Codes correcteurs d'erreurs

Petite fiche résumant ce qu'il faut savoir sur les codes correcteurs d'erreurs pour l'agrégation.

Pour tout le document, on fixe p un nombre premier, k et n deux entiers non nuls et $q = p^k$.

I - Théorie générale

Il s'agit, dans un premier temps, de choisir le corps $\mathbb{F}_q$ en fonction de l'information que l'on cherche à coder. Par exemple, le choix de $\mathbb{F}_2$ semble le plus naturel pour représenter la manière dont est stockée l'information dans un ordinateur, tandis que $\mathbb{F}_4$ serait plus approprié vis-à-vis de l'ADN.

Définition 1. On appelle **mot** un vecteur à coefficients dans $\mathbb{F}_q$.

Après avoir choisi $\mathbb{F}_q$ comme alphabet, il reste à choisir l'ensemble des mots $\mathscr{C}$ du code. Plus précisément :

Définition 2. On appelle **code correcteur** (ou simplement **code**) de taille n un sous-ensemble de $\mathbb{F}_q^n$.

Remarque 3. Le code correcteur $\mathscr{C}$ est l'ensemble des mots que l'on est en mesure de produire par codage : il ne peut pas occuper l'espace $\mathbb{F}_q^n$ entier, sinon tous les mots seraient valides !

Si l'on reçoit un mot qui n'est pas dans le code, on est donc sûr qu'il y a eu une erreur de transmission. L'opération de codage "ajoute" une information pour distinguer les mots valides des autres. C'est uniquement lors du décodage que l'on va pouvoir réparer une ou plusieurs erreurs. Le procédé général étant le suivant :

1. on transforme un message m en un mot c du code (c'est le processus de **codage**) ;
2. pendant la transmission, c est altéré en c' (c'est le processus de **transmission**) ;
3. on essaye de déterminer si c' est un mot du code (c'est le processus de **détection d'erreur**) ;
4. on essaye de retrouver c à partir de c' (c'est le processus de **correction d'erreur**) ;
5. on retrouve le message m à partir de c (c'est le processus de **décodage**).

Exemple 4 (Bit de parité)**.** Dans un ordinateur, chaque mot est coupé en "sous-mots" de 7 bits, c'est-à-dire, en vecteurs formés de 7 éléments de $\mathbb{F}_2$. Lors du codage de chaque vecteur, on ajoute un bit dit "de parité".

Ainsi, soit $b_1, \dots, b_7$ une suite de 7 bits. On calcule :

$$b_8 = b_1 + \cdots + b_7 \mod 2$$

Si le nombre de bits égaux à 1 est pair, $b_8 = 0$, sinon, $b_8 = 1$. Ainsi, le mot $(b_1, \dots, b_8)$ a toujours

un nombre de bits égaux à 1 qui est pair. On peut alors détecter, à la lecteur d'un mot, si une erreur a eu lieu lors de sa réception : il y aura un nombre impair de bits égaux à 1.

Dans le cadre d'un mot de taille 2, on peut représenter la situation par un cube. Sur cette illustration, nous voyons en turquoise l'ensemble des mots $\mathscr{C}$ du code. Une unique erreur correspond à un déplacement sur le cube le long d'une arête. Dans ce cas, le récepteur reçoit un point noir dont la somme de toutes les lettres est un entier impair. En revanche, un tel point est toujours à proximité de trois points turquoise, le récepteur ne dispose donc d'aucun moyen pour une correction automatique.

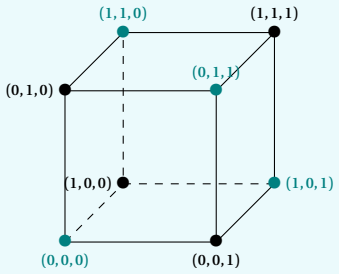

FIGURE 1 – Mots de $\mathbb{F}_2$ de longueur 2 avec un bit de parité.

Ainsi, ce code, a deux inconvénients :

— il est impossible de détecter où l'erreur a eu lieu, et donc, de la corriger ;

— si deux erreurs ont lieu, il est impossible de les détecter (car alors, le nombre de bits égaux à 1 reste pair).

