Master CSI 1 2017-2018

Théorie de l'information : Examen du 19 décembre 2017

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 considère 4 variables aléatoires X_1, X_2, X_3, X_4, indépendantes, de même loi $P(X_i = 1) = P(X_i = -1) = 1/2$. On pose $W_0 = 0$ et

$$W_i = \sum_{j=1}^{i} X_j \quad \text{pour } i = 1, 2, 3, 4.$$

Calculer les informations mutuelles $I(W_i, W_{i+1})$ pour $i = 0, 1, 2, 3$.

– EXERCICE 2. On considère des canaux d'alphabets d'entrée et de sortie $\mathcal{X} = \mathcal{Y} = \{0, 1\}^3$.

a) Un premier canal C_1 transforme chaque triplet binaire x en x avec probabilité $1/2$ et en le triplet complémentaire $\overline{x} = (1, 1, 1) - x$ avec probabilité $1/2$. Quelle est la capacité de ce canal ?

b) Décrire un moyen simple d'atteindre la capacité du canal C_1.

c) Un deuxième canal C_2 transforme
- (000) en (000) avec probabilité 1,
- (111) en (111) avec probabilité 1,
- chaque autre symbole x en x avec probabilité $1/2$ et en $\overline{x}$ avec probabilité $1/2$.

En appellant X et Y les variables d'entrée et de sortie, calculer $H(Y|X)$ en fonction de la probabilité p que X soit égal à (000) ou à (111).

d) Pour toute valeur de p fixée, calculer le maximum de $H(Y)$. On pourra écrire $H(Y) = H(Y, Z)$ où Z est la variable de Bernoulli qui vaut 1 si $X = (000)$ ou $X = (111)$, et qui vaut 0 sinon.

e) En déduire la capacité du canal C_2. On rappelle que la dérivée de $h(p)$ vaut $\log_2 \frac{1-p}{p}$.

f) Décrire un moyen simple d'atteindre la capacité du canal C_2.

– EXERCICE 3. Quelles conditions la matrice de parité d'un code linéaire ternaire (d'alphabet $\mathbb{Z}/3\mathbb{Z}$) doit elle vérifier pour que le code ait une distance minimale au moins 3 ? Quelle est la longueur maximale d'un code ternaire de distance minimale au moins 3, dont une matrice de parité a trois lignes ?

– EXERCICE 4. Le code de Golay ternaire C admet pour matrice de parité

$$\mathbf{H} = \left[\begin{array}{cccccc|ccccc} 1 & 1 & 1 & 2 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

a) Donner un mot de poids 5 du code.

b) On considère le vecteur $\mathbf{x} = [21212121212]$. A quelle distance est-il du code ? quel est le mot de code le plus proche ?

c) Combien y a-t-il de vecteurs de l'espace $\{0,1,2\}^{11}$ qui sont à distance 1 d'un mot du code ?

d) Montrer qu'un mot quelconque de poids 3 de $\{0,1,2\}^{11}$ est à distance 2 d'un mot du code C.

e) Combien y a-t-il de mots de poids 3 dans $\{0,1,2\}^{11}$? Soit $\mathbf{x}$ un mot de poids 5 : combien de mots de poids 3 sont à distance 2 de $\mathbf{x}$? En déduire que le code C admet 132 mots de poids 5.

– EXERCICE 5. Soit $\mathbf{H}$ une matrice $r \times n$ qui est une matrice de parité d'un code de dimension $k = n - r$ et de distance minimale au moins 5.

a) Montrer que si

$$1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} < 2^r$$

alors il est possible de rajouter une colonne à la matrice $\mathbf{H}$ pour former une matrice de parité d'un code de paramètres $[n+1, k+1, d \geqslant 5]$.

b) En déduire que si

$$2^k \leqslant \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}}$$

alors il existe un code de longueur n, de dimension k, et de distance minimale au moins 5.

c) Pour la longueur $n = 18$, quelle est la plus grande dimension d'un code de distance minimale $\geqslant 5$ que vous pouvez garantir avec cet argument ?

– EXERCICE 6. On considère le code linéaire binaire dont une matrice de parité est

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

a) Quels sont les paramètres de ce code ?

b) On reçoit le vecteur

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

dont les deux premiers caractères sont effacés. En supposant qu'au plus un symbole non effacé est erroné, corriger l'erreur et les effacements pour obtenir un mot de code.

c) Quels sont les paramètres du code dual ?