α une racine de f dans $I\!F_9$, montrons que α est un élément primitif de $I\!F_9$.
On a $\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha^2 = -\alpha - 2 = 2\alpha + 1$. (dans $I\!F_3\ -1 = 2$).
$\alpha^3 = 2\alpha^2 + \alpha = 2(2\alpha+1) + \alpha = 2\alpha + 2$.
$\alpha^4 = 2\alpha^2 + 2\alpha = 2(2\alpha+1) + 2\alpha = 2$.
$\alpha^5 = 2\alpha$.
$\alpha^6 = 2\alpha^2 = 2(2\alpha+1) = \alpha + 2$.
$\alpha^7 = \alpha^2 + 2\alpha = 2\alpha + 1 + 2\alpha = \alpha + 1$.
$\alpha^8 = \alpha^2 + \alpha = 2\alpha + 1 + \alpha = 1$.

Théoreme 2.7 (Caractérisation d'un sous corps) *Un corps fini $I\!F_{p^r}$ est un sous corps du corps fini $I\!F_{p^n}$ si et seulement si $r|n$.*

Démonstration.
Supposons $I\!F_{p^r}$ sous corps de $I\!F_{p^n}$, ce dernier est alors un espace vectoriel sur $I\!F_{p^r}$ qui est lui même un espace vectoriel sur $I\!F_p$. Les dimensions vérifient

$$[I\!F_{p^n} : I\!F_p] = n = [I\!F_{p^n} : I\!F_{p^r}] \underbrace{[I\!F_{p^r} : I\!F_p]}_{=r}$$

ce qui montre que $r|n$.
Réciproquement supposons que $r|n$, c'est à dire $n = rs$, ceci entraîne
$p^{rs} - 1 = (p^r - 1)(p^{r(s-1)} + p^{r(s-2)} + \cdots 1)$ autrement dit $p^r - 1|p^n - 1$ ce qui entraîne que $X^{p^r-1} - 1|X^{p^n-1} - 1$ et donc $X^{p^r} - X|X^{p^n} - X$. Tout zéro de $X^{p^r} - X$ est zéro de $X^{p^n} - X$. Le corps $I\!F_{p^n}$ qui est le corps de décomposition de $X^{p^n} - X$ contient donc le corps de décomposition de $X^{p^r} - X$ qui est de cardinal p^r. Ce sous corps d'ordre p^r est unique, sinon ce dernier polynôme aurait plus de p^r racines dans un corps.

Groupe de Galois de $I\!F_{q^m}$ sur $I\!F_q$.

Théoreme 2.8 *Il existe m automorphismes distincts de $I\!F_{q^m}$ qui laissent le sous corps $I\!F_q$ invariant. Ils sont définis par $\sigma_j(x) = x^{q^j}$, $0 \leq j \leq m-1$. Ils forment un groupe appelé groupe de Galois de $I\!F_{q^m}$ sur $I\!F_q$.*

Démonstration.
Les σ_j sont bien des morphismes de corps laissant $I\!F_q$ invariant, ce sont donc également des applications $I\!F_q$-linéaires, elles sont injectives et donc bijectives car $I\!F_{q^m}$ est fini. Ces applications sont deux à deux distinctes, car si ξ est un élément primitif de $I\!F_{q^m}$

$$\xi^{q^j} \neq \xi^{q^i} \ , \ i \neq j \ , \ 0 \leq i, j \leq m-1.$$

Montrons que tout automorphisme σ de $I\!F_{q^m}$ laissant $I\!F_q$ invariant est un des σ_i. Soit $f(X)$ le polynôme minimal de ξ sur $I\!F_q$. Ce polynôme étant a coefficients dans $I\!F_q$, on a

$$\sigma_i((fX)) = f(X) \ , \ 0 \leq i \leq m-1$$

ses zéros sont donc $\xi, \xi^q, \cdots \xi^{q^{m-1}}$, l'automorphisme σ laisse également $f(X)$ invariant et $\sigma(\xi)$ étant zéro de $f(X)$, on a donc $\sigma(\xi) = \xi^{q^i} = \sigma_i(\xi)$ pour un $i \in \{0, 1, \cdots, m-1\}$, la définition de ξ entraîne $\sigma = \sigma_i$.

2.4 Exercices.

Exercice 1.

1)Montrer que les polynômes $f(X) = X^2 + 1$ et $g(X) = X^2 + X + 4$ sont irréductibles sur $\mathbb{F}_{11}$. On note

$$K = \mathbb{F}_{11}[X]/(f(X)) \ , \ L = \mathbb{F}_{11}[X]/(g(X)).$$

2) Soient α et β deux éléments respectivement de K et L ayant le même polynôme minimal, de degré deux, sur $\mathbb{F}_{11}$. Montrer que

$$\phi\{ \begin{array}{c} \mathbb{F}_{11}[\alpha] \to \mathbb{F}_{11}[\beta] \\ a + b\alpha \to a + b\beta \end{array} \ , \ a, b \in \mathbb{F}_{11}$$

est un isomorphisme de K sur L.
3) Déterminer deux éléments α et β ayant les propriétés précédentes.

Exercice 2.

Déterminer tous les éléments primitifs de $\mathbb{F}_7$, $\mathbb{F}_{19}$ et $\mathbb{F}_9$, dans le dernier cas il est nécessaire de bien définir les éléments de ce corps.

Exercice 3.

1) Déterminer un polynôme irréductible, de degré deux sur $\mathbb{F}_5$.
2) En écrivant tous les éléments de $\mathbb{F}_{25}$ sous la forme $a + b\xi$, $a, b \in \mathbb{F}_5$, et ξ zéro du polynôme précédent, déterminer un élément primitif β de $\mathbb{F}_{25}$ et écrire tous les éléments de $\mathbb{F}_{25}$ sous la forme $\alpha = \beta^n$.

Exercice 4.

Soit p un entier premier et $q = p^n$. On définit une application, appelée trace, de $\mathbb{F}_q$ dans $\mathbb{F}_p$ par

$$Tr : \left\{ \begin{array}{lcl} \mathbb{F}_q & \to & \mathbb{F}_p \\ \alpha & \to & \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \end{array} \right.$$

1) Calculer $(Tr(\alpha))^p$, en déduire que $Tr(\alpha) \in \mathbb{F}_p$. Montrer que Tr est une application $\mathbb{F}_p$-linéaire surjective. Calculer $Tr(b)$ si $b \in \mathbb{F}_p$ et vérifier que
$\forall \alpha \in \mathbb{F}_q$, $Tr(\alpha^p) = Tr(\alpha)$.
2) Montrer que $Tr(\alpha) = 0 \Leftrightarrow \exists \beta \in \mathbb{F}_q \ , \ \alpha = \beta^p - \beta$.

Exercice 5.