L'exemple précédent montre bien qu'il est nécessaire de pouvoir évaluer les propriétés qualitatives d'un code. Ainsi :

Définition 5. Soient x et y deux mots de $\mathbb{F}_q$ de taille n.

— Le **poids** de x, noté $\omega(x)$, est le nombre de coefficients non nuls dans x.

— La **distance de Hamming** entre x et y, notée $d_H(x,y)$ est définie par

$$d_H(x,y) = \omega(x-y)$$

Proposition 6. (i) d_H correspond aux nombres de coefficients qui diffèrent entre x et y.

(ii) d_H est une distance sur $\mathbb{F}_q^n$.

Démonstration. (i) Soient $x, y \in \mathbb{F}_q^n$. Par définition, $\omega(x-y)$ est égal au nombre de coefficients non nuls de $x-y$, soit au nombre de coefficients qui diffèrent entre x et y.

(ii) Soient $x, y, z \in \mathbb{F}_q^n$.

(a) On a $d_H(x,y) \geq 0$ par positivité de ω et $d_H(x,y) = 0$ si et seulement s'il y a 0 coefficients qui diffèrent entre x et y ie. $x = y$.

(b) Le nombre de coefficients non nuls de $x-y$ est égal au nombre de coefficients non nuls de $y-x$. Donc,

$$d_H(x,y) = \omega(x-y) = \omega(y-x) = d_H(y,x)$$

(c) On note $(x_i)_{i\in[\![1,n]\!]}$, $(y_i)_{i\in[\![1,n]\!]}$ et $(z_i)_{i\in[\![1,n]\!]}$ les coefficients respectifs de x, y et z. Soient $\mathscr{A} = \{k \in [\![1,n]\!] \mid x_k = y_k\}$, $\mathscr{B} = \{k \in [\![1,n]\!] \mid y_k = z_k\}$ et $\mathscr{C} = \{k \in [\![1,n]\!] \mid x_k = z_k\}$. On a,

$$(\mathscr{A} \cap \mathscr{B}) \subseteq \mathscr{C}$$

En passant au complémentaire,

$${}^c\mathscr{C} \subseteq {}^c(\mathscr{A} \cap \mathscr{B}) = {}^c\mathscr{A} \cup {}^c\mathscr{B}$$

D'où,

$$\underbrace{d(x,z)}_{|{}^c\mathscr{C}|} \leq \underbrace{d(x,y)}_{|{}^c\mathscr{A}|} + \underbrace{d(y,z)}_{|{}^c\mathscr{B}|}$$

□

La distance d_H permet de quantifier la notion de "mot le plus proche". Avec elle, on peut donner la définition suivante.

Définition 7. Soit $\mathscr{C}$ un code. On appelle **distance minimale** de $\mathscr{C}$, l'entier suivant :

$$\min_{x,y\in\mathscr{C}} \{d_H(x,y) \mid x \neq y\}$$

Plus la distance minimale d'un code est grande, plus les mots vont être "espacés" les uns des autres. En ne prenant en compte que la plus petite des distances, on va pouvoir s'assurer que le code est en mesure de corriger une erreur sous certaines conditions.

Définition 8. Un code $\mathscr{C}$ est dit t-**correcteur** s'il peut corriger au maximum t erreurs.

Remarque 9. Cela signifie que, si $x \in \mathscr{C}$ désigne un mot codé et $x' \in \mathbb{F}_q^n$ le mot réceptionné, alors on est en mesure de retrouver le mot x original si $d(x,x') \leq t$.

Proposition 10. Soit $\mathscr{C}$ un code de distance minimale d. On suppose $d \geq 2t+1$. Alors, $\mathscr{C}$ est t-correcteur.

