1 Codes linéaires

Un *code* de longueur n est une partie de $\mathbb{F}_q^n$. Un code *linéaire* C de longueur n sur le corps fini $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$. Par défaut, un code sera supposé linéaire.

La *distance de Hamming* entre deux vecteurs de $\mathbb{F}_q^n$ est le nombre de coordonnées où les deux vecteurs diffèrent.

La *distance minimale* du code C est la plus petite distance non nulle entre deux mots du code C. C'est aussi le plus petit poids (nombre de coordonnées non nulles) d'un mot non nul de C.

Les *paramètres* $[n, k, d]$ d'un code C sont sa longueur, sa dimension (en tant que $\mathbb{F}_q$-espace vectoriel), sa distance minimale. Le code C contient q^k mots de code.

Si $t < d/2$, les boules de Hamming centrées sur les mots de code sont disjointes. Toute configuration de t erreurs peut être corrigée en cherchant le mot de code le plus proche (pour la distance de Hamming).

Une *matrice génératrice* d'un code C est une matrice $k \times n$ à éléments dans $\mathbb{F}_q$, dont les *lignes* constituent une base de C.

Le *code dual* $C^\perp$ de C est l'ensemble des vecteurs $\mathbf{y} = (y_1 \dots y_n)$ de $\mathbb{F}_q^n$ tels que, pour tout $\mathbf{x} = (x_1 \dots x_n) \in C$,

$$\mathbf{x}.\mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n = 0 \quad \text{dans } \mathbb{F}_q.$$

Le code dual $C^\perp$ a pour dimension $\dim C^\perp = n - \dim C$.

Une *matrice de contrôle* ou *de parité* de C est une matrice génératrice du code dual $C^\perp$.

Une matrice génératrice G est dite sous forme *systématique* si elle s'écrit :

$$\mathbf{G} = [I_k \mid \mathbf{A}].$$

Dans ce cas on constate que la matrice

$$\mathbf{H} = [-{}^t\mathbf{A} \mid I_{n-k}]$$

est une matrice de contrôle de C.

Le *syndrome* de $\mathbf{x} \in \mathbb{F}_q^n$ est le vecteur (colonne)

$$\sigma(\mathbf{x}) = \mathbf{H}\,{}^t\mathbf{x}.$$

Retenir :

$$\sigma(\mathbf{x}) = \sum_{i=1}^{n} x_i\mathbf{h}_i$$

où $\mathbf{x} = (x_1 \dots x_n)$ et $\mathbf{h}_1 \dots \mathbf{h}_n$ sont les colonnes de la matrice $\mathbf{H}$. Le vecteur $\mathbf{x}$ est un mot du code C de matrice de parité $\mathbf{H}$ si et seulement si $\sigma(\mathbf{x}) = 0$.

La distance minimale de C est le plus nombre de colonnes de $\mathbf{H}$ sommant à zéro.

Décodage par syndrome. Pour trouver le plus proche mot de code de $\mathbf{x}$, calculer $\mathbf{s} = \sigma(\mathbf{x})$, puis chercher le plus petit ensemble $I \subset \{1, 2, \dots n\}$ tel qu'il existe des $\lambda_i \in \mathbb{F}_q$ non nuls, $i \in I$, et

$$\sum_{i \in I} \lambda_i \mathbf{h}_i = \mathbf{s}.$$

Sur le corps $\mathbb{F}_2$, cette expression se réduit à

$$\sum_{i \in I} \mathbf{h}_i = \mathbf{s}.$$

Le mot de code le plus proche de $\mathbf{x}$ est

$$\mathbf{x} + \sum_{i \in I} \mathbf{e}_i$$

où $\mathbf{e}_i$ est le vecteur constitué de 1 en position i et de zéros partout ailleurs.

