Université Mohammed V - Agdal

Faculté des Sciences

Laboratoire de Mathématiques, Informatique et Applications

Master spécialisé Codes, Cryptographie et sécurité de l'information

Théorie des codes correcteurs d'erreurs I

El Mamoun SOUIDI

Année 2011

- - - - - - - - -

- - - -

-

Table des matières

Chapitre 1

Introduction à la théorie des codes [1]

1.1. Introduction

Cette théorie, initiée par Shannon en 1948 [**5**], traite la transmision de messages au travers d'un canal bruité ainsi que la détection et si possible la correction d'erreurs qui peuvent apparaître. Ce canal peut être une ligne téléphonique, une transmission radio, télévision, satellitaire, un périphérique d'enregistrement, clé USB, CD-ROM, DVD etc. Les erreurs peuvent être à cause des conditions climatiques, du matériel de transmission ou autres.

Un code est une transformation qui convertit la représentation d'une information en une autre pouvant être transmise à travers d'un canal de communication. Le codage est l'écriture d'un message au moyen de symboles d'un code. Le décodage est l'opération inverse, c'est à dire retrouver le message clair à partir de ces symboles.

Des codes permettent de détecter et/ou corriger des erreurs. Le principe est d'ajouter des redondances dans le message codé de telle façon que les erreurs puissent être détectées et corrigées.

1.2. Exemples de codes

1.2.1. Exemple 1 ISNB. Chaque livre est identifié par un numéro appelé ISNB (International Standard Number Book) formé de dix chiffres et parfois d'un x à la fin. Le premier chiffre représente la langue (0 pour l'anglais, 2 pour le français, 3 pour l'allemand ...), le bloc suivant de chiffre l'éditeur (Springer-Verlag en Allemagne : 540, aux États-Unis : 387, etc.), le suivant le numéro du livre chez l'éditeur. Le dixième est choisi de la façon suivante pour détecter les erreurs. Si $x_1x_2\cdots x_{10}$ est un ISBN, il doit vérifier $x_1+2x_2+\cdots+10x_{10}\equiv 0 \bmod 11$. Si x_{10} doit être égale à 10, on le note par x.

Si au lieu d'écrire x_k on écrit x_k+e par erreur alors $\sum_{i=1}^{10} ix_i = ke \not\equiv 0 \bmod 11$. On se rend compte alors qu'il y a erreur.

1. Pr. E. M. SOUIDI - souidi@fsr.ac.ma - Laboratoire de mathématiques, Informatique et Applications - Cours Master CSI - 2011/12 - Version 0.8 (Brouillon).

Dans le cas de deux erreurs : la formule de vérification est

$$1.x_1+\cdots+i(x_i+e_i)+\cdots+j(x_j+e_j)+\cdots+10x_{10} = \sum_{i=1}^{10} ix_i+ie_i+je_j = ie_i+je_j \mod 11$$

$ie_i + je_j$ peut être nul par exemple $1.3 + 8.1 = 0 \mod 11$ Il y a d'autre possibilités.

Si deux chiffres sont interverties alors $\sum_{i=1}^{10} ix_i = (k'-k)(x_k-x_{k'}) \not\equiv 0$. On se rend compte alors qu'il y a erreur aussi.

Supposons que la probabilité de saisir correctement un chiffre est $p = 0,98$. Alors la probabilité de saisir correctement un ISBN est $p^9 = 0,833$.

Si on utilise le dixième chiffre de correction la probabilité de saisir correctement un ISBN est (éventuellement après détection) $\geq\ p^{10} + 10p^9(1-p) = 0,983$.

1.2.2. Exemple 2. Nous avons à transmettre les réponses *oui* ou *non* au travers d'un canal bruité.

1) Si on code *oui* par 1 et *non* par 0. $C = \{0, 1\}$. Après transmission de 0 on peut recevoir 1 et 1 peut être reçu comme 0. Alors il n'y a aucun moyen de vérifier s'il y a erreur.

2) Si on code *oui* par 11 et *non* par 00. $C = \{00, 11\}$ Après transmission de 11, si on reçoit 11 on admet que c'est bon. Si on reçoit 01 ou 10 on constate qu'il y a erreur, car ces mots ne sont pas des mots de C. 00 est peut probable de le recevoir.

Dorénavant nous supposons que la probabilité de recevoir 0 et 1 en erreur est p ($< 1/2$) pour les deux symboles 0 et 1. La probabilité p est appelée probabilité d'erreur, elle dépend du canal de transmission et non du code.

3) Si on code *oui* par 111 et *non* par 000. $C = \{000, 111\}$. Après transmission de 111, si on reçoit 111 on admet que c'est bon. Si on reçoit 011, 110 ou 101 on constate qu'il y a erreur ce ne sont pas des mots de C. 000 est peut probable de le recevoir. Dans ce cas ce code peut détecter jusqu'à deux erreurs par mot. De plus il peut corriger s'il y a une seule erreur par mot :

111, 110, 101, 011 sont décodé comme 111.

000, 001, 010, 100 sont décodé comme 000.

S'il y a plus d'une erreur on obtient un résultat faux, mais la probabilité d'avoir plus d'une erreur est minime.

La probabilité de recevoir 111 en tant que 111 est $(1-p)^3$, en tant que 110, 101 ou 011 est $(1-p)^2p$. La probabilité de recevoir 111 en tant que 111, 110, 101 ou 011 est $P(C) = (1-p)^3 + 3(1-p)^2p = (1+2p)(1-p)^2$. Il en est de même pour 000.

La probabilité qu'un mot soit décodé faux est $P_{err}(C) = 1 - P(C)$ c'est une caractéristique de C et une fonction de p. $P_{err}(C) = (3-2p)p^2$.

Si $p = 0,1$ (en pratique p est plus petit) on a $P_{err}(C) = (3 - 0,2)0,01 = 0,028$ et $P(C) = 0,972$.

Si $p = 0,01$ on a $P_{err}(C) = 0,000298$ et $P(C) = 0,999702$.

Qu'en est-il si on prend $C = \{0000, 1111\}$? Certes $P_{err}(C)$ diminue mais ce code est moins efficace : le coût et le temps de transmission augmentent.

La probabilité d'erreur sur une ligne téléphonique est $p = 10^{-7}$, elle peut attendre 10^{-4}. Cette contrainte est mise en place au niveau de la couche 2, du modèle OSI : liaison de données.

1.2.3. Exemple 3. Le numéro de la sécurité sociale en France est formé de 15 chiffres, 13 chiffres d'identification qu'on note K et deux chiffres de redondance qu'on note C calculés de telle facon que $K + C$ soit un multiple de 97.

1.2.4. Code barre EAN. Le code EAN (European Article Numbering) est utilisé dans le commerce et l'industrie pour identifier de manière univoque des articles.

Le code EAN de 13 chiffres se décompose ainsi : Le premier chiffre isolé à gauche indique le pays où a été codifié l'article (3 pour la France, 4 pour l'Allemagne, 0 pour les USA . . .) ; Les 5 chiffres suivants permettent d'identifier le fabricant (CNUF, Code national unifié fournisseur) ; Les 6 chiffres suivants donne la référence du produit (CIF, Code interne fournisseur) ; Le dernier chiffre à droite est la clé de contrôle.

FIGURE 1. Un code barre

Ce code est composé de 13 chiffres $c_{12}c_{11}\cdots c_1c_0$. Les chiffres $c_{12}c_{11}\cdots c_1$ identifie le produit et c_0 est une redondance calculé de la façon suivante : on pose $a = \sum_{i=1}^{6} c_{2i}$ et $b = \sum_{i=1}^{6} c_{2i-1}$ d'où $c_0 = 10 - (a + 3b)\ mod\ 10$.

Ce code permet de détecter les erreurs mais ne les corrige pas.

1.2.5. Q-Code.

FIGURE 2. Un lecteur de QR-code affiche http ://www.souidi.net

Le QR Code (Quick Response Code) développé par en 1994 by Denso Wave pour l'industrie automobile au Japon, C'est un code à 2 dimensions qui permet de stocker des informations numériques (textes, adresses de site web, etc.).

DÉFINITION 1.2.1. *On appelle taux d'erreur la probabilité qu'un bit transmi par le canal soit différent du bit émis. C'est le rapport du nombre de bits erronés sur le nombre de bit transmis.*

1.3. Définitions de codes

On appelle alphabet de transmission un ensemble A de q (> 1) éléments qui peuvent être transmis au travers d'un canal de communication. Pour $n > 1$, on note les éléments de A^n, par $v_1 v_2 \cdots v_n$ et on les appelle mots ou vecteurs.

DÉFINITION 1.3.1. *Un code C de longueur n est une partie non vide de A^n. Ses éléments sont appelés mots du code.*

Si $q = 2$ ($q = 3$), C est appelé code binaire (trinaire) respectivement. Un code C est trivial si $|C| = 1$ ou $C = A^n$.

Un tel code, est aussi appelé code par bloc puisque tous ses mots sont de même longueur.

Rappelons qu'une distance sur un espace X est une application $d : X \to \mathbb{R}^+$ vérifiant pour tout x, y et z de X :
i) $d(x, y) = 0 \Leftrightarrow x = y$
ii) $d(x, y) = d(y, x)$
iii) $d(x, z) \leq d(x, y) + d(y, z)$

DÉFINITION 1.3.2. *Soit $x = x_1x_2 \cdots x_n$ et $y = y_1y_2 \cdots y_n$ deux éléments de A^n. La distance de Hamming entre x et y est définie par $d(x, y) = |\{i, \ / \ x_i \neq y_i\}|$.*

EXERCISE 1.4. *Dans $A = \{0, 1\}^3$ on a $d(110, 011) = 2$.*

EXERCISE 1.5. *Vérifier que la distance de Hamming est bien une distance.*

DÉFINITION 1.5.1. *La distance minimale d'un code C, notée $d(C)$ est définie par*

$$d(C) = min\,\{d(x, y) \ / \ x, y \in C, \ x \neq y\}$$

EXEMPLE 1.5.2. *Pour $C = \{000, 111\}$ on a $d(C) = 3$ et Pour $C = \{0000, 1110, 0111\}$ on a $d(C) = 2$.*

Le taux de correction d'un code C est définie par $\frac{d(C)}{n}$.
Le taux d'information ou rendement d'un code C est $R = \frac{k}{n}$, c'est le rapport de l'information utile sur l'information totale transmise à travers le canal.

DÉFINITION 1.5.3. *Deux codes $\mathcal{C}_1$ et $\mathcal{C}_2$ dans $\mathcal{A}^n$ sont équivalents si $\mathcal{C}_2$ est obtenu de $\mathcal{C}_1$ en appliquant à tous les mots de $\mathcal{C}_1$ une permutation fixe de coordonnées et à chaque coordonnées une permutation de l'alphabet.*

DÉFINITION 1.5.4. *Soit σ une permutation de $\{1, \cdots, n\}$ et $x = (x1, \cdots, xn)$ un mot de A^n ; on note : $\bar{\sigma}(x) = (x_{\sigma(1)}, \cdots, x_{\sigma(n)})$ On définit ainsi une permutation de A^n. On dit que deux codes C et C' sont équivalents, ssi, il existe une une permutation σ de $\{1, \cdots, n\}$ telle que : $C' = \bar{\sigma}(C)$.*

1.6. Capacité de détection et de correction d'un code

Supposons qu'on transmet un mot x d'un code C et qu' on reçoit y. Si $y \in C$, fort probablement $y = x$. Mais si $y \notin C$ il y a une ou plusieurs erreurs. Dans ce cas on décode y comme étant le mot $x' \in C$ le plus proche de y.
Par $[x]$ on note la partie entière du nombre réel x.

THÉORÈME 1.6.1. *Soit C un code de distance minimale d et $t = [(d-1)/2]$ alors :*

i) C peut détecter jusqu'à $d-1$ erreurs dans tout mot du code transmis.

ii) C peut corriger jusqu'à t erreurs dans tout mot du code transmis.

DÉMONSTRATION. Si un mot x est transmis et $y \neq x$ est reçu alors $d(x,y)$ est le nombre d'erreurs apparus lors de la transmission.

i) Si le nombre d'erreurs est $\leq d-1$ alors $d(x,y) < d$ d'où $y \notin C$ car $d(C) = d$. Donc au plus $d-1$ erreurs sont détectées. Si $d(x,y) \geq d$ alors y peut (ne pas) être un mot du code. Donc il est possible que plus de $d-1$ erreurs ne soient détectées.

ii) Supposons que le nombre d'erreurs est $\leq t$. Alors $d(x,y) \leq t$. x est le mot unique tel que $d(x,y) \leq t$. Soit $x' \in C$ tel que $d(x',y) \leq t$ alors $d(x,x') \leq d(x,y) + d(y,x') \leq 2t \leq d-1$ d'où $d(x,x') < d$ donc $x = x'$. Donc y est décodé comme étant x. Mais s'il y a plus de t erreurs alors un mot x' $(\neq x)$ de C peut être plus proche de y, dans ce cas le décodage est faux. □

Soit $\mathcal{C}$ un code de distance minimale d. Par $[x]$ on note la partie entière de x. L'entier $t = \left[\frac{d-1}{2}\right]$ s'appelle capacité de correction du code $\mathcal{C}$.

t est le plus grand entier tel que les sphères Hamming de rayon t centrées en des mots de $\mathcal{C}$ sont disjointes.

REMARQUE 1.6.2. *Si un code est t-erreurs alors sa distance minimale est $2t+1$ ou $2t+2$.*

Soit un code de longueur n, de distance minimale d et de cardinal M sur un alphabet à q éléments est noté (n, M, d)-code.

Les propriétés d'un "bon" code sont :

- petite longueur n (pour réduire le coût et la vitesse de transmission)
- M grand (pour pouvoir transmettre tout message)
- grande distance minimale (pour corriger plus de mots)

Ces propriétés sont liées entre elles. Par exemple pour n fixe et M grand, d est forcément petit.

Si on veut agrandir d, M se trouve réduit. Inversement, si on veut agrandir M, d se trouve réduit.

Le problème principale de la théorie des codes est le suivant : pour n et d donnés, trouver un code avec M le plus grand possible.

Soit $A_q(n,d)$ la plus grande valeur possible de M tel qu'il existe un (n, M, d)-code.

Un tel code est appelé code optimal si $M = A_q(n,d)$. Il est noté $(n,*,d)$-code. Tout code optimal est nécessairement maximal. On cherche une borne supérieure de $A_q(n,d)$.

EXERCISE 1.7. *Montrer que :*
$A_q(n,1) = q^n$ *et* $A_q(n,n) = q$.
Si d *est pair, alors* $A_2(n,d) = A_2(n-1,d-1)$.

1.8. Bornes sur les codes

Soit $u \in A^n$, un entier positif $r \leq n$ et $B_r(u) = \{v \in A^n \mid d(u,v) \leq r\}$ la boule de centre u et de rayon r. C'est l'ensemble des mots qui diffèrent de x en au plus r positions.

LEMME 1.8.1. *Soit* q *le nombre d'éléments de* A. *Le nombre des éléments de* $B_r(u)$ *est*

$$V_q(n,r) = \sum_{m=0}^{r} \binom{n}{m} (q-1)^m \tag{1}$$

DÉMONSTRATION. Soit $u = u_1u_2\cdots u_n$ et $v = v_1v_2\cdots v_n \in A^n$ pour m tel que $0 \leq m \leq r$ on considère $\{v \in A^n \mid d(u,v) = m\}$.

Il y a m indices i tels que $u_i \neq v_i$. Les m composantes peuvent être choisies de $\binom{n}{m}$ façons. Pour chaque indice i, v_i peut être choisi de $(q-1)$ façons. Donc le nombre de mots tels que $d(u,v) = m$ est $\binom{n}{m}(q-1)^m$. Doù le lemme. □

D'après le Lemme 1 $V_q(n,r)$ est indépendant du centre u de la boule $B_r(u)$.

REMARQUE 1.8.2. *Soit* $C \subset A^n$ *un code de distance minimale* d *et* $t = [(d-1)/2]$. *Les boules de rayon* t, *dont les centres sont des mots de* C, *sont disjointes deux à deux. En effet supposons qu'il existe un mot* $v \in B_t(u) \cap B_t(u')$ *où* $u, u' \in C$. *Alors* $d(u,u') \leq d(u,v) + d(v,u') \leq 2t < d$ *absurde car* d *est la distance minimale. En particulier l'union de toutes ces boules contient* $|C|\,.\,|B_t(u)|$ *mots.*

THÉORÈME 1.8.3. *Soit* $q \geq 2$, $n, d \in \mathbb{N}^*$ *et* $t = [(d-1)/2]$ *alors le nombre* $A_q(n,d)$ *de mots du code optimal vérifie*

$$\frac{q^n}{V_q(n,d-1)} \leq A_q(n,d) \leq \frac{q^n}{V_q(n,t)} \tag{2}$$

La première inégalité dans 2 s'appelle borne de Gilbert-Varshamov et la deuxième s'appelle borne de Hamming.

DÉMONSTRATION. Soit C un (n, M, d)-code optimal. C est alors maximal. Tout mot de A^n est de distance $\leq d-1$ d'un certain mot de C. En effet, (s'il existe un mot de A^n de distance $> d-1$ d'un mot de C, on peut ajouter ce mot à C, ce qui contredirait que C est maximal). La réunion des boules de rayon $d-1$ centrées en mots de C couvrent A^n, d'où $M.V_q(n, d-1) \geq q^n$ ce qui donne la première inégalité.

D'autre part, on a $2t+1 \leq d$. Les boules $B_t(x)$ où $x \in C$ sont disjointes d'où $M.V_q(n,t) \geq q^n$ ce qui donne la deuxième inégalité. □

PROPOSITION 1.8.4 (Inégalité de Singleton).

$$A_q(n,d) \leq q^{n-d+1} \tag{3}$$

DÉMONSTRATION. Il est facile de voir que $A_q(n,1) = q^n$. Nous montrons que pour tout n et $d > 1$ on a $A_q(n,d) \leq A_q(n-1,d-1)$. Soit $\mathcal{C}$ un (n, M, d)-code sur l'alphabet A de cardinal q. Il existe $c, c' \in C$ tels que $d(c,c') = d$, alors il existe un indice i pour lequel les composantes c_i et c'_i sont distinctes. A partir du code $\mathcal{C}$ on construit le code $\mathcal{C}'$ formé de tous les éléments de $\mathcal{C}$ auxquels on a supprimé la i^{eme} composante. Le code $\mathcal{C}'$ est de longueur $n-1$ et de distance minimale $d-1$. Si on considère le code C optimal, on a alors $|C| = A_q(n,d) = |C'| \leq A_q(n-1, d-1)$. D'où $A_q(n,d) \leq A_q(n-1,d-1) \leq \cdots \leq A_q(n-d+1,1) = q^{n-d+1}$ □

1.9. Codes Parfaits

Un code est dit parfait s'il ne contient aucune redondance inutile. Les codes parfaits sont utilisés dans la compression de données. Un code parfait est idéal pour décoder. en effet, tout mot reçu appartient à une et une seule boule de Hamming $B(c,t)$ $c \in C$ et t la capacité de correction du code C. Donc on peut décoder tout mot reçu affecté d'au plus t erreurs.

DÉFINITION 1.9.1. *Soit C un (q, n, M, d)-code. Alors C est parfait si*

$$M.\sum_{m=0}^{t} \binom{n}{m}(q-1)^m = q^n \tag{4}$$

En particulier un $(2, n, M, d)$-code est parfait si $M.\sum_{m=0}^{t}\binom{n}{m} = 2^n$.

Dans un code parfait tout mot reçu peut être décodé. En effet d'après l'équation 1.9.1 il découle que les boules centrées aux éléments de C et de rayon t sont disjointes deux à deux et forment une partition de A^n. Ainsi tout élément reçu $y \in A^n$ est dans une certaine boule $B_x(t)$ où $x \in C$ donc peut être décodé comme x.

Dans un code parfait tout mot de A^n est à une distance $\leq t$ d'un mot du code. Il s'en suit que la distance minimale d'un code parfait doit être un nombre impair.