Démonstration. Soient $x, y \in \mathscr{C}$ deux mots distincts du code. Alors,

$$d_H(x,y) \geq 2t+1$$

les boules $B(x,t)$ et $B(y,t)$ sont disjointes. Ainsi, soient $a \in \mathscr{C}$ un mot codé émis et $a' \in \mathbb{F}_q^n$ le mot réceptionné. Si $d(a,a') \leq t$, alors $a' \in B(a,t)$ et n'appartient pas à une autre boule de centre un mot du code et de rayon inférieur ou égal à t : on peut corriger a'. □

Remarque 11. Notons qu'alors

$$t \leq \frac{d-1}{2} \implies t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

II - Codes linéaires

Nous allons maintenant observer ce qui se passe en imposant une structure sur le code.

Définition 12. Un **code linéaire** $\mathscr{C}$ de taille n et de dimension m sur $\mathbb{F}_q$ est un sous-espace vectoriel de dimension m de $\mathbb{F}_q^n$.

Soit alors une base de $\mathscr{C}$. On considère G une matrice dont les colonnes sont les vecteurs de cette base. On dit que G est une **matrice génératrice** de $\mathscr{C}$.

Proposition 13. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Soit G une matrice génératrice de $\mathscr{C}$. On a,

$$\mathscr{C} = \{Gx \mid x \in \mathbb{F}_q^n\}$$

Démonstration. Soit $(v_1, \dots, v_m)$ une base de $\mathscr{C}$. On considère la matrice génératrice de $\mathscr{C}$ associée, que l'on note G.

Alors, $\forall i \in [\![1, m]\!]$, en notant e_i le i-ième vecteur de la base canonique de $\mathbb{F}_q^n$, on a $Me_i = v_i$. Donc, par linéarité, $\{Gx \mid x \in \mathbb{F}_q^n\} \subseteq \mathscr{C}$. Et comme $v_i = Me_i$, on a bien l'inclusion réciproque. □

Remarque 14. Dans le cadre d'un code linéaire $\mathscr{C}$, la distance minimale d s'exprime alors

$$d = \min_{x,y \in \mathscr{C}} \{d_H(x,y) \mid x \neq y\} = \min_{x \in \mathscr{C}} \{\omega(x) \mid x \neq 0\}$$

Proposition 15. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Il existe une matrice $H \in \mathscr{M}_{n-m,n}(\mathbb{F}_q)$ telle que

$$\forall x \in \mathbb{F}_q^n,\ x \in \mathscr{C} \iff Hx = 0$$

Démonstration. On considère le produit scalaire canonique sur $\mathbb{F}_q^n$:

$$\langle .,. \rangle : ((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto \sum_{i=1}^{n} x_i y_i$$

et $\mathscr{C}^\perp$ l'orthogonal de $\mathscr{C}$ pour ce produit scalaire. $\mathscr{C}^\perp$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension $n-m$, dont on note $(v_1, \dots, v_{n-m})$ une base. Définissons H comme étant la matrice

dont la i-ième ligne est v_i pour tout $i \in [\![1, n-m]\!]$. Soit $x \in \mathbb{F}_q^n$. Alors, on a

$$\begin{aligned} Hx = 0 &\iff \forall i \in [\![1, n-m]\!], \langle v_i, x\rangle = 0 \\ &\iff x \in (\mathscr{C}^\perp)^\perp \\ &\iff x \in \mathscr{C} \end{aligned}$$

On aurait aussi pu se contenter de considérer le noyau à gauche de la matrice génératrice (c'est une caractérisation plus commode à implémenter en algorithmique). □

Définition 16. En reprenant les notations précédentes, H est appelée **matrice de contrôle** du code $\mathscr{C}$.

Il s'agit là d'un critère extrêmement pratique pour permettre de tester l'appartenance d'un mot au code.

Exemple 17 (Code de répétition)**.** On se place sur le corps $\mathbb{F}_2$. L'idée est d'envoyer plusieurs copies de chaque bit à être transmis. Ainsi, sur $\mathbb{F}_2^4$, le code $\mathscr{C}$ est composé de deux mots :

$$(0,0,0,0) \text{ et } (1,1,1,1)$$

Des matrices génératrices G et de contrôle H sont données par

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

On corrige en remplaçant un message reçu reconnu erroné par le message émis potentiel le plus proche (c'est-à-dire avec le moins de bits différents). Par conséquent, le codage par répétition permet de corriger correctement une erreur portant sur un seul bit mais ne permet pas de corriger correctement une erreur portant sur deux bits.

