Université Paris 8 Année 2022–2023

M1 Mathématiques et applications, parcours ACC

Théorie de l'information – Solutions feuille de TD 5

19/10/2022

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/theorie-information.html`

($\star$) exercice fondamental ($\star\star$) pour s'entraîner ($\star\star\star$) pour aller plus loin sur machine

Solutions de l'Exercice ??.

Scripts à retrouver sur la page web du cours.

Exercice 1. ($\star$) Concaténation de 2 canaux binaires symétriques.

Considérons deux canaux binaires symétriques C_1 et C_2 de paramètres respectifs λ_1 et λ_2. L'entrée de C_1 est notée X, et on suppose que la sortie Y de C_1 est reliée à l'entrée de C_2. Enfin, on note Z la sortie de C_2. On note C le canal issu de la concaténation de C_1 et C_2.

Question 1.– Décrire la loi conditionnelle $Z \mid X$, ou de manière équivalente, calculer la matrice de transition de C.

Question 2.– Le canal C est-il équivalent à un canal binaire symétrique ?

Solutions de l'Exercice 1.

Solution Q1. On calcule :

$$\begin{aligned} p(Z=0 \mid X=0) &= p(Z=0 \mid Y=0)p(Y=0 \mid X=0) + p(Z=0 \mid Y=1)p(Y=1 \mid X=0) \\ &= (1-\lambda_2)(1-\lambda_1) + \lambda_2\lambda_1 \\ &= 1-(\lambda_1+\lambda_2-2\lambda_1\lambda_2). \end{aligned}$$

De la même manière, on observe que

$$\begin{aligned} p(Z=0 \mid X=1) &= \lambda_2(1-\lambda_1)+\lambda_1(1-\lambda_2) = \lambda_1+\lambda_2-2\lambda_1\lambda_2, \\ p(Z=1 \mid X=0) &= \lambda_1(1-\lambda_2)+\lambda_2(1-\lambda_1) = \lambda_1+\lambda_2-2\lambda_1\lambda_2, \\ p(Z=1 \mid X=1) &= 1-(\lambda_1+\lambda_2-2\lambda_1\lambda_2). \end{aligned}$$

Notons que ces valeurs auraient pu être obtenues en réalisant le produit des matrices de transition :

$$\begin{pmatrix} 1-\lambda_2 & \lambda_2 \\ \lambda_2 & 1-\lambda_2 \end{pmatrix} \begin{pmatrix} 1-\lambda_1 & \lambda_1 \\ \lambda_1 & 1-\lambda_1 \end{pmatrix} = \begin{pmatrix} 1-(\lambda_1+\lambda_2-2\lambda_1\lambda_2) & \lambda_1+\lambda_2-2\lambda_1\lambda_2 \\ \lambda_1+\lambda_2-2\lambda_1\lambda_2 & 1-(\lambda_1+\lambda_2-2\lambda_1\lambda_2) \end{pmatrix}.$$

Solution Q2. Oui, le canal C est binaire et symétrique, de paramètre $\lambda := \lambda_1+\lambda_2-2\lambda_1\lambda_2$.

Exercice 2. ($\star\star$) Capacité du canal à effacement.

Le but de cet exercice est de calculer la capacité du canal à effacement d'entrée binaire $\mathcal{X} = \{0,1\}$ et de paramètre λ. On rappelle que ce canal est donné par la matrice de transition

$$\begin{pmatrix} 1-\lambda & 0 \\ \lambda & \lambda \\ 0 & 1-\lambda \end{pmatrix}.$$

On note X l'entrée du canal et Y sa sortie. On désigne par $\perp$ le symbole d'effacement.

Question 1.– Exprimer $H(Y\,|\,X)$ en fonction de λ.

Question 2.– L'entrée du canal est une variable aléatoire X binaire, dont on note la probabilité $p_X(0) = \alpha$. Démontrer que

$$H(Y) = (1-\lambda)h(\alpha) + h(\lambda)\,.$$

Question 3.– En déduire que la capacité du canal à effacement est $1-\lambda$.

Solutions de l'Exercice 2.

Solution Q1. On utilise la formule générique :

$$H(Y\,|\,X) = \sum_x p(x) \underbrace{\sum_y p(y\,|\,x) \log_2 \frac{1}{p(y\,|\,x)}}_{H(Y|X=x)}$$

Calculons d'abord $H(Y\,|\,X=0)$.

$$\begin{aligned} H(Y\,|\,X=0) &= -p_{Y|X}(0\,|\,0)\log_2 p_{Y|X}(0\,|\,0) - p_{Y|X}(\perp|\,0)\log_2 p_{Y|X}(\perp|\,0) - p_{Y|X}(1\,|\,0)\log_2 p_{Y|X}(1\,|\,0) \\ &= (1-\lambda)\log_2 \frac{1}{1-\lambda} + \lambda \log_2 \frac{1}{\lambda} + 0 = h(\lambda)\,. \end{aligned}$$

