

Feuille d'exercices n° 7

Codes correcteurs linéaires : exemples numériques

Exercice 1. Soit C le code binaire linéaire de longueur 7 dont une matrice vérificatrice est

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

- Combien valent la dimension et la distance de C ? Écrire une matrice génératrice de C .
- Décoder les mots reçus $r_1 = 00001110$ et $r_2 = 00010011$, en supposant qu'il y a eu au plus une erreur de transmission.
- Parmi les mots $t_1 = \text{????}0000$, $t_2 = ?0?0?0000$ et $t_3 = ?0?0?0?0$ qui ont subi des effacements, les autres bits ayant été transmis correctement, lesquels peut-on décoder?
- Le code C est-il MDS? Cyclique? Parfait?
- Montrer que, pour tout mot de code m de C , le mot $m + 11111111$ appartient à C . En déduire le nombre de mots de C de poids 4.
- Montrer que C est équivalent au code étendu du code de Hamming H_8 .
- Montrer que C est son propre orthogonal.

Correction.

- $n = 8$, $k = 4$ puisque V est de rang 4. V est de la forme $V = [I_4 \mid A]$, on trouve donc G par $G = [-{}^tA \mid I_4]$, soit

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

Trois colonnes quelconques de V sont indépendantes (remarquer que toute somme de deux colonnes est de poids pair, donc ne peut pas être annulée par une troisième), mais on peut en trouver 4 liées (par exemples C_1, C_2, C_5 et C_6). Donc $d = 4$.

- Les syndromes sont

$$s_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad s_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

On cherche les colonnes correspondantes de V , et on trouve la 4^e pour s_1 et la 3^e pour s_2 . Les erreurs sont donc $e_1 = 00010000$ et $e_2 = 00100000$. Les mots de code transmis étaient donc $m_1 = r_1 + e_1 = 00011110$ et $m_2 = r_2 + e_2 = 00110011$.

- Comme $d = 4$ les mots avec 3 effacements sont corrigibles, donc t_2 ici. Les mots de C sont de la forme $[xA, x]$ avec $x = x_1x_2x_3x_4$ de longueur 4. Comme A est inversible, $t_1 = 0$. Pour t_3 , on résout

$$\begin{aligned} x_1 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_3 &= 0 \\ x_2 &= 0 \\ x_4 &= 0 \end{aligned}$$

On trouve donc les deux solutions 00000000 et 10101010.

4. $d = 4$ et $n - k + 1 = 5$ donc le code n'est pas MDS. Il n'est pas parfait pour des raisons de cardinalité. Le code n'est pas cyclique car le translaté de la première ligne de G , soit 11110000, n'est pas un mot de code.
5. On vérifie bien que 11111111 est un mot de code. Les 4 lignes de G plus leurs translatés font déjà 8 mots de poids 4. Or s'il y a plus de 8 mots de poids 4, alors ils le sont tous puisque le code a 16 mots. Comme ce n'est pas le cas, il y en a au plus 8, donc ce sont ceux-là.
6. On écrit une matrice génératrice de H_8 à partir d'une matrice génératrice de H_7 , et on trouve

$$G_{H_8} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

On permute les colonnes pour retrouver G . Donc les 2 codes sont équivalents.

7. Chaque ligne de G est paire. De plus, chaque paire de lignes de G a un produit scalaire 0. Donc C est inclus dans son orthogonal. Comme ils ont même dimension, ils sont égaux.

Exercice 2. Soit C le code linéaire binaire dont une matrice vérificatrice est

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

1. Quels sont les paramètres (longueur, dimension, distance) de C ?
2. Écrire une matrice génératrice de C .
3. Décoder le mot 0011101, en supposant qu'au plus un bit est faux.
4. Parmi les mots $r_1 = 0000111$ et $r_2 = 0000001$, lesquels peut-on décoder en sachant qu'il y a au plus 2 bits erronés?
5. Parmi les mots $t_1 = ??00111$, $t_2 = ???000$ et $t_3 = 0?0?0?$ ayant subi des effacements, les autres bits étant exacts, lesquels peuvent être décodés?
6. Le code C est-il MDS? Est-il t -correcteur parfait pour un certain entier?
7. Quels sont les paramètres (longueur, dimension, distance) du sous-code pair de C ? De l'orthogonal de C ? Du code étendu de C ?
8. Soit G le groupe des automorphismes de C , c'est-à-dire le sous-groupe de S_7 formé des permutations σ telles que $x \in C \Rightarrow \sigma \cdot x \in C$.
 - (a) Montrer qu'il existe une composante i telle que, pour tout $\sigma \in G$, $\sigma(i) = i$. En déduire que le code C n'est pas cyclique.
 - (b) Déterminer les sous-groupes de G laissant fixe chaque élément de G .
 - (c) Trouver un élément d'ordre 4 de G .

Correction.

1. On a $C_1 + C_3 + C_7 = 0$ donc $d = 3$. $n = 7$, $k = 3$.
- 2.

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

3. Le syndrome vaut

$$s = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

qui correspond à la 7^e colonne de V , donc $e = 0000001$.

4. Les syndromes valent

$$s_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad s_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

s_1 ne correspond à aucune colonne de V donc à aucune erreur à 1 bit. On cherche les paires de colonnes dont la somme donne s_1 : on trouve $C_1 + C_2$ uniquement. Le syndrome correspond soit à l'erreur simple C_7 , soit à $C_1 + C_3$.

5.

6.

7. (a) *Sous-code pair*. On écrit la matrice vérificatrice V' du sous-code pair :

$$V' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

On a $n = 7$, $k = 2$, $d = 4$.

(b) *Orthogonal*. $n = 7$, $k = 4$, $d = 3$.

(c) *Code étendu*. Matrice vérificatrice

$$V'' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$n = 8$, $k = 3$, $d = 4$.

8. (a) En additionnant les deux dernières lignes de G on constate que le mot 1111011 de poids 6 appartient à C . Au vu des deux premières lignes de la matrice de vérification V , tout mot de poids 6 de C doit avoir les deux premières et les deux dernières coordonnées égales à 1. Pour les 3 coordonnées centrales, on voit qu'elles sont alors nécessairement 110. Donc $i = 5$ est un point fixe pour tout $\sigma \in G$. En particulier C n'est pas cyclique.

(b) On voit que C contient exactement 3 mots de poids 3. On constate aussi que les coordonnées centrales 3,4,5 sont globalement invariantes en regardant l'action de σ sur les mots de poids 3. D'après l'action de G sur l'unique mot de poids 5, 34 et 1267 sont globalement invariantes. (2167) est effectivement d'ordre 4.