



Ecoles Nationale
Supérieure d'Arts
et Métiers



Forum des Professeurs
Agrégés du Maroc



Société Marocaine
d'Optique

Résumés des Exposés

de la journée :

"Traitement de l'information"

Organisée le 29 Novembre 2008 à l'ENSAM-Meknès

L'histoire de la théorie classique de l'information

M. A BENNANI

CPGE - Meknès-

Résumé :

Cet exposé retrace l'origine et l'évolution de la théorie de l'information. Il focalise un peu plus sur le travail du fondateur de l'ère d'information, l'électrotechnicien américain Claude Elwood Shannon. Bien que cette théorie est une représentation mathématique des conditions et des paramètres affectant la transmission et le traitement des renseignements et utilisée dans les domaines scientifiques et techniques, certains de ses concepts aient été adoptés et utilisés dans de telles disciplines que la sociologie, la psychologie et la linguistique.

Traitement optique de l'information :

La reconnaissance des caractères

M. A. KCHIKECH

CPGE - Meknès-

Résumé :

La reconnaissance des formes par voie optique est incontestablement un domaine qui suscite un grand intérêt : d'une part le besoin de reconnaître des formes est permanent d'autre part les systèmes optiques ont la capacité de traiter les données de façon parallèle réduisant ainsi les temps requis pour un traitement de données massives.

La corrélation optique, comme méthode de reconnaissance, est un outil de décision très puissant principalement du fait de son caractère global et de sa robustesse aux bruits. De plus ces dernières années ont vu d'importants progrès dans la conception et l'implémentation des filtres de corrélation.

Dans cet exposé, on proposera un aperçu sur la méthode de corrélation optique basée sur une architecture de type Vander Lugt. Puis on présentera une simulation numérique de la reconnaissance d'un caractère alphabétique dans une scène (teste) en utilisant une série de filtres (classique, inverse et de phase).

Les mathématiques et la protection de l'information

M. M'Hammed BOULAGOUAZ

Faculté des sciences et techniques de Fès

Résumé :

Si on peut présenter la cryptographie comme le domaine de la science qui a comme centre d'intérêt la protection de l'information contre une tierce personne estimée, elle est restée un domaine quasi réservé aux militaires et aux hommes d'état. En effet, les gouvernements pour assurer les secrets de leurs communications internes et diplomatiques, les armées pour cacher leurs plans à l'ennemi, cryptaient leurs correspondances et communications.

A travers toute l'histoire de l'humanité connue à nos jours, les sciences exactes n'ont offerts à la cryptographie que des techniques très élémentaires. Mais dès l'entrée du dernier quart du siècle dernier, et avec la croissance de la quantité d'information transitant sur les réseaux internationaux, crypter pour assurer la confidentialité et la sécurité des messages s'impose.

Ainsi la cryptographie et les problèmes qui lui sont associés vont occuper le premier rang des préoccupations et des centres d'intérêt de la communauté scientifique, pour permettre d'éviter l'interception, la lecture ou la modification des messages en clair, ainsi que la fabrication d'un message factice.

Dans cet exposé on donnera les grandes lignes du comment les mathématiques ont pu révolutionner ce domaine de la cryptographie ? et comment des disciplines mathématiques qualifiées d'abstraites (Algèbre, théorie des nombres, géométrie..) sont à la base de la révolution que connaissent les sciences de l'information depuis la fin du vingtième siècle ? (révolution que connaît les télécommunications, l'Internet, les Cartes à puces, le Commerce électronique..).

Dans cet exposé, on montre aussi qu'avant l'arrivée des ordinateurs, la cryptographie se contentait de formes très simples telles que la substitution ou la translation de caractères, ou au meilleur des cas des systèmes comprenant les deux, et que malheureusement ces systèmes étaient très vulnérables et que c'est en fait les mathématiques, notamment l'algèbre, la géométrie, la théorie des nombres qui ont donné les outils nécessaires à la conception d'algorithmes quasi sûrs à la cryptographie.

