Network Coding and Designs
Final Conference of COST Action IC1104
Centre for Advanced Academic Studies
Dubrovnik, Croatia • April 4–8, 2016

2012
BrusselsAscona
BarcelonaBerge
nZurichGhentTa
llinBordeauxPa
lmelaBanzNoviS
adSalamancaIst
anbulDubrovnik
2016
Network Coding and Designs
Final Conference of COST Action IC1104
Centre for Advanced Academic Studies
Dubrovnik, Croatia • April 4–8, 2016

2012
BrusselsAscona
BarcelonaBerge
nZurichGhentTa
llinBordeauxPa
lmelaBanzNoviS
adSalamancaIst
anbulDubrovnik
2016

Organizing committee:
Marcus Greferath • Aalto University, Finland
Vedran Krčadinac • University of Zagreb, Croatia
Mario Osvin Pavčević • University of Zagreb, Croatia
Kristijan Tabak • Rochester Institute of Technology Croatia
Jens Zumbrägel • EPFL, Switzerland
## Contents

Welcome from the Organizing committee .................................................. 1
Conference program .................................................................................. 2

### Invited talks

- S.Blackburn: *Cryptography and network coding* .................................. 8
- T.Etzion: *What is old, what is new, and what to do?* ......................... 8
- C.Hollanti: *Locally repairable codes with availability and hierarchy: Matroid theory via examples* .................................................. 9
- T.Honold: *Constant-dimension codes exceeding the LMRD code bound* . 9
- J.Jedwab: *How many mutually unbiased bases can exist in complex space of dimension d?* ...................................................... 10
- M.Kiermaier: *On q-analogs of the Fano plane* .................................. 11
- M.Kovaˇ cevi´ c: *Timing channels and shift-correcting codes* ............... 11
- D.E.Lucani: *Composite extension fields for (network) coding: Designs and opportunities* ...................................................... 13
- J.Rosenthal: *Public key cryptosystems based on rank metric codes and subspace codes* ............................................................. 14
- E.Soljanin: *On network-induced locality and decoding constraints* .... 15
- A.Vazquez-Castro: *Coding and network coding over flag varieties* ...... 15

### Contributed talks

- P.Almeida: *Optimal 2D convolutional codes* ..................................... 18
- M.Alsina: *On centers of hyperbolic tessellations and their applications* 18
- Á.Barbero: *Coding schemes with short erasure recovery delay* .......... 19
- D.Bartoli: *Equidistant subspace codes* ............................................. 20
- M.Braun: *On the q-analog of the revolving door algorithm* ............ 21
- M.Buratti: *Steiner triple systems and their automorphism groups* ...... 21
- M.Calderini: *Bounding the optimal rate of the ICCSI problem* ........ 21
- D.Dumiˇ ci´ c Danilovi´ c: *Block designs and self-orthogonal codes constructed from orbit matrices* .............................................. 22
- P.Farkaš: *Distributed method for topological interference alignment and its connection with network coding* .................................. 23
- T.Gaebel-Hoekenschnieder: *Network based measurement theory* ..... 25
- S.Gökelei: *A random network coding testbed* .................................. 25
- H.Gropp: *Orbital matrices again* ...................................................... 26
- D.Heinlein: *Coset construction for subspace codes* ............................ 27
- A.-L.Horlemann-Trautmann: *Maximum rank distance codes are generic sets* ............................................................. 28
- R.Judák and D.Mežoň: *Comparison of some linear codes with high noise binary channel* .............................................................. 29
- R.Jurrius: *On defining q-matroids* .................................................... 29
- V.Krčadinac: *New quasi-symmetric designs by the Kramer-Mesner method* ............................................................. 30
- S.Kurz: *Improved upper bounds for partial spreads* .......................... 31
- R.Laue: *Large sets of t-designs with large blocks* ............................. 31
- U.Martínez-Peñas: *On the roots and minimum rank distance of skew cyclic codes* ............................................................. 32
U. Martínez-Peñas: Rank error-correcting pairs ........................................ 33
V. Mikulić Crnković: On self-orthogonal codes generated by orbit matrices
of 1-designs ................................................................................................ 34
P. Moustrou: On the density of cyclotomic lattices constructed from codes 35
A. Nakić: On a property of \((n,2k-2,k)\)-subspace codes ......................... 36
D. Napp: Concatenation of convolutional codes and rankmetric codes for
multi-shot network coding ........................................................................ 37
K. Otal: Polynomial approach to construct cyclic subspace codes ............ 38
J. Pääkkönen: Ensuring data availability in device-to-device caching clus-
ters with regenerating codes ................................................................... 38
F. Pavese: On mixed dimension subspace codes ...................................... 39
R. Pinto: Rank metric convolutional codes ............................................. 40
A. Ravagnani: Equidistant subspace codes ............................................. 41
N. Raviv: Coding for locality in reconstructing permutations .................. 42
A.-E. Riet: Structure of large equidistant Grassmannian codes .............. 43
M. Rodgers: Cameron–Liebler type sets and completely regular codes in
Grassmann graphs ..................................................................................... 44
S. Schmidt: Generalized metrics for network coding ................................. 44
N. Silberstein: Binary locally repairable codes with high availability via an-
ticodes ...................................................................................................... 45
M. Šimac: LDPC codes based on \(\mu\)-geodetic graphs .................................. 46
V. Skachek: New bound for batch codes with restricted query size ........... 46
C. Stefanović: Random access via sign-compute-resolve on graphs ........ 47
L. Storme: Primitive \(t\)-intersection constant dimension codes ............... 48
A. Švob: The Cameron-Liebler problem for sets ..................................... 49
K. Tabak: Normalized difference sets tiling in \(\mathbb{Z}_p\) .................................. 50
M. Toste: On MDS convolutional codes over \(\mathbb{Z}_p^r\) ................................. 50
T. Westerbäck: Applications of algebraic combinatorics to codes and dis-
tributed storage systems ......................................................................... 51
W. Willems: On linear codes with complementary duals ......................... 51
J. Zumbrägel: Designs in affine geometry .................................................. 52

List of participants 53
Welcome from the Organizing committee

It is our utter pleasure to welcome you to the final event of COST Action IC1104: Random Network Coding and Designs over $GF(q)$. The venue for this conference has been chosen paying particular attention to various aspects defining the spirit of the COST programme. Beyond these, we feel that Dubrovnik, a city of long history and cultural wealth makes a perfect contrast with the cutting edge engineering and mathematical disciplines covered by this conference.

