UFR Sciences
M2 Calcul Formel M. WEIMANN

Codes correcteurs linéaires

1 Généralités

Un code correcteur sert à détecter et corriger des erreurs potentielles lors de la lecture ou la transmission des données sur un canal de communication peu fiable. La théorie a été initiée à la fin des années 1940 par C. Shannon, R. Hamming et M. J. E. Golay, dans le cadre de la théorie de l'information. C'est aujourd'hui un domaine très actif de la recherche à l'interface des mathématiques et de l'informatique. On peut citer quelques domaines d'applications :

– transmissions spatiales
– communications (téléphonie mobile, radio, internet, fibre optique)
– codes barres
– stockage (CD, DVD, disques durs, RAM,...)

L'idée générale est d'ajouter de la redondance d'information pour corriger les erreurs de transmissions. Cette idée n'est pas nouvelle : les aviateurs utilisent par exemple « Alpha Tango Charlie » pour transmettre correctement « ATC » à travers une radio, permettant de retrouver plus facilement le message originel en cas de friture.

Ce cours est destiné à une brève introduction à une famille de codes très utilisés en pratique, *les codes linéaires*. Les corps finis sont des éléments clés de la théorie.

Références : Ce cours s'inspire en grande partie des références suivantes :
- Notes de cours de Gilles Zémor *https ://www.math.u-bordeaux.fr/ gzemor/codes06.pdf*
- Notes de Coste, Pogam, Quarez *https ://agreg-maths.univ-rennes1.fr/documentation/docs/codes.pdf*
- Le livre *Cours d'Algèbre* de Demazure.

1.1 Principe général

On veut transmettre un message de longueur donnée, disons une suite $a = (a_1, \ldots, a_k)$ de k lettres $a_i \in \mathbb{F}$ d'un alphabet donné $\mathbb{F}$. On dit que a est le *mot source*. Le mécanisme de codage consiste à associer à chaque mot source possible a un mot distinct m de n lettres (avec $n > k$), appelé *mot code*. Autrement dit, coder les mots sources revient à considérer une injection $\mathbb{F}^k \hookrightarrow \mathbb{F}^n$. L'ensemble des mots de code $C \subset \mathbb{F}^n$ ainsi obtenu forme par définition un code. Le mot de code m est ensuite transmis. Le canal de transmission pouvant introduire des erreurs, on obtient à la sortie de ce canal, au lieu de m, un mot m'. Il s'agit, à partir de m', de reconstituer dans la mesure du possible m (correction), puis a (décodage).

$$a \in \mathbb{F}^k \overset{\text{codage}}{\longrightarrow} m \in C \subset \mathbb{F}^n \overset{\text{transmission}}{\longrightarrow} m' \in \mathbb{F}^n \overset{\text{correction}}{\longrightarrow} m \in \mathbb{F}^n \overset{\text{decodage}}{\longrightarrow} a \in \mathbb{F}^k$$

L'application de codage et son application réciproque de décodage jouent ici des rôles mineurs. Le problème essentiel est la construction du code lui-même, i.e. déterminer un ensemble de mots

$C \subset \mathbb{F}^n$ de n lettres choisis de façon à rendre possible (et numériquement praticable) l'opération de correction.

Un bon code doit obéir à trois principes fondamentaux :

- Un bon rendement (taux) c'est-à-dire un grand nombre de bits d'information par rapport aux bits codés (c'est le rapport k/n)
- Une bonne capacité de détection et correction d'erreurs.
- Une procédure de décodage (et de codage) suffisamment simple et rapide.

Tout le problème de la théorie des codes correcteurs d'erreurs est là : construire des codes qui détectent et corrigent le plus d'erreurs possible, tout en allongeant le moins possible les messages, et qui soient faciles à décoder.

1.2 Détection d'erreur *vs* correction d'erreur

Certains codes permettent de détecter une erreur, mais pas nécessairement de la corriger. C'est le cas par exemple du protocole TCP sur internet. Si une erreur est détectée, le destinataire demande à l'expéditeur de renvoyer son message. Considérons deux exemples concrets pour illustrer la différence.

Code de parité (détection) : à 7 bits de données, on ajoute 1 bit (dit de parité) valant 1 s'il y a un nombre impair de 1, et 0 sinon (somme dans $\mathbb{F}_2$). Si à la réception un des 8 bits est erroné, le bit de parité permet de détecter une erreur, mais ne permet pas de la localiser, donc de la corriger.

Code de répétition (détection et correction) : pour un bit d'information, 3 bits sont envoyés (cad codés) en respectant

$$0 \mapsto 000 \qquad \text{et} \qquad 1 \mapsto 111$$

Le décodage se fait par vote majoritaire. Par exemple, si le mot reçu est 001, alors on déduit que le bit émis était 0. Si au plus une erreur est commise, ce code permet de la détecter et de la corriger.

Exercice 1 En plus du bit de parité, on ajoute au code de parité la somme pondérée $S = \sum_{i=1}^{7} i x_i$ des bits de données (que l'on représente en pratique en base 2). Montrer que le code ainsi obtenu permet de détecter *et corriger* une erreur.

Corrigé. En supposant que le bit de parité détecte une erreur sur l'un des x_i, la position du bit altéré se calcule via $i = S - S'$ où S' est la somme pondérée des bits de données reçus. Il suffit alors de modifier le i-ème bit reçu.

2 Codes en blocs, distance de Hamming

Un code en bloc est un code correcteur traitant des messages de longueur fixe [1], relevant donc du principe général de codage présenté en Section 1.1. Les messages passant dans le canal de transmission sont supposés découpés en mots (blocs) de longueur n écrits avec un alphabet $\mathbb{F}$ de taille q. L'ensemble de tous les mots possibles est donc $\mathbb{F}^n$, de cardinal q^n.

Définition 1 Un code sur $\mathbb{F}$ de longueur n est un sous-ensemble C de $\mathbb{F}^n$. Lorsque $\mathbb{F} = \{0, 1\}$, ce qui est le cas le plus fréquemment étudié, on parle alors de *code binaire*.

1. D'autres types de codes existent, les codes convolutifs : la sortie d'un codeur convolutif dépend de l'information courante à coder ainsi que de l'information précédente et l'état du codeur. Nous ne les aborderons pas dans ce cours.

Il est à noter que certains auteurs définissent un code comme une application injective

$$\phi : \mathbb{F}^k \to \mathbb{F}^n.$$

Ici $\mathbb{F}^k$ représente les mots de la source (l'information que l'on veut transmettre), et $C = \mathrm{Im}(\phi)$ représente les mots du code (information transmise). Par exemple, le code de répétition $C = \{000, 111\}$ correspond au codage $\phi : \{0,1\} \to \{0,1\}^3$ défini par $0 \mapsto 000$ et $1 \mapsto 111$.

Définition 2 La *distance de Hamming* entre deux mots $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ est le nombre de coordonnées distinctes,

$$d(x, y) = \mathrm{Card}\{i \mid x_i \neq y_i\}.$$

La *distance minimum* du code C est la distance minimale entre deux mots de code distincts,

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

Exercice 2 Montrer que la distance de Hamming définit bien une distance sur $\mathbb{F}^n$.

Le mot $m \in C$ est émis et, après d'éventuelles erreurs de transmission, le mot $m' \in \mathbb{F}^n$ est reçu. Si $m' \notin C$, une erreur est détectée. On corrige alors le mot m' selon le *principe du maximum de vraisemblance* : on considère que le bon mot est le mot de C le plus proche de m' pour la distance de Hamming. Il faut bien sûr que ce "mot de code le plus proche" soit unique.

Lemme 1 Un code C de distance minimum d permet de *détecter* $d - 1$ erreurs, et pas plus. Il permet de *détecter et corriger* $\lfloor (d-1)/2 \rfloor$ erreurs, et pas plus.