La distance minimale d'un code parfait est un entier impair. En effet supposons $d(C) = 2t+2$. Soit $c \in C$ et $y \in A^n$ tels que $d(c,y) = t+1$. (on peut facilement construire un tel mot y). Il existe un $c' \in \mathbb{C}$ tel que $y \in B_{c'}(t)$ puisque C est un code parfait. D'où $d(c,c') \leq d(c,y) + d(c',y)t + 1 + t = 2t+1 < d$ ce qui contredit que d est la distance minimale de C.

REMARQUE 1.9.2. *Dans le cas d'un code parfait les boules de rayon t centrées aux éléments de C forment une partition de A^n. En particulier tout mot reçu est décodable.*

PROPOSITION 1.9.3. *Soit $C \subset A^n$ un code de distance minimale $d(C) = 2t+1$. Si pour tout mot $y \in A^n$, il existe $x \in C$ tel que $d(x,y) \leq t$ alors C est un code parfait.*

DÉMONSTRATION. Les $B_t(x)$ sont disjointes et $M.B_t(u) = q^n$ □

1.10. Exercices

Exercice 1. Pour chacun des QR-codes suivants apporter des modifications progressivement et tester sa lecteur à l'aide d'un lecteur QR-code de votre téléphone portable.



Exercice 2. Un code ISBN (International Standard Book Number) comporte dix chiffres $x_1x_2\cdots x_{10}$ structurés en quatre segments $A-B-C-D$ séparés par un tiret. Les neuf premiers chiffres $A-B-C$ identifient le livre : A identifie la communauté linguistique, B l'éditeur et C le numéro d'ouvrage chez l'éditeur. La clé de contrôle $D = x_{10}$ est un symbole de parité qui est, soit un chiffre entre 0 et 9, soit la lettre x qui représente 10. Cette clé x_{10} est telle que $\sum_{i=1}^{10} ix_i \equiv 0 \ \ mod\ 11$.

(1) Vérifier que 0-387-54894-7 (Introduction to Coding Theory de J. H. van Lint) est un code ISBN valide.

(2) Vérifier que 2-84225-007-1 n'est pas un ISBN valide. Peut-on le corriger ?

(3) Montrer que l'on peut détecter un chiffre inexact, ou l'interversion de deux chiffres dans un ISBN (en supposant qu'il n'y ait qu'une seule erreur de ce type).

Exercice 3. Le code de sécurité sociale française est formé de 13 chiffres contenant les informations suivantes :

- Sexe 1 :Homme, 2 :Femme ;
- Année de naissance sur deux chiffres ;
- Mois de Naissance sur deux chiffres ;
- Département de naissance, 99 si étranger ;
- Code INSEE (Institut national de la statistique et des études économiques) sur 3 chiffres de la commune ou du pays si étranger ;
- Numéro d'ordre INSEE de la personne sur 3 chiffres ;

en plus d'une clef de deux chiffres.

Si N est l'entier de 13 chiffres et c la clef, la contrainte de vérification est la relation

$$N + c \equiv 0 \ mod\ 97$$

(1) Quelle est la clef d'un individu dont le numéro de sécurité sociale serait 1-71-04-78-646-378 ?

(2) Un numéro de sécurité sociale est 2-xx-07-35-231-584, clé 19, mais les caractères xx sont illisibles. Pouvez-vous retrouver l'année de naissance de la personne en question ?

(3) Montrer que la clef de contrôle détecte une erreur sur un chiffre, ainsi que l'interversion de deux chiffres consécutifs.

(4) Montrer que 97 est un nombre premier et que n = 96 est le plus petit entier > 0 tel que $10^n \equiv 1 \ mod\ 97$.

(5) Montrer plus généralement que la clef de contrôle détecte l'interversion de deux chiffres quelconques.

Exercice 4. 1) Construire un code binaire de 4 mots de longueur 3 et de distance minimale 2.
2) Montrer qu'un code binaire de longueur 3 et de distance minimale 2 possède au plus 4 mots.

Exercice 5. On considère le code binaire C = {00000, 01101, 10110, 11011} (2 bits + bit de parité +répétition des deux premiers bits)
1. Calculer d(C).
2. Quel est le nombre maximum d'erreurs par mot que ce code peut détecter ? corriger ?
3. Faire la liste des mots binaires que ce code ne peut pas décoder.

Exercice 6. Montrer que $A_3(10, 6) \leq 120$.

Exercice 7. Montrer que si C est un $q-(3, M, 2)$-code alors $M \leq q^2$. Montrer que $A_q(3, 2) = q^2$ pour tout $q \geq 2$. et qu'un $q-(3, q^2, 2)$-code existe.

Exercice 8. Montrer que $A(2n, 2d) \geq A(n, d)$.

Exercice 9. Calculer $A(n, d)$ si $n = d$. Montrer que pour n impaire, ces codes sont parfaits.

Exercice 10. Montrer que si n est un multiple de 3 et $d = 2n/3$, alors $A(n, d) = 4$.

Exercice 11. Montrer que si $d > 2n/3$ alors $A(n, d) = 2$.

Exercice 12. Montrer

(1) Pour $n \geq 2$, $A_q(n, d) \geq qA_q(n-1, d)$.

(2) Pour un code binaire $A_2(n, 2t+1) = A_2(n+1, 2t+2)$.

(3) La borne d'empilement des sphères : pour $t = \left[\frac{d-1}{2}\right]$ on a $A_q(n, d) \leq \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k}(q-1)^k}$

(4) La borne de Plotkin : On pose $\theta = \frac{q-1}{q}$ si $d \geq \theta n$, alors $A_q(n, d) \leq \frac{d}{d-\theta n}$.

(5) Un code est parfait si l'égalité a lieu dans la formule d'empilement des sphères.

Exercice 13. Montrer qu'un code triaire de longueur 3 et de distance minimale 2 ne peut avoir plus de 9 mots. Montrer qu'un $(3, 9, 2)$-code triaire existe.

Exercice 14. Soit C un code de distance minimale $2t+2$. Si un mot v est à la distance $t+1$ d'un mot de C, montrer que v est à une distance $> t$ de tout mot de C.

Exercice 15. Soit C un code binaire de longueur 16 tel que :
i) tout mot du code est de poids 6 ;
ii) la distance entre deux mots quelconques du code est 8.
Montrer que $|C| \leq 16$. Existe-t-il un tel code avec $|C| = 16$?

Exercice 16. Montrer que si il existe un (n, M, d)-code binaire alors il existe un $(n-1, M', d)$-code binaire avec $M' \geq \frac{M}{2}$.

Exercice 17. Soit d un nombre entier impaire. Montrer qu'un (n, M, d)-code binaire existe si et seulement si un $(n+1, M, d+1)$-code binaire existe.

Exercice 18. Montrer que si les codes suivants existent, alors ils sont parfaits.

- le $(4, 9, 3)$-code triaire ;
- le $(2^r - 1, 2^{2^r - r - 1}, 3)$-code binaire où $r \in \mathbb{N}^*$;
- le $(23, 2^{12}, 7)$-code binaire ;
- le $(11, 3^6, 5)$-code triaire.
- le $(90, 2^{78}, 5)$-code binaire ;

Exercice 19. Montrer qu'un code C est parfait si pour tout $x \in A^n$ il existe un unique mot $c \in C$ qui réalise le minimum de $d(c, x)$.

Exercice 20. Montrer qu'il existe un $(8, 4, 5)$ code binaire et qu'il est optimal.

Exercice 21. Soit $q = 2$. Si $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n)$ on note $x * y = (x_1 y_1, \cdots, x_n y_n)$. Montrer que $\omega(x + y) = \omega(x) + \omega(y) - 2\omega(x * y)$

Exercice 22. Soit C un code binaire de longueur 5 et de distance 3 comportant le mot 00000.

1. Montrer que C comporte au plus 1 mot ayant au moins 4 symboles 1.

2. Combien C peut-il comporter de mots ayant exactement 1 ou 2 symboles 1 ?

3. Montrer que C a au plus 2 mots comportant exactement 3 fois le symbole 1.

4. En déduire que tout code de longueur 5 et de distance 3 a au plus 4 mots.

5. Construire un code de longueur 5 et de distance 3 ayant 4 mots. Ce code est-il unique ?

Exercice 23. Soit $C = \{00\cdots0, 11\cdots1\}$ un code binaire de longueur n impaire. C est parfait. Car tout $y \in \{0, 1\}^n$ est à une distance $\leq t = (n-1)/2$ de $00\cdots0$ ou $11\cdots1$.

Exercice 24. Soit un code C de longueur n sur un alphabet A. On appelle rayon de recouvrement du code C le plus petit rayon r tel que l'ensemble des boules de rayon r centrées en chaque mot du code forment un recouvrement de A^n. On le note $\rho(C)$.

Montrer qu'un code C est parfait si et seulement si sa capacité de correction est égal à son rayon de recouvrement.

Chapitre 2

Codes linéaires [1]

Dans ce chapitre on note par $\mathbb{F}_q$ ou $\mathbb{F}_q$ le corps fini à q éléments. Rappelons que le cardinal d'un corps fini est une puissance d'un nombre premier. Pour tout entier n, $\mathbb{F}^n$ est un $\mathbb{F}$-espace vectoriel de dimension n.

2.1. Définition

DÉFINITION 2.1.1. *Soit $\mathbb{F}$ un corps fini et n un entier > 0. Un code linéaire de longueur n et de dimension k sur $\mathbb{F}$ est un sous espace vectoriel de $\mathbb{F}^n$ de dimension k. Un tel code est noté $[n,k]$-code ou $[n,k,d]$-code quand on veut spécifier sa distance minimale. Si la distance minimale d'un code est d alors ce code est noté*

EXEMPLE 2.1.2. *$C = \{000, 111\}$ est un $[3,1]$-code linéaire sur le corps $\mathbb{Z}_2$.*

Le code binaire $C = \{000, 111, 011\}$ n'est pas linéaire car $111 + 011 = 100$ qui n'est pas un mot du code.

Soit C un $[n,k]$-code linéaire sur un corps $\mathbb{F}_q$. On a $|C| = q^k$. En effet puisque C est un espace vectoriel de dimension k, on sait que $C \simeq \mathbb{F}^k$. En particulier un $[n,k]$-code binaire a 2^k mots.

2.2. Matrice génératrice

C'est une des deux matrices importantes associées à tout code linéaire.

DÉFINITION 2.2.1. *Soit C un $[n,k]$-code linéaire. On appelle matrice génératrice de C toute matrice $k \times n$ dont les lignes forment une base de C.*

Il est facile de voir qu'un $[n,k]$-code C linéaire sur $\mathbb{F}$ est complètement déterminé par une matrice génératrice G de C. En plus

$$C = \left\{ v.G \mid v \in \mathbb{F}^k \right\} \tag{5}$$

1. Pr. E. M. SOUIDI - souidi@fsr.ac.ma - Laboratoire de mathématiques, Informatique et Applications - Cours Master CSI - 2007/08 - Version 0.1 (Brouillon).

Par exemple si $G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ est une matrice 2×3 alors

$$C = \{00.G = 000, 01.G = 111, 10.G = 101, 11.G = 010\}$$

.

La matrice G définie une bijection de $\mathbb{F}^k \to C$ par $v \mapsto vG$ et ainsi on représente q^k messages distincts par des mots du code C. Chaque mot de longueur k est codé par un mot de C de longueur n. Le nombre $n-k$ est appelé redondance du code C.

Une matrice génératrice G d'un code C n'est pas unique. Puisque les k colonnes de G sont linéairement indépendantes, en effectuant des opérations élémentaires sur les lignes, G peut être transformée en $G^* = \begin{pmatrix} I_k & \vdots & A \end{pmatrix}$ où I_k est la matrice identité d'ordre k et A est une matrice $k \times (n-k)$. Les lignes de G et G^* engendrent le même sous espace C. G^* est appelée matrice génératrice canonique de C.

Si un code linéaire C possède une matrice génératrice de la forme $\begin{pmatrix} I_k & \vdots & A \end{pmatrix}$, on dit que le code C est systématique.

Soit C un $[n,k]$-code linéaire sur un corps $\mathbb{F}$. Si $G = \begin{pmatrix} I_k & \vdots & A \end{pmatrix}$ est la matrice génératrice canonique de C. Alors $C = \left\{v.G \mid v \in \mathbb{F}^k\right\}$ et $v.G = v \vdots v.A$ on remarque que le codage ajoute $n-k$ symboles de redondance pour la détection d'erreurs par $v.A$.

EXERCISE 2.3. *Soit* $G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ *une matrice génératrice d'un code. Les mots de ce code sont* $00.G = 000$, $01.G = 101$, $10.G = 110$, $11.G = 011$

2.4. Code dual et matrice de contrôle

Rappelons que si $x = x_1 \dots x_n$, $y = y_1 \cdots y_n \in \mathbb{F}^n$ alors le produit scalaire de x et y est $x.y = x_1y_1 + \cdots + x_ny_n$. Les vecteurs x et y sont orthogonaux si $x.y = 0$.

DÉFINITION 2.4.1. *Soit* C *un* $[n,k]$*-code linéaire sur un corps* $\mathbb{F}$*. Le code dual de* C *est défini comme* $C^\perp = \{y \in \mathbb{F}^n \mid x.y = 0 \text{ pour tout } x \in C\}$.

$C^\perp$ est aussi l'ensemble des solutions du système $GX = 0$ où G est une matrice génératrice de C et X un vecteur inconnu, (car si $c \in C$, il existe $v \in \mathbb{F}^k$ tel que $c = vG$ d'où $cX = vGX = 0$).

REMARQUE 2.4.2.

$$kerG = C^\perp$$

Si G est de rang k alors $C^{\perp}$ est un sous espace vectoriel de $\mathbb{F}^n$ de dimension $n-k$.

THÉORÈME 2.4.3. *Soit C un $[n,k]$-code linéaire de matrice génératrice G. Alors :*
1) $C^{\perp} = Ker(G)$ 2) $C^{\perp}$ est un $[n, n-k]$-code linéaire.
3) $\left(C^{\perp}\right)^{\perp} = C$.

DÉMONSTRATION. 1) Soit $x \in \mathbb{F}^n$, $Gx = 0$ si et seulement si x est orthogonal à chaque lignes de G. Or, les lignes de G forment une base de C. Donc $Gx = 0$ si et seulement si $x \in C^{\perp}$
2) D'après le théorème du rang.
3) Soit $x \in C$, alors si $x.y = 0$ pour tout $y \in C^{\perp}$ on déduit que $x \in \left(C^{\perp}\right)^{\perp}$. Or si C est de dimension k alors $C^{\perp}$ est de dimension $n-k$ d'où $dim\left(C^{\perp}\right)^{\perp} = n-(n-k) = k$. On a $C \subset \left(C^{\perp}\right)^{\perp}$ et sont de même dimension donc sont égaux. □

EXERCISE 2.5. *Trouver le code dual du code de répétition de longueur n : $\{0\cdots 0, 1\cdots 1\}$.*

DÉFINITION 2.5.1. *Un code C est auto-orthogonale si $C \subset C^{\perp}$.*

EXERCISE 2.6. *Le dual du $[4,1]$-code binaire linéaire $C = \{0000, 1111\}$ est*

$$C^{\perp} = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$$

qui est un $[4,3]$-code et $C \subset C^{\perp}$ ie C est auto-orthogonal.

DÉFINITION 2.6.1. *Soit C un $[n,k]$-code linéaire, une matrice génératrice du code dual $C^{\perp}$ est appelée matrice de contrôle ou matrice de parité du code C.*

La matrice génératrice d'un code C linéaire est la matrice de contrôle du code $C^{\perp}$.

Si H est une matrice de contrôle de C, on a $x \in C \Leftrightarrow Hx^t = 0$ càd $C = kerH$ ce qui veut dire que la matrice de contrôle détermine complètement le code. D'où :

THÉORÈME 2.6.2. *Soit C un $[n,k]$-code linéaire sur un corps $\mathbb{F}$ de matrice génératrice G et H une matrice de contrôle du code C. On a :*
i) $C = \left\{xG \ : \ x \in \mathbb{F}^k\right\} = Im(G)$.
ii) $C = \{x \in \mathbb{F}^n \mid x.H^t = 0\} = Ker(H)$.
iii) $GH^t = 0$ et $HG^t = 0$.
vi) Inversement, si G est une matrice $k \times n$ de rang k et H est une matrice $(n-k) \times n$ de rang $n-k$, tel que $GH^t = 0$. Alors H est une matrice de contrôle de C si et seulement si G est une matrice génératrice de C.

DÉMONSTRATION. i) et ii) sont immédiats.

iii) D'après ii) où on prend en particulier $G^i H^t = 0$ où les G^i sont les lignes de G.

vi) Supposons que $GH^t = 0$ et H est une matrice de contrôle. Si on note par G_i les lignes de G alors $G_i H^t = 0$ pour tout i d'où $G_i \in C$. Puisque le rang de G est k, les G_i, $i = 1 \cdots k$ sont linéairement indépendants, d'où ils forment une base de C donc G est une matrice génératrice de C.

De même pour l'inverse. □

EXERCISE 2.7. *Trouver le code linéaire et binaire C de matrice de contrôle.* $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

COROLLAIRE 2.7.1. *Soit C un $[n,k]$-code linéaire et $G = \begin{pmatrix} I_k & \vdots & A \end{pmatrix}$ une matrice génératrice canonique de C. Alors $H = \begin{pmatrix} -A^t & \vdots & I_{n-k} \end{pmatrix}$ est une matrice de contrôle de C. Inversement, si $H = \begin{pmatrix} B & \vdots & I_{n-k} \end{pmatrix}$ est une matrice de contrôle de C alors $G = \begin{pmatrix} I_k & \vdots & -B^t \end{pmatrix}$ est une matrice génératrice de C.*

EXERCISE 2.8. *On considère le code binaire $C = \{000, 111\}$. Une matice génératrice de C est $G = (1,1,1)$. Le code dual de C est $C^\perp = \{000, 110, 101, 011\}$ d'où la matrice de contrôle de C est $H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$.*

DÉFINITION 2.8.1. *Soit C et C' deux $[n,k]$-codes linéaires sur un corps $\mathbb{F}$. Les codes C et C' sont équivalents s'il existe une bijection $f : C \to C'$ donnée par $f(x_1, \cdots, x_n) = \left(\alpha_1 x_{\sigma(1)}, \cdots, \alpha_n x_{\sigma(n)}\right)$ où $\alpha_1, \cdots, \alpha_n \in \mathbb{F}^*$ et σ est une permutation de l'ensemble $\{1, \cdots, n\}$.*

THÉORÈME 2.8.2. *Soit C et C' deux $[n,k]$-codes linéaires sur un corps $\mathbb{F}$ de matrices génératrices G et G' respectivement. Les codes C et C' sont équivalents si l'une des matrices peut être obtenue de l'autre en effectuant les opérations suivantes :*

1) opérations élémentaires sur les lignes

2) permutation de colonnes,

3) multiplication d'une colonne par un scalaire non nul de $\mathbb{F}$.

Preuve : en exercice.

2.9. Distance minimale

DÉFINITION 2.9.1. *Le poids d'un mot $x \in \mathbb{F}^n$ noté $\omega(x)$ est défini comme étant égale au nombre de composantes non nulles de x.*

Si $x, y \in \mathbb{F}^n$ alors $d(x,y) = \omega(x-y)$

THÉORÈME 2.9.2. *Soit C un code linéaire, la distance minimale de C est*

$$d(C) = min\{\omega(x) \mid x \in C,\ x \neq 0\}.$$

DÉMONSTRATION. Soit $d(C) = d$. Il existe $c, c' \in C$ tel que $d(c,c') = d$. D'où $c - c' \in C$ et $\omega(c-c') = d$. Soit $x \in C$ et $x \neq 0$ alors $\omega(x) = \omega(x-0) = d(x,0) \geq d$. Ce qui prouve que d est le plus petit poids de tout mot $\neq 0$ de C.

Soit C un code à m éléments. La distance minimale de C est obtenue :

- si C est linéaire on cherche le minimum de $m-1$ poids de mots ;
- sinon on cherche le minimum de $m(m-1)/2$ distances entre les différents éléments de C.

