
TP de théorie de l'information

Année 2010-11

Version 1.1

Université de Montpellier
Place Eugène Bataillon
34095 Montpellier Cedex 5

RODOLPHE GIROUDEAU
161, RUE ADA
34392 MONTPELLIER CEDEX 5
TEL : 04-67-41-85-40
MAIL : RGIROU@LIRMM.FR

1 Descriptif des tâches

Les travaux pratiques se déroulent en deux parties :

- La partie théorique est obligatoire
- Concernant la partie pratique vous avez le choix entre les trois exercices

Le document devra être écrit en Latex. Vous présenterez vos résultats pratiques lors d'une soutenance en janvier.

2 Partie théorique

Exercice 1 – Calcul de capacité de canaux symétriques

Nous considérons un canal discret sans mémoire d'entrée X et de sortie Y , où X est une variable aléatoire N -aire (pouvant prendre N valeurs) et où Y est une variable aléatoire M -aire. La distribution de probabilité de X (resp. Y) est donné par le vecteur colonne \bar{p}_X de taille N (resp. le vecteur \bar{p}_Y de taille M). Le canal est donné par sa matrice de transition P de taille $M \times N$, dont les coefficients sont les probabilités de transition $(P)_{y,x} = p(y|x)$. Nous cherchons à déterminer des conditions sur la matrice P pour que la capacité ait une expression simple.

1. Donner une condition sur ces colonnes pour que l'entropie $H(X|Y = x)$ ne dépende que du canal (et non de l'entrée du canal).
2. Donner l'équation donnant \bar{p}_Y en fonction de \bar{p}_X et de P . En déduire une condition simple sur les lignes de P pour que $H(Y)$ soit maximal si $H(X)$ l'est.

Capacité d'un canal fortement symétrique : le canal est dit fortement symétrique si

- les colonnes de P se déduisent les unes des autres par permutation des éléments ;
- les lignes de P sont de sommes égales.

3. Déduire des questions précédentes que la capacité d'un canal symétrique est donné par la formule

$$C = \log_2(M) - h$$

où h est l'entropie commune des colonnes de P .

Généralisation : on cherche maintenant à généraliser la formule de capacité sous les hypothèses suivantes : on partitionne l'alphabet de Y en sous-ensemble disjoints $\mathcal{Y}_1, \mathcal{Y}_2, \dots, \mathcal{Y}_L$ où \mathcal{Y}_k est de taille M_k avec $\sum_{k=1}^L M_k = M$. Cette partition définit une variable d'état K du canal par la relation $K = k \iff Y \in \mathcal{Y}_k$; on note $p(k) = \text{Prob}(K = k) = \text{Prob}(Y \in \mathcal{Y}_k)$. On suppose que pour chaque état k fixé, le sous-canal \mathcal{C}_k d'entrée X et de sortie $Y \in \mathcal{Y}_k$ (décrit

par les probabilités de transition $p(y|x, k)$ est (fortement) symétrique au sens de la définition ci-dessus.

On note P_k le sous-matrice de P dont les lignes correspondent aux valeurs de $y \in \mathcal{Y}_k$. C'est une sous-matrice de taille $M_k \times N$. Noter que P peut s'écrire (après éventuellement une permutation des lignes) sous la forme.

$$P = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_L \end{pmatrix}$$

4. Calculer $p(k|x)$ en fonction des valeurs de $p(y|x)$ et en déduire que K et X sont indépendants. Comment peut-on déterminer $p(k)$ à partir de P_k ? Montrer que $\frac{1}{p(k)}P_k$ est la matrice de transition du sous-canal \mathcal{C}_k .
5. Justifier (sans calcul) que la capacité du sous-canal \mathcal{C}_k est de la forme :

$$C_k = \log_2(M_k) - h_k$$

où on précisera comment h_k se détermine à partir de P_k .

6. Montrer que $I(X, Y)$ est maximisé pour des valeurs d'entrée x équiprobables, son maximum étant la capacité du canal global.

