The First Colombian Workshop on Coding Theory (CWC)

November 24-27, 2015

Universidad del Norte

Barranquilla, Colombia

Organizers

Javier de la Cruz, Universidad del Norte
Wilson Olaya, Universidad Industrial de Santander
Joachim Rosenthal, University of Zurich
Wolfgang Willems, University of Magdeburg
Welcome from the organizing committee

It is a pleasure to welcome everyone to CWC 2015, the first Colombian Workshop in Coding theory, which takes place at Universidad del Norte, Barranquilla, Colombia. The aim of this conference is to bring together researchers working in error correcting codes, network coding and related topics.

We are very proud that many worldwide experts agreed to attend the event. Apart from Europe and the USA a large variety of talks are from Colombia, Brazil and Argentina, which indicates that coding theory is a real issue in South America. Thus we believe that the conference will strengthen the collaboration between all these countries.

The event is organized by the Departamento de Matemáticas y Estadísticas de la Universidad del Norte. The organizers would like to thank the Dean of the College of Science, Joachim Hahn for the generous support provided by Uninorte. Thanks goes also to the University of Magdeburg, Germany, the University of Zurich, Switzerland and the Universidad Industrial de Santander for their respective support.

Once again, welcome to the Caribe and have a great time during your stay.

Javier de la Cruz
Wilson Olaya
Joachim Rosenthal
Wolfgang Willems
List of the Speakers

I. Invited Speakers

- Anton Betten, Colorado State University-U.S.A.
  betten@math.colostate.edu
- Diana Bueno-Carreño, Pontificia Universidad Javeriana Cali-Colombia.
  dbbueno@javerianacali.edu.co
- Joan-Josep Climent, Universitat d’Alacant-Spain.
  jcliment@ua.es
- Andreas Faldum, University of Münster-Germany.
  Andreas.Faldum@ukmuenster.de
- Marcelo Firer, State University of Campinas-Brazil.
  mfrer@ime.unicamp.br
- J. Carmelo Interlando, San Diego State University-U.S.A.
  interlan@mail.sdsu.edu
- Felice Manganiello, Clemson University-U.S.A.
  manganm@clemson.edu
- Edgar Martínez-Moro, University of Valladolid-Spain.
  edgar@maf.uva.es
- Diego Napp, University of Aveiro-Portugal.
  diegonapp@gmail.com
- Gabriele Nebe, RWTH Aachen University-Germany.
  gabriele.nebe@rwth-aachen.de
- Michael E. O’Sullivan, San Diego State University-U.S.A.
  mosullivan@mail.sdsu.edu
- Alberto Ravagnani, Université de Neuchâtel-Switzerland.
  alberto.ravagnani88@gmail.com
- Ángeles Vazquez-Castro, Universitat Autònoma de Barcelona-Spain.
  Angeles.Vazquez@uab.es
- Alfred Wassermann, University of Bayreuth-Germany.
  alfred.wasserman@uni-bayreuth.de

II. Contributed Speakers

- Carina Alves, Sao Paulo State University-Brazil
  carina@rc.unesp.br
- Sara D. Cardell, State University of Campinas-Brazil
  sdcardell@ime.unicamp.br
• Sueli I. R. Costa, University of Campinas-Brazil
  sueli@ime.unicamp.br

• Mario E. Duarte Gonzalez, University of Campinas-Brazil
  mduarte@dt.fee.unicamp.br

• Luis R. Fuentes Castilla, Universidad de Puerto Rico-U.S.A.
  luis.fuentes3@upr.edu

• Mehdi Garrousian, Universidad de los Andes-Colombia
  m.garrousian@uniandes.edu.co

• Grasiele C. Jorge, Federal University of São Paulo-Brazil
  grasiele.jorge@unifesp.br

• Anastacia Lonodoño, Universidad de los Andes-Venezuela
  anas.2720@gmail.com

• Carlos Alberto López-Andrade, Benemérita Universidad Autónoma de Puebla-Mexico
  clopez@fcfm.buap.mx

• Roberto A. Machado, State University of Campinas-Brazil
  guilherme@famat.ufu.br

• Gabriella Akemi Miyamoto, State University of Campinas-Brazil
  gabriellaakemimiyamoto@gmail.com

• Wilson Olaya-León, Universidad Industrial de Santander-Colombia
  wolaya@uis.edu.co

• Anderson Oliveira, State University of Campinas-Brazil
  anderson.oliveira@unifal-mg.edu.br

• Fernando L. Piñero, Indian Institute of Technology Bombay-India
  ferpi@math.iitb.ac.in

• Ricardo Podesta, Universidad de Córdoba-Argentina
  podesta@famaf.unc.edu.ar

• Claudio Qureshi, Universidade Estadual de Campinas-Brazil
  cquiresi@gmail.com

• Alonso Sepúlveda Castellanos, University Federal of Uberlândia-Brazil
  alonso@famat.ufu.br

• Klara Stokes, University of Skövde-Sweden
  klara.stokes@his.se

• Guilherme Tizziotti, University Federal of Uberlândia-Brazil
  guilherme@famat.ufu.br

• Vladimir Tonchev, Michigan Technological University-U.S.A.
  tonchev@mtu.edu

• Kasra Vakilinia, University of California, Los Angeles-U.S.A.
  vakiliniak@ucla.edu
# I. Conference Program

**Tuesday, Nov. 24, 2015**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 - 8:20</td>
<td>Registration</td>
<td>Lobby of Block G</td>
</tr>
<tr>
<td>8:30 - 9:15</td>
<td>Opening</td>
<td>31K</td>
</tr>
</tbody>
</table>

**Invited talks**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:20 - 10:05</td>
<td>Edgar Martinez</td>
<td>31K</td>
</tr>
<tr>
<td></td>
<td>Polynomials codes on PIPQR’s, A biased introduction to codes over rings</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:20 - 11:05</td>
<td>Anton Betten</td>
<td>Proyecciones</td>
</tr>
<tr>
<td></td>
<td>Classification of codes and combinatorial structures</td>
<td></td>
</tr>
</tbody>
</table>

**Coffee break**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:30 - 12:15</td>
<td>Gabriele Nebe</td>
<td>Proyecciones</td>
</tr>
<tr>
<td></td>
<td>Automorphisms of extremal lattices</td>
<td></td>
</tr>
</tbody>
</table>

**Lunch**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:15-15:00</td>
<td>Angeles Vázquez-Castro</td>
<td>Proyecciones</td>
</tr>
<tr>
<td></td>
<td>A geometric approach to dynamic network coding</td>
<td></td>
</tr>
</tbody>
</table>

