Des. Codes Cryptogr. (2015) 76:1–2
DOI 10.1007/s10623-015-0041-2

Foreword: Computer Algebra in Coding Theory and Cryptography

I. Kotsireas · Edgar Martínez-Moro

Published online: 10 February 2015

Computer algebra, coding theory and cryptography are areas that have evolved together, and there are many links and relationships between the three topics both in their pure and applied aspects. This volume contains eight papers covering a significant range of material and is a follow-up to the Special Session "Computer Algebra and Coding Theory 2013," hosted at ACA 2013 held at the University of Malaga, Spain, July 2–6, 2013. It is divided into three categories.

1. **General coding theory.** *In Efficient representation of binary nonlinear codes: constructions and minimum distance computation* M. Villanueva, F. Zeng and J. Pujol give a representation of a binary nonlinear code and compute its minimum distance from such a representation. The complexity of this approach is given in terms of the work factor. The paper *Heuristic Decoding of Linear Codes Using Commutative Algebra* by N. Dück and K.-H. Zimmermann shows a new heuristic decoding method based on the ordinary code ideal. In *Optimal codes as Tanner codes with cyclic component codes* the authors, T. Høholdt, F. Piñero and P. Zeng, study a class of graph codes with cyclic code component codes and they find some optimal binary codes.
2. **Algebraic geometry codes.** The paper *An improvement of the Feng-Rao bound for primary codes,* by O. Geil and S. Martin, poses a new bound for the minimum distance of a general primary linear code that in some families of codes is often an improvement on the Feng-Rao bound for primary codes. In *The second generalized Hamming weight of certain Castle codes*, W. Olaya-Léon and C. Granados-Pinzón examine a bound on the second generalized Hamming weight for some AG codes coming from Castle curves related to Weierstrass semigroups generated by two integers. The paper *Quantum codes*

I. Kotsireas
Department of Physics and Computer Science,
Wilfrid Laurier University, Waterloo N2L 3C5, Canada
e-mail: ikotsire@wlu.ca

E. Martínez-Moro (✉)
Institute of Mathematics and Applied Mathematics Department,
University of Valladolid, 42004 Castill, Spain
e-mail: edgar@maf.uva.es

from affine variety codes and their subfield-subcodes, by C. Galindo and F. Hernando, presents and analyzes a construction of quantum stabilizer codes from affine variety codes and their subfield-subcodes.

3. **Cryptography.** In *Hamming codes for wet paper steganography,* by C. Munuera, the author describes an application of Hamming codes to wet paper steganography with the remarkable property of using decoding algorithms that do not satisfy the minimum distance property. Finally, the paper *Theory of 2-rotation symmetric cubic Boolean functions*, by T. W. Cusick and B. Johns, provides a complete description of that family of Boolean functions.

We received a large number of submissions and we are thankful to the authors of all papers submitted to our special issue. Due to the high quality of submissions, the process of deciding which papers to accept was not easy and we are especially grateful to the expert referees for their crucial assistance in helping us compile the final selection of accepted papers. It is our belief that the valuable input of referees will have contributed in substantially improving the quality of all submissions, irrespective of whether they were accepted or rejected. It is also our hope that our special issue will contribute in further elucidating some of the intricate connections among computer algebra, coding theory and cryptography. Finally we would like to express our most sincere thanks to the DCC staff at Springer, for their tireless efforts and continuous support in helping us publish this special issue.