Pour décrire un $[n,k]-$code linéaire il suffit de donner une base de C.

□

THÉORÈME 2.9.3. *Soit H une matrice de contrôle d'un $[n,k]$-code linéaire sur un corps $\mathbb{F}$. Alors $d(C)$ est égale au nombre minimale de colonnes de H linéairement dépendantes. Par conséquent $d(C) \leq n - k + 1$.*

DÉMONSTRATION. Soit $X^1, \cdots, X^n$ les colonnes de H et $x \in \mathbb{F}^n$. $x \in C \Leftrightarrow Hx^t = x_1X^1 + \cdots + x_nX^n = 0$. Soit $d(C) = d$. Alors $\omega(x) \geq d$ et il existe un $c \in C$ tel que $\omega(c) = d$, on note par $c_{i_1}, \cdots, c_{i_d}$ les composantes non nulles de c. Alors $Hc^t = c_1X^1 + \cdots + c_nX^n = c_{i_1}X^{i_1} + \cdots + c_{i_d}X^{i_d} = 0$ c'est à dire que H a d vecteurs linéairement dépendants. Supposons qu'il existe $r(<d)$ vecteurs $X^{i_1}, \cdots, X^{i_r}$ linéairement dépendants. Alors il existe $\alpha_1, \cdots, \alpha_r$ non tous nuls tels que $\alpha_1X^{i_1} + \cdots + \alpha_rX^{i_r} = 0$. Soit $x \in \mathbb{F}^n$ dont les composantes $i_1, \cdots, i_r$ soient égales à $\alpha_1, \cdots, \alpha_r$ respectivement et toutes les autres nulles. $Hx^t = 0$ et $x \in C$ mais $\omega(x) < d$ contradiction.

d est le nombre minimal de colonnes linéairement dépendantes de H et c'est une matrice $(n-k) \times n$ de rang $n-k$ d'où tous $n-k+1$ colonnes de H sont linéairement dépendants donc $d \leq n-k+1$. □

COROLLAIRE 2.9.4. *Soit H une matrice de contrôle d'un $[n,k]$-code linéaire. La distance minimale est d si et seulement si*
i) d colonnes quelconques de H sont linéairement indépendants, et
ii) il existe d colonnes de H linéairement dépendants.

THÉORÈME 2.9.5 (Borne de Singleton). *La distance minimale d d'un $[n,k]$-code linéaire sur $\mathbb{F}_q$ est majorée par :*

$$d \leq n-k+1 \tag{6}$$

DÉMONSTRATION. Soit E le sous-espace vectoriel de $\mathbb{F}_q^n$ formé par les vecteurs dont les $k-1$ dernières composantes sont nulles. On a $dim(E) = n-k+1$ et $dim(E) + dim(C) = n+1 > n$. Il existe un $x \in E \cup C$ non nul. Puisque $a \in E$ on a $\omega(a) \leq n-k+1$ et puisque $a \in C$ on a $d(C) \leq \omega(a) \leq n-k+1$.

La Borne de Singleton impose à un $[n,k]$-code linéaire de distance minimale d d'avoir au moins $n-k \geq d-1$ chiffres de redandances. □

DÉFINITION 2.9.6. *Un $[n,k]$-code linéaire est dit MDS si il atteint la Borne de Singleton 6 càd $d = n-k+1$. MDS (maximum separable distance) peut se traduire par : plus grande distance minimale.*

EXERCISE 2.10. *Quelle est la distance minimale du code binaire C $[n,n-1]$-code linéaire de matrice de contrôle $H = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}$? Le nombre minimal de vecteurs colonnes linéairement dépendants est deux, d'où $d(C) = 2$.*

Quelle est la distance minimale du $[10,9]$-code linéaire C sur le corps $\mathbb{F}_{11}$ de matrice de contrôle $H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$? On a $d(C) = 2$.

Ce code est utilisé dans le traitement des ISBN. Voir chapitre précédant.

EXERCISE 2.11. *Quelle est la distance minimale du $[10,8]$-code C sur le corps $\mathbb{F}_{11}$ de matrice de contrôle $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$?*

On remarque que deux colonnes quelquonques sont linéairement indépendantes. D'où $d > 2$ et $d \leq n-k+1 = 3$ donc C est un code correcteur d'une seule erreur.

PROPOSITION 2.11.1 (Borne de Plotkin). *Soit C un $[n,k]$-code linéaire sur $\mathbb{F}_q$. Alors la distance minimale d de C vérifie*

$$d \leq \frac{n(q-1)q^{k-1}}{q^k-1} \tag{7}$$

DÉMONSTRATION. C contient q^k-1 vecteurs non nuls de poids minimal d. D'où la somme de leur poids est $d(q^k-1)$. Soit C_1 le sous-espace vectoriel de C dont la première composante de ses vecteurs est 0. On a $C/C_1 \equiv \mathbb{F}_q$, d'où $|C_1| = q^{k-1}$. Donc il y a $q^k - q^{k-1}$ vecteurs dont la première composante est non nulle. En tout il y a n composantes, donc $d(q^k-1) \leq n(q^k-q^{k-1})$. □

2.12. Décodage

Dans cette section nous traitons le décodage des codes linéraires. Le principe générale de décodage est de trouver le mot du code le plus proche du mot reçu. La structure algébrique de ces codes permet de construire une table à cette fin.

2.12.1. Décodage par table standard. Soit C un sous espace vectoriel de $\mathbb{F}^n$. En particulier C est un sous groupe de $\mathbb{F}^n$. Pour $x \in \mathbb{F}^n$ par définition $x + C = \{x + c \,|\, c \in C\}$. $x + C$ est appelé classe de x. Deux éléments x et y de $\mathbb{F}^n$ sont dans la même classe si $x - y \in C$. Ces classes forment une partition de $\mathbb{F}^n$.

THÉORÈME 2.12.1. *Soit $C \subset \mathbb{F}^n$ un code linéaire et $y \in \mathbb{F}^n$. Le mot x du code C le plus proche de y est donné par $x = y - e$ où e est le mot de plus petit poids dans la classe de y.*

DÉMONSTRATION. Pour tout $c \in C$, $d(y, x) \leq d(y, c)$ ie $\omega(y - x) \leq \omega(y - c)$. D'où $y - x$ est le vecteur de poids minimal dans la classe de y. □

DÉFINITION 2.12.2. *Soit C un code linéaire dans $\mathbb{F}^n$. Un représentant d'une classe de C est un vecteur de poids minimal de cette classe.*

Soit C un $[n, k]$-code linéaire sur un corps $\mathbb{F}_q$. Puisque $\left|\mathbb{F}_q^n\right| = q^n$ et chaque classe de C a q^k éléments alors il y a $N = q^{n-k}$ classes dans C. Soit $e_1, \cdots, e_N$ leurs représentants. Supposons que $\omega(e_i) \leq \omega(e_{i+1})$ pour $i = 1, \cdots, N-1$. Soit $e_1 = 0$ le représentant de la classe $C+0 = C$. Soit $C = \{c_1, \cdots, c_G\}$ où $G = q^k$ et $c_1 = 0$. On peut arranger les q^k vecteurs dans une table, appelée table standard, $N \times G$ où $e_i + c_j$ est le terme dans (i, j). Les termes de la i^e ligne sont les éléments de $e_i + C$, avec les e_i en premier. La première ligne est formée des mots du code C.

$$\begin{array}{ccccccc}
e_1 = 0 = c_1 & c_2 & \cdots & c_j & \cdots & c_G \\
e_2 & e_2 + c_2 & \cdots & e_2 + c_j & \cdots & e_2 + c_G \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
e_i & e_i + c_2 & \cdots & e_i + c_j & \cdots & e_i + c_G \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
e_N & e_N + c_2 & \cdots & e_N + c_j & \cdots & e_N + c_G
\end{array}$$

Pour décoder le mot reçu $y \in \mathbb{F}^n$. On cherche sa position dans la table. Si y est le terme (i, j) de la table alors $y = e_i + c_j$. Puisque e_i est de plus petit poids il s'en suit que le mot du code le plus proche de y est $x = y - e_i = c_j$. Donc le mot reçu y et décodé comme le premier mot de la colonne où apparait y.

REMARQUE 2.12.3. *Les e_i ne sont pas unique car si $C = \{0000, 1111\}$ alors la classe de* 1100 *est* $\{1100, 0011\}$ *qui a deux mots de même poids.*

EXERCISE 2.13. *Ecrire le tableau standard du code binaire de matrice génératrice* $G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ *et décoder le mot reçu* 01111.

Le code généré est $C = \{00000, 01011, 10101, 11110\}$. *Il y a* $2^3 = 8$ *classes. Il y a 8 lignes dans le tableau standard. La distance minimale est* 3 *et* $t = 1$. *Les cinq mots de poids* 1 *produisent* 5 *classes. On choisit 2 mots de poids 2 qui ne sont pas apparus dans les lignes précédentes.*

00000	*10101*	***01011***	*11110*
10000	*00101*	*11011*	*01110*
01000	*11101*	*00011*	*10110*
00100	*10001*	***01111***	*11010*
00010	*10111*	*01001*	*11100*
00001	*10100*	*01010*	*11111*
11000	*01101*	*10011*	*00110*
10010	*00111*	*11001*	*01100*

Pour décoder le vecteur 01111, on remarque qu'il est dans la 3e ligne. Il est décodé comme 01011.

Pour n grand, cette méthode n'est pas convenable. On décrit une autre méthode ci-dessous.

2.13.1. Décodage par syndrome.

DÉFINITION 2.13.1. *Soit C un $[n, k]$-code linéaire sur un corps $\mathbb{F}$ de matrice de contrôle H. Pour tout $y \in \mathbb{F}^n$, le syndrome de y est définie par $S(y) = yH^t$.*

D'après 2.6.2 on sait que $S(y) = 0 \Leftrightarrow y \in C$. Soit $y, y' \in \mathbb{F}^n$ alors $S(y) = S(y') \Leftrightarrow (y - y')H^t = 0 \Leftrightarrow y - y' \in C$. D'où deux mots ont même syndrome si et seulement si ils sont dans la même classe de C. Il y a une bijection entre les classes de C et les syndromes. On établit une table à deux colonnes, et sur chaque ligne un représentant d'une classe et son syndrome. Pour décoder un mot y reçu, on calcule son syndrome $S(y)$ et on cherche le représentant e tel que $S(y) = S(e)$. Alors y est décodé comme $x = y - e$. Cette procédure est appelée décodage du syndrome.

EXERCISE 2.14. *Traitons l'exemple précédent à l'aide de cette procédure.*

Une matrice de contrôle est $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$. *On calcule* eH^t *pour tout représentant.*

représentant	***syndrome***
10000	*101*
01000	*011*
00100	*100*
00010	*010*
00001	*001*
11000	*110*
10010	*111*

$S(y) = yG^t = 100$. *On utilisant le tableau, y peut être décodé comme* $x = y - e = 01011$.

2.14.1. Identités de MacWilliams. Soit $\mathcal{C} \subset \mathbb{F}^n$ un code linéaire. La distribution de poids de $\mathcal{C}$ est le vecteur $\mathcal{A}(\mathcal{C}) = (\mathcal{A}_0, \mathcal{A}_1, \cdots, \mathcal{A}_n)$ où

$$\mathcal{A}_i = |\{c \in \mathcal{C} \mid \omega(c) = i\}|$$

c'est à dire que la i^eme composante de $\mathcal{A}(C)$ est le nombre de mots de $\mathcal{C}$ de poids i. On note que $\mathcal{A}_0 = 1$

La distribution de distance est $\mathcal{B}(\mathcal{C}) = (\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_n)$ où

$$\mathcal{B}_i = \frac{1}{|\mathcal{C}|} |\{(c_1,\ c_2) \in \mathcal{C} \times \mathcal{C} \mid d(c_1, c_2) = i\}|$$

$\mathcal{B}_i$ est le nombre moyen de mots du code situé à la distance i de $\mathcal{C}$

Le polynôme-énumérateur est $A(X) = \sum_{i=0} n\mathcal{A}_i X^n$

EXEMPLE 2.14.1. *Pour* $C = F_q^n$ *on* $\mathcal{A}_i = \binom{n}{i}(q-1)^i$

REMARQUE 2.14.2. *Dans le cas de codes linéaires* $\mathcal{A}(\mathcal{C})$ *et* $\mathcal{B}(\mathcal{C})$ *coïncident. En général non.*

THÉORÈME 2.14.3. *Soit* $\mathcal{C}$ *un* $[n,k]$*-code linéaire sur* $\mathbb{F}_q$ *de polynôme énumérateur* $A(X) = \sum_{i=0} n\mathcal{A}_i X^n$. *Le polynôme énumérateur du code dual* $\mathcal{C}^\perp$ *est*

$$B(z) = q^{-k}(1 + (q-1)X)^n A\left(\frac{1-z}{1+(q-1)z}\right) \tag{8}$$

EXERCISE 2.15. *Montrer que pour le code de Hamming binaire* $\mathcal{H}_m$ *on :*

i)

$$i\mathcal{A}_i = \binom{n}{i-1} - A_{i-1} - (n-i+2)A_{i-2}$$

ii) En déduire $A'(z) = (1+z)^n - A(z) - nzA(z) + z^2A'(z)$, $A(0) = 1$.

THÉORÈME 2.15.1. *Soit* $\mathcal{C}$ *un code linéaire de longueur* n. *On note* $\mathcal{B}^\perp = \mathcal{B}(\mathcal{C}^\perp)$ *alors*

$$\mathcal{B}_j^\perp = \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n}\mathcal{B}_j P_j^n(i)$$

où

$$P_j^n(i) = \sum_{\ell=0}^{j}(-1)^\ell \binom{i}{\ell}\binom{n-i}{j-\ell}$$

est le polynôme de Krawtchouk de degré j.

DÉMONSTRATION. □

2.16. Rayon de couverture

Le rayon de couverture (Covering radius) est un paramètre fondamental des codes. Il caractérise la capacité maximale de correction d'erreur. Les codes de petits rayons de couverture s'appliquent en compression de données.

DÉFINITION 2.16.1. *Soit* $\mathcal{C}$ *un code dans* $\mathcal{A}^n$, *le rayon de couverture est le plus petit entier* ρ *tel que pour tout* $x \in \mathcal{A}^n$ *il existe* $c \in \mathcal{C}$ *tel que* $d(x,c) \leq \rho$ *c'est à dire*

$$\rho = \rho(\mathcal{C}) = \max_{x\in\mathcal{A}^n} d(x,c) = \max_{x\in\mathcal{A}^n}\min_{c\in\mathcal{C}} d(x,c)$$

Soit $\mathcal{C}$ un code. Le rayon de couverture de $\mathcal{C}$ noté $\rho = \rho(\mathcal{C})$ est le plus petit entier r tel que $\mathbb{F}_q^n$ est égal à la réunion des sphères centrées en mots de $\mathcal{C}$ et de rayon r. De façon équivalente

$$\rho(\mathcal{C}) = max_{x\in\mathbb{F}_q^n} min_{c\in\mathcal{C}} d(x,c)$$

Bien évidemment $t \leq \rho(\mathcal{C})$ et $d \leq 2\rho + 1$. Si $t = \rho(\mathcal{C})$ le corps $\mathcal{C}$ est parfait.

On a

$$\rho \geq min\{r : V_q(n,r).|\mathcal{C}| \geq q^n\}$$

où $V_q(n,r) = \sum_{i=0}^{r}\binom{n}{i}(q-1)^i$ est le volume de la sphère de Hamming.

Pour les codes linéaires nous avons :

THÉORÈME 2.16.2. *Soit* $\mathcal{C}$ *un code linéaire de matrice de contrôle* H. *Alors*
i) $\rho(\mathcal{C})$ *est le poids de l'orbite de* $\mathcal{C}$ *de plus grand poids ;*
ii) $\rho(\mathcal{C})$ *est le plus petit nombre* r *tel que le syndrome de tout vecteur de* $\mathbb{F}_q^m$ *est une combinaison d'au plus* r *colonnes de* H.

Le Rayon de couverture ρ du code $\mathcal{C}$ est aussi le plus petit entier tel que l'union des sphères Hamming de rayon ρ centrées en des mots de $\mathcal{C}$ est $\mathcal{A}^n$.

THÉORÈME 2.16.3. *Soit $\mathcal{C}$ un $[n,k]$-code linéaire binaire de matrice de contrôle H. $\rho(\mathcal{C})$ est le plus petit entier positif tel que tout $(n-k)$-uplet peut s'écrire comme somme d'au plus ρ colonnes de H.*

DÉMONSTRATION. Soit $x \in \mathbb{F}_2^n$ et $s = Hx^t$. Si la somme des colonnes $i_1, i_2, \cdots, i_t$ est égale à s, alors le vecteur obtenu en ajoutant 1 aux coordonnées $i_1, i_2, \cdots, i_t$ dans x appartient à $\mathcal{C}$ et inversement. Ce qui montre que $d(x, \mathcal{C})$ est le plus petit nombre de colonnes de H □

2.17. Construction de codes

La construction suivante introduite dans [**1**] s'appelle "Codes matrice produit". Elle permet de construire de nouveaux codes.

DÉFINITION 2.17.1. *Soit $\mathcal{C}_1$, $\mathcal{C}_2$, $\cdots$, $\mathcal{C}_M$ M codes linéaires de longueur n sur $\mathbb{F}_q$ et $A = (a_{ij})$ une matrice $M \times N$ à coefficients dans le corps $\mathbb{F}_q$. Le code matrice produit noté $[\mathcal{C}_1 \cdots \mathcal{C}_M].A$ est l'ensemble de tous les produits $[c_1 \cdots c_M].A$ où $c_i \in \mathcal{C}_i$ est un vecteur colonne $n \times 1$ pour $i = 1, \cdots M$.*

Les mots du codes $[\mathcal{C}_1 \cdots \mathcal{C}_m].A$ sont les matrices $n \times N$:

$$c = \begin{pmatrix} c_{11}a_{11} + \cdots + c_{1M}a_{M1} & \cdots & c_{11}a_{1N} + \cdots + c_{1M}a_{MN} \\ \vdots & \ddots & \vdots \\ c_{n1}a_{11} + \cdots + c_{nM}a_{M1} & \cdots & c_{n1}a_{1N} + \cdots + c_{nM}a_{MN} \end{pmatrix}$$

Le code $[\mathcal{C}_1 \cdots \mathcal{C}_m].A$ est un code de longueur $n.N$ et $c = (c_1, \cdots, c_{nN})$ où $c_k = \sum_{i=1}^{M} c_{hi}a_{ij}$, $h - 1 = (k-1) mod n$ et $j = 1, \cdots, N$

EXEMPLE 2.17.2. *Pour les codes $\mathcal{C}_1$ et $\mathcal{C}_2$ et la matrice*

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

on obtient le code $(u|u+v)$

EXEMPLE 2.17.3. *Pour les codes $\mathcal{C}_1$, $\mathcal{C}_2$ et $\mathcal{C}_3$ et la matrice*

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

on obtient le code $(u+v+w|2u+v)$

EXEMPLE 2.17.4. *Si A est la matrice identité d'ordre M alors $[\mathcal{C}_1 \cdots \mathcal{C}_M].A$ est la somme direct des codes $\mathcal{C}_1$, $\mathcal{C}_2$, $\cdots$, $\mathcal{C}_M$ M*

Si $\mathcal{C}_1$, $\mathcal{C}_2$, $\cdots$, $\mathcal{C}_M$ sont des codes linéaires de matrice génératrices G_1, G_2, $\cdots$, G_M respectivement alors $[\mathcal{C}_1 \cdots \mathcal{C}_M].A$ a pour matrice génératrice

$$G = \begin{pmatrix} G_1 a_{11} & \cdots & G_1 a_{1N} \\ \vdots & \ddots & \vdots \\ G_M a_{M1} & \cdots & G_M a_{MN} \end{pmatrix}$$

2.18. Exercices

Exercice 1. Montrer qu'un code linéaire à 20 mots ne peut exister.

Exercice 2. Soit C le code formé de tous les vecteurs de poids pairs de $\mathbb{F}_2^n$. Montrer que C est un code linéaire.

