

M1 ACC - Théorie de l'information

Contrôle continu – Corrigé

Notation Sur vos copies, chaque question est notée sur 1 point. La note finale (sur 26) est la partie entière supérieure de la somme de la moyenne pondérée de ces notes selon le barème indiqué ci-dessous et d'un bonus de rédaction (de 0, 0.5 ou 1 point).

Exercice 1 (Raisonnement élémentaire). (3 points)

1. (1.5 points) Montrer que $\lim_{n \rightarrow +\infty} \frac{1}{n} = 0$.

Solution Soit $\varepsilon > 0$. Posons $N = \lceil 1/\varepsilon \rceil \geq 1/\varepsilon$. Alors pour tout $n \geq N$,

$$\left| \frac{1}{n} \right| = \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon.$$

□

2. (1.5 points) Montrer que la composée de deux applications injectives est injective.

Solution Soient $f: A \rightarrow B$ et $g: B \rightarrow C$ deux applications injectives. Montrons que l'application $g \circ f: A \rightarrow C$ est injective. Soient $x, y \in A$ tels que $(g \circ f)(x) = (g \circ f)(y)$. Cela signifie que $g(f(x)) = g(f(y))$. Comme g est injective, on en déduit que $f(x) = f(y)$. Enfin, comme f est injective, $x = y$. □

Exercice 2 (Questions de cours). (6 points) Soit $\mathcal{P} = (\Omega, p)$ un espace probabilisé fini. Soient X, Y deux variables aléatoires sur \mathcal{P} à valeurs dans un ensemble fini S . Soit $C: S \rightarrow \{0, 1\}^*$ un code binaire sur S .

1. (1 point) Définir l'entropie du couple $H(X, Y)$, et l'entropie conditionnelle $H(Y|X)$.

Solution

$$\begin{aligned} H(X, Y) &= - \sum_{x \in S} \sum_{y \in S} p_{X, Y}(x, y) \log_2(p_{X, Y}(x, y)) \\ H(Y|X) &= - \sum_{x \in S} \sum_{y \in S} p_{X, Y}(x, y) \log_2(p(X = x|Y = y)). \end{aligned}$$

2. (2 points) Énoncer et démontrer la formule qui lie $H(X, Y)$ et $H(Y|X)$.

Solution Montrons l'égalité :

$$H(X, Y) = H(Y) + H(X|Y).$$

Pour tout $x \in S$,

$$p(X = x|Y = y) = \frac{p_{X, Y}(x, y)}{p_Y(y)}.$$

Par conséquent,

$$\begin{aligned} H(Y|X) &= - \sum_{x \in S} \sum_{y \in S} p_{X, Y}(x, y) [\log_2(p_{X, Y}(x, y)) - \log_2(p_Y(y))] \\ &= - \sum_{y \in S} \sum_{x \in S} p_{X, Y}(x, y) \log_2(p_{X, Y}(x, y)) + \sum_{y \in S} \underbrace{\left(\sum_{x \in S} p_{X, Y}(x, y) \right)}_{=p_Y(y)} \log_2(p_Y(y)) \\ &= H(X, Y) - H(Y). \end{aligned}$$

□

3. (1 point) Définir le codage C^* associé à C .

Solution Le codage C^* est l'application :

$$\begin{aligned} A^* &\longrightarrow \{0, 1\}^* \\ a_0 \cdots a_n &\longmapsto C(a_0) \cdots C(a_n). \end{aligned}$$

4. (1 point) Définir la longueur moyenne de C relativement à X et la comparer à l'entropie de X .

Solution La longueur moyenne de C relativement à X est le réel positif

$$\ell_X(C) = \sum_{x \in S} p_X(x) \ell(C(x)).$$

D'après le premier théorème de Shannon, $\ell_X(C) \geq H(X)$.

5. (1 point) Existe-t-il un code binaire C uniquement décodable sur $\{1, 2, \dots, 10\}$ tel que $\ell(C(i)) = 3$ pour $i = 1, \dots, 6$ et $\ell(C(i)) = 4$ pour $i = 7, \dots, 10$?

Solution Comme

$$6 \cdot \frac{1}{2^3} + 4 \cdot \frac{1}{2^4} = 1$$

la suite $(3, 3, 3, 3, 3, 3, 4, 4, 4, 4)$ est la suite des longueurs d'un code de Shannon-Fano, qui est uniquement décodable.

