

1 Code de Hamming

1. $\rho = \frac{k}{n} = \frac{11}{15}$.

2. Le code est:

$$\begin{aligned} b_1 &= b_3 + b_5 + b_7 + b_9 + b_{11} + b_{13} + b_{15} \\ b_2 &= b_3 + b_6 + b_7 + b_{10} + b_{11} + b_{14} + b_{15} \\ b_4 &= b_5 + b_6 + b_7 + b_{12} + b_{13} + b_{14} + b_{15} \\ b_8 &= b_9 + b_{10} + b_{11} + b_{12} + b_{13} + b_{14} + b_{15} \end{aligned}$$

Pour mettre sous forme canonique, on fait la permutation: $s_1 = b_3; s_2 = b_5; s_3 = b_6; s_4 = b_7; s_5 = b_9; s_6 = b_{10}; s_7 = b_{11}; s_8 = b_{12}; s_9 = b_{13}; s_{10} = b_{14}; s_{11} = b_{15}; s_{12} = b_1; s_{13} = b_2; s_{14} = b_4; s_{15} = b_8$; d'où une matrice génératrice sous forme canonique $G = [I_{11 \times 11}; R]$

avec $R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$.

3. On calcule les 4 derniers bits de parité $[s_{12}; s_{13}; s_{14}; s_{15}] = [s_1; \dots; s_{11}].R$. Le mot codé est alors: $[s_1; \dots; s_{11}; s_{12}; s_{13}; s_{14}; s_{15}]$.
4. Soit $[y_1; \dots; y_{15}]$ le mot reçu; on calcule $\sigma = [y_1; \dots; y_{11}].R - [y_{12}; y_{13}; y_{14}; y_{15}]$. On détecte une erreur ssi $\sigma \neq 0$.
5. On calcule comme à la question précédente: $\sigma = [\sigma_1; \sigma_2; \sigma_3; \sigma_4]$. Si $\sigma \neq 0$, soit $j = \sum_{i=1}^4 2^i \cdot \sigma_i$. On corrige alors l'erreur en complétant y_j dans y .

2 Codage et décodage des codes linéaires

1. Comme M est inversible, $Im(M^t) = V^k$; d'où :

$$Im(MG) = \{x^t.MG/x \in V^k\} = \{y^t.G/y \in Im(M^t)\} = \{y^t.G/y \in V^k\} = C$$

2.

Existence: comme L est inversible, la matrice $L^{-1}.G = [I_k|L^{-1}R]$ génère C d'après 1.

Unicité: Soit $[I_k|T_1]$ et $[I_k|T_2]$ 2 matrices génératrices de C . Pour tout $x \in V^k$, $[x^t, x^tT_1]$ et $[x^t, x^tT_2]$ sont donc dans C . Comme C est un sev, leur différence $[0x^t(T_1 - T_2)]$ est aussi dans C . Or, le seul élément de C dont les k premières composantes sont nulles est 0. D'où $\forall x \in V^k : x^tT_1 = x^tT_2$, i.e. $T_1 = T_2$.

$$T = L^{-1}R$$

3. Tout mot source $u \in V^k$ (vecteur ligne) est codé par $\phi(x) = uG' = [u, u.T]$.
Ainsi, on écrit u suivi de uT qui contient les chiffres de redondance. On a donc bien un code systématique.

4★. Soit $x \in C$; alors $\exists u \in V^k : x = u[I_k|T]$.

D'où $xH^t = u \cdot [I_k|T] \cdot \begin{bmatrix} T \\ -I_r \end{bmatrix}$.

Soit $M = [I_k|T] \cdot \begin{bmatrix} T \\ -I_r \end{bmatrix}$; M est une matrice $k \times r$ et

$$M_{i,j} = [e^{(k)}_i, T_{i,1}, \dots, T_{i,r}] \cdot \begin{bmatrix} T_{1,j} \\ \vdots \\ T_{k,j} \\ -e_j^{(r)} \end{bmatrix} \quad (1)$$

$$= [e^{(k)}_i] \cdot \begin{bmatrix} T_{1,j} \\ \vdots \\ T_{k,j} \end{bmatrix} + [T_{i,1}, \dots, T_{i,r}] \cdot [-e_j^{(r)}]^t \quad (2)$$

$$= T_{i,j} - T_{i,j} \quad (3)$$

$$= 0 \quad (4)$$

Donc $M = 0$, d'où $x.H^t = u.0 = 0$; i.e. pour tout x , $Hx = 0$.