Random network coding and all related theory is indeed of high interest nowadays within the mathematical, computer science, and electrical engineering community. We believe that, through all previous events of this Action, we have connected researchers from the entire spectrum between pure theoretic sciences to applied practical disciplines. We also hope that you share our belief that a respectable well-connected open European community of researchers has been established during the last four years of our cooperation.

As you will see, our scientific programme covers many areas and aspects of random network coding and combinatorial designs, in particular their connections and applications. We have received registrations from many interested members as well as some newcomers and are delighted to announce that our invited speakers are Simon Blackburn, Tuvi Etzion, Camilla Hollanti, Thomas Honold, Jonathan Jedwab, Michael Kiermaier, Mladen Kovačević, Daniel Lucani, Joachim Rosenthal, Emina Soljanin, and Angeles Vazquez-Castro. We have received 45 promising submissions for contributed talks resulting in a programme which cannot avoid parallel sessions.

Special thanks are devoted to the staff of the Centre of Advanced Academic Studies, the place where this conference is held, who have been of great support in the organization of this conference. Last but not least, we would like to acknowledge generous support not only from the COST foundation, but also from the Faculty of electrical engineering and computing of the University of Zagreb and Rochester Institute of Technology Croatia.

Thinking that this meeting makes a further albeit final highlight and formal end of a truly successful European project, we sincerely hope that you will find and remember this conference interesting and inspiring, giving you plenty of new ideas, impulses, opportunities and initiatives for your research and for future collaborations and scientific achievements.

Marcus, Vedran, Mario, Kristijan and Jens
## Conference program

**Monday, April 4th**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:45</td>
<td><strong>Opening</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:00</td>
<td>Invited talk</td>
<td>Mladen Kovačević:</td>
<td><em>Timing channels and shift-correcting codes</em></td>
</tr>
<tr>
<td>9:50</td>
<td>Invited talk</td>
<td>Michael Kiermaier:</td>
<td><em>On q-analogs of the Fano plane</em></td>
</tr>
<tr>
<td>10:40</td>
<td><strong>Coffee</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>Anna-Lena Horlemann-Trautmann:</td>
<td>Maximum rank distance codes are generic sets</td>
<td></td>
</tr>
<tr>
<td>11:35</td>
<td>Umberto Martínez-Peñas:</td>
<td><em>On the roots and minimum rank distance of skew cyclic codes</em></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td>Diego Napp:</td>
<td><em>Concatenation of convolutional codes and rankmetric codes for multi-shot network coding</em></td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td><strong>Lunch</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>Ago-Erik Riet:</td>
<td><em>Structure of large equidistant Grassmannian codes</em></td>
<td></td>
</tr>
<tr>
<td>14:25</td>
<td>Leo Storme:</td>
<td><em>Primitive t-intersection constant dimension codes</em></td>
<td></td>
</tr>
<tr>
<td>14:50</td>
<td>Sascha Kurz:</td>
<td><em>Improved upper bounds for partial spreads</em></td>
<td></td>
</tr>
<tr>
<td>15:15</td>
<td><strong>Coffee</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45</td>
<td>Reinhard Laue:</td>
<td><em>Large sets of t-designs with large blocks</em></td>
<td></td>
</tr>
<tr>
<td>16:10</td>
<td>Vedran Krčadinac:</td>
<td><em>New quasi-symmetric designs by the Kramer-Mesner method</em></td>
<td></td>
</tr>
<tr>
<td>16:35</td>
<td>Marco Buratti:</td>
<td><em>Steiner triple systems and their automorphism groups</em></td>
<td></td>
</tr>
</tbody>
</table>
### Tuesday, April 5th

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00</td>
<td><strong>Invited Talk</strong></td>
<td>Emina Soljanin: <em>On network-induced locality and decoding constraints</em></td>
<td></td>
</tr>
<tr>
<td>9:50</td>
<td><strong>Invited Talk</strong></td>
<td>Joachim Rosenthal: <em>Public key cryptosystems based on rank metric codes and subspace codes</em></td>
<td></td>
</tr>
<tr>
<td>10:40</td>
<td><strong>Coffee</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td></td>
<td>Jens Zumbrägel: <em>Designs in affine geometry</em></td>
<td></td>
</tr>
<tr>
<td>11:35</td>
<td></td>
<td>Relinde Jurrius: <em>On defining q-matroids</em></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td></td>
<td>Michael Braun: <em>On the q-analog of the revolving door algorithm</em></td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td><strong>Lunch</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td><strong>Section A</strong></td>
<td>Ángela Barbero: <em>Coding schemes with short erasure recovery delay</em></td>
<td>Francesco Pavese: <em>On mixed dimension subspace codes</em></td>
</tr>
<tr>
<td>14:25</td>
<td></td>
<td>Čedomir Stefanović: <em>Random access via sign-compute-resolve on graphs</em></td>
<td>Anamari Nakić: <em>On a property of (n, 2k − 2, k)-subspace codes</em></td>
</tr>
<tr>
<td>14:50</td>
<td></td>
<td>Joonas Pääkkönen: <em>Ensuring data availability in device-to-device caching clusters with regenerating codes</em></td>
<td>Kamil Otal: <em>Polynomial approach to construct cyclic subspace codes</em></td>
</tr>
<tr>
<td>15:15</td>
<td><strong>Coffee</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45</td>
<td></td>
<td>Selahattin Gökceli: <em>A random network coding testbed</em></td>
<td>Daniel Heinlein: <em>Coset construction for subspace codes</em></td>
</tr>
<tr>
<td>16:10</td>
<td></td>
<td>Peter Farkaš: <em>Distributed method for topological interference alignment and its connection with network coding</em></td>
<td>Alberto Ravagnani: <em>Equidistant subspace codes</em></td>
</tr>
<tr>
<td>16:35</td>
<td></td>
<td>Marco Calderini: <em>Bounding the optimal rate of the ICCSI problem</em></td>
<td>Daniele Bartoli: <em>Equidistant subspace codes</em></td>
</tr>
<tr>
<td>Time</td>
<td>Session</td>
<td>Speaker(s)</td>
<td>Title</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9:00</td>
<td>INVITED TALK</td>
<td>Thomas Honold</td>
<td>Constant-dimension codes exceeding the LMRD code bound</td>
</tr>
<tr>
<td>9:50</td>
<td>INVITED TALK</td>
<td>Angeles Vazquez-Castro</td>
<td>Coding and network coding over flag varieties</td>
</tr>
<tr>
<td>10:40</td>
<td>Coffee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>SECTION A</td>
<td>Stefan E. Schmidt</td>
<td>Generalized metrics for network coding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Andrea Švob</td>
<td>The Cameron-Liebler problem for sets</td>
</tr>
<tr>
<td>11:35</td>
<td>SECTION B</td>
<td>Tobias Gaebel-Hoekenschneider</td>
<td>Cameron–Liebler type sets and completely regular codes in Grassmann graphs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morgan Rodgers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network based measurement theory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Umberto Martínez-Peñas</td>
<td>Rank error-correcting pairs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Montserrat Alsina</td>
<td>On centers of hyperbolic tessellations and their applications</td>
</tr>
<tr>
<td>12:00</td>
<td>Lunch Package</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30</td>
<td>Individual tour</td>
<td></td>
<td>Individual tour of the city walls</td>
</tr>
<tr>
<td>15:15</td>
<td>Guided city tour</td>
<td></td>
<td>Guided city tour</td>
</tr>
<tr>
<td>17:45</td>
<td>Conference dinner</td>
<td></td>
<td>Conference dinner</td>
</tr>
</tbody>
</table>
### Thursday, April 7th

