Editorial

Philippe Gaborit

XLIM-DMI,
University of Limoges,
123, Avenue Albert Thomas,
87000 Limoges, France
E-mail: gaborit@unilim.fr

Jon-Lark Kim*

Department of Mathematics,
University of Louisville,
328 Natural Sciences Building,
Louisville, KY 40292, USA
E-mail: jl.kim@louisville.edu
*Corresponding guest editor

Patrick Solé

Telecom ParisTech,
Dept COMELEC,
46, rue Barrault,
75013 Paris, France
E-mail: sole@telecom-paristech.fr

Isaac Woungang

Department of Computer Science,
Ryerson University,
Toronto, Ontario M5B 2K3, Canada
E-mail: iwoungan@scs.ryerson.ca

Biographical notes: Philippe Gaborit received a PhD from the University of Bordeaux in 1997. After a two years post-doc with Vera Pless in Chicago, he became an Associate Professor at the University of Limoges in 1999 and a Professor in 2008. His main research interests are cryptography, coding theory and security.

Jon-Lark Kim received his BS in Mathematics from POSTECH, Pohang, Korea, in 1993, an MS in Mathematics from Seoul National University, Korea, in 1997 and a PhD in Mathematics from the University of Illinois at Chicago, in 2002 under the guidance of Prof. Vera Pless. From 2002 to 2005, he was with the Department of Mathematics at the University of Nebraska – Lincoln as a Research Assistant Professor. Since 2005, he has been an Assistant Professor in the Department of Mathematics at the University of Louisville, Louisville, KY. He was awarded a 2004 Kirkman Medal of the Institute of Combinatorics

and its Applications. He is a Member of the Editorial Board of the *Int. J. Information and Coding Theory*. His areas of interest include algebraic coding theory and its applications to quantum coding, network coding and biological coding.

Patrick Solé received the Ingénieur and Docteur-Ingénieur degrees both from Telecom ParisTech, Paris, France, in 1984 and 1987, and the habilitation à diriger des recherches from the Université de Nice-Sophia Antipolis, France in 1993. He has held visiting positions in Syracuse University, Syracuse, NY, from 1987 to 1989, Macquarie University, Sydney, Australia, from 1994 to 1996, Lille University, Lille, France, from 1999 to 2000. From 1989 to 2009, he was a permanent Member of the CNRS Laboratory I3S, Sophia Antipolis, France, with the rank of Directeur de Recherche since 1996. In 2009, he joined Telecom ParisTech, LTCI. His research interests include coding theory (covering radius, codes over rings, convolutional codes), interconnection networks (graph spectra, expanders), vector quantisation (lattices) and cryptography (pseudorandom sequences). He is the recipient (jointly with Hammons, Kumar, Calderbank and Sloane) of the IEEE Information Theory Society Best Paper Award for 1995.

Isaac Woungang received his MSc and PhD, all in Mathematics from the Université du Sud, Toulon-Var, Toulon, France, in 1990 and 1994, respectively. In 1999, he received an MASc from INRS-Énergie, Matériaux et Télécommunications, University of Quebec in Montreal, Montreal, Canada. From 1999 to 2002, he worked as a Software Engineer at Nortel Networks, Ottawa, Canada. Since 2002, he has been with Ryerson University, where he is now an Associate Professor of Computer Science. In 2004, he founded DABNEL (the Distributed Applications and Broadband Networks Laboratory) R&D group, hosted at Ryerson University. His research interests include network security, computer communication networks, mobile communication systems and coding theory.

Professor Vera Pless has been preeminent in the development of much of the algebraic theory of error-correcting codes. She is well-known for 'Pless power moments' which are an infinite family of equations relating to the weight distribution of the code to the weight distribution of its dual code. This family, although equivalent to the MacWilliams equations, is particularly useful in showing uniqueness of certain solutions. She is the first person to start the classification of binary self-dual codes in 1972 and also find the Pless symmetry codes and new 5-designs in 1972. This classification problem has expanded to the classification of self-dual codes over finite fields and finite rings, one of the most active research areas.

She attended the University of Chicago at the age of 15 and received her PhD from Northwestern University in 1957 with a thesis on ring theory. After teaching at Boston University and researching at the Air Force Cambridge Research Laboratory, she joined the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago as a Full Professor in 1975 and taught there until her retirement in 2005. She has three children Nomi, Ben and Dan and three grandchildren.

She is the author of the well-known textbook *An Introduction to the Theory of Error-Correcting Codes* and coeditor of *Handbook of Coding Theory* and *Fundamentals of Error-Correcting Codes* with W. Cary Huffman. She published more than 100 research papers independently or with Sloane, Conway and Assmus. Currently, she is in the Editorial Board of *Journal of Combinatorial Theory, Series A and Finite Fields and Their*

Applications. She had 11 PhD students including Jon-Lark Kim and Xiang-Dong Hou in this Special Issue. She had three post-docs including Philippe Gaborit and Keith Mellinger in this Special Issue. She invited Patrick Solé for seminar talks and research collaboration.