1) On définit la relation suivante sur $K = \mathbb{F}_{p^n}$

$$x \equiv y \Leftrightarrow \exists i \in \{0, 1, \cdots, n\} \ , \ y = x^{p^i}.$$

Montrer que c'est une relation d'équivalence.
2) $K = \mathbb{F}_{16}$ est engendré sur $\mathbb{F}_2$ par w zéro du polynôme irréductible

X^4+X+1. Vérifier que w est un élément primitif de K. Déterminer les classes d'équivalence, pour la relation définie dans la question précédente, en fonction de w.
3) On revient aux conditions de la question 1. Soit $x \in K$, $\{x, x^p, \cdots, x^{p^{s-1}}\}$ la classe d'équivalence de x. On définit le polynôme

$$P_x(X) = \prod_{j=0}^{s-1}(X - x^{p^j}) = \sum_{i=0}^{s-1} a_i X^i$$

Vérifier que $(P_x(X))^p = P_x(X^p)$ et que ceci entraîne
$\forall i \in \{0, 1, \cdots, s-1\}$ $a_i \in I\!F_p$.
4) Montrer que si $P(X)$ est le polynôme minimal de x sur $I\!F_p$, $x, x^p, \cdots, x^{p^{s-1}}$ sont racines de $P(X)$. En déduire que $P_x(X) = P(X)$. Montrer que si x engendre K on a $Tr(x) = -a_1$ où $P(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$.
5) Soit $\{P_x(X) | x \in U\}$ l'ensemble des polynômes minimaux distincts des éléments de K. Montrer que

$$X^{p^n-1} - 1 = \prod_{x \in U} P_x(X).$$

6) Déterminer les polynômes minimaux distincts dans $I\!F_{16}$.

Chapitre 3

Codes Linéaires.

3.1 Généralités.

Soit A un ensemble fini non vide, appelé alphabet.

Définition 3.1 *On définit la distance de Hamming sur A^n par*

$$d(x,y) = d((x_1, x_2, \cdots, x_n), (y_1, y_2, \cdots, y_n)) = card\{i \in \{1, \cdots, n\} | x_i \neq y_i\}$$

On peut vérifier sans difficulté que d a les propriétés d'une distance sur l'ensemble A^n.

Théoreme 3.1 *Un code sur A de longueur n est un sous ensemble C de A^n. Les éléments de C sont appelés les mots du code.*

Remarque.
Lorsqu'on utilise un code pour transmettre des messages, si $x = (x_1, x_2, \cdots, x_n)$ est le mot envoyé et $x' = (x'_1, x'_2, \cdots, x'_n)$ le mot reçu, le nombre d'erreurs commises sur les composantes du mot est $d(x, x')$. La finalité des codes correcteurs d'erreurs est de détecter et de corriger ces erreurs. Le principe consiste à transmettre en plus du mot un certains nombres de lettres (de bits) redondantes permettant de reconstituer le mot à l'arrivée.
Schématiquement

$$(x_1, x_2, \cdots, x_k) \rightarrow_{encodeur} (x_1, \cdots, x_k, \cdots x_{k+n})$$

$$\rightarrow canal \ \ bruite \rightarrow$$

$$(y_1, \cdots, y_{k+n}) \rightarrow_{decodeur} (y_1, \cdots, y_k).$$

L'encodeur transforme le mot transmis en un mot du code utilisé.
Le rapport $k/(k+n)$ est appelé taux de transmission, n est appelé redondance.
Dans le canal bruité certains symboles de A peuvent être modifiés. Détecter une erreur, c'est déterminer si
(y_1, y_{k+n}) et $(x_1, \cdots, x_{k+n})$ sont égaux ou non.
Corriger une erreur, c'est après détection obtenir par décodage

$(y_1, \cdots, y_k) = (x_1, \cdots, x_k)$.

Les boules utilisées dans les définitions suivantes sont des boules fermées relatives à la distance de Hamming.

Définition 3.2
- — *Un code est e-détecteur ($e \in \mathbb{N}^*$) si toute boule centrée en un mot de code, de rayon e ne contient auncun autre mot de code.*
- — *Un code est e-correcteur si deux boules de rayon e, centrées en des mots de code différents ont une intersection vide.*
- — *Si C est un code, $d = \min\{d(a,b) \neq 0 | a \in C \ , \ b \in C\}$ est appelée distance minimale du code*

Théoreme 3.2 *Soit C un code de distance minimale d. Ce code est $(d-1)$-détecteur d'erreurs et $[\frac{d-1}{2}]$ correcteur.*

La vérification est immédiate.

Exemple.
$A = \mathbb{F}_2 = \{0, 1\}$, $n = 5$
$C = \{x = (0,1,1,1,0), y = (1,0,1,0,1), z = (1,1,0,1,1)\}$. La distance minimale $d = 3$, C est 1-correcteur, c'est à dire qu'il peut rectifier un mot pour lequel s'est introduit une erreur. Par exemple si le mot reçu est $(1,1,1,0,1)$, le mot envoyé est y dans le cas ou une erreur au maximum est possible au cours de la transmission. Déterminons maintenant une relation entre l'alphabet, la longueur du code et sa capacité de correction.

Théoreme 3.3 *Soit C un code de longueur n sur un alphabet A et de capacité de correction e, on a*

$$|C| \sum_{r=0}^{e} C_n^r (|A| - 1)^r \leq |A|^n$$

où $|X|$ représente le cardinal d'un ensemble X.

Démonstration.
On a

$$B(x, r) = \cup_{i=0}^{r} S(x, i)$$

où $S(x,i)$ est la sphère de centre x et de rayon $i \in \mathbb{N}$, car d, distance de Hamming est à valeurs dans $\mathbb{N}$.
$|S(x,i)| = C_n^i (|A| - 1)^i$ car cet ensemble représente le nombre de mots y dont i composantes diffèrent de celles de x. On a
$|B(x,r)| = \sum_{i=0}^{r} C_n^i (|A|-1)^i$ d'après le résultat précédent. Si C est e-correcteur, toutes les boules $B(x,e)$, $x \in C$ sont deux à deux disjointes et

$$\sum_{x \in C} |B(x,e)| \leq |A|^n \Leftrightarrow |C| \sum_{r=0}^{e} C_n^r (|A| - 1)^r \leq |A|^n$$

3.2 Codes Linéaires.

Dans la suite $A = I\!F_q$, $q = p^n$, p premier. On prend souvent $q = 2$.

Définition 3.3 *Le poids d'un mot* $x = (x_1, x_2, \cdots x_n) \in I\!F_q^n$ *est défini par* $w(x) = Card\{i \in \{1, \cdots, n\} | x_i \neq 0\}$

Cette fonction possède les propriétés suivantes
- $d(x, y) = w(x - y)$.
- $w(x) = d(x, 0)$.
- $w(x) = 0 \Leftrightarrow x = 0$.
- $\forall \lambda \in I\!F_q^*$, $w(\lambda x) = w(x)$.
- $w(x + y) \leq w(x) + w(y)$.