Correction d'effacements. Un *effacement* se produit lorsqu'on ne connaît pas la valeur d'une coordonnée. Si l'on appelle vecteur effacement $\varepsilon \in \mathbb{F}_q^n$ le vecteur dont le support est l'ensemble des positions effacées, et si le code linéaire C est utilisé, alors on peut corriger les effacements si et seulement s'il existe un mot $c \in C$ non nul tel que

$$\mathrm{supp(c)} \subset \mathrm{supp}(\varepsilon).$$

Ceci est équivalent à dire que l'ensemble des colonnes de $\mathbf{H}$, $E = \{\mathbf{h}_i, i \in \mathrm{supp}(\varepsilon)\}$ est de rang $|E|$. En pratique, on corrige les effacements en résolvant le système linéaire donné par

$$\sum_{i \in E} \mathbf{h}_i = \sum_{i \notin E} \mathbf{h}_i.$$

En particulier, si le nombre d'effacements est $\leqslant d-1$, on peut toujours retrouver le mot émis sans ambiguïté.

2 Bornes, codes remarquables

Borne de Hamming. Soit $t = \lfloor (d-1)/2 \rfloor$. Comme les boules de Hamming de rayon t sont disjointes on peut écrire $|C||B| \leqslant q^n$ où B est une boule de rayon t : ceci donne

$$q^k \left(1 + \binom{n}{1}(q-1) + \cdots \binom{n}{t}(q-1)^t \right) \leqslant q^n. \tag{1}$$

S'il y a égalité dans (1), on dit qu'on a affaire à un code *parfait*.

Borne de Singleton.

$$d \leqslant n - k + 1. \tag{2}$$

Codes de Hamming binaires. Un code de Hamming binaire est obtenu en prenant comme matrice de parité $\mathbf{H}$ toutes les colonnes non nulles possibles de $\mathbb{F}_2^m$. On obtient un code de paramètres $[2^m - 1, 2^m - 1 - m, 3]$. Ce code est *parfait*.

Codes de Hamming q-aires. On prend cette fois pour colonnes de $\mathbf{H}$ 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

$$[n = (q^m - 1)/(q - 1), n - m, 3].$$

Ce code 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 $[11, 6, 5]$.

Codes BCH binaires. On définit une matrice de parité généralisée à éléments dans le corps $\mathbb{F}_{2^m}$. La première ligne est constitué de tous les éléments non nuls de $\mathbb{F}_{2^m}$. La deuxième ligne est le cube de la première, la troisième ligne, la puissance cinquième, et la ligne t la puissance $2t - 1$. En d'autres termes, chaque colonne de $\mathbf{H}$ est de la forme

$$\begin{bmatrix} x \\ x^3 \\ x^5 \\ \vdots \\ x^{2t-1} \end{bmatrix}.$$

La distance minimale de ces codes vérifie :

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

Ce dernier point se montre en utilisant le fait que les matrices de la forme

$$\begin{bmatrix} x_1 & x_2 & \dots & x_s \\ x_1^2 & x_2^2 & \dots & x_s^2 \\ \dots & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots \\ x_1^s & x_2^s & \dots & x_s^s \end{bmatrix}$$

sont singulières si et seulement il existe i, j, $1 \leqslant i, j \leqslant s$, $i \neq j$ tels que $x_i = x_j$.

Les paramètres de ces codes sont donc $[n = 2^m - 1, k \geqslant n - tm, 2t + 1]$.

3 Codes produits, décodage itératif

Si C_0 est un code de paramètres $[n_0, k_0, d_0]$ et C_1 est un code de paramètres $[n_1, k_1, d_1]$, on définit le code produit $C = C_0 \otimes C_1$ comme l'ensemble des matrices (c_{ij}), $1 \leqslant i \leqslant n_0$, $1 \leqslant j \leqslant n_1$, où tous les vecteurs $(c_{i1} \dots c_{in_1})$ sont des mots de C_1 et tous les vecteurs $(c_{1j} \dots c_{n_0 j})$ sont des mots de C_0.

