Joaquim Borges and Mercè Villanueva (eds.)

3rd International Castle Meeting on Coding Theory and Applications

Universitat Autònoma de Barcelona
Servei de Publicacions
Bellaterra, 2011

Dades catalogràfiques recomanades pel Servei de Biblioteques
de la Universitat Autònoma de Barcelona

3rd International Castle Meeting on Coding Theory and Applications : [September 11-15, 2011, Cardona, Spain, organized by the Combinatorics, Coding and Security Group, Universitat Autònoma de Barcelona] / Joaquim Borges and Mercè Villanueva (eds.)— Bellaterra (Barcelona) : Universitat Autònoma de Barcelona. Servei de Publicacions, 2011. — (Congressos de la Universitat Autònoma de Barcelona; 5)

ISBN 978-84-490-2688-1

I. Borges, J. (Joaquim); Villanueva, M. (Mercè)
III. Col·lecció
1. Criptografia – Informàtica – Congressos
2. Codificació, Teoria de la – Congressos
519.71

Edició:
Universitat Autònoma de Barcelona
Servei de Publicacions
Edifici A. 08193 Bellaterra (Cerdanyola del Vallès). Spain
Tel. 93 581 10 22
Fax 93 581 32 39
sp@uab.cat
www.uab.cat/publicacions

Impressió: Impulso

ISBN 978-84-490-2688-1
Dipòsit legal: B.29.077-2011

Imprès a Espanya. Printed in Spain

3ICMCTA

September 11-15, 2011, Cardona, Spain
organized by the Combinatorics, Coding and Security Group
Universitat Autònoma de Barcelona

Steering Committee

Ángela I. Barbero	University of Valladolid, Spain
Øyvind Ytrehus	University of Bergen, Norway

Organizing Committee

Joaquim Borges, UAB	Co-chair of the Scientific Committee
Cristina Fernández, UAB	Co-chair of the Local Committee
Jaume Pujol, UAB	Co-chair of the Local Committee
Josep Rifà, UAB	Chair of the Steering Committee
Mercè Villanueva, UAB	Co-chair of the Scientific Committee

Local Committee

Muhammad Bilal	UAB, Spain
Bernat Gastón	UAB, Spain
Jaume Pernas	UAB, Spain
Marta Pujol	UAB, Spain
Lorena Ronquillo	UAB, Spain

Sponsoring Institutions

Catalan Research Agency AGAUR
IEEE Information Theory Society
SARE-Consolider Ingenio 2010 Project
Spanish Ministry of Science and Innovation
Universitat Autònoma de Barcelona

Scientific Committee

Peter Beelen	Technical University of Denmark, Denmark
Juergen Bierbrauer	Michigan Technological University, USA
Maria Bras-Amorós	Universitat Rovira i Virgili, Spain
Claude Carlet	University of Paris VIII, France
Gérard Cohen	Telecom ParisTech, France
Italo Dejter	University of Puerto Rico, USA
Alexandros Dimakis	University of Southern California, USA
Steven Dougherty	University of Scranton, USA
Iwan Duursma	University of Illinois, USA
Cristina Fragouli	École polytechnique Fédérale de Lausanne, Switzerland
Heeralal Janwa	University of Puerto Rico, USA
San Ling	Nanyang Technological University, Singapore
Edgar Martínez-Moro	Universidad de Valladolid, Spain
Patric Östergard	Aalto University, Finland
Ruud Pellikaan	Eindhoven University of Technology, Netherlands
Kevin T. Phelps	Auburn University, USA
Ángel del Río	Universidad de Murcia, Spain
Eirik Rosnes	University of Bergen, Norway
Patrick Solé	Telecom ParisTech, France
Emina Soljanin	Bell Labs New Jersey, USA
Faina I. Solov'eva	Sobolev Institute of Mathematics, Russia
Jos Weber	Delft University of Technology, Netherlands
Victor A. Zinoviev	Institute for Problems of Information Transmission, Russia