**Coffee break**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:00-15:20</td>
<td>Carina Alves</td>
<td>22 G1</td>
</tr>
<tr>
<td></td>
<td>Construction of dense lattices from cyclic division algebras</td>
<td></td>
</tr>
<tr>
<td>15:30-16:00</td>
<td>Ricardo Podestá</td>
<td>23 G1</td>
</tr>
<tr>
<td></td>
<td>Cyclicity and asymptotic behavior of algebraic geometry codes</td>
<td></td>
</tr>
<tr>
<td>16:10-16:40</td>
<td>Grisiele Jorge</td>
<td>24 G1</td>
</tr>
<tr>
<td></td>
<td>On rotated $D_n$-lattices via number fields</td>
<td></td>
</tr>
<tr>
<td>16:50-17:20</td>
<td>Alonso Sepulveda C.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generalized Hamming weight over the GH curve</td>
<td></td>
</tr>
<tr>
<td>17:30-18:00</td>
<td>Sueli Costa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lattices and spherical codes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wilson Olaya-Léon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The rank MDS of hermitian codes</td>
<td></td>
</tr>
</tbody>
</table>
### Invited talks

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 - 9:45</td>
<td>Michael O’Sullivan</td>
<td>The combinatorics of conditional independence</td>
</tr>
<tr>
<td>9:55 - 10:40</td>
<td>Joan-Josep Climent</td>
<td>Maximum distance separable 2D convolutional codes based on superregular matrices</td>
</tr>
</tbody>
</table>

**Chair:**
- F. Manganiello
- Gabriele Nebe

---

### Contributed talks

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:40-11:10</td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td>11:00-11:30</td>
<td>Fernando Piñero:</td>
<td>Basic parameters and Schubert cell codes</td>
</tr>
<tr>
<td></td>
<td>Carlos Lopez-Andrade:</td>
<td>On the Gray map images of codes over Galois rings and finite chain rings</td>
</tr>
<tr>
<td></td>
<td>Roberto Assis Machado:</td>
<td>Characterization of metrics induced by hierarchical posets</td>
</tr>
<tr>
<td>11:50-12:20</td>
<td>Sara D. Cardell:</td>
<td>Performance of SPC product codes through graph theory</td>
</tr>
<tr>
<td></td>
<td>Mario Duarte Gonzalez:</td>
<td>Identification of Proteins as codewords of cyclic codes over finite ring with identity</td>
</tr>
<tr>
<td></td>
<td>Claudio Qureshi:</td>
<td>Perfect q-ary codes under the Chebyshev metric</td>
</tr>
</tbody>
</table>

**Chairs:**
- Ricardo Podestá: Section 1 Room: 22 G1
- Guilherme Tizziotti: Section 2 Room: 23 G1
- Mehdi Garrousian: Section 3 Room: 24 G1

---

### Invited talks

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:20 - 15:05</td>
<td>Alberto Ravagnani</td>
<td>Weight distribution of rank-metric codes</td>
</tr>
<tr>
<td>15:15 - 16:10</td>
<td>Carmelo Interlando</td>
<td>Lattice packing from certain p-extensions of Q</td>
</tr>
</tbody>
</table>

**Chair:**
- Gabriele Nebe
- Edgar Martínez

---

### Contributed talks

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:10-16:30</td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td>16:30-17:00</td>
<td>Klara Stokes:</td>
<td>Geometric decoding of subspace codes</td>
</tr>
<tr>
<td></td>
<td>Kasra Vakilina:</td>
<td>RCA analysis of polar codes and the use of feedback to aid polarization at short block lengths</td>
</tr>
<tr>
<td></td>
<td>Vladimir Tonchev:</td>
<td>The weight distribution of the self-dual [124,64] polarity design code</td>
</tr>
<tr>
<td>17:10-17:40</td>
<td>Gabriella Miyamoto:</td>
<td>Geometrically uniform subspace codes</td>
</tr>
<tr>
<td></td>
<td>Anderson Oliveira:</td>
<td>The relationship between Riemann surface and Fuchsian differential equation with the aim at coding of geodesics</td>
</tr>
<tr>
<td></td>
<td>Anastacia Londoño:</td>
<td>MDS Conjecture over prime fields</td>
</tr>
</tbody>
</table>
Friday, Nov. 27, 2015

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 - 9:45</td>
<td>Diego Napp</td>
<td>Distance properties of convolutional codes over $\mathbb{Z}_p$</td>
</tr>
<tr>
<td>Chair: Klara Stokes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:55 - 10:40</td>
<td>Felice Manganiello</td>
<td>Theory and applications of skew polynomial rings</td>
</tr>
<tr>
<td>Chair: Ángeles Vazquez-Castro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:40-11:10</td>
<td>Coffee break</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:10 - 11:55</td>
<td>Alfred Wassermann</td>
<td>LCD codes from matrix groups</td>
</tr>
<tr>
<td>Chair: Michael O’Sullivan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00 - 12:30</td>
<td>Andreas Faldum</td>
<td>Coded patient identifier in medicine</td>
</tr>
<tr>
<td>Chair: Joan-Josep Climent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30 - 14:30</td>
<td>Lunch</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:30 - 15:15</td>
<td>Diana Bueno</td>
<td>An algorithm to compute the apparent distance of an abelian code</td>
</tr>
<tr>
<td>Chair: Anton Betten</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:20 - 16:05</td>
<td>Marcelo Firer</td>
<td>Posets, graphs, blocks and other generalizations of the Hamming metric</td>
</tr>
<tr>
<td>Chair: Alberto Ravagnani</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
II. Minicourse Program

<table>
<thead>
<tr>
<th>Humberto Sarria Zapata</th>
<th>Room: 31 G2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Una introducción a la teoría de la información</td>
<td></td>
</tr>
<tr>
<td>15:30 - 17:30 Tuesday</td>
<td>Section 1</td>
</tr>
<tr>
<td>Las medidas de la información</td>
<td></td>
</tr>
<tr>
<td>11:10- 12:40 Wednesday</td>
<td>Section 2</td>
</tr>
<tr>
<td>Desigualdades de la información</td>
<td></td>
</tr>
<tr>
<td>16:30- 18:00 Wednesday</td>
<td>Section 3</td>
</tr>
<tr>
<td>La región entrópica. Una breve introducción a la teoría de códigos</td>
<td></td>
</tr>
</tbody>
</table>

III. Student contributed talk

<table>
<thead>
<tr>
<th>Diana Mejía</th>
<th>Room: 31 G2</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:30 - 18:00 Tuesday</td>
<td>On the binary self-dual [144, 72, 28] code</td>
</tr>
</tbody>
</table>

IV. Social Program

Wednesday, Nov. 25, 2015
18:30-19:15 Carneval Barranquilla show at Restaurant 1966
19:30-20:30 Cocktail at Restaurant 1966

Thursday, Nov. 26, 2015, Excursion to Cartagena (pre-registration required)
07:45-08:00 Meeting (Hotel Four Points by Sheraton)
08:00-10:00 Barranquilla-Cartagena Travel
10:00-12:30 Cocktail and Beach at Hotel
12:30-14:00 Lunch
14:00-16:30 Beach at Hotel (Free time)
16:30-20:00 Walk in the old town (Ciudad amurallada)
20:00-22:00 Cartagena-Barranquilla travel

Friday, Nov. 27, 2015
19:00-22:00 Cocktail at Bondi Beach Club.
IV. Book Abstract
Polynomial codes on PIPQR’s
A biased introduction to codes over rings