Exercice 3. Montrer que dans un code linéaire binaire, soit tous les mots sont de poids pairs ou exactement la moitié sont de poids pairs.

Exercice 4. Soit n un entier positif. Montrer qu'une condition nécessaire pour qu'il existe un code linéaire binaire parfait 1-correcteur de longueur n est que l'entier n soit de la forme $n = 2^r - 1$, où r est un entier positif.

Exercice 5. Soit C un code linéaire binaire.
1. Montrer que si C est de longueur 17 et de dimension 10, il ne corrige pas plus d'une erreur.
2. Montrer que si C est de longueur 10 et de distance minimale 3, alors $|C| \leq 64$.

Exercice 6. Soit C et C' deux codes linéaires binaires de même longueur. On défini $C + C' = \{x + x'/x \in C, x \in C'\}$. Montrer que $C + C'$ est un code linéaire et $(C + C')^{\perp} = C^{\perp} + C'^{\perp}$.

Exercice 7. Montrer si il existe un $[n, M, d]$ code linéaire binaire avec d paire alors il existe un $[n, M, d]$ code linéaire binaire dont tous les mots sont sont de poids paire.

Exercice 8. Soit $\mathbb{F}$ un corps fini, combien y a-t-il de mots de $\mathbb{F}^n$ de poids i ?

Exercice 9. Donner la distance de Hamming entre les mots 101101100010 et 101101010010 :
i) lorsqu'on les voit dans $\mathbb{F}_2^{12}$
ii) lorsqu'on les voit dans $\mathbb{F}_4^6$ où $\mathbb{F}_4$ est représenté par : $0 \to 00$, $1 \to 01$, $\alpha \to 10$, $\alpha + 1 \to 11$.

Exercice 10. Soit C_1 et C_2 deux codes linéaires dans $\mathbb{F}^n$. Montrer que $C_1 \cap C_2$ et $C_1 + C_2 = \{x_1 + x_2 \ / \ x_1 \in C_1,\ x_2 \in C_2\}$ sont des codes linéaires.

Exercice 11. Montrer que le code $C = \{0000, 1010, 0101, 1111\}$ est linéaire et auto-orthogonal.

Exercice 12. Montrer que le code binaire linéaire C de matrice génératrice

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

est auto-orthogonal. Trouvez le code dual de C.

Exercice 13. Trouvez la matrice génératrice canonique du $[4, 2]$-code ternaire linéaire de matrice de contrôle $M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$ et explicitez les mots du code.

Exercice 14. On considère le code binaire C dont la matrice génératrice est :

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

1. Donner tous les mots de C.
2. Donner la distance minimale de C, combien d'erreurs peut-on corriger ? Détecter ?

Exercice 15. On considère la matrice génératrice suivante d'un code C,

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

1) Déterminer les mots du code, la distance minimale du code, un tableau standard, la matrice de contrôle et la liste des syndromes de C.
2) Corriger et décoder les messages suivants : 01101, 10000.

Exercice 16. On considère le code C dont une matrice génératrice est

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

1) En utilisant la méthode de Gauss, mettez C sous forme systématique. En déduire une matrice de contrôle H pour C.
2) Calculer le syndrome du mot 1111000. Pouvez-vous le décoder ?

Exercice 17. Soit C le code linéaire sur $\mathbb{F}_5$ de matrice génératrice

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$$

1. Donner le nombre de mots de C.
2. Le code C est-il systématique ?
3. Déterminer une matrice de contrôle de C.
4. Calculer la capacité de correction t de C. Le code est-il MDS ?
5. Donner la table de contrôle contenant tous les vecteurs erreurs possibles de poids $\leq t$.
6. Décoder quand c'est possible les mots 3001, 1101 et 2311.

Exercice 18. Soit C le code linéaire sur $\mathbb{F}_3$ de matrice génératrice

$$G = \begin{pmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{pmatrix}$$

1. Montrer que C est systématique et en donner une matrice génératrice normalisée G'.
2. Encoder le message (12) avec G, puis avec G' .
3. Construire une matrice de contrôle de C et calculer sa distance minimale. Le code est-il MDS (Maximum Distance Separable) ?
4. On reçoit le message 11102 codé par G. Quel est le message d'origine ? Le mot 12121 est-il un mot de code ? Le décoder sachant qu'il a été encodé par G.

Exercice 19. Si C est un code linéaire de type (n, k, d), on définit le code étendu $\overline{C}$ comme le code formé des mots $(x_1, \cdots, x_{n+1}) \in F_2^n$ tels que $(x_1, \cdots, x_n) \in C$ et $\Sigma_{i=1}^{n+1} x_i = 0$. Quel est le type de C ?

Exercice 20. Soit un entier $r \geq 2$ et $Ham(2, r)$ le code de Hamming binaire de longueur $n = 2^r - 1$. Montrez que $Ham(2, r)$ est unique, dans le sens que tout code linéaire de paramètres $[2^r - 1, 2^r - 1 - r, 3]$ est équivalent à $Ham(2, r)$.

Exercice 21. Montrez que les matrices M et M' sont des matrices génératrices du même code si et seulement si $M = PM'$ où P est une matrice inversible.

Exercice 22. Soit C le code binaire linéaire de longueur 7 dont une matrice de contrôle est

$$H = \begin{pmatrix} 10000111010010110010110100011110 \end{pmatrix}$$

1. Combien valent la dimension et la distance de C ? Écrire une matrice génératrice de C.
2. Décoder les mots reçus $r_1 = 00001110$ et $r_2 = 00010011$, en supposant qu'il y a eu au plus une erreur de transmission.
3. Parmi les mots $t_1 =????0000$, $t_2 =?0?0?0000$ et $t_3 =?0?0?0?0$ qui ont subi des effacements, les autres bits ayant été transmis correctement, lesquels peut-on décoder ?
4. Le code C est-il MDS ? Cyclique ? Parfait ?
5. Montrer que, pour tout mode de code m de C, le mot $m + 11111111$ appartient à C. En déduire le nombre de mots de C de poids 4.
6. Montrer que C est équivalent au code étendu du code de Hamming Ham(8).
7. Montrer que C est son propre orthogonal.

Exercice 23. On considère le code binaire où on envoie 16 bits pour 9 bits significatifs de la manière suivante :
- on envoie les trois premiers bits p_1, p_2, p_3 suivis d'un bit de parité (paire) b_1,
- on envoie les trois bits s_1, s_2, s_3 suivants suivis d'un bit de parité (paire) b_2,
- on envoie les trois derniers bits d_1, d_2, d_3 suivis d'un bit de parité (paire) b_3,
- on envoie un paquet de 4 bits de contrôle c_1, c_2, c_3, c_4 où $c_1 = p_1 + s_1 + d_1$, $c_2 = p_2 + s_2 + d_2$, $c_3 = p_3 + s_3 + d_3$ et $c_4 = b_1 + b_2 + b_3$.

1. Montrer que ce code est linéaire, donnez sa matrice génératrice c'est à dire la matrice dont les lignes sont formées des images des vecteurs de base de $\mathbb{F}_2^9$.
2. Coder le mot 100111000.
3. On suppose avoir reçu le mot 0110101101100011. Retrouvez le mot envoyé.

Exercice 24. Trouvez le code dual du code binaire de répétition de longueur n.

Exercice 25. Trouez les matrices canoniques génératrice et de contrôle du code binaire de matrice génératrice $M = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Exercice 26. On dit que deux codes linéaires de même longueur sont équivalents si l'un s'obtient à partir de l'autre par une permutation des coordonnées. Vérifier que deux codes équivalents ont même type. Montrer que tout code est équivalent à un code donné par un codage systématique.

Exercice 27. On transmet des données par paquet de 16 bits, écrits dans un tableau 4 x 4, en ajoutant une ligne et une colonne de contrôle obtenue en associant à chaque ligne et chaque colonne son bit de parité.

a) Que pensez-vous des paquets reçus suivants :

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

b) Quels sont la longueur, la dimension et la distance du code décrit ?
c) Combien repère-t-il d'erreurs ? Combien en corrige-t-il ?
d) Si on ajoute en dernière position le bit de parité de la colonne

de contrôle, que deviennent la longueur, la dimension, la distance, le nombre d'erreurs repérées, corrigées du code ?

Exercice 28. i) Quel lien existe entre la dimension et la longueur d'un code 1-correcteur MDS ? i) Que peut-on dire des codes 1-correcteurs MDS parfaits sur le corps fini $\mathbb{F}_q$?

Exercice 29. Soit C le code de Hamming binaire de longueur 7.
1. Déterminer une matrice génératrice normalisée de C à l'aide de la méthode du pivot de Gauss. 2. En déduire une matrice de contrôle de C.
3. Décoder quand c'est possible les mots 1111111, 1101011, 0110110 et 1111010.

Exercice 30. Soit C le code binaire linéaire de matrice génératrice

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

1. Le code est-il systématique ?
2. Déterminer une matrice de contrôle et la capacité de correction de C.
3. Le code est-il MDS ?
4. Décoder si possible les mots 111110 et 111111.

Exercice 31. Soit un code de Hamming défini par la matrice de parité 4 x 6

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & h_{1,6} \\ 1 & 1 & 0 & 0 & 0 & h_{2,6} \\ 1 & 0 & 1 & 0 & 0 & h_{3,6} \\ 0 & 1 & 1 & 1 & 0 & h_{4,6} \end{pmatrix}$$

(a) Si l'on choisit $h_{1,6} = h_{2,6} = h_{3,6} = h_{4,6} = 1$, déterminer la liste des mots code. Quel est le nombre de bits d'information et de parité ? Combien d'erreurs ce code corrige-t-il ?
(b) Montrer que les variables $h_{1,6}, h_{2,6}, h_{3,6}, h_{4,6}$ peuvent être choisies de manière à ce que le code corrige les erreurs simples, mais aussi détecte (sans corriger) les erreurs doubles. Déterminer la liste des mots code, et montrer que la distance minimale du code est égale à 4. (Indication : Si la distance minimale de Hamming vaut x alors tout ensemble de $x-1$ colonnes de H doit être linéairement indépendant).

Exercice 32. Démontrer que la distance minimale d'un code de Hamming est égale à d si et seulement si tous les mots code non nuls ont

au moins d bits égaux à 1, et au moins l'un d'entre eux a exactement d bits égaux à 1.

Exercice 33. Générateur d'un code de Hamming. On appelle générateur d'un code binaire $(n; k)$ une matrice $k \times n$ dont les lignes sont k mots code linéairement indépendants. Chacun des $2k$ mots code peut alors s'exprimer comme une combinaison linéaire des lignes de G.
(a) Déterminer la matrice de parité du code dont le générateur est

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

Quelles sont les propriétés de correction et/ou détection d'erreur de ce code ?
(b) Même question pour le code de générateur

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

Exercice 34. Montrer qu'un code de Hamming corrige jusqu'à t et détecte (mais ne corrige pas nécessairement) jusqu'à t erreurs si et seulement si tout ensemble de $2t - 1$ colonnes de la matrice de parité est constitué de colonnes linéairement indépendantes.

Exercice 35. a) Construire un code binaire de 4 mots de longueur 3 et de distance minimum 2.

b) Montrer qu'un code binaire de longueur 3 et de distance minimum 2 possède au plus 4 mots.

c) Quelle est la distance maximale que peut avoir un code linéaire binaire de 64 éléments de longueur 10 ?

Exercice 36. Soit C le code binaire comportant tous les mots de longueur 11.

(1) Combien C comporte-t-il de mots ?

(2) Combien C peut-il détecter et corriger d'erreurs ?

On suppose que la transmission se fait à la vitesse de 10^6 bits par seconde, et que la probabilité qu'un bit soit modifié par le bruit est 10^{-7}.

(3) Calculer la probabilité qu'un mot soit modifié par le bruit.

(4) Combien de mots erronés peut-on s'attendre à recevoir en 24 heures sans pouvoir les détecter ?

Soit C' le code binaire obtenu à partir de C en ajoutant à chaque mot un bit de parité.

(5) Combien C' peut-il détecter et corriger d'erreurs ?

(6) Calculer la probabilité qu'au moins 2 erreurs affectent un même mot.

(7) Combien de mots erronés peut-on s'attendre à recevoir en 24 heures sans pouvoir les détecter ?

Exercice 37. Soit C le code binaire linéaire de matrice génératrice

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

1. Déterminer une matrice de contrôle et la capacité de correction de C.
3. Le code est-il MDS ?
4. Décoder si possible les mots 111110 et 111111.

Exercice 38. Soit C_1 un $[n, k_1, d_1]$ code linéaire et C_2 un $[n, k_2, d_2]$ code linéaire sur le corps fini $\mathbb{F}$. On construit le code $C = \{(y, x + y) \ / \ x \in C_1,\ y \in C_2\}$.
1) Si G_1 et G_2 sont des matrices génératrices de C_1 et C_2 respectivement, montrer que C est un $[2n, k_1 + k_2]$ code linéaire sur $\mathbb{F}$ de matrice génératrice

$$G = \begin{pmatrix} \mathbf{0} & G_1 \\ G_2 & G_2 \end{pmatrix}$$

où $\mathbf{0}$ est la matrice nulle $k_1 \times n$.
2) Montrer que $d(C) = min(d_1, 2d_2)$.
3) On suppose $d_1 > 2d_2$, montrer que tous les mots du code C de poids minimaux sont de la forme (y, y) où y est de poids minimal dans C_2.

Exercice 39. Formuler et montrer la version appropriée de l'exercice précédant dans le cas de codes non linéaires

Exercice 40. Soit C un $[n, k, d]$-code linéaire binaire auto-dual.
a) Montrer que le mot $1 \cdots 1$ est dans C.
b) Montrer que soit tous les mots de C sont de poids divisibles par 4 ; ou exactement la moitié de mots de C sont de poids divisibles par 4 tandis que l'autre moitié sont de poids pairs non divisibles par 4.
c) Pour $n = 6$. Déterminer d.

Exercice 41.
Soit C un $[n, k, d]$ code linéaire sur le corps $\mathbb{F}_q$. On suppose que pour tout $1 \leq i \leq n$ il existe au moins un mot de C dont la i^{eme} composante est non nulle.

i) Montrer que la somme des poids de tous les mots du code est $n(q-1)q^{k-1}$.

ii) Montrer que $d \leq n(q-1)q^{k-1}/(q^k-1)$.

iii) Peut-on construire un $[15, 7, d]$ code binaire linéaire avec $d \geq 8$?

Exercice 42.

Soit C un code linéaire de distance minimale d, avec d est paire. Montrer qu'une classe de C contient deux vecteurs de poids $t+1$, où t est la capacité de correction.

Chapitre 3

Les codes linéaires parfaits

Les codes linéaires parfaits sont certains codes triviaux, les codes de Hamming et deux codes de Golay.

Les codes de Hamming ont été inventés par Richard Hamming aux Bell Labs, à la fin des années 1940. A cette époque, quand les ordinateurs rencontrèrent une erreur, ils s'arrêtaient. Les travaux de Hamming ont porté sur la possibilité que les ordinateurs détectent, corrigent des erreurs isolées et continuent à fonctionner. Sa solution a consisté à grouper les informations en groupe de 4 bits et de calculer 3 bits de contrôle. Ainsi le code de Hamming $(7, 4, 3)$ a été né.

Ce code a été utilisé dans les années 1979-1981 pour la transmission d'images couleurs de Jupiter et de Saturne vers la Terre par la sonde américaine Voyager 1 et 2. C'est une généralisation de la construction des codes de Hamming par Marcel Golay, fin des années 1940.

Les codes de Hamming sont parfaits et de distance minimale 3. Y en a-t-ils d'autres codes parfaits de distance minimale > 3 ? Il y en a deux, qui ne sont pas de Hamming, ils ont été découvert par Golay.

Trois triplets vérifient l'égalité dans la borne de Hamming, sans être des codes de Hamming, sont $(23, 2^{12}, 7)$, $(90, 2^{78}, 5)$ pour $q = 2$ et $(11, 3^6, 5)$ pour $q = 3$. Le premier triplet défini le code linéaire binaire $[23, 12, 7]$, le troisième défini le code linéaire trinaire $[11, 6, 5]$ qui sont appelés code de Golay. On démontre qu'il n'existe pas de code $(90, 2^{78}, 5)$.

En 1973, Tietävainen, a montré que tout code parfait non trivial sur $\mathbb{F}_q^n$ est soit un $\left(\frac{q^r-1}{q-1}, q^{n-r}, 3\right)$-code de Hamming, soit un $(23, 2^{12}, 7)$-code binaire de Golay, soit un $(11; 3^6; 5)$-code trinaire de Golay.

Nous construisons ici le $(24, 2^{12}, 8)$-code de Golay étendu par une matice génératrice et nous déduisons le $(23, 2^{12}, 7)$-code de Golay en réduisant la longueur du premier d'un seul bit. Il y a d'autres constructions, voir [**3**, chap 4] pour les constructions de R. J. Turyn et J. H. Conway.

Le minitel français (Figure 3) code ses données avec un code de Hamming de paramètre $(2^r - r - 1, 2^r - 1) = (120, 128)$ où $r = 7$, on code 15 octet à l'aide d'un octet supplémentaire.

FIGURE 1. Minitel français

3.1. Les codes de Hamming

Un code de Hamming permet de détecter et de corriger une erreur.

Comment construire des codes qui corrigent une erreur ?

Rappelons qu'un code C est de distance minimale d si et seulement si, il existe d colonnes de sa matrice de contrôle linéairement dépendantes, tandis que $d-1$ colonnes quelconques sont linéairement indépendantes.

On construit une matrice de contrôle H d'un code de Hamming de façon est ce que deux colonnes quelconques ne soient pas linéairement dépendantes : Si r est le nombre de lignes de H, ces colonnes appartiennent à $\mathbb{F}_q^r$, doivent alors être non nulles, et on doit en choisir au plus une par droite de $\mathbb{F}_q^r$. Le nombre maximum de colonnes est donc $(q^r-1)/(q-1)$.

3.1.1. Définition.

DÉFINITION 3.1.1. *Soit le corps fini $\mathbb{F}_q$, r un entier positif >1 , $n=(q^r-1)/(q-1)$ et M une matrice $r\times n$ dont les colonnes sont des vecteurs non nuls de $\mathbb{F}_q^r$ tel que aucun n'est multiple de l'autre. Le $[n,n-r]$-code de matrice de contrôle M est appelé code de Hamming et noté par $Ham(r,q)$.*

L'ordre dont sont écrits les colonnes est sans importance, car toutes ces matrices génèrent des codes équivalents. Donc pour un r donné il y a $(2^r-1)!$ codes équivalents.

$Ham(r,q)$ est un code de longueur $n = q^r - 1$ et de dimension $k = n - r = q^r - 1 - r$, c'est un $[q^r - 1, q^r - 1 - r]$-code. Le paramètre $r = n - k$ représente la partie redondante du code.

EXEMPLE 3.1.2. *Pour $r = 2$, $Ham(2,2)$ est un $[3,1]$-code de matrice de contrôle $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ e2t de matrice génératrice $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. Donc $Ham(2,2) = \{000, 111\}$.*

Pour $r = 3$, $Ham(3,2)$ est un $[7,4]$-code de matrice de contrôle

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

Le nombre minimal de vecteur linéairement dépendants est 3 d'où la distance minimale de $Ham(3,2)$ est 3. La dimension du code est 4. Le cardinal de ce code est $2^4 = 16$.

EXERCISE 3.2. *Montrer que les codes $Ham(2,2)$ et $Ham(3,2)$ sont parfaits.*

EXEMPLE 3.2.1. *Pour $r = 2$ et $q = p$ un nombre premier, une matrice de contrôle de $Ham(2,p)$ est $\begin{pmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & 2 & \cdots & p-1 \end{pmatrix}$.*

THÉORÈME 3.2.2. *Le code de Hamming $Ham(r,q)$ est de distance minimale 3 et il est parfait.*

Preuve : Soit M une matrice de contrôle de $Ham(r,q)$. Des colonnes de M sont multiples de

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

qui sont linéairement dépendants. Par le Théorème 2.9.3 $Ham(r,q)$ est de distance minimale 3. Ce qui implique que c'est un code correcteur d'une seule erreur.