Preuve. Soit x le mot émis et y le mot reçu. Si $d(x, y) < d$, alors soit $y \notin C$ et l'erreur est détectée, soit $x = y$ (aucune erreur). Si $d(x, y) \geq d$, on peut avoir $y \neq x$ et $y \in C$ et l'erreur n'est pas détectée. Pour le second point, on remarque que $t = \lfloor (d-1)/2 \rfloor$ est le rayon maximal pour lequel les boules fermées de $\mathbb{F}^n$ (muni de la distance de Hamming) de centres les éléments de C et de rayon t sont disjointes. Ainsi, si $x \in C$ est le mot émis et si y le mot reçu vérifie $d(x, y) \leq t$, le mot de C le plus proche de y est nécessairement x. Si au contraire $d(x, y) > t$, le mot de C le plus proche de y ne correspondra pas au bon mot x. □.

Exercice 3 Combien d'erreurs le code de répétition $C = \{000, 111\} \subset \{0,1\}^3$ peut-il détecter au maximum ? Combien d'erreurs peut-il corriger au maximum ?

Corrigé. On a ici $d = 3$. Donc on peut détecter 2 erreurs au maximum et corriger 1 erreur au maximum. Si par exemple le mot reçu est 001, l'erreur est détectée. S'il y a au plus une erreur, on sait que le bon mot est 000, mais si deux erreurs sont autorisées, on ne peut pas retrouver le bon mot.

On dira que C est *t-correcteur* (ou corrige t erreurs) quand toute erreur portant sur au plus t coordonnées est *détectée et corrigée* correctement. Ainsi, le Lemme 1 assure que C est t-correcteur si et seulement si la distance minimum d de C vérifie

$$d \geq 2t + 1.$$

3 Codes linéaires

Afin de construire des codes de petite distance minimum, on ajoute de la structure linéaire. Pour ce faire, on suppose que notre alphabet $\mathbb{F}$ est un corps fini à q éléments, $\mathbb{F} = \mathbb{F}_q$. Les mots de longueurs n sont donc des vecteurs de $\mathbb{F}^n$, que l'on écrira comme des vecteurs lignes.

3.1 Définitions

Définition 3 Un *code linéaire* de longueur n sur un corps fini $\mathbb{F}$ est un sous-espace vectoriel $C \subset \mathbb{F}^n$. La *dimension* k du code C est sa dimension en tant que $\mathbb{F}$-espace vectoriel.

Le *poids de Hamming* d'un mot $x \in \mathbb{F}^n$, noté $w(x)$, est le nombre de coordonnées non nulles. On a donc $d(x,y) = w(x-y)$ et la structure d'espace vectoriel de C conduit à la formule (pourquoi ?)

$$d = \min\{w(x), x \in C \setminus \{0\}\}.$$

Un premier avantage des codes linéaires est que la distance minimale se calcule plus rapidement.

Exercice 4 Notons $N = q^k$. Montrez que le calcul de la distance minimum d'un code linéaire ne nécessite que $O(nN)$ tests à zéro au lieu de $O(nN^2)$ tests d'égalité pour un code en bloc quelconque.

Corrigé. Calculer le poids d'un mot coûte n tests à zéros dans $\mathbb{F}$. On a Card C = Card $\mathbb{F}^q = N$. Si C est linéaire, il faut donc calculer le poids des $N-1$ mots non nuls de C. Si C est quelconque, il faut calculer un poids pour chacune des $\binom{N}{2} = O(N^2)$ paires de mots distincts. □

On dit que $[n,k,d)]$ sont *les paramètres* de C, ou encore que C est de type $[n,k,d]$. Le quotient $0 \leq k/n \leq 1$ est *le taux de transmission*, rapport entre la longueur k des mots de la source et la longueur n des mots du code.

Exercice 5 Soit C un code linéaire binaire de type $[n,k,d]$. On définit le code étendu $\bar{C}$ comme le code formé des mots $(x_1,\ldots,x_{n+1}) \in \mathbb{F}_2^{n+1}$ tels que $(x_1,\ldots,x_n) \in C$ et $\sum_{i=1}^{n+1} x_i = 0$. Montrer que $\bar{C}$ est de type $[n+1,k,d]$ si d est pair, et de type $[n+1,k,d+1]$ sinon.

Corrigé. $\bar{C}$ est de longueur $n+1$. Notons $\sigma(x_1,\ldots,x_n) = x_1 + \cdots + x_n$. L'application $C \to \mathbb{F}_2^{n+1}$ définie par $x \mapsto (x,\sigma(x))$ est linéaire injective, d'image $\bar{C}$ (caractéristique 2). Donc $\dim \bar{C} = k$. On a $w(x,\sigma(x)) = w(x)$ si $\sigma(x) = 0$, i.e. si le nombre de coordonnées non nulles $w(x)$ est pair et $w(x,\sigma(x)) = w(x)+1$ sinon. Le résultat s'ensuit. □

Lemme 2 (borne de Singleton) On a toujours $d \leq n-k+1$. On dit qu'un code est MDS [2] s'il y a égalité.

Exercice 6 (**A faire !**) Vérifiez cette inégalité en intersectant C avec le sous espace de $\mathbb{F}^n$ formé des mots dont les $k-1$ premières coordonnées sont nulles.

Corrigé. Le sous-espace $V \subset \mathbb{F}^n$ formé des mots dont les $k-1$ premières coordonnées sont nulles est de dimension $n-k+1$ de sorte que $\dim(C)+\dim(V) = n+1$ et donc $C \cap V \neq \{0\}$. Si $x \in C \cap V \setminus \{0\}$, on a $w(x) \leq n-k+1$. □

La borne de Singleton quantifie le fait qu'on ne peut pas avoir à la fois une capacité de correction importante et un nombre de mots de code important, pour une longueur n fixée. Il faut nécessairement faire des compromis. Il existe d'autres bornes.

Lemme 3 (borne de Hamming) Soit C un code de type $[n,k,d]$ et soit $t = \lfloor (d-1)/2 \rfloor$. On a l'inégalité

$$1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \leq q^{n-k}.$$

On dit que le code C est *parfait* s'il y a égalité. Un code est parfait si et seulement si $\mathbb{F}^n$ est réunion disjointe de boules de rayon t centrées en les mots de C.

2. acronyme anglais de Maximum Distance Separable, que l'on peut penser comme Majoration De Singleton.

Exercice 7 (A faire !) Montrer ce lemme (quel est le cardinal d'une boule de rayon t) ?

Corrigé. Puisque C est t-correcteur d'après le Lemme 1, les boules (fermées) centrées en les mots de C de rayon t sont disjointes. Les boules ayant même cardinal N, on a donc $N \operatorname{Card}(C) \leq \operatorname{Card}(\mathbb{F}^n)$, soit $N \leq q^{n-k}$. On a $y \in B(x,t)$ (boule fermée) si et seulement si y a exactement i parmi ses n coordonnées qui sont distinctes des coordonnées de x, où $i \in \{0,\ldots,t\}$. Il y a $q-1$ possibilités pour chacune de ces i coordonnées, d'où $N = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$. □

3.2 Matrices génératrices

Définition 4 Une matrice génératrice d'un code linéaire C est une matrice G dont les lignes forment une base de C.

Une matrice génératrice est donc de taille $k \times n$ et de rang k. Si m est un vecteur ligne de $\mathbb{F}^k$, le produit mG est un mot du code C et l'application $m \mapsto mG$ est un isomorphisme de $\mathbb{F}^k$ sur C (que l'on peut voir comme une opération de codage). On dit que le codage est *systématique* si la matrice G est de la forme (I_k, A). Dans ce cas, les k premiers bits d'un mot de code portent l'information (on y recopie le vecteur de $\mathbb{F}^k$), les $n-k$ suivants sont de la redondance.

Exemple 1 Sur $\mathbb{F} = \mathbb{F}_2$, la matrice

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

est une matrice génératrice pour le code

$$C = (00000, 10000, 11010, 11101, 01010, 01101, 00111, 10111).$$

Ce code est de type $[5, 3, 1]$.

