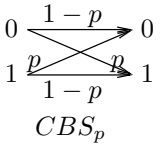
# Devoir Maison 2

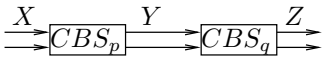
*Les notations qui ne sont pas rappelées sont celles du cours. Vous êtes autorisés à réfléchir à plusieurs sur les exercies (pas plus de deux ou trois). Cependant, la rédaction doit être individuelle et chacun doit rendre une copie. Précisez les noms de vos collaborateurs.*

## Exercice 1 — Canaux en série

On note $CBS_p$ le canal binaire symétrique avec probabilité d'erreur $p$. On note $Y = CBS_p(X)$. On s'intéresse à la capacité d'un canal composé de canaux en série. On suppose le comportement de ces canaux mutuellement indépendants.



$CBS_p$




**1.** Décrire le canal composé de deux canaux $CBS_p$ et $CBS_q$, selon le schéma, c'est-à-dire la relation $(X, Z)$, oú $Y = CBS_p(X)$ et $Z = CBS_q(Y)$. Quelle est sa capacité ?

**2.** Montrer que dans le cas $p = q$, cette capacité est plus petite que la capacité de $CBS_p$. Quels sont les cas d'égalité ?

**3.** On suppose maintenant $n$ canaux $CBS_p$ en série. Quelle est la capacité du canal résultant ? Quelle est la limite de cette capacité quand $n$ tend vers $+\infty$ ?

## Exercice 2 — Canaux en parallèle

On considère $n$ canaux sur des alphabets d'entrée et de sortie deux-à-deux disjoints respectifs $\mathcal{X}_i$ et $\mathcal{Y}_i$ et de capacité respective $C_i$, $i \in \{1, \dots, n\}$. Un encodeur peut utiliser ces canaux pour transmettre un message. À chaque instant, il choisit un canal et transmet par celui-ci. Il ne peut donc utiliser deux canaix simultanément. Cela donne donc un canal avec alphabet d'entrée $\cup_i \mathcal{X}_i$ et alphabet de sortie $\cup_i \mathcal{Y}_i$.

**1.** Montrer que la capacité du canal résultant est

$$C = \log_2 \sum_{i=1}^{n} 2^{C_i}.$$

*Indication :* On exprimera d'abord la caparité comme une expression à maximiser, et on la résoudra par la méthode des lagrangiens

**2.** Que vaut la capacité dans le cas d'un canal binaire symétrique $CBS_p$ et d'un canal qui transmet 2 sans erreur ? dans le cas de deux canaux binaires symétriques $CBS_p$ et $CBS_q$ ?

## Exercice 3 — problème des chapeaux

Il y a 7 prisonniers dans une salle. Chacun a un chapeau bleu ou rouge avec probabilité 1/2 indépendamment des autres. Chaque prisonnier connaît la couleur des chapeaux des autres prisonniers mais aucun prisonnier ne connaît la couleur de son propre chapeau. Le gardien de prison demande aux prisoniers de deviner la couleur de leur chapeau : si un prisonnier se trompe, tous les prisonniers sont tués. Un prisonnier a la possibilité de ne rien dire (au lieu de deviner) mais si aucun prisonnier ne parle, ils sont également tous tués. Aucune communication n'est permise entre les prisonniers sauf pour fixer la stratégie avant de rentrer dans la salle et le gardien de prison interroge chaque prisonnier séparément.

**1.** Donner une stratégie qui maximise la chance de survie des prisonniers.

**2.** Généraliser ce résultat. Pour quelles valeurs du nombre de prisionniers est-ce possible ?

`Exercice 4` `Un exemple de code non linéaire`

**1.** Montrer que parmi les codes de longueur 11 pouvant corriger deux erreurs, le code linéaire le plus grand contient au plus 16 mots code.

Nous allons construire un code plus performant. Une matrice de Hadamard de taille $n$ est une matrice carrée $n \times n$ à coefficients dans $\{-1, 1\}$ et telle que $HH^T = nI$, où $I$ est la matrice identité de taille $n$ : le produit scalaire de deux lignes distinctes de $H$ est nul, et celui d'une ligne avec elle-même est égal à $n$. Comme $H^{-1} = \frac{1}{n}H$, on a aussi $H^T H = nI$ et donc les colonnes de $H$ ont la même propriété

**2.** Etant donné $H$, montrer qu'on peut toujours construire à partir de $H$ une matrice de Hadamard telle que la première colonne ainsi que la première ligne soient constitués de 1 (tout en gardant les propriétés du produit scalaire des lignes et colonnes de la matrice initiale).

On dira qu'une telle matrice de Hadamard est normalisée. Voici des exemples de matrices de Hadamard normalisées (avec la convention $-$ au lieu de $-1$) :

$$H_1 = (1) \qquad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \qquad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}$$

**3.** Montrer que si $H$ est une matrice de Hadamard de taille $n$ alors $n$ est 1, 2 ou un multiple de 4. *Indication :* On pourra d'abord condidérer les 3 premières lignes d'une matrice normalisée

L'existence de matrices de Hadamard pour tout $n$ multiple de 4 est une question ouverte.