Edgar Martínez-Moro
University of Valladolid-Spain
edgar@maf.uva.es

In this talk we will introduce the basic facts about codes over finite rings. This introduction will be biased towards the study of polynomial codes over principal ideal polynomial quotient rings with applications to additive modular codes. Finally (if we have time) we will end with some applications of additive codes over rings to quantum codes.
Classification of Codes and Combinatorial Structures
Anton Betten
Colorado State University-U.S.A.
betten@math.colostate.edu

We propose a framework for modeling combinatorial objects and their equivalence using functions and groups acting on them. We consider a set of functions between two finite sets $N$ and $X$. Two groups $G$ and $H$ act on $N$ and $X$, respectively. The product $G \times H$ then acts on the set of functions: $G$ acts on the domain and $H$ acts on the image. The equivalence classes of functions under this action are called symmetry classes of mappings. A special case of this model is when the sets are vector spaces over a finite field and the groups act linearly. We will describe how both models apply to the problem of classifying linear codes.
Automorphisms of extremal lattices
Gabriele Nebe
RWTH Aachen University-Germany
gabriele.nebe@rwth-aachen.de

The notion of “Type” of a permutation has been introduced by Conway, Huffman, and Pless, to obtain restrictions on the possible automorphisms of extremal self-dual codes and to classify the codes admitting an automorphism of a given Type.

The talk shows how one can transfer this notion of Type to automorphisms of lattices. I present restrictions on the possible Types of automorphisms of extremal lattices in dimension 24, 48, and 72. For certain Types (the “large” automorphisms) the invariant extremal lattices can be constructed from ideal lattices using algebraic number theory.
A geometric approach to dynamic network coding
Angeles Vázquez-Castro
Universitat Autònoma de Barcelona-Spain
Angeles.Vazquez@uab.es

Coding over linear operator channels assuming incoherent transmission allows independent design of channel and network codes. Joint design however would be desirable for dynamic network conditions. In this work a geometrical approach (in the Kleinian sense) to dynamic network coding is presented. The approach consists of capturing the communication process with group actions. Specifically, codes are chosen as geometries and the dynamic network code is the stabiliser of the action. Capacity optimality is discussed for the ergodic erasure channel. The approach subsumes other approaches and provides natural adaptive encoding and decoding schemes with linear algebra tractability over different communication ambient spaces.

For illustration purposes, the applicability over realistic wireless erasure channels will be shown identifying the mapping between mathematical abstractions and the physical network communication process.
Perfect domination and cube-sphere tilings of $\mathbb{Z}^n$

Luis R. Fuentes Castilla
Universidad de Puerto Rico
luis.fuentes3@upr.edu

Co-authors: Carlos A. Araujo Martinez, Italo J. Dejter.

We ask whether there exist lattice-like tilings of the $n$-dimensional integer lattice $\Lambda_n$ by generalized Lee spheres around cubes of at least two different dimensions. This is known for $n = 2$. For $n = 3$, a perfect dominating set is constructed whose induced components are squares $Q_2$ and isolated vertices. In generalizing this, an extension of the notion of generalized Lee sphere in a graph-theoretical context is given to one of "cube-sphere". A lattice-like cube-sphere tiling of $\Lambda_n$ by the connected union $T$ of two generalized Lee spheres of radius 1 around $(n-1)$-cubes and two "cube-spheres" of radius $n - 2$ around isolated vertices. In showing this, an additive-group epimorphisms $\mathbb{Z}_n \to G$ is used that becomes bijective over $T$, a lattice fundamental region.
Cyclicity and asymptotic behavior of algebraic geometry codes
Ricardo Podesta
Universidad de Cordoba, Arg.
podesta@famaf.unc.edu.ar
Co-authors: María Chara, Ricardo Toledano, Orlando Villamayor

We give conditions for an AG-code to be cyclic and we present a criterion and 2 methods of construction of such codes. With one method, we obtain rational cyclic AG-codes, i.e. defined over some rational function field $\mathbb{F}_q(x)$, hence of genus 0. With the other method, given a Galois extension $F'/F$ of algebraic function fields over $\mathbb{F}_q$, we can obtain cyclic AG-codes defined on $F'$ starting from cyclic AG-code defined on $F$. This allows to construct cyclic AG-codes of genus $g > 0$. Finally, by using certain sequences of function fields, we can construct families of asymptotically good AG-codes with some additional structure that generalizes transitive codes.
The Fitting module of a linear code
Mehdi Garrousian
Universidad de los Andes-Colombia
m.garrousian@uniandes.edu.co

In commutative algebra, the Fitting module of a finitely generated module is formed by taking the consecutive quotients of its fitting ideals. These are determinantal ideals that tell us whether the module can be generated with a given number of elements. From a linear code, we naturally construct a Fitting module and show that its alpha-invariant (the smallest nonzero graded part) determines the minimum distance of the linear code. The goal of this talk is to show how various commutative/homological algebra invariants capture the minimum distance of linear codes. This is a joint work with Stefan Tohaneanu.
Construction of dense lattices from cyclic division algebras

Carina Alves
Sao Paulo State University, UNESP/Rio Claro-SP, Brazil
carina@rc.unesp.br
Co-authors: Cintya W.O. Benedito, Sueli I.R. Costa.

Signal constellations having lattice structure have been studied as meaningful tools for transmitting data over both Gaussian and single-antenna Rayleigh fading channels. More recently, the need for higher data transmission has led to consider communication channels using multiple antennas at both transmitter and receiver ends (MIMO).

Quaternion structure has been used to propose space-time block codes since the introduction of Alamouti code for two transmit antennas [3]. From probability point of view [1], designing a space-time block code requires the maximization of two parameters: diversity gain and coding gain. In the context of lattice, maximizing the coding gain is equivalent to maximizing the density of the corresponding lattice. Maximal orders have been proposed in the context of space-time block codes in [2] and complex codes constructions based on cyclic division algebras are proposed in [4]. Thus, having the construction of lattices as our goal, in this work we present constructions of dense lattices from maximal orders of the division algebras.

References


Automorphism Group of Generalized Hermitian Codes
Guilherme Tizziotti
Universidade Federal de Uberlandia
guilherme@famat.ufu.br

We determine the full automorphism group of the Generalized Hermitian curve, denoted by $\mathcal{GH}$, which generalize the Hermitian curve. The automorphism group of a code is important in Coding Theory and in this way we determine completely the automorphism group of the one-point AG codes over the $\mathcal{GH}$ curve.
On fourth-power residue self-dual codes
Darwin Villar
Lehrstuhl D für Mathematik, RWTH Aachen
darwin.villar@rwth-aachen.de

From the late 20th century Self-dual codes have drawn much attention for their multiple relations to other mathematical structures, such as designs or lattices. Only those over $GF(q)$, $q = 2, 3, 4$, are non-trivial divisible self-dual codes and thus much of the work has been directed towards them. In this work we show a technique when the code $C$ has an automorphism of order $p$, $p \equiv 1 \mod 4$, useful to obtain self-dual codes that yield even extremal ones in some cases.
On rotated $D_n$-lattices via number fields
Grasiele C. Jorge
Federal University of São Paulo
grasiele.jorge@unifesp.br
Co-authors: Sueli I. R. Costa and Antonio A. de Andrade

In this talk we will approach algebraic constructions of full diversity rotated $D_n$-lattices via number fields and their minimum product distances. Diversity and minimum product distance are important lattice parameters related to signal transmission over Rayleigh fading channels [3].