External Reviewers

Ezio Biglieri
Stanislav Bulygin
Pierre-Louis Cayrel
Lara Dolecek
Mark Flanagan
Ryan Gabrys
Iiro Honkala
Carmelo Interlando
Denis S. Krotov
Antoine Lobstein
Carmen Martínez
Carlos Munuera
Irene Márquez Corbella
Frederique Oggier
Carla Ràfols
Bernardo G. Rodrigues
Leo Storme
Horacio Tapia Recillas

Table of Contents

Invited speakers

Communications

Preface

The *III International Castle Meeting on Coding Theory and Applications* has been held at Cardona Castle in Catalonia (Spain) on September 11-15, 2011. It was organized by the research group CCSG (Combinatorics, Coding and Security Group) from the Universitat Autònoma de Barcelona. The main objectives of the conference were the communication of scientific and technological results, the cooperation among research groups at an international level, and the promotion of young pre-doc and post-doc researchers on the topics of the conference.

The present *Proceedings* contain the extended abstracts of 4 invited talks and 43 communications. The previous review process assures the high quality of these works. It is remarkable the international character of the conference, since there were participants, invited speakers, steering committee, organizing committee, scientific committee and local committee members from 22 different countries.

The organizing committee thanks to all for their contribution, specifically, to the steering and scientific committees, as well as to the people out of these committees helping in the reviewing process, to the 4 invited speakers and to all the participants. Also, the conference has been possible thanks to the financial support of the following institutions: IEEE Information Theory Society, Spanish Ministry of Science and Innovation, Catalan Research Agency AGAUR, and Universitat Autònoma de Barcelona.

We are also grateful with the journal *Designs, Codes and Cryptography* for accepting to publish a full version of the more excellent papers presented at the conference.

September 2011

Joaquim Borges
Mercè Villanueva
Co-chairs of the Scientific Committee

Managing Interference

Robert Calderbank

`calderbk@math.princeton.edu`
Duke University, USA

1 Extended abstract

We consider a framework for full-duplex communication in ad-hoc wireless networks recently proposed by Dongning Guo. An individual node in the wireless network either transmits or it listens to transmissions from other nodes but it cannot to both at the same time. There might be as many nodes as there are 48 bit MAC addresses but we assume that only a small subset of nodes contribute to the superposition received at any given node in the network.

We use ideas from compressed sensing to show that simultaneous communication is possible across the entire network. Our approach is to manage interference through configuration rather than to eliminate or align it through extensive exchange of fine-grained Channel State Information. Our approach to configuration makes use of old fashioned coding theory.

Error-correcting Codes in the Projective Space*

Tuvi Etzion

`etzion@cs.technion.ac.il`
Technion — Israel Institute of Technology, Israel

1 Extended abstract

Let $\mathbb{F}_q$ be the finite field of order q, and let $\mathcal{W}$ be an arbitrary (fixed) vector space of dimension n over $\mathbb{F}_q$. Since $\mathcal{W}$ is isomorphic to $\mathbb{F}_q^n$, we can assume that $\mathcal{W}$ is in fact $\mathbb{F}_q^n$. The *projective space* of order n over $\mathbb{F}_q$, denoted herein by $\mathcal{P}_q(n)$, is the set of all the subspaces of $\mathbb{F}_q^n$, including $\{\mathbf{0}\}$ and $\mathbb{F}_q^n$ itself. Given a nonnegative integer $k \leq n$, the set of all subspaces of $\mathbb{F}_q^n$ that have dimension k is known as a *Grassmannian*, and usually denoted by $\mathcal{G}_q(n,k)$. Thus $\mathcal{P}_q(n) = \cup_{0 \leq k \leq n} \mathcal{G}_q(n,k)$. It is well known that

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \stackrel{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the *q-ary Gaussian coefficient*. It turns out that the natural measure of distance, the *subspace distance* in $\mathcal{P}_q(n)$, is given by

$$d_S(X,Y) \stackrel{\text{def}}{=} \dim(X) + \dim(Y) - 2\dim(X \cap Y)$$

for all $X, Y \in \mathcal{P}_q(n)$. It is well known (cf. [1,2]) that the function above is a metric; thus both $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$ can be regarded as metric spaces. Given a metric space, one can define codes. We say that $\mathbb{C} \subseteq \mathcal{P}_q(n)$ is an (n,M,d) *code in projective space* if $|\mathbb{C}| = M$ and $d_S(X,Y) \geq d$ for all $X, Y \in \mathbb{C}$. If an (n,M,d) code $\mathbb{C}$ is contained in $\mathcal{G}_q(n,k)$ for some k, we say that $\mathbb{C}$ is an (n,M,d,k) code. An (n,M,d,k) code is also called a *constant dimension code*.