Une construction simple repose sur l'observation que si $H_n$ est une matrice de Hadamard de taille $n$ alors

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

est une matrice de Hadamard de taille $2n$. Cette construction permet d'obtenir les matrices données en exemple. On définit un $(n, M, d)$ code un ensemble de $M$ mots-code de longueur $n$ ayant distance minimale $d$.

**4.** Montrer qu'à partir d'une matrice de Hadamard normalisée $H_n$, il est possible de construire des codes binaires ayant les caractéristiques suivantes : $(n-1, n, n/2)$, $(n-1, 2n, n/2-1)$ et $(n, 2n, n/2)$. Conclure quant au problème initial.

`Exercice 5` *`Broadcast channel`*

Soit $\mathcal{X}$ un alphabet d'entrée et 2 canaux ayant tous $\mathcal{X}$ comme alphabet d'entrée et le $i$ème ayant $\mathcal{Y}_i$ comme alphabet de sortie, avec $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \emptyset$.

Ces canaux peuvent être utilisés par une même source, pour envoyer des messages à $k$ destinataires. À chaque instant, le même symbole de l'alphabet d'entrée est envoyé à tous les destinataires.

Un tel canal (*broadcast channel* ou BC) est décrit par une probabilité de transition $p(y_1, y_2 \mid x)$ pour tous $y_i \in \mathcal{Y}_i$, $x \in \mathcal{X}$. On suppose le canal sans mémoire.

Un $((2^{nR_1}, 2^{nR_2}), n)$-code pour un BC à information indépendante consiste en une paire de codes $(\mathcal{C}_1, \mathcal{C}_2)$ avec $|\mathcal{C}_1| = 2^{nR_i}$, muni d'un encodeur $X : \mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{X}^n$ et de deux décodeurs $g_i : \mathcal{Y}_i \to \mathcal{C}_i$.

On utilise le schéma de transmission suivant : on souhaite transmettre à travers le canal 1 et le canal 2, des mots-code, $W_1$ et $W_2$. Ces mots sont encodés en un mot $X$ de longueur $n$ sur l'alphabet $\mathcal{X}$. Les décodeurs $g_i$ décodent alors le message pour chaque canal.

La probabilité d'erreur du code est

$$p_e^{(n)} = \mathbf{P}(g_1(Y_1^n) \neq W_1 \text{ ou } g_2(Y_2^n) \neq W_2),$$

quand $W_1$ et $W_2$ sont choisis indépendemment et uniformément dans respectivement $\mathcal{C}_1$ et $\mathcal{C}_2$.

Une paire de taux $(R_1, R_2)$ est dite atteignable s'il existe une suite de $((2^{nR_1}, 2^{nR_2}), n)$-codes telle que la probabilité d'erreur tend vers 0.

On peut définir les distributions marginales $p(y_1|x)$ et $p(y_2|x)$. On note $C_1$ et $C_2$ les capacités des canaux avec ces marginales. On s'intéresse aux différents taux atteignables.

On note $p_1^{(n)} = \mathbf{P}(g_1(Y_1^n) \neq W_1)$ et $p_2^{(n)} = \mathbf{P}(g_2(Y_2^n) \neq W_2)$

**1.** Montrer que $\max(p_1^{(n)}, p_2^{(n)}) \leq p_e^{(n)} \leq p_1^{(n)} + p_2^{(n)}$

**2.** En déduire que les taux de transmission ne dépendent que des marginales $p(y_1|x)$ et $p(y_2|x)$ (et pas de $p(y_1, y_2 \mid x)$ au-delà de ces marginales).

**3.** Montrer que les taux $(0, R_2)$ et $(R_1, 0)$ sont atteignables si $R_i < C_i$.

**4.** Montrer que si les taux $(R_1, R_2)$ et $(R_1', R_2')$ sont atteignables, alors pour tout $\lambda \in [0, 1]$, $(\lambda R_1 + (1-\lambda)R_1', R_2 + (1-\lambda)R_2')$ l'est aussi,

On définit le canal à information commune Un $((2^{nR_0}, 2^{nR_1}, 2^{nR_2}), n)$-code pour un BC à information commune consiste en un triplet de codes $(\mathcal{X}_0, \mathcal{C}_1, \mathcal{C}_2)$ avec $|\mathcal{C}_i| = 2^{nR_i}$, muni d'un encodeur $X : \mathcal{C}_0 \times \mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{X}^n$ et de deux décodeurs $g_i : \mathcal{Y}_i \to \mathcal{C}_0 \times \mathcal{C}_i$.

Le taux devient alors $(R_0 + R_1, R_0 + R_2)$, et les définitions de taux atteignables, probabilité d'erreurs sont les mêmes que précédemment.

**5.** Montrer qu'il existe un encodage tel que le taux $C_{\min} = \min(C_1, C_2)$ est atteignable pour chaque canal.

On suppose maintenant que chaque canal $i$ est un canal binaire symétrique $CBS(p_i)$, avec $p_1 \leq p_2 < 1/2$.

**6.** Montrer que pour tous $\lambda \in [0, 1]$ pour tous $R_1 < C_i$, $i \in \{1, 2\}$, il existe un encodage tel que le taux $(\lambda R_1, \lambda R_1 + (1-\lambda)R_2)$ est atteignable.