Let $K$ be a number field of degree $n$, $O_K$ its ring of integers and $\alpha \in O_K$ a totally positive real element. In [1, 2] it was introduced a twisted embedding $\sigma_\alpha : K \to \mathbb{R}^n$ such that if $I \subseteq O_K$ is a free $\mathbb{Z}$-module of rank $n$, then $\sigma_\alpha (I)$ is a lattice in $\mathbb{R}^n$ and it was shown that if $K$ is a totally real number field, then $\sigma_\alpha (I)$ is a full diversity lattice. Let $r \geq 3$ be an integer and $p, p_1, p_2$ prime numbers with $p \geq 7$, $p_1 \geq 5$, $p_2 \geq 5$ and $p_1 \neq p_2$. In order to get full diversity rotated $D_n$-lattices, constructions of $D_n$-lattices via twisted embeddings applied to free $\mathbb{Z}$-modules of rank $n$ contained in the totally real number fields $K_1 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $K_2 = \mathbb{Q}(\zeta_{2r} + \zeta_{2r}^{-1})\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $K_3 = \mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})\mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})$ were presented in [4, 5]. If it were possible to construct such rotated $D_n$-lattices via principal ideals of $O_{K_i}$, for $i = 1, 2, 3$, their minimum product distances would be twice those obtained in such constructions. However, in [5] it was shown that it is impossible to construct these lattices via fractional ideals of $O_{K_i}$, for $i = 1, 2, 3$, and it was presented a necessary condition for constructing a rotated $D_n$-lattice via a fractional ideal in a totally real Galois extension $K|\mathbb{Q}$. In particular, if $K|\mathbb{Q}$ is a totally real Galois extension of degree $n \notin \{1, 2, 4\}$ with odd discriminant, then it is impossible to construct a rotated $D_n$-lattice via a fractional ideal of $O_K$. Recently, we have considered other constructions of full diversity rotated $D_n$-lattices via free $\mathbb{Z}$-modules contained in subfields of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $p$ prime.

References


---

1This work was partially supported by FAPESP under grant number 2013/25977-7, Brazil, 4 University of Campinas, Brazil, 5 São Paulo State University, Brazil
Generalized Hamming Weight over the $\mathcal{GH}$ curve
Alonso Sepúlveda Castellanos
University Federal of Uberlândia
alonso@famat.ufu.br

We studied the generalized Hamming weights of geometric Goppa codes over the $\mathcal{GH}$ curve. These codes, for any $q = p^t$ where $p$ is a prime, were studied by Munuera, Sepúlveda and Torres in [1]. Furthermore, we apply the Hamming weights for characterizes the performance of the $\mathcal{GH}$ codes on a noiseless communication channel.

References

Lattices and Spherical Codes
Sueli I. R. Costa
University of Campinas
sueli@ime.unicamp.br

Point sets on a sphere used in communications over a Gaussian channel and are a natural generalization of phase shift keyed signal sets (PSK) to dimensions greater than two. While it is important to maximize the packing density, additional practical considerations such as storage and easy decoding are also important. Spherical codes given as orbits of a unit vector under the action of commutative groups of orthogonal matrices were introduced by D. Slepian [1] and deserve special attention due of the symmetry and homogeneity arising from their algebraic structure. For spheres in even-dimensional space these codes lie on a flat torus, are described as quotient of lattices in half of the dimension and we can derive bounds for their packing density from the density of these lattices. The foliation of a sphere in even-dimensional space by flat tori can be used to construct discrete spherical codes (quasi-commutative group codes) and also homogeneous curves for transmitting a continuous alphabet source over an AWGN channel. In both cases the performance of the code is related to the packing density of specific lattices and their orthogonal sub-lattices. In the continuous case the packing density of curves relies on the search for projection lattices with good packing density. In this talk, which is based in several works such as the ones listed here, it will be presented a survey of this topic including some recent research results and perspectives.

References


2Work partially supported by FAPESP/CNPq
The rank MDS of Hermitian codes
Wilson Olaya-León
Universidad Industrial de Santander
wolaya@uis.edu.co

Let \( \mathbb{F}_q \) be the finite fields with \( q \) elements. For a vector \( x \in \mathbb{F}_q^n \), the support of \( x \) is the set \( \text{supp}(x) = \{ i : 1 \leq i \leq n, x_i \neq 0 \} \). If \( C \subset \mathbb{F}_q^n \) is a linear \([n,k]\) code, the support of \( C \) is defined as \( \text{supp}(C) = \bigcup_{x \in C} \text{supp}(x) \) y for any \( r, 1 \leq r \leq k \), the \( r \)-th generalized Hamming weight of \( C \) is

\[
d_r(C) = \min \{ \#\text{supp}(V_r) : V_r \text{ is an } r \text{- dimensional subcode of } C \}.
\]

These notions of generalized Hamming weights have been introduced by Wei in [4], motivated by applications from cryptography.

In particular, the first generalized Hamming weight of \( C \) is the usual minimum distance. The weight hierarchy of the code \( C \) is the set of generalized Hamming weights \( \{d_1(C), d_2(C), \ldots, d_k(C)\} \). The \( r \)-th generalized Hamming weight of \( C \) satisfies the inequality \( d_r(C) \leq n - k + r \) that is called the generalized Singleton bound for \( d_r(C) \), and a code \( C \) which satisfies the equality in this bound is called the \( r \)-th rank maximum distance separable (MDS) code, moreover it has the property of domino effect, if \( d_{r'}(C) = n - k + r' \) for some \( r' \), then \( d_r(C) = n - k + r \) for all \( r \) with \( r' \leq r \leq k \), see [4]. We define the touch at the first \( \tau \), \( 1 \leq \tau \leq k \), so that \( C \) is a \( \tau \)-th rank MDS code, and the discrete interval \([\tau,k]\) is called the rank MDS of \( C \).

A Hermitian code is an one-point algebraic geometric code coming from the Hermitian curve \( \mathcal{H}: y^q + y = x^{q+1} \) of genus \( g = \frac{q(q-1)}{2} \) over \( \mathbb{F}_q^2 \). Hermitian codes have been studied by many authors. In [3] we characterized in a simple manner the minimum distance of the Hermitian codes. In this talk we compute the touch of all Hermitian codes and therefore we obtain the rank MDS of all Hermitian codes.

