Master CSI 1 2023-2024

Théorie de l'information, 4TCY806U : DSI du 20 février 2024

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

Responsable : Elena Berardini

Durée : 1h30. Sans document. Les exercices sont indépendants. Toutes les réponses doivent être justifiées.

– EXERCICE 1. On tire à pile ou face avec une pièce équilibrée.

a) Quelle est l'information mutuelle entre chacune des deux faces de la pièce ?

b) Supposons que l'on effectue 4 lancers à la suite

(i) On appelle X_{12} le nombre de «face» obtenus au cours des lancers 1 et 2 et X_{23} le nombre de «face» obtenus au cours des lancers 2 et 3. Calculer l'information mutuelle $I(X_{12}, X_{23})$.

(ii) On appelle X_{123} le nombre de «face» obtenus au cours des trois premiers lancers et X_{234} le nombre de «face» obtenus au cours des trois derniers lancers. Calculer $I(X_{123}, X_{234})$.

– EXERCICE 2. 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 3. Soit $X = \sum_{i=1}^{n} X_i$ où les variables X_i sont indépendantes et de même loi de Bernoulli $B(\alpha)$ de paramètre $P(X_i = 1) = \alpha$. En d'autres termes, X suit une loi binomiale de paramètres n et α.

a) Rappeler ce que vaut la divergence de Kullback $D(B(\beta) \parallel B(\alpha))$ où $B(\alpha)$ et $B(\beta)$ sont deux lois de Bernoulli de paramètres α et β respectivement.

b) En supposant que αn et βn sont des entiers, montrer que

$$P(X = \beta n) \leqslant 2^{-nD(B(\beta)\|B(\alpha))}.$$

– Exercice 4. Soit X une variable aléatoire à valeurs dans $\mathcal{X} = \{A, B, C, D\}$ et soit $p = (0.25, 0.125, 0.5, 0.125)$ la loi sur X.

a) Calculer $H(p)$.

b) Soit $q = (0.625, 0.125, 0.125, 0.125)$ une autre loi sur X. Calculer $H(q)$ et $D(p \parallel q)$.

c) Soit $c : \mathcal{X} \to C$ l'encodage de X suivant :

$$c(A) = 000, c(B) = 001, c(C) = 01, c(D) = 1.$$

Donner les définitions de codage *sans perte* et *uniquement décodable*, puis déterminer si le code C est sans perte et/ou uniquement décodable.

d) Calculer la distribution des longeurs du code C. Est-ce que C vérifie l'inégalité de Kraft ?

e) Calculer la longueur moyenne du code pour la loi p et pour la loi q. Enoncer le premier théorème de Shannon. Est-ce que le code C est optimal pour la loi p ? Et pour la loi q ?

– Exercice 5. Un joueur A jette deux dés équilibrés. On note X la somme des deux faces.

a) Décrire l'image $\mathcal{X}$ de la variable aléatoire X et sa loi.

b) Construire un arbre binaire de Huffman pour X.

c) Un joueur B doit découvrir la valeur de X en posant à A des questions dont la réponse est «oui» ou «non». Une procédure est dite optimale si elle permet au joueur B de poser une suite de questions successives dont les réponses déterminent X, et telle que le nombre moyen de questions est minimum.

(i) Quel est le nombre moyen de questions pour une procédure optimale ?

(ii) Quelle est la première question de la procédure optimale ?