Aix-Marseille Université
Préparation à l'agrégation: Option C
`https://www.i2m.univ-amu.fr/perso/david.kohel/tch/Agreg/`

Codes linéaires

Exercices

1. Soit $\mathcal{C}$ 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 $\mathcal{C}$.

b. Calculer une matrice de contrôle.

c. Calculer la distance minimum de $\mathcal{C}$.

d. Déterminer le nombre d'erreurs que $\mathcal{C}$ peut détecter/corriger.

Solution.

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

b. *Une matrice génératrice en forme systématique 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 $\mathcal{C}$ le code avec 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 $\mathcal{C}$.

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

Solution.

a. *La matrice de contrôle est en forme systématique, 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 $r' \mapsto r' = 110011$.*

3. 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 (isomorphisme) près on peut supposer que la i-ème colonne de $H(r)$ représente l'écriture binaire de l'entier i.

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

Solution. *Les matrices de contrôles sont*

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

b. 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 systématique $[I|P]$: $G(2) = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ et*

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

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

Solution. *On établie des conditions pour une code binaire $\mathcal{C}$ d'avoir distance minimum 1 et 2 :*
— *$d(\mathcal{C}) = 1$ si et seulement s'il y a un colonne de zéros dans H.*
— *$d(\mathcal{C}) = 2$ si et seulement s'il y a deux colonnes égaux dans H.*
En général, $d(\mathcal{C}) \leq t$ 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.

d. Montrer que ce sont des codes parfaits, en particulier l'union des boules de rayon $t = 1$ centré sur un mot du code est égale à $\mathbb{F}_2^n$.

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*

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

éléments, ils sont parfait.

e. 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 $r = 2$.*

f. 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.*

4. Montrer que le code binaire de répétition de longueur n (code linéaire avec $G = [1, 1, \ldots, 1]$) est un code MDS, et si $n = d = 2t + 1$, il est parfait.

Solution. *Les paramètres du code de répétition sont $[n, k, d] = [n, 1, n]$, donc il est MDS ($k + d = n + 1$). Si $n = d = 2t + 1$, on a*

$$2^n = \sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{t} \binom{n}{i} + \sum_{i=0}^{t} \binom{n}{i+t+1} = 2\sum_{i=0}^{t} \binom{n}{i} = |\mathcal{C}|\, V(2, n, t).$$

5. Remplir les valeurs de $V(2, n, t)$ dans le tableau suivant :

t	0	1	2	3	4	5	6	7
$V(2,2,t)$								
$V(2,3,t)$								
$V(2,4,t)$								
$V(2,5,t)$								
$V(2,6,t)$								
$V(2,7,t)$								

Pour quelles valeurs $[n, k, d]$ ci-dessus est-ce qu'il peut exister un codage linéaire en bloc parfait ?

Solution. *Les valeurs de $V(2, n, t)$ sont :*

t	0	1	2	3	4	5	6	7
$V(2,1,t)$	1	2	2	2	2	2	2	2
$V(2,2,t)$	1	3	4	4	4	4	4	4
$V(2,3,t)$	1	4	7	8	8	8	8	8
$V(2,4,t)$	1	5	11	15	16	16	16	16
$V(2,5,t)$	1	6	16	26	31	32	32	32
$V(2,6,t)$	1	7	22	42	57	63	64	64
$V(2,7,t)$	1	8	29	64	99	120	127	128
$\vdots$	$\vdots$							$\vdots$
$V(2,15,t)$	1	16	121	576	1941	4944	9949	16384
$\vdots$	$\vdots$							$\vdots$
$V(2,23,t)$	1	24	277	2048	10903	44552	145499	390656

Un codage linéaire binaire peut être parfait seulement si $V(2,n,t) = 2^{n-k}$ où $d = 2t+1$. Alors, selon la table ci-dessus, les seules valeurs possible pour $[n,k,2t+1]$, avec n dans $\{2,\ldots,7,15,23\}$, sont les cas triviaux,
— le $[n,n,1]$-code plein ($t=0$),
— le $[n,1,n]$-code de répétition ($t=(n-1)/2$) pour n impair,
— le $[n,0,\infty]$-code zéro ($t=n$),
et les code de paramètres $[7,4,3]$ et $[15,11,3]$ avec $t=1$, et les paramètres exceptionnels $[23,12,7]$. Ces derniers valeurs correspondent aux $[n,n-r,3]$-codes de Hamming, avec $n=2^r-1$, pour $r=3$ et 4, et le code binaire de Golay (un code parfait exceptionnel et isolé en dehors des cas trivaux et les codes de Hamming).