Pour montrer que ce code est parfait on utilise la définition 1.9.1 . On a $|Ham(r,q)| = q^{n-r}$ où $n = (q^r - 1)/(q - 1)$. De plus $t = 1$. D'où

$$M \sum_{m=0}^{t} \binom{n}{m} (q-1)^m = q^{n-r}(1 + n(q-1)) = q^n$$

Donc $Ham(r,q)$ est parfait.

PROPOSITION 3.2.3. *Le code dual $Ham(r,q)^{\perp}$ est un code simplexe, c'est-à-dire tous ses mots non nuls sont de même poids. La valeur commune de leur poids est q^{r-1}.*

Preuve en exercice.

3.2.1. Décodage des codes de Hamming. La procédure de décodage des codes de Hamming est simple. On n'a pas besoin de calculer la table des syndromes et les représentants de classes. Car pour les $[q^r-1, q^r-1-r, 3]$-codes de Hamming les représentants de classes sont les q^r vecteurs de poids au plus 1. Soit H_r la matrice de contrôle dont les colonnes sont les nombres $1, 2, \cdots, 2^r-1$ écrit en binaire et compété de 0 au début (par exemple pour $r=3$, 7 s'écrit (1,1,1), 3 s'écrit (0,1,1), 2 s'écrit (0,1,0)). Puisque le syndrome du n-uplet de poids un dont le seul 1 est dans la ie position esl r-tuplet représentant en binaire le nombre i. L'algorithme de décodage par syndrome des codes de Hamming est :

Soit $y \in \mathbb{F}_q^n$ Pour trouver le mot $x \in Ham(r,q)$ le plus proche de y, il suffit de :
- calculer $S(y) = Hy^t$.
- si $S(y) = 0$, alors $y = x \in C$.
- si $S(y) \neq 0$, on cherche l'indice i tel que $S(y) = \lambda c_i$, où les c_i sont les colonnes de H car tous les vecteurs non nuls de $\mathbb{F}_q^r$ sont des colonnes de H.
- Remplacer y_i par $y_i - \lambda$, et retourner $x = y$.

Preuve : Notons e_i le mot dont les coordonnées sont toutes nulles sauf la i-ème qui vaut 1. Clairement, on a

$$Hy^t = H(\lambda e_i)^t = H(y - \lambda r_i)^t = Hy^t - \lambda He_i^t = 0$$

Donc $x = y - \lambda e_i \in H(r,q)$ et est à distance 1 de y.

Cet algorithme est facilement adaptable aux codes de Hamming sur un corps quelconque $\mathbb{F}_q$.

EXERCISE 3.3. *Considérer le code de Hamming $Ham(3,2)$ et décoder le mot reçu $y = 0000001$*

3.3.1. Codes de Hamming étendus. Un code étendu peut augmenter la capacité de correction ou de détection d'erreurs.

DÉFINITION 3.3.1. *Soit un code de Hamming $Ham(r,2)$, on ajoute à chaque mot du code $Ham(r,2)$ un 0 ou un 1 de manière à ce que le poids de ce mot soit pair. On note $Ham(r,2)^*$ le code ainsi obtenu.*

PROPOSITION 3.3.2. *Le code $Ham(r,2)^*$ est un $[2^r, 2^r-1-r]$-code linéaire de distance minimale 4.*

Preuve : Soient $c_1^*, c_2^* \in Ham(r,2)*$ tel que c_1 et c_2 sont les mots du code correspondant dans $Ham(r)$. $c_1^* + c_2^*$ et $c_1 + c_2$ ont les $2^r - 1$ premières composantes identiques. Clairement $Ham(r,2)*$ est un espace vectoriel. Puisque $Ham(r,2)^*$ et $Ham(r,2)$ ont même nombre d'éléments, donc même dimension. D'où $Ham(r,2)*$ est un $[2^r, 2^r - 1 - r]$-code linéaire.

3.4. Unicité des codes de Hamming

THÉORÈME 3.4.1. *1) Ils existent des codes sur $\mathbb{F}_q$ parfaits corrigeant une et une seule erreur qui sont non linéaires et tous ces codes ont même paramètres que les codes de Hamming : de longueur $n = \frac{q^r-1}{q-1}$, nombres de mots q^{n-r} et de distance minimale 3.*

2) Tout code linéaire parfait sur $\mathbb{F}_q$ corrigeant une et une seule erreur est un code de Hamming.

3.5. Codes de Golay

3.5.1. Code de Golay étendu.

3.5.1.1. *Définition.* Soit M la matrice 12×12 : $M = \begin{pmatrix} M_1 & I^t \\ I & 0 \end{pmatrix}$ où $I = (1 \cdots 1)$ et M_1 est la matrice dont la première ligne est (11011100010) et les autres sont les permutations circulaires de cette ligne. M est symétrique et s'écrit :

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

DÉFINITION 3.5.1. *Le code de Golay étendu est défini par la matrice génératrice $G = \left(Id_{12} \vdots M\right)$ et est noté $\mathcal{G}_{24}$.*

3.5.1.2. *Propriétés du code de Golay étendu.* 1) Le code $\mathcal{G}_{24}$ est de longueur 24, de dimension 12 et formé de $2^{12} = 4096$ mots.

2) Une matrice de contrôle de $\mathcal{G}_{24}$ est la matrice 24×12 : $\binom{M}{Id_{12}}^t$

3) Une matrice génératrice de $\mathcal{G}_{24}$ est la matrice 12×24 : $(M \vdots Id_{12})$

4) Le code $\mathcal{G}_{24}$ est auto-dual

5) la distance minimale de $\mathcal{G}_{24}$ est 8.

6) Le code $\mathcal{G}_{24}$ corrige jusqu'à 3 erreurs.

Preuve : Les propriétés 1, 2 et 3 sont videntes.

4) $G = (Id_{12} \vdots M)$ et $H^t = (M^t \vdots Id_{12})$ or $M = M^t$ car elle est symétrique. D'où $\mathcal{G}_{24}$ est auto-dual.

5) Cette démonstration se fait en trois étapes :

i) Tout mot de $\mathcal{G}_{24}$ est de poids divisible par 4, en effet : les lignes de $G = (Id_{12}, M)$ sont toutes de poids 8 ou 12. Soit un mot $c \in \mathcal{G}_{24}$. Supposons que c est somme de deux lignes $r_i + r_j$. Les lignes de M sont orthogonales d'où les lignes de G sont aussi orthogonales. D'où ℓ_i et ℓ_j ont un nombre paire de 1 en commun. Disons $2x$. D'où $\omega(c) = \omega(\ell_i) + \omega(\ell_j) - 2(2x)$ est un multiple de 4.

Supposons maintenant que c est somme de trois lignes $\ell_i + \ell_j + \ell_k$. Si on note $m_1 = \ell_i + \ell_j$ alors $c_1.\ell_k = 0$ car $\mathcal{G}_{24}$ est auto-dual. D'où c_1 et ℓ_1 ont un nombre paire de 1 en commun. Disons $2y$. D'où $\omega(c) = \omega(c_1) + \omega(\ell_k) - 2(2y)$ est un multiple de 4. Ainsi on montre que tout mot de $\mathcal{G}_{24}$ est de poids multiple de 4.

ii) Les 11 premières lignes de G sont des mots du code $\mathcal{G}_{24}$ de poids 8. Ainsi la distance minimale de $\mathcal{G}_{24}$ est soit 4 soit 8.

iii) Aucun mot de $\mathcal{G}_{24}$ n'est de poids 4. Le code $\mathcal{G}_{24}$ est auto-dual. $(M^t \vdots Id_{12})$ est aussi une matrice génératrice de ce code. Si $(a, b) \in \mathcal{G}_{24}$ alors il en est de même pour (b, a) où $a, b \in \mathbb{F}_2^{12}$. Supposons que (a, b) est de poids 4 et $\omega(a) \leq \omega(b)$.

Si $\omega(a) = 0$ alors $a = 0$ et donc $b = 0$ aussi, ce qui est impossible. Si $\omega(a) = 1$ alors (a, b) est une ligne de $\mathcal{G}_{24}$, ce qui est impossible. Si $\omega(a) = 2$ alors (a, b) est une somme de 2 lignes de G. Mais en faisant la somme de 2 lignes quelconques, on ne trouve aucune somme de poids 4.

THÉORÈME 3.5.2. *Si C est un code binaire de longueur 24, $|C| = 2^{12}$, de distance minimale 8 et $0 \in C$, alors C est équivalent à $\mathcal{G}_{24}$.*

Preuve voir [**3**, Chap 4].

3.5.2. Code de Golay.

LEMME 3.5.3. *Si un $q - (n, M, d)$-code existe, alors il existe un $q - (n-1, M, d-1)$-code.*

Preuve : Soient x et y deux mots du $q-(n, M, d)$-code tels que $d(x, y) = d$ on choisit une composante de x et y où ils diffèrent et on supprime cette composante de tous les mots de ce code. Le résultat est un $q-(n-1, M, d-1)$-code.

THÉORÈME 3.5.4. *Soit d un nombre pair. Un (n, M, d)-code binaire existe si seulement si $(n-1, M, d-1)$-code binaire existe .*

Preuve : $\Rightarrow$) D'après le lemme.
$\Leftarrow$) Soit C un $(n-1, M, d-1)$-code binaire. Pour $x \in C$ on note $\omega(x)$ le poids de x. Soit C' le code obtenu en ajoutant à $x \in C$, $\omega(x) \mod 2$. Tous les mots de C' ainsi obtenus sont de poids pair. Or $d(x, y) = \omega(x) + \omega(y) - 2\omega(x + y)$ doit être pair pour tout $x, y \in C'$ d'où $d(C')$ est pair et $d - 1 \leq d(C') \leq d$ mais $d - 1$ est impair, d'où $d(C') = d$. Donc C' est un (n, M, d)-code.

REMARQUE 3.5.5. *Ayant construit le $[24, 12, 8]$-code de Golay étendu $\mathcal{G}_{24}$, on déduit d'après le théorème précédant le $[23, 12, 7]$-code de Golay qui est parfait.*

3.5.2.1. *$[11, 6, 5]$-code de Golay trinaire.* Matrice génératrice du $[11, 6, 5]$-code de Golay trinaire et parfait :

$$\mathcal{G}_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

EXERCISE 3.6. *Montrer que le $[11, 6]$-code linéaire trinaire de Golay engendré par les 11 premières colonnes de la matrice $\mathcal{G}_{12}$ ci-dessous est de distance minimale 5.*

$$\mathcal{G}_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

EXERCISE 3.7. *Montrer que pour $q = 2$, le triplet $(90, 2^{78}, 5)$ vérifie l'inégalité de Hamming.*

THÉORÈME 3.7.1. *Il n'existe pas de code binaire de paramètres $(90, 2^{78}, 5)$.*

Preuve : Supposons qu'un tel code C existe, parfait et de distance minimale 5. On peut supposer que $0 \in C$. Soit Y l'ensemble des $x \in \mathbb{F}_2^{90}$ commençant par deux 1 et de poids 3. On a $|Y| = 88$. Puisque C est parfait pour tout $y \in Y$ il existe un unique $x \in C$ tel que $d(x, y) = 2$. on a

$$2 = d(C) - \omega(y) \leq \omega(x) - \omega(y) \leq \omega(x - y) \leq 2$$

d'où $\omega(x) = 5$ puisque $\omega(y) = 3$ et $d(x, y) = \omega(x - y) = 2$. Ce qui veut dire que x doit avoir un 1 là où y en a. Soit X l'ensemble des $x \in C$ commençant par deux 1 et $\omega(x) = 5$. On sait que pour tout $y \in Y$ il existe un unique $x \in X$ tel que $d(x, y) = 2$. Dans $\{(x, y) \in X \times Y | d(x, y) = 2\}$ il y a $|Y| = 88$ éléments. Mais chaque $x \in X$ contient exactement trois 1 après les deux premières positions. D'où pour chaque $x \in X$ il y a trois vecteurs $y \in Y$ tel que $d(x, y) = 2$. D'où $3|X| = 88$ ce qui est impossible car $|X|$ est un entier.

3.7.1. Unicité des codes de Golay.

THÉORÈME 3.7.2 (Tietavainen et Van Lint, 1971.). *Tout code parfait C corrigeant jusqu'à t-erreurs, de longueur n sur $\mathbb{F}_q$ satisfait une des condition suivantes :*
1) $|C| = 1$, $t = n$;
2) $|C| = q^n$, $t = 0$;
3) $|C| = 2$, $q = 2$, $n = 2t + 1$;
4) $|C| = 3^6$, $q = 3$, $t = 2$, $n = 11$;
5) $|C| = 2^{12}$, $q = 2$, $t = 3$, $n = 23$;
6) $|C| = q^{n-r}$, $t = 1$, $n = (q^r - 1)/(q - 1)$, *pour tout* $r > 1$.

Dans ce théorème on ne fait aucune hypothèse de linéarité. Les codes de 1) et 2) sont parfaits et triviaux. Le code 3) est un code de répitition. 4) et 5) sont les codes de Golay. 6) sont les codes de Hamming.

Best et Hong ont montré que ce théorème est valable pour tout alphabet fini, et non seulement pour $\mathbb{F}_q$, si $t \geq 3$.

COROLLAIRE 3.7.3. *1) Tout code non-trivial, parfait, corrigeant plusieurs erreurs a même longueur, même nombre de mots et même distance minimale que le [23, 12, 7]-code binaire ou le [11, 6, 5]-code trinaire de Golay.*

2)Tout code binaire (respectivement, trinaire) linéaire ou non ayant 2^{12} *(respectivement,* 3^6 *) mots, contenant 0, de longueur 23 (respectively, 11) et de distance minimale 7 (respectivement, 5) est équivalent au [23, 12, 7]-code binaire (respectivement, [11, 6, 5]-code trinaire) de Golay.*

3.7.2. Décodage. On cherche à corriger des erreurs de poids ≤ 3. On note $e = (e_1, e_2)$ où e_i est de longueur 12. Puisque $\omega(e) \leq 3$ on a soit $\omega(e_1) \leq 1$ ou $\omega(e_2) \leq 1$. Soit $y = x + e$ et $H^t = \binom{Id}{M}$ on a $s_1 = yH^t = (e_1, e_2)H^t = e_1 + e_2M$.

Si $\omega(e_2) \leq 1$ alors s_1 est un mot de poids ≤ 3 si $\omega(e_2) = 0$ sinon c'est une ligne de G dont au plus 2 bits ont été changés.

De même si $\omega(e_1) \leq 1$, $s_2 = y\binom{M}{I} = e_1M + e_2$.

Dans tous les cas si $\omega(e) \leq 3$ on a $s_1 = e_1 + e_2M = yH^t$ et $s_2 = e_1G + e_2 = (e_1 + e_2G)G = s_1G$.

Algorithme :
1) calculer $s = yH^t$;
2) si $\omega(e) \leq 3$, $e = (s, 0)$;
3) si $\omega(s + b_i) \leq 2$ pour une ligne b_i de M, alors $e = (s + b_i, e_i)$;
4) calculer sM ;
5) si $\omega(sM) \leq 3$ alors $= (0, sG)$;
6) si $\omega(sG + b_i) \leq 2$ pour une ligne b_i de G, alors $e = (\overline{e}_i, sM + b_i)$ où $\overline{e}_i = (0, \cdots, 1, 0, \cdots, 0)$;
7) si e est non déterminé, demander rediffusion.

Cet algorithme nécessite au plus 26 calculs de poids pour décoder.

EXEMPLE 3.7.4. *Le code de Gloay* $(23, 12, 7)$ *est cyclique de polynôme générateur* $g_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$ *ou* $g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$. *Les polynômes* $g_1(x)$ *et* $g_2(x)$ *sont des facteurs de* $x^{23} + 1$ *en fait :* $x^{23} + 1 = (1 + x)g_1(x)g_2(x)$.

Le code de Gloay $(11, 6, 5)$ est cyclique de polynôme générateur $g(x) = x^5 + x^4 - x^3 + x^2 - 1$ et si $h(x) = x^6 - x^5 - x^4 - x^3 + x^2 + 1$ alors $x^{11} - 1 = g(x)h(x)$

$$G = \begin{pmatrix} 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 \end{pmatrix}$$

3.8. Exercices

Exercice 1. Montrer l'Inégalité de Singleton suivante :

$$A_q(n, d) \leq q^{n-d+1}$$

Exercice 2. Soit C un code linéaire binaire. Montrer que tous les mots de C sont de poids paire ou exactement la moitié d'entre eux sont de poids paire.

Exercice 3. On transmet des données par paquet de 16 bits, écrits dans un tableau 4 x 4, en ajoutant une ligne et une colonne de contrôle obtenue en associant à chaque ligne et chaque colonne son bit de parité.

a) Que pensez-vous des paquets reçus suivants :

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

b) Quelles sont la longueur, la dimension et la distance du code décrit ?
c) Combien repère-t-il d'erreurs ? Combien en corrige-t-il ?
d) Si on ajoute en dernière position le bit de parité de la colonne de contrôle, que deviennent la longueur, la dimension, la distance, le nombre d'erreurs repérées, corrigées du code ?

Exercice 4. 1) Écrivez une matrice de contrôle et une matrice génératrice canaonique du code

- binaire de Hamming $Ham(4, 2)$.
- trinaire de Hamming $Ham(2, 3)$. Décoder $y = 11000$
- trinaire de Hamming $Ham(3, 3)$.

Exercice 5. Écrivez la table de syndrome du code binaire de Hamming $Ham(3, 2)$. Décodez les mots suivants : 1001011, 1100110, 1111001.

Exercice 6. On appelle code MDS un code de paramètres (k, n, d) avec $d = n + 1 - k$. Montrer que le code de Hamming de longueur 7 n'est pas MDS.

Exercice 7. Construire la matrice de contrôle de $Ham(4, 2)$ dont les colonnes sont les nombres binaires 1, 2, ..., 15 dans cet ordre. Décoder les mots suivants et vérifier que les mots obtenus sont bien des mots du code $Ham(4, 2)$. 001000001100100, 101001110101100 et 000100100011000.

Exercice 8. Montrer que pour tout entier $r \geq 2$, on a $A_2(2^r - 1, 3) = 2^{2^r-1-r}$.

Exercice 9. Montrer que les triplets $(23; 2^{12}; 7)$, $(90; 2^{78}; 5)$ pour $q = 2$, et $(11; 3^6; 5)$ pour $q = 3$ satisfont l'égalité dans la borne de Hamming.

Exercice 10. Montrer qu'il n'existe pas de code binaire de paramètres $(90, 2^{78}, 5)$.

Exercice 11. Montrer que le $[11, 6]$-code triaire engendré par les 11 premières colonnes de la matrice G_{12} ci-dessous est de distance minimale 5.

$$G_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

Exercice 12. Montrer qu'un $[n, M, 7]$-code binaire parfait vérifie $n = 7$ ou $n = 23$.

Exercice 13. Montrer que la distance minimale d'un code parfait est impaire.

Exercice 14. Montrer que le code binaire de répétition de longueur n impaire est parfait. Combien d'erreurs corrige-t-il ?

Exercice 15. Le code de Hamming étendu de longueur 8 a pour matrice de parité

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

C'est un code de paramètres [8, 4, 4].
1. Combien d'effacements corrige-t-il correctement ?
2. Corrigez les effacements suivants :
00 ? ? ?011, ?01100 ? ?, ? ?100 ?01, ?1 ?0 ?001, 1111 ? ? ?1, 1 ?1 ?1 ?11

Exercice 16. Montrer que le code dual $Ham(r, q)^{\perp}$ d'un code de Hamming $Ham(r, q)$ est un code simplexe, et la valeur commune des poids (non nulle) est q^{r-1}.

Exercice 17. Montrer que le code de Hamming $Ham(r, 2)$ est équivalent à un code cyclique.

Exercice 18. Soit C le [7, 4]-code de Hamming de polynôme générateur $g(x) = 1 + x + x^3$. Décoder le mot reçu 0101111.

