# Master CSI 1 2008-2009

## Théorie de l'information, MHT 813 : Examen du 24 avril 2009

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

*Responsable :* Gilles Zémor

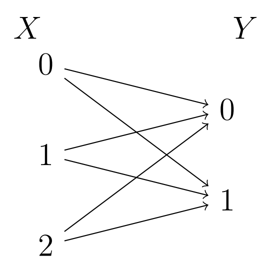
*Durée : 3h. Sans document. Les exercices sont indépendants.*

– Exercice 1. Quels sont les arbres qui sont associés à un code de Huffman binaire ?

– Exercice 2. On prend le $n$-uple ordonné $(1, 2, \ldots, n)$ et on le perturbe aléatoirement en tirant un numéro au hasard et en le réinsérant au hasard dans la suite. Par exemple, pour $n = 10$, on produit $(1, 2, 3, 7, 4, 5, 6, 8, 9, 10)$ en retirant 7 de sa place initiale entre 6 et 8 et en l'insérant entre 3 et 4.

Quelle est l'entropie du $n$-uple résultant ?

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

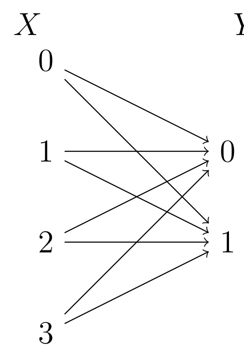



où les probabilités de transition sont données par

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

pour un certain paramètre $p$. Calculer la capacité de ce canal.

– Exercice 4. On considère le canal discret sans mémoire :




où les probabilités de transition sont données par

$$
\begin{array}{llll}
P(Y=1|X=0) & = p & \qquad P(Y=0|X=0) & = 1-p \\
P(Y=0|X=1) & = p & \qquad P(Y=1|X=1) & = 1-p \\
P(Y=1|X=2) & = p & \qquad P(Y=0|X=2) & = 1-p \\
P(Y=0|X=3) & = p & \qquad P(Y=1|X=3) & = 1-p
\end{array}
$$

pour un certain paramètre $p$.

**a)** Calculer, en fonction de $p$, la capacité de ce canal.

**b)** En déduire, dans le cas où la loi de $X$ est uniforme, la valeur de $H(X|Y)$.

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

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

**a)** Quels sont les paramètres $[n, k, d]$ (longueur, dimension, distance minimale) de ce code ?

**b)** Démontrer qu'un quelconque vecteur de $\{0,1\}^{16}$ de poids 3 se transforme de manière unique en un mot de code de poids 4 en changeant un «0» en un «1». En déduire le nombre de mots de poids 4 du code $C$.

**c)** Par une démarche analogue, trouver le nombre de mots de poids 6 de ce code.

**d)** Montrer que n'importe quel vecteur de $\{0,1\}^{16}$ est à distance de Hamming au plus 2 d'un mot de $C$.

**e)** Combien y a-t-il de vecteurs de $\{0,1\}^{16}$ qui ne sont ni des mots de code ni à distance de Hamming 1 d'un mot de $C$ ?

**f)** Soit $\mathbf{x}$ un vecteur de $\{0,1\}^{16}$ qui n'est ni un mot de $C$, ni à distance de Hamming 1 d'un mot de $C$. Montrer qu'il existe 8 mots de $C$ à distance de Hamming 2 de $\mathbf{x}$.

**g)** Quels sont les paramètres du code dual $C^{\perp}$ de $C$ ?

**h)** On reçoit le vecteur suivant avec cinq coordonnées effacées :

$$[????01011101110?].$$

Montrer que le mot du code $C$ coïncidant avec les coordonnées non effacées est unique et le trouver.

**i)** On efface aléatoirement et avec une loi uniforme quatre coordonnées d'un mot $\mathbf{c}$ du code $C$. Calculer la probabilité qu'il soit possible de décoder et de retrouver $\mathbf{c}$ sans ambiguïté.

**j)** Montrer que le code $C$ peut corriger simultanément une erreur et un effacement dans n'importe quelle paire $\{i,j\}$ de positions.

**k)** Soit $\sigma$ la fonction syndrome associée à $\mathbf{H}$,

$$\begin{array}{ccc} \{0,1\}^{16} & \longrightarrow & \{0,1\}^{5} \\ \mathbf{x} & \mapsto & \mathbf{H}\,{}^{t}\mathbf{x}. \end{array}$$

Soit $\mathbf{x} = [x_1 \ldots x_{16}]$ un vecteur aléatoire uniforme de $\{0,1\}^{16}$. Quel est le nombre minimum de coordonnées $x_i$ qu'il faut connaître pour avoir un bit d'information (un shannon) sur la valeur du syndrome $\sigma(\mathbf{x})$ ? Trouver un ensemble minimal de coordonnées $x_i$ dont la connaissance procure deux bits d'information sur la valeur de $\sigma(\mathbf{x})$.