Réseaux, information et communications (INFO-F303)
Partie Théorie de l'Information
Contenu et Organisation

Christophe Petit

Université libre de Bruxelles

Réseaux, information et communications

Crédit image : www.news.ucsb.edu/

Deux parties

- Réseaux (Guy Leduc)
  - Protocoles réseaux, de la couche physique à la couche internet
- Théorie de l'information (Christophe Petit)
  - Fondements théoriques liés à la quantification, au stockage et à la communication d'information digitale

Théorie de l'information : applications

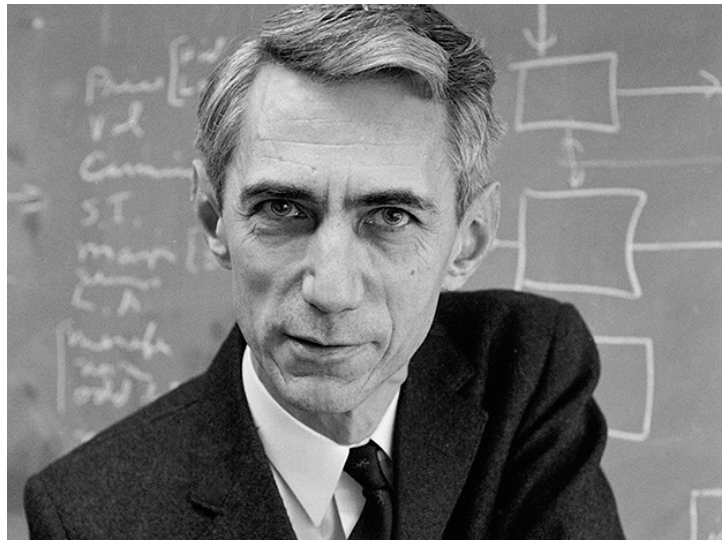
Applications of fundamental topics of information theory include lossless data compression (e.g. ZIP files), lossy data compression (e.g. MP3s and JPEGs), and channel coding (e.g. for DSL). Its impact has been crucial to the success of the Voyager missions to deep space, the invention of the compact disc, the feasibility of mobile phones and the development of the Internet. The theory has also found applications in other areas, including statistical inference, cryptography, neurobiology, perception, linguistics, the evolution and function of molecular codes (bioinformatics), thermal physics, molecular dynamics, quantum computing, black holes, information retrieval, intelligence gathering, plagiarism detection, pattern recognition, anomaly detection and even art creation.

Quote : Wikipedia

Théorie de l'information

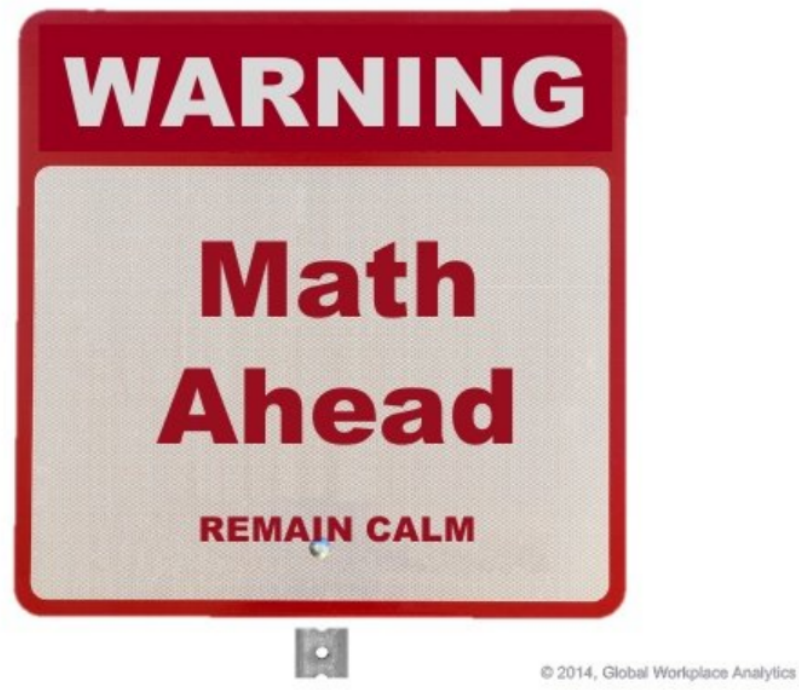
- Qu'est-ce que l'information ?
- Comment quantifier l'information ?
- Comment représenter l'information disponible de façon efficace ?
- Qu'est-ce qu'un canal de communication ?
- Comment transmettre de l'information en présence de bruit ?