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00</td>
<td>INVITED TALK</td>
<td>Locally repairable codes with availability and hierarchy: Matroid theory via examples</td>
<td>Camilla Hollanti</td>
</tr>
<tr>
<td>9:50</td>
<td>INVITED TALK</td>
<td>How many mutually unbiased bases can exist in complex space of dimension d?</td>
<td>Jonathan Jedwab</td>
</tr>
<tr>
<td>10:40</td>
<td>Coffee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>Natalia Silberstein:</td>
<td>Binary locally repairable codes with high availability via anticodes</td>
<td></td>
</tr>
<tr>
<td>11:35</td>
<td>Vitaly Skachek:</td>
<td>New bound for batch codes with restricted query size</td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td>Thomas Westerbäck:</td>
<td>Applications of algebraic combinatorics to codes and distributed storage systems</td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>Marina ˇSimac:</td>
<td>LDPC codes based on μ-geodetic graphs</td>
<td>Harald Gropp: Orbital matrices again</td>
</tr>
<tr>
<td>14:25</td>
<td>Regina Judák and Dávid Mezőfi:</td>
<td>Comparison of some linear codes with high noise binary channel</td>
<td>Doris Dumićić Danilović: Block designs and self-orthogonal codes constructed from orbit matrices</td>
</tr>
<tr>
<td>14:50</td>
<td>Wolfgang Willems:</td>
<td>On linear codes with complementary duals</td>
<td>Vedrana Mikulić Crnković: On self-orthogonal codes generated by orbit matrices of 1-designs</td>
</tr>
<tr>
<td>15:15</td>
<td>Coffee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45</td>
<td>Paulo Almeida:</td>
<td>Optimal 2D convolutional codes</td>
<td>Netanel Raviv: Coding for locality in reconstructing permutations</td>
</tr>
<tr>
<td>16:10</td>
<td>Marisa Toste:</td>
<td>On MDS convolutional codes over $\mathbb{Z}_p$</td>
<td>Kristijan Tabak: Normalized difference sets tiling in $\mathbb{Z}_p$</td>
</tr>
<tr>
<td>16:35</td>
<td>Philippe Moustrou:</td>
<td>On the density of cyclotomic lattices constructed from codes</td>
<td></td>
</tr>
</tbody>
</table>
### Friday, April 8th

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker/Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00</td>
<td>INVITED TALK</td>
<td>Daniel E. Lucani: <em>Composite extension fields for (network) coding: Designs and opportunities</em></td>
</tr>
<tr>
<td>9:50</td>
<td>INVITED TALK</td>
<td>Simon R. Blackburn: <em>Cryptography and network coding</em></td>
</tr>
<tr>
<td>10:40</td>
<td>COFFEE</td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>Raquel Pinto:</td>
<td><em>Rank metric convolutional codes</em></td>
</tr>
<tr>
<td>11:35</td>
<td>INVITED TALK</td>
<td>Tuvi Etzion: <em>What is old, what is new, and what to do?</em></td>
</tr>
<tr>
<td>12:25</td>
<td>CLOSING</td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td>LUNCH</td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>MC MEETING</td>
<td></td>
</tr>
</tbody>
</table>
Invited talks
Cryptography and network coding

Simon R. Blackburn
Royal Holloway University of London, United Kingdom
Department of Mathematics, Royal Holloway University of London
Egham, Surrey TW20 0EX

Cryptography and network coding influence each other in various ways: cryptographic schemes have been designed to prevent packet pollution for network coding by adding signatures; linear techniques connect notions of privacy when network coding is used with the construction of secret sharing schemes; network codes have been proposed as platform for asymmetric cryptosystems (analogues of the McEliece cryptosystem). This talk will survey some of these connections, in particular highlighting some of the advances made under the COST Action.

What is old, what is new, and what to do?

Tuvi Etzion
Technion, Israel
Department of Computer Science
Technion, Haifa 32000, Israel

In this talk we will give the history before network coding was introduced, the main results in network coding before the COST Action, and new results obtained during the Action. The focus will be on results related to the basics of network coding, error-correcting codes in random network coding, and related designs over GF(q). Finally, we will discuss the main directions for future research.
Invited talks

9

Locally repairable codes with availability and hierarchy:
Matroid theory via examples

Camilla Hollanti
Aalto University, Finland

Dept. of Mathematics and Systems Analysis, P.O.Box 11100, FI-00076 Aalto

Joint work with Ragnar Freij-Hollanti and Thomas Westerbäck.

