



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

Acknowledgments

In my experience as a Ph.D. candidate, I had the privilege of working with two of the highest experts in my field of interest, namely Ronald Cramer and Gilles Zémor. Ronald, your non-constant presence had the twofold effect of teaching me that a scientist needs to be independent, but at the same time can count on other scientists as sources of ideas: and you are an endless one. Gilles, during my stay in Bordeaux we regularly spent infinite hours in your office, staring at your whiteboard and working not as a supervisor with his student, but as peers. This wonderful combination of different ways to play the role of supervisor allowed me to make the best out of this experience, and I am grateful for that. On top of that, I had the pleasure to share out-of-office situations with both of you: this should be a mandatory part of your role in my opinion, thank you for doing it spontaneously.

The paternity of two thirds of the content of this thesis is shared with Ignacio Cascudo. Nacho, you were the first person who welcomed me when I arrived at CWI and the best possible co-supervisor for the first year and a half of my career. Thank you for all the mathematical discussions we had and for guiding me through my first steps as a Ph.D. candidate.

This thesis would never have existed as a concrete book without the support of my colleague and friend Gabriele Spini. Gabriele, thank you for teaching me the existence and, through your example, the meaning of the word “dependable”. And congratulations for your Ph.D..

The Cryptology group at CWI was the perfect setting for these four years of hard work. I am grateful to all people who have been part of the group throughout these years and who have shared with me their knowledge, or even just a lunch. I thank also all CWI people who were present at any of my well-deserved breaks: all people I shared a coffee with, all people I played football or table-football with, all people I met at a Praethuys or at a gaming night.

Ringrazio le persone conosciute in questi anni e che, ciascuno a proprio modo, mi hanno aiutato a continuare questo difficile percorso. Un pensiero spe-

ziale è dedicato ai miei amici Alberto, Giovanni, Giuseppe, Marcello, Nicola e Samuele: la lontananza da casa è sempre stata per me un peso, il mio più profondo ringraziamento per essere stati la mia seconda famiglia. Grazie a Andrea, Emanuele, Fortunato, Luca, Marco, Rosanna e Tommaso, incontri virtuali trasformati in amicizie reali.

Ho la fortuna di avere in Italia una famiglia, degli amici, e una città pronti ad abbracciarmi a ogni mio ritorno e a salutarmi a ogni mia ripartenza. A tutti voi, grazie per essere un motivo per tornare. A Maddalena, grazie per esserci sempre stata per me. A Giacomino, grazie per credere in me anche più di quanto non creda io stesso. Ad Anna, scusa per essermi perso i sei anni più belli della tua vita: spero che un giorno tu possa capire quanto questa scelta sia stata difficile ma allo stesso tempo importante, e magari trarne ispirazione. A Matteo, semplicemente grazie: non c'è altro da aggiungere per chi è allo stesso tempo un cugino, un fratello e un migliore amico.

Concludo ringraziando Madre e Padre per aver sopportato la mancanza del loro unico figlio: posso solo dirvi che è stato difficile per me almeno quanto lo è stato per voi, e che sono tornato.

Curriculum Vitae

Diego Mirandola was born on the 14th of November 1988 in Verona, Italy. He grew up in the nearby town of Caldiero, and obtained his high school diploma from the “Liceo Scientifico A. Messedaglia” in 2007.

He then started his Bachelor in Mathematics at the University of Padua, Italy (Università degli Studi di Padova), obtaining the corresponding diploma in 2010. During these years, he was supported by a grant from INdAM, the Italian National Institute of High Mathematics.

That same year he was accepted in the Algant-Master program, a double-degree Erasmus Mundus project; he spent the first year (2010-2011) at the University of Stellenbosch, South Africa, and the second year (2011-2012) at the University of Bordeaux, France – then Université de Bordeaux 1. He wrote his master thesis, with title “Schur products of linear codes: a study of parameters”, under the supervision of Professor Gilles Zémor from the University of Bordeaux, obtaining his master degree in 2012.

In 2012 he was awarded an ALGANT-Doc joint Ph.D. fellowship to continue his studies in Mathematics at Universiteit Leiden, the Netherlands, and Université de Bordeaux, under the supervision of Prof. Dr. Ronald Cramer and Prof. Dr. Gilles Zémor (Bordeaux), in cooperation with the Centrum Wiskunde & Informatica (CWI) of Amsterdam, the Netherlands.

Publications

- I. Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, 2015.
- II. Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information*

Theory, 61(3):1159–1173, March 2015.

- III. Diego Mirandola and Gilles Zémor. Critical Pairs for the Product Singleton Bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, Sept. 2015.