Claude Shannon



"A Mathematical Theory of Communication", Bell System Technical Journal, vol. 47, no 3, juillet 1948, p. 379–423.

“Théorie” de la communication



- Concepts intuitifs et problèmes concrets
- Modélisés de façon rigoureuse
- En vue de développer des solutions optimales

Prérequis

- Notions de statistiques
  (probabilités, variables aléatoires, espérance, etc)
- Notions d'algèbre et mathématiques discrètes
  (anneaux de polynômes, corps finis, espaces vectoriels, matrices, etc)
- Notions de structures de données (manipulations d'arbres)
- Notions de programmation et de complexité algorithmique

Plan du cours

1. Notion de code
2. Source aléatoire et codes efficaces
3. Entropie et codage efficace
4. Compression sans perte
5. Canal bruité
6. Codes correcteurs d'erreurs
7. Codes linéaires
8. Quelques familles de codes linéaires

A. Rappels mathématiques (chapitre 7.1 du syllabus)

Chapitre 1 : notion de code

- Terminologie et notations
- Codes univoques
- Codes en bloc
- Codes sans préfixe et arbre de code
- Inégalité de Kraft
- Théorème de McMillan

Chapitre 2 : source aléatoire et codes efficaces

- Hypothèses : alphabet fini, source markovienne
- But : longueur moyenne du code optimale
- Code de Shannon
- Code de Shannon-Fano
- Code de Shannon-Fano-Elias
- Code de Huffman (optimal, utilisé pour ZIP, JPEG, MP3)

Chapitre 3 : entropie et codage efficace

- But : quantifier l'information d'une source (en fonction de la loi de probabilité)
- Entropie : définitions et propriétés
- Inégalité de Gibbs
- Codage asymptotique (source répétée à l'infini)
- Entropie = mesure du codage théorique le plus efficace
- Premier théorème de Shannon : on peut se rapprocher asymptotiquement de l'efficacité maximale

Chapitre 4 : compression sans perte

- But : étant donné un message
  - Estimer la probabilité de distribution des symboles
  - Stocker la même information de façon plus courte
  - Tout en permettant la reconstruction du message initial
  - Le tout de façon efficace (rapide)
- Codage par dictionnaire : algorithmes de Lempel-Ziv et Lempel-Ziv-Welch (transmissions analogiques, formats GIF, TIFF, MOD, PDF, etc)
- Codage de Huffman adaptatif : algorithme de Vitter

Chapitre 5 : canal bruité

- Buts : modéliser un processus de transmission d'information avec erreurs, et quantifier l'information transmise ou perdue
- Canal markovien
- Entropie résiduelle, conditionnelle, croisée ; information mutuelle
- Capacité d'un canal (quantité d'information maximale qu'il peut transporter de l'émetteur au récepteur)
- Canal symétrique

Chapitre 6 : codes correcteurs d'erreurs

- But : introduire de la redondance dans le codage pour compenser les erreurs introduites par le canal bruité
- Code à répétition ; code par somme de contrôle
- Fiabilité ; capacités de détection et correction d'erreurs
- Décodage par maximum de vraisemblance
- Débit d'un code (information minimale par symbole)
- Second théorème de Shannon : pour tout canal, il existe une famille de codes avec (asymptotiquement) un taux d'erreur nul et un débit égal à la capacité du canal
- Inverse du théorème de Shannon (borne de Fano) : information transmise limitée par la capacité du canal

Chapitre 6 : codes correcteurs d'erreurs (suite)

- Distance minimale d'un code ; liens avec les capacités de détection et correction d'erreurs
- Borne de Singleton
- Rayons d'empilement et de recouvrement
- Borne de Hamming et codes parfaits
  (i.e. codes atteignant cette borne)
- Borne de Gilbert-Varshamov

Chapitre 7 : codes linéaires

- But : familles de codes avec de bonnes propriétés (et une représentation compacte)
- Rappels mathématiques : anneau, corps fini, espace vectoriel
- Codes linéaires : définition et propriétés
- Spécialisation des bornes de Hamming et Singleton
- Matrice génératrice, syndrome et matrice de contrôle
- Forme canonique et matrice de parité
- Décodage par syndrome

