Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

# Théorie de l'Information – Solutions des exercices de révision

04/12/2023

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

`https://lvzl.fr/teaching/2023-24/ti.html`

(⋆) exercice fondamental (⋆⋆) pour s'entraîner (⋆⋆⋆) pour aller plus loin 💻 sur machine

## Exercice 1. (⋆⋆) Entropie de la somme de deux variables réelles.

Soient $X$ et $Y$ deux variables aléatoires discrètes à valeurs dans $\mathbb{R}$, définies sur un même espace probabilisé. On définit ensuite $Z = X + Y$.

**Question 1.–** Démontrer que $H(Z) \leq H(X) + H(Y)$.

**Question 2.–** Démontrer que $H(Z \mid X) = H(Y \mid X)$.

**Question 3.–** Démontrer que si $X$ et $Y$ sont indépendantes, alors on a

$$H(X) \leq H(Z) \quad \text{et} \quad H(Y) \leq H(Z)\,.$$

**Question 4.–** Trouver un exemple de variables $X$ et $Y$ pour lesquelles on a simultanément

$$H(Z) < H(X) \quad \text{et} \quad H(Z) < H(Y)\,.$$

## Solutions de l'Exercice 1.

**Solution Q1.** On a

$$H(Z) = H(X+Y) \leq H(X,Y) \leq H(X) + H(Y)$$

où la première inégalité est dûe au principe de non-création d'information, utilisé avec la fonction $f : (x,y) \mapsto x+y$ sur la variable conjointe $X, Y$. La seconde inégalité est une propriété vue en cours.

**Solution Q2.** Avec un raisonnement similaire à la question 1, on montre que

$$H(Z|X) \leq H(X,Y|X) \leq H(Y|X) + H(X|X) = H(Y|X)\,.$$

De même,

$$H(Y|X) \leq H(Z-X|X) \leq H(Z|X) + H(X|X) = H(Z|X)\,.$$

**Solution Q3.** Si $X$ et $Y$ dont indépendantes, alors $H(X|Y) = H(X)$ et $H(Y|X) = H(Y)$. D'après la question 2 (où $X$ et $Y$ peuvent jouer des rôles symétriques), on obtient donc

$$H(Z) \geq H(Z|X) = H(Y|X) = H(Y) \quad \text{et} \quad H(Z) \geq H(Z|Y) = H(X|Y) = H(X)\,.$$

**Solution Q4.** On peut prendre par exemple $X = -Y = c$ où $c$ est une constante, de sorte que $Z = c$ et $H(Z) = 0$. Si $H(X) > 0$, on a alors également $H(Y) = H(X) > 0$.

## Exercice 2. (⋆) Codes préfixes et uniquement décodables.

Parmi les codes suivants, lesquels sont préfixes ? Lesquels sont uniquement décodables ?

1. $\{0, 101\}$
2. $\{01, 0001, 0\}$
3. $\{0, 10, 1111, 1101, 10001, 011\}$

## Solutions de l'Exercice 2.

**Solution Q1.**

1. Le code est préfixe, car 0 n'est pas un préfixe de 101, et car 101 n'est pas un préfixe de 0. Il est donc aussi uniquement décodable.
2. Le code n'est pas préfixe, car 0 est un préfixe de 01. Il n'est pas non plus uniquement décodable, car 0001 est à la fois le deuxième mot du code, et la concaténation de deux fois le premier mot et une fois le troisième mot.
3. L'inégalité de Kraft–MacMillan n'est pas satisfaite pour le code. En effet :

$$2^{-1} + 2^{-2} + 2^{-4} + 2^{-4} + 2^{-5} + 2^{-3} = \frac{33}{32} > 1$$

Par conséquent, le code n'est ni préfixe, ni uniquement décodable.

---

## Exercice 3. $(\star)$ Codes de Shannon–Fano et de Huffman.

Soit $X$ une variable aléatoire donnée par la distribution de probabilité $(\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{2}{5})$.

**Question 1.–** Donner un code de Shannon–Fano associé à cette variable aléatoire.

**Question 2.–** Donner un code de Huffman associé à cette variable aléatoire.

## Solutions de l'Exercice 3.

**Solution Q1.** Pour le code de Shannon–Fano, on doit commencer par déterminer les longueurs des mots de codes. Ces longueurs $n$ sont définies par la relation $n = \lceil \log_2(1/p) \rceil$, où $p$ est la probabilité d'occurence du symbole. Ici,

— comme $2^2 = 4 < 5 \leq 8 = 2^3$, on a $\lceil \log_2(1/(1/5)) \rceil = 3$,
— comme $2^1 = 2 < 5/2 \leq 4 = 2^2$, on a $\lceil \log_2(1/(2/5)) \rceil = 2$.

Le code de Shannon–Fano aura donc pour longueurs $(3, 3, 3, 2)$. Un choix possible de mots de codes est alors :

$$(000, 001, 010, 10)$$

**Solution Q2.** On applique l'algorithme de Huffman sur la distribution $p = (\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{2}{5})$. Notons $a$, $b$, $c$ et $d$ les quatre symboles à encoder.

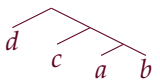
— Première étape : on construit l'arbre associé aux deux probabilités les plus faibles, par exemple les deux premières :


Notons que les autres choix de probabilité plus petites ne modifient pas fondamentalement la forme de l'arbre final.
— Deuxième étape : La distribution passée en argument de l'appel récursif est alors $(\frac{2}{5}, \frac{1}{5}, \frac{2}{5})$. Pour la deuxième étape, nous aurons donc essentiellement deux choix.
  — *Choix* 1 *:* dans la sélection des deux probabilités, on choisit celles associées à « $a$ ou $b$ » et $c$. L'arbre est alors :


  — *Choix* 2 *:* les probabilités choisies sont celles de $c$ et $d$. On obtient alors les deux arbres suivants :

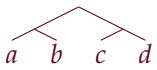


— Troisième étape : Suivant le choix de l'étape précédente, nous obtenons deux arbres différents.
  — *Choix* 1 *:* on obtient l'arbre




  associé, par exemple, aux mots de codes $(110, 111, 0, 10, 110, 111)$.

— *Choix* 2 : on obtient l'arbre

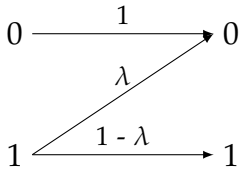



associé, par exemple, aux mots de codes $(00, 01, 10, 11)$.

---

## Exercice 4. $(\star\star)$ 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 $f_\lambda$ 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 4.

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

**Solution Q2.** On obtient $H(Y\,|\,X=0) = 0$. 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 $H(Y\,|\,X=1) = h(\lambda)$. Puis, le calcul donne :

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

**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.

---