Théorie de l'Information et Codage: Fiche d'exercices 2

à rendre pour le 20 mai 2014.

Instructions: merci à chacun de rendre une copie manuscrite. Si vous avez réfléchi à plusieurs sur un problème, mettez les noms de vos collaborateurs.

Problème 1: (5 points)

Nous allons montrer le résultat suivant: on considère un canal binaire symétrique de capacité $C = 1 - H(p)$. Pour toute suite de codes de longueurs n ayant $M = \lfloor 2^{Rn} \rfloor$ mots code et une probabilité d'erreur moyenne $P_E^n = \frac{1}{M} \sum_{i=1}^{M} P_E^{(i)}$, si $R > C$ alors $P_E^n \to 1$ quand $n \to \infty$.

Soit $e < 1$. Pour tout n, on définit r_n le plus petit entier tel que:

$$\sum_{j=0}^{r_n} \binom{n}{j} p^j (1-p)^{n-j} \geq 1 - e.$$

On considère un (M, n)-code avec $\max_{i=1}^{M} P_E^{(i)} \leq e$.

1. Montrer que $M \sum_{j=0}^{r_n - 1} \binom{n}{j} < 2^n$.
2. Montrer que pour tout $\delta > 0$, pour n suffisament grand, on a $r_n \geq n(p - \delta)$.
3. En conclure que pour tout $\epsilon > 0$ et pour n suffisament grand, $M \leq 2^{n(C+\epsilon)}$.
4. Démontrer le résultat voulu, c'est à dire que l'erreur moyenne doit approcher 1.

Problème 2: Canal avec mémoire (4 points)

On considère un canal binaire symétrique avec $Y_i = X_i \oplus Z_i$ où $\oplus$ est l'addition modulo 2 et $X_i, Y_i \in \{0, 1\}$. Les $Z_1, Z_2, \ldots$ ne sont pas forcément indépendants mais pour tout $n \geq 1$, $(Z_1, \ldots, Z_n)$ est indépendant de $(X_1, \ldots, X_n)$.

1. On suppose que $\mathbb{P}(Z_i = 1) = p = 1 - \mathbb{P}(Z_i = 0)$.Soit $C = 1 - H(p)$. Montrer que

$$\max_{\mathbb{P}_{X_1, \ldots, x_n}} I(X_1, \ldots, X_n; Y_1, \ldots, Y_n) \geq nC.$$

2. On suppose que $\mathbb{P}(Z_1 = 0) = \mathbb{P}(Z_1 = 1) = 1/2$ et que pour $i \geq 1$, $\mathbb{P}(Z_{i+1} \neq Z_i | Z_1, \ldots, Z_i) = q \in [0, 1]$. Montrer que:

$$I(X_1, \ldots, X_n; Y_1, \ldots, Y_n) \quad \leq \quad (n-1)(1 - H(q)).$$

Montrer que cette borne peut être atteinte et comparer au cas sans mémoire.

Problème 3: Codes de Hadamard (5 points)

1. Montrer que parmi les codes de longueur 11 pouvant corriger deux erreurs, le code linéaire le plus grand contient au plus 16 mots code.

Nous allons construire un code plus performant. Une matrice d'Hadamard de taille n est une matrice carrée $n \times n$ à coefficicents dans $\{-1, +1\}$ et telle que: $HH^T = nI$, i.e. le produit scalaire dans $\mathbb{R}$ de deux lignes distinctes est nul et le produit scalaire d'une ligne avec elle-même est n. Comme $H^{-1} = \frac{1}{n} H^T$, on a aussi $H^T H = nI$ et donc les colonnes de H ont la même propriété.

2. Etant donné H, montrer qu'on peut toujours construire à partir de H une matrice de Hadamard telle que la première colonne ainsi que la première ligne soient constituées de $+1$.

On dira qu'une telle matrice de Hadamard est normalisée. Voici des exemples de matrices de Hadamard normalisées (avec la convention $-$ au lieu de -1):

$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}. \tag{1}$$

3. Montrer que si H est une matrice d'Hadamard de taille n alors $n = 1, 2$ ou n est multiple de 4 (Il suffit de considerer les 3 premières lignes d'une matrice normalisée).

L'existence de matrices de Hadamard pour tout n multiple de 4 est une question ouverte. Une construction simple repose sur l'observation que si H_n est une matrice de Hadamard de taille n alors

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

est une matrice de Hadamard de taille $2n$. Cette construction permet d'obtenir les matrices de Sylvester $H_1, H_2, \ldots$ (1). On définit un (n, M, d) code un ensemble de M mots code de longueur n ayant distance minimale d.

4. Montrer qu'à partir d'une matrice de Hadamard normalisée H_n, il est possible de construire des codes binaires ayant les caractéristiques suivantes: $(n-1, n, n/2)$, $(n-1, 2n, n/2-1)$ et $(n, 2n, n/2)$. Conclure.

Problème 4: (4 points)

Il y a n prisonniers dans une salle qui peuvent décider d'une stratégie avant que le jeu ne commence. Ensuite, chacun a un chapeau bleu ou rouge avec probabilité $1/2$ indépendamment des autres. Chaque prisonnier connaît la couleur des chapeaux des autres prisoniers mais aucun prisonnier ne connaît la couleur de son propre chapeau. Le gardien de prison demande aux prisonniers de deviner la couleur de leur chapeau: si un prisonnier se trompe, tous les prisonniers sont tués.

1. Dans une première variante du jeu, tous les prisonniers doivent parler. Dans ce cas, donner une stratégie donnant une probabilité de survie de $1/2$.

2. Dans une seconde variante du jeu, les prisonniers sont interrogés les uns après les autres (séparément) et chaque prisonnier a la possiblité de ne rien dire (au lieu de deviner). Mais si aucun prisonnier ne parle, ils sont également tous tués. Donner une stratégie optimale pour $n = 7$. Généraliser aux cas où $n + 1$ est une puissance de 2.

Problème 5: (2 points)

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

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