Le code produit C a pour paramètres $[n_0 n_1, k_0 k_1, d_0 d_1]$.

Le décodage lignes-colonnes permet de corriger n'importe quelle configuration de strictement moins que $d_0 d_1/4$ erreurs.

L'algorithme min-sum se décrit ainsi. Soit (x_{ij}) le vecteur (la matrice) reçu.

Première étape de décodage. Un décodage ligne :

$$\kappa^1_{ij}(0) = \min_{\substack{c \in C_1 \\ c_j = 0}} d(c, x_i)$$
$$\kappa^1_{ij}(1) = \min_{\substack{c \in C_1 \\ c_j = 1}} d(c, x_i)$$

où x_i désigne la i-ème ligne de la matrice (x_{ij}), soit le vecteur $(x_{i1} \dots x_{in_1})$. Ici $d(\cdot, \cdot)$ désigne la distance de Hamming.

Deuxième étape de décodage. Un décodage colonne :

$$\kappa^2_{ij}(0) = \min_{\substack{c \in C_0 \\ c_i = 0}} \sum_{m=1}^{n_0} \kappa^1_{mj}(c_m)$$
$$\kappa^2_{ij}(1) = \min_{\substack{c \in C_0 \\ c_i = 1}} \sum_{m=1}^{n_0} \kappa^1_{mj}(c_m)$$

$(2e-1)$-ème étape (décodage ligne) :

$$\kappa^{2e-1}_{ij}(0) = \min_{\substack{c \in C_1 \\ c_j = 0}} \sum_{m=1}^{n_1} \kappa^{2e-2}_{im}(c_m)$$
$$\kappa^{2e-1}_{ij}(1) = \min_{\substack{c \in C_1 \\ c_j = 1}} \sum_{m=1}^{n_1} \kappa^{2e-2}_{im}(c_m)$$

$2e$-ème étape (décodage colonne) :

$$\kappa^{2e}_{ij}(0) = \min_{\substack{c \in C_0 \\ c_i = 0}} \sum_{m=1}^{n_0} \kappa^{2e-1}_{mj}(c_m)$$
$$\kappa^{2e}_{ij}(1) = \min_{\substack{c \in C_0 \\ c_i = 1}} \sum_{m=1}^{n_0} \kappa^{2e-1}_{mj}(c_m).$$

On montre que deux étapes successives de l'algorithme min-sum corrigent n'importe quelle configuration de $\lfloor d_0 d_1 - 1 \rfloor / 2$ erreurs.

4 Codes cycliques

On appelle *code cyclique q-aire de longueur n* tout $\mathbb{F}_q$-sous-espace vectoriel C de $\mathbb{F}_q^n$ stable par décalage circulaire, c'est-à-dire tel que :

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

Il est commode d'identifier les vecteurs de $\mathbb{F}_q^n$ avec l'ensemble des polynômes de $\mathbb{F}_q[X]$ de degré inférieur ou égal à $n-1$ par la correspondance

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}.$$

L'ensemble des polynômes de degré $\leqslant n-1$ est lui-même un système de représentants de l'anneau quotient $A = \mathbb{F}_q[X]/(X^n - 1)$. L'intérêt de cette identification est que le décalage circulaire est exactement la multiplication par X dans l'anneau A. Ceci nous permet d'énoncer :

Proposition 1 *Les codes cycliques q-aires de longueur n sont les idéaux de l'anneau $A = \mathbb{F}_q[X]/(X^n - 1)$.*

On appelle *polynôme générateur* du code cyclique $C \subset \mathbb{F}_q^n$ le polynôme unitaire non nul de plus petit degré représentant un élément de C.

