Université de Caen Normandie, UFR des Sciences
Licence 3

Module “Sécurité Informatique et Protection de données”
TD - codage de canal ; durée : 2h30

Exercice 1 : Canal binaire symétrique

Soit X une source sans mémoire sur l'alphabet binaire $\{0, 1\}$ donnée par la distribution :

$$\mathbb{P}[X = 0] = \frac{1}{8}, \qquad \mathbb{P}[X = 1] = \frac{7}{8}.$$

Considérons le canal symétrique binaire $\mathcal{C}$ de paramètre $p = \frac{1}{16}$.

1. Si X est la source en entrée du canal $\mathcal{C}$, et Y la source en sortie du canal, donnez la loi conjointe de (X, Y).
2. En déduire la loi de Y. Est-ce la même que celle de X ?
3. Quelle est l'entropie de X et de Y ? Quelle est l'entropie conjointe de (X, Y) ?
4. En déduire l'information mutuelle $I(X, Y)$ et les entropies conditionnelles $H(X|Y)$ et $H(Y|X)$.
5. Donnez la capacité du canal $\mathcal{C}$.

Exercice 2 : Canal

Soit X une source sans mémoire sur l'alphabet ternaire $\{0, 1, 2\}$ donnée par la distribution :

$$\mathbb{P}[X = 0] = \frac{1}{8}, \qquad \mathbb{P}[X = 1] = \frac{3}{8}, \qquad \mathbb{P}[X = 2] = \frac{4}{8}.$$

Considérons le canal ternaire $\mathcal{C}$ dont la matrice de transition est donnée par

$$\mathcal{M} = \begin{pmatrix} 3/4 & 1/8 & 1/8 \\ 1/8 & 3/4 & 1/8 \\ 1/8 & 1/8 & 3/4 \end{pmatrix}.$$

1. Si X est la source en entrée du canal $\mathcal{C}$, et Y la source en sortie du canal, donnez la loi conjointe de (X, Y).
2. En déduire la loi de Y. Est-ce la même que celle de X ?
3. Quelle est l'entropie de X et de Y ? Quelle est l'entropie conjointe de (X, Y) ?
4. En déduire l'information mutuelle $I(X, Y)$ et les entropies conditionnelles $H(X|Y)$ et $H(Y|X)$.
5. Soit X' une source sans mémoire sur l'alphabet $\{0, 1, 2\}$. Montrez que l'information mutuelle $I(X', Y')$ avec Y' la source à la sortie du canal vérifie

$$I(X', Y') = H(Y') - H(\mathcal{M}) \quad \text{avec} \quad H(\mathcal{M}) = -\frac{3}{4}\log_2\frac{3}{4} - 2 \times \frac{1}{8}\log_2\frac{1}{8}.$$

6. Donnez la capacité du canal $\mathcal{C}$.

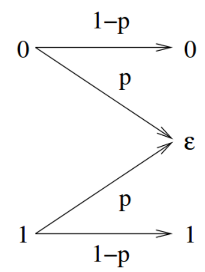
Exercice 3 : Canal symétrique binaire

Considérons le canal symétrique binaire $\mathcal{C}_1(p)$ de paramètre p sur l'alphabet binaire $\{0,1\}$. Pour tout entier positif k, on peut définir un canal $\mathcal{C}_k$ de la manière suivante : le canal agit sur $\{0,1\}^k$ et pour un mot $w = w_1 w_2 \dots w_k \in \{0,1\}^k$, le canal change le symbole w_i avec la probabilité p, indépendamment des autres i, et ceci pour tout $i = 1..k$.

1. Pour $i = 1..k$, quelle est la probabilité que le canal $\mathcal{C}_k$ produise i erreurs ?
2. Quelle est la capacité de $\mathcal{C}_k$?