Proposition 18 (Borne de Singleton)**.** Soit $\mathscr{C}$ un code linéaire de taille n, de dimension m et de distance minimale d sur $\mathbb{F}_q$. Alors,

$$d \leq n - m + 1$$

Démonstration. Pour prouver ceci, exhibons un mot x de $\mathscr{C}$ de poids inférieur ou égal à $n-m+1$ (car alors, on aura $d \leq \omega(x) \leq n-m+1$). Soit F, le sous-espace vectoriel de $\mathbb{F}_q^n$ constitué des vecteurs dont les $m-1$ dernières coordonnées sont nulles. C'est un espace de dimension $n-m+1$,

et la formule de Grassmann donne :

$$\begin{aligned}\dim(\mathscr{C} \cap F) &= \dim(\mathscr{C}) + \dim(F) - \dim(\mathscr{C} + F)\\ &= m + n - m + 1 - \dim(\mathscr{C} + F)\\ &= n + 1 - \dim(\mathscr{C} + F)\\ &\geq n + 1 - n\\ &= 1\end{aligned}$$

Il existe donc $x \neq 0$ dans $\mathscr{C} \cap F$, et ce mot a un poids inférieur ou égal à $n - m + 1$. □

Ce dernier résultat illustre le choix à faire entre capacité de correction, et redondance de l'information transmise.
Terminons cette sous-section par la méthode pratique permettant de corriger un mot reçu. Pour cela, on a besoin d'une dernière définition.

Définition 19. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Soit H une matrice de contrôle de $\mathscr{C}$. On appelle **syndrome** d'un mot $x \in \mathbb{F}_q^m$ le vecteur Hx.

Imaginons maintenant que l'on réceptionne un mot $a' \in \mathbb{F}_q^m$. On calcule son syndrome via une matrice de contrôle H et on a deux cas :

— Le syndrome est nul : $a' \in \mathscr{C}$: on considère alors qu'il n'y a pas d'erreur.

— Le syndrome est non nul : il existe $a \in \mathscr{C}$ (le mot d'origine) et $e \in \mathbb{F}_q^n$ (l'erreur) tels que $a' = a + e$. Alors,

$$Ha' = H(a + e) = Ha + He = He$$

En notant h_j le j-ième vecteur colonne de H et e_j la j-ième coordonnée de e :

$$Ha' = \sum_{j \text{ tel que } e_j \neq 0} h_j e_j \qquad (*)$$

On en déduit e en résolvant le système $(*)$. Il est possible que ce système n'ait pas de solution, s'il y a trop d'erreurs par exemple. S'il y a une solution, elle est unique et on peut effectuer la correction : $a = a' - e$.

III - Codes cycliques

Nous avons vu dans la section précédente qu'imposer une structure d'espace vectoriel sur un code rendait le codage de l'information beaucoup plus simple via les matrices génératrices. Renforçons davantage la structure de notre code et observons les conséquences.

Définition 20. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. $\mathscr{C}$ est dit **cyclique** s'il est stable par décalage circulaire, ie.

$$(a_0, a_1, \dots, a_{m-1}) \in \mathscr{C} \implies (a_1, \dots, a_{m-1}, a_0) \in \mathscr{C}$$

Notons maintenant

$$\varphi : \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q[X]/(X^n-1) \\ (a_0,\dots,a_{n-1}) & \mapsto & \overline{\sum_{i=0}^{n-1} a_i X^i} \end{array}$$

Lemme 21. φ est un isomorphisme d'espaces vectoriels.