Théorème 2 *Soit C un code cyclique q-aire de longueur n et soit $g(X)$ son polynôme générateur. Alors*

1. *Le code C est l'idéal $(g(X))$ de l'anneau A.*
2. *Le polynôme de $g(X)$ divise $X^n - 1$ dans $F_q[X]$ (et dans A).*
3. *La dimension de C, en tant que $\mathbb{F}_q$-espace vectoriel, égale $n - \deg g(X)$ et une base en est $(g(X), Xg(X), \ldots, X^{n-\deg g-1} g(X))$. Les vecteurs associés constituent les lignes d'une matrice génératrice de C.*

Preuve :

1. Un quelconque élément de C peut être représenté par un polynôme $c(X)$ de degré $\leqslant n-1$. La division euclidienne de $c(X)$ par $g(x)$ s'écrit

   $$c(X) = q(X)g(X) + r(X)$$

   où $\deg r(X) < \deg g(X)$. Mais dans A on a $r(X) = c(X) - q(X)g(X)$ où $c(X)$ et $q(X)g(X)$ sont tous les deux dans C. On en déduit que $r(X) \in C$ et que $r(X) = 0$ par hypothèse de minimalité du degré de $g(X)$.

3. Comme $\deg c(X) \leqslant n-1$, on a $\deg q(X) \leqslant n-1-\deg g(X)$, ce qui montre que $c(X)$ est une combinaison linéaire des polynômes

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

Par ailleurs, comme toute combinaison linéaire de ces polynômes est de degré au plus $n-1$, ils forment un système libre dans A.

2. L'argument est similaire à celui du *1.* On écrit la division euclidienne dans $\mathbb{F}_q[X]$ de X^n-1 par $g(X)$

$$X^n - 1 = q(X)g(X) + r(X)$$

où $\deg r(X) < \deg g(X)$. On en déduit donc que $r(X) = q(X)g(X) \bmod (X^n - 1)$, donc que $r(X) \in C$, ce qui implique $r(X) = 0$ par hypothèse de minimalité du degré de $g(X)$. ∎

Théorème 3 *Soit $g(X)$ le polynôme générateur d'un code cyclique C de longueur n sur $\mathbb{F}_q$ et de dimension $k = n - \deg g(X)$. Soit $h(X) = h_0 + h_1X + \cdots + h_{k-1}X^{k-1} + X^k = (X^n-1)/g(X)$. Alors le code dual $C^\perp$ de C a comme polynôme générateur le polynôme unitaire réciproque de $h(X)$*

$$h_0^{-1}(h_0X^k + h_1X^{k-1} + \cdots + h_{k-1}X + 1) = h_0^{-1}X^k h(1/X).$$

Preuve : Il suffit de montrer que le vecteur des coefficients du polynôme $1 + h_{k-1}X + \cdots + h_1X^{k-1} + h_0X^k$, soit le vecteur

$$\mathbf{h} = (1, h_{k-1}, \ldots, h_1, h_0, 0 \ldots 0)$$

est orthogonal à une base de C, soit les vecteurs associés aux polynômes

$$g(X), Xg(X), \ldots, X^{k-1}g(X).$$

Mais le vecteur associé au polynôme $g(X)$ est

$$\mathbf{g} = (g_0, g_1, \ldots, g_{n-k}, 0 \ldots 0).$$

On voit que $\mathbf{h}.\mathbf{g}$ est le coefficient de X^{k-1} du polynôme $h(X)g(X)$. De même, lorsque $\mathbf{x}$ décrit les vecteurs décalés de $\mathbf{g}$, les produits $\mathbf{h}.\mathbf{x}$ égalent les autres coefficients du produit $h(X)g(X)$ modulo $X^n - 1$. Mais ce produit est justement nul. ∎

La dimension d'un code cyclique se déduit de manière immédiate de son polynôme générateur. Ce n'est pas le cas de sa distance minimale. C'est l'étude des *racines* du polynôme minimal, (le cas échéant dans un corps d'extension de $\mathbb{F}_q$), qui permet d'évaluer la distance minimale.