Deux matrices G et G' engendrent le même code si et seulement s'il existe une matrice inversible P de taille $k \times k$ telle que $G = PG'$, ce qui revient à effectuer des permutations et des combinaisons linéaires réversibles de lignes (changement de base du sous-espace vectoriel $C \subset \mathbb{F}^n$).

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.

Lemme 4 Deux codes équivalents ont même type. De plus, tout code est équivalent à un code donné par un codage systématique.

Exercice 8 (A faire !) Prouver le lemme 3.

Correction. Deux codes équivalents ont même longueur n et même dimension k (le caractère libre/lié d'une famille de vecteur est invariant par permutation de coordonnées). Le poids d'un mot est également invariant par permutation des coordonnées. Donc la distance minimale d l'est aussi. Le second point se déduit du fait que toute matrice G admet une forme échelonnée réduite en ligne $G' = PG$, avec P inversible. Le code engendré par G et G' est le même. La matrice G' étant de rang k et échelonnée réduite en ligne, elle devient de la forme (I_k, A) après une permutation convenable de ses colonnes. □

Exemple 2 Soit $C \subset \mathbb{F}_2^4$ le code de matrice génératrice

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

L'algorithme de Gauss-Jordan (changement de base pour le code C) fournit la nouvelle matrice génératrice de C sous forme échelonnée réduite

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

En permutant les colonnes 3 et 4, on obtient la matrice génératrice

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

qui engendre un nouveau code C' équivalent à C, donné cette fois par codage systématique, correspondant à l'application

$$(x_1, x_2, x_3) \longmapsto (x_1, x_2, x_3, x_2, x_1 + x_3)$$

3.3 Matrice de contrôle

On peut aussi se donner un sous-espace vectoriel par un système d'équations indépendantes. Soit C un code linéaire.

Définition 5 Une matrice de contrôle (ou de parité) de C est la matrice d'un système d'équations linéaires homogènes indépendantes dont l'espace des solutions est C.

Autrement dit, une matrice de contrôle H est une matrice de taille $(n-k) \times n$ et de rang $n-k$ qui vérifie

$$C = \{x \in \mathbb{F}^n\,,\ H\,{}^t x = 0\}.$$

Exercice 9 Justifier que la matrice de contrôle peut se voir comme une matrice génératrice du code dual

$$C^\perp := \{y \in \mathbb{F}^n,\ y \cdot c = 0\ \forall\, c \in C\}$$

où $\cdot$ désigne le produit scalaire usuel.

Correction. Les $n-k$ lignes de H sont par définition dans $C^\perp$, et linéairement indépendantes. Comme $\dim C^\perp = n - \dim C = n-k$, elles forment une base de $C^\perp$. □

Exercice 10 Justifier que si C est donné sous forme systématique par la matrice génératrice $G = (I_k, A)$, alors $H = (-{}^t A, I_{n-k})$ est une matrice de contrôle de C.

Correction. Soit $H = (-{}^t A, I_{n-k})$. On remarque que H est de de taille $(n-k) \times n$ et de rang $n-k$, son noyau est donc de dimension $k = \dim C$. On vérifie que $H \cdot {}^t G = 0$. Donc $C \subset \ker(H)$. Donc $\ker(H) = C$. □

On peut calculer la distance minimale via la matrice de contrôle grâce au *lemme important* suivant.

Lemme 5 Soit H une matrice de contrôle du code C. La distance minimum d de C est caractérisée par les propriétés suivantes :

- $d-1$ colonnes de H sont toujours linéairement indépendantes.
- Il y a un système de d colonnes de H qui est lié.

Preuve. Soit d l'unique entier tel que $d-1$ colonnes de H sont toujours linéairement indépendantes et tel qu'il existe d colonnes de H liées. Soit c un mot de code non nul. On a $H^t c = 0$. Si $w(c) < d$ alors on a relation non triviale entre moins de d colonnes de H, contredisant notre hypothèse. Donc $d_{\min}(C) \geq d$. D'un autre côté, la relation entre d colonnes de H fournit un mot $c \in C$ de poids $\leq d$. Donc $d_{\min}(C) = d$. □

Remarquer que le lemme implique que le rang $n-k$ de H est au moins $d-1$: on retrouve la borne de Singleton.

Exemple 3 Calculons la distance minimum d du code C de l'exemple 2. D'après le Lemme 4, d est aussi la distance minimum du code équivalent C' de codage systématique

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

(exemple 2). D'après l'exercice 9, le code C' admet pour matrice de contrôle

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

et le lemme 5 assure que $d = 2$ (chaque famille de 1 colonne est libre et il existe 2 colonnes liées).

3.4 Décodage (ou plutôt correction) par syndrome.

Soit $C \subset \mathbb{F}^n$ un code linéaire de matrice de contrôle H. Le *syndrome* d'un vecteur $r \in \mathbb{F}^n$ (mot reçu) est le vecteur colonne

$$\sigma(r) = H^t r \ \in \ \mathbb{F}^{n-k}$$

Autrement dit, $\sigma(r) = \sum_{i=1}^{n} r_i H_i$ où les r_i sont les coordonnées de r et les H_i les colonnes de H. *Le syndrome est nul si et seulement si* $r \in C$. L'application syndrome $\sigma : \mathbb{F}^n \to \mathbb{F}^{n-k}$ induit donc un isomorphisme du quotient $\mathbb{F}^n/C$ sur $\mathbb{F}^{n-k}$.

Supposons que $c \in C$ est le mot du code envoyé et $r \in \mathbb{F}^n$ est le mot reçu. La différence $e = r - c$ est le *vecteur d'erreur*. Son poids $w(e)$ est le nombre de bits erronés dans le mot reçu. On a $\sigma(r) = \sigma(e)$. Si le syndrome est non nul, on corrige le mot reçu r en appliquant le principe du maximum de vraisemblance : on considère que le bon mot est le mot de C le plus proche de r. Autrement dit, on cherche e tel que :

— $\sigma(e) = \sigma(r)$ (ce qui équivaut à $r - e \in C$)

— $w(e)$ est minimal.

Autrement dit, *on soustrait à r un mot de poids minimum dans sa classe modulo C*. Dans le cas où $w(e) < d/2$, alors e est uniquement déterminé et on récupère $c = r - e$ sans ambiguïté.

Exemple 4 Soit $C \subset \mathbb{F}_2^6$ le code binaire de dimension 3 donné par la matrice de contrôle

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

Pour établir le décodage de ce code, on calcule tout d'abord des représentants de poids minimal

(appelés leader) pour chacune des classes d'erreur de $\mathbb{F}_2^6/C$, ainsi que leurs syndromes.

Leader	*Syndrome*
000000	000
100000	110
010000	101
001000	011
000100	100
000010	010
000001	001
100001	111

Supposons que $r = 100011$ est reçu. Son syndrome est $\sigma(r) = H^t r = 101$. Pour décoder r il faut donc lui soustraire le leader $e = 010000$, et le mot du code envoyé est donc $c = 110011$.

Remarque 1 Une fois la liste des leaders établies, le décodage est très rapide. Mais établir la liste des leaders (de manière exhaustive) coûte cher, $O(2^n)$ opérations binaires.

Une autre approche est la suivante : on cherche à corriger au plus $t = \lfloor (d-1)/2 \rfloor$ erreurs. Pour chaque mot reçu, il y a donc en pratique $O(n^t)$ vecteurs d'erreurs à explorer (cardinal d'une boule de rayon t) : étant donné un mot reçu r, on regarde alors si $r - e \in C$ (i.e. si $\sigma(e) = \sigma(r)$) pour tous les vecteurs d'erreurs possibles. Si aucune solution : trop d'erreurs. Sinon, un seul vecteur d'erreur e convient, et $c = r - e$ est nécessairement le bon mot (il ne peut y avoir plus de deux solutions par choix de t). Le coût est en $O(n^{t+1})$, plus efficace que $O(2^n)$ dès lors que $t << n/\log(n)$, mais il faut répéter l'opération pour chaque mot reçu.