The (n,M,d), respectively (n,M,d,k), codes in projective space are akin to the familiar codes in the Hamming space, respectively (constant weight) codes in the Johnson space, where the Hamming distance serves as the metric. There are, however, important differences. For all q, n and k, the metric space $\mathcal{G}_q(n,k)$ corresponds to a distance-regular graph, similar

---

* This research was supported in part by the United States — Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2006097.

Finally, some more results, new related references, and a list of open problems for further research are given.

References

1. R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, *On perfect codes and related concepts, Designs, Codes, and Cryptography,* 22 (2001), 221–237.
2. R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding, IEEE Trans. Inform. Theory,* IT-54 (2008), 3579–3591.
3. L. Chihara, *On the zeros of the Askey-Wilson polynomials, with applications to coding theory, SIAM J. Math. Anal.,* 18 (1987), 191–207.
4. W. J. Martin and X. J. Zhu, *Anticodes for the Grassman and bilinear forms graphs, Designs, Codes, and Cryptography,* 6 (1995), 73–79.
5. M. Schwartz and T. Etzion, *Codes and anticodes in the Grassman graph, Journal of Combinatorial Theory, Series A,* 97 (2002), 27–42.
6. T. Etzion and A. Vardy, *Error-correcting codes in projective space,* in *Proc. ISIT 2008,* Toronto (2008), 871–875.
7. T. Etzion and A. Vardy, *Error-correcting codes in projective space, IEEE Trans. Inform. Theory,* IT-57 (2011), 1165–1173.
8. A. Kohnert and S. Kurz, *Construction of large constant dimensiona codes with a prescribed minimum distance, Lecture Notes in Computer Science,* 5393 (2008), 31–42.
9. D. Silva, F. R. Kschischang, and R. Koetter *A Rank-metric approach to error control in random network coding, IEEE Trans. Inform. Theory, Series A,* IT-54 (2008), 3951–3967.
10. S. T. Xia and F. W. Fu, *Johnson type bounds on constant dimension codes, Designs, Codes, Designs, Codes, and Cryptography,* 50 (2009), 163–172. *IEEE Trans. Inform. Theory,* IT-56 (2010), 3207–3216.
11. M. Gadouleau and Z. Yan, *Packing and covering properties of subspace codes for error control in random linear network coding, IEEE Trans. Inform. Theory,* IT-56 (2010), 2097–2108.
12. M. Gadouleau and Z. Yan, *Constant-rank codes and their connection to constant-dimension codes, IEEE Trans. Inform. Theory,* IT-56 (2010), 3207–3216.
13. P. Frankl and R. M. Wilson, *The Erdos-Ko-Rado theorem for vector spaces, Journal of Combinatorial Theory, Series A,* 43 (1986), 228–236.
14. S. Thomas, *Designs over finite fields, Geom. Dedicata,* 21 (1987), 237–242.
15. S. Thomas, *Designs and partial geometries over finite fields, Geom. Dedicata,* 63 (1996), 247–253.
16. H. Suzuki, *2-designs over $\mathrm{GF}(2^m)$, Graphs Combin.,* 6 (1990), 293–296.
17. H. Suzuki, *2-designs over $\mathrm{GF}(q)$, Graphs Combin,* 8 (1992), 381–389.
18. M. Miyakawa, A. Munemasa and S. Yoshiara, *On a class of small 2-designs over $\mathrm{GF}(q)$, Journal Combinatorial Designs,* 3 (1995), 61–77.
19. T. Itoh, *A new family of 2-designs over $\mathrm{GF}(q)$ admitting $\mathrm{SL}_m(q^\ell)$, Geom. Dedicata,* 69 (1998), 261–286.
20. H. Wang, C. Xing, and R. M. Safavi-Naini, *Linear authentication codes: bounds and constructions, IEEE Trans. Inform. Theory,* IT-49 (2003), 866–872.
21. M. Braun, A. Kerber and R. Laue, *Systematic construction of q-analogs of t-(v,k,λ)-designs, Designs, Codes, and Cryptography,* 34 (2005), 55–70.
22. C. Bachoc, *Semidefinite programming, harmonic analysis, and coding theory,* in Lecture Notes *CIMPA Summer School on Semidefinite Programming in Algebraic Combinatorics,* (2009), 1–47.
23. T. Etzion and N. Silberstein, *Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams, IEEE Trans. Inform. Theory,* IT-55 (2009), 2909–2919.
24. P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory, Journal of Combinatorial Theory, Series A,* 25 (1978), 226–241.