Exercice 19.
Soit C le $[7, 4]$-code binaire de Hamming. Décoder le mot reçu 0101110 si possible.

Exercice 20.
Montrer que le code dual $Ham(r,q)^{\perp}$ est un code simplexe, c'est-à-dire tous ses mots non nuls sont de même poids, et la valeur commune de leur poids est q^{r-1}.

Chapitre 4

Codes de Reed-Muller

Les codes de Reed-Muller ont été introduits séparément par I.S. Reed et D.E. Muller en 1954. Ils forment une classe de codes généralisant les codes de Hamming et ils sont définis récursivement. Ils sont utiles pour la transmission sur des canaux très bruités. De plus ils sont faciles à implèmenter et à décoder. En particulier, $\mathcal{RM}(1,m)$ a une distance minimale égale à la moitié de sa longueur. $\mathcal{RM}(1,5)$ a été utilisé entre 1969 et 1973 par le satellite Mariner 9 et Viking du NASA pour la transmission d'images en noir et blanc de Mars vers la Terre. Ce code a $2^6 = 64$ mots de longueur $2^5 = 32$, de distance minimale $2^4 = 16$ et peut corriger jusqu'à 7 erreurs dans chaque mot transmi. Chaque mot du code correspond à un niveau de gris, soit 64 niveaux.

4.1. Définition récursive

DÉFINITION 4.1.1. *Le code de Reed-Muler d'ordre r noté $\mathcal{RM}(r,m)$ et de longueur 2^m où $0 \leq r \leq m$ est :*
$\mathcal{RM}(0,m) = \{00\cdots0, 11\cdots1\}$ *chaque mot est de longueur* 2^m. $\mathcal{RM}(m,m) = \{0,1\}^{2^m} = \mathbb{F}_2^{2^m}$.
et pour $0 < r < m$ *:* $\mathcal{RM}(r,m) = \{(x, x+y) \mid x \in \mathcal{RM}(r,m-1),\ y \in \mathcal{RM}(r-1,m-1)\}$

EXEMPLE 4.1.2. $\mathcal{RM}(0,0) = \{0,1\}$.
$\mathcal{RM}(0,1) = \{00,11\}$.
$\mathcal{RM}(1,1) = \{0,1\}^2 = \{00,01,10,11\}$.
$\mathcal{RM}(0,2) = \{0000,1111\}$.
$\mathcal{RM}(2,2) = \{0,1\}^4$.

$$\begin{aligned}\mathcal{RM}(1,2) &= \{(x,x+y) \mid x \in \{00,01,10,11\},\ y \in \{00,11\}\} \\ &= \{0000,0101,1001,1010,0110,0011,1100,1111\}\end{aligned}$$

EXERCISE 4.2. *Donnez les mots du code* $\mathcal{RM}(1,3)$.

4.3. Matrice génératrice

PROPOSITION 4.3.1. $\mathcal{G}(r,m)$ *est une matrice génératrice de* $\mathcal{RM}(r,m)$ *où on pose*

$\mathcal{G}(0,m) = (11\cdots1)$, $\mathcal{G}(m,m) = \binom{\mathcal{G}(m-1,m)}{0\cdots01}$ *et pour* $0 < r < m$ *on a*

$$\mathcal{G}(r,m) = \begin{pmatrix} \mathcal{G}(r,m-1) & \mathcal{G}(r,m-1) \\ 0 & \mathcal{G}(r-1,m-1) \end{pmatrix}$$

EXEMPLE 4.3.2. $\mathcal{G}(0,1) = (11)$, $\mathcal{G}(0,2) = (11\cdots1)$, $\mathcal{G}(1,1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$,

$$\mathcal{G}(1,2) = \begin{pmatrix} \mathcal{G}(1,1) & \mathcal{G}(1,1) \\ 0 & \mathcal{G}(0,1) \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right)$$

$$\mathcal{G}(2,2) = \begin{pmatrix} \mathcal{G}(1,2) \\ 0\cdots01 \end{pmatrix} = \left(\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

$$\mathcal{G}(1,3) = \begin{pmatrix} \mathcal{G}(1,2) & \mathcal{G}(1,2) \\ 0 & \mathcal{G}(0,2) \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$$\mathcal{G}(2,3) = \begin{pmatrix} \mathcal{G}(2,2) & \mathcal{G}(2,2) \\ 0 & \mathcal{G}(1,2) \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

4.4. Propriétés

THÉORÈME 4.4.1. *Le code de Reed-Muler* $\mathcal{RM}(r,m)$ *a les propriétés suivantes :*

1) il est de longueur 2^m *;*
2) $\mathcal{RM}(r-1,m) \subset \mathcal{RM}(r,m)$ *pour* $r > 0$ *;*
3) de dimension $k = \sum_{i=0}^{r} \binom{m}{i}$ *;*
4) de distance minimale 2^{m-r} *;*
5) son code dual est $\mathcal{RM}(m-r-1,m)$ *pour* $r < m$*.*
6) $\mathcal{RM}(m-2,m)$ *est le* $[n, n-m-1]$*-code de Hammimg étendu.*

Preuve :
1) Par définition des codes de Reed-Muller.

2) Pour $m = 1$ on a $\mathcal{RM}(0,1) = \{00, 11\} \subset \mathcal{RM}(1,1) = \{0,1\}^2$. On démontre par récurrence sur m.

Supposons que pour $0 < r < m$ on a $\mathcal{RM}(r-1, m-1) \subset \mathcal{RM}(r, m-1)$.

$$\begin{aligned}\mathcal{RM}(r-1,m) &= \{(x, x+y) \mid x \in \mathcal{RM}(r-1,m-1),\ y \in \mathcal{RM}(r-2,m-1)\} \\ &\subset \{(x, x+y) \mid x \in \mathcal{RM}(r,m-1),\ y \in \mathcal{RM}(r-1,m-1)\} \\ &= \mathcal{RM}(r,m).\end{aligned}$$

3) Par définition de $\mathcal{G}(r,m)$, on a

$$\begin{aligned}dim\mathcal{RM}(r,m) &= dim\mathcal{RM}(r,m-1) + dim\mathcal{RM}(r-1,m-1) \\ &= \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \\ &= \binom{m-1}{0} + \sum_{i=1}^{r} \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right).\end{aligned}$$

Or $\binom{m}{n-i} = \binom{m}{i}$, $\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$ et que $\binom{m-1}{0} = \binom{m}{0} = 1$, d'où $\dim \mathcal{RM}(r,m) = \sum_{i=0}^{r} \binom{m}{i}$.

4) On montre par récurrence sur m. Pour $m = 1$ on a $\mathcal{RM}(0,1) = \{00, 11\}$ de distance minimale $2 = 2^{1-0}$, et $\mathcal{RM}(1,1) = \{00, 01, 10, 11\}$ de distance minimale $1 = 2^{1-1}$. On suppose que la distance minimale de $\mathcal{RM}(r, m-1) = 2^{m-1-r}$ pour $0 \leq r \leq m-1$ On sait que

$$\mathcal{RM}(r,m) = \{(x, x+y) \mid x \in \mathcal{RM}(r,m-1),\ y \in \mathcal{RM}(r-1,m-1)\}$$

et $\mathcal{RM}(r-1,m-1) \subset \mathcal{RM}(r,m-1)$ d'après 2) càd $x+y \in \mathcal{RM}(r,m-1)$ et par hypothèse de récurrence on a pour $x \neq y$, $\omega(x+y) \geq 2^{m-1-r}$. De plus $\omega(x) \geq 2^{m-1-r}$. D'où $\omega(x, x+y) = \omega(x+y) + \omega(x) \geq 2.2^{m-1-r} = 2^{m-r}$. Si $x = y$, alors $(x, x+y) = (y, 0)$ mais $y \in \mathcal{RM}(r-1, m-1)$. Donc $\omega(y, 0) = \omega(y) \geq 2^{m-1-(r-1)} = 2^{m-r}$.

5) Rappelons que

$$\mathcal{RM}(r,m) = \{(x, x+y) \mid x \in \mathcal{RM}(r,m-1),\ y \in \mathcal{RM}(r-1,m-1)\}$$

$$\mathcal{RM}(m-r-1,m) =$$

$$\{(x', x'+y') \mid x' \in \mathcal{RM}(m-r-1,m-1),\ y' \in \mathcal{RM}(m-r-2,m-1)\}$$

Par récurrence sur m. $\mathcal{RM}(0,2) = \{0000, 1111\}$ et $\mathcal{RM}(1,2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$ sont orthogonaux puisque tous les vecteurs sont de poids paire.

Le dual de $\mathcal{RM}(r, m-1)$ est $\mathcal{RM}(m-r-2, m-1)$ et le dual de $\mathcal{RM}(r-1, m-1)$ est $\mathcal{RM}(m-r-1, m-1)$ d'où $x.y' = 0$ et $x'.y = 0$.

Or d'après 2) $\mathcal{RM}(r-1,m-1) \subset \mathcal{RM}(r,m-1)$ d'où $y.y'=0$. Donc

$$\begin{aligned}(x,x+y).(x',x'+y') &= x.x'+(x+y).(x'+y')\\ &= 2x.x'+x.y'+yx'+y.y'\end{aligned}$$

ce qui veut dire que tout vecteur de $\mathcal{RM}(r,m)$ est orthogonal à tout vecteur de $\mathcal{RM}(m-r-1,m)$ De plus on a

$$dim\mathcal{RM}(r,m)+dim\mathcal{RM}(m-r-1,m)=\sum_{i=0}^{r}\binom{m}{i}+\sum_{i=0}^{m-r-1}\binom{m}{i}$$

$$\sum_{i=0}^{m-r-1}\binom{m}{i}=\sum_{i=0}^{m-r-1}\binom{m}{m-i}=\sum_{i=r+1}^{m}\binom{m}{i}$$

$$dim\mathcal{RM}(r,m)+dim\mathcal{RM}(m-r-1,m)=2^m.$$

Donc $\mathcal{RM}(m-r-1,m)$ est le dual de $\mathcal{RM}(r,m)$.

4.5. Décodage de $\mathcal{RM}(1,m)$

On présente un algorithme de décodage rapide des codes $\mathcal{RM}(1,m)$. La définition récursive de ce code suggère un décodage récursive aussi. On commence par définir le produit de Kronecher de deux matrices $A=(a_{ij})$ et B par $A\times B=(a_{ij}B)$. Par exemple : si $H=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ et $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ alors

$$I_2\times H=\left(\begin{array}{cc|cc}1&1&0&0\\1&-1&0&0\\\hline 0&0&1&1\\0&0&1&-1\end{array}\right) \text{ et } H\times I_2=\left(\begin{array}{cc|cc}1&0&1&0\\0&1&0&1\\\hline 1&0&-1&0\\0&1&0&-1\end{array}\right)$$

DÉFINITION 4.5.1. *Soit* $H=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$. *On défini* $H_m^i=I_{2^{m-i}}\times H\times I_{2^{i-1}}$.

EXERCISE 4.6. *Calculer* H_3^1, H_3^2 *et* H_3^3.

Algorithme de décodage. Soit $\mathcal{G}(1,m)$ une matrice génératrice de $\mathcal{RM}(1,m)$. Soit y un mot reçu et x le mot du code le plus proche de y.
1) soit $\hat{y}$ le mot obtenu en remplaçant les 0 par des -1 dans y,
2) on calcule $y_1 = \hat{y}H_m^1$ et $y_i = y_{i-1}H_m^i$ pour $i = 2, 3, \cdots, m$,
3) trouver la position j de la plus grande composante en valeur absolue de y_m. (la première position est 0).

Soit $B(j) \in \mathbb{F}_2^m$ la représentation binaire de j (les unités d'ordre petit d'abord). Si la composante j de y_m est positive alors $x = (1, B(j))$, si elle est négative alors $x = (0, B(j))$.

EXERCISE 4.7. *Pour $m = 3$ et $y = 10101011$ montrer que $x = 1100$.*

4.8. Fonctions booléennes

4.8.1. Définition.

DÉFINITION 4.8.1. *Une fonction booléenne à m variables est une fonction $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$.*

Notons par x_i l'application qui à $y \in \mathbb{F}_2^m$ associe sa i-eme composante y_i. Les expressions $x_i + x_j$, $x_i x_j$, et de façon plus générale, toute expression polynomiale en les x_i, définissent une fonction booléenne. Remarquons que $x_i^2 = x_i$ dans $\mathbb{F}_2$, donc il est inutile d'introduire des exposants plus grands que 1. Pour $I \subset \{1, \cdots, m\}$, notons $x_I = \prod_{i \in I} x_i$.

PROPOSITION 4.8.2. *L'espace $\mathcal{F}_m$ des fonctions booléennes à m variables est un $\mathbb{F}_2$- espace vectoriel de dimension $n = 2^m$. Toute fonction booléenne $f \in \mathcal{F}_m$ a une écriture unique sous la forme*

$$f = \sum_{I \subset \{1,\cdots,m\}} a_I x_I = \sum_{1 \leq i_1 < i_2 < \cdots < i_s \leq m} a_{i_1,\cdots,i_s} x_{i_1} \cdots x_{i_s}$$

Le plus grand I pour lequel $a_I \neq 0$ s'appelle le degré de f.

Preuve : Soit la fonction booléenne $\delta_y(x) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y \end{cases}$ définit sur $\mathbb{F}_2^m$. Les δ_y où $y \in \mathbb{F}_2^m$ forment une base de $\mathcal{F}_m$ qui est donc de dimension 2^m. D'autre part, on peut exprimer les fonctions δ_y algébriquement en fonction des x_i :

$$\delta_y = \prod_{i=1}^{m} (x_i + y_i + 1)$$

Donc les monômes $x_{i_1} \cdots x_{i_s}$ engendrent bien l'espace $\mathcal{F}$ comme il y en a exactement $\sum_{s=0}^{m} \binom{m}{s} = 2^m$ ils forment une base de $\mathcal{F}_m$.

Pour $n = 2^m$, on considère la bijection de $\{0, \cdots, n-1\}$ dans $\mathbb{F}_2^m$: $k \longrightarrow 2^{m-1}k_1 + 2^{m-2}k_2 + \cdots + 2k_{m-1} + k_m$ (l'écriture binaire

de i). qu'on identifie avec $u = (k_1, k_2, \cdots, k_{m-1}, k_m)$. Posons $\mathbb{F}_{2^m} = \{\alpha_0, \alpha_1, \cdots, \alpha_{2^m-1}\}$. Tout élément $u = (u_1, \cdots, u_{2^m-1}) \in \mathbb{F}_2^m$ est identifié à un élément α_i de $\mathbb{F}_{2^m}$ (dans un ordre quelconque mais fixe, par exemple α_i s'identifie à l'écriture binaire de i) qu'on identifie encore avec la fonction booléenne f en m variables défini par $u = (f(\alpha_0), \cdots, f(\alpha_{2^m-1}))$.

4.8.2. Codes de Reed-Muller.

DÉFINITION 4.8.3. *Le code de Reed-Muller $\mathcal{RM}(r, m)$ est le code binaire engendré par les éléments de $\mathbb{F}_2^m$ associés aux fonctions booléennes : x_I telles que $|I| \leq r$.*

Autrement dit :

$$\mathcal{RM}(r, m) = \{(f(\alpha_0), \cdots, f(\alpha_{2^m-1})) \ : f \in \mathcal{F}_m \text{ et } deg(f) \leq r\}$$

Le code $\mathcal{RM}(1, 3)$ est engendré par les lignes ci-dessous :

$\mathbb{F}_2^3$:	000	100	010	110	001	101	011	111
1	1	1	1	1	1	1	1	1
x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1

Le code $\mathcal{RM}(2, 3)$ est engendré par les lignes ci-dessous :

$\mathbb{F}_2^3$:	000	100	010	110	001	101	011	111
1	1	1	1	1	1	1	1	1
x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
x_1x_2	0	0	0	1	0	0	0	1
x_1x_3	0	0	0	0	0	1	0	1
x_2x_3	0	0	0	0	0	0	1	1

4.9. Exercices

chercher exercices

Exercice 1. Montrer que pour $r < m$ le code de Reed-Muler $\mathcal{RM}(r, m)$ a pour code dual $\mathcal{RM}(m - r - 1, m)$.

Chapitre 5

Codes cycliques

Les codes cycliques forment une classe de codes linéaires très importante, dont le codage et le décodage sont faciles à implémenter à l'aide des registres à décalage à rétroaction linéaire. Leur étude a commencé en 1957. Plusieurs des codes vus précédemment, codes de Hamming, codes Golay, codes de Reed-Muller sont des codes cycliques ou des codes cycliques étendus.

5.1. Définition

Soit $\mathbb{F}$ un corps fini et $n \in \mathbb{N}^*$ Par σ on note l'application linéaire de $\mathbb{F}^n \to \mathbb{F}^n$ définie par

$$\sigma(x_1, x_2, \cdots, x_n) = (x_n, x_1, x_2, \cdots, x_{n-1}).$$

DÉFINITION 5.1.1. *Un code linéaire $C \subset \mathbb{F}^n$ est appelé code cyclique si $\sigma(x) \in C$ pour tout $x \in C$.*

EXEMPLE 5.1.2. *$C = \{000, 110, 011, 101\}$ est un code binaire cyclique.*

THÉORÈME 5.1.3. *Soit $\mathcal{G}$ une matrice génératrice d'un code linéaire C. Alors C est un code cyclique si et seulement si $\sigma(L_i) \in C$ pour chaque ligne L_i de $\mathcal{G}$.*

DÉMONSTRATION 1. *Si C est cyclique alors $\sigma(x) \in C$ pour tout $x \in C$ en particulier $\sigma(L_i) \in C$ pour chaque ligne L_i de $\mathcal{G}$. Inversement, supposons que $\sigma(L_i) \in C$ pour chaque ligne L_i de $\mathcal{G}$. Soit $x \in C$, $x = \sum_{i=1}^{k} \alpha_i L_i$ où les $\alpha_i \in \mathbb{F}$ d'où $\sigma(x) = \sigma(\sum_{i=1}^{k} \alpha_i L_i) = \sum_{i=1}^{k} \alpha_i \sigma(L_i) \in C$. Donc C est cyclique.*

On considère $p(x)$ un polynôme de l'anneau $\mathbb{F}[x]$, $(p(x))$ l'idéal engendré par $p(x)$ et l'anneau quotient

$$\mathbb{F}[x]/p(x) = \left\{a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \mid a_0, a_1, \cdots, a_{n-1} \in \mathbb{F}\right\}$$

où t est la classe $x + (p(x))$, i.e. $p(t) = 0$.

Pour $p(x) = x^n - 1$. On note $\mathcal{F}_n = \mathbb{F}[x]/(x^n - 1)$ c'est un anneau, où le produit est obtenu en posant $x^n = 1$, $x^{n+1} = x$ etc, dans le produit usuel de polynômes. L'addition est l'addition des polynômes usuelle

notée $+$. $\mathcal{F}_n$ est aussi un $\mathbb{F}$-espace vectoriel, il est isomorphe à l'espace vectoriel $\mathbb{F}^n$, en identifiant tout polynôme $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ de $\mathcal{F}_n$ avec le vecteur $(a_0, a_1, \cdots, a_{n-1})$ de $\mathbb{F}^n$.

Soit $C \subset \mathbb{F}^n$ un code linéaire. Un élément de C peut être vu comme mot $a_0a_1 \cdots a_{n-1}$ ou comme polynôme $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

$$x.p(x) = a_{n-1} + a_0x + \cdots + a_{n-2}x^{n-1} = a_{n-1}a_0a_1 \cdots a_{n-2}$$

ce qui veur dire qu'un code C linéaire est cyclique si et seulement si $xp(x) \in C$ pour tout $p(x) \in C$.