Réciproquement : si $Hx = 0$ alors $[x_1, \dots, x_n] \cdot \begin{bmatrix} T \\ -I_r \end{bmatrix} = [0, \dots, 0]_r$.

La composante j ($1 \leq j \leq r$) donne alors: $[x_1, \dots, x_k] \cdot \begin{bmatrix} T_{1,j} \\ \vdots \\ T_{k,j} \end{bmatrix} - x_{k+j} = 0$

Soit $x_{k+j} = [x_1, \dots, x_k] \cdot \begin{bmatrix} T_{1,j} \\ \vdots \\ T_{k,j} \end{bmatrix}$

D'où $[x_{k+1}, \dots, x_{k+r}] = [x_1, \dots, x_k].T$.

Finalement on a : $[x_1, \dots, x_n] = [x_1, \dots, x_k].[I_k|T] = [x_1, \dots, x_k].G'$; ainsi $x \in C$.

5. Si on reçoit $y \in V^n$, il suffit de calculer le syndrome d'erreur Hy :

- si $Hy = 0$, alors $y \in C$ et on ne détecte pas d'erreurs;
- sinon $Hy \neq 0$: $y \notin C$ et on détecte une erreur.

6.

a. H peut être vue comme la matrice génératrice d'un code $C_H(n, r)$ sur V ; donc $|Im(H)| = Card(C_H) = |V|^r$.

b. Comme C est t -correcteur, $\exists! x/d_H(x, y) \leq t$. Comme $d_H(x, y) = w_H(x - y) = w_H(e)$, on en déduit : $\exists! e/w_H(e) \leq t$.

De plus $He = Hy - Hx = Hy$ car $Hx = 0$.

c. On tabule toutes les valeurs $(H.e, e)$ pour tous les e tels que $w_H(e) \leq t$ dans une table de hachage, la clé étant le syndrome $H.e$. Il y a $\sum_{i=0}^t (|V| - 1)^i C_n^i$ entrées dans la table; à

chaque élément de clef z_i de $\text{Im}(H)$; correspond dans la table l'élément unique $e_i \in V^n$ de poids minimal tel que $He_i = z_i i$.

La correction est alors triviale : quand on reçoit y , on calcule le syndrome $s = H.y$ et l'on cherche dans la table de hachage ce syndrome; on trouve ainsi e_i de poids minimal tel que $H.e_i = s$. On corrige les erreurs en renvoie $x = y + e_i$.

3 Codes de Golay

1. Code $(12,6,6)$. On remarque que R est symétrique.
2. On vérifie que si r et s sont deux lignes quelconques de G , alors $r.s = 0$; donc $\mathcal{G}_{12} \subset \mathcal{G}_{12}^\perp$. Or $\mathcal{G}_{12}$ et $\mathcal{G}_{12}^\perp$ ont la même dimension $(12,6)$; ils sont donc égaux.
3. Il ne peut pas être parfait car il est de distance paire $(= 6)$.
(En effet: soit x et y 2 mots de code situés à une distance 6; on construit facilement un mot de $\mathbb{F}_3^{12}$ à une distance 3 de x et y , donc impossible à corriger de manière unique).
4. $G_{11} = [I_6 | R_5]$ avec

$$R_5 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 & 2 \\ 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 \end{bmatrix}$$

Comme $\mathcal{G}_{12}$ est de distance 6, $\mathcal{G}_{11}$ est de distance au moins 5. La première ligne est de poids 5 (car la ligne 1ère ligne de R est de poids 4). Or toutes les lignes sont des éléments du code. On en déduit que le code possède un mot de poids 5. Il est donc de distance 5. Le code est donc $(11,6,5)$.

5. Comme $\mathcal{G}_{11}$ est de distance 5, il est 2-correcteur. Ainsi, les boules de rayon 2 centrées sur les mots de $\mathcal{G}_{11}$ sont disjointes et forment un sous-recouvrement de $\mathbb{F}_3^{11}$, de cardinal $3^6(1 + 2.C_{11}^1 + 2^2.C_{11}^2) = 177147$.
Or $\text{card}(\mathbb{F}_3^{11}) = 3^{11} = 177147$; le sous-recouvrement est en fait un recouvrement.
Le code est donc parfait.