

# Cours de théorie de l'information et du codage

## Matière de l'examen écrit de janvier 2012

*L'examen porte sur l'ensemble de la matière vue au cours oral et dans le cadre des travaux pratiques. Il est organisé en deux parties. La première partie porte spécifiquement sur la matière abordée dans le cadre des travaux pratiques et la seconde partie sur le reste de la matière. Le syllabus du cours constitue la référence à utiliser pour préparer l'examen.*

*Répartition des points:*

- *Correction des travaux pratiques: 30%*
- *Partie 1, examen écrit: 30%*
- *Partie 2, examen écrit: 40%*

### 1 Première partie (2h) à livre ouvert

Les questions seront posées sous la forme d'exercices et de questions choix multiples.

- Modélisation probabiliste d'un problème et application de notions de théorie de l'information à son analyse. Manipulation des grandeurs de la théorie de l'information (entropies, informations mutuelles, simples et conditionnelles).
- Construction d'arbres et de poly-arbres (algorithme de Chow-Liu, propagation des bassins de causalité) à partir d'un oracle sur la loi de probabilité conjointe cible.
- Détection des I-map, D-map, P-map entre différents modèles probabilistes graphiques. Apprentissage à partir d'un échantillon de données i.i.d. générées à partir de celle-ci.
- Propriétés principales des codes de compression de données (codes de source réguliers, déchiffrables, sans préfixes, complets, instantanés). Codage de Huffman, arbres de codes complets et incomplets.

### 2 Seconde partie (2h30) à livre fermé

La seconde partie porte sur les autres parties du cours oral, tel que précisé ci-dessous. Il y aura une question pour chaque chapitre, avec éventuellement une sous-question sous forme de petit exercice ou question à choix multiples. La liste ci-dessous indique l'ensemble de la matière à maîtriser, sous la forme d'exemples de questions qui pourraient être posées.

#### Chapitre 4

1. Définir les notions d'entropie, entropie conditionnelle moyenne, entropie conjointe, information mutuelle. Enoncer et représenter graphiquement les relations entre ces grandeurs et leurs principales propriétés, en indiquant les principales étapes des démonstrations.

2. Énoncer les règles de chaînage pour les entropies conjointes. Définir la notion d'information mutuelle conditionnelle et énoncer la règle de chaînage pour les informations mutuelles. Indiquer les principales étapes des démonstrations.
3. Définir la notion de chaîne de Markov (sur trois variables). Énoncer, démontrer, discuter et illustrer le théorème de non-cr ation d'information. Donner un exemple de cas particulier de trois variables al atoires o  le th or eme ne s'applique pas et o  l'in egalit  n'est pas v rifi e.  noncer les corollaires.

## Chapitre 8

1. D finir la convergence en probabilit , formuler le th or eme AEP. Donner le principe de la d monstration du th or eme AEP, puis la d monstration elle-m me. D finir la notion d'ensemble de messages typiques  $A_\epsilon^{(n)}$ , donner 4 propri t s. Messages repr sentatifs versus typiques : discuter le cas g n ral, et le cas particulier o  plusieurs symboles  mis par la source sont  quiprobables. Expliquer la relation entre messages typiques et compression de donn es.
2. D finir la notion de processus stationnaire. D finir la convergence presque s re et la notion de processus stationnaire et ergodique. Donner les 2 d finitions de l'entropie d'une source discr te stationnaire  $H(S)$  et  $H'(S)$ . L'existence de  $H'(S)$  implique celle de  $H(S)$  : donner le principe de la d monstration, puis la d monstration elle-m me. Montrer pourquoi  $H'(S)$  existe pour toute source stationnaire. Expliquer la relation entre entropie de source et codage de source.
3. D finir la notion de cha ne de Markov et de cha ne de Markov invariante dans le temps. Expliquer comment caract riser par  $(\boldsymbol{\pi}, \boldsymbol{\Pi})$  et repr senter par un graphe orient  une cha ne de Markov invariante dans le temps. D finir  tats communicants,  tats p riodiques,  tats r currents; cha ne de Markov irr ductible, ap riodique, r currente. D finir les notions de r gime permanent et de distribution stationnaire. Donner et  tablir l' quation entre  $\boldsymbol{p}$  et  $\boldsymbol{\Pi}$  si  $\boldsymbol{p}$  est une distribution stationnaire. D finir la notion d'extension de source  $S^k$ . D finir la source de Markov de m moire  $m \geq 0$  finie ; montrer comment celle-ci peut se ramener   une source de Markov (de m moire 1).
4. Exprimer la longueur moyenne des mots n cessaires au codage d chiffable d'une source stationnaire sans m moire ; en donner une borne inf rieure et le principe de d monstration pour  tablir cette borne. Donner une borne sup rieure (sans recourir   l'extension de source) et le principe de d monstration pour  tablir cette borne. D finir la notion d'extension de source.  noncer le premier th or eme de Shannon et donner le principe de la d monstration.

