Preface: geometry, combinatorial designs and cryptology

Arrigo Bonisoli · James Hirschfeld · Spyros Magliveras

Received: 28 December 2011 / Accepted: 30 December 2011 / Published online: 12 January 2012
© Springer Science+Business Media, LLC 2012

This issue of the journal is devoted to the themes of Geometry, Combinatorial Designs and Cryptology. The guest editors selected sixteen contributions covering various areas within these themes, ranging from public-key cryptography to matters related to key distribution and authentication, from problems in graph theory to resolvability issues in designs, from finite projective planes to higher-dimensional geometries. Many problems in these areas share common methods, including purely combinatorial techniques, but also algebraic methods for finite fields, geometric issues mainly involving incidence and collineations, and computational approaches.

The papers “Projective k -arcs and 2-level secret-sharing schemes” by Korchmáros–Lanzone–Sonnino (doi:[10.1007/s10623-011-9562-5](https://doi.org/10.1007/s10623-011-9562-5)), “Singer 8-arcs of Mathon type in $PG(2, 2^7)$ ” by De Clerck–De Winter–Maes (doi:[10.1007/s10623-011-9502-4](https://doi.org/10.1007/s10623-011-9502-4)) and “42-arcs in $PG(2, q)$ left invariant by $PSL(2, 7)$ ” by Indaco–Korchmáros (doi:[10.1007/s10623-011-9532-y](https://doi.org/10.1007/s10623-011-9532-y)) deal with arcs and address questions related to their construction, maximality and classification up to projective equivalence.

Polar spaces are the subject of the papers “Two forms related to the symplectic dual polar space in odd characteristic” by Cardinali–Pasini (doi:[10.1007/s10623-011-9545-6](https://doi.org/10.1007/s10623-011-9545-6)) and “Collineations of polar spaces with restricted displacements” by Temmermans–Thas–Van Maldeghem (doi:[10.1007/s10623-011-9509-x](https://doi.org/10.1007/s10623-011-9509-x)). In particular the description of these spaces in terms of forms and properties of their collineations are considered.

Communicated by J. D. Key.

A. Bonisoli (✉)
Università di Modena e Reggio Emilia, Modena, Italy
e-mail: arrigo.bonisoli@unimore.it

J. Hirschfeld
University of Sussex, Brighton, UK
e-mail: jwph@sussex.ac.uk

S. Magliveras
Florida Atlantic University, Boca Raton, FL, USA
e-mail: spyros@fau.edu

Embedding problems for the near polygon $\mathbb{H}_n$ into a projective space over the binary field are the subject of “A decomposition of the universal embedding space for the near polygon $\mathbb{H}_n$ ” by De Bruyn (doi:[10.1007/s10623-011-9533-x](https://doi.org/10.1007/s10623-011-9533-x)), while a review of the known constructions for finite self-dual generalized quadrangles is presented in “An essay on self-dual generalized quadrangles” by Payne–Thas (doi:[10.1007/s10623-011-9531-z](https://doi.org/10.1007/s10623-011-9531-z)). A more basic approach aimed at the development of a theory for quotients of geometries has been pursued in “Quotients of incidence geometries” by Cara–Devillers–Giudici–Praeger (doi:[10.1007/s10623-011-9488-y](https://doi.org/10.1007/s10623-011-9488-y)).

Circulant matrices are the subject of two papers, namely “Self-dual codes from circulant matrices” by Georgiou–Lappas (doi:[10.1007/s10623-011-9510-4](https://doi.org/10.1007/s10623-011-9510-4)) and “New restrictions on possible orders of circulant Hadamard matrices” by Leung–Schmidt (doi:[10.1007/s10623-011-9493-1](https://doi.org/10.1007/s10623-011-9493-1)). In the former, circulant matrices are used to construct linear codes and the conditions for them to be self-dual are given. In the latter, field descent methods are used to rule out many open cases of the circulant Hadamard matrix conjecture.

The paper “Irreducible pseudo 2-factor isomorphic cubic bipartite graphs” by Abreu–Labbate–Sheehan (doi:[10.1007/s10623-011-9522-0](https://doi.org/10.1007/s10623-011-9522-0)) characterizes a class of graphs in terms of the irreducible point-line symmetric configurations that were already introduced by Martinetti in the late 19th century.

The next three papers deal specifically with security issues. The setting of the article “Security of message authentication codes in the presence of key-dependent messages” by González Muñoz–Steinwandt (doi:[10.1007/s10623-011-9523-z](https://doi.org/10.1007/s10623-011-9523-z)) involves the possibility that an adversary can access tags of a message authentication code on key-dependent message inputs. The complexity of the construction of the 2^k -diamond structure is analyzed in the paper “On the complexity of the herding attack and some related attacks on hash functions” by Blackburn–Stinson–Upadhyay (doi:[10.1007/s10623-010-9481-x](https://doi.org/10.1007/s10623-010-9481-x)). Errors in previous estimates are corrected and a new approach based on random graphs is proposed. The third paper “Identity-based non-interactive key distribution with forward security” by Steinwandt–Suárez Corona (doi:[10.1007/s10623-011-9486-0](https://doi.org/10.1007/s10623-011-9486-0)) proposes a notion of forward security which is then analyzed for the random oracle model and is applied suitably to key-exchange.

The construction of pseudorandom sequences is as central as ever in cryptology and an algebraic technique using random covers for large finite groups, in particular elementary abelian 2-groups, is developed in “Pseudorandom number generators based on random covers for finite groups” by Marquardt–Svaba–Tran van Trung (doi:[10.1007/s10623-011-9485-1](https://doi.org/10.1007/s10623-011-9485-1)).

Finally, the paper “On quasigroups with few associative triples” by Grošek–Horák (doi:[10.1007/s10623-010-9482-9](https://doi.org/10.1007/s10623-010-9482-9)) proposes yet another cryptographic application of algebraic techniques, this time considering the weaker structure of a quasigroup and measuring how far from being a group it can be in terms of associativity and still produce interesting hash functions.

The guest editors believe that the papers appearing in this issue form a faithful state-of-the-art picture of some topics of current interest in the selected areas. They hope that these articles will stimulate further developments of the subject matter. They are grateful to authors and reviewers for contributing to this special issue.