

Théorie de l'information : DS du 22 octobre 2013

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

Responsable : Gilles Zémor

Durée : 1h30. Sans document. Les exercices sont indépendants.

– EXERCICE 1. Soient X et Y deux variables indépendantes, toutes deux de loi uniforme dans $\mathcal{X} = \{0, 1, 2, 3\}$. Soit Z la variable de Bernoulli qui vaut 0 si $X > Y$ et 1 sinon.

- a) Calculer $H(Z|X)$, $H(Z|Y)$ et $H(Z)$.
- b) En déduire $H(X|Z)$ et $H(Y|Z)$.

– EXERCICE 2. Démontrer que quelles que soient les variables X, Y, Z on a :

$$H(X, Y) + H(Y, Z) \geq H(X, Y, Z) + H(Y).$$

On pourra utiliser la relation $H(X|Y) \geq H(X|(Y, Z))$.

– EXERCICE 3. Soit $\pi = (p_1, \dots, p_m)$ une loi de probabilité. Soit π' la loi obtenue à partir de π en sélectionnant deux coordonnées i et j dans $\{1, 2, \dots, m\}$ et en remplaçant les probabilités p_i et p_j par $(p_i + p_j)/2$ et $(p_i + p_j)/2$.

Montrer que $H(\pi) \leq H(\pi')$. On pourra introduire des variables X et X' à valeurs dans $\{1, 2, \dots, m\}$ et de lois π et π' , ainsi qu'une variable Y qui vaut 1 si $X, X' \in \{i, j\}$ et 0 sinon, et s'intéresser à $H(X|Y)$ et $H(X'|Y)$.

– EXERCICE 4. Soit une variable aléatoire X prenant les valeurs a, b, c, d, e, f, g de loi de probabilité $(P(X = a), P(X = b), \dots, P(X = g))$ égale à :

$$\pi = (0.35, 0.3, 0.2, 0.05, 0.05, 0.03, 0.02).$$

- a) Trouver un code de Huffman binaire pour X .
- b) Trouver la longueur moyenne $\bar{\ell}$ pour ce code et cette loi de probabilité.
- c) Quelles sont toutes les distributions des longueurs

$$\ell_1 \geq \ell_2 \geq \ell_3 \geq \ell_4 \geq \ell_5 \geq \ell_6 \geq \ell_7$$

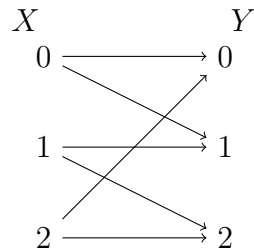
possibles pour tous les codes de Huffman associés à la loi π ?

– EXERCICE 5. On considère les trois codes suivants :

$$C_1 = \{00, 10, 001, 101, 011, 111\}, C_2 = \{00, 10, 01, 101, 110, 011\}, C_3 = \{01, 10, 01110\}.$$

Lesquels sont uniquement déchiffrables ? Pourquoi ?

– EXERCICE 6. On considère le canal discret sans mémoire :



où les probabilités de transition sont données par :

$$P(Y = 0|X = 0) = P(Y = 1|X = 1) = P(Y = 2|X = 2) = 1 - p$$

$$P(Y = 1|X = 0) = P(Y = 2|X = 1) = P(Y = 0|X = 2) = p.$$

Calculer la capacité de ce canal en fonction du paramètre p .