Indication : on pourra raisonner soit sur les entropies $H(Y)$ et $H(Y|X)$ (en montrant que $H(Y|X = x)$ ne dépend pas de x), soit directement sur l'information mutuelle $I(X, Y)$ (en introduisant l'information conditionnelle $I(X, Y|K)$).

Capacité d'un canal faiblement symétrique : le canal est dit faiblement symétrique si on peut trouver une partition de sous-matrices P_k de tailles $M_k \times N$ de la matrice P telle que

- pour tout k
- les colonnes de P_k se déduisent les unes des autres par permutation des éléments ;
- les lignes de P_k sont de sommes égales.

7. En déduire des questions précédentes que la capacité d'un canal faiblement symétrique est donné par l'une des deux formules

$$C = \sum_{k=1}^L p(k)(\log_2(M_k) - h_k) = \left(\sum_{k=1}^L p(k) \log_2 \frac{M_k}{p(k)} \right) - h$$

8. Déterminer si chacun de ces canaux suivants est symétrique (fortement ou faiblement), et dans ce cas, donner leur capacité.

(a) Canal binaire donné par $P = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$

(b) Canal à effacement $P = \begin{pmatrix} 1-\pi & 0 \\ \pi & \pi \\ 0 & 1-\pi \end{pmatrix}$

(c) Canal à effacement et erreur $P = \begin{pmatrix} (1-\pi)(1-p) & (1-\pi)p \\ \pi & \pi \\ (1-\pi)p & (1-\pi)(1-p) \end{pmatrix}$

(d) Canal en Z : $P = \begin{pmatrix} 1 & p \\ 0 & 1-p \end{pmatrix}$

(e) Canal donné par $P = \begin{pmatrix} 1/3 & 1/6 \\ 1/3 & 1/6 \\ 1/6 & 1/3 \\ 1/6 & 1/3 \end{pmatrix}$

(f) Canal donné par $P = \begin{pmatrix} 1/3 & 1/6 \\ 1/3 & 1/3 \\ 1/6 & 1/6 \\ 1/6 & 1/3 \end{pmatrix}$

(g) Canal donné par $P = \begin{pmatrix} 1/3 & 1/6 \\ 1/4 & 0 \\ 1/4 & 1/2 \\ 1/6 & 1/3 \end{pmatrix}$

Exercice 2 – Code de Reed-Muller

Définition 2.1 Nous noterons $RM(r, m)$ le code de Reed-Muller d'ordre r et de longueur 2^m avec $0 \leq r \leq m$. Nous définissons ces codes ainsi :

$$G = \begin{cases} RM(0, m) &= \{00 \dots 0, 11 \dots 1\}, \text{ chaque mot est de longueur } 2^m \\ RM(m, m) &= \{0, 1\}^{2^m} \\ RM(r, m) &= \{(x, x + y) : x \in RM(r, m - 1), y \in RM(r - 1, m - 1)\} \text{ pour } 0 < r < m \end{cases}$$

$RM(m, m)$ comprend tous les mots de longueur 2^m et $RM(0, m)$ est constitué des seuls mots 0 et 1.

- Donner les mots de code $RM(1, 2)$ et $RM(1, 3)$.
- Les matrices génératrices de ces codes amettent également une définition inductive. On note $G(r, m)$ la matrice génératrice de $RM(r, m)$:

$$G(r, m) = \begin{pmatrix} G(r, m - 1) & G(r, m - 1) \\ 0 & G(r - 1, m - 1) \end{pmatrix}$$

En posant pour $r = 0$ $G(0, m) = (11 \dots 1)$, et pour $r = m$ $G(m, m) = \begin{pmatrix} G(m - 1, m) \\ 0 \dots 01 \end{pmatrix}$

Calculer $G(1, 3)$.