Recent research on distributed storage systems has revealed interesting connections between matroid theory and locally repairable codes (LRCs). The goal of this talk is to illustrate these as well as some new results via simple examples. The examples embed all the essential features of LRCs, namely locality, availability, and hierarchy alongside with related generalized Singleton bounds. The talk is based on [1].

References


Constant-dimension codes exceeding the LMRD code bound

Thomas Honold
Zhejiang University, China

Department of Information Science and Electronics Engineering
Zhejiang University, 38 Zheda Road, 310027 Hangzhou, China

Joint work with J. Ai and H. Liu.

The $k$-dimensional codewords of a lifted maximum rank distance (LMRD) code $\mathcal{L}$ have a common complementary subspace $S$ in their ambient space $V$ and, for some $t \in \{1, \ldots, k-1\}$, form a perfect cover of the set of $t$-dimensional subspaces of $V$ disjoint from $S$. This implies that the remaining codewords in any constant-dimension code $\mathcal{C}$ containing $\mathcal{L}$ meet $S$ in a subspace of dimension $> k - t$, and leads to an upper bound on the size of such codes [3], which we call the *LMRD code bound*. When extending the expurgation-augmentation method [5],[4] for constructing good plane subspace codes to packet lengths $v > 7$, we have recently found infinite families of binary plane subspace codes exceeding the LMRD code bound [1], as predicted in [2]. In my talk I will present an overview of the new construction and its ramifications, which include subspace polynomials and Dickson invariants.
References


How many mutually unbiased bases can exist in complex space of dimension \(d\)?

Jonathan Jedwab
Simon Fraser University, Canada

8888 University Drive, Burnaby BC, V5A 1S6, Canada

Joint work with Lily Yen, Capilano University, Canada.

A set of \(m\) mutually unbiased bases in \(\mathbb{C}^d\) comprises \(md\) unit vectors in \(\mathbb{C}^d\), partitioned into \(m\) orthonormal subsets (bases) of size \(d\) such that the pairwise angle between all vectors from distinct subsets is \(\arccos(1/\sqrt{d})\). Schwinger noted in 1960 that no information can be obtained when a quantum system is prepared in a state belonging to one of the bases of such a set but is measured with respect to any other one of the bases. This property can be exploited in secure quantum key exchange, quantum state determination and quantum error-correcting codes.

The central problem is to determine the largest number \(\mu(d)\) of mutually unbiased bases that can exist in \(\mathbb{C}^d\). It has been known for 40 years that \(\mu(d) \leq d + 1\), but a construction achieving the upper bound \(d + 1\) is known only when \(d\) is a prime power. Despite considerable effort and a huge literature, there has been little progress in
determining $\mu(d)$ when $d$ is not a prime power, with the notable exception of Weiner’s 2013 result that $\mu(d)$ never equals $d$. Even the smallest non-prime-power case $d = 6$ remains baffling: all that is known is that $\mu(6) \in \{3, 4, 5, 7\}$.

I shall give an overview of the current state of knowledge for this problem, and describe some new insights involving combinatorial designs.

---

**On $q$-analogs of the Fano plane**

Michael Kiermaier  
University of Bayreuth, Germany

Motivated by the application in error-correction in randomized network coding, $q$-analogs of combinatorial designs have gained a lot of interest lately. Arguably the most important open problem in this field is the question of the existence of a $q$-analog of the Fano plane, as it has the smallest admissible parameter set of a non-trivial $q$-Steiner system with $t \geq 2$.

In this talk, an introduction to this problem will be given. Several results on the structure of $q$-analogs of the Fano plane will be discussed, including intersection numbers and the automorphism group.

---

**Timing channels and shift-correcting codes**

Mladen Kovačević  
National University of Singapore

Dept of ECE, 4 Engineering Drive 3, Singapore 117583  
Joint work with Petar Popovski and Miloš Stojaković.

In several communication and information storage systems the dominant type of “noise” introduced by the channel are shifts of symbols of the transmitted sequence. A classic example is the so-called bit-shift or peak-shift channel [7] which has been introduced as a model for some magnetic recording devices wherein the electric charges (the 1-bits) can be shifted to the left or to the right of their original position due to various physical effects. Another familiar scenario is the transmission of information packets through a queue with random service times. Such a queue is intended to model, e.g., a network router processing the packets and then forwarding them towards their destination. It has been shown [1] that the capacity of such channels can be increased by encoding the information in the transmission times of
packets, in addition to their contents. Unknown delays of packets at the output of the queue represent the noise in this case. Another setting where timing channels naturally arise are molecular communications. The information here is contained in the number and the types of particles released at given time instants, and the noise are random delays that particles experience on their way to the receiving side, caused by their interaction with the fluid medium. Motivated by the above examples, we introduce a channel model that is intended to capture such impairments. The model is described in combinatorial, rather than probabilistic terms, as we are interested primarily in the zero-error problems [8].

The channel is most easily defined in terms of its effect on the possible inputs. Let \( n, P, K_1, K_2 \) be integers, with \( K_1 \leq K_2 \) and \( n, P \) nonnegative. The channel inputs are sequences \( x = (x_1, \ldots, x_n) \) of length \( n \) over an alphabet \( \{0, 1, \ldots, P\} \). One can think of these sequences as representing the states of an \( n \)-cell register, where \( x_i = 0 \), \( 1 \leq i \leq n \), means that the \( i \)’th cell is empty, while \( x_i = p, p \in \{1, \ldots, P\} \), means that the \( i \)’th cell contains a “particle” of type \( p \). For any such input sequence the channel outputs (at random) one of the sequences \( y = (y_1, \ldots, y_n) \) satisfying the following conditions: 1) The subsequences \( \tilde{x} = (x_{i_1}, \ldots, x_{i_m}) \) and \( \tilde{y} = (y_{j_1}, \ldots, y_{j_{m'}}) \) obtained by deleting all the zeros in \( x \) and \( y \) respectively, are identical (and hence \( m = m' \)), and 2) \( K_1 \leq j_l - i_l \leq K_2 \) for all \( 1 \leq l \leq m \). In words, every particle can shift \( k \) cells away from its original position, \( K_1 \leq k \leq K_2 \), and no two particles can swap cells or end up in the same cell.

