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.

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 $r' = 11011$.

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 $H(3)$.
- **b.** Donner une matrice génératrice pour ces codes.
- **c.** Montrer que les codes de Hamming sont de distance 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 $\mathbb{F}_2^n$.
- **e.** Montrer qu'un code de Hamming est MDS 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.

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.

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 ?

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.

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.