De manière général, le décodage par syndrome (chercher des petits vecteurs dans des sous-espaces affines) est un problème difficile, sur lequel sont d'ailleurs basés certains cryptosystèmes (McEliece, Niederreiter).

4 Quelques codes linéaires

4.1 Codes de Hamming

Définition 6 Un code de Hamming binaire est obtenu en prenant comme matrice de contrôle H la matrice dont les colonnes sont, en notation binaire, tous les entiers de 1 à $2^m - 1$.

La matrice H est donc constituée de toutes les colonnes non nulles possibles de $\mathbb{F}_2^m$.

Lemme 6 Le code de Hamming est un code de paramètres $[2^m - 1, 2^m - 1 - m, 3]$. Ce code est parfait.

Preuve. La matrice H est de taille $m \times (2^m - 1)$ et de rang maximal m. Donc le code est de longueur $n = 2^m - 1$ et de dimension $k = 2^m - 1 - m$. Il est facile de voir que 2 colonnes (non nulles par définition) sont nécessairement linéairement indépendantes (i.e. distinctes sur $\mathbb{F}_2$) et qu'il existe 3 colonnes liées. Donc $d = 3$ d'après le lemme 5. On a ici $\lfloor (d-1)/2 \rfloor = 1$ et on vérifie que l'inégalité du Lemme 3 est une égalité, donc le code est parfait. □

Exemple 5 Le code du minitel est le code de Hamming $[128, 120, 3]$. Ce qui correspond à coder 15 octets à l'aide d'un octet supplémentaire pour corriger une erreur.

Décodage. Un autre intérêt des codes de Hamming est que l'on peut décrire facilement un procédé de décodage : si on reçoit r de syndrome $\sigma(r) = H^t r$ non nul, on cherche un vecteur d'erreur e de

poids 1 telle que $H^t e = H^t r$. Or si e a son unique 1 en i-ème position, alors $H^t e$ est la i-ème colonne de H, qui correspond par définition à l'écriture binaire de l'entier i. Il faut donc corriger le i-ème bit du mot reçu, où i est l'entier dont l'écriture binaire est $H^t r$.

Exemple 6 Le code de Hamming de longueur 7 est donné par la matrice de contrôle

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

Ce code est parfait, de type $[7, 4, 3]$, permettant de corriger une erreur. Supposons que le mot reçu soit $r = 0111010$ et qu'au plus une erreur a été commise. On calcule le syndrome $\sigma(r) = 110$, non nul, qui correspond à l'écriture binaire de $i = 3$. Il faut donc modifier le 3-ème bit de r. Le bon mot de code est ainsi $c = 0101010$.

Exercice 11 Donner une matrice génératrice du code de Hamming $[7, 4, 3]$. Peut-on donner ce code par un codage systématique ?

Corrigé. Il suffit de calculer la matrice dont les lignes forment une base du noyau de H. Une autre approche possible est d'utiliser l'exercice 9. On transforme (si possible) H en une matrice $H' = (-{}^t A, I_3)$ par permutation et combinaison linéaires de lignes (on a $H' = PH$ pour une matrice inversible P, le code reste donc le même). Une matrice génératrice est alors $G = (I_4, A)$, donnant un codage systématique du code. On trouve ici

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

Une matrice génératrice est donc

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

Ce codage est systématique. □

Codes de Hamming q-aires. On prend cette fois pour colonnes de H un ensemble maximal d'éléments de $\mathbb{F}_q^m$ avec la propriété qu'aucun élément de l'ensemble n'est multiple d'un autre. On obtient un code de paramètres $[n = (q^m - 1)/(q - 1), n - m, 3]$. Il est encore parfait.

Il existe deux autres, et deux autres seulement, codes linéaires parfaits non triviaux, à savoir les codes de Golay, respectivement binaires et ternaires et de paramètres $[23, 12, 7]$ et $[11, 6, 5]$.

4.2 Codes BCH binaires

Soit m un entier et soit α un générateur du groupe des unités $\mathbb{F}_{2^m}^\times$. On note $n = 2^m - 1$, de sorte que $\alpha^n = 1$ et les éléments de $\mathbb{F}_{2^m}$ sont $0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ (i.e. α est une racine primitive n-ème de l'unité). Soit δ un entier. On considère la matrice

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \cdots & \alpha^{(\delta-1)(n-1)} \end{pmatrix},$$

que l'on considère à coefficients dans $\mathbb{F}_2$, en remplaçant chaque élément α^j du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_{2^m}$ par la colonne de ses coefficients dans une base donnée.

Définition 7 On a appelle code BCH [3] binaire (primitif) de longueur n et de distance prescrite δ le code linéaire $C = \ker(H) \subset \mathbb{F}_2^n$.

Attention, la matrice H n'est pas nécessairement ici de rang maximal : elle admet $m(\delta - 1)$ lignes après substitution des α^j par leurs vecteurs colonnes, mais on ne peut pas dire si ces lignes sont $\mathbb{F}_2$-linéairement indépendantes. Ce code est donc de dimension $k \geq n - m(\delta - 1)$.

Lemme 7 Le code BCH binaire C associé à H a pour paramètres $[n, k, d]$,avec $n = 2^m - 1$, $k \geq n - m(\delta - 1)$ et $d \geq \delta$.

Preuve. Il reste à montrer que $d \geq \delta$, c'est à dire que tout mot non nul $c \in C$ est de poids $\geq \delta$. Supposons au contraire qu'il existe $c = (c_0, \ldots, c_{n-1}) \in C$ non nul avec $\leq \delta - 1$ coordonnées non nulles. Du fait de l'égalité $H^t c = 0$, on obtient alors une dépendance $\mathbb{F}_2$-linéaire non triviale entre δ colonnes distinctes de H, soit

$$\sum_{i=1}^{\delta-1} c_i \begin{pmatrix} \alpha^{j_i} \\ \alpha^{2j_i} \\ \vdots \\ \alpha^{(\delta-1)j_i} \end{pmatrix} = 0,$$

pour une famille d'indice $0 \leq j_1 < j_2 < \cdots < j_{\delta-1} \leq n - 1$. Or on remarque que le système linéaire sous-jacent (vu à coefficients dans $\mathbb{F}_{2^m}$) est un système de Vandermonde. Ayant un noyau non trivial, il existe donc au moins deux indices j_s, j_t tels que $\alpha^{j_s} = \alpha^{j_t}$, contredisant que α est une racine primitive n-ème de l'unité. □

Remarque 2 Ces codes BCH sont dits *primitifs*. Il existe d'autres familles de codes BCH construits en considérant des racines non primitives de l'unité.

5 Codes cycliques

On met maintenant encore plus de structure sur l'espace des mots : il s'agit maintenant d'une structure d'algèbre sur le corps $\mathbb{F}$.

5.1 Définitions

Un code linéaire $C \subset \mathbb{F}^n$ est dit *cyclique* quand il est stable par l'automorphisme de décalage cyclique

$$\begin{array}{rcl} T : \mathbb{F}^n & \longrightarrow & \mathbb{F}^n \\ (x_0, \ldots, x_{n-1}) & \longmapsto & (x_{n-1}, x_0, \ldots, x_{n-2}) \end{array}$$

On identifie $\mathbb{F}^n$ à l'algèbre quotient $\mathbb{F}[X]/(X^n - 1)$ via l'isomorphisme de $\mathbb{F}$-espace vectoriels

$$(x_0, \ldots, x_{n-1}) \longmapsto x_0 + x_1 X + \cdots + x_{n-1} X^{n-1}$$

On désigne ici abusivement par la même lettre l'indéterminée X et son image dans le quotient. Remarquer que tout polynôme de $\mathbb{F}[X]$ est congru modulo $X^n - 1$ à un unique polynôme de degré $< n$ (son reste dans la division euclidienne par $X^n - 1$).