We shall construct optimal zero-error codes of arbitrary length \( n \) for this channel, determine its zero-error capacity and describe its dependence on the channel parameters \( P, K_1, K_2 \). Several variants and extensions of the model – with multiple particles per cell, with continuous-time shifts, and with additional types of noise – will also be discussed, as well as some related open problems.

References
Composite extension fields for (network) coding: Designs and opportunities

Daniel E. Lucani
Aalborg University, Denmark
Fredrik Bajers Vej 7, A3-110, Aalborg

Joint work with Olav Geil, Diego Ruano, Janus Heide.

Coding theory has typically relied on a single finite field for the design of specific codes with few exceptions. One such exception are concatenated codes [1], which may use two codes with different finite fields as their inner and outer code. However, exploiting a mixture of different field sizes in the design of a single code without concatenation has only been considered recently in the context of network coding (NC) [2]. Part of the limitation may be related to the finite field construction: finite fields of different sizes are not compatible in general. This means that a product operation in the smaller field over a group of symbols in the small field does not necessarily map to the equivalent operation in the higher field, where the group of symbols in the smaller field is seen as a single symbol. Using multiple fields of different size that are compatible provides interesting opportunities from the perspective of speeding up computation and catering to a multiplicity of devices with different computation capabilities.

From this perspective, this talk will focus on (i) the construction of composite extension fields that maintain compatibility of smaller fields with larger fields constructed from the smaller fields; (ii) the design of codes that use multiple extension fields for reducing signalling overhead and increasing encoding and decoding speed; (iii) the application of these fields in network coding [3], e.g., as an extension to standard Random Linear Network Coding (RLNC) [4] or Fulcrum network codes [5]; and (iv) rethinking standard code constructions in the light of these composite extension fields.

References


Public key cryptosystems based on rank metric codes and subspace codes

Joachim Rosenthal
University of Zürich, Switzerland
Mathematics Institute
Winterthurerstr 190
CH-8057 Zurich, Switzerland

Joint work with Kyle Marshall and Anna-Lena Trautmann.

Asymmetric ciphers based on hard decoding problems belong to the most prominent public key ciphers in the post-quantum crypto area. This is based on the hope that their security might still exist even if a quantum computer is ever built. Since the original paper of Robert McEliece many variants have been proposed and crypto-analysed.

In this overview talk we will study public key ciphers where the public key represents a disguised Gabidulin code or more generally a subspace code. We will show how such systems can be possibly constructed and point out weaknesses of systems proposed in the literature.

References


On network-induced locality and decoding constraints

**Emina Soljanin**
Rutgers University, USA

94 Brett Rd, Piscataway, NJ 08854

In networks that implement linear network coding, edges carry linear combinations of their parent node inputs, and consequently, linear combinations of the source symbols. The classical network coding multicast problem asks: How should nodes combine their inputs to ensure that the edges observed by a receiver carry independent combinations of the source symbols? Moreover, what is the minimum field size necessary to realize linear combinations throughout the network with these properties? This problem is completely solved in the case of two sources and arbitrarily many receivers, but in no other cases. It is strongly related to problems in other areas of coding theory, such as the classical problem of finding MDS generator matrices over small fields with zeros in certain prescribed entries, and the more recent problem of locality in coding for distributed storage. This talk will introduce network multicast in an elementary way through a combinatorial/algebraic framework as in [1], present an open problem, and discuss connections with classical coding theory.

References


Coding and network coding over flag varieties

**Angeles Vazquez-Castro**
Autonomous University of Barcelona, Spain

Campus Universitari, Bellaterra, Barcelona

Joint work with Gabriele Nebe, Aachen University, Germany.

Coding for errors and erasures over random network coding is a well established area of research since the seminal work by Koetter and Kschischang in [1], where a novel framework of subspace coding is proposed. The key assumption underlying subspace coding is that channel and network codes operate separately (incoherent transmission), i.e. the error/erasure correcting code is designed end-to-end, oblivious of what the network coding coefficients are.

In this work, we extend the applicability of such framework under the assumption that in-network nodes can keep track of packet sequence numbering, as it is
the case on the Internet. To such aim, we introduce a geometrical approach consisting of capturing the communication process with group actions [2] and encoding information over flag varieties.

Let \( q \) be some prime power, \( n \in \mathbb{N} \), and \( V = \mathbb{F}_q^n \). A flag is a set of subspaces \( \Lambda := \{ V_i : 0 \leq i \leq m \} \) of \( V \) with \( \{0\} = V_0 < V_1 < \ldots < V_m = V \). The dimension of a flag \( \Lambda \) is \( |\Lambda| - 2 = m - 1 \). The intersection of two flags is again a flag. There is just one 0-dimensional flag \( \{\{0\}, V\} \); it is contained in all other flags. The 1-dimensional flags \( \{\{0\} \subseteq V_1, V\} \) are in bijection to the proper subspaces \( V_1 \) of \( V \). A flag is called full, if its dimension is \( n - 1 \). The number of full flags in \( V \) is

\[
N_{\text{flag}}^n = \left( \frac{q^n - 1}{q - 1} \right) \times \left( \frac{q^n - q}{(q - 1)q} \right) \times \ldots \times \left( \frac{q^n - q^{n-1}}{(q - 1)q^{n-1}} \right).
\]

Under our approach, we encode information over flags such that maximal flags correspond to transmission when there are no errors nor erasures in the network. Then, by using known facts of group actions over flag varieties, we show that network codes are the stabilisers of the flag-encoded information as it traverses the network.

Our approach subsumes other approaches, including codes over Grassmannians over random network coding and network coding over noiseless networks. Furthermore, it provides a framework for adaptive encoding and decoding for dynamic networks over different communication ambient spaces.

References


Contributed talks
Optimal 2D convolutional codes

Paulo Almeida
CIDMA, Universidade de Aveiro, Portugal

Joint work with D. Napp and R. Pinto.

