UNIVERSITE "MOHAMED BOUDIAF" 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 discrètes

Par

Mohamed CHAREF

Sujet

Codes Cycliques Optimaux de Rendement 1/2 sur GF(5)

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 : 2014/2015

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.

Ce mémoire consiste à présenter et à analyser les differents concepts mathématiques et les differentes structures algébriques associés aux codes linéaires et codes cycliques.

Dans ce travail, pour un code de paramètres $[n, k, d]$, on considère les codes cycliques de rendement $1/2$ sur le corps fini $GF(5)$ et on accentue notre étude sur ceux optimaux.

MOTS CLÉS : Divisibilité; Polynômes irréductibles; Corps finis; Codes linéaires; Codes cycliques; Codes optimaux.

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. we find it in the recording of the compact disks, the transmission of information on the networks or in the satellite communications.

This memoir to present and analyze the differents mathematicals concepts and the different algebraic structures associated to the linear codes and cyclic codes.

Then in this work, for a code of parameters $[n, k, d]$, we consider the cyclic codes of rate $1/2$ over the finite field $GF(5)$ and we check our study over whose are optimal.

KEY WORDS : Divisibility; Irreducible polynomials; Finite fields; linear Codes; Cyclic Codes; optimal Codes.

Table des matières

INTRODUCTION GENERALE

Le codage correcteur d'erreur introduit une forme de redondance controlée dans un message à transmettre pour le protéger face aux erreurs de transmission, cette technique joue aujour'hui un role fondamental dans les systèmes modernes de transmission et de stockage de l'information numérique.

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 efficaces 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.

La théorie du codage vise à construire des codes correcteurs performant opérant au plus proche des limites théoriques établiés par la théorie de l'information, dans ce contexte il s'agit de rechercher des codes optimaux ayant la meilleure distance minimale pour une longeur n pair et une dimension $n/2$.

Dans ce travail on s'intéresse aux codes optimaux $[n, n/2]$ sur le corps fini F_5. En considérant les codes cycliques de paramètres $[n, n/2]$, pour n pair, nous avons recherché ces codes au sens de la distance minimum.

Déroulement du mémoire :

Dans le premier chapitre nous présentons les notions et propriétés fondamentales nécessaires pour la réalisation de ce travail concernant : Anneau, Corps fini, Sous-corps, 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, Algébre des polynômes, 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 la distance minimale des codes cycliques de rendement $1/2$ sur F_5 pour $n < 50$, on utilise l'algorithme de Chen pour déterminer cette distance, on va choisir les codes optimaux parmis tous les codes $[n, n/2]$.

CONCLUSION

Le travail de ce mèmoire entre, dans le cadre de la classification des codes linéaires optimaux sur un corps fini F_q, en particulier nous avons étudié les codes cycliques optimaux de rendement $1/2$ sur F_5. Dans ce contexte nous avons calculer la distance minimale optimale des codes de paramètres $[n, n/2]$ sur le corps fini F_5, avec n pair et $k = n/2$ impair jusqu'à la longeur $n < 50$.

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 of rate* 1/2 *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] **Frédéric Butin.** *Algébre Polyncômes, théorie Galois et applications informatiques* Hermann éditeur 2012, 6 rue de la sorbonne 75005 paris

[9] **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.

[10] **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.

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

[12] **Meftah Imane.** *divisibliti des trinômes $x^{am}+x^{bs}+1$ par un polyncôme irréductible sur F_2.*Mémoire présenté pour l'obtention du diplome de Master en Mathématiques, Université de M'sila 1012/2013.

[13] **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.

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

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

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

[17] **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.

[18] **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.

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

[20] **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.

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