Définition 3.4 *Un code linéaire* (n, k, d) *sur* $A = I\!F_q$ *est un sous espace vectoriel de* A^n *de dimension* $k \leq n$ *et de distance minimale* d. *Il contient* q^k *mots.*

Remarque.
On a $d = \min\{w(x) | x \in C - \{(0, 0, \cdots, 0)\}\}$, en effet
$\{d(x, y) | (x, y) \in C^2\} = \{w(z) | z \in C\}$ en appelant C le code, car $d(x, y) = w(x - y)$ et $x - y \in C$, réciproquement $w(z) = d(z, 0)$, $0 \in C$, $z \in C$.

3.2.1 Matrice Génératrice.

Définition 3.5 *Une matrice génératrice d'un code linéaire* C *sur* A *est une matrice dont les lignes forment une base de* C.

Propriétés.
Les propriétés suivantes relèvent de l'algèbre linéaire élémentaire et sont données sans démonstration.
- Une matrice génératrice est une matrice $k \times n$ sur A, $k \leq n$, dont le rang est k.
- Toute matrice $k \times n$ sur A , de rang k est une matrice génératrice d'un code (n, k) sur A.
- Les matrices génératrices de C sont de la forme BGoù B est une matrice $k \times k$ inversible sur A et G une matrice génératrice.
- Le code C est l'ensemble des mots
  $m_u = (u_1, u_2, \cdots, u_k)G$ où $u = (u_1, u_2, \cdots, u_k) \in A^k$ et l'application $u \to m_u$ est un isomorphisme d'espace vectoriel.
- Si $(c_1, c_2, \cdots, c_n)$ sont les vecteurs colonnes de G, les mots du code C sont de la forme

$$m_u = ((c_1|u), (c_2|u), \cdots, (c_n|u)) \ , \ u \in A^k$$

  et $(.|.)$ représentant le produit scalaire usuel de A^k.

Exemple.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ est de rang 3}$$

Les mots du code sont
$C = \{(1,0,0,1,0),(0,1,0,1,1),(0,0,1,0,1),(1,1,0,0,1)(1,0,1,1,1),(0,1,1,1,0),$
$(1,1,1,0,0),(0,0,0,0,0)\}$
la distance minimale est $d = w(C) = 3$. C est un code linéaire $(5,3,3)$.

Définition 3.6 — *Deux codes C_1 et C_2 son téquivalents si les mots de C_2 sont obtenus à partir de ceux de C_1 par une même permutation.*
— *Un code linéaire de dimension k est dit systématique si la matrice formée par les k première colonnes de sa matrice génératrice est la matrice unité.*

En utilisant les opérations élémentaires sur les lignes et les colonnes d'une matrice, on obtient
— Tout code linéaire est équivalent à un code linéaire systématique.
— Si le code (n,k,d), C, est systématique, pour chaque $u = (u_1,\cdots,u_k) \in A^k$, il existe un mot et un seul de C de la forme $m_u = (u_1,\cdot,u_k,x_{k+1},\cdots,x_n)$. Les k premiers symboles sont appelés symboles d'information et les $n-k$ suivants, symboles de contrôle ou de redondance.

Exemple.
Soit C_1 le code linéaire de matrice génératrice

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

dont les vecteurs colonnes sont $c_1, c_2, \cdots c_6$.En les écrivant dans l'ordre $c_1, c_2, c_4, c_5, c_3, c_6$ la matrice devient

$$G' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

c'est la matrice d'un code équivalent à C_1 obtenu à partir de la permutation $\sigma = (3,4,5)$.
Soient l'_1, l'_2, l'_3, l'_4 les lignes de G' et soit G la matrice dont les lignes sont $l_1 = l'_2 + l'_3, l_2 = l'_1 + l'_2, l_3 = l'_1 + l'_2 + l'_3, l_4 = l'_2 + l'_4$, la matrice est alors

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Le code systématique C de matrice G est équivalent au code C_1. La matrice G permet de coder $2^4 = 16$ messages, chacun d'eux est associé à un élément $u = (u_1,u_2,u_3,u_4) \in I\!F_2^4$. Un mot de code s'écrit $uG = (u_1,u_2,u_3,u_4,u_1 + u_2, u_3 + u_4)$. Ce code est détecteur mais non correcteur d'erreur car son poids est 2.

3.2.2 Matrices de contrôle.

On définit sur $\mathbb{F}_q^n$ le produit scalaire
$x.y = (x|y) = \sum_{i=1}^{n} x_i y_i$, $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_n)$.

Définition 3.7 — *Soit C un code linéaire de paramètres (n, k, d), le code orthogonal de C est le sous espace vectoriel de A^n orthogonal à C, c'est un code de longueur n et de dimension $n - k$, il n'y a pas de relation simple entre d et le poids de ce code.*

— *On appelle matrice de contrôle de C toute matrice génératrice de son orthogonal.*

Propriété.
Le mot $(x_1, x_2, \cdots, x_n)$ appartient au code C de matrice de contrôle H si et seulement si
$H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Ceci exprime en effet que x est orthogonal aux lignes de cette matrice, donc à $C^\perp$ ce qui donne $x \in (C^\perp)^\perp = C$.

Remarque.
En appelant $c_1, c_2, \cdots, c_n$ les colonnes de H et en notant
$H^t x = \sum_{i=1}^{n} x_i c_i$ on obtient le résultat : Le code C contient un mot de poids r si et seulement si il existe une combinaison linéaire à coefficients non nuls de r colonnes de H qui est nulle.
Le poids minimum de C est donc le plus petit entier $r > 0$ vérifiant cette propriété.

Propriété.
Soit $G = [I_k, M]$ où I_k est la matrice unité $k \times k$ et M une matrice $k \times (n - k)$, la matrice génératrice d'un code C systématique. La matrice de contrôle est
$H = [{}^t M, -I_{n-k}]$.

Démonstration.
Soit $M = (v_{ij})_{1 \le i \le k \, , \, 1 \le j \le n-k}$. Le code étant systématique, un mot de code s'écrit
$x = (x_1, \cdots, x_k, x_{k+1}, \cdots, x_n) = (x_1, \cdots, x_k)G$, ce qui entraîne
$x_{k+j} = \sum_{i=1}^{k} v_{ij} x_i$, $1 \le j \le n - k$.
Ce qui exprime que x est orthogonal à la j-ième ligne de la matrice H. Le code C est donc inclus dans le code admettant H comme matrice de contrôle. Ces deux codes ayant même dimension sont identiques.

