Master CSI 1 2012-2013

Théorie de l'information, MA7W08EX : Examen du 18 décembre 2012

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. Soit $X_1, X_2, \ldots, X_i, \ldots$ une suite de variables indépendantes de même loi de Bernoulli $P(X_1 = 0) = P(X_1 = 1) = 1/2$. La suite (X_i) est encodée par la fonction :

$$0 \mapsto 0$$
$$1 \mapsto 01$$

pour former la suite de symboles binaires $Y_1, Y_2, \ldots, Y_i, \ldots$

a) Que valent les entropies $H(Y_1)$, $H(Y_2)$, $H(Y_3)$ et $H(Y_4)$? Vers quoi tend $H(Y_i)$ lorsque i devient grand ?

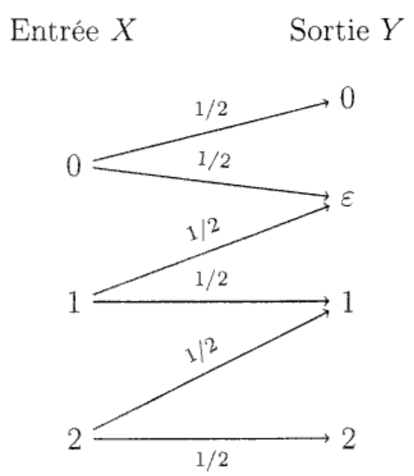
b) Que valent $H(Y_2 \mid Y_1)$, $H(Y_3 \mid Y_2)$, $H(Y_4 \mid Y_3)$?

– EXERCICE 2. On considère un canal à N entrées et N sorties. On suppose que chaque valeur de la *sortie* Y est reliée à au plus Δ valeurs de l'entrée X. Montrer que la capacité du canal, exprimée en shannons, est minorée par :

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

On pourra utiliser l'expression $I(X, Y) = H(X) - H(X|Y)$.

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



On posera $P(X=0)=a$, $P(X=1)=b$, $P(X=2)=c$.

a) Calculer, en fonction de a,b,c, les probabilités $P(Y=\varepsilon)$ et $P(Y=1)$, ainsi que les probabilités conditionnelles $P(X=0\,|\,Y=\varepsilon)$ et $P(X=1\,|\,Y=1)$.

b) Donner une expression de $H(X\,|\,Y)$ en fonction de a,b,c.

c) Montrer que $I(X,Y)=(h(a)+h(c))/2$ où h désigne la fonction entropie binaire.

d) En déduire la capacité du canal. Quel codage simple permet d'atteindre la capacité ?

– EXERCICE 4. On considère le code C de matrice de parité $\mathbf{H}$ dont les colonnes décrivent tous les quintuplets de poids 5, 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 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 ?

– EXERCICE 5. On considère la matrice $\mathbf{H}$ suivante :

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

À chaque vecteur $X \in \{0,1\}^6$ on associe le vecteur $S \in \{0,1\}^2$ par la transformation linéaire

$$S = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = \mathbf{H}\,{}^t\!X.$$

Le vecteur $X = (x_1, \ldots, x_6)$ est choisi aléatoirement avec une loi uniforme dans $\{0,1\}^6$. Puis il est soumis à un canal à effacement, de probabilité de transition $1/2$, pour donner le 6-uple $Y \in \{0,1,?\}^6$.

a) Montrer que s'il y a au moins 3 bits effacés, alors Y n'apporte aucune information sur S.

b) Montrer que s'il y a exactement 1 bit effacé, alors Y apporte 1 bit d'information sur S.

c) Quelles sont les configurations de deux effacements pour lesquelles Y apporte 1 bit d'information sur S ?

d) Soit A l'ensemble des $y \in \{0,1,?\}^6$ tels que $H(S \mid Y = y) = 1$. Calculer $P(Y \in A)$.

e) En déduire $H(S \mid Y)$.