Chapitre 8 : quelques familles de codes linéaires

- But : construire des familles de codes correcteurs d'erreurs ayant toutes les propriétés requises
- Codes polynomiaux, codes cycliques et codes BCH
- Codes linéaires parfaits, codes de Hamming et codes de Golay
- Codes de Reed-Muller
- Codes MDS
- Codes de Goppa

Sujets non couverts (a priori)

- Codes LDPC et MDPC (low and medium density parity check codes) et algorithmes de décodage itératif
- Turbo codes
- Codes géométriques (généralisation des codes de Goppa)
- Décodage par listes (algorithme de Sudan)
- Connections avec la cryptographie (cryptosystèmes de McEliece et variantes, utilisation dans des algorithmes à base de réseaux euclidiens, ...)

Références

- Transparents du cours
- Syllabus INFO-F303 par Yves Roggeman
- Guide d'étude
- Examens de l'an dernier
- Livres de références supplémentaires
- Internet (mais attention !)

Syllabus

- INFO-F303 par Yves Roggeman
- Référence principale
- Soucis du détail, très complet
- Inclut des rappels mathématiques

Transparents du cours

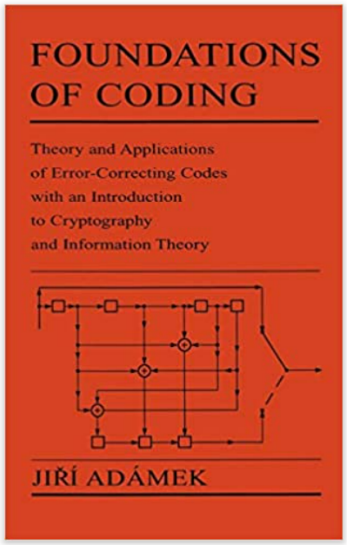
- Autre référence principale
- Reprend l'essentiel du syllabus
- Petits ajouts et restructuration

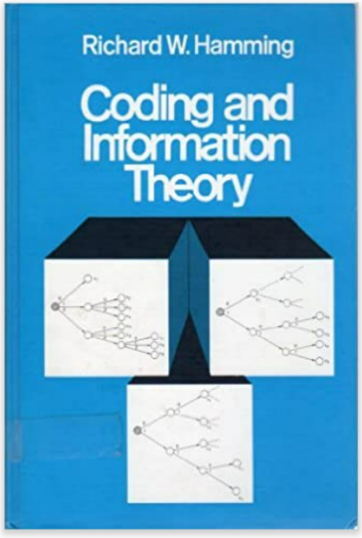
Guide d'étude

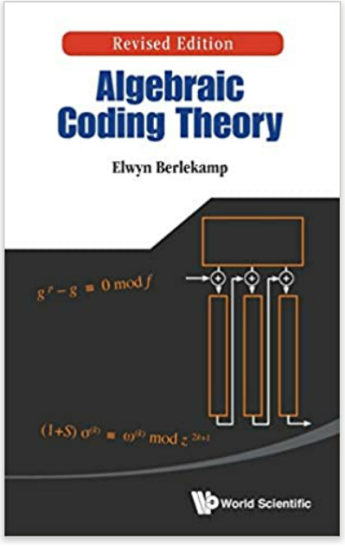
- Questions critiques sur la matière du cours, pour vous guider dans l'acquisition des concepts et intuitions
- Exercices d'application

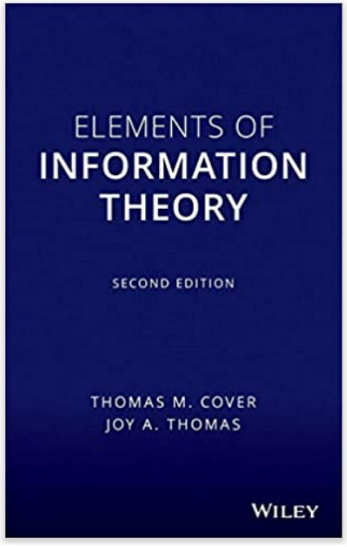
Livres de références

- Références additionnelles, disponibles en bibliothèque









Evaluation

- Examen écrit à livres ouverts ($\neq$ plus facile !)
- Pas de “par coeur”. Vise à tester la compréhension et la capacité de mise en oeuvre des concepts
- Calculatrice non programmable autorisée ; téléphones évidemment interdits