THÉORÈME 5.1.4. *Une partie $C \subset \mathcal{F}_n$ est un code cyclique si et seulement si C est un idéal de l'anneau $\mathcal{F}_n$.*

DÉMONSTRATION 2. *Soit C un code cyclique et $p(x)$, $q(x)$ dans C. Alors $p(x) - q(x) \in C$, $\lambda p(x) \in C$ et $xp(x) \in C$. D'où $x^2p(x) \in C$ etc. Donc pour tout $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in \mathcal{F}_n$ on a $r(x).p(x) = r_0p(x) + r_1xp(x) + \cdots + r_{n-1}x^{n-1}p(x) \in C$ c'est à dire C est un idéal dans $\mathcal{F}_n$.*

Inversement : Supposons que C soit un idéal et $p(x)$, $q(x)$ dans C et $\lambda \in \mathbb{F}$ alors $p(x) - q(x) \in C$ et $\lambda p(x) \in C$ donc C est un code linéaire. De plus $r(x)p(x) \in C$ pour tout $r(x) \in C$ en particulier $xp(x) \in C$. Donc C est cyclique.

5.2. Polynômes générateur et de contrôle

THÉORÈME 5.2.1. *Soit C un idéal non nul de $\mathcal{F}_n$ alors :*

i) il existe un unique polynôme unitaire $g(x)$ dans C de degré minimal ;

ii) $g(x)$ divise $x^n - 1$ dans $\mathbb{F}[x]$;

iii) pour tout $p(x) \in C$, $g(x)$ divise $p(x)$ dans $\mathbb{F}[x]$;

iv) Inversement supposons $C = (p(x))$ où $p(x) \in \mathcal{F}_n$. Alors $p(x)$ est de degré minimal dans C si et seulement si $p(x)$ divise $x^n - 1$ dans $\mathbb{F}[x]$.

Preuve : i) Supposons que $f(x)$ et $g(x)$ sont deux polynômes distincts, unitaires et de degré minimal k . On pose $h(x) = f(x) - g(x) \in C$. Il est de degré $< k$. Si λ est le coefficient du plus haut monôme alors $\lambda^{-1}h(x)$ est unitaire de degré $< k$. Contradiction.

ii) En faisant la division euclidienne : $x^n - 1 = q(x)g(x) + r(x)$ où $q(x), r(x) \in \mathbb{F}[x]$ et $deg(r(x)) < deg(g(x))$ ou $r(x) = 0$. En passant aux classes on a dans $\mathcal{F}_n$: $r(x) = -q(x)g(x) \in C$. Mais puisque $g(x)$ est de degré minimal on a $r(x) = 0$ et donc $g(x)$ divise $x^n - 1$ dans $F[x]$.

iii) Soit $p(x) \in C$. On a $p(x) = q(x)g(x) + r(x)$ où $q(x)$, $r(x) \in \mathbb{F}[x]$ et $deg(r(x)) < deg(g(x))$ ou $r(x) = 0$. Puisque $deg(p(x)) < n$ alors en

passant à $\mathcal{F}_n$ on a $r(x) = p(x) - \overline{q(x)g(x)} \in C$, or $g(x)$ est de degré minimal d'où $r(x) = 0$ et donc $g(x)$ divise $p(x)$ dans $\mathbb{F}[x]$.

iv) $\Rightarrow$) par ii) et $\Leftarrow$) évident.

EXEMPLE 5.2.2. *On cherche les idéaux non triviaux de $\mathbb{F}_3[x]$ et on déduit tous les codes cycliques de longueur 3. On a $x^3 - 1 = (x - 1)(x^2+x+1)$ ces facteurs sont irréductibles sur $\mathbb{F}_2$. D'où $C_1 = (x-1) = \{0,\ 1+x,\ x+x^2,\ 1+x^2\}$ et $C_2 = (x^2+x+1) = \{0,\ 1+x+x^2\}$ ou $C_1 = \{000, 110, 011, 101\}$ et $C_2 = \{000, 111\}$.*

DÉFINITION 5.2.3. *Soit un idéal non nul $C \subset \mathcal{F}_n$ et $g(x)$ l'unique polynôme minimal unitaire de C. Alors $g(x)$ est appelé polynôme générateur du code cyclique C.*

REMARQUE 5.2.4. *Soit $C = (p(x))$. Alors $p(x)$ est le polynôme générateur de C si et seulement si $p(x)$ est unitaire et divise $x^n - 1$.*

Le polynôme générateur d'un code cyclique détermine, une matrice génératrice et une matrice de contrôle.

THÉORÈME 5.2.5. *Soit $C \subset \mathcal{F}_n$ un code cyclique de polynôme générateur $g(x) = g_0+g_1x+\cdots+g_{r-1}x^{r-1}+g_rx^r$. Alors C est de dimension $n-r$. De plus la matrice $(n-r)\times n$*

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & & & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & & & g_{r-1} & g_r & 0 & \cdots & \\ \vdots & \vdots & \vdots & & & & & & & & \vdots \\ 0 & 0 & & 0 & g_0 & g_1 & & & \cdots & & g_r \end{pmatrix}$$

est une matrice génératrice de C.

Preuve : Par le Théorème 5.2.1, il existe $h(x)$ tel que $g(x)h(x) = x^n - 1$. D'où $g_0 \neq 0$. Les lignes de G sont linéairement indépendantes. En les écrivant comme polynômes les lignes de G sont : $g(x)$, $xg(x)$, $\cdots$, $x^{k-1}g(x)$. Soit $p(x) \in C$, d'après le Théorème 5.2.1 $p(x) = q(x)g(x)$ où $q(x)$ est un polynômes tel que $deg(q(x)) < n-r$ puisque $deg(p(x)) < n$. D'où $q(x)$ est de la forme $q(x) = q_0 + q_1x + \cdots + q_{n-r-1}x^{n-r-1}$ et $p(x) = q_0g(x)+q_1xg(x)+\cdots+q_{n-r-1}x^{n-r-1}g(x)$ et $p(x)$ est combinaison linéaire des lignes de G. Donc G est une matrice génératrice de C.

On sait que si G est une matrice génératrice d'un code C alors un mot $x \in \mathbb{F}^k$ est codé comme $xG \in C$.

Si C est un code cyclique de polynôme générateur $g(x)$ alors $r = deg(g(x)) = n - k$ et les lignes de G sont $g(x)$, $xg(x)$, $\cdots$, $x^{k-1}g(x)$. Soit $u = u_0u_1\cdots u_{k-1}$, $u(x) = u_0 + u_1x + \cdots + u_{k-1}x^{k-1}$ Alors

$$uG = u_0g(x) + u_1xg(x) + \cdots + u_{k-1}x^{k-1}g(x) = u(x)g(x)$$

Donc un message polynômial $u(x)$ est codé comme $u(x)g(x)$.

DÉFINITION 5.2.6. *Soit $g(x)$ le polynôme générateur d'un code cyclique $C \subset \mathcal{F}_n$. Le polynôme $h(x)$ tel que $x^n - 1 = g(x)h(x)$ est appelé polynôme de contrôle de C.*

Si C est un $[n, k]$-code cyclique, alors son polynôme générateur $g(x)$ est de degré $n - k$ et son polynôme de contrôle est de degré k.

THÉORÈME 5.2.7. *Soit $C \subset \mathcal{F}_n$ un code cyclique de polynôme de contrôle $h(x)$ et $p(x) \in \mathcal{F}_n$. Alors $p(x) \in C$ si et seulement si $p(x)h(x) = 0$.*

Preuve : Soit $g(x)$ le polynôme générateur de C alors $g(x)h(x) = x^n - 1$ d'où $g(x)h(x) = 0$ dans $\mathcal{F}_n$. Soit $p(x) \in C$, par le Théorème 5.2.1 on a $p(x) = q(x)g(x)$ et $p(x)h(x) = q(x)g(x)h(x) = 0$ dans $\mathcal{F}_n$.

Inversement si $p(x) \in \mathcal{F}_n$ tel que $p(x)h(x) = 0$, alors $p(x)h(x) = f(x)(x^n - 1)$. D'où $p(x)h(x) = f(x)g(x)h(x)$. Donc $p(x) = f(x)g(x)$ d'où $p(x) \in C$.

THÉORÈME 5.2.8. *Soit C un $[n, k]$-code de polynôme de contrôle $h(x) = h_0 + h_1x + \cdots + h_{k-1}x^{k-1} + h_kx^k$. Alors*

1) la matrice $(n - k) \times n$

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & & & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & & & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & & & & \cdots & h_0 \end{pmatrix}$$

est une matrice de contrôle du code C.

2) Le code dual est cyclique et de polynôme générateur

$$\overline{h}(x) = h_k + h_{k-1}x + \cdots + h_0x^k = x^k h(1/x).$$

Preuve : Les lignes de H sont linéairement indépendantes. On montre que chaque ligne est orthogonale à C, donc dans $C^\perp$. Soit $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in C$. On a $p(x)h(x) = 0$ d'où $a_{i-k}h_k + a_{i-k+1}h_{k-1} + \cdots + a_ih_0 = 0$ pour $i = k, k + 1, \cdots, n - 1$. D'où

$$H \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

d'où les lignes de H sont $n - k$ vecteurs linéairement indépendants dans l'espace dual $C^\perp$. Donc H est une matrice génératrice de $C^\perp$ et par conséquent une matrice de contrôle de C.

EXEMPLE 5.2.9. *Écrivez les matrices génératrice et de contrôle du code cyclique de Hamming $Ham(3,2)$. Écrivez le code complet.*

On a montré que $g(x) = x^3 + x + 1$ est le polynôme générateur de $Ham(3,2)$ par l'exemple 5.2.12

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

le polynôme de contrôle est $h(x) = (x^7-1)/(x^3+x+1) = x^4+x^2+x+1$ par le Théorème .

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

est une matrice de contrôle de C.

THÉORÈME 5.2.10. *Le code binaire de Hamming $Ham(r,2)$ est équivalent à un code cyclique.*

Preuve : Soit $p(x)$ un polynôme irréductible dans $\mathbb{F}_2[x]$. On sait que $\mathbb{F}_2[x]/(p(x))$ est un corps dont les éléments s'écrivent $\{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^r-2}\}$ où α est un élément primitif. On associe chaque élément $a_0 + a_1x + a_2x^2 + \cdots + a_{r-1}x^{r-1} \in \mathbb{F}_2[x]/(p(x))$ avec le vecteur colonne

$$\begin{pmatrix} a_0 \\ a_1 \\ \cdots \\ a_{r-1} \end{pmatrix}$$

Soit $n = 2^r - 1$. La matrice $r \times n$

$$H = [1, \alpha, \alpha^2, \cdots, \alpha^{n-1}]$$

est une matrice de contrôle de $C = Ham(r,2)$ puisque ses colonnes sont les éléments non nuls de $\mathbb{F}_{2^r}$. On a

$$C = \{c(x) \in \mathcal{F}_n : c(\alpha) = 0\}$$

et C est cyclique.

Exercice : Quel est le polynôme générateur de $Ham(r,2)$?

COROLLAIRE 5.2.11. *Tout polynôme primitif dans $\mathbb{F}_{2^r}$ est un polynôme générateur du code cyclique de Hamming $Ham(r,2)$.*

Soit α un élément primitif de $\mathbb{F}_{2^r}$ et $p(x)$ son polynôme minimal. Alors $Ham(r,2) = (p(x))$.

EXEMPLE 5.2.12. *Trouvez le polynôme générateur du code cyclique* $Ham(3,2)$.

Le polynôme $p(x) = x^3+x+1$ *sur* $\mathbb{F}_2$ *est irréductible. Le sous-groupe multiplicatif du corps* $\mathbb{F}_2^3$ *est d'ordre 7, dont tout élément non nul est primitif. D'après le théorème* $(x^3 + x + 1) = Ham(3,2)$.

EXERCISE 5.3. *Ecrivez les matrices génératrice et de contrôle canoniques du code cyclique de Hamming* $Ham(3,2)$.

THÉORÈME 5.3.1. *Soit* C *un* $[n,k]$*-code sur un corps* $\mathbb{F}$ *de polynôme générateur* $g(x)$ *et* A *une matrice* $k \times (n-k)$ *dont la* i^{eme} *ligne est le reste de la division de* $x^{n-k+i-1}$ *par* $g(x)$, $i = 1, \cdots, k$. *Les matrices génératrice et de contrôle canoniques de* C *sont* $G = (I_k \vdots -A)$ *et* $H = (A^t \vdots I_{n-k})$ *respectivement.*

Preuve : Par $res_{g(x)}(f(x))$ on note le reste de la division euclidienne du polynôme $f(x)$ par $g(x)$.

On sait que $deg(g(x)) = n-k$. D'où $res_{g(x)}(x^j) = x^j$ pour $j < n-k$. Puisque $g(x)$ divise $x^n - 1$ on a $res_{g(x)}(x^{n+j}) = res_{g(x)}(x^j)$ pour tout $j \geq 0$. Il suffit alors de calculer $res_{g(x)}(x^j)$ seulement pour $j = n-k, \cdots, n-1$.

On pose $G_i(x) = x^{i-1} - x^k res_{g(x)}(x^{n-k+i-1})$ pour $i = 1, \cdots, k$. On a $deg(G_i(x)) < n$ d'où $G_i(x) \in \mathcal{F}_n$. De plus $x^{n-k+i-1} - res_{g(x)}(x^{n-k+i-1}) \in C$ d'où $G_i(x) = x^k(x^{n-k+i-1} - res_{g(x)}(x^{n-k+i-1})) \in C$.

Soit G la matrice $k \times n$ dont la i^e ligne est $G_i(x)$ (écrite comme vecteur) $i = 1, \cdots, k$, alors

$$G = (I_k \vdots -A)$$

où A est une matrice $k \times (n-k)$ dont la i^e ligne est $res_{g(x)}(x^{n-k+i-1})$. Les lignes de G sont des éléments de C et sont linéairement indépendantes. Donc G est la matrice canonique de C. D'où la matrice de contrôle canonique de C est $H = (A^t \vdots I_{n-k})$.

5.4. Décodage

Le théorème suivant montre qu'on n'a pas besoin d'avoir une matrice de contrôle d'un code linéaire cyclique pour calculer le syndrome.

THÉORÈME 5.4.1. *Soit* C *un* $[n,k]$*-code cyclique sur un corps* $\mathbb{F}$ *de polynôme générateur* $g(x)$. *Alors pour tout* $a \in \mathbb{F}^n$, *le syndrôme* $S(a)$ *est égale au reste de la division de* $x^{n-k}a(x)$ *par* $g(x)$.

Preuve : On sait par le Théorème 5.3.1 que $H^t = \binom{A}{I_{n-k}}$ où A est une matrice $k \times (n-k)$ dont la i^{eme} ligne est $res_{g(x)}(x^{n-k+i-1})$

, $i = 1, \cdots, k$. La i^{eme} ligne de I_{n-k} est x^{j-1}, $j = 1, \cdots, n-k$. En utilisant la relation $res_{g(x)}(x^{n+j}) = res_{g(x)}(x^j)$ on déduit que la i^{eme} ligne de H^t est $res_{g(x)}(x^{n-k+i-1})$, $i = 1, \cdots, n$.

Soit $a = a_0 a_1 \cdots a_{n-1}$ et $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{F}_n$

$$\begin{aligned} S(a) &= (a_0 a_1 \cdots a_{n-1})H^t \\ &= \sum_{i=1}^{n} a_{i-1} res_{g(x)}(x^{n-k+i-1}) \\ &= res_{g(x)}\left(\sum_{i=1}^{n} a_{i-1}x^{n-k+i-1}\right) \\ &= res_{g(x)}(x^{n-k}a(x)) \end{aligned}$$

REMARQUE 5.4.2. *Si C est un code cyclique de polynôme générateur $g(x)$, deux polynômes $a(x)$ et $b(x)$ sont dans la même classe si et seulement si $g(x)$ divise $a(x) - b(x)$ ce qui veut dire $res_{g(x)}(a(x)) = res_{g(x)}(b(x))$, donc on peut aussi définir le syndrome de $a(x)$ par $S(a) = res_{g(x)}(a(x))$*

EXERCISE 5.5. *Soit C un code cyclique de polynôme générateur $g(x)$ et H la matrice dont les lignes sont $res_{g(x)}(x^{j-1})$ pour $j = 1, \cdots, n$. Montrer que H est une matrice de contrôle de C.*

REMARQUE 5.5.1. *Dans le cas des codes cycliques, le polynôme générateur joue un rôle principale, contrairement aux matrice de génératrice et de contrôle.*

LEMME 5.5.2. *Soit $C \subset F_q^n$ un code linéaire de distance minimale d. Montrer qu'un mot $xinF_q^n$ est l'unique représentant de la classe $x+C$ si $\omega(x) \leq (d-1)/2$.*

COROLLAIRE 5.5.3. *Soit C un code cyclique de polynôme générateur $g(x)$. Soit y un mot reçu de syndrome $S(y)$. Si $deg(S(y)) =\leq [(d(C)-1)/2]$ alors $y(x)$ est décodé comme $y(x) - S(x)$.*

On a y et $S(y)$ sont dans la même classe de plus $S(y)$ est un représentant puisque $\omega(x) \leq (d-1)/2$.

LEMME 5.5.4. *Soit C un $[n,k]$-code cyclique de polynôme générateur $g(x)$ et $s(x) = \sum_{i=0}^{n-k-1} s_i x^i$ le syndrome de $c(x)$. Le syndrome de*

$$S(xc(x)) = xS(x) - s_{n-k-1}g(x) \tag{9}$$

Preuve : On divise $c(x)$ par $g(x)$ on obtient $c(x) = q(x)g(x) + S(x)$ d'où

$$xc(x) = xq(x)g(x) + xS(x) \quad (10)$$

$$= (xq(x) + s_{n-k-1})g(x) + (xS(x) - s_{n-k-1}g(x)). \quad (11)$$

Puisque $deg(xs(x) - s_{n-k-1}g(x)) < n - k = deg(g(x))$. on déduit le résultat.

EXEMPLE 5.5.5. *Soit le* $[7, 4]$*-code de polynôme générateur* $g(x) = 1 + x^2 + x^3$*. Le mot* $w = 0110110$*, s'écrit* $w(x) = x + x^2 + x^4 + x^5 = x + x^2g(x)$*. Donc* $S(w(x)) = x$ *s'écrit 010. Les syndromes de* $xw(x)$ *et* $x^2w(x)$ *sont* $xx = x^2$ *et* $xx^2 - g(x) = 1 + x^2$*, respectivement.*

Soit x un n-tuple. Un cycle de 0 de longueur ℓ est une succession de ℓ zéro consécutifs. Par exemple $(0, 0, 3, 2, 0, 0, 0, 1, 0, 0)$ a un cycle de 0 de longueur 4.

Algorithme de décodage. Soit C un $[n, k, d]$-code cyclique de polynôme générateur $g(x)$. $y(x)$ un mot reçu, $e(x)$ l'erreur telle que $\omega(e(x)) \leq (d-1)/2$ avec un cycle de 0 de longueur $\leq k$. Le but est de déterminer $e(x)$. On note $t = [(d-1)/2]$.

Étape 1 : calculer les syndromes de $S(x^i y(x))$ et on note $s_i(x) = S(x^i y(x))$ *mod* $g(x)$, pour $i = 0, 1, 2, \cdots$;

Étape 2 : trouver m tel que le $\omega(s_m(x)) \leq t$.

Étape 3 : calculer $e(x) = x^{n-m}s_m(x) \mod (x^n - 1)$. Décoder $y(x)$ par $y(x) - e(x)$.

Preuve : On montre l'existence de m de l'étape 2. $y(x) = c(x) + e(x)$ en multipliant $y(x)$ par x^m, on peut ramener le cycle de 0 de longueur $\leq k$ de $e(x)$ à la fin et les composantes non nulles dans les $n - k$ premières composantes. Soit $r(x) := ((x^m y(x) \ (mod x^n - 1)) \ (mod \ g(x))) = (x^m y(x) \ (mod \ g(x)))$. on a $\omega(r(x)) = \omega(e(x)) \leq t$. D'où l'existence de m.