3. Des initiales de ses inventeurs : Bose, Ray-Chaudhuri et Hocquenghem.

L'endomorphisme T, modulo cette identification, est l'endomorphisme de multiplication par X :

$$\begin{aligned} T(x_0 + x_1X + \cdots + x_{n-1}X^{n-1}) &:= x_{n-1} + x_0X + \cdots + x_{n-2}X^{n-1} \\ &= X(x_0 + x_1X + \cdots + x_{n-1}X^{n-1}) \mod (X^n - 1) \end{aligned}$$

Par définition, un code cyclique est donc un sous-espace vectoriel stable par multiplication par X, et donc par n'importe quel polynôme en X. Ainsi :

Lemme 8 Un code linéaire C de longueur n est cyclique si et seulement si C est un idéal de $\mathbb{F}[X]/(X^n - 1)$. □

5.2 Polynôme générateur, base, dimension

L'homorphisme de passage au quotient $\mathbb{F}[X] \to \mathbb{F}[X]/(X^n - 1)$ induit une bijection entre l'ensemble des idéaux de $\mathbb{F}[X]/(X^n - 1)$ et l'ensemble des idéaux de $\mathbb{F}[X]$ qui contiennent $X^n - 1$. Puisque $\mathbb{F}[X]$ est principal, ce sont exactement les idéaux engendrés par les diviseurs (que l'on prend unitaires pour assurer l'unicité) de $X^n - 1$ dans $\mathbb{F}[X]$. Autrement dit :

Lemme 9 Un code cyclique C est uniquement déterminé par un diviseur unitaire g de $X^n - 1$. Le polynôme g s'appelle le *polynôme générateur* de C.

Si $g = X^n - 1$, le code C est nul. Sinon, $\deg g < n$ et on vérifie que le code C admet pour base

$$g, Xg, \ldots, X^{n-1-\deg(g)}g$$

en tant que $\mathbb{F}$-espace vectoriel. En particulier :

Lemme 10 La dimension du code cyclique C engendré par g est $k = n - \deg(g)$.

Exercice 12 Justifier que $g, Xg, \ldots, X^{n-1-\deg(g)}g$ est effectivement une base de C.

Corrigé. Soit c un mot du code, représenté par $c \in \mathbb{F}[X]$, $\deg c < n$. Par définition de C, il existe donc $a, b \in \mathbb{F}[X]$ tels que $c = ag + b(X^n - 1)$. Puisque g divise $X^n - 1$, il suit que g divise c, donc c est combinaison linéaire des vecteurs en questions. Ces vecteurs formant une famille libre de $\mathbb{F}[X]$, et étant de degrés $< n$, ils forment une famille libre modulo $X^n - 1$. D'où le résultat. □

5.3 Codage

Pour tout r, notons $\mathbb{F}[X]_{<r} \simeq \mathbb{F}^r$ l'espace vectoriel des polynômes de degrés $< r$. Un codage de C consiste ainsi en une application linéaire injective $\phi : \mathbb{F}[X]_{<k} \to \mathbb{F}[X]_{<n}$ d'image C.

Codage naïf. Un procédé de codage naïf consiste à considérer

$$\begin{aligned} \phi : \mathbb{F}[X]_{<k} &\longrightarrow \mathbb{F}[X]_{<n} \\ m(X) &\longmapsto m(X)g(X). \end{aligned}$$

Elle est injective d'image C, donc sa matrice est une matrice génératrice. En écrivant $X^n - 1 = hg$, alors l'application linéaire $\mathbb{F}[X]_{<n} \to \mathbb{F}[X]_{<n-k}$ définie par $f \mapsto fh \mod g$ a pour noyau C et sa matrice est donc une matrice de contrôle de C.

Codage systématique. L'application ϕ a l'inconvénient de requérir une division par g pour décoder. Il y a un procédé de codage plus malin. On considère l'application

$$\begin{aligned} \psi : \mathbb{F}[X]_{<k} &\longrightarrow \mathbb{F}[X]_{<n} \\ m(X) &\longmapsto X^{n-k}m(X) - r(X) \end{aligned}$$

où $r(X)$ est le reste de la division euclidienne de $X^{n-k}m(X)$ par $g(X)$, de degré $< n-k$. Le polynôme $X^{n-k}m(X)$ porte l'information, et $r(X)$ la redondance. L'image de ψ est à nouveau C (vérifiez-le), mais le codage est cette fois de décodage trivial : le mot source $m(X)$ est constitué des k dernières coordonnées du mot code (un codage systématique consisterait en les k premières coordonnées, mais cela ne change essentiellement rien).

5.4 Zéros d'un code cyclique

On suppose ici que $\mathbb{F} = \mathbb{F}_p$ où p est premier et que n *est premier à* p. Donc $X^n - 1$ a n racines distinctes dans son corps de décomposition sur $\mathbb{F}_p$. Notons K ce corps de décomposition, c'est à dire le corps engendré par les racines n-èmes de l'unité sur $\mathbb{F}_p$. On fixe une racine primitive n-ème de l'unité α dans K. On a donc

$$X^n - 1 = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} (X - \alpha^i).$$

Le polynôme générateur g d'un code cyclique de longueur n sur $\mathbb{F}_p$ divisant $X^n - 1$, il va être déterminé par ses racines dans K, qui forment un sous-ensemble de l'ensemble $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ des racines n-èmes de l'unité. On appelle ce sous-ensemble *les zéros du code*.

Tout diviseur de $X^n - 1$ dans $K[X]$ est ainsi de la forme

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

où Σ un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$. Pour que g_Σ soit effectivement le polynôme générateur d'un code cyclique, il faut et il suffit que $g_\Sigma \in \mathbb{F}_p[X]$. Ceci équivaut au fait que

$$g_\Sigma(X^p) = g_\Sigma(X)^p$$

(se souvenir que $\mathbb{F}_p$ est le sous-corps de K stable par le Frobenius $x \mapsto x^p$), c'est à dire

$$\prod_{i \in \Sigma} (X^p - \alpha^i) = \prod_{i \in \Sigma} (X^p - \alpha^{pi}).$$

Autrement dit, l'ensemble des racines de g_Σ doit-être stable sous l'action du Frobenius. Puisque α est une racine primitive n-ème de l'unité, ceci équivaut au fait que $\Sigma \subset \mathbb{Z}/n\mathbb{Z}$ soit stable par multiplication par p (cf aussi [Dem, Prop 10.19]). En conclusion :

Lemme 11 Il y a une bijection entre les codes cycliques sur $\mathbb{F}_p$ de longueur n et les sous-ensembles de $\mathbb{Z}/n\mathbb{Z}$ stables par multiplication par p.

5.5 Classes cyclotomiques

Pour déterminer les parties E de $\mathbb{Z}/n\mathbb{Z}$ stables par multiplication par p, on considère la relation « il existe i tel que $p^i j = j'$» entre éléments j et j' de $\mathbb{Z}/n\mathbb{Z}$. C'est une une relation d'équivalence (exo). Les classes d'équivalence sont appelées *classes cyclotomiques*. Ce sont donc les orbites de la multiplication par p dans $\mathbb{Z}/n\mathbb{Z}$. Pour chaque élément $j \in \mathbb{Z}/n\mathbb{Z}$, sa classe cyclotomique est

$$\Sigma_j = \{j, pj, p^2 j, \ldots, p^{s-1} j\}$$

où $s > 0$ est le plus petit entier tel que $p^s j = j$.

Lemme 12 Le polynôme $g_j := g_{\Sigma_j} = (X - \alpha^j)(X - \alpha^{pj}) \cdots (X - \alpha^{p^{s-1} j}) \in \mathbb{F}_p[X]$ associé à la classe cyclotomique Σ_j coïncide avec le polynôme minimal de α^j, de degré s. En particulier, g_j est irréductible.