25. E. M. Gabidulin, *Theory of codes with maximum rank distance*, *Problems of Information Transmission,* 21 (1985), 1–12.
26. R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction*, *IEEE Trans. Inform. Theory,* IT-37 (1991), 328–336.
27. A.-L. Trautmann and J. Rosenthal, *New improvements on the echelon-Ferrers construction,* in *Proc. Int. Symp. on Math. Theory of Networks and Systems,* (2010), 405–408.
28. N. Silberstein and T. Etzion, *Large constant dimension codes and lexicodes*, *Advances in Mathematics of Communications,* 5 (2011), 177-189.
29. N. Silberstein and T. Etzion, *Codes and designs related to lifted MRD codes,* to be presented in *Proc. ISIT 2011,* Saint Petersburg (2011).
30. T. Etzion and A. Vardy, *On q-Analogs for Steiner Systems and Covering Designs*, *Advances in Mathematics of Communications,* 5 (2011), 161-176.

On Old and New Results in Algebraic Coding Theory over Ring Alphabets

Marcus Greferath

`marcus.greferath@ucd.ie`
University College Dublin, Ireland

1 Extended abstract

Ring-linear algebraic coding theory gained importance during the last decade of the previous century, when it was discovered that certain non-linear binary codes of high quality can be better understood as linear codes over the ring of integers modulo 4.

Since then, a number of workgroups worldwide have been doing research in this new discipline of Applicable Algebra. Their results suggest that most of the foundational questions of algebraic coding over rings have been settled by now, whereas strong examples of record-breaking codes are still in demand.

This talk gives some insight into this amazingly beautiful chapter of Discrete Mathematics. We will report on a collection of results from the literature and from our own previous and current research. The talk will finish with open problems and projects for future research.

Codes from Incidence Matrices of Graphs

Jennifer D. Key

keyj@clemson.edu
University of the Western Cape, South Africa

1 Introduction

An incidence matrix for an undirected graph $\Gamma = (V, E)$ is a $|V| \times |E|$ matrix $G = [g_{X,e}]$ with rows labelled by the vertices $X \in V$ and columns by the edges $e \in E$, where $g_{X,e} = 1$ if $X \in e$, $g_{X,e} = 0$ if $X \notin e$.

For any prime p let $C_p(G)$ denote the row span of G over $\mathbb{F}_p$ from a graph Γ. In a number of recent papers, for example [5,4,7,12,13], the codes $C_p(G)$ for some classes of regular connected graphs were studied. It was found that for these classes the codes have parameters

$$[|E|, |V| - \varepsilon_p, \delta(\Gamma)]_p$$

where $\varepsilon_2 = 1$, $\varepsilon_p = 0, 1$ for p odd, $\delta(\Gamma)$ is the minimum degree of Γ, and the words of minimum weight are precisely the non-zero scalar multiples of the rows of G of weight $\delta(\Gamma)$. In particular when Γ is k-regular and so $\delta(\Gamma) = k$, this implies that in these cases the graph can be retrieved from the code. Furthermore, in some of the classes, these properties led to similar facts for the binary codes of the adjacency matrices of the associated line graphs, these being subcodes of the binary codes from the incidence matrices of the original graphs. Indeed, it was a study of the codes from the adjacency matrices of triangular graphs in [11] that pointed to this focus on the incidence matrices.

