UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du diplôme de **Master**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Mathématiques Appliquées et discrètes

Par

Kadiri Soufiane

Sujet

Codes Cycliques Iso-duaux de Rendement 1/2 sur GF(2)

Soutenu le : 16 / 06 / 2014

Devant le jury composé de :

President :	A. Amroune	Prof	Univ M'sila
Rapporteur :	C. Mihoubi	MC/B	Univ M'sila
Examinateur :	L. Ladjlat	MA/A	Univ M'sila

Promotion : 2013/2014

RESUME

La théorie du codage est l'étude des méthodes permettant le transfert d'informations de façon efficace et précise. Cette théorie est utilisée dans de multiples champs d'applications. On la retrouve dans l'enregistrement des disques compacts, dans la transmission d'information sur les réseaux ou encore dans les communications par satellites.

Le présent mémoire consiste à présenter et à analyser les differents concepts mathématiques et les differentes structures algébriques associés aux codes linéaires et codes cycliques. Alors dans ce travail, pour un code de paramètres $[n, k, d]$, on considère les codes cycliques de rendement $1/2$ sur le corps fini $GF(2)$ et on accentue notre étude sur ceux iso-duaux.

MOTS CLÉS : Anneaux des polynômes $A[X]$, Divisibilité, Polynômes irréductibles, Corps finis, Codes linéaires, Codes cycliques, Codes iso-duaux.

ABSTRACT

The theory of coding is the methods engineering allowing the transfer of information in an effective and precise way. This theory is used in multiple fields of application. One finds it in the recording of the compact disks, the transmission of information on the networks or in the satellite communications. The present report consists in having and analyzing the various mathematical concepts and the various algebraic structures associated the linear codes and cyclic codes. Then in this work, for a code of parameters $[n, k, d]$, one considers the cyclic codes of output $1/2$ on the finished body $GF(2)$ and one accentuates our study on those iso-duaux.

KEY WORDS : Rings of polynomials $A[x]$, Divisibility, Polynomials irreducible, Finite fields, linear Codes, Cyclic Codes, Isodual Codes.

Table des matières

INTRODUCTION GENERALE

Les codes correcteurs d'erreurs sont présents aujourd'hui dans tous les réseaux. Voyons tout d'abord pourquoi cette nécessité de codage, en informatique et dans les télécommunication le corps fini F_2 est le plus simple et le plus commode utilisé pour coder l'information à transmettre entre deux sites vu que les opérations d'addition et multiplication modulo 2 sont faciles à réaliser sur calculateur électronique

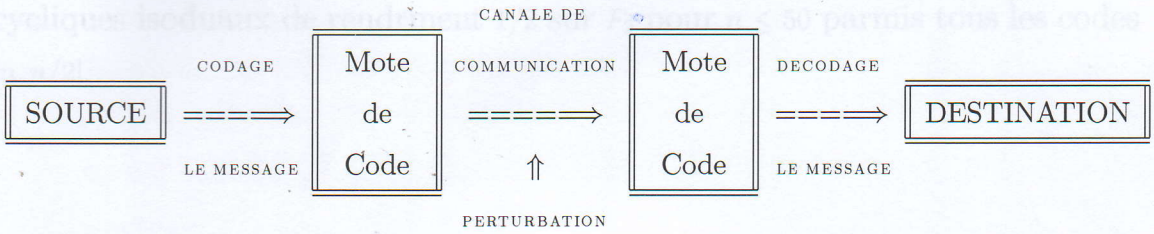

Schéma fondamental du codage

Le transfert d'informations prend de plus en plus d'importance dans notre société. Que ce soit pour la transmission de photographies de planètes éloignées, pour des communications entre ordinateurs ou encore pour la lecture de nos disques lasers, le besoin de communications effcaces et sans erreurs est plus important que jamais. Nous savons tous que des communications sans erreurs sont physiquement impossibles. Les codes ne sont pas là pour eliminer les erreurs mais plutôt pour les détecter et si possible les corriger. Afin d'illustrer sommairement un code, exploitons une idée intuitive qui consiste a répéter l'information un certain nombre de fois.

Dans ce travail on s'intéresse aux codes isodaux $[n, n/2]$ sur le corps fini F_2. En considérant les codes cycliques de paramètres $[n, n/2]$, pour n pair, nous avons recherché ces codes au sens du polynôme réciproque.

Déroulement du mémoire :

Dans le premier chapitre nous présentons les notions et propriétés fondamentales nécessaires pour la réalisation de ce travail concernant : Anneau, anneau quotient, corps, corps fini, Construction d'un corps fini. Les notions citées dans ce chapitre représentent l'outil mathématique utilisé pour l'étude des codes correcteurs d'erreurs.

