

N° d'ordre:

THÈSE

présentée à

L'UNIVERSITÉ PARIS VI

pour obtenir le titre de

DOCTEUR DE L'UNIVERSITÉ PARIS VI

Spécialité

INFORMATIQUE

par

Françoise LEVY-DIT-VEHEL

Sujet de la thèse :

**DIVISIBILITÉ DES CODES CYCLIQUES :
APPLICATIONS ET PROLONGEMENTS**

Soutenue le 20 octobre 1994 devant le jury composé de :

MM. Daniel LAZARD	Président
Mme Pascale CHARPIN	Directeur
MM. François LAUBIE Claude CARLET	Rapporteurs
Edward ASSMUS Paul CAMION Gérard COHEN	Examineurs

Résumé

Nous utilisons des outils récents de type combinatoire et algébrique pour étudier la divisibilité des codes cycliques et affine-invariants, la distance minimale des duaux des codes BCH étendus sur \mathbb{F}_p , et les codes autoduaux affine-invariants.

En adaptant aux codes affine-invariants un résultat dû à McEliece sur la divisibilité des codes cycliques, nous construisons de tels codes 4-divisibles sur \mathbb{F}_2 . Nous obtenons également une formule pour la divisibilité de tout code irréductible sur \mathbb{F}_p . Nous donnons en outre des éléments pour l'étude de la divisibilité de l'image binaire de codes cycliques sur \mathbb{F}_4 .

Nous isolons une classe de duaux de codes BCH étendus sur \mathbb{F}_p , présentant des propriétés combinatoires particulières. C'est cette structure qui nous permettra de déduire des bornes sur leur distance minimale, et par suite sur la distance minimale de tous les duaux des codes BCH étendus sur \mathbb{F}_p .

Les résultats que nous obtenons sur les codes autoduaux affine-invariants constituent peut-être l'exemple le plus probant de l'intérêt qu'il y a à considérer les codes affine-invariants du point de vue combinatoire. En effet, la caractérisation de l'autodualité faible en termes de relation d'ordre nous permet non seulement de donner une liste exhaustive des autoduaux affine-invariants en petites longueurs, mais induit également une méthode de construction de tels codes sur \mathbb{F}_2 , en toutes longueurs de la forme 2^m , m impair.

Mots-clefs

Codes correcteurs d'erreurs, codes cycliques, codes divisibles, duaux des codes BCH, codes autoduaux.

Abstract

We use recent combinatorial and algebraic tools to study the divisibility of cyclic and affine-invariant codes, the minimum distance of the duals of BCH codes over \mathbb{F}_p , and the class of self-dual affine-invariant codes.

We adapt a result due to McEliece on the divisibility of cyclic codes to the case of affine-invariant codes, and this enables us to construct such 4-divisible codes over \mathbb{F}_2 . We obtain a formula for the divisibility of any irreducible code over \mathbb{F}_p . We also give some elements to study the divisibility of binary images of cyclic codes over \mathbb{F}_4 .

We isolate a class of duals of extended BCH codes over \mathbb{F}_p , with noteworthy combinatorial properties. This will allow us to derive a bound on their minimum distance, and consequently on the minimum distance of all duals of extended BCH codes over \mathbb{F}_p .

The results obtained on self-dual affine-invariant codes are probably the most convincing example of the interest of considering affine-invariant codes from a combinatorial viewpoint. Indeed, the characterization of weak self-duality in terms of a partial order relation does not only permit us to list all self-dual affine-invariant codes in small lengths, but induces also a method to construct such codes over \mathbb{F}_2 , in any length of the form 2^m for odd m .

ISBN - 2 - 7261 - 0856 - 3



Table des matières

Introduction générale	7
I Quelques résultats généraux de théorie des codes	15
1 Codes linéaires	15
2 Codes cycliques et cycliques étendus	17
3 Codes de l'algèbre $\mathcal{A} = \mathbb{F}_p^r[(\mathbb{F}_q, +)]$	20
4 Codes affine-invariants	22
5 Deux importantes classes de codes	25
5.1 Les codes de Reed et Muller généralisés	25
5.2 Les codes BCH	27
II Divisibilité des codes cycliques: Le théorème de McEliece	29
1 Introduction	29
2 La divisibilité des codes linéaires	30
3 Présentation du théorème de McEliece	33
3.1 Rappel sur les nombres p-adiques	33
3.2 Le théorème de McEliece	39
3.3 Un exemple: La divisibilité des codes de Reed et Muller Généralisés raccourcis	48
4 Applications	50
4.1 Les codes cycliques primitifs étendus	51
4.2 Les codes irréductibles	58
III Bornes sur la distance minimale des duaux des codes BCH étendus sur \mathbb{F}_p	65
1 Introduction	65
2 Une classe particulière de duaux de codes BCH étendus	66
3 Sur la distance minimale de $\bar{B}^\perp(t, i)$	72
3.1 La borne de Roos adaptée aux codes affine-invariants	72
3.2 La borne de Weil	77
3.3 Comparaison des différentes bornes	81
3.4 Exemples numériques	82
4 Distance minimale d'un code affine-invariant compris entre deux codes de cette classe	85
4.1 Sur \mathbb{F}_2	85
4.2 Sur $\mathbb{F}_p, p \neq 2$	97

5	Conclusion	110
IV Codes autoduaux affine-invariants		113
1	Préliminaires	114
2	La condition d'autodualité faible	116
3	Les autoduaux en longueur 128	120
4	Une classe infinie de codes affine-invariants autoduaux binaires	123
5	Conclusion	130
6	Annexe	131
6.1	L'ensemble des mots de poids minimum du code R_3^*	131
6.2	L'ensemble des mots de poids minimum du code R_2^*	132
6.3	Sur le poids minimum des codes cycliques étendus autoduaux en longueur 128	134
V Divisibilité de l'image binaire de codes autoduaux sur \mathbb{F}_4		139
1	Introduction-Position du problème	139
2	Forme de l'image binaire	140
2.1	Définitions et premières propriétés	140
2.2	Structure de l'image binaire de codes cycliques sur \mathbb{F}_4	141
3	Le théorème de Delsarte dans ce contexte	147
4	Sur la divisibilité	149
4.1	Remarques préliminaires	149
4.2	Conditions suffisantes de 4-divisibilité	152
4.3	Applications	155
5	Conclusion	159
Conclusion		161
ANNEXES		163
A Bornes supérieures sur le nombre de points rationnels de courbes algébriques à partir de bornes inférieures sur la distance minimale de codes cycliques		163
1	Préliminaires	164
2	Une borne supérieure	165
3	Exemples d'application	167
3.1	Courbes associées aux GRM raccourcis sur \mathbb{F}_q	167
3.2	Courbes associées à des duaux de codes BCH sur \mathbb{F}_q	169
4	Conclusion	173
B Présentation des algorithmes et mise en oeuvre		175
1	Algorithmes de calcul des bornes du chapitre III	175
1.1	Sur $\mathbb{F}_p, p \neq 2$	175
1.2	Sur \mathbb{F}_2	180

2	La méthode de Schaub pour borner la distance minimale des duaux des BCH	182
3	Recherche d'idempotents des codes autoduaux affine-invariants raccourcis de longueur 511	186
3.1	Les idempotents de poids 31	186
3.2	Les idempotents de poids 27	189