# Master CSI 1 2017-2018

## Théorie de l'information, MA7W08EX : Examen du 28 juin 2018

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

*Responsable :* Gilles Zémor

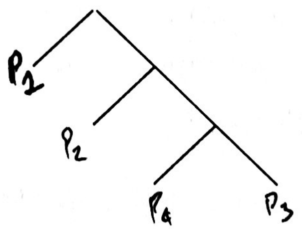
*Durée : 3h. Sans document. Les exercices sont indépendants.*

– EXERCICE 1. On tire à pile ou face 4 fois de suite.

**a)** On appelle $X_{12}$ le nombre de «face» obtenus au cours des lancers 1 et 2 et $X_{23}$ le nombre de «face» obtenus au cours des lancers 2 et 3. Calculer l'information mutuelle $I(X_{12}, X_{23})$.

**b)** On appelle $X_{123}$ le nombre de «face» obtenus au cours des trois premiers lancers et $X_{234}$ le nombre de «face» obtenus au cours des trois derniers lancers. Calculer $I(X_{123}, X_{234})$.

– EXERCICE 2. Quelle est la plus petite valeur de $p_1$ pour laquelle l'algorithme de Huffman appliqué à la loi de probabilité $p_1 \geqslant p_2 \geqslant p_3 \geqslant p_4$ mène à l'arbre suivant ?




– EXERCICE 3. Un joueur A jette deux dés : on note $X$ la somme des deux faces.

**a)** Construire un code de Huffman pour $X$.

**b)** Un joueur B doit découvrir la valeur de $X$ en posant à A des questions dont la réponse est «oui» ou «non». Une procédure est dite optimale si elle permet au joueur B de poser une suite de questions successives dont les réponses déterminent $X$, et telle que le nombre moyen de questions est minimum.

— Quel est le nombre moyen de questions pour une procédure optimale ?

— Quelle est la première question de la procédure optimale ?

– **Exercice 4.** Soit $C$ un code linéaire binaire de paramètres $[n, k, d]$. Soit $I \subset \{1, 2, \dots, n\}$ l'ensemble des coordonnées nulles d'un mot de $C$ de poids $d$. On considère le code poinçonné $C_{|I}$ de support $I$ et déduit de $C$, c'est-à-dire le code de longueur $|I| = n - d$ constitué de tous les mots $\mathbf{x}_{|I} = (x_i)_{i \in I}$ déduits des mots $\mathbf{x} = (x_1, \dots, x_n) \in C$.

**a)** Montrer que $C_{|I}$ a pour paramètres $[n - d, k - 1, d']$ avec $d' \geqslant d/2$.

**b)** En déduire qu'un code $C$ de dimension 3 et de distance minimale $d$ a une longueur au moins égale à $\frac{7}{4}d$.

**c)** Donner une borne inférieure sur la longueur $n$ d'un code de dimension $k$ et de distance minimale $d$.

– **Exercice 5.** Soit $G$ la matrice géneratrice d'un code linéaire binaire $C$ de longueur $n$ et de dimension $k$. On suppose que la matrice $G$ ne contient pas de colonne tout à 0. Montrer que la somme des poids de tous les mots de $C$ égale $n2^{k-1}$.

– **Exercice 6.** On considère un canal d'alphabet d'entrée et de sortie $\mathcal{X} = \mathcal{Y} = \{1, 2, 3, 4, 5\}$ et qui

— transforme 5 en 5 avec probabilité 1,

— pour $x \neq 5$ transforme $x$ en $x$ avec probabilité 1/2 et transforme $x$ en $5 - x$ avec probabilité 1/2.

On appelle $X$ et $Y$ les variables d'entrée et de sortie. Soit $p = P(X = 5)$.

**a)** Calculer $H(Y|X)$ en fonction de $p$.

**b)** Pour toute valeur de $p$ fixée, calculer le maximum de $H(Y)$. On pourra écrire $H(Y) = H(Y, Z)$ où $Z$ est la variable de Bernoulli qui vaut 1 si $X = 5$ et 0 sinon.

**c)** En déduire la capacité du canal. On rappelle que la dérivée de $h(p)$ vaut $\log_2 \frac{1-p}{p}$.

**d)** Décrire une méthode de codage simple permettant d'atteindre la capacité du canal sans faire d'erreur de décodage.

– **Exercice 7.** Soit $C$ le code binaire de matrice génératrice

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

**a)** Quels sont les paramètres de ce code ?

**b)** Montrer que ce code est *uniquement décodable.* Ceci veut dire que pour tout mot $\mathbf{y} \in \mathbb{F}_2^{10}$, il existe un unique mot de code $\mathbf{c}$ qui minimise la distance $d(\mathbf{c}, \mathbf{y})$. On pourra utiliser une matrice de parité du code.