Démonstration. On sait (par la théorie des corps), que $\mathbb{F}_q[X]/(X^n-1)$ est un espace vectoriel sur $\mathbb{F}_q$ de dimension n. En effet, en notant $\overline{X}$ la classe de X dans $\mathbb{F}_q[X]/(X^n-1)$:

— La famille $(\overline{1},\dots,\overline{X}^{n-1})$ est libre. Soient $\lambda_0,\dots,\lambda_{n-1} \in \mathbb{K}$ tels que

$$\sum_{i=0}^{n-1} \lambda_i \overline{X}^i = \overline{\sum_{i=0}^{n-1} \lambda_i X^i} = 0$$

Alors, le polynôme $\sum_{i=0}^{n-1} \lambda_i X^i$ est dans l'idéal (X^n-1), mais est de degré strictement inférieur à n. Donc ses coefficients sont nuls : on a $\forall i \in [\![1,n]\!]$, $\lambda_i = 0$.

— La famille $(\overline{1},\dots,\overline{X}^{n-1})$ est génératrice. Soit $\overline{P} \in \mathbb{F}_q[X]/(X^n-1)$. On fait la division euclidienne de P par X^n-1 dans $\mathbb{F}_q[X]$:

$$\exists (Q,R) \in \mathbb{F}_q[X] \text{ tel que } P = Q(X^n-1)+R \text{ avec } \deg(R) < n \text{ ou } R = 0$$

En repassant modulo (X^n-1), on a bien

$$\overline{P} = \overline{R}$$

de degré inférieur à n, donc appartenant à l'espace vectoriel engendré par $(\overline{1},\dots,\overline{X}^{n-1})$.

Ainsi, $\mathbb{F}_q^n$ et $\mathbb{F}_q[X]/(X^n-1)$ sont isomorphes en tant qu'espaces vectoriels de même dimension sur $\mathbb{F}_q$. L'application φ étant surjective et linéaire (par définition), on a bien un isomorphisme. □

À l'aide de cet isomorphisme, nous allons pouvoir identifier un code linéaire de taille n sur $\mathbb{F}_q$ à un sous-espace vectoriel $\widetilde{\mathscr{C}} = \varphi(\mathscr{C})$ de $\mathbb{F}_q[X]/(X^n-1)$. Ce raisonnement va nous permettre de caractériser les codes cycliques.

Proposition 22. Soit $\mathscr{C}$ un code linéaire de taille n. Alors, $\mathscr{C}$ est cyclique si et seulement si $\widetilde{\mathscr{C}} = \varphi(\mathscr{C})$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$.

Démonstration. Soient $a = (a_0, a_1, \dots, a_{n-1}) \in \mathscr{C}$ et $a' = (a_{n-1}, a_0, \dots, a_{n-2})$. Remarquons que,

$$\begin{aligned}\varphi(a') &= \overline{a_{n-1} + \sum_{i=0}^{n-2} a_i X^{i+1}} \\ &= a_{n-1}(\overline{1} - \overline{1} + \overline{X}^n) + \sum_{i=0}^{n-2} a_i \overline{X}^{i+1} \\ &= \sum_{i=0}^{n-1} a_i \overline{X}^{i+1} \\ &= \overline{X} \sum_{i=0}^{n-1} a_i \overline{X}^{i} \\ &= \overline{X}\varphi(a)\end{aligned}$$

— Supposons $\mathscr{C}$ cyclique. Alors, par ce qu'on vient de dire, $\widetilde{\mathscr{C}}$ est stable par multiplication par X. Mais $\widetilde{\mathscr{C}}$ est un sous-espace vectoriel de $\mathbb{F}_q[X]/(X^n-1)$, donc il est aussi stable par addition et par multiplication par un scalaire. Finalement, $\widetilde{\mathscr{C}}$ est bien un idéal de $\mathbb{F}_q[X]/(X^n-1)$.

— Supposons $\widetilde{\mathscr{C}}$ idéal de $\mathbb{F}_q[X]/(X^n-1)$. Alors, $\widetilde{\mathscr{C}}$ est stable par multiplication par X. Donc par le raisonnement précédent, $\mathscr{C}$ est clairement cyclique.

□

Nous arrivons au théorème suivant qui nous indique que, pour fabriquer un code cyclique de dimension m, il suffit de savoir factoriser $X^m - 1$ dans $\mathbb{F}_q[X]$ (ce qui peut se faire par l'algorithme de Berlekamp).

