Master 1 Mathématiques 2024–2025
MYMAA008 – Théorie de l'Information – Examen– 2h00

Les documents ne sont pas autorisés. Tout support numérique est interdit. Toute erreur dans le sujet sera prise en compte dans la correction. Le barème est donné à titre indicatif. La qualité de la rédaction sera prise en compte dans la notation.

Questions de cours (8 points)

1 *(2 points)* Donner le schéma général du cours qui décrit comment on réalise la communication entre deux entités, au travers d'un canal qui peut apporter des erreurs dans la communication. Indiquer comment on modélise les entrées et les sorties, le canal et quels algorithmes et outils on utilise à chaque étape afin de garantir une communication qui limite la quantité d'erreur tout en limitant le coût de la communication.

2 *(1 point)* On considère un espace probabilisé joint XY. Donner la définition de l'information mutuelle entre les événements $x \in \mathcal{X}$ et $y \in \mathcal{Y}$. Donner les valeurs pour l'information mutuelle quand X définit l'entrée d'un canal binaire symétrique et Y sa sortie.

3 *(1,5 points)* Montrer la règle de chainage de l'entropie, c'est à dire que pour toute v.a $X_1, \dots, X_n$, on a

$$H(X_1, \dots, X_n) = H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_1, \dots, X_{n-1}) .$$

4 *(1 point)* Énoncer le premier théorème de Shannon.

5 *(2,5 points)* Rappeler la définition de la capacité d'un canal ainsi que la définition d'un canal fortement symétrique. Montrer ensuite pourquoi la capacité d'un canal fortement symétrique est égale à $\log_2(J) - H(\Pi)$ où J est le cardinal de l'espace de sortie du canal et $H(\Pi)$ est la somme des coefficients pris sur la première ligne de la matrice de transition du canal. Tous les arguments doivent être présent dans la preuve.

Exercice 1 : Le code de Shannon-Fano-Elias (5 points)

Soit $X = (\mathcal{X}, p)$ une source sur l'alphabet $\mathcal{X}$ et de mesure de probabilité p. On munit l'alphabet $\mathcal{X}$ d'une relation d'ordre totale et on note, pour tout $x \in \mathcal{X}$,

$$S(x) = \sum_{x' < x} p(x') \text{ , } \bar{S}(x) = \frac{p(x)}{2} + S(x) \text{ et } \ell(x) = \lceil -\log_2 p(x) \rceil .$$

De plus, pour tout entier i et pour tout réel dans $[0, 1[$, on note $D_i(x)$ les i premiers termes du développement 2-adique de x (son développement en base 2, tronqué).

On considère alors $\phi(x) = D_{\ell(x)+1}(\bar{S}(x))$.

1 *(1 point)* Montrer que pour tout $x, y \in [0, 1[$, si $D_i(x) = D_i(y)$, alors $|x - y| < 2^{-i}$.

2 *(0,5 points)* Pour tout $x, y \in \mathcal{X}$, montrer que si $\ell(x) > \ell(y)$, alors $\phi(x)$ ne peut pas être préfixe de $\phi(y)$.

3 *(1,5 points)* Pour tout $x, y \in \mathcal{X}$, en supposant $\ell(x) \leq \ell(y)$, donner une borne inférieure sur $|\bar{S}(x) - \bar{S}(y)|$. (Indice : considérer séparément les cas $x < y$ et $x > y$)

4 *(1 point)* En déduire que ϕ est un code préfixe.

5 *(1 point)* Montrer que $|\phi| < H(X) + 2$

Exercice 2 : Codes cycliques (7 points)

1 *(0,5 points)* Montrer que dans $\mathbb{F}_5[X]$, $g = (X^2 - 1)^2$ divise $X^{10} - 1$.

2 *(1 point)* On considère maintenant le code cyclique $\mathcal{C}$ de longueur 10 sur $\mathbb{F}_5$ engendré par g. Quelle est la dimension de $\mathcal{C}$? Quel est le cardinal de $\mathcal{C}$?

3 *(1 point)* Donner une matrice génératrice de $\mathcal{C}$.

4 *(1 point)* Donner une matrice de parité de $\mathcal{C}$.

5 *(1,5 points)* En utilisant un résultat vu en cours, montrer que la distance minimale de $\mathcal{C}$ est 3. Combien d'erreurs peuvent-elles être corrigées ?

6 *(2 points)* On reçoit le mot $(1, 1, 1, 1, 3, 1, 1, 1, 1, 1)$. Décoder ce mot. (Indice : syndrome et code de Hamming).