Exercice 3 (Codes de Huffman et Shannon-Fano). (6 points) Soit X une variable aléatoire à valeurs dans $A = \{a, b, c, d, e\}$ de loi p_X définie par le tableau suivant.

x	a	b	c	d	e
$p_X(x)$	$1/9$	$1/9$	$1/9$	$1/3$	$1/3$

1. (1 point) Calculer l'entropie $H(X)$ de X ; donner le résultat sous la forme $a + b \log_2(3)$ avec $a, b \in \mathbb{Q}$.

Solution

$$\begin{aligned} H(X) &= - \sum_{x \in A} p_X(x) \log_2(p_X(x)) \\ &= -3 \cdot \frac{1}{9} \log_2\left(\frac{1}{9}\right) - 2 \cdot \frac{1}{3} \log_2\left(\frac{1}{3}\right) \\ &= \frac{1}{3} \log_2(9) + \frac{2}{3} \log_2(3) \\ &= \frac{4}{3} \log_2(3). \end{aligned}$$

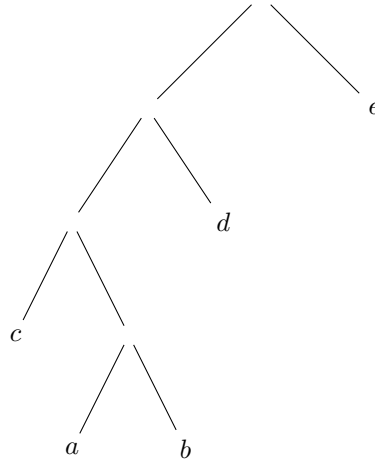
□

2. (1 point) Existe-t-il un code binaire uniquement décodable sur A dont la longueur moyenne relativement à X est $H(X)$?

Solution Comme les $p_X(x), x \in A$ ne sont pas tous des puissances entières de $1/2$, il n'y a pas de code binaire uniquement décodable sur A dont la longueur moyenne relativement à X est $H(X)$. \square

3. (1.5 points) Construire un code de Huffman C associé à X .

Solution L'algorithme vu en cours produit l'arbre de Huffman suivant :



Cela correspond au code:

x	a	b	c	d	e
$C(x)$	0010	0011	001	01	1

\square

4. (1.5 points) Construire un code de Shannon-Fano SF associé à X .

Solution Rappelons que pour tout $x \in A$, la longueur de SF(x) est $\lceil -\log_2(p_X(x)) \rceil$.

x	a	b	c	d	e
$\ell(\text{SF}(x))$	4	4	4	2	2

Les sommes consécutives des $2^{\lceil -\log_2 p_X(x) \rceil}$ dans l'ordre décroissant, et leurs écritures binaires, sont :

$$0, 1/4 = \overline{0.01}, 1/2 = \overline{0.1}, 9/16 = \overline{0.1001}, 10/16 = \overline{0.101}.$$

Le code obtenu, en choisissant l'ordre d, e, a, b, c , est le suivant :

x	a	b	c	d	e
SF(x)	1000	1001	1010	00	01

\square

5. (1 point) Est-ce que SF est optimal ?

Solution La longueur moyenne de SF est

$$\ell_X(SF) = 3 \cdot 4 \cdot \frac{1}{9} + 2 \cdot 2 \cdot \frac{1}{3} = \frac{28}{9}.$$

La longueur moyenne de C est

$$\ell_X(C) = 2 \cdot 4 \cdot \frac{1}{9} + 3 \cdot \frac{1}{9} + 2 \cdot \frac{1}{3} + 1 \cdot \frac{1}{3} = \frac{20}{9}.$$

Par conséquent, $\ell_X(SF) > \ell_X(C)$, et SF n'est pas optimal. \square

Exercice 4 (Codes suffixes). (10 points) Soit A un alphabet. On dit qu'un mot $x \in \{0, 1\}^*$ est un suffixe d'un mot $y \in \{0, 1\}^*$ s'il existe $z \in \{0, 1\}^*$ tel que $y = zx$. On dit qu'un code binaire C sur A est suffixe si pour tous $a \neq b \in A$, le mot $C(a)$ n'est pas un suffixe de $C(b)$.