Théorème 23 (Structure des codes cycliques)**.** Soit $m \in [\![0, n]\!]$.

(i) Soit $P = \sum_{i=0}^{n-m} a_i X^i$ un diviseur unitaire de $X^n - 1$ dans $\mathbb{F}_q[X]$. Soit $a = \varphi^{-1}(\overline{P})$ le mot correspondant à P. Alors, en notant $\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n$ l'application de "permutation circulaire",

$$\mathscr{C} = \mathrm{Vect}(\sigma^i(a))_{i \in [\![0, m-1]\!]} \qquad (*)$$

forme un code cyclique de dimension m.

(ii) Réciproquement, si $\mathscr{C}$ est un code cyclique de dimension m sur $\mathbb{F}_q^n$, il existe un polynôme $P \in \mathbb{F}_q[X]$ diviseur de $X^n - 1$ vérifiant $(*)$ pour $\mathscr{C}$.

Démonstration. (i) Clairement, $\mathscr{C} = \mathrm{Vect}(\sigma^i(x))_{i \in [\![0, m-1]\!]}$ est un sous-espace vectoriel de $\mathbb{F}_q^n[X]$ de dimension m : c'est un code linéaire. Reste à montrer qu'il est cyclique. Soit $b = \sum_{i=0}^{m-1} b_i \sigma^i(a)$ un mot de $\mathscr{C}$. Il s'agit de montrer que $\sigma(b) \in \mathscr{C}$. Or,

$$\sigma(b) = \sum_{i=0}^{m-1} b_i \sigma^{i+1}(a) = b_{m-1}\sigma^m(a) + \sum_{i=1}^{m-1} b_{i-1}\sigma^i(m)$$

et, d'après la base choisie pour $\mathscr{C}$, $\sum_{i=1}^{m-1} b_{i-1}\sigma^i(m) \in \mathscr{C}$. Reste à montrer que $b_{m-1}\sigma^m(a) \in \mathscr{C}$.

On a,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= b_{m-1}\overline{X}^m\varphi(a)\\ &= b_{m-1}\overline{X}^m\overline{P}\end{aligned}$$

Or, P est de degré $n-m$, unitaire et divise X^n-1, donc il existe $Q\in\mathbb{F}_q[X]$ unitaire de degré m tel que $X^n-1=PQ$. D'où,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= b_{m-1}(\overline{X}^m-\overline{Q})\overline{P}+b_{m-1}\overline{QP}\\ &= b_{m-1}(\overline{X}^m-\overline{Q})\overline{P}\end{aligned}$$

Comme $b_{m-1}(X^m-Q)$ est de degré au plus $m-1$, on peut l'écrire $\sum_{i=0}^{m-1}c_iX^i$. Ainsi,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= \sum_{i=0}^{m-1}c_i\overline{X}^i\overline{P}\\ &= \sum_{i=0}^{m-1}c_i\varphi(\sigma^i(a))\\ &= \varphi\left(\sum_{i=0}^{m-1}c_i\sigma^i(a)\right)\\ &\in \varphi(\mathscr{C})\end{aligned}$$

D'où $b_{m-1}\sigma^m(a)\in\mathscr{C}$: on a bien ce qu'on voulait.

(ii) Soient $\mathscr{C}$ un code cyclique de dimension m sur $\mathbb{F}_q^n$ et $\pi=\pi_{(X^n-1)}$ la projection de $\mathbb{F}_q[X]$ sur le quotient $\mathbb{F}_q[X]/(X^n-1)$. Alors, d'après la Proposition 22, $\varphi(\mathscr{C})=\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, donc $\pi^{-1}(\widetilde{\mathscr{C}})$ est un idéal de $\mathbb{F}_q[X]$, qui est principal par principalité de $\mathbb{F}_q[X]$. On peut noter P le générateur unitaire. Montrons que $P\mid X^n-1$.

$\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, donc $\overline{0}\in\widetilde{\mathscr{C}}$, donc $X^n-1\in\pi^{-1}(\widetilde{\mathscr{C}})$: il existe $Q\in\mathbb{F}_q[X]$ tel que $X^n-1=QP$. On a bien $P\mid X^n-1$.