References


The Combinatorics of Conditional Independence
Michael E. O’Sullivan
San Diego State University-U.S.A.
mosullivan@mail.sdsu.edu

Let $X_1, \ldots, X_n$ be discrete random variables and, for a nonempty subset $A$ of $\{1, \ldots, n\}$, let $X_A$ be the random vector indexed by $A$. We look at two combinatorial objects related to distributions on $X_N$. One is the set of triples $A \perp B \mid C$ such that $X_A$ is independent of $X_B$ given $X_C$. The independence triples of $X_N$ satisfy the semigraphoid properties (as defined by Dawid): symmetry, decomposition, weak union, contraction. Matus and Studeny showed that identifying all combinatorial properties satisfied by the independence triples of $X_N$ gets very messy, even for 4 random variables.

The vector of entropies $H(X_A)$ indexed by $A$ introduces another combinatorial object. It satisfies inequalities discovered by Shannon as well as numerous non-Shannon inequalities discovered by Zhang and Yeung, Dougherty et al., Matus, and others. I will show that many of the properties for independence triples are easily derived from these non-Shannon information inequalities. I will also show connections to coding theory, which provides interesting extremal examples.
Maximum distance separable 2D convolutional codes based on superregular matrices

Joan-Josep Climent
Universitat d’Alacant-Spain
jcliment@ua.es

In the transmission of information through a noisy channel, the information is often corrupted due to the noise of the channel and therefore data correctly sent from the source may suffer alterations at the receiving end. In order to bypass this problem some level of coding can be implemented on the information sequence. One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction. To encode data recorded in \( m \) dimensions (mD, with \( m > 1 \)), e.g., pictures or videos, it is conventional to transform it into arrays of 1D sequences by means of scanning and then apply 1D encoding techniques, ignoring the interdependence in all other directions.

However, it is possible to work in a framework that takes advantage of the correlation of the data in several directions. Such framework would lead to \( m \) dimensional (mD) convolutional codes, generalizing the notion of 1D convolutional code.

In this talk 2D convolutional codes with finite support are considered, i.e., convolutional codes whose codewords have compact support indexed in \( \mathbb{N}^2 \) and take values in \( \mathbb{F}^n \), where \( \mathbb{F} \) is a finite field. The main goal of this work is to analyze the (free) distance properties of this type of codes. We first establish an upper bound on the maximum possible distance for these codes. Then we present particular constructions of 2D convolutional codes with finite support that attain such a bound and therefore have the maximum distance among all 2D convolutional codes with finite support with the same rate and degree. We call such codes maximum distance separable 2D convolutional codes.
Affine Grassmann codes are certain subcodes of generalized Reed-Muller codes, which were introduced in [1]. From [1, 2, 4, 3], we know that affine Grassmann codes possess several remarkable properties. In particular, their length, dimension and minimum distance are explicitly known. Duals of affine Grassmann codes have a very low minimum distance and are generated by their minimum weight codewords. Affine Grassmann codes have large automorphism groups, which are fully known. Finally, affine Grassmann codes are closely related to Grassmann codes which are of an older vintage as well as much recent interest.

We consider a generalization of affine Grassmann codes, called Schubert cell codes. To explain these, consider the Grassmannian (over the finite field $\mathbb{F}_q$ with $q$ elements) $G_{\ell,m}$ consisting of all $\ell$-dimensional subspaces of $\mathbb{F}_q^m$, with its Plücker embedding in $\mathbb{P}^{k-1}$, where $k := \binom{m}{\ell}$. It has a cellular decomposition, whereby $G_{\ell,m}$ is a disjoint union of cells that are indexed by subsets of $\{1, \ldots, m\}$ of cardinality $\ell$. Each cell is isomorphic to an affine space, but has a nondegenerate embedding (inherited from the Plücker embedding) in a high-dimensional projective space. Schubert cell codes are precisely the linear codes corresponding to projective systems (in the sense of Tsfasman-Vlăduţ) given by a Schubert cell with its associated embedding in a projective space. In this set-up, affine Grassmann codes correspond to the Schubert cell indexed by the “maximal” $\ell$-subset of $\{1, \ldots, m\}$ w.r.t. Bruhat order, namely, $\{m - \ell + 1, m - \ell + 2, \ldots, m - 1, m\}$. Alternatively, and in the spirit of [1], Schubert cell codes are evaluation codes corresponding to certain evaluations of polynomials in a $\mathbb{F}_q$-linear space spanned by some minors.

It turns out that questions concerning the determination of basic parameters such as length, dimension, and minimum distance, of Schubert cell codes are intimately tied with interesting combinatorial questions concerning arrangements of nonattaching rooks in a square board or more generally, a Ferrers board. We exploit this to determine coding theoretic properties of Schubert cell codes. As a dividend, we obtain an explicit information set for the Schubert cell codes, the special case of which for affine Grassmann codes appears to be new and hitherto unnoticed. Further, we give an explicit description of the duals of Schubert cell codes, compute the dual minimum distance, and show that the duals are generated by their minimum weight codewords. It is also shown that the automorphism group of a Schubert cell code contains a large subgroup.

References


On Gray Map Images of Codes over Galois Rings and Finite Chain Rings
Carlos Alberto López-Andrade
Benemérita Universidad Autónoma de Puebla
clopez@fcfm.buap.mx

In this talk results on the Gray map image of different kinds of codes defined over the Galois ring $GR(p^2, m)$ and a class of linear cyclic codes over a finite chain ring $R$ of nilpotency index two are both presented.
Characterization of metrics induced by hierarchical posets

Roberto A. Machado
State University of Campinas
guilherme@famat.ufu.br
Co-authors: Marcelo Firer, Jerry A. Pinheiro.

A message transmitted through a communication channel is subjected to transmission errors, that is, the receiver cannot identify the original message that was sent him. There is a decoding method called nearest neighbour that uses a metric to determine the closest codeword to the received message. In the classical coding theory, we often consider the Hamming or Lee metrics. Considering these metrics, some metric aspects of codes were studied, such as: packing radius, covering radius, MacWilliams identity, perfect codes, etc. The use of the Hamming or Lee metrics is justified by the fact that the nearest neighbour decoding matches to the maximum likelihood decoding for the simplest channel model, the memoryless symmetric channel. For complex channels it is necessary to define and study other families of metrics and the metric aspects of the codes admitting these metrics.

In 1995, Brualdi, Graves and Lawrence introduced a generalization for Hamming metric called poset metrics. Several relations obtained for the Hamming metric were extended to the family of hierarchical poset metrics over the years. These results appear dispersed throughout the literature with long proofs. Considering the systematic-canonical form for linear codes, introduced in 2012 by Felix and Firer, we prove these and other properties, that characterize the hierarchical poset metrics in a simple and short way, in the following sense, given a metric induced by a poset \( P \) then this metric is hierarchical if, and only if, for every code \( C, C' \subseteq \mathbb{F}_q^n \) one of the following items hold:

(i) \( P \) admits a MacWilliams-type Identity: the weight distribution of a code \( C \) determines the weight distribution of its dual \( C^\perp \), concerning the metric induced by dual poset \( \overline{P} \);

(ii) the packing radius of \( C \) is uniquely determined by the minimum distance of \( C \);

(iii) \( P \) admits association schemes;

(iv) the group of linear isometries acts transitively on spheres of fixed radius centered around zero;

(v) MacWilliams extension theorem: each linear isometry \( \rho : C \to C' \) can be extended to a linear isometry on \( \mathbb{F}_q^n \);

(vi) the weight is a shape mapping;

(vii) the entry of adjacency matrix of \( P \) satisfy the triangle inequality, i.e., \( a_{ij} \leq a_{ik} + a_{kj} \).
Performance of SPC product codes through graph theory
Sara D. Cardell
State University of Campinas
sdcardell@ime.unicamp.br
Co-authors: Joan-Josep Climent.