6. Soit $\mathcal{C}_i : X \to \{0,1\}^n$ les codages linéaires avec matrices génératrices

$$G_1 = \begin{bmatrix} 1&1&0&0&0&1 \\ 0&0&1&1&1&0 \end{bmatrix},\ G_2 = \begin{bmatrix} 1&1&0&0&1&1 \\ 0&0&1&1&1&1 \end{bmatrix},\ \text{et } G_3 = \begin{bmatrix} 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 0&0&1&0&1&1&1 \\ 0&0&0&1&1&0&1 \end{bmatrix}.$$

Rappelons que pour chaque x dans $\mathcal{A}^n$ où $|\mathcal{A}| = q$, et entier t, le cardinal de la boule $B(x,t)$ est

$$|B(x,t)| = V(q,n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

a. Trouver les paramètres $[n,k,d]$ pour chaque code, vérifier les bornes de Singleton et Hamming.

Solution. *Les distances entre les mots de code de $\mathcal{C}_1$ et $\mathcal{C}_2$ sont :*

$d(x,y)$	c_0	c_1	c_2	c_3
c_0	0	3	3	6
c_1	3	0	6	3
c_2	3	6	0	3
c_3	6	3	3	0

$d(x,y)$	c_0	c_1	c_2	c_3
c_0	0	4	4	4
c_1	4	0	4	4
c_2	4	4	0	4
c_3	4	4	4	0

alors leurs distances minimums sont 3 et 4, et leurs paramètres sont $[6,2,3]$ et $[6,2,4]$. Les paramètres de $\mathcal{C}_3$ sont $[7,4,3]$. Les codes satisfont les bornes de Singleton (sans être MDS) et Hamming (avec $\mathcal{C}_3$ parfait).

b. Pour chaque code $\mathcal{C}_i$ et t entre 0 et 2, compter $|B(\mathcal{C}_i,t)|$, le nombre de mots à distance t d'un mot de code.

Solution. *Comme la distance minimum de chaque code est au moins 3, on a*

$$|B(\mathcal{C}_i,0)| = |\mathcal{C}_i| \text{ et } |B(\mathcal{C}_i,1)| = |\mathcal{C}_i|(1+n),$$

Le voisinage $B(\mathcal{C}_1,3)$ est $\{0,1\}^6$ tout entier, car chaque mot est au moins distance 3 de 000000 ou 111111 $\in \mathcal{C}_1$. En effet, le voisinage de rayon 2 de $\mathcal{C}_1$ est aussi $\{0,1\}^6$, car chaque mot avec trois 0 et trois 1 est à distance 2 de 001110 ou 110001.

Le voisinage $B(\mathcal{C}_2, 3)$ est aussi $\{0,1\}^6$ tout entier, mais on voit qu'il y a 8 vectors

$$\left\{ \begin{array}{lll} 010101, & 100101, & 011001, \\ 101010, & 011010, & 100110 \end{array} \right\}$$

en dehors de $B(\mathcal{C}_2, 2)$, donc $|B(\mathcal{C}_2, 2)| = 56$.
Par le comptage ci-dessus, $|B(\mathcal{C}_3, 1)| = |\{0,1\}^7| = 128$, ce que monte que $\mathcal{C}_3$ est parfait. On trouve donc, les valeurs suivantes pour les $|B(\mathcal{C}_i, t)|$.

t	$\lvert B(\mathcal{C}_1, t)\rvert$	$\lvert B(\mathcal{C}_2, t)\rvert$	$\lvert B(\mathcal{C}_3, t)\rvert$
0	4	4	16
1	28	28	128
2	64	56	128