Il s'agit maintenant de montrer que P est bien de degré $n-m$. Notons $k=\deg(P)$. Soit

$$E=\{h\in\mathbb{F}_q[X]\mid \deg(h)\in[\![0,n-k-1\}$$

On a,

$$\pi(P\cdot E)=\{\overline{Ph}\in\mathbb{F}_q[X]/(X^n-1)\mid \deg(h)\in[\![0,n-k-1\}$$

et $P\cdot E\subseteq\pi^{-1}(\widetilde{\mathscr{C}})\implies\pi(P\cdot E)\subseteq\widetilde{\mathscr{C}}$.

Soit $R\in\pi^{-1}(\widetilde{\mathscr{C}})$. Par définition de P, il existe $S\in\mathbb{F}_q[X]$ tel que $R=PS$. On effectue la division euclidienne de S par Q :

$$\exists(T,U)\in\mathbb{F}_q[X]\text{ tel que }S=QT+U\text{ avec }\deg(U)<n-k\text{ ou }U=0$$

d'où :

$$\begin{aligned} R &= P(QT+U) \\ &= T(X^n-1)+PU \\ \implies \pi(R) &= \pi(PU) \\ &\in \pi(P\cdot E) \end{aligned}$$

Ainsi, on a $\widetilde{\mathscr{C}} \subseteq \pi(P\cdot E)$. On a alors montré que $\widetilde{\mathscr{C}} = \pi(P\cdot E)$. Or, $|\pi(P\cdot E)| = q^{n-k}$ et $\mathscr{C}$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension m. Par isomorphisme, on a donc :

$$|\mathscr{C}| = q^m = |\widetilde{\mathscr{C}}|$$

ce qui permet de conclure que $m = n-k$.

Pour terminer, on écrit $P = \sum_{i=0}^{n-m} a_i X^i$ et on considère $a = (a_0, \dots, a_{m-1}) \in \mathbb{F}_q^m$. Comme $\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$,

$$\forall i \in [\![0, m-1]\!], \overline{X}^i\overline{P} \in \widetilde{\mathscr{C}} \implies \forall i \in [\![0, m-1]\!], \sigma(a)^i \in \mathscr{C}$$

Et $(\sigma^i(a))_{i\in[\![0,m-1]\!]}$ est une famille libre de cardinal m, donc est bien une base de $\mathscr{C}$.

□

IV - Étude d'un code de Hamming

D'après Wikipédia, un code de Hamming est un code correcteur linéaire. Il permet la détection et la correction automatique d'une erreur si elle ne porte que sur une lettre du message. Un code de Hamming est parfait : pour une longueur de code donnée il n'existe pas d'autre code plus compact ayant la même capacité de correction. En ce sens son rendement est maximal. Il existe une famille de codes de Hamming; le plus célèbre et le plus simple après le code de répétition binaire de dimension 3 et de longueur 1 est sans doute le code binaire de longueur 7, de dimension 4 et de distance minimale 3 : ça tombe bien, il est au programme de l'option C de modélisation !

Définition 24. Le code Hamming $\mathscr{C}_H$ de longueur 7 permet de coder un mot de longueur 4 en un mot de code de longueur 7. C'est un code linéaire, dont une matrice génératrice est

$$G_H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathscr{M}_{7,4}(\mathbb{F}_2)$$

Exemple 25. On souhaite coder le mot $(1,0,0,1)$. On calcule :

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

Le mot codé est donc $(1,1,0,0,1,0,1)$.

On peut en fait expliciter les mots de ce code : il y en a $2^4 = 16$.

