Master CSI 1 — 2019-2020

Théorie de l'information : Examen du 18 décembre 2019

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

Responsable : Gilles Zémor

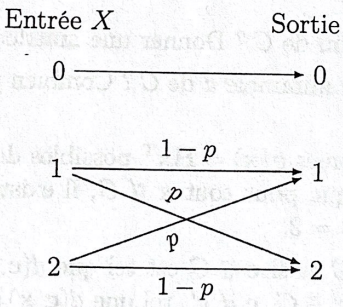
Durée : 3h. Sans document. Les exercices sont indépendants.

– EXERCICE 1. On forme le quintuplet X_1, X_2, X_3, X_4, X_5 de variables aléatoires à valeurs dans $\{0,1,2\}$ en choisissant au hasard avec loi uniforme une ligne de la matrice :

$$\begin{matrix} X_1 & X_2 & X_3 & X_4 & X_5 \end{matrix}$$
$$\begin{bmatrix} 1 & 1 & 2 & 2 & 0 \\ 1 & 2 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 1 \end{bmatrix}.$$

Calculer $H(X_i)$ pour $i = 1 \ldots 5$ et $H(X_j|X_i)$ pour toutes les valeurs de i et j.

– EXERCICE 2. On considère le canal représenté par la figure suivante :



où $p = P(Y = 1|X = 2) = P(Y = 2|X = 1)$. Soient $\alpha = P(X = 0), \beta = P(X = 1)$ et $\gamma = P(X = 2)$.

a) Soit Z la variable aléatoire qui vaut 0 si $Y = 0$ et 1 sinon. Justifier l'égalité $H(Y) = H(Z) + H(Y|Z)$ et en déduire $H(Y)$.

b) Pour α fixé, montrer que $H(Y)$ est maximum pour $\beta = \gamma$.

c) Dans ce cas, trouver la valeur de α qui maximise l'information mutuelle $I(X,Y)$. On rappelle que $\frac{d}{dx}h(x) = \log_2 \frac{1-x}{x}$ où $h(x)$ désigne la fonction entropie binaire.

d) Que vaut la capacité du canal ? Dans le cas $p = 1/2$, donner un code simple qui permet d'attendre de manière fiable la capacité.

– EXERCICE 3. Quel est le plus grand nombre de mots d'un code linéaire binaire de distance minimale 3 dans $\{0,1\}^{20}$ (de longueur 20) ?

– EXERCICE 4. On considère un code de Hamming de paramètres $[7,4,3]$.

a) Combien y a-t-il de mots de poids 3 dans le code ?

b) Montrer que si on efface 4 coordonnées d'un mot $\mathbf{c}$ du code, il n'est pas possible de reconstituer $\mathbf{c}$.

c) On soumet un mot $\mathbf{c}$ du code à un canal à effacements qui efface chaque coordonnée indépendamment des autres avec une probabilité 1/2. Montrer que la probabilité que $\mathbf{c}$ puisse être reconstitué vaut 57/128.

– EXERCICE 5. Soit C le code binaire de matrice génératrice

$$\mathbf{G} = \left[\begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right].$$

a) Quelle est la dimension de C ? Donner une matrice de parité $\mathbf{H}$ de C.

b) Quelle est la distance minimale d de C ? Combien y a-t-il de mots de poids d dans C ?

c) Quels sont les syndromes $\sigma(\mathbf{x}) = \mathbf{H}\mathbf{x}^{\mathrm{T}}$ possibles des mots $\mathbf{x} \in \mathbb{F}_2^{10}$ de poids 1 et 2 ? En déduire que pour tout $\mathbf{x} \notin C$, il existe un mot $\mathbf{c} \in C$ tel que $d(\mathbf{c},\mathbf{x}) = 1$ ou $d(\mathbf{c},\mathbf{x}) = 2$.

d) Montrer que si $\mathbf{x} \notin C$ et si $\mathbf{c} \in C$ est tel que $d(\mathbf{c},\mathbf{x})$ est minimale, alors il n'existe pas de mot $\mathbf{c}' \in C$, $\mathbf{c} \neq \mathbf{c}'$, tel que $d(\mathbf{c},\mathbf{x}) = d(\mathbf{c}',\mathbf{x})$.

– EXERCICE 6. Soit C le code binaire défini par la matrice de parité

$$\mathbf{H} = \left[\begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

a) Quels sont les paramètres de C ?

b) Montrer que tous les mots du code C sont de poids pair.

c) Soit $\mathbf{c} = 101????1??$ un mot de code dont les positions 3,5,6,7,9,10 ont été effacées. Quels sont les mots de code possibles pour $\mathbf{c}$?

d) Donner une matrice génératrice du code C.

e) Quels sont les différents poids possibles des mots de C ? Combien y a-t-il de mots de C pour chacun des poids ?

f) Montrer que tout vecteur $\mathbf{x}$ de $\mathbb{F}_2^{10}$, il existe un mot $\mathbf{c} \in C$, tel que $d(\mathbf{c}, \mathbf{x}) \leqslant 3$.

g) Combien y a-t-il de vecteurs $\mathbf{x}$ tels que pour tout $\mathbf{c} \in C$, $d(\mathbf{c}, \mathbf{x}) > 2$?