## Chapitre 9

1. D finir les notions de canal discret, canal causal, canal causal sans m moire, canal discret sans m moire stationnaire. Donner la d finition de la capacit  en information par symbole du canal discret causal, sans m moire et stationnaire; expliquer pourquoi la capacit  ne d pend que des propri t s du canal. Pr senter l'exemple du canal sym trique binaire, et calculer sa capacit  en fonction de  $p$ , la probabilit  d'erreur de transmission. D finir la notion de canal sym trique.
2. D finir la notion de code  $(M, n)$  pour un canal  $(\mathcal{X}, P(\mathcal{Y}|\mathcal{X}), \mathcal{Y})$ . Expliquer les r gles de d codage suivantes : la r gle du maximum de probabilit  a posteriori (r gle de Bayes) et son inconv nient en pratique, et la r gle du maximum de vraisemblance. D finir le taux (ou d bit) de communication  $R$  d'un code  $(M, n)$ , la notion de d bit r alisable, la notion de capacit  op rationnelle. Rappeler la d finition de la capacit  en information par symbole.  noncer le second th or eme de Shannon.

3. Expliquer la notion de séquences conjointement typiques. Rappeler les notions de débit réalisable et de capacité en information d'un canal. Expliquer la notion de codes aléatoires. Énoncer le second théorème de Shannon. Présenter les grands principes de la démonstration.

## Chapitre 10

1. Variables aléatoires continues: définir les notions d'entropie différentielle, entropie différentielle conditionnelle moyenne, et information mutuelle entre variables aléatoires continues. Donner les principales propriétés de ces grandeurs, et leurs valeurs pour le cas de variables aléatoires gaussiennes. Montrer que la densité qui maximise l'entropie différentielles sous la contrainte  $E\{\mathcal{X}^2\} \leq P$  est la loi gaussienne de moyenne nulle et de variance égale  $P$ .
2. Canal Gaussien en temps discret: donner la relation entrée-sortie du canal continu gaussien. Donner la condition de limitation de puissance sur les symboles d'entrée dans le cas général et dans le cas de signaux d'entrée ergodiques. Expliquer comment exploiter le canal gaussien limité en puissance en le convertissant en un canal discret (par exemple en canal binaire symétrique); donner avantages et inconvénients de ce mode d'utilisation du canal. Définir la capacité en information du canal gaussien limité en puissance, et en donner la valeur pour une limitation de puissance à  $P$  et une variance du bruit  $N$ .
3. Canal Gaussien en temps continu limité en puissance et en fréquence: donner la relation entrée-sortie du canal continu à bande passante limitée et bruit blanc gaussien. Définir le bruit blanc gaussien en temps continu et à bande limitée (fréquence  $f_0$ ). Dire à quels instants il est nécessaire d'échantillonner le signal pour pouvoir le reconstruire. Donner la capacité de ce canal mesurée en bits par échantillon puis en bits par seconde. Discuter l'effet de la largeur de bande sur la capacité en bits par seconde.

## Chapitre 13 (compression de données réversible)

1. Expliquer le principe du codage arithmétique: code de Shannon-Fano-Elias et principales propriétés, principe du codage (et décodage) arithmétique dans le cas binaire avec source sans mémoire, discuter les extensions au cas où la source utilise un alphabet fin quelconque et lorsqu'elle n'est pas sans mémoire.
2. Expliquer le principe du codage par dictionnaire et en énoncer et expliquer les principales propriétés (code universellement asymptotiquement optimal)
3. Expliquer les principes du codage arithmétique et du codage par méthode de dictionnaire et leurs propriétés principales. Expliquer pourquoi et comment ces deux méthodes peuvent toutes les deux fonctionner sans modèle de source, c'est-à-dire de manière purement adaptative. Expliquer en quoi la propriété d'ergodicité de la source est importante.

## Chapitre 15 (lutte contre le bruit de canal)

1. Expliquer le code de Hamming (7,4), sa règle de décodage (distance minimale vs maximum de vraisemblance, vs maximum de probabilité a posteriori). Démontrer ses principales propriétés (détection et correction d'erreurs, linéarité). Discuter le débit et la probabilité d'erreur de décodage du code de Hamming (Figure 15.1). Définir la notion de code algébrique et donner deux exemples importants.

2. Discuter les trois modes suivants d'utilisation du canal gaussien: full analogique, semi analogique, full numérique. Expliquer comment choisir le codage de canal selon le rapport signal/bruit.
3. Expliquer, sur base d'un exemple la notion de code convolutionnel, de treillis de code, et l'algorithme de Viterbi. Expliquer la notion de décisions souples. Discuter les deux stratégies de décodage (minimisation du taux d'erreur par message, vs par bit source) et dans ce contexte les algorithmes de Viterbi et BCJR. Expliquer le principe général des Turbo-codes.