Mot	**Mot codé**	**Poids**	**Mot**	**Mot codé**	**Poids**
$(0,0,0,0)$	$(0,0,0,0,0,0,0)$	0	$(1,0,0,0)$	$(1,1,0,1,0,0,0)$	3
$(0,0,0,1)$	$(0,0,0,1,1,0,1)$	3	$(1,0,0,1)$	$(1,1,0,0,1,0,1)$	4
$(0,0,1,0)$	$(0,0,1,1,0,1,0)$	3	$(1,0,1,0)$	$(1,1,1,0,0,1,0)$	4
$(0,0,1,1)$	$(0,0,1,0,1,1,1)$	4	$(1,0,1,1)$	$(1,1,1,1,1,1,1)$	7
$(0,1,0,0)$	$(0,1,1,0,1,0,0)$	3	$(1,1,0,0)$	$(1,0,1,1,1,0,0)$	4
$(0,1,0,1)$	$(0,1,1,1,0,0,1)$	4	$(1,1,0,1)$	$(1,0,1,0,0,0,1)$	3
$(0,1,1,0)$	$(0,1,0,1,1,1,0)$	4	$(1,1,1,0)$	$(1,0,0,0,1,1,0)$	3
$(0,1,1,1)$	$(0,1,0,0,0,1,1)$	3	$(1,1,1,1)$	$(1,0,0,1,0,1,1)$	4

Proposition 26. (i) $\mathscr{C}_H$ a une distance minimale de 3.

(ii) $\mathscr{C}_H$ est 1-correcteur.

(iii) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ est une matrice de contrôle de ce code.

Démonstration. (i) Le minimum des poids est bien 3 d'après le tableau précédent.

(ii) D'après la Remarque 11, la capacité de correction du code est égale à

$$\left\lfloor \frac{3-1}{2} \right\rfloor = 1$$

(iii) Soit $x \in \mathbb{F}_2^7$. On note $(v_0, \dots, v_3)$ la base de $\mathscr{C}_H$ associée à G_H. Alors,

$$\begin{aligned} x \in \mathscr{C}^\perp &\iff \forall i \in [\![0,3]\!], \langle x, v_i \rangle = 0 \\ &\iff x = a h_1 + b h_2 + c h_3 \text{ pour } a, b, c \in \mathbb{F}_2 \end{aligned}$$

où $h_1 = (1,0,0,1,0,1,1)$, $h_2 = (0,1,0,1,1,1,0)$ et $h_3 = (0,0,1,0,1,1,1)$. Donc (h_1, h_2, h_3) est une base de $\mathscr{C}^\perp$, ce qui mène au résultat voulu.

□

Proposition 27. Le code de Hamming est cyclique, engendré par $P = X^3 + X + 1$.

Démonstration. Les 4 vecteurs colonnes de la matrice G_H se déduisent les uns des autres par permutation circulaire. Par conséquent, l'ensemble du code est invariant par permutation circulaire : $\mathscr{C}_H$ est bien cyclique. Et le polynôme P correspond au mot $(1,1,0,1,0,0,0)$ qui est le premier vecteur colonne de la matrice G_H. □

En pratique, le code de Hamming se manipule de la manière suivante :

1. On a un mot $x \in \mathbb{F}_2^4$. On calcule
$$a = G_H x$$
et on envoie a.
2. Le receveur reçoit a'. Il calcule le syndrome $s = H a'$. Si s est nul, il pose $a = a'$. Sinon, il pose $a = a' + e_j$ où pour $j \in [\![1,7]\!]$, $s = H e_j$.
3. Le receveur résout $G_H x = a$.

Bibliographie

Objectif agrégation **[BMP]**

Vincent Beck, Jérome Malick et Gabriel Peyré. *Objectif agrégation*. 2e éd. H&K, 22 août 2005. https://objectifagregation.github.io.

Algèbre et calcul formel **[FFN]**

Loïc Foissy Odile Fleury et Alain Ninet. *Algèbre et calcul formel. Agrégation de Mathématiques Option C*. 2e éd. Ellipses, 9 mai 2023. https://www.editions-ellipses.fr/accueil/14799-algebre-et-calcul-formel-agregation-de-mathematiques-option-c-2e-edition-9782340078567.html.

L'algèbre discrète de la transformée de Fourier **[PEY]**

Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier. Niveau M1*. Ellipses, 15 jan. 2004. https://adtf-livre.github.io.