Solution des Exercices du cours de Théorie de l'Information et Codage
cours 8 du 6 avril 2010.

1. Soit C un code linéaire sur les entiers $F_3 = \{0, 1, 2\}$ modulo 3 généré par la matrice

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}.$$

Décoder par la méthode du sydrome les vecteurs: $2121, 1201, 2222$.

- On suppose que le canal est le canal q-aire symétrique. Comme $GG^t = 0$, on a $H = G$ et les sydromes sont $21, 00, 02$ et donc au final le décodage donne: $0121, 1201, 2220$.

2. Montrer que si C est un code linéaire sur F_2 et toute combinaison linéaire de $\leq e$ colonnes de H sont distinctes alors $d_{\min}(C) \geq 2e + 1$ et le code C peut corriger des erreurs de poids $\leq e$.

- si $d_{\min}(C) \leq 2e$ alors il existe $u_1, \ldots, u_e, v_1, \ldots, v_e$ tels qu'on ait une relation de dépendance entre les colonnes de H qui s'écrit puisqu'on est dans F_2: $H_{u_1} + \cdots + H_{u_e} = H_{v_1} + \ldots H_{v_e}$. Le deuxième point est une conséquence directe du cours.

3. Soit C un code (n, k)-linéaire sur F_q et pour tout $\mathbf{y} \in F_q^n$, on définit $C - \mathbf{y} = \{\mathbf{x} - \mathbf{y}, \mathbf{x} \in C\}$. $C - \mathbf{y}$ est un coset de C. Montrer que $C - \mathbf{y} = C$ ssi $\mathbf{y} \in C$, puis que:

(a) si $\mathbf{x}_j$ est un mot code de C, le nombre de mots code à distance de Hamming i de $\mathbf{x}_j$ est A_i, le nombre de mots code de poids i.

(b) le nombre de paires de mots code $(\mathbf{x}, \mathbf{x}')$ avec $d_H(\mathbf{x}, \mathbf{x}') = i$ est exactement $q^k A_i$.

- Deux cosets sont soit disjoints soit égaux d'où le premier résultat. Le nombre de mots code à distance de Hamming i de $\mathbf{x}_j$ est égal à $|\{\mathbf{z} \in C, w_H(\mathbf{z} - \mathbf{x}_j) = i\}| = |\{\mathbf{z} \in C - \mathbf{x}_j, w_H(\mathbf{z}) = i\}|$ qui vaut A_i si $C - \mathbf{x}_j = C$. Pour chaque $\mathbf{x} \in C$, il y a A_i mot code à distance i, d'où le résultat (b).

4. Pour n et d fixés, soit $M_L(n, d)$ le nombre maximum de mots code d'un code linéaire binaire de longueur n et de distance minimale $\geq d$. Montrer que

$$M_L(n, d) \geq \frac{2^n}{1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}}.$$

- Soit k tel que $2^k < \frac{2^n}{1+\binom{n-1}{1}+\cdots+\binom{n-1}{d-2}}$. Nous allons construire une matrice H de taille $n-k \times n$ telle que aucun ensemble de $d-1$ colonnes n'est linéairement dépendant. La première colonne peut être n'importe quelle colonne non-nulle. Si i colonnes ont été choisies de telle sorte qu'aucun ensemble de $d-1$ colonnes ne soit linéairement dépendant. Il y a au plus $\binom{i}{1} + \cdots + \binom{i}{d-2}$ combinaisons linéaires distinctes de ces i colonnes prises $d-2$ ou moins de fois. Si ce nombre est plus petit que $2^{n-k} - 1$, alors on peut ajouter une colonne. On peut construire la matrice H de taille $n - k \times n$ si

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^{n-k}$$