Université Paris 8 Année 2022–2023

M1 Mathématiques et applications, parcours ACC

Théorie de l'information – Solutions feuille de TD 6

26/10/2022

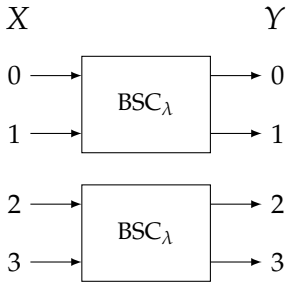
Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`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

Exercice 1. ($\star\star$) Canaux binaires symétriques en parallèle.

On considère deux canaux binaires symétriques de même paramètre λ, placés en parallèle. Le premier prend en entrée les valeurs $\{0,1\}$, le second $\{2,3\}$, comme sur la figure ci-contre. Cela permet de définir un canal avec une entrée de taille 4, que l'on appelle C. On nomme également X l'entrée du canal et Y sa sortie.



Question 1.– Donner la matrice de transition du canal C.

Question 2.– Calculer $H(Y \mid X = x)$ pour tout $x \in \{0,1,2,3\}$, puis en déduire $H(Y \mid X)$.

Question 3.– Démontrer que la capacité du canal C est $2 - h_2(\lambda)$ où h_2 est la fonction d'entropie binaire.

Question 4.– Commenter la capacité pour $\lambda = 1$.

Question 5.– Pour $\lambda = 1/2$, la capacité d'un BSC$_\lambda$ est nulle car le bruit est maximal. Pourquoi la capacité n'est-elle pas nulle dans le cas du canal C ?

Solutions de l'Exercice 1.

Solution Q1. La matrice est

$$\boldsymbol{M} = \begin{pmatrix} 1-\lambda & \lambda & 0 & 0 \\ \lambda & 1-\lambda & 0 & 0 \\ 0 & 0 & 1-\lambda & \lambda \\ 0 & 0 & \lambda & 1-\lambda \end{pmatrix}$$

Solution Q2. Pour $x = 0$, on a

$$\begin{array}{ll} p(Y=0 \mid X=0) = 1-\lambda & p(Y=1 \mid X=0) = \lambda \\ p(Y=2 \mid X=0) = 0 & p(Y=3 \mid X=0) = 0 \end{array}$$

Par conséquent $H(Y \mid X = 0) = -\lambda \log \lambda - (1-\lambda)\log(1-\lambda) = h_2(\lambda)$.

Par le même raisonnement on montre que $H(Y \mid X = 1) = H(Y \mid X = 2) = H(Y \mid X = 3) = h_2(\lambda)$, puis on obtient

$$H(Y \mid X) = h_2(\lambda)\,.$$

Solution Q3. Pour calculer la capacité, on doit maximiser selon X l'information mutuelle $I(X\,;Y) = H(Y) - H(Y \mid X)$. Comme $H(Y \mid X)$ est constant, il suffit de maximiser $H(Y)$. Sa valeur maximale est $\log(4) = 2$, et peut être atteinte si Y est uniforme. Observons maintenant que si X est uniforme, alors Y l'est. Par conséquent, la capacité du canal C vaut $2 - h_2(\lambda)$.

Solution Q4. Pour $\lambda = 1$, le canal opère l'action suivante sur les entrées : il permute 0 et 1 d'une part, et il permute 2 et 3 d'autre part. Ainsi, aucune information n'est perdue lors de la transmission : par exemple s'il l'on reçoit 2 en sortie, c'est nécessairement que 3 a été introduit en entrée du canal.

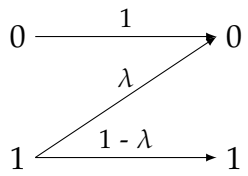
Cela explique la valeur de la capacité, qui est maximale $\mathrm{Cap}(C) = 2 = \log(|\mathcal{X}|)$.

Solution Q5. Pour $\lambda = 1/2$, la capacité du canal est 1, ce qui signifie qu'on peut obtenir juqu'à 1 bit d'information sur l'entrée lorsqu'on observe la sortie du canal. Quel est ce bit d'information ?

C'est simplement l'information du sous-ensembles $\{0,1\}$ ou $\{2,3\}$ auquel appartient l'entrée. Par exemple, si on a reçu 2 en sortie, on peut en déduire que c'est ou bien 2, ou bien 3 qui a été donné en entrée du canal, et que ce ne peut être ni 0, ni 1.