Nous nous limitons à des codes binaires. Supposons d'abord que $g(X)$ soit un polynôme irréductible *primitif* de degré m dans $\mathbb{F}_2[X]$. Soit $n = 2^m - 1$. Comme $g(X)$ est un diviseur de $X^n - 1$, il engendre un code cyclique C de longueur n qui est un code de Hamming. Les codes de Hamming peuvent donc être mis sous forme cyclique. De même, les codes BCH peuvent être mis sous forme cyclique.

Codes BCH. Cherchons maintenant à obtenir un code de distance minimale 5. Soit α de nouveau un élément primitif de $\mathbb{F}_{2^m}$. Définissons C comme le code cyclique de longueur $n = 2^n - 1$ constitué des polynômes $c(X)$ de $\mathbb{F}_2[X]/(X^n - 1)$ ayant *simultanément* α et α^3 comme racines. Dis autrement, il s'agit du code cyclique de polynôme générateur $P_\alpha(X)P_{\alpha^3}(X)$ où P_α et P_{α^3} sont les polynômes minimaux de α et α^3.

Proposition 4 *Le code cyclique C défini ci-dessus a un distance minimale*

$$d \geqslant 5.$$

Preuve : Soit $c(X) = c_0 + c_1X + \cdots c_{n-1}X^{n-1}$ un mot du code C. Notons, qu'outre les racines α et α^3, il a aussi α^2 et α^4, conjuguées de α, comme racines. Ceci s'écrit :

$$\sum_{i=0}^{n-1} c_i \begin{bmatrix} \alpha^i \\ \alpha^{2i} \\ \alpha^{3i} \\ \alpha^{4i} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Si $c(X)$ est un mot de poids 4 ou moins, alors tous les c_i sont nuls, sauf au plus quatre d'entre eux. Ceci veut dire qu'il existe une combinaison linéaire non triviale sommant à zéro des colonnes de la matrice

$$\begin{bmatrix} x & y & z & t \\ x^2 & y^2 & z^2 & t^2 \\ x^3 & y^3 & z^3 & t^3 \\ x^4 & y^4 & z^4 & t^4 \end{bmatrix}$$

où x, y, z, t sont des puissances distinctes de α. Mais cette matrice (van der Monde) est non singulière si x, t, z, t sont des éléments distincts du corps $\mathbb{F}_{2^m}$, ce qui est le cas puisque α est primitif. Contradiction. ∎

Généralisation. Tout code cyclique de longueur $n = 2^m - 1$ dont le polynôme générateur a s racines consécutives, soit $\alpha, \alpha^2, \ldots \alpha^s$ où α est un élément primitif de $\mathbb{F}_{2^m}$, a une distance minimale $d \geqslant s + 1$. En particulier le code cyclique de longueur $n = 2^m - 1$ constitué des polynômes ayant pour racines $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$ a une distance minimale $d \geqslant 2t + 1$. Sa dimension est au moins $n - tm$ (regarder le degré du polynôme générateur). De tels codes sont appelés codes BCH t-correcteurs.

Remarque. La construction s'étend à des longueurs n qui ne sont pas nécessairement de la forme $n = 2^m - 1$. Il suffit de remplacer l'élément α par une racine primitive n-ème de 1, c'est-à-dire une racine ζ de $X^n - 1$ telle que toutes les racines de $X^n - 1$ soient des puissances de ζ. Un tel ζ existe toujours. Tout polynôme diviseur de $X^n - 1$ dont $\zeta, \zeta^2, \ldots \zeta^s$ sont des racines engendre un code cyclique de distance minimale au moins $s + 1$.

5 Codes de Reed Solomon

Soit $\{\alpha_1, \ldots, \alpha_n\}$ une partie à n éléments du corps $\mathbb{F}_q$. Soit C l'ensemble des vecteurs de $\mathbb{F}_q^n$ de la forme $(f(\alpha_1), \ldots, f(\alpha_n))$ où $f(X)$ est un polynôme de degré strictement inférieur à $k \leqslant n$.