Principe de décodage d'un code linéaire.
Après avoir transmis un message codé à l'aide d'un code correcteur d'erreur, il est nécessaire de le décoder pour qu'il soit compréhensible. Soit H la matrice de contrôle d'un code linéaire C, $x \in C$, soit y le mot reçu.
$\epsilon = y - x$ est appelé vecteur d'erreur. On a l'équivalence
$y \in C \Leftrightarrow H^t y = 0$. Supposons C e-correcteur, si $y = x + \epsilon$, $H^t y = H^t \epsilon$ car $x \in C$.
Cette quantité $H^t \epsilon$ est appelée syndrome d'erreur de x. On peut remarquer que

$H^t y = H^t z \Leftrightarrow z - y \in C$.
Chaque élément d'une classe latérale $u + C$, $u \in A^n$ a donc le même syndrome d'erreur. La capacité de correction du code est $e = [\frac{d-1}{2}]$ et pour tout mot x non nul du code on a $w(x) \geq d$. Dans la suite on fait l'hypothèse que les mots reçus contiennent au plus e erreurs.

$$x \in C \ , \ w(\epsilon) \leq e \Rightarrow w(x + \epsilon) \geq d - \frac{d-1}{2} > e$$

On a donc

$$w(\epsilon) = \min\{w(x + \epsilon) | x \in C\}$$

Le vecteur d'erreur est l'unique mot de poids minimum d'un translaté de C.
L'algorithme de décodage peut se résumer comme suit

- Calcul du syndrome du mot reçu y.
- Détermination de la classe latérale associée.
- Recherche dans cette classe du mot erreur ϵ.
- Calcul de $x = y - \epsilon$.

Cet algorithme est mis en oeuvre en utilisant une table, dite table de décodage, des syndromes des mots erreurs, c'est à dire des mots dont le poids est au plus e.
Pour décoder on calcule le syndrome et on le cherche dans la table. On lit alors le mot erreur et on peut corriger.

Certains codes particuliers permettent de décoder tout mot de l'espace ambiant, on les appelle codes parfaits.

Définition 3.8 *Le code e-correcteur linéaire, de longueur n est dit parfait si*

$$A^n = \cup_{x \in C} B(x, e)$$

les boules $B(x, e)$ étant fermées.

Dans ce cas tout mot reçu peut être corrigé. Il y a peu de codes parfaits. L'un d'entre eux, le code de Hamming, marque le début des travaux concernant les codes correcteurs d'erreurs.

Définition 3.9 *Soient $A = \mathbb{F}_2$, $m > 1$. Le code de Hamming binaire est le code linéaire dont la matrice de contrôle, de dimension $m \times (2^m - 1)$ admet pour colonnes les éléments non nuls de $\{0, 1\}^m$.*

Exemple.

$$m = 3 \ , \ H_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

La matrice génératrice de ce code est

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

C'est un code $(7, 4, 3)$, il est donc 1-correcteur.

Théoreme 3.4 *Un code de Hamming a pour longueur* $2^m - 1$*, pour dmension* $2^m - m - 1$*, et pour capacité de correction* $e = 1$*. Un code de Hamming est parfait.*

Démonstration.
La longueur, correspondant au nombre de mots non nuls, est $2^m - 1$, son othogonal est de dimension n d'après la définition, le code est donc de dimension $2^m - m - 1$.
On utilise la remarque 3.2.2 Si le code contenait un mot de poids 1, la matrice de contrôle H contiendrait une colonne nulle, ce qui n'est pas le cas.
S'il contenait un mot de poids 2, il y aurait deux colonnes identiques, ce qui est faux.
c_i et c_j étant deux colonnes distinctes de H, $c_i + c_j$ est une autre colonne de H, c_l, l'égalité $c_i + c_j + c_l = 0$ montre que le poids du code est 3.
Posons $n = 2^m - 1$, $k = n - m$. On a
$2^n = 2^k 2^m = 2^k(n + 1)$.
Chaque boule de rayon 1 centrée en un mot du code contient $1 + C_n^1 = 1 + n$ mots. Le code contenant 2^k mots, il est donc parfait.

3.3 Exercices

Exercice 1

Déterminer tous les mots de codes, la distance minimale et la matrice de contrôle du code $[5, 3]$ sur $\mathbb{F}_2$ qui est défini par la matrice génératrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Exercice 2

Montrer que les codes de matrices génératrices G_1 et G_2 suivantes sont équivalents et donner leur forme systématique.

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \ , \ G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Exercice 3

On considère $f : \mathbb{F}_2^n \to \mathbb{R}$ et on note $(u|v)$ le produit scalaire canonique sur cet espace.
$(u|v) = \sum_{i=1}^{n} u_i v_i$ où $u = (u_1, u_2, \cdots, u_n)$, $v = (v_1, v_2, \cdots, v_n)$.
1) Soit C un code linéaire sur $\mathbb{F}_2^n$, montrer que

$$\sum_{u \in C} (-1)^{(u|v)} = \begin{cases} |C| & \text{si} \quad v \in C^{\perp} \\ 0 & \text{si} \quad v \notin C^{\perp} \end{cases}$$

On note $\hat{f}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{(u|v)} f(v)$. Montrer que

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).$$

2) On note $A_i = |\{u \in C | w(u) = i\}|$ et on appelle polynôme des poids du code C le polynôme à deux variables

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i.$$

En utilisant la question précédente, montrer que

$$W_{C^{\perp}} = \frac{1}{|C|} W_C(X + Y, X - Y).$$

3) $n = 4$, $C = \{(0, 0, 0, 0), (1, 1, 1, 1)$. Déterminer le polynôme des poids du code C, en déduire le polynôme des poids du code $C^{\perp}$ et en déduire les paramètres de ce code.

Exercice 4

Soit C_m le code de Hamming de longueur $n = 2^m - 1$ et de dimension $k = n - m$.
1) Montrer que tous les mots non nuls de $C_m^{\perp}$ ont le même poids 2^{m-1}.
2)Déterminer le polynôme des poids du code $C_m^{\perp}$, en déduire le polynôme des poids de C_m puis la distribution des poids de ce code C_m.

Chapitre 4

Codes Cycliques.

4.1 Définitions.

On pose $q = p^r$ où p est un nombre premier et $K = I\!F_q$. Dans la suite la longueur n d'un code linéaire vérifiera toujours $\text{pgcd}(q, n) = 1$.
En pratique, les codes cycliques sont les codes linéaires les plus importants. Pour une longueur n et un corps de base $I\!F_q$, on dispose d'un assez large choix de codes cycliques pour une capacité de correction et/ou une dimension.

Définition 4.1
— *Soit C un code linéaire de longueur n et σ une permutation de $\{1, 2, \cdots, n\}$. On dit que σ est un automorphisme du code C si $\sigma(C) = C$.*
— *Un code linéaire de longueur n sur K est un code cyclique si son groupe d'automorphismes (définis au dessus) contient le shift, c'est à dire la permutation $\sigma = (1, 2, \cdots, n)$, autrement dit le code est caractérisé de la façon suivante*

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

On dit que le code C est invariant par le shift.

4.2 Représentation Polynomiale.

A tout mot $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ on peut faire correspondre le polynôme

$$f(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

Le polynôme associé au shifté de c s'obtient en multipliant par X puis en posant $X^n = 1$. Formalisons cette définition en définissant un morphisme d'anneau

$$\Theta : \{ \begin{array}{l} K^n \to K[X]/(X^n - 1) \\ (c_0, c_1, \cdots, c_{n-1}) \to \sum_{i=0}^{n-1} c_i x^i \end{array}$$

où $x = \overline{X} = X + (X^n - 1)$, on a $x^n = 1$. L'image $\Theta(C)$ du code, qui est comme on le verra un idéal de $K[X]/(X^n + 1)$, est appelée représentation polynomiale de C.