De même $H(Y\,|\,X=1) = h(\lambda)$. Par conséquent,

$$H(Y\,|\,X) = \sum_x p(x)\cdot h(\lambda) = 1\cdot h(\lambda) = h(\lambda)\,.$$

Solution Q2. Il faut calculer $p(Y=0)$, $p(Y=\perp)$ et $p(Y=1)$:

$$\begin{aligned} p(Y=0) &= \sum_x p(X=x)p(Y=0\,|\,X=x) = \alpha(1-\lambda) \\ p(Y=\perp) &= \lambda\alpha + \lambda(1-\alpha) = \lambda \\ p(Y=1) &= (1-\lambda)(1-\alpha) \end{aligned}$$

Puis :

$$\begin{aligned} H(Y) &= \left(\alpha(1-\lambda)\log_2 \frac{1}{\alpha(1-\lambda)}\right) + \left(\lambda \log_2 \frac{1}{\lambda}\right) + \left((1-\alpha)(1-\lambda)\log_2 \frac{1}{(1-\alpha)(1-\lambda)}\right) \\ &= \left(\lambda \log_2 \frac{1}{\lambda}\right) + \left((\alpha + (1-\alpha))(1-\lambda)\log_2 \frac{1}{(1-\lambda)}\right) \\ &\qquad + \left(\alpha(1-\lambda)\log_2 \frac{1}{\alpha} + (1-\alpha)(1-\lambda)\log_2 \frac{1}{1-\alpha}\right) \\ &= h(\lambda) + (1-\lambda)h(\alpha) \end{aligned}$$

Solution Q3. On doit maximiser $I(X\,;Y) = H(Y) - H(Y\,|\,X)$ en fonction de α. On a :

$$I(X\,;Y) = h(\lambda) + (1-\lambda)h(\alpha) - h(\lambda) = (1-\lambda)h(\alpha)\,.$$

On sait que la fonction $\alpha \mapsto h(\alpha)$ est maximale pour $\alpha = 1/2$, et vaut 1 dans ce cas. Donc la capacité du canal binaire à effacement est :

$$1-\lambda\,.$$

Remarquons que cette capacité est atteinte si et seulement si la source X est uniforme.

Exercice 3. ($\star\star$) Canal q-aire symétrique.

Dans certains modèles de communication, notamment pour la cryptographie, il est commode de considérer comme alphabet des corps ayant un nombre fini $q \neq 2$ d'élements. On considère donc un canal dont les entrées et sorties sont à valeurs dans $\mathcal{X} = \{x_1, \dots, x_q\}$, et qui admet comme une matrice de transition

$$\Pi = \begin{pmatrix} 1-\lambda & \frac{\lambda}{q-1} & \cdots & \cdots & \frac{\lambda}{q-1} \\ \frac{\lambda}{q-1} & 1-\lambda & \frac{\lambda}{q-1} & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \frac{\lambda}{q-1} \\ \frac{\lambda}{q-1} & \cdots & \cdots & \frac{\lambda}{q-1} & 1-\lambda \end{pmatrix}.$$

Autrement dit, un symbole $x_i \in \mathcal{X}$ est preservé avec probabilité $1-\lambda$. Il est donc modifié avec probabilité λ, et ce de manière équiprobable sur les autres symboles de la sortie.

Question 1.– Calculer la capacité du canal, et commenter.

Solutions de l'Exercice 3.

Solution Q1. Pour tout x_i, on a

$$H(Y \mid X = x_i) = (q-1) \times \frac{\lambda}{q-1} \log_2 \frac{q-1}{\lambda} + (1-\lambda) \log_2 \frac{1}{1-\lambda} = h_2(\lambda) + \lambda \log_2(q-1)\,.$$

Donc $H(Y \mid X) = h_2(\lambda) + \lambda \log_2(q-1)$. On observe que cette valeur est indépendante de X. Il reste donc qu'à maximiser $H(Y)$.

La variable Y est à valeurs dans $\{x_1, \dots, x_q\}$, donc $H(Y) \leq \log_2(q)$. Par ailleurs, si Y est uniforme, on a égalité. Cherchons une source X telle que Y est uniforme. Comme dans le cas du canal binaire symétrique, si X est uniforme alors Y l'est également :

$$\Pi \begin{pmatrix} 1/q \\ \vdots \\ 1/q \end{pmatrix} = \begin{pmatrix} 1/q \\ \vdots \\ 1/q \end{pmatrix}$$

La capacité du canal est donc :

$$\log_2(q) - h_2(\lambda) - \lambda \log_2(q-1)$$

Remarque : on peut exprimer cette capacité comme

$$\log_2(q)\,\big(1 - h_q(\lambda)\big)$$

où

$$h_q(\lambda) := \lambda \log_q(q-1) - \lambda \log_q \lambda - (1-\lambda) \log_q(1-\lambda)$$

est appelée fonction d'entropie q-aire. Cette fonction d'entropie h_q généralise la fonction d'entropie binaire vue en cours.