Math.Comput.Sci. (2012) 6:107–108
DOI 10.1007/s11786-012-0116-7

Foreword

Ilias S. Kotsireas · Irene Márquez-Corbella · Edgar Martínez-Moro

Published online: 3 July 2012

This issue of *Mathematics in Computer Science* is a follow up of the special sessions on "Applications of Matroid Theory in Coding Theory" organized by I. Márquez-Corbella and E. Martínez-Moro at the 3rd Biennial Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM) held on May 31–June 3, 2011, at the University of Victoria, British Columbia, Canada. The volume includes a selection of research papers related to the applications of matroid theory in coding theory and cryptography. Since much of the work on the subject is still ongoing, the special issue encouraged authors not only to present recent results, but also to propose new guidelines and research insights as well as potential applications. We have grouped the accepted papers in two categories: (i) Foundations of Matroid Theory and Computation (3 papers) and (ii) Applications to Coding Theory and Cryptography (3 papers).

In the paper *Relations between Möbious and coboundary polynomial*, R. Jurrius considers the relation between the coboundary polynomial and the Möbius polynomial (also called Whitney polynomial) of a matroid. The main result proves that the Möbius polynomials of a matroid and its dual determine the coboundary polynomial of the matroid under the sufficient condition $2(d + d^*) \geq n + 3$, where n is the number of elements in the matroid and d and d' are the sizes of the smallest cocircuits and circuit, that is, for matroids that are close to the uniform matroid. Stated in terms of codes, this means codes that are close to MDS codes.

The paper *Truncation formulas for invariant polynomials of matroids and geometric lattices* by R. Jurrius and R. Pellikaan considers the truncation of matroids and geometric lattices. The authors show that the truncated matroid of a representable matroid is again representable and truncation formulas are given for the coboundary and Möbius polynomial of a geometric lattice and the spectrum polynomial of a matroid. These formulas generalize a result of T. Britz.

In *On Brylawski's generalized duality*, G. Gordon introduces a notion of duality (due to Brylawski) for arbitrary rank functions. This generalized duality allows for generalized operations and a generalized polynomial based

I. S. Kotsireas (✉)
Department of Physics and Computer Science,
Wilfrid Laurier University, Waterloo, ON, Canada
e-mail: ikotsire@wlu.ca

I. Márquez-Corbella (✉) · E. Martínez-Moro (✉)
Institute of Mathematics, University of Valladolid, Valladolid, Castilla, Spain
e-mail: imarquez@agt.uva.es

E. Martínez-Moro
e-mail: edgar@maf.uva.es

on the matroid Tutte polynomial that also satisfies a deletion–contraction recursion. The author also explores this duality for greedoids, antimatroids and demi-matroids.

We then have three papers that are related to Applications to Coding Theory and Cryptography.

In *Decomposition of Modular codes for computing test sets and graver basis*, I. Márquez Corbella and E. Martínez Moro propose a decomposition theory for codes defined over $\mathbb{Z}_q$. This theory provides a procedure to reduce the complexity of the algorithm proposed by the authors in a previous article for computing the set of codewords of minimal support using Gröbner bases.

The paper *On families of graphs of large cycle indicator, matrices of large order and key exchange protocols with nonlinear polynomial maps of small degree*, by U. Romańczuk and V. Ustimenko, studies the group theoretical protocol of Diffie–Hellman key exchange in the case of symmetrical group and the general Cremona group of polynomial automorphisms of a free module over arbitrary commutative ring. The algorithm is dependent on the choice of the base and thus the authors suggest fast algorithms for its generation. The method is based on properties of infinite families of graphs with large cycle indicator and families of graphs of large girth in particular. They also discuss some cryptographical applications of these maps.

Finally, in the paper *On the comparison of cryptographical properties of two different families of graphs with large cycle indicator* M. Klisowski and V. Ustimenko study some implementations of the public key algorithms based on simple algebraic graphs $A(n, K)$ and $D(n, K)$ defined over the same finite commutative ring K. They also study the family $A(n, q)$, $\mathrm{char} F_q \neq 2$ of connected graphs with large cycle indicator with the largest possible speed of growth. They exhibit computer simulations that demonstrates the advantage of public rules derived from $A(n, q)$ in comparison with symbolic algorithms based on graphs $D(n, q)$.

The number of papers submitted to this special issue demonstrates that there is an active and quite intense interest in this research area within Coding Theory. We thank the authors of all papers submitted. We also thank all the referees for their valuable assistance with improving the accepted papers and providing detailed and constructive feedback to the authors of rejected papers, as well as for their critical help with deciding which papers to include in this special issue. We do hope that this issue will help disseminate novel results and stimulate further interest in Matroid Theory and Coding Theory.