When considering data recorded in two dimensions, like pictures and video, two-dimensional (2D) convolutional codes seem to be a better framework to encode such data than one-dimensional (1D) codes, since it takes advantage of the interdependence of the data in more than one direction. The distance of a 2D convolutional code of rate $1/n$ and degree $\delta$, is bounded by the 2D generalized Singleton bound, i.e.

$$\text{dist}(C) \leq \frac{(\delta + 1)(\delta + 2)}{2} n.$$ 

We introduce a new type of superregular matrices that give rise to novel constructions of two-dimensional convolutional codes with finite support. These codes are of rate $1/n$ and degree $\delta$ with $n \geq \delta + 1$ and achieve the 2D generalized Singleton bound.

On centers of hyperbolic tessellations and their applications

Montserrat Alsina
Universitat Politècnica de Catalunya, Spain

Dept. Matemàtiques, EPSEM, Manresa

Signal constellations in the hyperbolic plane have been considered in several papers (cf. [2]-[5], among others), since hyperbolic geometry provides significative properties and strong relations with algebraic structures such as quaternion algebras, quadratic forms and Fuchsian groups (cf. [1]). In particular, infinitely many hyperbolic tessellations can be derived by using fundamental domains of Shimura curves associated to orders in quaternion algebras.

In this work we explore how to choose well centered points on those tessellations in order to obtain a good behaviour for applications to signals and codes. Hyperbolic geometry tools play an important role, and have been studied in conjunction with elements of euclidian geometry also present on the applications. Mathematics visualization software to deal with hyperbolic geometry is also explored.

References


Coping schemes with short erasure recovery delay

Ángela Barbero
Universidad de Valladolid, Spain
Joint work with Øyvind Ytrehus.

In many practical communication applications, such as multimedia transmission over packet erasure channels, on-time delivery is an important quality-of-service criterion. This has led to an increased interest [1] in the design and analysis of coding systems designed for such applications. There are two main approaches to this coding problem that have been discussed in the literature.

In [2,3], random coding has been proposed as a solution. Basically, in these schemes, the sender transmits \( k \) uncoded information packets, followed by \( n - k \) parity check packets formed by random linear combinations of all information that have not been acknowledged by the receiver so far.

The other approach is presented in [4,5], where packets are sent using a \( q \)-ary convolutional code with a good column distance profile.

We analyze and compare these two approaches with respect to code rate, delay of recovery, probability of recovery failure, recovery complexity, and flexibility. For completeness, binary convolutional codes [6] are also included in the comparison. It turns out that it may be an advantage to apply a hybrid combination of the two approaches. We present such a hybrid scheme and analyze its properties and performance.

References


---

**Equidistant subspace codes**

**Daniele Bartoli**

University of Perugia, Italy

via Vanvitelli 1, Perugia

Joint work with F. Pavese, S. Marcugini, F. Pambianco.

In [1] a classification of the largest 1-intersecting codes in $PG(5, 2)$, whose codewords are planes, is provided. In this talk I will present new results concerning sets of 3-spaces pairwise intersecting in lines in binary spaces.

**References**

On the $q$-analog of the revolving door algorithm

Michael Braun
University of Applied Sciences, Darmstadt, Germany

Faculty of Computer Sciences
Schoefferstr. 8b
D-64295 Darmstadt

In this talk we describe a recurrence to generate a sequence containing all $n \times k$ column reduced Echelon forms over the finite field $\mathbb{F}_q$ with $q$ elements such that two consecutive Echelon forms differ in exactly one position. The corresponding sequence of subspaces generated by the Echelon forms define a cyclic Gray code sequence on the Grassmannian containing all $k$-dimensional subspaces of $\mathbb{F}_q^n$ with respect to the injection metric of subspaces. Furthermore, plugging $q = 1$ into the recurrence yields a revolving door algorithm of the set of $k$-element subsets on a set with $n$ elements.

Steiner triple systems and their automorphism groups

Marco Buratti
Università di Perugia, Italy

I will survey known results and open problems about the automorphism groups of Steiner triple systems.

Bounding the optimal rate of the ICCSI problem

Marco Calderini
University of Trento, Italy

Joint work with Eimear Byrne.

The index coding with side information (ICSI) problem, introduced by Birk and Kol [1], has attracted considerable attention in recent years. In the scenario of the ICSI problem, there are $m$ receivers, each with a request for a data packet from a set of $n$ packets. A central server broadcasts data to the recipients, each of which is assumed to have some side-information. The goal of the sender is then to meet each request, minimizing the total number of transmissions, given knowledge of the each receiver’s side information. The optimal rate for a scalar linear index code of an
instance of the ICSI problem was characterized, in the work of Bar-Yossef et al. [2], by the so-called min-rank its associated side information hyper graph.

Most of the methods for constructing index code (i.e. upper bounds for index coding rate) are graph theoretic. Shanmugam et al. in [3] introduced new graph theoretic index coding schemes and showed that they provably out-perform all previously known graph theoretic bounds.

The ICSI problem was generalized by Shum et al. [4] including the case of coded side information, such a problem is called index coding with coded side information (ICCSI) problem. This more general viewpoint has applications to relay networks.

In this talk we generalize the schemes given in [3] to the case of ICCSI problem, in particular we introduce the generalized clique cover number, the local generalized clique cover number, the partitioned generalized multicast number, the partitioned local generalized clique cover number and their fractional versions.

References


Block designs and self-orthogonal codes constructed from orbit matrices

Doris Dumičić Danilović
University of Rijeka, Croatia

Radmile Matejčić 2, Rijeka

Joint work with D. Crnković and S. Rukavina.

We present an algorithm for constructing 2-designs admitting a solvable automorphism group. Applying this algorithm, we construct some new Steiner 2-designs $S(2, 5, 45)$ and some new symmetric $(78, 22, 6)$ designs. One of the results is the proof of the nonexistence of $(78, 22, 6)$ difference set in the group $\text{Frob}_{39} \times Z_2$. 
Further, extending previous results on codes obtained from orbit matrices of 2-designs (see [1], [2]), we show that under certain conditions both fixed and non-fixed part of an orbit matrix span a self-orthogonal code over the finite field $F_{p^n}$ or the ring $Z_m$. We construct self-orthogonal codes over $Z_4$ spanned by orbit matrices of symmetric (78, 22, 6) designs.