- (1 point) Dans cette question uniquement, $A = \{a, b, c\}$. Donner un exemple de code préfixe sur A qui n'est pas suffixe, et un exemple d'un code suffixe sur A qui n'est pas préfixe.

Solution Le code $(0, 10, 110)$ est préfixe et pas suffixe. Le code $(0, 01, 011)$ est suffixe et pas préfixe. \square

- (2 points) Montrer qu'un code régulier de longueur fixe sur A est à la fois préfixe et suffixe.

Solution Soit $C: A \rightarrow \{0, 1\}^*$ un tel code. Soient $x, y \in C$. Si $C(x)$ est un préfixe ou un suffixe de $C(y)$, alors comme $\ell(C(x)) = \ell(C(y))$, on a $C(x) = C(y)$, ce qui contredit la régularité du code. Par conséquent, C est à la fois préfixe et suffixe.

- (2 points) Pour tout alphabet B , on définit l'application :

$$w_B: \begin{cases} B^* & \longrightarrow B^* \\ a_0 \cdots a_n & \longmapsto a_n \cdots a_0 \end{cases}$$

Que vaut $w \circ w$? Montrer que pour tous $b_1, \dots, b_m \in B^*$, $w(b_1 \| \cdots \| b_m) = w(b_m) \| \cdots \| w(b_1)$. \square

Solution L'application $w \circ w$ est l'identité. Soient $b_1, \dots, b_m \in B^*$. Pour tout $i \in \{1, \dots, m\}$, écrivons $b_i = b_{i,1} \cdots b_{i,r_i}$, avec $b_{i,j} \in B$ pour tout $j \in \{1, \dots, r_i\}$. Alors

$$\begin{aligned} w(b_1 \| \cdots \| b_m) &= w(b_{1,1} \cdots b_{1,r_1} \cdots b_{m,1} \cdots b_{m,r_m}) \\ &= b_{m,r_m} \cdots b_{m,1} \cdots b_{1,r_1} \cdots b_{1,1} \\ &= w(b_m) \| \cdots \| w(b_1). \end{aligned}$$

\square

- (1.5 points) Soit C un code binaire sur A . Montrer que C est préfixe si et seulement si $w \circ C$ est suffixe.

Solution Supposons C préfixe et montrons que $w \circ C$ est suffixe. Soient $x, y \in A$ et $b \in \{0, 1\}^*$ tels que $w(C(y)) = b \| w(C(x))$. Alors $C(y) = C(x) \| w(b)$. Comme C est préfixe, on en déduit que $x = y$. Réciproquement, supposons $w \circ C$ suffixe et montrons que C est préfixe. Soient $x, y \in A$ et $b \in \{0, 1\}^*$ tels que $C(y) = C(x) \| b$. Alors $w(C(y)) = w(b) \| w(C(x))$ et comme $w \circ C$ est suffixe, on en déduit que $x = y$.

- (1 point) Montrer que pour tout code binaire C sur A , $C^* = w_{\{0,1\}} \circ (w_{\{0,1\}} \circ C)^* \circ w_A$. \square

Solution Soit $a = a_1 \cdots a_n \in A^*$. Alors

$$\begin{aligned} w_{\{0,1\}} \circ (w_{\{0,1\}} \circ C)^* \circ w_A(a) &= w_{\{0,1\}} \circ (w_{\{0,1\}} \circ C)^*(a_n \cdots a_0) \\ &= w_{\{0,1\}} (w_{\{0,1\}}(C(a_n)) \cdots w_{\{0,1\}}(C(a_0))) \\ &= C(a_0) \cdots C(a_n) \\ &= C^*(a). \end{aligned}$$

□

6. (1 point) Montrer que tout code suffixe sur A est uniquement décodable.

Solution Le code $w \circ C$ est préfixe, donc uniquement décodable. D'après la question précédente, C^* est donc une composée d'applications injectives : elle est elle-même injective. □

7. (1 point) Soit X une variable aléatoire à valeurs dans A . Existe-t-il un code suffixe optimal pour X ?

Solution Oui : si C désigne un code de Huffman pour X , alors $w \circ C$ est suffixe et de même longueur moyenne que C . Il est donc optimal. □