Méthodes d'apprentissage

- Apprentissage individuel (!)
  - Etude du syllabus et des slides
  - Réponses aux questions du guide de lecture
  - Réponses aux questions des anciens examens
- Cours magistraux (6 x 2h)
- Exercices (2 x 2h) sous-ensemble des questions d'examens et du guide de lecture
- Questions/réponses lors du cours, sur l'UV, lors de la permanence

Recette pour réussir : “flipped classroom”

- Etudier la matière du cours AVANT le cours
- Tenter les exercices AVANT les séances d'exercices
- Poser vos questions avant, pendant, après
- Profiter du cours magistral et séances d'exercices
  pour renforcer les intuitions, lier les morceaux de matière,
  clarifier les points non compris
- Revoir ensuite la matière AVANT le blocus
- Objectifs
  - Apprentissage en profondeur, esprit critique
  - Tirer le maximum des (rares) moments d'interactions

Apprentissage individuel

- Essentiel pour une compréhension en profondeur
- Prélecture de la théorie via le syllabus, slides, guide d'étude
- Résolution des exercices et examens précédents

Cours magistraux : approche

- "Flipped classrooms" :
  - AVANT le cours, vous étudiez du contenu de référence, et testez votre compréhension sur une série de questions
  - PENDANT le cours, mon but principal est de consolider votre intuition ; je peux aussi revoir certains aspects techniques à la demande
- Objectifs
  - Apprentissage en profondeur, esprit critique
  - Tirer le maximum des (rares) moments d'interactions
- En pratique : sollicitez des points à revoir via l'UV

Séances d'exercices : approche

- Vous faites le programme !
- En pratique
  - Vous tentez la résolution d'exercices du guide d'étude et examens précédents individuellement ou en groupe
  - Vous sollicitez l'ajout de certains exercices au programme via l'UV
  - Je confectionne un programme équilibré à partir de vos demandes

Posez vos questions !

- Objectifs :
  - Améliorer votre compréhension (et celle des autres !)
  - Développer votre esprit critique
  - Améliorer le cours !
- De préférence au cours, via l'UV, à la permanence
- Par email si nécessaire

Permanences

- Je serai disponible pour répondre aux questions sur le cours tous les lundis de 14h à 15h (contactez-moi sur Teams pour démarrer une session)
- Présence de votre part facultative ; aucune nouvelle matière ou tuyau
- Objectif : canal plus convivial et efficace que l'email pour me rencontrer et poser vos questions

Université Virtuelle et Teams

- Université virtuelle
  - Transparents, guide d'étude
  - Forums de discussion
- Teams pour les permanences

Horaires

- Cours magistraux et TPs
  - Mardis 10h-12h en semaines 2-3-4-5-6-7
  - Vendredis 14h-16h en semaines 4 et 9
- 2 blocs de (3 séances de cours puis 1 séance de TP)
- Permanence : lundis 14h-15h (sur Teams)

Tentative de programme

Cours 1	Présentation du cours Ch1. Notion de Code
Cours 2	Ch2. Source aléatoire et codes efficaces Ch3. Entropie et codage efficace
Cours 3	Ch4. Compression sans perte Ch5. Canal bruité
TP 1	Première séance de TPs
Cours 4	Ch6. Codes correcteurs d'erreurs
Cours 5	Ch7. Codes linéaires Ch8. Codes polynomiaux
Cours 6	Ch8. Autres familles de codes linéaires
TP 2	Deuxième séance de TPs

Mes attentes pour le cours

- Participation active (lecture des notes avant le cours, préparation des exercices, questions)
- Esprit critique, curieux

Feedback bienvenu !

- N'attendez pas la fin du cours si vous êtes perdus
- Je suis preneur de tout feedback pour améliorer le cours
  - Transparents ou explications confus
  - Typos et erreurs
  - ...

Questions ?

?

Crédits et remerciements

- Mes transparents suivent fortement les notes de cours développées par le Professeur Yves Roggeman pour le cours INFO-F303 à l'Université libre de Bruxelles
- Une partie des transparents et des exercices ont été repris ou adaptés des transparents développés par le Professeur Jean Cardinal pour ce même cours
- Je remercie chaleureusement Yves et Jean pour la mise à disposition de ce matériel pédagogique, et de manière plus large pour toute l'aide apportée pour la reprise de ce cours
- Les typos et erreurs sont exclusivement miennes (merci de les signaler !)