Théorème canal bruyant de Shannon

1. Rappelons la formule pour la capacité d'un canal binaire symétrique, en fonction de

$$H(\varepsilon) = -\varepsilon \log_2(\varepsilon) - (1-\varepsilon)\log_2(1-\varepsilon).$$

Déterminer la capacité pour un canal binaire symétrique avec ε égal à 0,125, 0,250, 0,375, et 0,500.

2. On suppose que les probabilités conditionelles de transmission pour un canal binaire, sans mémoire, ne sont pas symétriques. Par exemple, il est possible qu'un 0 soit plus souvent modifé en 1 (à cause du bruit) que le contraire.

a. Soit donnée la table de probabilités relatives (x en ligne et y en colonne) :

$p(y\|x)$	0	1
0	$1-\varepsilon_1$	ε_1
1	ε_2	$1-\varepsilon_2$

,

trouver les entropies conditionnelles $H(Y|X{=}0)$ et $H(Y|X{=}1)$.

b. Si $p_X(0) = \varepsilon_0$, et donc $p_X(1) = 1-\varepsilon_0$, déterminer $p_Y : Y \to [0,1]$ en termes de ε_0, ε_1, et ε_2, et trouver une expression pour $H(Y)$.
Indication : Laisser l'expression pour $H(Y)$ dans la forme $H(\varepsilon)$.

c. Remplir la table de probabilités joints ci-dessous.

$p(xy)$	0	1
0		
1		

d. Exprimer l'entropie conditionelle $H(Y|X)$ en terms de ε_0, ε_1, et ε_2, et donc trouver une expression pour l'information mutuelle $I(X,Y)$.
Indication : Laisser l'expression pour $H(Y|X)$ en termes de ε_0 et $H(\varepsilon_i)$.

Codes non linéaires

3. Calculer la distance de Hamming entre 1001001 et 1011100.

4. Supposons que les mots de code pour un codage $C : X \to \{0,1\}^6$ sont

$$C(X) = \{000000, 001110, 110001, 111111\},$$

Trouver la distance minimum $d(C)$ de C.

5. On considère le code binaire

$$\mathcal{C} = \{0000101, 0011101, 1111100, 1111111, 0101011\}.$$

On suppose que la probabilité d'erreur de transmission pour chaque symbole est $p = 1/4$. Si $r = 1101001$ et $r' = 0110101$ sont reçus, décoder r et s selon le principe de maximum de vraisemblance.

6. Soit $\mathcal{A}$ un alphabet à q symboles. On pose

$$A_q(n, d) = \sup\{\#\mathcal{C} \,|\, \mathcal{C} \subset \mathcal{A}^n, d(\mathcal{C}) = d\}.$$

Montrer que $A_q(n, 1) = q^n$ et $A_q(n, n) = q$.

Codes linéaires

7. Soit $\mathcal{C}$ le code engendré par la matrice $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$.

a. Déterminer le nombre de mots de code de $\mathcal{C}$.

b. Calculer une matrice de contrôle.

c. Calculer la distance minimum de $\mathcal{C}$.

d. Déterminer le nombre d'erreurs que $\mathcal{C}$ peut détecter/corriger.

8. Soit $\mathcal{C}$ le code de matrice de contrôle $H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$.

a. Donner une matrice génératrice pour $\mathcal{C}$.

b. Décoder par syndrome $r = 11101$ et $r' = 11011$.

Codes de Hamming

On appelle *code de Hamming* de paramètre $r \geq 2$ un code binaire de longueur $2^r - 1$ et dimension $2^r - r - 1$ ayant pour matrice de contrôle une matrice $H(r)$ de r lignes et $2^r - 1$ colonnes dont toutes les colonnes sont distinctes et non nulle. A équivalence près on peut supposer que la i-ème colonne de $H(r)$ représente l'écriture binaire de l'entier i.

9. Construire $H(2)$ et $H(3)$.

10. Donner une matrice génératrice pour ces codes.

11. Montrer que les codes de Hamming sont de distance 3.

12. Montrer que ce sont des codes parfaits, en particulier l'union des boules de centre les mots du code et de rayon $t = 1$ est égale à $\{0, 1\}^{2^r - 1}$.

13. Montrer qu'un code de Hamming est MDS si et seulement si $r = 2$.

14. Ces codes sont très faciles à décoder : montrer qu'on peut choisir pour leader de classe un mot ayant un seul 1 à la place i pour les $2^r - 1$ classes non triviales.