References


Distributed method for topological interference alignment and its connection with network coding

Peter Farkaš

University of Electrical Eng. and Information Technology, Slovakia

Department of Transmission Systems, Inst. of Telecommunications, University of Electrical Eng. and Information Technology, Bratislava, Slovakia

Joint work with Matej Staroň and Martin Rakús and Frank Schindler.

Interference Alignment (IA) techniques are actually in focus of research, mainly, but not only because their application could increase throughput of communications networks. The roots of IA could be traced back to Informed-Source Coding-On-Demand (ISCOD) [1]. IA in context of the X channel was implicitly used in [2] and for the compound MISO broadcast channel in [3]. The idea was developed further in [4] and generalized in [5]. Since that IA has drawn lot of attention in different research areas [6]. Recently it was shown, that Index coding problem is a representative special case of network coding problem under linear coding [7]. IA could provide linear solutions at least to a part of index coding problems and so also to other equivalent problems such as Hat guessing [8], ISCOD [1], Network coding [7], and IA in partially connected interference networks [9]. The last one is equivalent to index coding problem in case that all transmitters have full knowledge about the topology of the network. These problem is known as Topological IA (TIA). Its main practical advantage is that channel knowledge is not needed in transmitters and receivers. In this talk a new very simple distributed TIA is proposed for partially

---

1Department of Transmission Systems, Inst. of Telecommunications, University of Electrical Eng. and Information Technology, Bratislava, Slovakia.

2Institute of Applied Informatics, Faculty of Informatics, Pan European University.
connected interference networks. In contrast to the known techniques it does not need full topological knowledge. Proof of concept was obtained via simulations.

References


Network based measurement theory

Tobias Gaebel-Hoekenschneider
Dresden University of Technology, Germany

We introduce an algebraic measurement setup for networks and investigate the universal measurement monoid associated with this approach. Here we provide a solution for the question how the functorial map given by a measurement setup can be extended to a generalized metric. The latter is relevant for network coding since metric considerations are crucial for information flow on networks.

A random network coding testbed

Selahattin Gökceli
Istanbul Technical University, Turkey

Joint work with Semiha Tedik Başaran and Güneş Karabulut Kurt.

From the cooperative communication perspective, network coding implies combining packets at relay nodes that aid communications. As shown by Ahlswede et al. in their prominent work, significant transmission quality improvement can be obtained through network coding [1]. Traditionally, network coding is used in wired networks. However, it cannot be adapted easily to wireless networks, where transmission errors significantly limit the transmission performance [2]. In order to address this issue, cooperative communication concept can be resorted to. Cooperative communication techniques can aid to improve the robustness of communication systems through the presence of independent transmission paths. Additionally, the time varying nature of the wireless channels, and hence the associated network topologies, need to be considered. To combat varying network topologies, instead of classical network coding which is based on deterministic coding coefficients, random network coding can be used [4]. Random network coding is the technique that transmission of linear combination of packets are realized with randomly generated coefficients [4].

Although there is a very solid theoretical background, the implementation works are sparse, especially considering the effects of the wireless communication channel. In our previous work, we have implemented a network coded cooperation system using software defined radio nodes (SDRs) [5]. In this work, we target to present our finding about implementing a random network code in a wireless testbed using SDRs. To the best of our knowledge this is the first time to implement random network coding in a wireless environment. Our observations will highlight the lessons learned during the design and realization of the considered system.
Contributed talks

References


---

Orbital matrices again

Harald Gropp

Orbital matrices are generalizations of incidence matrices of symmetric designs. The main difference is that these matrices do not only contain the entries 0 and 1 but also greater integers. Somehow a point lies on a line more than once whatever this may mean geometrically. Of course, the inner product condition has to be fulfilled, as in the case of symmetric designs.

In matrix and design theory (and in graph theory if you will) the results are comparable to symmetric designs, however there are more non-existence results, not only those by applying the theorem of Bruck-Ryser-Chowla (which also holds for orbital matrices).

Altogether this talk is meant to make orbital matrices better known to the community of people working in design theory. There will be a survey on known results as well as an idea how to go on with research in the future.
Coset construction for subspace codes

Daniel Heinlein
University of Bayreuth, Germany

Universitätsstraße 30, 95447 Bayreuth

Joint work with Sascha Kurz.

One of the main problems of the research area of network coding is to compute good lower and upper bounds of the achievable so-called subspace codes in $\text{PG}(n,q)$ for a given minimal distance. Here we generalize a construction of Etzion and Silberstein [2] to a wide range of parameters. This construction, named coset construction [1], improves several of the previously best known subspace codes and attains the MRD bound of [2] for an infinite family of parameters:

**Theorem**  For each $k \geq 4$ and arbitrary $q$ we have

$$A_q(3k - 3, 2k - 2; k) \geq q^{4k-6} + \frac{q^{2k-3} - q}{q^{k-2} - 1} - q + 1.$$

and

**Theorem**  $A_2(10, 6; 4) \geq 4173.$

**References**


Maximum rank distance codes are generic sets

Anna-Lena Horlemann-Trautmann
EPF Lausanne, Switzerland
Lausanne, Switzerland

Joint work with Alessandro Neri, Tovohery Randrianarisoa, Joachim Rosenthal.

Rank-metric codes have been around for more than 35 years. In recent years they have received increased interest due to their application in network coding. Rank-metric codes are defined as sets of matrices of a fixed size over some field, equipped with the rank metric, defined below. In this paper, as in most of the known literature, we will restrict ourselves to rank-metric codes over finite fields.

We denote the finite field with $q$ elements by $F_q$. A rank-metric code is a subset of $F_q^{m \times n}$ for some $m, n \in \mathbb{N}$. The rank metric $d_R$ on $F_q^{m \times n}$ is defined as $d_R(A, B) := \text{rank}(A - B)$ for $A, B \in F_q^{m \times n}$. The minimum rank distance of a code $C \subseteq F_q^{m \times n}$ is defined as $d(C) := \min\{d_R(A, B) \mid A, B \in C, A \neq B\}$. If we represent $F_q^{m \times n} \cong F_{q^m}$, then $C \subseteq F_q^{m \times n}$ becomes a block code in $F_{q^m}$. The definition of the rank metric translates to this setting straightforwardly. Representing codes in $F_{q^m}$ we can define linear rank metric codes, namely as subspaces of $F_{q^m}$. For a linear code $C \subseteq F_{q^m}$ of dimension $k$ we have the Singleton-type bound

$$d_R(C) \leq n - k + 1.$$ 

Codes achieving this bound are called maximum rank distance (MRD) codes. In 1979 Delsarte, and in 1985 Gabidulin, derived a construction for MRD codes for any set of parameters. This construction is based on linearized polynomials; the corresponding codes are usually called Gabidulin codes.