Le code C est un code linéaire sur $\mathbb{F}_q$ de longueur n, dimension k, et distance minimale $d = n - k + 1$. Il atteint donc la borne de Singleton (2).

On appelle un tel code, *code de Reed-Solomon*.

Interpolation, correction d'effacements. Soit $(c_1, c_2, \ldots, c_n)$ un mot d'un code de Reed-Solomon de paramètres $[n, k, d]$. Soit $K \subset [1, n]$, $|K| \geqslant k$, un ensemble d'indices de positions non effacées $|K| \geqslant k$. Rappelons que *l'interpolation de Lagrange* permet de reconstituer le polynôme $f(X)$ à partir des valeurs $(c_i)_{i \in K}$.

$$f(X) = \sum_{i \in K} c_i \frac{\prod_{j \in K, j \neq i} (X - \alpha_j)}{\prod_{j \in K, j \neq i} (\alpha_i - \alpha_j)}.$$

Matrice génératrice. Une matrice génératrice $\mathbf{G}$ du code de Reed-Solomon C est donnée par :

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}.$$

Lorsque $n = q - 1$, que γ est un élément primitif de $\mathbb{F}_q$, et que

$$\alpha_1 = 1, \alpha_2 = \gamma, \alpha_3 = \gamma^2, \ldots, \alpha_n = \gamma^{q-1},$$

le code C est un code *cyclique*.

5.1 Correction d'erreurs

Soit $(c_1, \ldots, c_n)$ un mot de code associé au polynôme $f(X)$. Notons le vecteur reçu $(r_1, \ldots, r_n)$. Soit e le nombre de symboles erronés, $e = \#\{i, r_i \neq c_i\}$. On

appelle *polynôme localisateur d'erreur* le polynôme

$$E(X) = \prod_{i, r_i \neq c_i} (X - \alpha_i).$$

On a clairement

$$\forall i, \quad f(\alpha_i)E(\alpha_i) = r_i E(\alpha_i).$$

Écrivons $Q(X) = f(X)E(X)$. Soit $t = \lfloor (n-k)/2 \rfloor$ et supposons $e \leqslant t$. On constate que le couple $(Q(X), E(X))$ vérifie les conditions

1. $\deg E \leqslant t$, $\deg Q < k + t$, $E(X)$ est unitaire,
2. $\forall i, \quad Q(\alpha_i) = r_i E(\alpha_i)$.

Le théorème suivant assure que le décodage équivaut à la recherche d'un tel couple $(Q(X), E(X))$.

Théorème 5 *Tout couple $(Q(X), E(X))$ vérifiant les conditions 1 et 2 ci-dessus est tel que :*

$$f(X) = \frac{Q(X)}{E(X)}.$$

Preuve : On a déjà constaté l'existence d'un tel couple $(Q(X), E(X))$. Soit $(Q_1(X), E_1(X))$ un autre couple satisfaisant aux mêmes conditions. On a alors

$$\forall i, \quad Q(\alpha_i)E_1(\alpha_i)r_i = r_i E(\alpha_i)Q_1(\alpha_i)$$

ce qui implique

$$\forall i, \quad Q(\alpha_i)E_1(\alpha_i) = E(\alpha_i)Q_1(\alpha_i)$$

puisque si $r_i = 0$ alors $Q(\alpha_i) = Q_1(\alpha_i) = 0$. Mais la condition 1 implique $\deg(QE_1 - EQ_1) < n$, d'où $QE_1 - EQ_1 = 0$ et $\frac{Q_1(X)}{E_1(X)} = \frac{Q(X)}{E(X)}$. ∎

Les coefficients des polynômes $Q(X), E(X)$ peuvent se trouver simultanément par la résolution d'un système linéaire de n équations à au plus n inconnues (condition 2).