Master CSI 1 2013-2014

Théorie de l'information, MA7W08EX : Examen du 18 décembre 2014

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

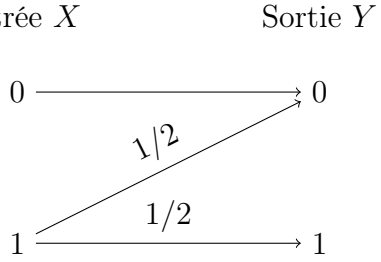
Responsable : Gilles Zémor

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

– Exercice 1. Donner un exemple de deux variables aléatoires X et Y indépendantes, non constantes, telles que $H(X+Y) = H(X) + H(Y)$.

– Exercice 2. Est-ce que la distribution des longueurs $(1, 2, 3, 4)$ peut être obtenue par l'algorithme de Huffman ?

– Exercice 3. On considère le canal représenté par le diagramme suivant :



où $P(Y = 0 \,|\, X = 1) = P(Y = 1 \,|\, X = 1) = 1/2$. Calculer l'information mutuelle entre X et Y en fonction de $\alpha = P(X = 1)$ et montrer que celle-ci est maximum pour $\alpha = 2/5$. En déduire la capacité du canal.

– Exercice 4. Soient U_1 et U_2 deux variables aléatoires indépendantes, chacune à valeurs dans $\{0, 1\}$, et chacune de loi uniforme. On considère par ailleurs un canal binaire à effacement $X \to Y$ de probabilité d'effacement p. On rappelle que ceci veut dire que si X est à valeurs dans $\{0, 1\}$ alors Y vaut X avec probabilité $1 - p$ et vaut le symbole effacement ε avec probabilité p.

a) On soumet au canal deux symboles, soit $X_1 = U_1$, puis $X_2 = U_2$. On obtient deux symboles de sortie, soit Y_1 et Y_2. On note $Y^{(2)}$ le couple (Y_1, Y_2). Que valent les informations mutuelles $I(U_1, Y^{(2)})$ et $I(U_2, Y^{(2)})$?

b) On change maintenant de stratégie et on soumet une première fois au canal $X_1 = U_1 + U_2$, puis on soumet au canal le symbole $X_2 = U_2$. On note toujours $Y^{(2)}$ le couple de sorties (Y_1, Y_2). Calculer les informations mutuelles $I(U_1, Y^{(2)})$ et $I(U_2, Y^{(2)})$.

– Exercice 5. Est-ce qu'un code ternaire (sur l'alphabet $\{0, 1, 2\}$) de paramètres $[8, 4, 5]$ existe ?

– Exercice 6. On considère le code C de matrice de parité

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

a) Quels sont les paramètres de ce code ?

b) Montrer que si on reçoit un mot du code C avec un effacement sur la première coordonnée et une erreur sur la sixième coordonnée, alors on peut corriger l'erreur et l'effacement sans ambiguïté.

c) Montrer qu'il y a quatre coordonnées j, $j \neq 1$, telles que le code C puisse corriger simultanément un effacement sur la première coordonnée, ainsi qu'une erreur sur la j-ème coordonnée. Donner ces valeurs de j.

d) On considère le code C' de longueur 10, constitué de tous les vecteurs de la forme $(x_2, x_3, \ldots, x_{11})$ tels que le vecteur $(x_1, x_2, x_3, \ldots, x_{11})$ soit dans le code C, pour une certaine valeur x_1. Quels sont les paramètres de C' ?

e) Combien C' admet-il de mots de poids 2 ?

f) Trouver le nombre de mots de poids 2 de $\{0, 1\}^{11}$ qui ne sont pas à distance 1 d'un mot du code C.

g) Montrer qu'un mot quelconque de $\{0, 1\}^{11}$ qui n'est pas un mot du code C est soit à distance 1 d'un mot de C, soit à distance 2 d'un mot de C.

h) Si on soumet un mot du code C à un canal binaire symétrique de probabilité d'erreur p, donner, en fonction de p, la probabilité de décoder correctement, sous l'hypothèse où le décodeur est le meilleur possible.

i) Trouver la distance minimale du code dual $C^\perp$ et le nombre de mots de poids minimum de $C^\perp$.

j) On considère la fonction syndrome associée à $\mathbf{H}$,

$$\begin{array}{ccc} \{0,1\}^{11} & \longrightarrow & \{0,1\}^4 \\ \mathbf{x} & \mapsto & \mathbf{H}\,{}^t\mathbf{x}. \end{array}$$

Soit $\mathbf{x} = [x_1 \ldots x_{11}]$ un vecteur aléatoire uniforme de $\{0, 1\}^{11}$. 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 $\sigma(\mathbf{x})$.