We would like to mention one anecdote related to Vera. She had a small heart attack during the AMS-MAA joint meeting at Atlanta in January 2005. She went to the hospital immediately. Steven Dougherty, Reshma Ramadurai and Jon-Lark Kim visited her at the ward as they were at the conference as well. As soon as Vera saw Reshma, one of her master students from India, she said regretfully "Reshma, I might not teach the class for the first week". Later when the nurse entered, she was very surprised to see three people of such diverse age race and looks. Steven said to Vera "the nurse thinks that we are your children and that must be one strange gene pool". Vera then proceeded to grill the doctor on her condition as if it were a thesis defence. Finally, there were two doctors in the room and her daughter, who is a doctor, on the phone. Vera then ran a series of questions to all three doctors about her condition, demanding precise terminology for everything they said. After seven months, Vera retired.

In 2006, W. Cary Huffman and Jon-Lark Kim organised a special session on *Algebraic Coding Theory – Honouring the Retirement of Vera Pless* at AMS sectional meeting at Cincinnati. Vera's son, colleagues and students participated for the meeting and enjoyed the memorable moment. It brings this Special Issue of the *Int. J. Information and Coding Theory* (*IJICoT*) on *Algebraic and Combinatorial Coding Theory*, in Honour of the Retirement of Vera Pless. We accepted 18 papers in this Special Issue after a thorough and a critical review process by experts in the field. These papers are grouped into three series, all in 2010.

In this first Series of papers, the first paper is titled, 'On the construction of bent vectorial functions' and is authored by Claude Carlet and Sihem Mesnager. The authors have presented a comprehensive survey of bent vectorial functions and have introduced a generalisation of the known primary and secondary constructions of bent functions. They have also proposed some new constructions of such functions.

The second paper this Series is titled, 'Differential properties of power functions' and is authored by Céline Blondeau, Anne Canteaut and Pascale Charpin. The authors have investigated some properties of power permutations. They have derived the relationship between the differential spectrum of a power permutation and the weight enumerator of a cyclic code with two zeroes. They have also studied functions with a two-valued differential spectrum and have been able to compute the differential spectra of several infinite families of exponents.

The third paper in this Series is titled, 'Constructions of self-dual codes over finite commutative chain rings' and is authored by Steven T. Dougherty, Jon-Lark Kim and Hongwei Liu. In the paper, the authors have studied self-dual codes over chain rings and described their structure. They have also proposed a technique for constructing new self-dual codes from existing codes. Finally, the authors have extended this technique to self-dual codes over principal ideal rings by using the Chinese Remainder Theorem. From their study, they found the first examples of MDS self-dual codes of lengths 6 and 8 and near-MDS self-dual codes of length 10 over a certain chain ring, which is not a Galois ring.

The fourth paper in this Series is titled, 'Binomial moments for divisible self-dual codes' and is authored by Iwan M. Duursma. The author has proposed some improved upper bounds on the minimum distance of self-dual codes with all weights divisible by an integer greater than one. These bounds are derived from short relations with constant coefficients on suitable binomial moments of the codes.

The fifth paper in this Series is titled, 'There is no Euclidean self-dual quaternary [18,9,7] code' and is authored by Carlos Aguilar, Christophe Chabot and Philippe Gaborit. The authors proved that there is no Euclidean self-dual quaternary [18,9,7] code for the Hamming distance. Their proof is based on a generalisation of the balance principle to Euclidean self-dual quaternary codes. The authors also provided an updated table of Euclidean self-dual quaternary codes.

The sixth paper in this Series is titled, 'MDS self-dual codes of lengths 16 and 18' and is authored by T. Aaron Gulliver and Masaaki Harada. The authors proved that an MDS self-dual [16,8,9] code over GF(p), the finite field of p elements, exists for an odd prime number p, where p is an integer in the interval [23, 499]. They have constructed new MDS self-dual codes for the open cases, using two construction methods based on negacirculant matrices. Finally, the authors have also constructed MDS self-dual [18,9,10] codes over GF(p), for p = 53, 61, 73, 89 and 97.

The last paper in this Series is titled, 'Enumeration of AGL($\frac{m}{3}$,$\mathbb{F}_{p^3}$)-invariant extended cyclic codes' and is authored by Xiang-Dong Hou. The author has proposed methods for enumerating all linear codes of length p^m over $\mathbb{F}_{p^r}$ which are invariant under the affine linear group AGL($\frac{m}{e}$,$\mathbb{F}_{p^e}$) when e = 3.

We hope that readers will enjoy reading these papers and find them valuable. The readers are encouraged to contact the authors, if they need any further clarification regarding their works presented. We take this opportunity to express a few words of our thankfulness. We would like to thank all the authors for considering *IJICoT* as a medium for publishing their work. Also, we are very much thankful to many thoughtful, diligent, and timely referees for their support in reviewing all the papers.