



N° d'ordre 19 /2014

THESE DE DOCTORAT

Présentée par

Khalid ABDELMOUMEN

Discipline : Mathématiques et Informatique

Spécialité : Codes correcteurs d'erreurs et Sécurité de l'Information

Décodages des codes alternants et codes sur les anneaux commutatifs finis (via la dualité de Pontrjagin)

Soutenue le 07 juin 2014 devant le jury composé de :

Omar SIDKI	Professeur à la FST de Fès	Président
Omar KHADIR	Professeur à la FST de Mohammedia	Rapporteur
Mostafa BELKASMI	Professeur à l'ENSIAS de Rabat	Rapporteur
Najib MAHDOU	Professeur à la FST de Fès	Rapporteur
Mohammed CHARKANI	Professeur à la Faculté des Sciences de Fès	Examineur
Hussain BEN AZZA	Professeur à l'ENSAM de Meknès	Directeur de thèse
M'Hammed BOULAGOUAZ		Invité

Laboratoire d'accueil : Laboratoire d'Algèbre, Analyse fonctionnelle et Applications

Etablissement : FACULTE DES SCIENCES ET TECHNIQUES - FES

Table des matières

Table des figures	8
1 Introduction générale	10
Bibliographie	13
2 Codes correcteurs d'erreurs	15
2.1 Introduction	15
2.2 Généralités sur les codes	16
2.2.1 Notions de base	16
2.2.2 Codes linéaires	18
2.3 Bornes sur les paramètres d'un code	21
2.4 Énumération de poids et l'identité de MacWilliams	23
2.5 Sous-code sur un sous-corps et code trace	25
2.6 Codes cycliques et codes de Goppa rationnels	26
2.6.1 Codes cycliques	26
2.6.2 Codes de Reed-Solomon et codes BCH	28
2.6.3 Codes de Goppa rationnels	31
2.7 Codes alternants	33
2.7.1 Notions de base des codes alternants	33
2.7.2 Exemples	34
2.8 Codes algébriques géométriques	35
2.8.1 Courbes algébrique	35
2.8.2 Diviseurs	41
2.8.3 Différentielle sur une courbe	44
2.8.4 Théorème de Riemann - Roch	45
2.8.5 Codes de Goppa géométriques	46
2.9 Codes géométriques généralisés	54
2.10 Décodage algébrique des codes alternants et Goppa rationnels	54
2.10.1 Problème de décodage	54

2.10.2	Décodage algébrique de codes alternants et de Goppa rationnels	55
2.11	Conclusion	58
Bibliographie		59
3	Décodage des codes alternants par l'approximation de Padé et les fractions continues	62
3.1	Approximation de Padé	62
3.1.1	Calcul des approximations de Padé	66
3.1.2	Quelques résultats de convergence	68
3.2	Les fractions continues	69
3.2.1	Lien entre approximation de Padé et fractions continues	73
3.2.2	Le qd-algorithme (Rutishauser 1957)	73
3.3	Décodage des codes alternants par l'approximation de Padé	75
3.3.1	Décodage des codes alternants par l'approximation de Padé	77
3.4	Décodage des codes de Goppa par les fractions continues	80
3.5	Algorithme de Berlekamp-Massey	82
3.6	Conclusion	85
Bibliographie		86
4	Lattices et décodage des codes alternants	87
4.1	Introduction	87
4.2	Lattices	88
4.2.1	Lattices de \mathbb{R}^n	88
4.2.2	Lattices sur un anneau de polynômes	94
4.3	Décodage des codes alternants par les lattices	95
4.3.1	L'algorithme en $t(\log t)^3$	103
4.4	Conclusion	104
Bibliographie		105
5	Codes sur les anneaux commutatifs finis	107
5.1	Codes linéaires sur les anneaux	107
5.2	Dualité de Pontrjagin	109
5.2.1	Dual d'un groupe topologique	109
5.2.2	Dual d'un groupe abélien fini	111
5.2.3	Dual d'un \mathfrak{R} -module	111
5.3	Décodage par syndrome	112
5.4	Matrice de contrôle	113

5.5	Exemple	116
5.6	Codes trace	118
5.6.1	Trace dans une extension	118
5.6.2	Une forme du théorème de Delsarte	119
5.7	Conclusion	121
	Bibliographie	122
	Conclusion et perspectives	124
	Annexes	125
	A 1 : Anneaux de Galois	126
	Bibliographie	128
	A 2 : A propos des codes euclidiens sur les anneaux	128
5.8	Introduction	129
5.9	Codes sur des anneaux commutatifs euclidiens	129
5.10	Codes sur des anneaux non commutatifs	135
5.11	Conclusion	138
	Bibliographie	139