In addition, it was noticed that the weight enumerator of the code of the incidence matrix had, in all cases studied, a gap between the weight k for the valency, and $2k - 2$ for the difference of two rows, i.e. the valency of the line graph. This then immediately shows that, in these cases, the binary code of an adjacency matrix of the line graph of a graph Γ has the property that the minimum weight is either the valency of Γ or the valency of the line graph; in the latter case, that the words of that weight are the rows of the adjacency matrix might not necessarily follow, but does in fact seem to be true in most of the classes studied.

The question was thus asked whether these properties are in fact general for graphs satisfying certain conditions. We make a start at answering this question here by using the concept of edge-connectivity to show that this is indeed the case for many classes of graphs. We outline this method and some of the results obtained in Section 3, but first we mention, in Section 2 below, the classes studied that led to this observation.

2 Classes of graphs studied previously

Infinite classes of graphs studied and found, by combinatorial and coding theoretic methods, along with induction, to have the properties described for $C_p(G)$, G an incidence matrix, include:

- Hamming graphs $H^k(n,m)$ (see [5,4])
  The Hamming graph $H^k(n,m)$, for n,k,m integers, $1 \leq k < n$, is the graph with vertices the m^n n-tuples of R^n, where R is a set of size m, and adjacency defined by two n-tuples being adjacent if they differ in k coordinate positions. They are the graphs from the Hamming association scheme. In particular, the n-cube: $\mathcal{Q}_n = H(n,2) = H^1(n,2)$ $(R = \mathbb{F}_2)$.
- Uniform subset graphs $\Gamma(n,k,m)$
  A uniform subset graph $\Gamma(n,k,m)$ has vertex set $\Omega^{\{k\}}$, where $|\Omega| = n$, and adjacency defined by $a \sim b$ if $|a \cap b| = m$. The symmetric group S_n always acts on these graphs. All classes studied satisfy the properties described, and include:
    - the odd graphs $\Gamma(2k+1,k,0)$ (see [2])
    - triangular graphs $\Gamma(n,2,1)$ (strongly regular) and $\Gamma(n,2,0)$ (see [6])
    - $\Gamma(n,3,m)$ for $m = 0,1,2$. (see [3])
- Complete multipartite graphs $K_{n_1,n_2,\ldots,n_k}$
    - K_n the complete graph (see [12])
    - $K_{n,n}$ the complete bipartite graph (see [13,14])
    - $K_{n,m}$ for $n \neq m$
    - $K_{n_1,n_2,\ldots,n_k}$ where $n_i = n$ for $i = 1,\ldots,k$
- Strongly regular graphs (n,k,λ,μ)
  A k-regular graph $\Gamma = (V,E)$ with $|V| = n$ is strongly regular with parameters $(n,k,\lambda,$ $\mu)$ if
    - for any $P,Q \in V$ such that $P \sim Q$, $|\{R \in V \mid R \sim P \,\&\, R \sim Q\}| = \lambda$, and
    - for any $P,Q \in V$ such that $P \not\sim Q$, $|\{R \in V \mid R \sim P \& R \sim Q\}| = \mu$.

  The classes found to have the described property include:
    - Triangular graphs $T(n) = L(K_n)$, (line graph of the complete graph, also a uniform subset graph), $n \geq 4$, $(\binom{n}{2}, 2(n-2), n-2, 4)$ (see [12])
    - Paley graphs $P(q)$, vertex set $\mathbb{F}_q$ where $q \equiv 1 \pmod 4$ and $x \sim y$ if $x - y$ is a non-zero square, $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ (see [7])
    - Lattice graphs $L_2(n) = L(K_{n,n})$, the line graph of the complete bipartite graph, $(n^2, 2(n-1), n-2, 2)$ (see [14])
    - Symplectic graphs (see [10]):
      $\Gamma_{2m}(q)$ with parameters $(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-2}-1}{q-1} - 2, \frac{q^{2m-2}-1}{q-1})$
      and complement
      $\Gamma^c_{2m}(q)$ with parameters $(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-2}(q-1), q^{2m-2}(q-1))$
      where $m \geq 2$, q a prime power.