Master CSI 1 2024–2025

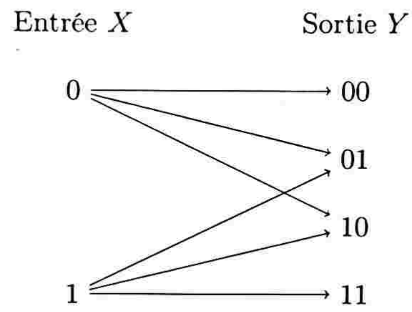
Théorie de l'information, 4TCY806U : Session 1 du 23/04/2025

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

Responsable : Elena Berardini

Durée : 3h. Sans document. Les exercices sont indépendants. Toutes les réponses doivent être justifiées. La qualité de la rédaction sera un facteur d'appréciation.

– EXERCICE 1. **Calcul de capacité.** On considère le canal représenté par le diagramme suivant :



Toutes les probabilités de transition valent 1/3. Calculer la capacité de ce canal.

– EXERCICE 2. **Arbre de Huffman.** Soit p une loi de probabilité dont la plus grande probabilité est p_1. Montrer que si $p_1 < \frac{1}{3}$ alors un code de Huffman n'encode jamais le symbole de probabilité p_1 par un mot de longueur 1.

– EXERCICE 3. **Codes et matrice génératrice.** Soit C le code binaire de matrice génératrice

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

a) Déterminer le nombre de mots du code C.

b) Ecrire la matrice génératrice de C en forme systématique et donner la matrice de parité du code C.

c) Quels sont les paramètres de C ? Et du code dual de C ?

d) Le mot (111?00) est un mot $\mathbf{c}$ de C qui a subi un effacement. Est-il possible de retrouver $\mathbf{c}$? Justifier et, dans le cas affirmatif, determiner $\mathbf{c}$.

e) Le mot (111001) est un mot $\mathbf{c}'$ de C qui a subi une erreur. Est-il possible de retrouver $\mathbf{c}'$? Justifier et, dans le cas affirmatif, determiner $\mathbf{c}'$.

– EXERCICE 4. **Matrice de parité et syndrome.** Soit C le code linéaire binaire dont la matrice de parité est

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

a) Est-ce que le code C atteint la borne de Griesmer ?

b) Décoder par syndrome le message $y = (11101)$.

– EXERCICE 5. **Code poinçonné.** Soit C un code linéaire binaire de paramètres $[n, k, d]$. Soit $I \subset \{1, 2, \ldots, n\}$ l'ensemble des coordonnées nulles d'un mot de C de poids d. Soit $\pi_I : \mathbb{F}_q^n \to \mathbb{F}_q^{|I|}$ la projection sur les coordonnées indexées pas I. On considère le code poinçonné $\pi_I(C)$ de support I et déduit de C, c'est-à-dire le code de longueur $|I|$ constitué de tous les mots $\pi_I(\mathbf{x}) = (x_i)_{i \in I}$ déduits des mots $\mathbf{x} = (x_1, \ldots, x_n) \in C$.

a) Montrer que $\pi_I(C)$ a pour paramètres $[n - d, k - 1, d']$ avec $d' \geqslant d/2$.

b) En déduire qu'un code C de dimension 3 et de distance minimale d a une longueur au moins égale à $\frac{7}{4}d$.

– EXERCICE 6. **Poids de mots d'un code.** Soit G la matrice génératrice d'un code linéaire binaire C de longueur n et de dimension k. On suppose que la matrice G ne contient pas de colonne tout à 0. Montrer que la somme des poids de tous les mots de C égale $n2^{k-1}$. On pourra considérer un tableau $2^k \times n$ dont toutes les lignes décrivent les mots du code C, et compter le nombre de 1 dans chaque colonne.