Théoreme 4.1 *La représentation polynomiale du code cyclique C est un idéal principal de $K[X]/(X^n-1)$. Un code cyclique est dit primitif si $n = q^m - 1$ pour un entier positif m.*

Démonstration. Vérifions tout d'abord que deux mots de code distincts ont deux représentations polynomiales différentes.

$$\Theta(c_1) = \Theta(_2) \Leftrightarrow f(x) = g(x) \Leftrightarrow X^n - 1 | f(X) - g(X)$$

$$\Leftrightarrow f = g \ (d^o f \leq n-1 \ , \ d^o g \leq n-1) \Leftrightarrow c_1 = c_2.$$

Montrons que l'anneau $K[X]/(X^n-1)$ est principal. Rappelons d'abord qu'un idéal I de cet anneau est de la forme $J/(X^n-1)$ pour un idéal J contenant l'idéal (X^n-1). $K[X]$ étant principal on a $J = (g(X))$ pour un polynôme $g(X)|X^n-1$. L'idéal I est alors l'idéal principal engendré par $g(x)$.
$\Theta(C)$ est bien un idéal de $K[X]/(X^n-1)$ car il est stable par l'addition et par multiplication par x d'après la définition d'un code cyclique, car multiplier par x revient à considérer l'image du mot shifté. Il est donc stable par la multiplication par un polynôme quelconque.

Remarque.
Ce qui précède montre qu'un élément de $\Theta(C)$ s'écrit sous la forme
$h(x) = g(x)v(x)$ où h est un polynôme mutiple du polynôme g et de degré $\leq n-1$, on peut donc écrire $v(x) = \sum_{i=0}^{n-d^o g-1} \lambda_i x^i$. Le polynôme g est appelé polynôme générateur du code cyclique C.

Dimension et matrice génératrice d'un code cyclique.

Théoreme 4.2 *Soit C un code cyclique (n,k) sur $\mathbb{F}_q$ dont le polynôme générateur est g de degré t. Alors la dimension du code est $k = n-t$ et la matrice génératrice de C est*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_t & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{t-1} & g_t & \cdots & 0 \\ \vdots & \vdots & & & & & \vdots \\ 0 & 0 & \cdots & & & g_{t-1} & g_t \end{pmatrix}$$

où $g(X) = g_0 + g_1 X + \cdots + g_t X^t$.

Soit $h(x)$ la représentation polynomiale du mot de code c.

$$h(X) = \sum_{i=0}^{n-t-1} \lambda_i X^i g(X)$$

en gardant les notations précédentes. Or les $k = n-t$ lignes de G sont les coordonnées de

$$g(X), Xg(X), \cdots, X^{n-t-1} g(X)$$

dans la base canonique de $K_{n-1}[X]$, ensemble des polynômes a coeficients dans K et de degré inférieur ou égal à $n-1$.

4.3 Dual d'un code cyclique.

Remarque.
Soit $g(X)$ le polynôme générateur du code cyclique C, le polynôme $g(X)$ divise $X^n - 1$. En effet
$X^n - 1 = g(X)h(X) + R(X)$, $d^oR < d^og$, ceci entraîne $R(X) = 0$, sinon $R(X)$ serait dans $\Theta(C)$ et de degré strictement plus petit que le degré de $g(X)$, ce qui est impossible.

Définition 4.2 *Le polynôme $h(X)$ défini par $X^n - 1 = g(X)h(X)$ est appelé polynôme de contrôle de C.*
$d^oh = n - d^og = dimC = k$.

Théoreme 4.3 *Soit $h(X) = \sum_{i=0}^{k} h_iX^i$ le polynme de contrôle du code C, la matrice de contrôle de ce code s'écrit alors*

$$H = \begin{pmatrix} 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \\ 0 & \cdots & h_k & h_{k-1} & \cdots & h_0 & 0 \\ \vdots & & & & & & \vdots \\ h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \end{pmatrix}$$

Démonstration.

$$f(x) \in \Theta(C) \Leftrightarrow g(X)|f(X)$$

$$\Leftrightarrow h(X)f(X) \equiv 0 \ \text{ mod. } \ X^n - 1 \Leftrightarrow \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} f_j h_{i-j} \right) X^i = 0$$

les différences $i - j$ sont calculées modulo n.

$$\Leftrightarrow \forall i \in \{0, 1, \cdots, n-1\} \ \ \sum_{j=0}^{n-1} f_j h_{i-j} = 0$$

Ceci exprime que $f = (f_0, f_1, \cdots, f_{n-1})$ est orthogonal à chaque ligne de la matrice H, ce qui montre qu'il s'agit de la matrice de contrôle du code C.

Remarque.
Le polynôme générateur du code $C^\perp$ est

$$\tilde{h}(X) = \frac{X^k}{h_0} \, h(X^{-1}) \ , \ k = n - t \ , \ t = d^og.$$

4.4 Encodage.

La dimension du code étant $n-t$, les mots sources sont de la forme $u_0, u_1, \cdots, u_{n-t-1})$, on représente ce mot par le polynôme $u(X) = u_0 + u_1X + \cdots + u_{n-t-1}X^{n-t-1}$,
la matrice génératrice du code cyclique étant G, le mot de code correspondant au mot précédent est $(u_0, u_1, \cdots, u_{n-t-1})G$.

Exercice.
1) Montrer que le mot de code précédent s'obtient en calculant le produit $uX).g(X)$, g étant le polynôme générateur du code cyclique.
2)Vérifier que si

$$X^t u(X) = g(X)q(X)+r(X)\ , d^o r < n-t\ , X^t v(X) = g(X)q(X)+r'(X)\ , d^o r' < n-t$$

alors $u(X) = v(X)$.

4.5 Construction des codes cycliques.

On peut remarquer que le polynôme $X^n - 1$ n'a que des racines simples dans $I\!F_q$ car son polynôme dérivé nX^{n-1} ne s'annule que pour $X = 0$ car $\text{pgcd}(n, q) = 1$.
Déterminer tous les codes cycliques de longueur n sur $I\!F_q$, c'est déterminer tous les polynômes générateurs éventuels, c'est à dire les polynômes de $I\!F_q[X]$ qui divisent $X^n - 1$. On va présenter dans cette partie un méthode pratique de détermination de ces polynômes.