Exercice 4 : exam 2018 (5pts)

Considérons le canal binaire à effacement $\mathcal{C}$ suivant, de paramètre $p \in [0,1]$:



1. Donnez la matrice de transition du canal $\mathcal{C}$. (0,5pt)

Soit X une source sans mémoire sur l'alphabet $\{0,1\}$ telle que

$$\text{Prob}\,(X = 1) = 1 - \text{Prob}\,(X = 0) = a.$$

Soit Y la source résultant du passage de la source X à travers le canal $\mathcal{C}$.

2. Calculez en fonction de a et p, les entropies $H(X)$, $H(Y)$, $H(X,Y)$ et l'information mutuelle $I(X,Y)$.
   Pour simplifier les formules, nous posons $h(t) = -t\log_2 t - (1-t)\log_2(1-t)$. (3pts)
3. En déduire la capacité du canal $\mathcal{C}$. (1,5pt)

Exercice 5 : Code de Hamming (7,4)

L'alphabet d'entrée du code de Hamming(7,4) est $\{0,1\}^4$ et l'alphabet de sortie est $\{0,1\}^7$. Si les quatre bits d'entrée sont donnés par $m = (m_1, m_2, m_3, m_4)$, alors les sept bits en sortie $y = (y_1, y_2, \dots, y_7)$ sont définis par :

$$y_7 = m_4, \quad y_6 = m_3, \quad y_5 = m_2, \quad y_3 = m_1$$

$$y_1 = y_3 + y_5 + y_7 \mod 2, \quad y_2 = y_3 + y_6 + y_7 \mod 2, \quad y_4 = y_5 + y_6 + y_7 \mod 2.$$

Rappelons que les sommes de contrôle précédentes permettent de corriger jusqu'à une erreur. La première (resp. deuxième/troisième) somme de contrôle indique une erreur potentielle à une position d'indice paire (resp. dont le deuxième/troisième bit est à 1) si la somme de contrôle n'est pas vérifiée.

1. Quel est le code associé aux mots suivants :

$$0000, \quad 0001, \quad 0010, \quad 0100, \quad 1000, \quad 1001, \quad 0110$$

2. Y a-t'il une erreur dans les mots de code suivants ? Si oui, corriger la.

$$y = (1, 0, 1, 0, 1, 1, 0), \qquad y = (1, 1, 1, 0, 1, 1, 1), \qquad y = (0, 0, 1, 0, 0, 1, 0).$$

3. La matrice génératrice d'un code linéaire (ce qu'est le code de Hamming) est une matrice G telle que si $m = (m_1, m_2, m_3, m_4)$ est encodée en $y = (y_1, \ldots, y_7)$, alors $G \cdot {}^t m = {}^t y$. Trouvez une expression de G.
4. La matrice de contrôle est une matrice H tel que pour tout mot de code $y = (y_1, \ldots, y_7)$ sans erreur, on a $H \cdot {}^t y = {}^t(0, 0, 0)$. Trouvez une expression de H
5. Calculez $H \cdot G$.
6. Le syndrome d'un mot de code y (avec ou sans erreur) est défini par $s = H \cdot {}^t y$. Donnez le syndrome des y de la question 2.

Exercice 6 : Code de Hamming généraux

En s'inspirant du code de Hamming $(7, 4)$, il est possible de construire des codes de Hamming dont :

- l'alphabet de sortie sont les blocs de $2^n - 1$ bits,
- l'alphabet d'entrée sont les blocs de $m = (2^n - 1) - n$ bits,
- dont les sommes de contrôles C_i sont en position 2^i pour $i = 0, 1, 2, \ldots, n - 1$.

Questions :

1. Construisez le code de Hamming $(15, 11)$ (qui correspond à $n = 4$).
2. Considérons le message codé $y = (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$. Décodez ce message.
3. Quelle est l'efficacité des codes de Hamming $(7, 4)$, $(15, 11)$ et $(31, 26)$? Que se passe-t'il lorsque n tend vers l'infini ?