Preuve. Par construction, Σ_j est stable par multiplication par p, donc $g_j \in \mathbb{F}_p[X]$ d'après le Lemme 11. Le polynôme minimal $P \in \mathbb{F}_p[X]$ de α^j vérifiant $P(X)^p = P(X^p)$, on déduit que $\alpha^j, \alpha^{jp}, \ldots, \alpha^{jp^{s-1}}$ sont racines de P, *distinctes* par définition de s. Donc g_j divise P dans $\mathbb{F}_p[X]$, donc $g_j = P$ par minimalité de P. □

Ainsi, les différents g_j sont les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}_p[X]$. On en déduit en particulier :

Lemme 13 La décomposition de $\mathbb{Z}/n\mathbb{Z}$ comme réunion disjointe des classes cyclotomiques correspond à la décomposition de $X^n - 1$ en facteurs irréductibles dans $\mathbb{F}_p[X]$. □

Les parties stables E sont exactement les réunions de classes cyclotomiques, de la même façon que les diviseurs de $X^n - 1$ sont exactement les produits des facteurs irréductibles.

Exemple 7 Déterminons tous les codes cycliques de longueur 7 sur $\mathbb{F}_2$. Un rapide calcul montre que $\mathbb{Z}/7\mathbb{Z}$ se décompose comme la réunion disjointe de trois classes cyclotomiques

$$\mathbb{Z}/7\mathbb{Z} = \{0\} \cup \{1, 2, 4\} \cup \{3, 5, 6\}.$$

Il y a donc trois codes cycliques *irréductibles* de longueurs 7 sur $\mathbb{F}_2$, correspondants aux classes cyclotomiques Σ_0, Σ_1 et Σ_3, de polynômes générateurs irréductibles

$$g_0 := (X - 1), \quad g_1 := (X - \alpha)(X - \alpha^2)(X - \alpha^4), \quad g_3 := (X - \alpha^3)(X - \alpha^5)(X - \alpha^6),$$

où α est une racine primitive 7-ème de l'unité sur $\mathbb{F}_2$. Le code de g_0 est de dimension $7 - 1 = 6$ tandis que les codes de g_1 et g_3 sont de dimension $k = 7 - 3 = 4$ (on peut montrer que les codes g_1 et g_3 sont équivalents). Les polynômes g_0, g_1, g_3 correspondent aux facteurs irréductibles de $X^7 - 1$:

$$X^7 - 1 = (X - 1)(X^3 + X^2 + 1)(X^3 + X + 1) \in \mathbb{F}_2[X].$$

Les autres codes cycliques de longueur 7 sur $\mathbb{F}_2$ (non irréductibles) sont donnés par les produits $g_0 g_1$ et $g_0 g_3$ (dimension 4), $g_1 g_3$ (dimension 1), et enfin $g_0 g_1 g_3 = X^7 - 1$ correspondant au code nul.

Remarque 3 Notez que $c \in \mathbb{F}_p[X]_{<n} \simeq \mathbb{F}^n$ est un mot du code g_j si et seulement si $c(\alpha^j) = 0$. En effet, g_j étant le polynôme minimal de α^j, ceci équivaut au fait que c est dans l'idéal engendré par g_j. On remarque que α^j engendre une extension K de $\mathbb{F}_p$ de degré $\deg(g_j) = n - k$ où k est la dimension du code. L'équation $c(\alpha^j) = 0$ équivaut donc à un système de $n - k$ équations linéaires à coefficients dans $\mathbb{F}$, dont la matrice est une matrice de contrôle du code g_j.

5.6 Borne pour la distance minimum d'un code cyclique

Un autre aspect important des zéros d'un code cyclique est que la configuration des racines du polynôme générateur nous renseigne sur la distance minimale du code cyclique. On a la proposition suivante [Dem, Prop. 10.21].

Proposition 1 Soit $\Sigma \subset \mathbb{Z}/n\mathbb{Z}$ stable par multiplication par p. Si Σ contient s entiers consécutifs $a + 1, a + 2, \ldots, a + s$ modulo n, alors soit le code cyclique de polynôme générateur g_Σ est nul, soit il a une distance minimum supérieure ou égale à $s + 1$.

Preuve. Il suffit de démontrer qu'un polynôme $c \in \mathbb{F}_p[X]_{<n}$, qui a au plus s termes non nuls et qui satisfait aux conditions $c(\alpha^{a+i}) = 0$ pour $1 \leq i \leq s$ est identiquement nul. Soit $c = \sum_{j=1}^{s} c_j X^{d_j}$ un tel polynôme. Notons $\lambda_j = \alpha^{d_j}$ On a alors :

$$c(\alpha^{a+i}) = \sum_{j=1}^{s} c_j \lambda_j^a \lambda_j^i = 0, \quad i = 1 \ldots, s.$$

Or la matrice carrée $(\lambda_j^i)_{1\leq i,j\leq s}$ est une matrice de Vandermonde, et α étant une racine primitive de l'unité, les $\lambda_j = \alpha^{d_j}$ sont distincts. La matrice est donc inversible et on a donc nécessairement $c_j\lambda_j^a = 0$ (donc $c_j = 0$) pour tout j. Donc $c = 0$. $\square$.

Exemple 8 Les codes cycliques g_1 et g_3 de l'exemple 7 sont chacun de distance minimum au moins 3, car leurs classes cyclotomiques admettent deux entiers consécutifs.

5.7 Les codes de Hamming sont des codes cycliques

Considérons le cas $p = 2$ et $n = 2^m - 1$. Fixons une racine primitive n-ème de l'unité α dans $\mathbb{F}_{2^m}$, de sorte que $\mathbb{F}_{2^m} = \mathbb{F}_2[\alpha]$. D'après le Lemme 12, le polynôme minimal g de α est un facteur irréductible de $X^n - 1$ de degré l'ordre de 2 dans $\mathbb{Z}/n\mathbb{Z}^\times$. Ce degré est donc m par choix de n, et on a :

$$g(X) = \prod_{i=0}^{m-1}(X - \alpha^{2^i}).$$

Ce polynôme g correspond par construction à la classe cyclotomique

$$\Sigma_1 = \{1, 2, 2^2, \ldots, 2^{m-1}\}.$$

Le code cyclique C de polynôme générateur g est donc de longueur $n = 2^m - 1$ et de dimension $n - \deg(g) = 2^m - 1 - m$. Sa distance minimale est au moins 3 car Σ_1 contient deux entiers consécutifs (Proposition 2). L'analogie avec les codes de Hamming n'est pas un hasard :

Lemme 14 Le code cyclique C engendré par le polynôme minimal d'une racine primitive $(2^m - 1)$-ème de l'unité sur $\mathbb{F}_2$ coïncide avec le code de Hamming de paramètres $[2^m - 1, 2^m - 1 - m, 3]$.

Preuve. Le code C est par définition le sous-espace vectoriel de $\mathbb{F}_2^n$ formé des mots $x = (x_0, ..., x_{n-1})$ tels que le polynôme $m(X) = x_0 + \cdots + x_{n-1}X^{n-1}$ soit divisible par g, i.e. tel que $m(\alpha) = 0$, i.e. tel que

$$u(x) := \sum_{i=0}^{n-1} x_i\alpha^i = 0.$$

Mais les α^i sont par hypothèse tous les éléments non nuls du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_{2^m} \simeq \mathbb{F}_2^m$, de dimension m. La matrice de l'application linéaire $u : \mathbb{F}_2^n \to \mathbb{F}_2^m$, à m lignes et n colonnes, possède donc exactement comme colonnes les $n = 2^m - 1$ vecteurs non nuls, chacun une fois. On retrouve bien la définition du code de Hamming *via* sa matrice de contrôle. $\square$

5.8 Les codes BCH binaires sont des codes cycliques

On garde les notations et hypothèses précédentes. Soit $1 \leq \delta \leq n = 2^m - 1$. On note Σ la plus petite partie de $\mathbb{Z}/n\mathbb{Z}$ contenant $\{1, 2, \ldots, \delta - 1\}$ et qui soit stable par multiplication par 2. On note

$$g := \prod_{i\in\Sigma}(X - \alpha^i).$$

On a $g \in \mathbb{F}_2[X]$ d'après le Lemme 11, et g divise $X^n - 1$.