Soit $\phi(n)$ le nombre d'éléments inversibles de $Z\!\!Z/nZ\!\!Z$ (ϕ est appelée fonction d'Euler), q et n étant premiers entre eux q est un de ces éléments et on a donc $q^{\phi(n)} = 1$ d'après le théorème de Lagrange. Soit m le plus petit entier strictement positif tel que $q^m \equiv 1$ mod. n.
L'entier m est appelé ordre multiplicatif de q modulo n., c'est son ordre dans le sous groupe multiplicatif des éléments inversibles de $Z\!\!Z/nZ\!\!Z$.
On peut remarquer que c'est le plus petit entier $k > 0$ tel que $n|q^k - 1$, on en conclut que $L = I\!F_{q^m}$ est le corps de décomposition de $X^n - 1$, considéré comme polynôme de $I\!F_q[X]$, car L est la plus petite extension de $I\!F_q$ contenant toutes les racines de $X^n - 1$.

$$X^n - 1 = \prod_{\xi \in T} (X - \xi) \quad \text{sur L}$$

T est un ensemble contenant n éléments de L, ce sont les racines n-ièmes de l'unité dans L. On peut démontrer que ces racines n-ièmes forment un groupe cyclique pour le produit, une racine de l'unité engendrant ce groupe est appelée racine n-ième primitive de l'unité, il y en a $\phi(n)$.
Soit $g(X)$ un polynôme générateur d'un code cyclique, c'est un diviseur de $X^n - 1$, ses racines sont donc des racines de l'unités éléments de T, elles forment un sous ensemble T_g de T, déterminer tous les polynômes générateurs, c'est déterminer tous les sous ensembles T_g pour lesquels le polynôme associé est à coefficient est à coefficients dans $I\!F_q$. Quand cette condition est réalisée, l'ensemble T_g est appelé ensemble des zéros du code cyclique dont $g(X)$ est le polynôme générateur.

Théoreme 4.4 *Le polynôme*

$$g(X) = \prod_{\xi \in T_g} (X - \xi)$$

est à coefficients dans $\mathbb{F}_q$ si et seulement si T_g est stable par l'automorphisme de Frobenius

$$\sigma : \{ \begin{array}{l} \mathbb{F}_q \to \mathbb{F}_q \\ x \to x^q \end{array}$$

c'est à dire $\sigma(T_g) = T_g$.

Démonstration.
Supposons que $g(X) = \sum_{i=0}^{n-1} a_i X^i \in \mathbb{F}_q[X]$, on sait que le sous corps $\mathbb{F}_q$ de L est caractérisé par $\mathbb{F}_q = \{x \in L | x^q = x\}$.
Soit $\beta \in T_g$ une racine de g.

$$g(\sigma(\beta)) = \sum_{i=0}^{n-1} a_i (\beta)^{q^i} = \left(\sum_{i=0}^{n-1} a_i \beta^i \right)^q = (g(\beta))^q = 0$$

ce qui montre que $\sigma(\beta) \in T_g$, c'est à dire que T_g est stable par σ.
Réciproquement supposons T_g stable par σ.

$$(g(X))^q = \prod_{\beta \in T_g} (X^q - \beta^q) = \prod_{\beta \in T_g} (X^q - \beta)$$

c'est à dire

$$(g(X))^q) = g(X^q) = \sum_{i=0}^{n-1} a_i^q X^{qi} = \sum_{i=0}^{n-1} a_i X^{qi}$$

ce qui entraîne $\forall i \in \{0, 1, \cdots, n-1\}$ $a_i^q = a_i$ c'est à dire $g(X) \in \mathbb{F}_q[X]$.

Classes cyclotomiques.
On garde les notations précédentes, $L = \mathbb{F}_{q^m}$ est le corps de décomposition du polynôme $X^n - 1 \in \mathbb{F}_q[X]$. Soit $\alpha \in L$ une racine primitive n-ième de l'unité $T = \{1, \alpha, \cdots, \alpha^{n-1}\}$ ensemble des zéros de $X^n - 1$. On représente $\mathbb{Z}/n\mathbb{Z}$ par $\{0, 1, \cdots, n-1\}$ et on considère la bijection

$$F : \{ \begin{array}{lll} \mathbb{Z}/n\mathbb{Z} & \to & T \\ i & \to & \alpha^i \end{array}$$

Définissons une relation d'équivalence sur $\mathbb{Z}/n\mathbb{Z}$ qui permettra d'établir une condition nécessaire et suffisante pour qu'un polynôme, ayant un ensemble de zéros inclus dans T, soit à coefficients dans $\mathbb{F}_q$.
$i, j \in \mathbb{Z}/n\mathbb{Z}$, iRj si il existe un entier k tel que $j \equiv iq^k$ mod. n. C'est bien une relation d'équivalence, la symétrie, en particulier, étant vérifiée car
$q^m \equiv 1$ mod. n. Une classe d'équivalence pour cette relation est appelée classe cyclotomique modulo n.
La bijection F permet de définir une relation d'équivalence sur T et si $\alpha^i \in T$ sa classe d'équivalence est
$Cl(\alpha^i) = \{\alpha^i, \alpha^{iq}, \alpha^{iq^2}, \cdots, \alpha^{iq^{s-1}}\}$ où s est le plus petit entier positif tel que $iq^s \equiv i$ mod. n.
Soit

$$\Sigma \subset \mathbb{Z}/n\mathbb{Z} \text{ et } g_\Sigma(X) = \prod_{i \in \Sigma} (X - \alpha^i) \in L[X]$$

Déterminons une condition sur Σ pour que ce polynôme, qui divise $X^n - 1$, soit dans $I\!F_q[X]$.
Supposons que $g_\Sigma(X) \in I\!F_q[X]$ et que $i \in \Sigma$. D'après le théorème précédent, l'ensemble des zéros T_Σ de ce polynôme étant invariant par l'automorphisme de Frobénius σ, $Cl(\alpha^i) \subset T_\Sigma$, une condition nécessaire pour que ce polynôme soit à coefficients dans $I\!F_q$ est donc que Σ soit une réunion de classes cyclotomiques. Réciproquement, si cette condition est vérifiée, T_Σ est stable par σ et le polynôme g_Σ est à coefficients dans $I\!F_q$. On a démontré

Théoreme 4.5 *Le polynôme*

$$g_\Sigma(X) = \prod_{i \in \Sigma} (X - \alpha^i)$$

est à coefficients dans $I\!F_q$ si et seulement si Σ est une réunion de classes cyclotomiques modulo n.

Remarque.
Soit $i \in Z\!\!Z/nZ\!\!Z$ et Σ_i la classe cyclotomique de i modulo n. $g_{\Sigma_i} = \prod_{j \in \Sigma_i}(X - \alpha^j)$ est le polynôme minimal de α^i sur $I\!F_q$, car il est à coefficients dans $I\!F_q$ et de plus si g est le polynôme minimal de α^i on a $g(\alpha^{iq^k}) = (g(\alpha^i))^{q^k} = 0$, le polynôme g_{Σ_i} est donc un diviseur de g, étant à coefficient dans $I\!F_q$ il est égal à g.

