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**	Rapporteurs
	Claude	**CARLET**	
	Edward	**ASSMUS**	Examinateurs
	Paul	**CAMION**	
	Gérard	**COHEN**	

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 caracterization 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.

I S B N - 2 - 7261 - 0856 - 3

Table des matières