Master CSI 1 — 2010-2011

Théorie de l'information, MHT 813 : Examen du 15 avril 2011

Master Sciences et Technologies, mention Mathématiques ou Informatique, spécialité Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

Durée : 3h. Sans document. Les exercices sont indépendants.

– Exercice 1. Une urne contient b boules blanches, n boules noires et r boules rouges. On réalise deux expériences : la première consiste à tirer k boules de l'urne où chaque boule est remise dans l'urne avant de tirer la suivante, et la deuxième consiste à tirer k boules sans remettre les boules tirées dans l'urne. Il en résulte deux k-uples aléatoires $X = (X_1, X_2, \dots, X_k)$ et $Y = (Y_1, Y_2, \dots Y_k)$ de couleurs (c'est-à-dire que $X_i, Y_i \in \{$blanc, noir, rouge$\}$) correspondant aux couleurs des boules tirées dans les deux expériences. Lequel des deux k-uples a la plus grande entropie ? Justifier en évitant de calculer.

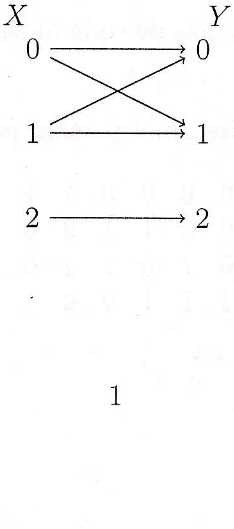
– Exercice 2. Soit X une variable aléatoire à valeurs dans l'ensemble $\mathcal{X} = \{0, 1, \dots, n-1\}$. Soit Z une variable à valeurs dans $\{-1, 0, 1\}$ et soit $Y = X + Z \bmod n$. On considère le canal qui à X associe Y.

$\log n - H(Z)$

a) On suppose que Z est indépendant de X. Calculer la capacité du canal en fonction de n et de $H(Z)$. Quelle est la loi de X qui permet d'atteindre la capacité ?

b) Dans le cas $n = 8$ et $P(Z = -1) = P(Z = 1) = 1/2$, $P(Z = 0) = 0$, donner un code optimal simple qui permet d'atteindre la capacité.

– Exercice 3. On considère le canal discret sans mémoire :



où les probabilités de transition sont données par

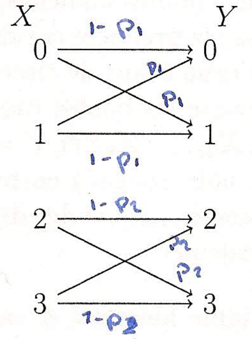
$$P(Y=1|X=0) = P(Y=0|X=1) = p$$
$$P(Y=0|X=0) = P(Y=1|X=1) = 1-p$$
$$P(Y=2|X=2) = 1$$

pour un certain paramètre p.

a) On suppose que $P(X=2)=\alpha$ et on note $I_\alpha(X,Y)$ le maximum de l'information mutuelle $I(X,Y)$ sur toutes les lois de X telles que $P(X=2)=\alpha$. Montrer que $I_\alpha(X,Y)$ est atteinte pour $P(X=0)=P(X=1)$ et en déduire l'expression de $I_\alpha(X,Y)$ en fonction de p et de α.

b) En déduire la capacité du canal en fonction de p. $2 - \frac{1}{2} h(p)$

c) On considère maintenant le canal :



où les probabilités de transition sont données par

$$P(Y=1|X=0) = P(Y=0|X=1) = p_1$$
$$P(Y=0|X=0) = P(Y=1|X=1) = 1-p_1$$
$$P(Y=3|X=2) = P(Y=2|X=3) = p_2$$
$$P(Y=2|X=2) = P(Y=3|X=3) = 1-p_2.$$

Calculer la capacité de ce canal en fonction de p_1 et p_2. On pourra introduire la variable Z qui vaut 0 si $X=0$ ou $X=1$ et qui vaut 1 si $X=2$ ou $X=3$.

– Exercice 4. Montrer qu'il n'existe pas de code linéaire binaire de paramètres $[11,5,5]$.

– Exercice 5. Soit C un code linéaire binaire défini par la matrice de parité $\mathbf{H}$ suivante :

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$ $r=4$

$n=10$

$k = n - r = 6$

a) Quels sont les paramètres de ce code ?

b) Combien C admet-il de mots de poids 3 ? Donnez-en la liste. 6

c) Combien le code C admet-il de mots de poids 7 ?

d) Soit le vecteur

$$\mathbf{x} = [1101001010].$$

Quel est le mot de code le plus proche ?

e) On soumet un mot de code $\mathbf{c}$ au canal binaire à effacements et on reçoit :

$$[101?1???01].$$

Quel est le mot de code $\mathbf{c}$?

f) On note T l'ensemble des mots de $\{0,1\}^n$ qui ne sont ni des mots de code, ni à distance de Hamming 1 d'un mot de code. Combien de mots y a-t-il dans l'ensembe T ? 320

g) Quels sont les syndromes des mots de T ? Montrer qu'un mot de T est à distance 2 d'exactement trois mots de code.

h) On soumet des mots du code C à un canal binaire symétrique de probabilité de transition p. Le décodeur décode le mot reçu $\mathbf{x}$ au maximum de vraisemblance, c'est-à-dire qu'il choisit le mot de code le plus proche de $\mathbf{x}$, ou bien, s'il y a plusieurs mots de code à égale distance de $\mathbf{x}$, il choisit aléatoirement parmi les candidats les plus proches. Quelle est, en fonction de p, la probabilité que le mot émis soit décodé correctement par le décodeur ?

– Exercice 6. On considère le code de Hamming $[7,4,3]$ et on soumet ses mots au canal binaire à effacements de probabilité d'effacement p. Quelle est, en fonction de p, la probabilité que le mot reçu soit décodable sans ambiguïté ?