Exemple.
prenons $q = 2$, $n = 5$. Déterminons l'ordre multiplicatif de 2 modulo 5.
$2^1 \equiv 2$ mod. 5, $2^2 \equiv 4$ mod. 5, $2^3 \equiv 3$ mod. 5, $2^4 \equiv 1$ mod. 5, l'ordre multipicatif de 2 modulo 5 est donc 4.
Le corps de décomposition de $X^5 - 1 \in I\!F_2[X]$ est $L = I\!F_{2^4} = I\!F_{16}$.
Soit β un élément primitif de $I\!F_{16}$

$$\beta^{15} = 1 \ \text{ et } \ \beta^k \neq 1 \ \text{ pour } \ 1 \leq k < 15.$$

$\alpha = \beta^3$ est une racine primitive cinquième de l'unité.
$X^5 - 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4)(X - 1)$ dans $I\!F_{16}[X]$.
Les classes cyclotomiques modulo 5 sont
$\{0\}$, $\{1, 2, 3, 4\}$. Il n'y a que deux polynômes générateurs, donc deux codes cycliques possibles de longueur 5 sur $I\!F_2$.

$$g_1 X) = X - 1 \ \text{ ou } \ g_2(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4) = \frac{X^5 - 1}{X - 1}.$$

$g_2 X) = X^4 + X^3 + X^2 + X + 1$. La remarque précédente montre que le polynôme $X^4 + X^3 + X^2 + X + 1$ est irréductible sur $I\!F_2$.

4.6 Exercices

Exercice 1

1) Déterminer l'ordre multiplicatif de 2 modulo 9. Déterminer les classes cyclotomiques de $\mathbb{Z}/9\mathbb{Z}$.
2) Décomposer $X^9 - 1$ en facteurs irréductibles dans $\mathbb{F}_2$. Combien existe t-il de codes cycliques de longueur 9 sur $\mathbb{F}_2$?

Exercice 2

1) Vérifier que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

$$\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)\ ,\ \alpha = \overline{X}.$$

α est-il un élément primitif de F_{16} ?
2) Quelle est la classe cyclotomique de 1 modulo 15. En déduire la factorisation de $X^4 + X + 1$ dans F_{16}.
3) Soit C le code cyclique de polynôme générateur $X^4 + X + 1$. Quelles sont sa dimension et sa distance minimale ?

Exercice 3

1) Combien existe t-il de codes cycliques de longueur 7 sur $\mathbb{F}_2$?
2) Vérifier que $X^3 + X + 1$ est le polynôme générateur d'un code cyclique de longueur 7 sur $\mathbb{F}_2$ et déterminer la matrice génératrice et la matrice de contrôle de ce code.

Exercice 4

Un code C est dit réversible si

$$(a_0, a_1, \cdots, a_{n-1}) \in C \Rightarrow (a_{n-1}, a_{n-2}, \cdots, a_1, a_0) \in C.$$

1) Montrer qu'un code cyclique de polynôme générateur $g(X)$ est réversible si et seulement si x racine de $g(X)$ entraîne $1/x$ racine de $g(X)$.
2) Montrer que si -1 est une puissance de q modulo n tout code cyclique sur $\mathbb{F}_q$ de longueur n est réversible.

Chapitre 5

Codes de Bose-Chaudury-Hocquenghem.

Les codes B. C. H. sont les codes cycliques de plus grande dimension pour une capacité de correction donnée. Cette capacité est controlée par une borne sur leur distance minimale, la borne B. C. H. La distance minimale est souvent supérieure à la borne.

5.1 Borne B. C. H.

Soit C un code cyclique de longueur n et m l'ordre multiplicatif de q modulo n.
$G = \mathbb{F}_{q^m}$ est le corps de décomposition de $X^n - 1 \in \mathbb{F}_q[X]$. Soit α un élément primitif de $\mathbb{F}_{q^m}$.
$n|q^m - 1$, ce que l'on peut écrire $q^m - 1 = nn'$, auquel cas $\beta = \alpha^{n'}$ est une racine primitive n-ième de l'unité dans G.
On appelle

$$g(X) = \prod_{i \in \Sigma} (X - \beta^i)$$

le polynôme générateur de C, l'ensemble Σ étant une réunion de classes cyclotomiques dans $\mathbb{Z}/n\mathbb{Z}$.

Théoreme 5.1 *Si l'ensemble Σ contient un sous ensemble*

$$\{\beta^l, \beta^{l+1}, \cdots, \beta^{l+\delta-2}\}$$

de $\delta - 1$ termes consécutifs, le code C a une distance minimale supérieure ou égale à δ. La plus grande valeur δ obtenue par ce procédé est appelée borne B. C. H. du code C.

Démonstration.
Soit $(x_0, x_1, \cdots, x_{n-1}) \in C$. Les β^i , $i \in \Sigma$ étant les zéros de ce code, le polynôme $\sum_{i=0}^{n-1} x_i X^i$ s'annule pour ces β^i, car ce polynôme est un multiple de $g(X)$. On

obtient

$$\left\{\begin{array}{lcl} x_0 + x_1\beta^l + x_2\beta^{2l} + \cdots + x_{n-1}\beta^{(n-1)l} & = & 0 \\ \vdots & \vdots & \vdots \\ x_0 + x_1\beta^{l+\delta-2} + x_2(\beta^2)^{l+\delta-2} + \cdots + x_{n-1}(\beta^{n-1})^{l+\delta-2} & = & 0 \end{array}\right.$$

Soit

$$V_i = \begin{pmatrix} (\beta^i)^l \\ \vdots \\ (\beta^i)^{l+\delta-2} \end{pmatrix}$$

le système s'écrit
$x_0V_0 + x_1V_1 + \cdots xn - 1V_{n-1} = 0$. Soit $V_{i_1}, V_{i_2}, \cdots, V_{i_{d-1}}$ $d-1$ vecteurs distincts choisis parmi $V_0, V_1, \cdots, V_{n-1}$. La matrice dont les colonnes sont formées de ces vecteurs est inversible car son déterminant est un déterminant de Van der Monde non nul. $d-1$ (ou moins de $d-1$) vecteurs sont donc toujours linéairement indépendants. Le système d'équations ne peut donc être résolu avec moins de d coefficients non nuls, le poids de x est donc au moins égal à d.

Notation.
On notera $M_x(X) \in \mathbb{F}_q[X]$ le polynôme minimal de $x \in \mathbb{F}_{q^m}$. On a vu (remarque suivant le théorème 4.5) que

$$g(X) = \prod_{i \in D} M_{\beta^i}(X)$$

où D contient un représentant au plus dans chaque classe cyclotomique de $\mathbb{Z}/n\mathbb{Z}$.

Définition 5.1 *Un code cyclique C de longueur n sur $\mathbb{F}_q$ est un code B. C. H. de distance construite δ si son polynôme générateur est le produit, sans répétition de facteurs, des plynômes minimaux de $\beta^{l+1}, \beta^{l+2}, \cdots, \beta^{l+\delta-1}$. Si $l = 0$ on dit que c'est un code B. C. H. au sens strict.*

Remarque.
Le code de Hamming est un code B. C. H. au sens strict, de distance construite 3 et de longueur $n = 2^m - 1$ sur $\mathbb{F}_2$. L'ordre multiplicatif de 2 modulo n est m et un élément primitif α de $\mathbb{F}_{2^m}$ est racine n-ième de l'unité. Une matrice de contrôle du code est formée des colonnes correspondant aux coordonnées de $1, \alpha, \cdots, \alpha^{n-1}$ dans une base de $\mathbb{F}_{2^m}$ sur $\mathbb{F}_2$. En notant
$C_0, C_1, \cdots, C_{n-1}$ les colonnes de cette matrice on a, pour un élément

$$f(X) = \sum_{i=0}^{n-1} f_i X^i \text{ du code } \sum_{i=0}^{n-1} f_i C_i = 0 \text{ ou } f(\alpha) = 0.$$

Ceci entraîne que $f(\alpha^2) = (f(\alpha))^2 = 0$.