The single parity-check (SPC) code is one of the most popular MDS error detection codes, since it is very easy to implement [1]. One bit is appended to an information sequence of length $n - 1$, such that the resultant codeword has an even number of ones. Two SPC codes can be used jointly to obtain an SPC product code, which has 4 as minimum distance. Therefore, it can recover all erasure patterns with one, two, and three erasures. However, up to $2n - 1$ erasures can be corrected in some special cases. Furthermore, a codeword of length $n^2$ can be represented by an erasure pattern of size $n \times n$, where the unique information considered is the position of the erasures. In [1], authors proposed an approach of the post-decoding erasure rate of the SPC product code. This process was based on observing the structure of the erasure patterns, classifying them into correctable or uncorrectable. In this work, we represent each erasure pattern by a bipartite graph [2] with $n$ nodes in each vertex class and the same number of edges as erasures. Then, the problem of counting uncorrectable erasure patterns can be seen as a problem of counting bipartite graphs with cycles.

References


Identification of Proteins as Codewords of Cyclic Codes Over Finite Rings with Identity

Mario E. Duarte Gonzalez
University of Campinas
mduarte@dt.fee.unicamp.br
Co-authors: Reginaldo Palazzo Jr.

In a recent work [1], a methodology for the identification of proteins as codewords of error-correcting codes (ECC) over \( \mathbb{Z}_{20} \) and over \( \mathbb{F}_4 \times \mathbb{Z}_5 \) has been proposed. The ECCs over \( \mathbb{Z}_{20} \) and over \( \mathbb{F}_4 \times \mathbb{Z}_5 \) with length \( n \) were constructed as proposed in [2, 3] by joining componentwise, through the cartesian product, every codeword of two BCH codes over \( \mathbb{Z}_4 \) and \( \mathbb{Z}_5 \) (or \( \mathbb{F}_4 \) and \( \mathbb{Z}_5 \)), respectively. This construction requires that both BCH codes \( C_1 \) and \( C_2 \) have the same length \( n \), therefore, it is possible to construct codes over \( \mathbb{Z}_4 \times \mathbb{Z}_5 \) and \( \mathbb{F}_4 \times \mathbb{Z}_5 \) from BCH codes only for a restricted number of codeword lengths.

Any finite commutative ring with identity \( A \) is isomorphic to a direct sum of local rings (Theorem 3.14 in [4]): \( A \cong \bigoplus A_i \). In this work, a more general methodology for constructing a code \( C \) over \( A \) by joining \( s \) codes \( C_1, \ldots, C_s \) over \( A_1, \ldots, A_s \) is proposed. The length of the resulting code \( C \) is \( n = \text{lcm}(n_1, \ldots, n_s) \) and its properties are deduced from the properties of the component codes, \( C_1, \ldots, C_s \). It is shown that \( C \) is cyclic when every \( C_i \) is cyclic, that \( C \) is a free submodule of dimension \( k \) if every \( C_i \) is a free submodule of dimension \( k \) and a minimum set of generators is given. Algorithms for detecting and correcting errors, based on equivalent algorithms for \( C_1, C_2, \ldots, C_s \), are introduced.

When \( A \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \) (or \( A \cong \mathbb{F}_4 \times \mathbb{Z}_5 \)), given two BCH codes \( C_1 \) and \( C_2 \) over \( \mathbb{Z}_4 \) and \( \mathbb{Z}_5 \) (or \( \mathbb{F}_4 \) and \( \mathbb{Z}_5 \)), respectively, with parameters \( (n_1, k, d_1) \) and \( (n_2, k, d_2) \), the resulting code \( C \) over \( A \) has length \( n = \text{lcm}(n_1, n_2) \), dimension \( k \) and minimum Hamming distance \( d = \min\{\alpha d_1, \beta d_2\} \), where \( n = \alpha n_1 = \beta n_2 \). Although \( C \) does not have good error-correcting capability, it has been noticed that \( C \) is an appropriate code for identifying proteins as codewords due to the fact that the identification process makes use of single error-correcting codes. In addition to this fact, it is easy to construct such a code, its error detection algorithm is simple, its mathematical structure is well-known, it is a generalization of already known codes which identify proteins [1], and, as shown in [1, 5], the ECCs for the identification of mRNA sequences and proteins do not have a large error-correcting capability.

References

Perfect $q$-ary codes under the Chebyshev metric
Claudio Qureshi
Universidade Estadual de Campinas
cquier@gmail.com
Co-authors:Sueli Costa

We consider perfect codes in the Chebyshev (or maximum) metric and tiling of the $n$-torus by cubes. A characterization of such codes and several constructions are given. In some cases we parametrize the set of perfect codes with prescribed packing radius and cardinality through a certain ring of matrices, in such a way isometry and isomorphism classes of perfect codes correspond to certain generalized cosets. This talk is based on a join work with Prof. Sueli Costa (Imecc-Unicamp).
Weight distribution of rank-metric codes
Alberto Ravagnani
University of Neuchatel
alberto.ravagnani88@gmail.com
Co-authors: J. de la Cruz, E. Gorla, and H. Lopez.

A rank-metric code is a linear space of rectangular matrices defined over a finite field. In this context, the distance between two matrices is the rank of their difference. Rank-metric codes received a lot of attention in the last years, mainly because of their applications in coherent and non-coherent linear network coding.

In my talk I will present the main properties of the weight distribution of a rank-metric code, discussing in particular anticodes, bounds, generalized weights, and MacWilliams identities for the rank weight.

In analogy with the Singleton defect for classical codes, I will then introduce a notion of rank defect for rank-metric codes, and describe the properties of this new algebraic invariant. In particular, I will show that the rank distribution of a code whose defect and dual defect are both zero is completely determined by its parameters. This extends a famous result by Delsarte on the weight distribution of an MRD code.

The new results that I will present are joint work with J. de la Cruz, E. Gorla, and H. Lopez.
Lattice Packings from Certain $p$-extensions of $\mathbb{Q}$

J. Carmelo Interlando
San Diego State University-U.S.A
interlan@mail.sdsu.edu
Co-authors: José Valter Lopes, Trajano Nóbrega Neto.

