Master CSI 1   2020-2021

Théorie de l'information : Examen du 16 décembre 2020

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. Soient X et Y deux variables indépendantes, toutes deux de loi uniforme dans $\mathcal{X} = \{0, 1, 2, 3\}$. Soit Z la variable de Bernoulli qui vaut 0 si $X > Y$ et 1 sinon.

a) Calculer $H(Z|X)$, $H(Z|Y)$ et $H(Z)$.

b) En déduire $H(X|Z)$ et $H(Y|Z)$.

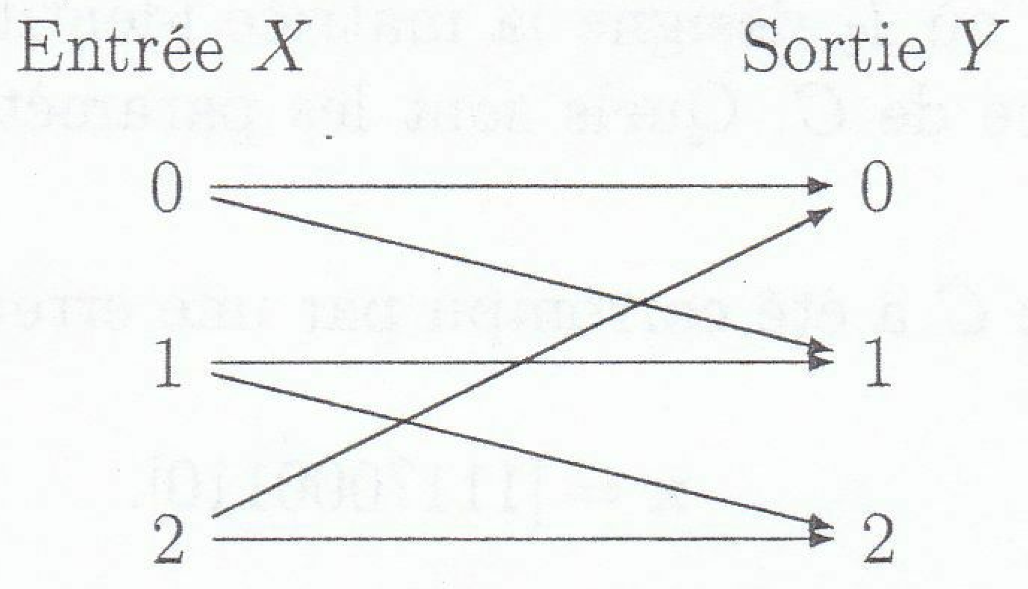
– EXERCICE 2. Soit $X = \sum_{i=1}^{n} X_i$ où les variables X_i sont indépendantes et de même loi de Bernoulli $B(\alpha)$ de paramètre $P(X_i = 1) = \alpha$. En d'autres termes, X suit une loi binomiale de paramètres n et α.

a) Rappeler ce que vaut la divergence de Kullback $\mathrm{D}(B(\beta)\,||\,B(\alpha))$ où $B(\alpha)$ et $B(\beta)$ sont deux lois de Bernoulli de paramètres α et β respectivement.

b) En supposant que αn et βn sont des entiers, montrer que

$$P(X = \beta n) \leqslant 2^{-n\mathrm{D}(B(\beta)\,||\,B(\alpha))}.$$

– EXERCICE 3. On considère le canal représenté par la figure suivante :



où toutes les probabilités de transition de la forme $P(Y = i|X = i)$ sont égales à $1-p$ et les autres sont égales à p pour un certain paramètre p. Calculer sa capacité en fonction de p.

– EXERCICE 4. On considère un canal à N entrées et N sorties, où chaque valeur de la sortie Y est reliée à au plus d valeurs de l'entrée X. Montrer que la capacité C du canal, exprimée en shannons, vérifie :

$$C \geqslant \log_2 N - \log_2 d.$$

– EXERCICE 5. Soit C un code binaire de longueur n. On peut le supposer linéaire mais ce n'est pas nécessaire. On considère un canal binaire symétrique de probabilité de transition $p < 1/2$. On soumet en entrée du canal les symboles $X_1, \dots X_n$ où $X^n = (X_1 \dots X_n)$ est un mot du code C, choisi avec la loi uniforme dans C. Soit Y^n le n-uple de sortie du canal. Pour $\mathbf{c} \in C$ un mot du code et pour $\mathbf{y} \in \mathbb{F}_2^n$ un mot quelconque, exprimer la probabilité conditionnelle $P(X^n = \mathbf{c}|Y^n = \mathbf{y})$ en fonction de $P(Y^n = \mathbf{y}|X^n = \mathbf{c})$. En déduire que pour deux mots de code $\mathbf{c}, \mathbf{c}'$, si $d(\mathbf{y}, \mathbf{c}) < d(\mathbf{y}, \mathbf{c}')$ alors $P(X^n = \mathbf{c}|Y^n = \mathbf{y}) < P(X^n = \mathbf{c}'|Y^n = \mathbf{y})$.

– EXERCICE 6. Montrer qu'il n'existe pas de code linéaire binaire de paramètres $[16, 9, 5]$.

– EXERCICE 7. On considère le code C de matrice de parité $\mathbf{H}$ dont les colonnes décrivent tous les quintuplets de poids 3, soit :

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

a) Quels sont les paramètres du code C ?

b) Donner une matrice de parité de C sous forme systématique, c'est-à-dire de la forme $[A|I_5]$ où I_5 désigne la matrice identité 5×5. En déduire une matrice génératrice de C. Quels sont les paramètres du code dual $C^\perp$ de C ?

c) Un mot $\mathbf{c}$ du code C a été corrompu par une erreur et un effacement pour donner le 10-uple

$$\mathbf{x} = [111?000110].$$

Retrouver $\mathbf{c}$.

d) Un autre mot $\mathbf{c}$ du code C a été corrompu par quatre effacements pour donner le 10-uple

$$\mathbf{y} = [?010100???].$$

Pourquoi est-il possible de retrouver $\mathbf{c}$ sans ambiguïté ? Le faire.

e) Combien y a-t-il de mots de C de poids minimum ?

f) On dit qu'un mot $\mathbf{x} \in \{0,1\}^{10}$ est à distance m du code C si m est la plus petite distance $d(\mathbf{x}, \mathbf{c})$ pour $\mathbf{c} \in C$. Montrer que la distance au code C d'un mot de l'espace $\{0,1\}^{10}$ est au plus 3.

g) Montrer qu'il y a exactement $192 = (1+5) \times 32$ mots de $\{0,1\}^{10}$ à distance 3 du code C.

h) Combien y a-t-il de mots de $\{0,1\}^{10}$ à distance 1 de C ? Combien y a-t-il de mots de $\{0,1\}^{10}$ à distance 2 de C ?