Exercice 2. ($\star\star$) Canal Z.

Dans cet exercice, on se propose de calculer la capacité d'un canal de transmission appelé « canal Z ». Ce canal est binaire (l'entrée et la sortie ont taille 2), et peut être défini par le diagramme suivant, lui donnant son nom.



On note X et Y les variables aléatoires, toutes deux définies sur $\{0,1\}$, associées à la sortie et à l'entrée du canal. On note $\alpha := p(X = 0)$. On rappelle que

$$h(t) := t \log_2 \frac{1}{t} + (1-t) \log_2 \frac{1}{1-t}$$

est la fonction d'entropie binaire.

Question 1.– Donner la matrice de transition $\boldsymbol{M}$ du canal.

Question 2.– Calculer $H(Y \,|\, X = 0)$. Interpréter.

Question 3.– Montrer que $H(Y \,|\, X) = (1-\alpha)h(\lambda)$.

Question 4.– Calculer $H(Y)$ puis $I(X\,;Y)$.

Pour $\lambda \in]0,1[$ fixé, on pose $f_\lambda(x) := h((1-\lambda)(1-x)) - (1-x)h(\lambda)$ et on note

$$\mu(\lambda) := 1 - \frac{1}{(1-\lambda)(1+2^{h(\lambda)/(1-\lambda)})}\,.$$

Question 5.– Démontrer que le minimum de f_λ sur $[0,1]$ est atteint en $x = \mu(\lambda)$.

Question 6.– En déduire que la capacité du canal Z est

$$\log_2\left(1 + \frac{1}{2^{h(\lambda)/(1-\lambda)}}\right)\,.$$

Question 7.– Que vaut cette capacité pour $\lambda \to 0$? Interpréter.

Solutions de l'Exercice 2.

Solution Q1. On a $\boldsymbol{M} = \begin{pmatrix} 1 & \lambda \\ 0 & 1-\lambda \end{pmatrix}$.

Solution Q2. On obtient $H(Y \mid X = 0) = 0$. L'interprétation est la suivante : lorsque $X = 0$, nécessairement $Y = 0$ donc il n'y a aucun aléa dans la sortie.

Solution Q3. Observons que $H(Y \mid X = 1) = h(\lambda)$. Puis, le calcul donne :

$$H(Y \mid X) = p(X = 0)H(Y \mid X = 0) + p(X = 1)H(Y \mid X = 1) = 0 + (1-\alpha)h(\lambda)\,.$$

Solution Q4. On a $p(Y = 0) = \alpha + \lambda(1-\alpha)$ et $p(Y = 1) = (1-\alpha)(1-\lambda)$. Donc

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

et

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

Solution Q5. On calcule $f'(x) = -(1-\lambda)h'((1-x)(1-\lambda)) + h(\lambda)$, et on vérifie facilement que $h'(t) = \log_2((1-t)/t)$. Donc,

$$f'(x) = h(\lambda) - (1-\lambda)\log_2\left(\frac{1-(1-x)(1-\lambda)}{(1-x)(1-\lambda)}\right)\,.$$

Ainsi, $f'(x) = 0$ si et seulement si $2^{h(\lambda)/(1-\lambda)} = \frac{1-(1-x)(1-\lambda)}{(1-x)(1-\lambda)}$. Ceci équivaut à $x = \mu(\lambda)$.

Solution Q6. Si l'on pose $u = \frac{1}{1+2^{h(\lambda)/(1-\lambda)}}$, alors on a $\frac{1-u}{u} = 2^{h(\lambda)/(1-\lambda)}$. Puis, la capacité est obtenue en évaluant f en $\mu(\lambda)$, ce qui donne :

$$\begin{aligned}
C = f(\mu(\lambda)) &= h(u) - \frac{h(\lambda)}{1-\lambda}u \\
&= u\log\frac{1}{u} - (1-u)\log(1-u) - \frac{h(\lambda)}{1-\lambda}u \\
&= u\log\frac{1-u}{u} - \log(1-u) - \frac{h(\lambda)}{1-\lambda}u \\
&= u\frac{h(\lambda)}{1-\lambda} + \log\left(\frac{1}{1-u}\right) + \frac{h(\lambda)}{1-\lambda}u \\
&= \log\left(\frac{1}{1-u}\right) = \log\left(1 + \frac{1}{2^{h(\lambda)/(1-\lambda)}}\right).
\end{aligned}$$

Solution Q7. Pour $\lambda \to 0$, on a $C \to 1$. Interprétation : pas d'erreur, donc on transmet toute l'information.

