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

BENADEL Mohammed

Sujet

Codage et Décodage des Codes Cycliques C[n, n/2] Sur F_2

Devant le jury composé de :

A. Amroune	Prof	Président	Univ de M'sila
C. Mihoubi	MC/B	Encadreur	Univ de M'sila
L. Ladjlat	MA/A	Examinateur	Univ de M'sila

Promotion : 2013/2014

Table des matières

Résumé

Dans ce travail, on a essayé de donner un aperçu sur les différentes propriétés des extensions algébriques finis, et nous avons traité ensuite les notions fondamentales des corps finis et on a fini par la construction d'un corps finis.
Et ensuite nous avons donné les concepts sur les polynômes en particulier les polynômes irréductibles sur un corps finis, et on a donné également les principales propriétés de ces polynômes .
En fin on a évoque une étude sur les codes, codes linéaires et codes cycliques, qu'on a achevé par l'étude du codage et décodage d'un code cyclique $C[n, \frac{n}{2}]$ sur F_2.

MOTS CLÉS : Extensions algébriques finis, Corps finis, Divisibilité, Polynômes irréductibles, Codes linéaires, Codes cycliques.

Abstract

In this work, we tried to give an overview on the different properties of finite algebraic extensions, and we then treated the fundamentals of finite fields and finally the construction of a finite fields.
And then we gave the concepts of polynomials in particular irreducible polynomials over finite fields, and also gave the main properties of these polynomials.
In the end it was mentioned a study on codes, linear codes, cyclic codes, which was completed by the study of encoding and decoding of a cyclic code $C[n, \frac{n}{2}]$ over F_2 .

KEY WORDS : Algebraic Extensions finished, finished fields, divisibility, irreducible polynomials, linear codes, cyclic codes.

INTRODUCTION

Le codage correcteur d'erreurs, appelé aussi codage du canal, dont l'origine remonte à la fin des années 40 par Claude Shannon. Il consiste à rajouter à l'information numérique, des symboles binaires, appelés symboles redondance, suivant une loi mathématique particulière, qui permettent de reconstituer l'information au niveau du récepteur.
Le décodeur vérifie que la loi de codage n'a pas été modifiée lors des divers traitements réalisés sur l'information numérique codée. Si c'est le cas, le décodeur conclut à l'absence d'erreur ; dans le cas contraire, par un traitement approprié, il repaire les symboles erronés puis les corrige par simple inversion binaire. Malheureusement, le codage correcteur d'erreurs à des capacités de correction limitées et ainsi, certaines erreurs peuvent lui échapper.

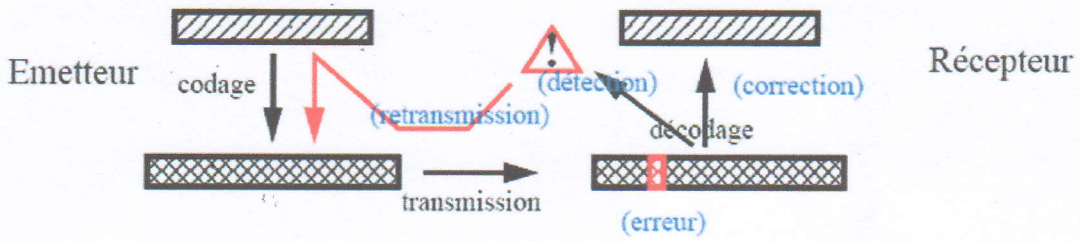

Schéma de transmission de l'information

Ce mémoire est organisé de la manière suivante :

– Le premier chapitre est constitué des définitions et des concepts de base, à ce niveau, Nous commençons par définir la notion des extensions algébriques finis. Nous passerons ensuite à la définition de la caractéristique d'un corps fini, et nous donnons la construction d'un corps fini en utilisant le corps $F_p[x]/(f)$ avec f un polynôme irréductible sur F_p, et proposons un exemple illustratif.

– Dans le deuxième chapitre, Nous donnons des définitions sur les polynômes, ensuite nous présentons les notions fondamentales de la divisibilité et l'irréductibilité des polynômes dans l'anneau $k[x]$, et nous donnons les principales propriétés des polynômes

irréductibles.

– Dans le troisième chapitre, nous présentons des définitions sur les codes et donnons les définitions sur les codes linéaire et les codes cycliques, et enfin nous étudions le codage et décodage des codes cycliques $C[n, \frac{n}{2}]$ sur F_2.

Conclusion

Les codes cycliques ont été au centre de l'intérêt pour la théorie des codes correcteurs d'erreurs. L'objectif de ces codes est la correction automatique de certaines altérations de message.

Dans ce travail on s'est intéressé à étudier le codage et décodage des codes cyclique. Pour le codage on a utilisé deux méthodes, la première appelé méthode systématique et la deuxième appelé méthode non systématique. On a étudié également le décodage des codes cyclique par syndrôme.

Bibliographie

[1] **Hans Bherer,** Théorie Algébrique Du Codage, Mémoire présenté pour l'obtention du grade de mâtre ès Sciences (M.Sc.), Université Laval, 2000.

[2] **Arnaud Bodin**, Polynômes, Basé sur des cours de Guoting Chen et Marc Bourdon, "http ://exo7.emath.fr/cours/ch_polynome.pdf."

[3] **A. Bonnecaze**, Introduction à l'algèbre pour les Codes cycliques, 2006 – 2007.

[4] **Claude Carlet**, Cours de Codes Correcteurs d'erreurs (et fonctions booléennes), D.E.A de mathématiques et d'informatique de Bamako Année 2007.

[5] **karima Chatouh,** Les codes Cortex et les codes auto- duaux de type I et de type II, Mémoire présenté pour l'obtention du diplôme de Magistère, Université de Batna, 2007.

[6] **Eric Fabre,** Théorie de l'information et Codes correcteurs d'erreurs, 2000.

[7] **Alain Kraus**, Cours de cryptographie MM067, Université de Pierre et Marie Curie, 2012 – 2013.

[8] **Pierre Lissy**, Polynôme irréductible. Corps de rupture. Exemples et applications, 2010.

[9] **Ahlem Melakhessou,** Théorie Algébrique Des Codes Convolutionnels Cycliques, Mémoire présenté pour l'obtention du diplôme de Magistère, Université de Batna, 2011.

[10] **Dany-Jack Mercier,** Corps finis, IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, 2003.

[11] **Cherif Mihoubi**, Etude sur l'irréductibilité d'un polynôme sur un corps finis , Mémoire présenté pour l'obtention du diplôme de Magistère, Université de M'sila, 2001.

[12] **Ameur Saadi,** Etude sur les bornes des codes correcteurs d'erreurs, Mémoire présenté pour l'obtention du diplôme de Magistère, Université de M'sila, 1999 – 2000.

[13] **Lionel Schwartz**, Algèbre 3, Université de Paris, 2003.

[14] **Sergei Silvestrov,** Extension fields II, Spring term 2011.

[15] **Mathieu Vienney**, corps finis,
"http ://www.umpa.ens-lyon.fr/~mivenney/agreg/corps_finis.pdf".