Master CSI 1 2015-2016

Théorie de l'information, MA7W08EX : Examen du 11 décembre 2015

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. Soient X une variable aléatoire de Bernoulli de loi uniforme $P(X=0) = P(X=1) = 1/2$. Soient Y et Z deux variables de même loi que X et telles que X, Y, Z sont indépendantes dans leur ensemble. Calculer l'information mutuelle $I(X+Y, X+Y+Z)$ où l'addition s'entend dans les entiers.

– EXERCICE 2. On considère le canal dont l'entrée X prend ses valeurs dans l'alphabet $\{0,1,2,3\}$ et dont la sortie Y prend ses valeurs dans $\{0,1,2,3,4\}$ et est obtenue à partir de X en lui ajoutant l'entier 0 ou l'entier 1, avec probabilité 1/2. En faisant l'hypothèse raisonnable que l'information mutuelle $I(X,Y)$ est maximisée pour une loi de X telle que $P(X=0) = P(X=3)$ et $P(X=1) = P(X=2)$, trouver la capacité du canal.

– EXERCICE 3. Soit $\mathcal{C}$ un canal discret sans mémoire. Soit X_1, X_2 deux variables aléatoires, prenant chacune leurs valeurs dans l'alphabet d'entrée du canal. Soient Y_1 et Y_2 les variables de sortie correspondantes. En supposant que X_1 et X_2 sont indépendantes de même loi, montrer que $I((X_1, X_2), (Y_1, Y_2)) = 2I(X_1, Y_1)$.

– EXERCICE 4. Soit C un code de Hamming binaire en longueur $15 = 2^4 - 1$.

a) Rappeler quels sont ses paramètres.

b) Montrer qu'étant données deux positions distinctes $i, j \in \{1, 2, \ldots, 15\}$, il existe un unique mot $\mathbf{x} = (x_1, x_2, \ldots x_{15})$ du code C de poids 3 tel que $x_i = x_j = 1$. En constatant qu'un mot $\mathbf{x}$ de poids 3 admet 3 paires de positions $\{i, j\}$ telles que $x_i = x_j = 1$, en déduire le nombre total de mots de C de poids 3.

c) On considère maintenant un code de Hamming ternaire (sur l'alphabet $\{0, 1, -1\}$) de longueur $13 = (3^3 - 1)/2$. Calculer le nombre de mots de poids 3 du code.

– EXERCICE 5. Soit la matrice de parité

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

Alice transmet un 7-uple binaire $\mathbf{x} = [x_1, \ldots, x_7]$ à Bob avec la convention que le message secret associé est le syndrome $\sigma(\mathbf{x})$. Pour communiquer un secret de trois bits, on transmet donc sur le canal sept symboles binaires. On suppose que $\mathbf{x}$, et donc $\mathbf{s}$, suivent des lois uniformes dans $\{0,1\}^7$ et $\{0,1\}^3$.

On suppose maintenant que Alice communique à Bob deux secrets de trois bits, soit $\mathbf{s}$ et $\mathbf{t}$, en transmettant les deux 7-uples $\mathbf{x} = [x_1, \ldots, x_7]$ et $\mathbf{y} = [y_1, \ldots, y_7]$. Une espionne, Eve, est capable d'intercepter jusqu'à 7 des 14 symboles transmis, mais pas plus. Montrer qu'elle est capable d'obtenir un des secrets, mais que quels que soient les symboles qu'elle intercepte, elle a zéro bit d'information sur au moins un des deux secrets $\mathbf{s}$ ou $\mathbf{t}$.

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

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

a) Quels sont les paramètres du code C ?

b) Combien le code C a-t-il de mots de poids minimum ?

– Exercice 7. Montrer que si un code linéaire C a une distance minimale 4, alors il existe des mots $\mathbf{x}$ de l'espace tels que pour tout mot de code $\mathbf{c} \in C$, la distance de Hamming de $\mathbf{x}$ à $\mathbf{c}$ vérifie $d(\mathbf{x}, \mathbf{c}) \geqslant 2$. En déduire qu'il n'existe pas de code linéaire binaire de paramètres $[7,4,4]$.

– Exercice 8. On considère le code binaire C de matrice de parité

$$\mathbf{H} = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{matrix} \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

a) Quels sont les paramètres de ce code ?

b) On reçoit le mot

$$[? \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1]$$

où la première coordonnée a été effacée. En faisant l'hypothèse qu'au plus une coordonnée non effacée est en erreur, montrer qu'on peut retrouver le mot de code d'origine sans ambiguïté et le donner.

c) Donner une configuration minimale d'effacements (avec un nombre minimum d'effacements) non corrigible, et une configuration maximale d'effacements corrigible.

d) Quels sont les paramètres du code dual $C^{\perp}$?

e) Calculer le nombre de mots de l'espace $\{0,1\}^{10}$ qui ne sont pas à distance 0 ou 1 d'un mot de code.