



Universiteit
Leiden
The Netherlands

On products of linear error correcting codes

Mirandola, D.

Citation

Mirandola, D. (2017, December 6). *On products of linear error correcting codes*. Retrieved from <https://hdl.handle.net/1887/57796>

Version: Not Applicable (or Unknown)

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/57796>

Note: To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/57796> holds various files of this Leiden University dissertation

Author: Mirandola, Diego

Title: On products of linear error correcting codes

Date: 2017-12-06

On Products of Linear Error Correcting Codes

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 6 december 2017
klokke 15:00 uur

door

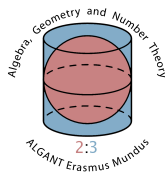
Diego Mirandola
geboren te Verona, Italië,
in 1988

Promotores: Prof. dr. Ronald Cramer (CWI & Universiteit Leiden)
Prof. dr. Gilles Zémor (Université de Bordeaux)
Copromotor: Dr. Ignacio Cascudo (Aalborg University)

Samenstelling van de promotiecommissie:

Dr. Anne Canteaut (Inria Paris)
Dr. Ruud Pellikaan (Technische Universiteit Eindhoven)
Prof. dr. Bart de Smit (Universiteit Leiden)
Prof. dr. Aad van der Vaart (Universiteit Leiden)
Prof. dr. Qing Xiang (University of Delaware)

This work was funded by Erasmus Mundus Algant-Doc and was carried out at Universiteit Leiden, Université de Bordeaux and CWI Amsterdam.





Universiteit Leiden

THÈSE EN COTUTELLE PRÉSENTÉE
POUR OBTENIR LE GRADE DE
DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX
ET DE L'UNIVERSITÉ DE LEYDE

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE
INSTITUT DES MATHÉMATIQUES DE L'UNIVERSITÉ DE LEYDE
SPÉCIALITÉ Mathématiques Pures

Par Diego MIRANDOLA

Sur les Produits
de Codes Correcteurs d'Erreurs Linéaires
Sous la direction de Ronald CRAMER et Gilles ZÉMOR

Soutenue le : 6 decembre 2017 à Leyde

Rapporteurs :

Ruud PELLIKAAN	Universitair Docent, TU Eindhoven
Qing XIANG	Professeur, University of Delaware

Membres du jury :

Anne CANTEAUT	Directrice de recherche, Inria Paris	Examinatrice
Ruud PELLIKAAN	Universitair Docent, TU Eindhoven	Rapporteur
Bart DE SMIT	Professeur, Universiteit Leiden	Président
Aad VAN DER VAART	Professeur, Universiteit Leiden	Examineur

Ai miei nonni

Contents

1	A Survey on Code Products	1
1.1	Codes and Code Products	1
1.2	Error Locating Pairs	6
1.3	Secret Sharing and Secure Multiparty Computation	8
1.4	Bilinear Multiplication Algorithms	11
1.5	Additive Combinatorics	12
1.6	Cryptanalysis of McEliece Cryptosystem	13
1.7	Outline of the Thesis	15
2	Preliminaries	17
2.1	Overview	17
2.2	Notation	18
2.3	Bilinear Algebra	18
2.4	Quadratic Forms	21
2.4.1	Classification in $\text{char } \mathbb{K} \neq 2$	23
2.4.2	Classification in $\text{char } \mathbb{K} = 2$	26
2.4.3	Number of Zeros of a Quadratic Form	28
2.4.4	Number of Quadratic Forms of Given Rank	30
2.5	Coding Theory	38
2.5.1	MDS Codes and Reed-Solomon Codes	40
2.5.2	Code Products	44
2.5.3	Error Correcting Pairs	48
2.5.4	Code Products and Bilinear Maps	50
2.6	Arithmetic Secret Sharing	51
2.6.1	Composition of Secret Sharing Schemes	56
2.6.2	Threshold Schemes and Shamir's Scheme	57
2.6.3	Connection between Coding Theory and Secret Sharing	58
2.6.4	From Secret Sharing to Multiparty Computation	61
3	Squares of Random Linear Codes	65
3.1	Overview	65
3.2	Proof of Theorem 3.1.5	70

3.3	Quadratic Forms	75
3.4	Proof of Main Theorem 3.1.2	76
3.5	Changing the Probabilistic Model	83
4	Critical Pairs for the Product Singleton Bound	85
4.1	Overview	85
4.2	Kneser's Theorem	87
4.3	Vosper's Theorem	91
	4.3.1 Consequences of Theorem 4.3.2	96
4.4	Classification of PMDS pairs	99
4.5	Concluding Comments	103
5	On Secret Sharing with Non-linear Product Reconstruction	105
5.1	Overview	105
5.2	Separating Quadratic Forms	109
5.3	Finding "Exotic Schemes"	111
5.4	Composition and Proof of the Main Result	114
5.5	The Smallest Examples	116
	Bibliography	123
	Summary	131
	Samenvatting	133
	Résumé	135
	Acknowledgments	137
	Curriculum Vitae	139