Solutions des Exercices du cours de Théorie de l'Information et Codage
cours 8 du 5 avril 2011.

1. Montrer que $(1-xy)^M \leq 1-x+e^{-yM}$ pour $0 \leq x, y \leq 1$ et $M > 0$.

   - Soit $f(y) = e^{-y} - 1 + y$. Alors $f(0) = 0$, $f'(y) = -e^{-y} + 1 > 0$ pour $y > 0$ et donc pour $0 \leq y \leq 1$, on a $1 - y \leq e^{-y}$ et donc $(1-y)^n \leq e^{-ny}$. On a donc démontré la formule pour $x = 1$ et elle est aussi vraie pour $x = 0$. De plus la fonction $x \mapsto (1-xy)^n$ est convexe et donc
   $$(1-xy)^n \leq (1-x) + x(1-y)^n \leq 1 - x + xe^{-yn} \leq 1 - x + e^{-yn}.$$

2. Dans la preuve du théorème de canal-source, montrer que le choix des β_0, δ_0, δ_1, C' et R' est licite.

   - Les paramètres β, δ et r sont donnés tels que $\beta > \beta_{\min}$, $\delta > \delta_{\min}$ et $r < C(\beta)/R(\delta)$. Alors pour $\beta_{\min} \leq \beta_0 < \beta$ et $\delta_{\min} \leq \delta_0 < \delta$, on a donc $C' < C(\beta_0) \leq C(\beta)$ et $R' > R(\delta_0) \geq R(\delta)$ donc $C'/R' < C(\beta_0)/R(\delta_0) \leq C(\beta)/R(\delta)$ mais la fonction $(\beta, \delta) \mapsto C(\beta)/R(\delta)$ est continue pour $\beta > \beta_{\min}$ et $\delta \in [\delta_{\min}, \delta_{\max})$ tendeant vers l'infini quand $\delta \to \delta_{\max}$ et donc le choix est licite.

3. 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.

4. 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: $0121, 1201, 2220$.

5. 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).