- Retrouver les mots de $G(1, 3)$ par sa matrice génératrice.
- Montrer que $G(1, 3)$ est un code équivalent au dual d'un code de Hamming étendu de redondance 3.
- Montrer les propriétés suivantes du code Reed-Muller $RM(r, m)$ défini comme ci-dessus :
 - longueur $n = 2^m$,
 - distance $d = 2^{m-r}$

(c) dimension $k = \sum_{i=0}^r \binom{m}{i}$

(d) $RM(r - 1, m)$ est contenu dans $RM(r, m)$ pour $r > 0$.

(e) comme code dual, $RM(m - 1, r - 1)$ pour $r < m$.

6. Sur le problème de décodage. On ne s'intéresse qu'aux codes de Reed-Muller d'ordre 1, $RM(1, m)$. Pour $G(1, 3)$, décoder les mots :

- 0101 1110
- 0110 0111
- 0001 0100
- 1100 1110

Exercice 3 – Code linéaire

Soit C le code sur linéaire sur \mathbb{F}_5 de matrice génératrice

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$$

- Donner le nombre de mots de C .
- Le code est-il systématique ?
- Déterminer une matrice de contrôle de C .
- Calculer la capacité de correction t de C . Le code est-il MDS¹ ?
- Construire la table de contrôle contenant tous les vecteurs erreurs possibles de poids $\leq t$.
- Décoder quand c'est possible les mots 3001, 1101 et 2311.

Exercice 4 – Code de Hamming de longueur 7

- Dresser la table de décodage du code binaire de Hamming de longueur 7.
- Décoder quand c'est possible les mots 1111111, 1101011, 0110110 et 1111010.

Exercice 5 – Code de Hamming étendu de longueur 8

Nous rajoutons un bit de parité à chaque mot du code binaire de Hamming de longueur 7, de sorte que chaque mot est obtenu soit de poids pair.

- Montrer que le code ainsi obtenu est linéaire.
- En donner une matrice génératrice et une matrice de contrôle.
- Déterminer la distance minimum de C .

3 Partie pratique

Exercice 6 – Compression de données

Le projet consiste à comparer les trois algorithmes suivants

¹Un code linéaire est dit MDS, (Maximum Distance Separable) si $d + k = n + 1$.

- l'algorithme de Huffman,
- l'algorithme LZ77
- l'algorithme LZ78

Vous les testerez sur un jeu de données (textes, ...)

Exercice 7 – Compression des données bis

Vous devez programmer l'algorithme de Huffman statique et adaptatif. Vous procéderez à des tests.

Exercice 8 – Compression des images

Le projet consiste à développer un **CODEC** pour la compression d'images. Le projet est à rendre avant le 15 janvier. Vous serez en groupe de deux. Le minimum demandé est de construire un pour les images en niveaux de gris.

Vous avez le choix de la méthode de compression :

- perte vs sans perte,
- *DCT* ou autre,
- quantificateur de votre choix,
- compresseur binaire (Huffman, LZ, Arithmétique, ...) de votre choix.

Les 8 images benchmarks en niveau de gris sont disponibles à l'adresse suivante :

<http://www.lirmm.fr/~rgirou/enseignement/t di.html>

Ce sont des benchmarks très connus en traitement d'image. Chaque image est un gif de résolution $512 \times 512 \times 8$.

Les 8 images couleurs benchmarks sont disponibles à l'adresse suivante :

<http://www.lirmm.fr/~rgirou/enseignement/t di.html>

A nouveau ce sont des benchmarks très connus en traitement d'image. Les images sont des TIFF avec une profondeur de 24 bits.

En plus des benchmarks ci-dessous, vous pouvez tester votre compresseur sur les images que vous souhaitez.

Un codec avec l'exécutable et le code source

Un rapport d'environ 25 pages maximum, expliquant :

- la méthode de compression/décompression, et
- les résultats obtenus sur les images.

Concernant les résultats, une comparaison avec les compresseurs existants est demandée.