On pose $p(x) := (x^{n-m}s_m(x) \ (mod \ x^n - 1))$

$$\begin{aligned} x^m(y(x) - p(x)) &\equiv x^m(y(x) - x^{n-m}s_m(x)) \\ &\equiv x^m y(x) - x^n s_m(x) \\ &\equiv s_m(x) - x^n s_m(x) \\ &\equiv (1 - x^n)s_m(x) \\ &\equiv 0 \ mod g(x) \end{aligned}$$

Puisque x^m et $g(x)$ sont premiers entre eux, $y(x) - p(x)$ est divisible par $g(x)$, $p(x)$ et $e(x)$ sont dans la même classe, d'où

$$e(x) = p(x) = (x^{n-m} s_m(x) \ (mod\ x^n - 1))$$

par le Lemme 5.5.2.

i	$s_i(x)$
0	$1 + x + x^2$
1	$1 + x$
2	$x + x^2$
3	1

EXEMPLE 5.5.6. *Déterminons tous les codes binaires cycliques de longueur 7. On a :*

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1) = (x+1)(x^3+x+1)(x^3+x^2+1).$$

Comme il y a trois facteurs, il y a $2^3 = 8$ *codes cycliques y compris* 0 *et* $\mathbb{F}_2^7$.
i) $1 = 1$, *engendre* $\mathbb{F}_2^7$
ii) $x + 1 = x + 1$, *engendre le code de parité*
iii) $x^3 + x + 1 = x^3 + x + 1$, *engendre le code [7, 4] de Hamming*
iv) $x^3 + x^2 + 1 = x^3 + x^2 + 1$, *engendre le code [7, 4] de Hamming*
v) $(x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$, *engendre le code [7, 3]*
vi) $(x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$, *engendre le code [7, 3]*
vii) $(x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, *engendre le code de répitition*
viii) $(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^7 + 1$, *engendre le code 0.*

5.6. Idempotents

En plus du polynôme générateur d'un code cyclique qui détermine ce dernier, il y a le polynôme idempotent.

Un élément e d'un anneau est appelé idempotent si $e^2 = e$.

THÉORÈME 5.6.1. *Soit C un code cyclique dans $\mathcal{F}_n$. Alors :*
i) il existe un unique idempotent $e(x) \in C$ tel que $C = (e(x))$,
ii) si $e(x)$ est un idempotent non nul de C, alors $C = (e(x))$ si et seulement si $e(x)$ est un unité de C.

Preuve :

THÉORÈME 5.6.2. *Soit C un code cyclique sur $\mathbb{F}_q$ de polynôme idempotent $e(x)$. Alors le polynôme générateur de C est $g(x) = pgcd(e(x), x^n - 1)$ dans $\mathbb{F}_q[x]$.*

Preuve :

THÉORÈME 5.6.3. *Soit C un $[n,k]$-code cyclique de polynôme idempotent $e(x) = \sum_{i=0}^{n-1} e_i x^i$. Alors la matrice $k \times n$ matrix*

$$\begin{pmatrix} e_0 & e_1 & e_2 & \cdots & e_{n-2} & e_{n-1} \\ e_{n-1} & e_0 & e_1 & \cdots & e_{n-3} & e_{n-2} \\ & & \cdots & & & \\ e_{n-k+1} & e_{n-k+2} & e_{n-k+3} & \cdots & e_{n-k-1} & e_{n-k} \end{pmatrix}$$

est une matrice génératrice de C.

Preuve :

Exercice : Combien y a t-il de codes cycliques triaires de longueur 4 ? Pour chacun déterminer un polynôme générateur et une matrice génératrice.

Exercice : Combien y a t-il de codes cycliques de longueur 8 sur $\mathbb{F}_3$? Donnez un polynôme générateur pour chacun.

Puisque $(1 + x^{2n}) = (1 + x^n)^2$, on a besoin de trouver seulement les facteurs de $1 + x^n$, où n est impair.

5.7. Codes quasi-cycliques

DÉFINITION 1. *Un code C de longueur n est quasi-cyclique d'ordre s où s est un diviseur de n si on a $\sigma^s(x) \in C$ pour tout $x \in C$ où σ est la permutation circulaire.*

Un code cyclique est un code quasi-cyclique d'ordre $s = 1$.

Si C est un code de longueur n alors C est quasi-cyclique d'ordre s pour tout s qui divise n.

Si C est un code quasi-cyclique d'ordre s alors le code dual $C^\perp$ est quasi-cyclique d'ordre s.

n	factorisation de (x^n-1) dans $\mathbb{Z}_2$
	$(1+x^{2n})=(1+x^n)^2$
1	$(1+x)$
3	$(1+x)(1+x+x^2)$
5	$(1+x)(1+x+x^2+x^3+x^4)$
7	$(1+x)(1+x+x^3)(1+x^2+x^3)$
9	$(1+x)(1+x+x^2)(1+x^3+x^6)$
11	$(1+x)(1+x+\cdots+x^9+x^{10})$
13	$(1+x)(1+x+\cdots+x^{11}+x^{12})$
15	$(1+x)(1+x+x^2)(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x^3+x^4)$
17	$(1+x)(1+x+x^2+x^4+x^6+x^7+x^8)(1+x^3+x^4+x^5+x^8)$
19	$(1+x)(1+x\cdots+x^{17}+x^{18})$
21	$(1+x)(1+x+x^2)(1+x^2+x^3)(1+x+x^3)$ $(1+x^2+x^4+x^5+x^6)(1+x+x^2+x^4+x^6)$
23	$(1+x)(1+x+x^5+x^6+x^7+x^9+x^{11})$ $(1+x^2+x^4+x^5+x^6+x^{10}+x^{11})$
25	$(1+x)(1+x+x^2+x^3+x^4)(1+x^5+x^{10}+x^{15}+x^{20})$
27	$(1+x)(1+x+x^2)(1+x^3+x^6)(1+x^9+x^{18})$
29	$(1+x)(1+x+\cdots+x^{27}+x^{28})$
31	$(1+x)(1+x^2+x^5)(1+x^3+x^5)(1+x+x^2+x^3+x^5)$ $(1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5)$

TABLE 1. Factorisation de (x^n-1) dans $\mathbb{Z}_2$

PROPOSITION 5.7.1. *Soit C est un $[n,k]$-code quasi-cyclique d'ordre s avec $n=rs$ alors il existe une matrice $k'\times n$ (où $k'\times k$) génératrice G de a forme :*

$$G=\begin{pmatrix} A_1 & A_2 & A_3 & \cdots & A_r \\ A_r & A_1 & A_2 & \cdots & A_{r-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2 & A_3 & A_4 & \cdots & A_1 \end{pmatrix}$$

où les A_i sont des matrice $\frac{k'}{r}\times s$.

Preuve : Par récurrence. Soit G^0une matrice $1\times n$ nulle et un mot aléatoire $c=(c_1,\cdots,c_n)$ de C. Partageons c en $r=n/s$ parties égales : $(c_1,\cdots,c_s)$, $(c_{s+1},\cdots,c_{2s})$, $\cdots$,$(c_{n-s+1},\cdots,c_n)$. On construit les matrices $1\times s$ $A_i^1=(c_{s(i-1)+1},\cdots,c_{si})$, $1\le i\le r$ obtenus par r shifs

cycliques. On considère alors la matrice

$$G = \begin{pmatrix} A_1^1 & A_2^1 & A_3^1 & \cdots & A_r^1 \\ A_r^1 & A_1^1 & A_2^1 & \cdots & A_{r-1}^1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2^1 & A_3^1 & A_4^1 & \cdots & A_1^1 \end{pmatrix}$$

elle engendre un code C_1, si $C_1 = C$ alors on arrête sinon on considère un mot $c_2$de C qui n'est pas dans C_1. On partage c_2 en s parties égales on ajoute la deuxième ligne à la matrice A_i^1 pour obtenir la matrice A_i^2. On considère alors les matrices G^2, G^3,$\cdots$, G^j,

Puisque le rang de matrice G^j crois strictement avec j, ça va s ?arrêter pour un certain j_0 vérifiant $k' = j_0.r \geq k$ puisque G^{j_0} engendre C. Remarquons que j_0 varie et dépend des élements aléatoires $c_1, c_2, \cdots$

REMARQUE 5.7.2. *1) Vu la forme de la matrice génératrice, il suffit de connaitre les matrices A_1,$\cdots$ A_n pour déduire la matrice G.*

2) La matrice G engendre le code C mais elle n'est pas nécessairement une matrice génératrice de C puisque k' peut être plus grand que k.

Dans ce qui suit nous montrons comment construire des sous-codes quasi-cycliques d'ordre s à partir d'un code quasi-cyclique d'ordre s.

THÉORÈME 1. *Soit C un $[n, k]$-code quasi-cyclique d'ordre s et $n = rs$. Alors il existe un sous-code quasi-cyclique d'ordre s strictement inclue dans C et de dimension $\geq k - r = k - \frac{n}{s}$.*

Si C est quasi-cyclique d'ordre s alors le dual $C^\perp$ de C est quasi-cyclique d'ordre s. Soit x un mot aléatoire de $F_2^n - C^\perp$ et considérons la matrice génératrice obtenue en ajoutant x et ses $r-1$ s-shift à une matrice génératrice de $C^\perp$. Le code C_x engendré par G_x est quasi-cyclique par construction d'ordre s et de dimension $n - k + r$. Le dual de $C_x^\perp$ est quasi-cyclique d'ordre s de dimension $\geq k - r = k - \frac{n}{s}$.

PROPOSITION 5.7.3. *Soit C un $[n, k]$-code quasi-cyclique d'ordre s. Alors au moins 2^{k-r} codes distincts peuvent être construit par le théorème précédant.*

Preuve : Le nombre de sous codes distinct est égale au nombre de duaux de ces codes distincts. Le code dual est dimension au plus $n - k + r$. L'union de tous les duaux possibles doit être l'espace en entier, puisque chaque code est de dimension au plus $n - k + r$ alors il y a au moins $2^{n-(n-k+r)} = 2^{k-r}$ sous-codes quasi-cycliques distincts.

5.8. Exercices

Exercice 2. Déterminer tous les codes cycliques binaires de longueur 7.

Exercice 3. Trouvez tous les codes binaires cycliques de longueur 4. Ainsi que ses matrices génératrice et de contrôle. De même pour 5, 6 et 7.

Exercice 4. Montrez que le code $Ham(2,3)$ n'est pas cyclique.

Exercice 5. Trouvez tous les codes triaires cycliques de longueur 4. Écrire une matrice de contrôle pour chacun d'entre eux.

Exercice 6. Montrer que le code $\{0000, 1001, 0110, 1111\}$ est équivalent à un code cyclique.

Exercice 7. Combien y a t-il de codes cycliques binaires de longueur 10.

Exercice 8. Soit C le code de longueur 7 sur $\mathbb{F}_2$ et de polynôme générateur $g(x) = x^3 + x + 1$.
1) Déterminer le polynôme de contrôle de C.
2) Déterminer une matrice génératrice et une matrice de contrôle de C.
3) C est-il un code de Hamming ?

Exercice 9. i) Montrer que le code binaire de Hamming H$am(r,2)$ est équivalent à un code cyclique.
ii) Quel est le polynôme générateur de $Ham(r,2)$?

Exercice 10. Soient C_1 et C_2 deux codes cycliques de polynômes générateurs $g_1(x)$ et $g_2(x)$ respectivement . Montrer que $C_1 \subset C_2$ si seulement si $g_2(x)$ divise $g_1(x)$.

Exercice 11. 1) Trouvez tous les codes linéaires cycliques trinaires de longueur 4.
2) Écrire une matrice de contrôle pour chacun des codes de la question 1).
3) Montrer que le code $Ham(2,3)$ n'est pas cyclique.

Exercice 12. Soit C_1 et C_2 deux codes cycliques sur $\mathbb{F}$ de longueur n et de polynômes générateurs $g_1(x)$ et $g_2(x)$ respectivement. Montrer que les ensembles suivants sont des codes cycliques sur $\mathbb{F}$ de longueur n et déterminer leur polynômes générateurs.
1) $C_1 \cap C_2$;

2) $C_1 + C_2$;
3) $\{c(x) \in \mathcal{F}_n : c(x) \equiv g_2(x)c_1(x)\ mod(x^n - 1), c_1(x) \in C_1\}$
(Indication : considérer d'abord le cas $pgcd(g_1(x), g_2(x)) = 1$).

Exercice 13. Soit m un mot non nul de $\mathbb{F}_q^n$ et soit C_m le sous-espace vectoriel de $\mathbb{F}_q^n$ engendré par la famille

$$\{\sigma^i(m) \mid i = 0, 1, \cdots, n-1\}.$$

1. Montrer que
(a) C_m est un code cyclique de longueur n.
(b) C_m est le plus petit code cyclique de longueur n sur $\mathbb{F}_q$ contenant le mot m.
(c) Le polynôme générateur du code C_m est le pgcd des polynômes $X^n - 1$ et $m(X)$.
2. Déterminer le polynôme générateur de C_m lorsque q = 3, n = 9 et m = 022011000.

Exercice 14. Dans $\mathbb{F}_2$, $(1+x)$ divise (x^n-1). Soit C le codes binaire cyclique de polynôme de polynôme générateur $1 + x$ et de longueur n. Soit C_1 un code quelconque binaire cyclique de polynôme générateur $g(x)$ et de longueur n.
a) Quelle est la dimension de C ?
b) Montrer que C est l'ensemble des vecteurs de $\mathbb{F}_2^n$ de poids pair.
c) Si C_1 a seulement des mots de poids pair, quelle relation y a-t-il entre $1 + x$ et $g(x)$?
d) Si C_1 a certains mots de poids impair, quelle relation y a-t-il entre $1 + x$ et $g(x)$?

Exercice 15. 1. Montrer, sans effectuer de division euclidienne, que dans $\mathbb{F}_3[X]$, le polynôme $g(x) = (X - 1)^5$ divise le polynôme $(X^9 - 1)$.
2. Soit C le code cyclique de longueur 9 sur $\mathbb{F}_3$, engendré par le polynôme g.
a) Quelle est la dimension de C ?
b) Quel est le nombre de mots de C ?
3. Développer le polynôme g dans $\mathbb{F}_3[X]$, en détaillant et justifiant les calculs.
4. Pourquoi la matrice

$$G = \begin{pmatrix} 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$

est-elle une matrice génératrice du code C ?
5. Montrer que C contient un mot de poids 3.
6. Montrer que le polynôme de contrôle de C est le polynôme $h(x) = X^4 + 2X^3 + 2X + 1$. 7. Déterminer une matrice de contrôle de C.
8. Déterminer la distance minimale du code C et le nombre d'erreurs que C peut corriger.
9. Le mot $m = 121102210$ est reçu.

a) Sous l'hypothèse d'au plus une erreur, quel est le mot de code émis ?

b) Quel est le message envoyé, sachant qu'il est encodé par la matrice G ?

Exercice 16. Code ternaire de Golay.

(1) Montrer que le polynôme cyclotomique Φ_{11} a pour facteurs irréductibles sur $\mathbb{F}_3$ polynômes $P(X) = X^5 + X^4 - X^3 + X^2 - 1$ et $Q(X) = X^5 - X^3 + X^2 - X - 1$ sur $\mathbb{F}_3$.

(2) On considère le code G_{11} engendré par $P(X)$. Donner sa longueur, sa dimension et montrer que sa distance minimale est 4 ou 5.

(3) Donner un générateur du sous-code pair de G_{11}.

(4) Montrer que G_{11} est la somme directe de son sous-code pair et du code engendré par Φ_{11}.

(5) On introduit la forme bilinéaire symétrique $\langle x, y\rangle$ sur $\mathbb{F}_3[X]/(X^{11}-1)$ pour laquelle $\{1, X, X^2, \cdots, X^{10}\}$ est une base orthonormale. Montrer que pour tout $x \in F_3[X]/(X^{11} - 1)$, on a $\omega(x) \equiv \langle x, x\rangle \ mod\ 3$ où $\omega(x)$ désigne le poids de x.

(6) Vérifier que G_{11} est orthogonal a son sous-code pair et calculer le poids de Φ_{11}.

(7) En déduire que, pour tout $x \in G_{11}$, $\omega(x) \equiv 0$ ou $2\ mod\ 3$ et que la distance minimale de G_{11} est 5.

(8) Montrer que le code G_{11} est parfait.

Le code G_{11} s'appelle code ternaire de Golay

Exercice 17. Soit C le code binaire linéaire de longueur 7 dont une matrice de contrôle est

$$H = \begin{pmatrix} 10000111010010110010110100011110 \end{pmatrix}$$

1. Combien valent la dimension et la distance de C ? Écrire une matrice génératrice de C.
2. Décoder les mots reçus $r_1 = 00001110$ et $r_2 = 00010011$, en supposant qu'il y a eu au plus une erreur de transmission.

3. Parmi les mots t_1 =????0000, t_2 =?0?0?0000 et t_3 =?0?0?0?0 qui ont subi des effacements, les autres bits ayant été transmis correctement, lesquels peut-on décoder ?
4. Le code C est-il MDS ? Cyclique ? Parfait ?
5. Montrer que, pour tout mode de code m de C, le mot $m + 11111111$ appartient à C. En déduire le nombre de mots de C de poids 4.
6. Montrer que C est équivalent au code étendu du code de Hamming Ham(8).
7. Montrer que C est son propre orthogonal.

Exercice 18. Soit $g(x)$ le polynôme générateur d'un code cyclique binaire C.
a) Montrer que si $x + 1$ divise $g(x)$ alors C ne contient aucun mot de poids impair.
b) Montrer que si n est impair et $x + 1$ ne divise pas $g(x)$ alors C contient le mot $1 \cdots 1$.
c) Montrer que si n est le plus petit entier tel que $g(x)$ divise $x^n + 1$ alors la distance minimale de C est au moins 3.
d) On suppose que C contient des mots de poids pairs et impaires. Soit $A(z)$ le polynôme énumérateur de poids de C. Montrer que le polynôme $(x+1)g(x)$ engendre un code cyclique binaire de polynôme énumérateur de poids $A_1(z) = \frac{1}{2}[A(z) + A(-z)]$.

Rappel ; le polynôme énumérateur de poids $A(X) = \sum_{i=0}^{n} A_i x^n$ où $A_i = |\{c \in C \mid \omega(c) = i\}|$

Exercice 19.
1. Montrer, sans effectuer de division euclidienne, que dans $\mathbb{F}_3[X]$, le polynôme $g(x) = (X-1)^5$ divise le polynôme $(X^9 - 1)$.
2. Soit C le code cyclique de longueur 9 sur $\mathbb{F}_3$, engendré par le polynôme g.
   a) Quelle est la dimension de C ?
   b) Quel est le nombre de mots de C ?
3. Développer le polynôme g dans $\mathbb{F}_3[X]$, en détaillant et justifiant les calculs.
4. Pourquoi la matrice

$$G = \begin{pmatrix} 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$

est-elle une matrice génératrice du code C ?
5. Montrer que C contient un mot de poids 3.
6. Montrer que le polynôme de contrôle de C est le polynôme $h(x) =$

$X^4 + 2X^3 + 2X + 1$. 7. Déterminer une matrice de contrôle de C.
8. Déterminer la distance minimale du code C et le nombre d'erreurs que C peut corriger.
9. Le mot $m = 121102210$ est reçu.

a) Sous l'hypothèse d'au plus une erreur, quel est le mot de code émis ?

b) Quel est le message envoyé, sachant qu'il est encodé par la matrice G ?

Bibliographie

[1] Blackmore, T., Norton, G.H. : Matrix-product codes over $\mathbb{F}_q$. Appl. Algebra Eng. Comm. Comput. 12(6), 477-500 (2001).

[2] W. Cary Huffman et Vera Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.

[3] J. H. van Lint, Introduction to Coding Theory, Springer.

[4] D. G. Hoffman, D. A. Leonard, Coding Theory the essentials, Marcel Dekker.

[5] C. E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J., 27, pp. 379-423, 623-656 (1948).

[6] Tietävïnen A. : On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. 24, 88-96 (1973).

[7] Matthieu Finiasz : Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie. Thèse doctorat, ÃĽcole Polytechnique.

[8] M. Van Der Vlugt, The True Dimension of Certain Binary Goppa Codes IEEE Trans. Inform. Theory 31, no. 2, pp 397-398, 1990.

[9] Reed, I. S. and Solomon, G., Polynomial Codes Over Certain Finite Fields, SIAM Journal of Applied Math., vol. 8, 1960, pp. 300-304.