Exercice 13 Montrer que le code cyclique C engendré par g coïncide avec le code BCH binaire de longueur n et de distance prescrite δ introduit en Definition 7. Montrer de plus que l'on a l'égalité

$$g = \mathrm{ppcm}(g_1, \ldots, g_{\delta-1})$$

où g_i est le polynôme associé à la classe cyclotomique de l'entier i. Justifier que le cas $\delta = 2$ correspond au code de Hamming.

Correction. Un polynôme $c = \sum_{i=0}^{n-1} c_i X^i$ est un mot du code si et seulement si

$$c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{\delta-1}) = 0$$

(cf Section 5.5). Ceci équivaut au fait que $H \cdot {}^t c = 0$ où H est la matrice introduite à la définition 7, montrant le premier point. Par définition de Σ, les racines de g sont simples et coïncident avec les racines des polynômes $g_1, \ldots, g_{\delta-1}$, montrant le second point. En particulier, si $\delta = 2$, alors $g = g_1$, montrant le dernier point. □

Combiné avec la Proposition 1, on retrouve en particulier le fait que la distance minimale des codes BCH binaire de distance prescrite δ vérifie $d \geq \delta$.

Exercice 14 Montrer que si δ est paire, alors le code BCH binaire de distance prescrite δ est en fait de distance minimale $d \geq \delta + 1$.

Correction. Si δ est paire, on peut écrire $\delta = 2b$ avec $b \in \{1, \ldots, \delta - 1\} \subset \Sigma$. Puisque Σ est stable par multiplication par 2, il s'ensuit que $\delta = 2b \in \Sigma$, d'où l'inclusion $\{1, \ldots, \delta\} \subset \Sigma$. On conclut avec la Proposition 1. □.

5.9 Correction des codes BCH binaires.

D'après la Proposition 1, on pourra donc corriger t erreurs avec un code BCH de distance prescrite $\delta = 2t + 1$. Expliquons un procédé de décodage qui permet de faire cette correction.

On envoie un mot de code c, qui vérifie donc

$$c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{2t}) = 0.$$

Le mot reçu est $r = c + e$. On suppose que le polynôme d'erreur e est de poids $w \leq t$ (on ne cherche pas à corriger plus de t erreurs). On a donc

$$e = X^{\ell_1} + \cdots + X^{\ell_w}$$

avec $0 \leq \ell_1 < \cdots < \ell_w \leq n - 1$. Le but du décodage est de déterminer les entiers ℓ_i qui sont les numéros des bits erronés du mot reçu.

Posons $\beta_j = \alpha^{\ell_j}$ pour $j = 1, \ldots, w$. Les β_j sont des éléments distincts et tous non nuls de $\mathbb{F}_{2^m}$. On introduit le *polynôme localisateur d'erreurs*

$$\sigma(Z) = \prod (1 - \beta_j Z) = 1 + \sigma_1 Z + \sigma_2 Z + \cdots + \sigma_w Z^w \in \mathbb{F}_{2^m}[Z],$$

polynôme réciproque du polynôme unitaire de racines β_j. Les σ_i sont, au signe près, les polynômes symétriques élémentaires des β_j.

Par construction, les entiers ℓ_j correspondent aux entiers i entre 0 et $n - 1$ tels que α^{-i} est racine de σ. Donc si on connaît le polynôme localisateur d'erreurs σ, on pourra récupérer aisément les ℓ_j et corriger le mot r. Il reste à calculer σ, c'est à dire les σ_j.

On peut calculer à partir du mot reçu r les valeurs

$$S_i := r(\alpha^i) = e(\alpha^i) = \sum_{j=1}^{w} \alpha^{i\ell_j} = \sum_{j=1}^{w} \beta_j^i, \quad i = 1, \ldots, 2t.$$

On connaît donc les $2t$ premières sommes de Newton des β_j, desquelles on veut déduire les fonctions symétriques σ_i pour $i = 1, \ldots, w$. Les formules de Newton (cf CM8) donnent ici :

$$S_i + \sigma_1 S_{i-1} + \sigma_2 S_{i-2} + \cdots + \sigma_{i-1} S_1 + i\sigma_i = 0 \tag{1}$$

avec la convention $\sigma_i = 0$ pour $i > w$. On récupère usuellement $\sigma_1, \ldots, \sigma_w$ en considérant les w premières équations qui forment un système triangulaire.

$$\begin{aligned} -\sigma_1 &= S_1 \\ -2\sigma_2 &= S_2 + \sigma_1 S_1 \\ -3\sigma_3 &= S_3 + \sigma_1 S_2 + \sigma_2 S_1 \\ &\cdots \\ -w\sigma_w &= S_w + \sigma_1 S_{w-1} + \cdots + \sigma_{w-1} S_1 \end{aligned}$$

Malheureusement, nous sommes en caractéristique positive 2, et cette formule ne permet pas de récupérer directement les σ_i par récurrence du fait du facteur i de σ_i qui peut s'annuler mod 2. Il faut procéder différemment et regarder les équations suivantes, tenant compte du fait que $\sigma_i = 0$ pour $i > w$.

$$\begin{aligned} 0 &= S_{w+1} + \sigma_1 S_w + \cdots + \sigma_w S_1 \\ 0 &= S_{w+2} + \sigma_1 S_{w+1} + \cdots + \sigma_w S_2 \\ &\cdots \\ 0 &= S_{2w} + \sigma_1 S_{2w-1} + \cdots + \sigma_w S_w \\ &\cdots \end{aligned}$$

Définissons pour tout i

$$H_i = \begin{pmatrix} S_1 & S_2 & \cdots & S_i \\ S_2 & S_3 & \cdots & S_{i+1} \\ \vdots & \vdots & \vdots & \vdots \\ S_i & S_{i+1} & \cdots & S_{2i-1} \end{pmatrix}$$

On vérifie que

$$H_w = V \begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_w \end{pmatrix} {}^tV \quad \text{avec} \quad V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_w \\ \vdots & \vdots & \vdots & \vdots \\ \beta_1^{w-1} & \beta_2^{w-1} & \cdots & \beta_w^{w-1} \end{pmatrix}$$

Puisque les β_j sont non nuls et distincts, H_w est inversible (V est une matrice de Vandermonde). Donc H_t ayant H_w comme sous-matrice (on a supposé $w \leq t$), elle est de rang $\geq w$. Par ailleurs, les formules de Newton (1) impliquent que chaque colonne de H_t d'indice $\geq w+1$ est combinaisons linéaires des w colonnes précédentes. Le nombre d'erreurs w est donc égal au rang de la matrice H_t. Une fois w trouvé, on retrouve les σ_j en résolvant le système de Cramer

$$H_w \begin{pmatrix} \sigma_w \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_{w+1} \\ \vdots \\ -S_{2w} \end{pmatrix}$$

donné par les formules de Newton (1) pour $i = w+1, \ldots, 2w$.

5.10 Appendice : factorisation des polynômes cyclotomiques sur les corps finis

Profitons de ce chapitre pour parler de la factorisation des polynômes cyclotomiques sur les corps finis. On rappelle que le n-ème polynôme cyclotomique est le polynôme ayant pour racines les racines (complexes) primitives n-èmes de l'unité

$$\Phi_n(X) := \prod_{k \in \mathbb{Z}/n\mathbb{Z}^\times} (X - e^{\frac{2ik\pi}{n}})$$

Ce polynôme est unitaire à coefficients dans $\mathbb{Z}$, de degré $\varphi(n)$. En partitionnant les racines n-èmes de l'unité selon leurs ordres multiplicatifs, on obtient l'égalité

$$X^n - 1 = \prod_{r|n} \Phi_r \in \mathbb{Z}[X]. \tag{2}$$

Le n-ème polynôme cyclotomique sur $\mathbb{F}_p$ est par définition la réduction $\bar{\Phi}_n \in \mathbb{F}_p[X]$ modulo p de Φ_n. Il est connu que Φ_n est irréductible sur $\mathbb{Z}$. Cependant sa réduction $\bar{\Phi}_n$ ne l'est pas nécessairement sur $\mathbb{F}_p$. Etudions ce phénomène de plus près. Commençons par un lemme :

Lemme 15 Si n est premier à p, alors $\bar{\Phi}_n$ admet à nouveau pour racines les racines n-ème primitive de l'unité (dans $\bar{\mathbb{F}}_p$ cette fois-ci).