Lattices (discrete subgroups of $\mathbb{R}^n$) have played an important role in coding theory since the pioneer work of Claude Shannon. In particular, dense lattice packings may be used to design optimal codes for a band-limited channel with white Gaussian noise. The objective of this talk is to present constructions of lattices from sub-modules $M$ of the ring of integers $\mathcal{O}_F$ of a number field $F$ where $F/\mathbb{Q}$ is a Galois extension of degree $p$, with $p$ an odd prime. To achieve the objective, the trace form of $F$, as well as a method for determining its minimum in $M$, will be presented. Those results will then yield an algorithm for optimizing the choice of $M$, ultimately leading to dense $p$-dimensional lattices. Numerical examples will illustrate the method.
Geometric decoding of subspace codes

Klara Stokes
University of Skövde
klara.stokes@his.se

Grassmannian codes are subspace codes of constant dimension. The Grassmannian can be embedded into a projective space using Plücker coordinates as an algebraic variety $V$. A geometric subspace code is a set of subspaces with Plücker coordinates cut out by the intersection of this variety and another algebraic variety $U$. Geometric subspace codes can be decoded with an algorithm first described by Rosenthal -Silberstein -Trautmann for Lifted Gabidulin codes. In this talk I will give some examples of geometric subspace codes and discuss their properties.
RCA Analysis of the Polar Codes and the use of Feedback to aid Polarization at Short Blocklengths

Kasra Vakilinia
University of California, Los Angeles (UCLA)
vakilinia@ucla.edu

This work uses an extension of Reciprocal Channel Approximation (RCA) to accurately and efficiently predict the frame error rate (FER) performance of polar codes by analyzing the probability density function (p.d.f) of log likelihood ratios (LLR) associated with information bits. A feedback scheme uses the RCA to predict the p.d.f of LLRs in conjunction with a repetition coding system to decrease the blocklength required for a target FER by a factor of 16. Using a rate-0.5 128-bit polar code as the initially transmitted code, the FER of the system with feedback is obtained by theoretical analysis and verified by simulation. Including the additional incremental transmissions the average blocklength for the system with feedback is 137.55 bits and the rate is 0.4653. Without feedback, a polar code with blocklength 2048 is required to achieve a comparable FER at a comparable rate. Intuitively, feedback allows the polar code to use fewer frozen bits in the initial transmission and then uses repetition codes to provide the needed reliability to resolve unreliable unfrozen bits identified by feedback.
The weight distribution of the self-dual $[128,64]$ polarity design code

Vladimir Tonchev
Michigan Technological University
tonchev@mtu.edu

The weight distribution of the binary self-dual $[128, 64]$ code being the extended code $C^*$ of the code spanned by the incidence vectors of the blocks of the polarity design in $PG(6, 2)$ is computed. The code $C^*$ has the same weight distribution as the 3rd order Reed-Muller code of length 128.
Network coding is a very active research area and has as motivational elements the efficient and reliable transmission of information in traditional communication networks. Up to now, the modus operandi of the intermediate nodes was to process and route each received packet. With the advent of network coding, the intermediate nodes can do much more than simply process and route the received packets, [1]. For instance, the received packets can now be encoded by use of proper subspace codes, [3]. This is the reason network coding has provided high throughput and reliability.

In addition to these characteristics, a correspondence between an error-correcting code and a subspace code may be described as follows: 1) the "codeword" in an error-correcting code corresponds to a subspace of a projective vector space, and 2) the error-correcting code corresponds to the union of subspaces of the projective vector space. Hence, the subspace codes are the proper codes to be used in network coding to achieve the previously mentioned objectives. Among the traditional classes of error-correcting codes, the class of geometrically uniform codes is one of the most important for the easiness of being generated and the inherent least complexity in the decoding process.

The aim of this paper is in addition to presenting the construction of geometrically uniform subspace codes (GUSC) to proving that the resulting codes satisfy the property of geometric uniformity, [2]. This construction is based on the application of cyclic-shifts on a given set of codewords, or equivalently, by using an appropriate set of permutations acting transitively on the set of codewords. For instance, consider the simple example as shown next.

References


The relationship between Riemann surface and Fuchsian differential equation
with the aim at coding of geodesics

Anderson Oliveira
State University of Campinas
anderson.oliveira@unifal-mg.edu.br

A Fuchsian differential equation (FDE) has as its main characteristic the fact that every singular point in the extended complex plane is regular. The previous cases considered in the open literature consist of three and four regular singular points. One may observe an interesting relationship between the singularities of a Fuchsian differential equation, the vertices of the fundamental triangle in the Farey tessellations, and the surface associated with the Moebius transformations applied to the edge-pairings of the fundamental polygon. One may notice that the three regular singular points \( \{0, 1, \infty\} \) besides being the roots of an algebraic curve are the vertices of a triangular fundamental region and that the edge-pairings (elliptic and parabolic transformations) leads to a spherical surface. These regular singular points are part of the Farey series \( \mathbb{F}_1 \). As a consequence, we have a relationship of the FDE coefficients, the singularities, the fundamental triangle and the associated surface. In this direction, we propose to generalize these result for other fundamental regions containing \( n \) edges and with the vertices (regular singular points) as elements of the Farey series \( \mathbb{F}_{n-2} \). Consequently, the objective is to establish a relationship between the coefficients of the FDE containing \( n \) regular singular points with the surface associated with the edge-pairings of the fundamental polygon. In this paper we consider as a particular case where the FDE consists of three regular singular points (Legendre equation) and with four regular singular points (Heun equation) under the Farey series approach. An important application of the construction of these models is the coding of geodesics where the relationship is established using the coefficients of the Fuchsian differential equations and the elements of the Farey series \( \mathbb{F}_m \).
The main objective of this paper is to show the MDS conjecture for finite fields following the method used by S. Ball. Essentially we will give a test of a sub-case of the conjecture that set out below when $q$ is a prime number:

**MDS Conjecture** A set $S \subseteq \mathbb{F}_q^k$ with the property that every subset of $S$ of cardinality $k$ is a basis of $\mathbb{F}_q^k$ has at most $q+1$ elements, except if $q$ is even and $k = 3$ or $k = q - 1$, in which case has at most $q+2$.

In fact, we will prove that such a set of cardinality $q + 1$ is equivalent in some sense we will define later to:

$$S_1 = \{(1, t, t^2, \ldots, t^{k-1}) : t \in \mathbb{F}_q\} \cap \{(0, \ldots, 0, 1)\}$$

Clearly $|S_1| = q + 1$ and since each matrix size $k \times k$ formed by vectors $k$ of $S_1$ is a Vandermonde matrix of nonzero determinant, then $S_1$ fulfills the property described above.

The **MDS Conjecture** - or maximum distance separable codes conjecture proposed in terms of linear codes, there is no linear codes MDS over $\mathbb{F}_q$ of dimension at most $q$, longer than the longest of the Reed-Solomon, even more, if codes are maximum dimension codes are then Reed-Solomon codes. In this paper we will see that the set $S$ described above, results in a linear maximum distance separable code of length $|S|$ and $k$ dimension. And more than that, $S_1$ results in a Reed-Solomon code.