Exemple.
$K = \mathbb{F}_2$, $n = 9$. L'ordre de 2 modulo 9 est 6, le corps de décomposition de

$X^9 - 1 \in \mathbb{F}_2[X]$ est $\mathbb{F}_{64}$ et $\beta = \alpha^7$ est une racine primitive 9 ième de l'unité.
Les classes cyclotomiques de $\mathbb{Z}/9\mathbb{Z}$ sont
$\{0\}$, $\{1, 2, 4, 8, 7, 5\}$, $\{3, 6\}$. On a
$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$.
$X^3 - 1 = (X - 1)(X^2 + X + 1) = (X - 1)(X - \beta^3)(X - \beta^6)$.
$X^6 + X^3 + 1 = (X - \beta)(X - \beta^2)(X - \beta^4)(X - \beta^8)(X - \beta^7)(X - \beta^5)$.
L'ensemble $\Sigma = \{0, 1, 2, 4, 8, 7, 5\}$ permet d'obtenir un code B.C.H. de distance construite $\delta = 4$. C'est un code B. C. H. au sens strict. Le polynôme générateur de ce code est
$g(X) = (X - 1)(X^6 + X^3 + 1) = X^7 + X^6 + X^4 + X^3 + X + 1$. C'est un code de dimension $k = 9 - 2 = 7$ et de matrice génératrice

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

La distance minimale de ce code est 6, elle est strictement supérieure à la distance construite.

5.2 Codes de Reed-Solomon.

Définition 5.2 *Un code de Reed-Solomon est un code B. C. H. sur $\mathbb{F}_q$, de longueur $n = q - 1$.*

Théoreme 5.2 *La distance minimale d'un code de Reed-Solomon est égale à la distance construite.*

Démonstration.
On remarque que toutes les classes cyclotomiques de $\mathbb{Z}/n\mathbb{Z}$ sont des singletons car $q \equiv 1$ mod. n.
Soit C un code B. C. H. de longueur $n = q - 1$ et de distance construite δ. Soit d sa distance minimale.
Son polynôme générateur est de la forme

$$g(X) = \prod_{i=1}^{\delta-1} (X - \alpha^{l+i})$$

chaque classe cyclotomique ne contenant qu'un élément. On a $d \geq \delta$, $d^o g(X) = \delta - 1$ donc $0 < w(g) \leq \delta$ ce qui nous donne bien $d = \delta$.

Exemple.
$K = \mathbb{F}_7$, $\alpha = 5$ est un élément primitif de $\mathbb{F}_7$.Le polynôme
$g(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^3)$ est le polynôme générateur d'un code de Reed-Solomon $[6, 3, 4]$.

5.3 Exercices

Exercice 1

Soient p un nombre premier, $q = p^n$, $K = I\!F_q$ et α un élément primitif de $I\!F_q$. On définit $K_{k-1}[X]$ l'ensemble des polynômes de degré inférieur ou égal à $k-1$ sur K, $k \leq q-2$,

$$C = \{(P(1), P(\alpha), \cdots, P(\alpha^{q-2}) | P \in K_{k-1}[X]\}.$$

1) Montrer que

$$\phi : \left\{ \begin{array}{ccc} K_{k-1} & \rightarrow & C \\ P & \rightarrow & (P(1), P(\alpha), \cdots, P(\alpha^{q-2})) \end{array} \right.$$

est un isomorphisme d'espace vectoriel. Quelle est la dimension de C ? Déterminer une base $\mathcal{B} = \{c_0, c_1, \cdots, c_{k-1})$ de C.
2) Soit

$$g(X) = (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^r)) \ , \ r = q-1-k.$$

On appelle C_2 le code de Reed-Solomon de polynôme générateur $g(X)$ sur K. Montrer que si $c_i(X)$ est la représentation polynômiale du vecteur c_i de la base $\mathcal{B}$ on a
$c_i(\alpha^v) = 0$ pour $1 \leq v \leq r$. En déduire que $c_0, c_1, \cdots, c_{k-1}$ sont dans C_2 et que $C_2 = C$.

Exercice 2

Vérifier que $\alpha = 5$ est un élément primitif de $I\!F_7$. On appelle C le code de Reed-Solomon sur $I\!F_7$ de polynôme générateur
$g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)$. Déterminer le polynôme générateur de $C^\perp$. En déduire que $C^\perp$ est un code de Reed-Solomon de mêmes paramètres que C.

Exercice 3

Vérifier que $X^2 + 2X + 2$ est irréductible sur $I\!F_3$.

$$I\!F_9 = I\!F_3[X]/(X^2 + 2X + 2) \ , \ \alpha = \overline{X}.$$

Montrer que α est un élément primitif de $I\!F_9$. Déterminer un polynôme générateur pour un code B.C.H. de longueur 8 et de dimension 4 sur $I\!F_3$. Déterminer la distance minimale de ce code. Déterminer une matrice génératrice et une matrice de contrôle de ce code.

Exercice 4

Déterminer le polynôme générateur d'un code B.C.H. de distance construite $\delta = 3$ sur $I\!F_2$ de longueur $n = 15$. On pourra vérifier que $X^4 + X^3 + 1$ est irréductible sur $I\!F_2$ et que α racine de ce polynôme est primitif dans $I\!F_{16}$.

Table des matières

1 Anneaux et idéaux. 1
- 1.1 Anneaux principaux. . . . 1
  - 1.1.1 Définitions. . . . 1
  - 1.1.2 Anneaux Principaux. . . . 2
- 1.2 Anneaux $\mathbb{Z}$ et $k[X]$. . . . 3
- 1.3 Exercices. . . . 5

2 Corps finis. 6
- 2.1 Caractéristique. Sous corps premier. . . . 6
- 2.2 Extensions de corps. . . . 7
- 2.3 Propriétés des corps finis. . . . 8
- 2.4 Exercices. . . . 11

3 Codes Linéaires. 13
- 3.1 Généralités. . . . 13
- 3.2 Codes Linéaires. . . . 15
  - 3.2.1 Matrice Génératrice. . . . 15
  - 3.2.2 Matrices de contrôle. . . . 17
- 3.3 Exercices 20

4 Codes Cycliques. 22
- 4.1 Définitions. . . . 22
- 4.2 Représentation Polynomiale. . . . 22
- 4.3 Dual d'un code cyclique. . . . 24
- 4.4 Encodage. . . . 24
- 4.5 Construction des codes cycliques. . . . 25
- 4.6 Exercices 28

5 Codes de Bose-Chaudury-Hocquenghem. 29
- 5.1 Borne B. C. H. . . . 29
- 5.2 Codes de Reed-Solomon. . . . 31
- 5.3 Exercices 32