Des. Codes Cryptogr. (2014) 70:1–2
DOI 10.1007/s10623-012-9775-2

Editorial: 3rd International Castle Meeting on Coding Theory and Applications

Joaquim Borges · Mercè Villanueva · Victor Zinoviev

Received: 26 October 2012 / Accepted: 15 November 2012 / Published online: 8 December 2012

This volume contains 19 journal refereed papers devoted to coding, related topics and applications. These papers are the full journal versions of a selection of the communications presented at the *3rd International Castle Meeting on Coding Theory and Applications* (3ICMCTA-2011) held at Cardona Castle in Catalonia (Spain) on September 11–15, 2011.

After the revision of the Program Committee, 43 extended abstracts were selected for presentation at the workshop together with four invited talks. The authors of the presented papers were in turn invited to submit full versions of their papers to the *Designs, Codes and Cryptography* journal. Each of these submissions were again refereed by at least two reviewers. This special issue is the final result of all this process.

We are grateful to the reviewers for their hard work, which contributed to guarantee the high level of these papers. We would like to thank all the authors and all the participants of the 3ICMCTA for making the conference a highly enjoyable event. We also thank some institutions for their financial support: IEEE Information Theory Spanish Chapter, Spanish Ministry of Science and Innovation, Ingenio Mathematica (i-math), and Universitat Autònoma de Barcelona.

Algebraic Coding Theory has been one of the topics with more papers. *Bernal and Simón* study the relationship between two different constructions of information sets: one for every abelian code by means of its defining set; and another one for binary two-dimensional cyclic

Communicated by D. Jungnickel.

J. Borges (✉)· M. Villanueva
Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain
e-mail: joaquim.borges@autonoma.edu

M. Villanueva
e-mail: merce.villanueva@autonoma.edu

V. Zinoviev
Institute for Problems of Information Transmission, Russian Academy of Sciences, GSP-4, Bol'shoi Karetnyi per. 19, Moscow 127994, Russia
e-mail: zinov@iitp.ru

codes and binary abelian codes, based on the computation of Groebner basis. In the context of algebraic geometric codes, *Bras-Amoros and Vico-Oton* derive some results related to the Geil-Matsumoto bound, in particular, a closed formula for Weierstrass semigroups generated by two integers. *Feulner* prove the nonexistence of a $[21, 14, 6]$-code over F_4 and a $[16, 5, 10]$-code over F_5, which implies also some new upper bounds for minimum distance of linear codes of given length and dimension. *Ghinelli, Key, and McDonough* consider general methods for construction of codes with specific values of hulls from incidence matrices of graphs. *Malevich and Willems* prove that the known extremal self-dual doubly-even codes with 2-transitive automorphism group are the only such codes. *Pernas, Pujol, and Villanueva* study the order and structure of the permutation automorphism group of quaternary linear Hadamard codes. *Tomlinson, Jibril, Tjhai, Grassl, and Ahmed* present an efficient construction of extended Goppa codes, which leads to four new binary codes with better minimum distances.

Algorithmic Methods for solving problems in *Coding Theory* are investigated in some papers. *Piñero and Janwa* give a fast algorithm to compute the dimensions of subfield subcodes of Hermitian codes. Some of the subfield subcodes are at least as good as previously known codes and existence results are also derived. *Sidorenko and Bossert* propose a fast algorithm for the problem of skew-feedback shift-register synthesis for multiple sequences of varying lengths. This algorithm improves a previous version in terms of time complexity. Other papers are devoted to the computation of some parameters or the construction of codes. *Kampf* obtains the maximum decoding radius for interleaved Hermitian codes if a collaborative decoding scheme on a division algorithm is used. As a result, it is showed for which rates noninterleaved Hermitian codes can be decoded beyond half the minimum distance.

Cryptography has been the main subject on several papers. *Khan, Gabidulin, Honary, and Ahmed* propose an advanced approach for Niederreiter type GPT public key cryptosystem based on reducible rank codes. The proposed modification makes the system more secure against attacks. *Márquez-Corbella, Martínez-Moro, and Pellikaan* show that certain algebraic geometry codes are not secure if used in the McEliece public-key cryptosystems. Other works are related to applications on data storage. *Haymaker and Kelley* investigate the design and application of write-once memory (WOM) codes for use on multilevel flash memories. More specifically, they present a construction of WOM codes with new parameters based on finite Euclidean geometries.

Relationships between *Graph Theory and Coding Theory* is also the subject of some papers. *Auger, Cohen, and Mesnager* consider the covering problem in a simple, finite, connected graph by the minimum number of spheres with fixed radius and connected it to some other problems in combinatorics, in particular to identifying codes. *Araujo, Dejter, and Horak* introduce the notion of perfect distance-dominating set, PDDS, in a graph, which is a generalization of perfect Lee codes. *Borges, Rifà, and Zinoviev* construct new infinite families of binary linear completely regular codes with covering radius 3 and 4. These families induce also families of distance regular graphs with diameter 3 and 4. *Seneviratne* consider binary codes which can be obtained from designs associated with circulant graphs.

Some works investigate *Constructions* of some special classes of codes. *Galindo and Montserrat* construct codes of large size defined by weight functions obtained from finitely many weight functions defined by plane valuations at infinity. *Pinho, Pinto, and Rocha* investigate the problem of constructing minimal realizations of two-dimensional convolutional codes of rate $1/n$ by means of separable Roesser models.