In 1947, Bose said that if $p \geq k = 3$, then $|S| \leq p + 1$. Later, in 1955, Segre showed that if $p \geq k = 3$, then the equality is only archived for of sets $S$ equivalent to the set $S_1$. The following lemma was proved in 1952 by Bush

**Lemma 1** $|S| \leq k + 1$. Moreover, if $|S| = k + 1$ then is equivalent to

$$\{(\lambda_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, \lambda_k), (1, \ldots, 1)\}$$

for some $\lambda_i \in \mathbb{F}_q \setminus \{0\}$.

In 1955 B. Segre wondered what could be a final bound for the cardinality of such a set $S$, resulting in the **MDS Conjecture** as is stated here. In this paper the most significant progress in achieving a demonstration and the problems that remain open will be discussed.
Distance properties of convolutional codes over $\mathbb{Z}_p^r$

Diego Napp
University of Aveiro-Portugal
diegonapp@gmail.com

In this talk we present convolutional codes over finite rings of the type $\mathbb{Z}_p^r$. In particular we aim to investigate their distance properties, namely, the free distance and their column distances. We derive novel upper bounds for both types of distances and introduce then the notions of Maximal Distance Separable (MDP) and Maximal Distance Profile (MDP). The existence of these codes is shown by presenting concrete constructions of MDS and MDP. Our proofs and results on sequences over the finite ring $\mathbb{Z}_p^r$ rely heavily on the recently developed new framework of $p$-bases.
Theory and Applications of Skew Polynomial Rings
Felice Manganiello
Clemson University-U.S.A
manganm@clemson.edu

Skew polynomial rings are a non commutative generalization of polynomial rings. Their applications to coding theory and cryptography have been investigated in the last decade. In this talk, we explore the algebraic structure of these rings when defined over a finite field, as well as the evaluation of their polynomials. From the evaluation, we construct a notion of independency which induces a matroid structure on the finite field. Two are the applications we then focus on: a duality theory for codes defined by skew evaluation and the use of the underlined matroid in multicast network communication.
An error-correcting code $C$ is called a linear code with a complementary dual (in short LCD code) if it is linear and $C \cap C^\perp = \{0\}$. LCD codes were introduced by Massey in 1993. Carlet, Guilley (2015) use these types of codes as counter-measure to side-channel attacks.

In a recent work, Dougherty, Kim, Ozkaya, Sok and Solé (2015) describe constructions of LCD codes by codes over rings, orthogonal matrices and block designs. In this talk, sufficient conditions for the existence of LCD codes with prescribed parameters are given. These conditions can be formulated as a Diophantine linear system which may be solved with the help of computers. In order to reduce the number of equations and unknowns of these systems, the search is restricted to LCD codes with special symmetry given by matrix groups.

With this approach the parameters of known good LCD codes for small dimensions could be improved in many cases. Often the parameters of the new LCD codes reach the upper bounds for general linear codes. This is not surprising since it is known that LCD codes are asymptotically good.
Coded patient identifier in medicine

Andreas Faldum
University of Münster-Germany
Andreas.Faldum@ukmuenster.de

Generating unique pseudonymous patient (or person) identifiers (PID) is a basic need in medical research networks. Erroneous data transmission and entry of a PID lead to an incorrect assignment to therapy. Moreover, statistical analyses may result in biased conclusions. Therefore, it is important to detect incorrect patient identifiers. In addition, automatic error correction of PIDs is desirable since typing errors frequently occur. To face this problem an [8, 6, 3] MDS code over a 32-character alphabet was constructed that detects up to two errors and corrects one error. The resulting PIDs distinguish 1 billion individuals. The code is most trustworthy and clearly superior to double data entry which is the standard solution. Additionally, it is possible to reverse a transposition of adjacent characters which is a common source of mistake. The PID algorithm was first applied to controlled clinical trials of the International Society of Paediatric Oncology (SIOP). It is also embedded as a component of the pseudonymisation service that is used in the TMF—the German telematics platform for health research networks.

References


An algorithm to compute the apparent distance of an abelian code  
Diana H. Bueno-Carreño  
Pontificia Universidad Javeriana Cali-Colombia  
dhbueno@javerianacali.edu.co  
Co-authors: José Joaquín Bernal and Juan Jacobo Simón

The BCH bound is the oldest lower bound for the minimum distance of a cyclic code. The study of this bound and its generalizations are classical topics, which includes the study of the very well-known family of BCH codes.

In 1970, P. Camion \(^3\) extended the notion of BCH bound to the family of abelian codes by introducing the apparent distance of polynomials. Camion showed that the minimum value of the apparent distance of certain polynomials associated to codewords is less than or equal to the minimum distance of the code. The mentioned minimum value is known as the apparent distance of a code.

Then, in 1992, R. E. Sabin \(^4\) introduced one method of formulating an extension of the BCH bound to abelian codes based on the paper of Camion. The apparent distance of a polynomial is computed by considering its coefficient matrix and permuting rows and columns; this yields a simplification of the original method.

In this talk, an algorithm to compute the apparent distance of an abelian code, based on some manipulations of hypermatrices associated to its generating idempotent, is presented. This method uses less computations than those given by Camion and Evans; furthermore, in the bivariate case, the order of the computations is reduced from exponential to linear. In addition, a notion of BCH multivariate code is given.


Posets, graphs, blocks and other generalizations of the Hamming metric

Marcelo Firer
State University of Campinas-Brazil.
mfirer@ime.unicamp.br

Binary and $q$-ary symmetric channels play a central role in Information Theory, so the metric counterparts of those channels, Hamming and Lee metric, have the same distinguished role in Coding Theory. In the 90’s, some generalizations of the Hamming metric were introduced, starting with a possible metric model for an hypothetical channel with an order structure of errors (Niederreiter, 1991) and later, in 1995, being generalized by Brualdi, Graves and Lawrence, that defined what is currently known as poset metric.

Poset metric became interesting because many rare properties of codes may become more abundant, such as the existence of MDS and perfect codes. Since then, those metric were investigated from the point of view of Coding Theory, concerned with invariants as minimal distance, packing and covering radii and properties as MDS and perfectness, as much as coded-related algorithmic-processes, such as determination of the packing radius and syndrome decoding.

The intense investigation of codes, in the perspective of poset metrics, allowed a deep understanding of codes properties and invariants, generally taken for grant, due to the very special role of the Hamming metric.

In the last decade further generalizations of a metric determined by a weight (that is, $d(x, y) = \text{weight}(x - y)$) and of a weight that respects the support of vectors ($\text{supp}(x) \subseteq \text{supp}(y)$ implies $\text{weight}(x) \leq \text{weight}(y)$) have been introduced: block metric (Feng, Xu and Hickernell, 2006), poset-block metric (Panek, Firer and Alves, 2010), oriented-graphs and block-valued-oriented-graphs metrics (D’Oliveira, Etzion and Firer, 2015, undergoing work).

In this talk we will present a survey of results about coding with poset-metrics (many of them being counter-intuitive for our Hamming-shaped intuition), present many of those generalizations, including many (hopefully interesting) open problems.