IFT6100 A95 **Claude Crépeau**
Sujets spéciaux en théorie des systèmes:

– Théorie et application des codes correcteurs –

CONTENU DU COURS

La théorie des codes correcteurs étudie les façons de transmettre sur un canal imparfait des messages avec grande fiabilité. Ce cours considèrera tout d'abord des modèles de transmission et des modèles d'erreurs jugés réalistes. On apprendra (ou revisera) ensuite des notions mathématiques de base afin d'étudier les codes correcteurs: les calculs sur les corps finis et dans les espaces vectoriels. On définira la notion de code et considérera les problèmes généraux du codage et du décodage des informations pour leur transmission sur un canal imparfait.

On verra de nombreux types de code: Hamming, cyclique, Reed-Müller, Reed-Solomon, BCH, alternant, Golay, Goppa, Hadamard, intersectant, etc, ainsi que les diverses méthodes de codage et décodage qui leur sont associées. On considérera le problème de la construction de codes ayant de bonnes performances et montrera des bornes inférieures et supérieures sur les performances possibles des codes. À cette fin, on apprendra des méthodes de combinaisons de codes: concaténation, produit. On analysera les performances des codes *aléatoires*, qui sont généralement bien supérieures à celles obtenues par des construction explicites. On verra que le probème général de décodage qui consiste à trouver le mot de code le plus près d'un mot donné, est NP-complet et donc difficile en pratique pour des codes construits de façon aléatoire.

On élaborera des exemples d'applications de codes correcteurs aux systèmes de télécommunications (avec des sondes spatiales par exemple), au stockage des données (sur des Disques Numériques par exemple) et à la cryptographie (systèmes de chiffrements basés sur des codes, problèmes cryptographiques équivalent à des problèmes de codage).

On verra enfin des sujets plus avancés: géométrie algébrique et codes algébriques de Goppa (seule méthode de construction connue produisant des codes meilleurs que les codes aléatoires), graphes expandeurs, codes expandeurs et codes superconcentrateurs de Spielman (seuls codes pour lesquels on dispose d'une méthode de codage et décodage en temps linéaire).

À QUI S'ADRESSE CE COURS

La science des codes correcteurs se situe à mi-chemin entre la théorie et la pratique: surtout guidée par des considérations d'ordre pratique, il n'en reste pas moins que sa structure simple et fondamentale lui donne de nombreuses applications de nature algorithmique. Ceux qui s'intéressent à la confrontation entre la stabilité que nécessite l'information et l'entropie qui régit notre monde, aux télécommunications, à la complexité, à la cryptographie ou tout simplement ceux qui sont curieux trouveront leur place dans ce cours.

PRÉREQUIS

Le seul prérequis du cours est de ne pas craindre les mathématiques discrètes.

ÉVALUATION

L'évaluation se fera par des devoirs (4–5 de valeurs égales) distribués, ça et là, durant la session.

RÉFÉRENCES

Aucun livre n'est obligatoire pour ce cours. Il existe par contre de nombreux ouvrages de base sur la théorie des codes correcteurs dont principalement:

[Be84] E. R. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill, New York, NY, 1968; version revisée: Aegean Park Press, Laguna Hills, CA, 1984.

[Bl83] R. E. Blahut. *Theory and Practice of Error Control Codes.* Addison-Wesley, Reading, MA, 1983.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

et pour les sujets plus avancés:

[Go88] V. D. Goppa. *Geometry and Codes.* Kluwer Academic Publishers, Dordrecht, 1988.

[Sp95] D. A. Spielman. *Computationally Efficient Error-Correcting Codes and Holographic Proofs.* PhD Thesis, Dept. Mathematics, Massachusetts Institute of Technology, 1995.