Introduction à la compression de données

E. ZEMMOURI

ENSAM- Meknès

Résumé :

La théorie des communication s'intéresse aux moyens et outils pour transmettre une information depuis une source jusqu'à une destination à travers un canal. La théorie de l'information et du codage a été introduite aux systèmes de communication par C. E. Shannon dans les années 1940. Avant d'être transmise sur canal, une information subit un ensemble de traitements : codage source (compression), codage canal, chiffrement, modulation, amplification ...

Le codage source, ou compression, consiste à faire parvenir une quantité donnée d'informations au récepteur en utilisant le minimum de ressources, et donc utiliser la ressource canal d'une manière efficace.

Dans cette présentation on va donner quelques définitions de mesure de l'information et d'entropie d'une source. Puis on présentera la notion de codes instantanés avec l'importante inégalité de Kraft. Par la suite quelques algorithmes de compression seront présentés avec des exemples de codage de sources discrètes sans mémoire en séquences binaires. Et enfin on définira les limites de la compression.

Course de Shannon : théorème du canal bruité

H. Ben-Azza

ENSAM- Meknès

A la mémoire d'un collègue F. Elmarjany

Résumé :

En 1948, dans l'introduction de son papier classique " A mathematical theory of communication", Claude Shannon a écrit : " The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point." (D'après la référence 3)) Shannon associe à chaque canal de communication une capacité, définie par le concept d'information mutuelle (donc par une entropie mesurant l'incertitude dans une variable aléatoire).

Le théorème du canal bruité affirme l'existence d'un code tel que si le taux de transmission est plus petit que la capacité du canal (bruité), alors il existe une méthode de décodage de ce code telle que la probabilité de l'erreur de décodage est proche de zéro (lorsque la longueur du code est assez grande).

Mais alors, comment construire ces codes performants ? Ce théorème (dont l'inverse annonce que si le taux est plus grand que la capacité du canal bruité alors la probabilité de l'erreur de décodage est toujours plus grande strictement que zéro) justifie une course graduelle des chercheurs pour construire des codes dans le but d'approcher la borne de Shannon (transmission proche de la capacité et décodage performant), donnant lieu à une vaste littérature des codes correcteurs d'erreurs théorique et appliquée.

En 1993, C. Berrou, A. Glavieux, et P. Thitimajshima construisent des codes à 0.7 dB de la capacité. C'est une révolution dans la communauté des codes correcteurs. Ainsi, le concept turbo décodage est né, qui d'après ses concepteurs il est intéressant de penser à la conception d'un décodeur d'abord et trouver le code adéquat ensuite (schématiquement).

En 1963 !, dans sa thèse, Gallager a proposé une classe de codes basés sur des matrices creuses (LDPC : Low Density Parity Check) avec un décodage itératif. Ces codes sont redécouverts en 1995 par Mackay montrant une efficacité aussi bonne que les turbo codes.

Il se trouve que le décodage des turbo codes et les LDPC codes s'approche du même principe BP (Belief Propagation) connu en intelligence artificielle.

Mais la course continue, et notre objectif premier dans cet exposé est de présenter à nos étudiants quelques ingrédients pour comprendre le versatile théorème de Shannon et ses conséquences (voir 4)).

Références :

- 1) C. Berrou, A. Glavieux, and P. Thitimajshima " *Near Shannon limit error-correcting coding and decoding : Turbo codes*", IEEE Int. Communications Conference, 1993.
- 2) R. G. Gallager, "*Low-Density Parity-Check Codes*", Cambridge", MA, MIT Press, 1963.
- 3) Robert J. McEliece, "*The theory of information and coding : A mathematical framework for communication*". Addison-Wesley, 1977.
- 4) R.G. Gallager, "*Information Theory and Reliable Communication*", New York, Wiley, 1968 .