Codes linéaires

1. Soit C le code engendré par la matrice

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

a. Déterminer le nombre de mots de code de C.

b. Calculer une matrice de contrôle.

c. Calculer la distance minimum de C.

d. Déterminer le nombre d'erreurs que C peut détecter/corriger.

Solution.

a. *La dimension est $k = 4$, donc il y a $16 = 2^4$ éléments.*

b. *Une matrice génératrice en form canonique est*

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

d'où la matrice de contrôle est

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

c. *La distance minimum est 2 car il y a des colonnes égaux dans H.*

d. *Le code peut détecter un erreur, mais il ne peut pas corriger des erreurs.*

2. Soit C le code de matrice de contrôle

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

a. Donner une matrice génératrice pour C.

b. Décoder par syndrome $r = 11101$ et $r' = 11011$.

Solution.

a. *La matrice de contrôle est en forme canonique, et la matrice génératrice associée est*

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

b. *Le syndrome de* $r = 11101$ *est* $rH^t = 110 = eH^t$ *pour* $e = 01000$*, donc* $r \mapsto r + e = 10101$*. Comme* $r'H^t = 000$*, son décodage est* $r' \mapsto r = 110011$*.*

Codes de Hamming

On appelle *code de Hamming* de paramètre $r \geq 2$ un code binaire de longueur $2^r - 1$ et dimension $2^r - r - 1$ ayant pour matrice de contrôle une matrice $H(r)$ de r lignes et $2^r - 1$ colonnes dont toutes les colonnes sont distinctes et non nulle. A équivalence près on peut supposer que la i-ème colonne de $H(r)$ représente l'écriture binaire de l'entier i.

3. Construire $H(2)$ et $H(3)$.

Solution. *Les matrices de contrôles sont*

$$H(2) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{ et } H(3) = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

4. Donner une matrice génératrice pour ces codes.

Solution. *Les matrices de contrôles sont de la forme* $[P^t|I]$*, donc les matrices génératrices sont de la forme canonique* $[I|P]$ *:* $G(2) = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ *et*

$$G(3) = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

5. Montrer que les codes de Hamming sont de distance 3.

Solution. *On établie des conditions pour une code binaire* C *d'avoir distance minimum* 1 *et* 2 *:*

— $d(C) = 1$ *si et seulement s'il y a un colonne de zéros dans* H*.*

— $d(C) = 2$ *si et seulement s'il y a deux colonnes égaux dans* H*.*

En général, $d(C) \leq t$ *si et seulement s'il y a* t *colonnes de* H *qui sont linéairement dépendents.*

Par construction de la matrice génératrice de $H(r)$*, il n'y a pas deux colonnes qui sont linéairement dépendent, mais chaque somme de deux colonnes est un colonnes de* $H(r)$*, donc la distance minimum est* 3*.*

6. Montrer que ce sont des codes parfaits, en particulier l'union des boules de centre les mots du code et de rayon $t = 1$ est égale à $\{0, 1\}^{2^r - 1}$.

Solution. *Les codes de Hamming sont des* $[n, n-r, 3]$*-codes, où* $n = 2^r - 1$*. En particulier ils sont* 1*-correcteurs. Comme la voisinage de rayon un contient*

$$|C|(1+n) = 2^{n-r}2^r = 2^n$$

éléments, ils sont parfait.

7. Montrer qu'un code de Hamming est MDS si et seulement si $r = 2$.

Solution. *Comme* $k = n-r$ *et* $d = 3$*, la borne de Singleton est* $k+d = n-r+3 \leq n+1$*, avec égalité si et seulement si* $r = 2$*.*

8. Ces codes sont très faciles à décoder : montrer qu'on peut choisir pour leader de classe un mot ayant un seul 1 à la place i pour les $2^r - 1$ classes non triviales.

Solution. *Comme le code est parfait, la boule de rayon un* $B(0\ldots0,1)$ *est surjective sur les syndromes :* $|B(0\ldots0,1)| = n+1 = 2^r = |\mathbb{F}_2^{n-k}|$*. Alors le vecteur zéro et les vecteurs de poids* 1 *suffisent pour les leaders de classes.*