Exercice 3. ($\star$) Mise en application d'un code convolutif.

On considère le code convolutif défini par les relations :

$$\begin{aligned}
c_m^{(1)} &= x_m + x_{m-2} + x_{m-3}, \\
c_m^{(2)} &= x_m + x_{m-1} + x_{m-3}.
\end{aligned}$$

Question 1.– Donner les représentations

1. algébrique,
2. sous forme de registre à décalage,
3. sous forme d'automate,
4. sous forme de treillis,

de ce code convolutif.

Question 2.– Encoder le mot $\boldsymbol{x} = (0101000\ldots)$.

Question 3.– À l'aide de l'algorithme de Viterbi, décoder la séquence $\boldsymbol{y} = (\boldsymbol{y}^{(1)}, \boldsymbol{y}^{(2)})$ donnée par

$$\begin{aligned} \boldsymbol{y}^{(1)} &= (111100100\dots), \\ \boldsymbol{y}^{(2)} &= (010001000\dots). \end{aligned}$$

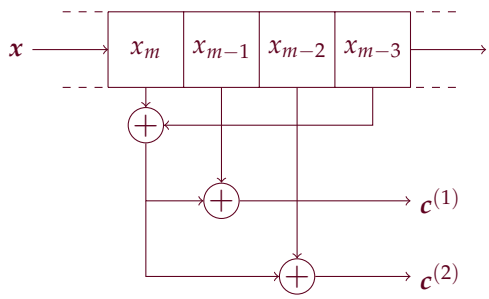
Solutions de l'Exercice 3.

Solution Q1.

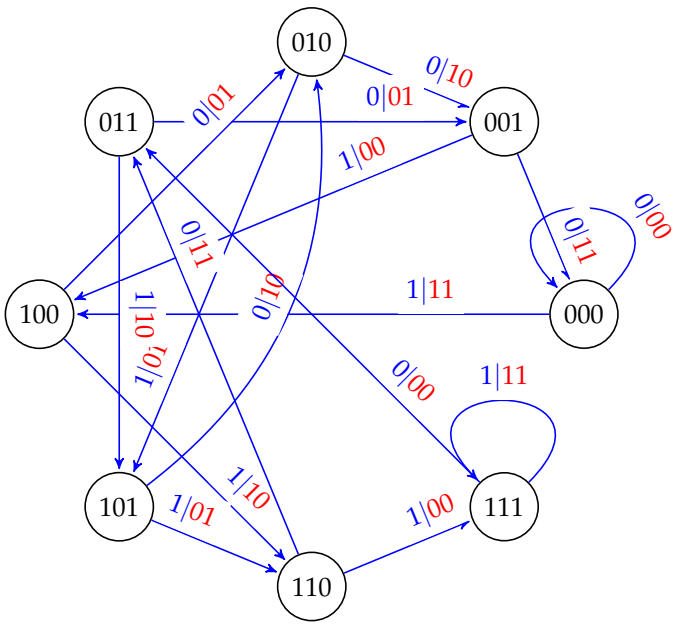
1. **Forme algébrique.** Les polynômes sont :

$$G^{(1)}(Z) = 1 + Z^2 + Z^3 \quad \text{et} \quad G^{(2)}(Z) = 1 + Z + Z^3 .$$

2. **Registre à décalage :**



3. **Automate.** L'automate correspondant est le suivant :



4. **Treillis :** à venir

Solution Q2. Pour encoder $\boldsymbol{x} = (0101000\cdots)$, on peut par exemple utiliser le formalisme algébrique. Le polynôme $X(Z) = Z + Z^3$ représente le message $\boldsymbol{x}$. On a ensuite (dans $\mathbb{F}_2[Z]$) :

$$\begin{aligned} C^{(1)}(Z) &= G^{(1)}(Z)X(Z) = (1 + Z^2 + Z^3)(Z + Z^3) = Z + Z^4 + Z^5 + Z^6 , \\ C^{(2)}(Z) &= G^{(2)}(Z)X(Z) = (1 + Z + Z^3)(Z + Z^3) = Z + Z^2 + Z^3 + Z^6 . \end{aligned}$$

Cela donne les mots de code :

$$\begin{aligned} c^{(1)} &= (01001110\cdots) \\ c^{(2)} &= (01110010\cdots) \end{aligned}$$

Solution Q3. à venir