Master CSI 1 — 2023-2024

Théorie de l'information, 4TCY806U : DST du 14 mai 2024

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. **Entropie, capacité d'un canal, et codage.** On considère un canal d'alphabet d'entrée et de sortie $\mathcal{X} = \mathcal{Y} = \{1, 2, 3, 4, 5\}$ et qui

- transforme 5 en 5 avec probabilité 1,
- pour $x \neq 5$ transforme x en x avec probabilité 1/2 et transforme x en $5 - x$ avec probabilité 1/2.

On appelle X et Y les variables d'entrée et de sortie. Soit $p = P(X = 5)$.

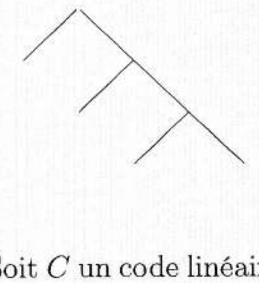
a) Calculer $H(Y|X)$ en fonction de p.

b) 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 $X = 5$ et 0 sinon.

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

d) Décrire une méthode de codage simple permettant d'atteindre la capacité du canal sans faire d'erreur de décodage.

– EXERCICE 2. **Arbre de Huffman.** Quelle est la plus petite valeur de p_1 pour laquelle l'algorithme de Huffman appliqué à la loi de probabilité $p_1 \geqslant p_2 \geqslant p_3 \geqslant p_4$ mène à l'arbre suivant ?



– EXERCICE 3. **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. On considère le code poinçonné $C_{|I}$ de support I et déduit de C, c'est-à-dire le code de longueur $|I| = n - d$ constitué de tous les mots $\mathbf{x}_{|I} = (x_i)_{i \in I}$ déduits des mots $\mathbf{x} = (x_1, \ldots, x_n) \in C$.

a) Montrer que $C_{|I}$ 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 $\frac{3}{2}d$.

– EXERCICE 4. **Codes et boules de Hamming.** Existe-t-il un code linéaire ternaire (sur l'alphabet $\mathbb{F}_3 = \{0, 1, 2\}$) de paramètres $[12, 7, 5]$? Il s'agit de calculer le nombre d'éléments dans une boule de rayon 2 de l'espace $\{0, 1, 2\}^{12}$.

– EXERCICE 5. **Codes et matrices de parité.** Soit C le code binaire de matrice de parité

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

a) Quels sont les paramètres de ce code ?

b) Considérer toutes les valeurs s de $\mathbb{F}_2^5$, et trouver le nombre minimal de colonnes de H qui somment à s. Quel est le plus petit entier t tel que pour tout vecteur $\mathbf{y} \in \mathbb{F}_2^{10}$, il existe un mot de code $\mathbf{c} \in C$ avec $d(\mathbf{y}, \mathbf{c}) \leqslant t$?

c) Montrer que le code C est *uniquement décodable.* Ceci veut dire que pour tout mot $\mathbf{y} \in \mathbb{F}_2^{10}$, il existe un unique mot de C qui minimise la distance $d(\mathbf{c}, \mathbf{y})$. En d'autres termes, il existe un unique mot de code $\mathbf{c}$ tel que pour tout $\mathbf{c}' \in C$, $\mathbf{c}' \neq \mathbf{c}$, $d(\mathbf{c}', \mathbf{y}) > d(\mathbf{c}, \mathbf{y})$.

– EXERCICE 6. **Code de Reed–Solomon étendu.** Soit $\mathbf{x} = (x_1, \ldots, x_q) \in \mathbb{F}_q^q$ tel que $\mathbb{F}_q = \{x_1, \ldots, x_q\}$. Soit $k \leqslant q$ et $\mathbb{F}_q[X]_{<k}$ l'espace vectoriel de polynômes à une variable de degré strictement inférieur à k. On définit l'évaluation à l'infini d'un polynôme $f \in \mathbb{F}_q[X]_{<k}$, notée $f(\infty)$, comme l'évaluation en 0 de $X^{k-1} f\left(\frac{1}{X}\right)$.

On considère le code $\mathrm{ERS}_k(\mathbf{x})$ comme l'image de l'application linéaire

$$\mathrm{ev}_k : \left\{ \begin{array}{ccc} \mathbb{F}_q[X]_{<k} & \to & \mathbb{F}_q^{q+1} \\ f & \mapsto & (f(x_1), \ldots, f(x_q), f(\infty)). \end{array} \right.$$

a) Prouver que pour tout $f \in \mathbb{F}_q[X]_{<k}$,l'évaluation à l'infini $f(\infty)$ est égale au coefficient d'ordre $k-1$.

b) Rappeler la borne de Singleton.

c) Donner les paramètres $[n, k, d]$ de ERS_k et prouver que pour tout $k \geqslant 0$ il s'agit d'un code MDS (*Rappel : un code est dit MDS si ses paramètres atteignent la borne de Singleton).*

d) Quel est la dimension du dual du code $\mathrm{ERS}_k(\mathbf{x})$?

e) Prouver que le dual du code $\mathrm{ERS}_k(\mathbf{x})$ est encore un code ERS.