Le deuxième chapitre regroupe les définitions et les propriétés fondamentales des polynômes sur un corps fini, Division Euclidienne dans $K[X]$ et Factorisation de $X^n - 1$, en polynômes irréductibles, sur un corps fini.

Enfin, dans le dernier chapitre, on présente en premier lieu les paramètres des codes linéaires et des codes cycliques, puis on va rechercher les codes cycliques isoduaux de rendrment $1/2$ sur F_2 pour $n \leq 50$ parmis tous les codes $[n, n/2]$.

CONCLUSION GENERALE

Le travail de ce mèmoire entre, dans le cadre de la recherche des codes linéaires isoduaux sur un corps fini F_q, en particulier nous avons étudié les codes cycliques iso-duaux de rendement $1/2$ sur F_2. Dans ce contexte nous avons rechercher les codes cycliques iso-duaux de paramètres $[n, n/2]$ sur le corps fini F_2, avec n pair et $m = n/2$ impair et premier jusqu'à la longeur ≤ 50.

Bibliographie

[1] **A.A.Pantchichkine.** *Mathématiques des codes correcteurs d'erreurs.* Master 2 de mathématiques (M2P),"Cryptologie, Sécurité et Codage d'Information", 2004/2005, Module 506a.

[2] **A. Bonnecaze.** *Introduction à l'algèbre pour les Codes cycliques* 2006/2007, (Cours sur internet).

[3] **Cherif Mihoubi.** *Classification des Codes linéaires tertiaires optimaux* $[n, n/2]$. Thèse présenté pour l'obtention du diplôme de Doctorat, Université Hadj Lakhdar Batna, 2012.

[4] **Cherif Mihoubi.** *Etude sur l'irréductibilité d'un polynôme sur un corps fini.* Mémoire présenté pour l'obtention du diplome de Magistére en Mathématiques, Université de M'sila 2001.

[5] **Cherif Mihoubi.** *Isodual Cyclic Codes over* $GF(5)$. Into . J. Open Problems Compt. Math., Vol. 4, No. 4, December 2011 ISSN 1998-6262; Copyright c ICSRS Publication, 2011 www.i-csrs.org.

[6] **Cherif Mihoubi** et **Patrick Sole.** *Optimal and isodual ternary cyclic codes of rate* $1/2$. Received: 12 January 2012 / Revised: 9 May 2012 / Accepted: 4 July 2012 / Published online: 26 July 2012 © The Author(s) 2012. This article is published with open access at SpringerLink.com.

[7] **Dany-Jack Mercier.** *Corps finis*, IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, dany-jack.mercier@univ-ag.fr, 11 avril 2003.

[8] **Hans Bherer.** *Théorie Algébrique du Codage.* Mémoire présenté à la Faculté des études supérieures de l'université Laval présenté pour l'obtention du grade de M.Sc, Septembre 2000.

[9] **Heboub Lakhdar**. *Etude de Techniques de décodage des codes linéaires.* Mémoire présenté pour l'obtention du diplome de Magistére, Université de M'sila 2009/2010.

[10] **Jean-Jacques Risler** et **Pascal Boyer**. *Algèbre pour la licence 3, Groupes, anneaux, corps, cours et exercice corrigés.*

[11] **Marc Lelarge.** *Théorie de l'information et codage* 2010/2011, (Cours sur internet), Page web du cours http://www.di.ens.fr/~lelarge/info11.html.

[12] **Nicolas Bruyere.** *Eléments de théorie des corps finis. Application : les codes correcteurs.* Université de Rouen. Agrégation de mathématiques 2005/2006.

[13] **Pierre Abbrugiati.** *Introduction aux codes correcteurs d'erreurs*, 23 janvier 2006, (Cours sur internet).

[14] **Pierre Lissy.** *Polynômes irréductibles. Corps de rupture. Exemples et applications*, 4 January 2010, (Cours sur internet).

[15] **Pierre Wassef**. *Arithmétique Application aux Codes Correcteurs et à la Crypographie,cours et 122 exercice corrigés*, licence de mathématiques, l'université de pierre et Marie Curie/paris-VI.

[16] **Reynald Lercier**. *Algorithmique des courbes elliptiques dans les corps finis*, Thèse présenté pour l'obtention du diplôme de Doctorat de l'école politechnique, spécialité informatique, 1996/1997.

[17] **Robert Rolland**. *Introduction à l'étude des Corps fini (Résumé)*, (Cours sur internet).

[18] **Saadi Ameur.** *Etude sur les bornes des codes correcteurs d'erreurs.* Mémoire présenté pour l'obtention du diplome de Magistére en Mathématiques, Université de M'sila 1999/2000.

[19] Ex7 polynôme, corps finis, Théorie et codage de l'information (Les codes de Hamming et les codes cycliques), (troix cours sur internet).