Master CSI 1 2021-2022

Théorie de l'information : Examen du 15 décembre 2021

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

Responsable : Gilles Zémor

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

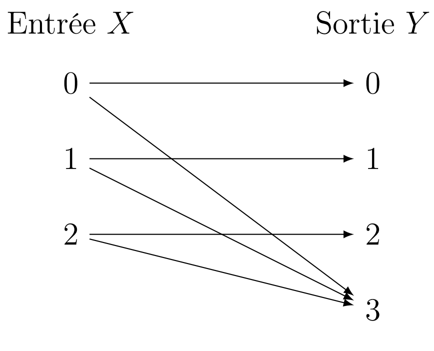
– Exercice 1. On forme un quadruplet aléatoire $X = (X_1, X_2, X_3, X_4)$ de la manière suivante : on part du quadruplet $(1, 2, 3, 4)$. Puis on tire deux variables Y, Z indépendantes et uniformes dans $\{1, 2, 3, 4\}$. On retire ensuite l'entier Y du quadruplet $(1, 2, 3, 4)$ pour l'insérer en position Z. Par exemple pour $Y = 2$ et $Z = 3$ on obtient $X = (1, 3, 2, 4)$. Pour $Y = 4$ et $Z = 1$ on obtient $X = (4, 1, 2, 3)$.

a) Calculer $H(X)$.

b) Calculer $H(X_1)$.

c) Calculer $H(X_2|X_1)$.

– Exercice 2. 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 3. On considère un canal dont les alphabets d'entrée et de sortie sont tous les deux $\mathbb{F}_2^8$. Si $e_1, \ldots, e_8$ désignent les huits mots de poids 1, le canal transforme toute entrée x en $x + e_i$ avec probabilité $1/8$. En d'autres termes, le canal modifie aléatoirement et uniformément un bit de l'octet transmis.

a) Calculer la capacité de ce canal.

b) Montrer comment atteindre la capacité simplement à l'aide d'un code de Hamming.

– EXERCICE 4. On définit un code binaire C de longueur 16, où chaque coordonnée est indexée par un couple (i, j), $1 \leqslant i, j \leqslant 4$. Le code C est l'ensemble des mots tels que pour tout i dans $\{1, 2, 3, 4\}$, chaque sous-mot indexé par les coordonnées $(i, 1,), (i, 2), (i, 3), (i, 4)$ est de poids pair, et chaque sous-mot indexé par les coordonnées $(1, i), (2, i), (3, i), (4, i)$ est de poids pair également.

a) Montrer que ce code est linéaire et quels sont ses paramètres, dimension et distance minimale ?

b) Pour ce code, quel est le plus grand entier w tel que n'importe quelle configuration de w effacements est corrigible ? Quel est le plus grand entier w tel qu'il existe une configuration de w effacements corrigible ?

c) Trouver les paramètres du code dual de C.

d) Si k est la dimension du code C, montrer qu'il existe un autre code linéaire de même longueur 16, de dimension $k + 2$, et de même distance minimale que C.

– EXERCICE 5. On considère la matrice

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

a) Ajoutez une colonne et une ligne à M pour former une matrice H de dimension 5×9 qui est la matrice de parité d'un code C de distance minimale 4 et qui contient le vecteur tout-à-un $[1, 1, 1, 1, 1, 1, 1, 1, 1]$.

b) Décrire toutes les manières d'ajouter une colonne et une ligne pour obtenir ce résultat.

– EXERCICE 6. On considère le code binaire C de matrice de parité

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

a) Quels sont les paramètres de ce code ?

b) On reçoit le mot

$$\begin{bmatrix} ? & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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.