Preuve. Par récurrence forte sur n. Si $n = 1$, c'est clair. Sinon, soit $\alpha \in \bar{\mathbb{F}}_p$ une racine de $\bar{\Phi}_n$. D'après (2), $\bar{\Phi}_n$ divise $X^n - 1$ dans $\mathbb{F}_p[x]$. Donc α est une racine n-ème de l'unité, d'ordre multiplicatif r divisant n d'après le théorème de Lagrange. Si $r < n$, alors α serait racine de $\bar{\Phi}_r$ par hypothèse de récurrence et il s'en suivrait que $\gcd(\bar{\Phi}_r, \bar{\Phi}_n) \neq 1$ dans $\mathbb{F}_p[X]$. On aurait alors $X^n - 1$ avec facteurs multiples dans $\mathbb{F}_p[X]$ d'après (2) modulo p, ce qui est exclu puisque n est premier à p. □

Soit n premier à p et soit α une racine de $\bar{\Phi}_n$. D'après le lemme précédent, les autres racines de $\bar{\Phi}_n$ sont les α^i, avec $1 \leq i \leq n-1$ premier à n :

$$\bar{\Phi}_n(X) = \prod_{i \in \mathbb{Z}/n\mathbb{Z}^\times} (X - \alpha^i)$$

La factorisation irréductible de $\bar{\Phi}_n(X)$ découle alors du corollaire suivant du Lemme 12 :

Lemme 16 Soit α une racine primitive n-ème de l'unité sur $\mathbb{F}_p$. Le polynôme minimal P de α sur $\mathbb{F}_p$ a pour degré le plus petit entier r tel que $\alpha^{p^r} = \alpha$, et admet pour racines $\alpha, \alpha^p, \ldots, \alpha^{p^{r-1}}$. □

Puisque α est une racine primitive n-ème de l'unité, l'entier r est aussi le plus petit entier tel que n divise $p^r - 1$, i.e. r est l'ordre de p dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$. *Il ne dépend donc pas du choix de α.*

En combinant le lemme 15 et le lemme 16 on en déduit finalement :

Proposition 2 Soit n premier à p. Le polynôme cyclotomique $\bar{\Phi}_n \in \mathbb{F}_p[X]$ est de degré $\varphi(n)$. Il admet exactement $\varphi(n)/r$ facteurs irréductibles sur $\mathbb{F}_p[X]$, tous de même degrés r, où r est l'ordre de p dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exemple 9 Considérons $\bar{\Phi}_{15} \in \mathbb{F}_2[X]$. L'ordre de $p = 2$ dans $\mathbb{Z}/15\mathbb{Z}^\times$ est 4 et on a la factorisation irréductible

$$\bar{\Phi}_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 = (X^4 + X + 1)(X^4 + X^3 + 1) \in \mathbb{F}_2[X].$$

Codes ou pas codes, il est important de revoir ce qui concerne les polynômes cyclotomiques et les racines de l'unités sur les corps finis (par exemple [Dem, Ch.3 et Ch.9]).

Exercice 15 Déterminer les polynômes cyclotomiques divisant $X^{20}-1$ sur $\mathbb{F}_3[X]$ et déterminer les degrés de leurs facteurs irréductibles.

Corrigé. On remarque que $p=3$ est premier à $n=20$. On a l'égalité

$$X^{20}-1 = \prod_{d|n} \bar{\Phi}_d = \bar{\Phi}_1\bar{\Phi}_2\bar{\Phi}_4\bar{\Phi}_5\bar{\Phi}_{10}\bar{\Phi}_{20}$$

où $\bar{\Phi}_d$, de degré $\varphi(d)$, a pour racine les racines primitives d-èmes de l'unité. Cette factorisation correspond à la partition du groupe cyclique $\mathbb{Z}/20\mathbb{Z} = \sqcup_{d|n} S_d$ où S_d est l'ensemble des éléments d'ordre d. Plus précisément, en notant α une racine primitive 20-ème de l'unité, on a :

$$\bar{\Phi}_d = \prod_{k\in S_d} (X-\alpha^k) \in \mathbb{F}_3[X].$$

Il reste à déterminer les degrés des facteurs irréductible de $\bar{\Phi}_d$ sur $\mathbb{F}_3[X]$ pour chaque diviseur d de 20. D'après le Lemme 16, $\bar{\Phi}_d$ admet $\varphi(d)/r_d$ facteurs irréductibles, tous de même degré r_d, où r_d est le plus petit entier tel que d divise $3^{r_d}-1$. On note que r_d divise $\varphi(d)$. On trouve ici :

- $\bar{\Phi}_1 = (X-1)$, de degré $\varphi(1)=1$, avec $S_1=\{0\}$.
- $\bar{\Phi}_2 = (X+1)$, de degré $\varphi(2)=1$, avec $S_2=\{10\}$.
- $\bar{\Phi}_4 = (X-\alpha^5)(X-\alpha^{15})$ de degré $\varphi(4)=2$, avec $S_4=\{5,15\}$. On trouve $r_4=2$ ($d=4$ divise 3^2-1), donc $\bar{\Phi}_4$ est irréductible.
- $\bar{\Phi}_5 = \prod_{k\in S_5}(X-\alpha^k)$ de degré $\varphi(5)=4$, avec $S_5=\{4,8,12,16\}$. On trouve $r_5=4$ ($d=5$ divise 3^4-1), donc $\bar{\Phi}_5$ est irréductible.
- $\bar{\Phi}_{10} = \prod_{k\in S_{10}}(X-\alpha^k)$ de degré $\varphi(10)=4$, avec $S_{10}=\{2,6,14,18\}$. On trouve $r_{10}=4$ ($d=10$ divise 3^4-1), donc $\bar{\Phi}_{10}$ est irréductible.
- $\bar{\Phi}_{20} = \prod_{k\in S_{20}}(X-\alpha^k)$ de degré $\varphi(20)=8$, avec $S_{20}=\{1,3,7,9,11,13,17,19\}$. On trouve $r_{20}=4$ ($d=20$ divise 3^4-1), donc $\bar{\Phi}_{20}$ admet deux facteurs irréductibles de degrés 4, l'un noté $\bar{\Phi}_{20,1}$ correspondant à la classe cyclotomique $\{1,3,7,9\}$ de 1 et l'autre noté $\bar{\Phi}_{20,11}$ correspondant à la classe cyclotomique $\{11,13,17,19\}$ de 11.

Autre approche : On peut aussi (et c'est plus rapide) utiliser le Lemme 13 : l'entier r_d coïncide avec le cardinal de la classe cyclotomique de n'importe quel élément de S_d. Remarquant que $20/d \in S_d$, il suffit donc de calculer la taille des classes cyclotomiques de $1,2,4,5,10,20$ pour avoir les degrés et le nombre des facteurs irréductibles des différents $\bar{\Phi}_d$.

Conclusion : $X^{20}-1$ admet deux facteurs irréductibles $\bar{\Phi}_1$, $\bar{\Phi}_2$ de degrés 1, un facteur irréductible $\bar{\Phi}_4$ de degré 2, et quatre facteurs irréductibles $\bar{\Phi}_5$, $\bar{\Phi}_{10}$, $\bar{\Phi}_{20,1}$, $\bar{\Phi}_{20,11}$ de degrés 4. □