Only recently, other, non-equivalent constructions of MRD codes have been derived. It remains an open question however, for which parameters there are non-Gabidulin MRD codes, and how many different equivalence classes of MRD codes there are for a given set of parameters.

In this work we show that MRD codes form generic sets over the algebraic closure of $F_q$, which means that over the algebraic closure a randomly chosen linear rank-metric code almost certainly is an MRD code. Moreover, we also show that, over the algebraic closure, most of the MRD codes are non-Gabidulin. Finally we give a rough estimate on the underlying field extension degree needed, such that with high probability a randomly chosen linear code is MRD and not Gabidulin.
Comparison of some linear codes with high noise binary channel

Regina Judák and Dávid Mezőfi
University of Szeged, Hungary

Bolyai Institute, Aradi vértanúk tere 1, H-6725 Szeged

Joint work with Gábor P. Nagy.

We want to send binary packages of bit length 3000 through a binary symmetric channel with BER (bit error probability) $p = 0.1$. We search for binary linear codes of rate $R > 0.3$ such that the package error rate $PER < 0.2$. We determine the PER by simulation. In particular, the codes must have an efficient decoding algorithm. We tested two types of codes.

a) Using a binary code $M$ of dimension $d \in \{6, 7, 8\}$, we turned the binary channel into a $q$-ary erasure channel. We applied Reed-Solomon codes over the field $\mathbb{F}_q (q = 2^d)$ to correct errors and erasures. The code $M$ can be used to correct and to detect wrong symbols; its behavior depends on a threshold value. Using simulations, we determined the optimal threshold value and the optimal dimension of the RS code.

b) We studied random binary codes of dimension 16, length 32, 40 and 48, and density $\delta$ of the parity check matrix; $\delta \in [0.15, 0.55]$. We found many good $[16, 48]$-codes. The simulation showed that codes with higher density are typically better.

In our talk, we will present the statistics and some details on the implementation.

On defining $q$-matroids

Relinde Jurrius
University of Neuchâtel, Switzerland

Joint work with Ruud Pellikaan\textsuperscript{1}.

The motivation to study $q$-matroids comes from rank metric codes. There is a link between the weight enumerator of a linear code (in the Hamming metric) and the Tutte polynomial of the associated matroid. Can we do the same in the rank metric case? We will not answer that question here, but focus on the first step: we define a $q$-matroid, the $q$-analogue of a matroid.

A strong feature of matroids is that they have several cryptomorphic definitions: definitions that are equivalent, but look very different. Best known are the axiom systems for independent sets, bases, and the rank function. These definitions all

\textsuperscript{1}Eindhoven University of Technology.
have a \(q\)-analogue, however, these \(q\)-analogues are not always equivalent!

To solve this problem, we first have to ask ourselves the question: what properties do we want a \(q\)-matroid to have? We think a \(q\)-matroid should “behave nicely” under deletion, contraction, and duality. Also, we want the duality to coincide with duality in rank metric codes, which are our main examples of \(q\)-matroids.

In this talk, we will discuss the problems and possible solutions concerned with the different ways to define a \(q\)-matroid, illustrated by examples.

\[\text{Contributed talks}\]

New quasi-symmetric designs by the Kramer-Mesner method

\textbf{Vedran Krčadinac}
University of Zagreb, Croatia
Bijenička 30, Zagreb, Croatia

Joint work with Renata Vlahović.

A \(t-(v, k, \lambda)\) design is \textit{quasi-symmetric} if any two blocks intersect either in \(x\) or in \(y\) points, for non-negative integers \(x < y\). Quasi-symmetric designs have important connections with strongly regular graphs and self-orthogonal codes. We refer to the monograph [2] and the survey [3] for the main results.

In this talk we will describe how to adapt the celebrated Kramer-Mesner construction method [1] for designs with prescribed automorphism groups to the quasi-symmetric case. Using the adapted method, we can significantly increase the number of known quasi-symmetric \(2-(28, 12, 11)\) designs with \(x = 4, y = 6\) and \(2-(36, 16, 12)\) designs with \(x = 6, y = 8\). We can also construct quasi-symmetric \(2-(56, 16, 18)\) designs with \(x = 4, y = 8\), which had previously been unknown. We will give some information on the binary codes associated with the new designs.

\textbf{References}


Improved upper bounds for partial spreads

Sascha Kurz
University of Bayreuth, Germany

A partial \((k - 1)\)-spread in \(\text{PG}(n - 1, q)\) is a collection of \((k - 1)\)-dimensional subspaces with trivial intersection such that each point is covered exactly once. So far the maximum size \(A_q(n, 2k; k)\) of a partial \((k - 1)\)-spread in \(\text{PG}(n - 1, q)\) was known for the cases \(n \equiv 0 \pmod{k}\), \(n \equiv 1 \pmod{k}\) and \(n \equiv 2 \pmod{k}\) with the additional requirements \(q = 2\) and \(k = 3\). We completely resolve the case \(n \equiv 2 \pmod{k}\) for the binary case \(q = 2\).

**Theorem**  For each pair of integers \(t \geq 1\) and \(k \geq 4\) we have \[A_2(k(t+1)+2, 2k; k) = \frac{2^{k(t+1)+2} - 3 \cdot 2^{k-1}}{2^{k-1}}.\]

**Theorem**  For integers \(t \geq 1\) and \(k \geq 4\) we have \[A_3(k(t+1)+2, 2k; k) \leq \frac{3^{k(t+1)+2} - 3}{3^t - 1}.\]

Large sets of \(t\)-designs with large blocks

Reinhard Laue
University of Bayreuth, Germany

Joint work with Michael Kiermaier.

New recursion strategies give doubly infinite series of Large Sets of \(t\)-designs with large block sizes.

**Theorem**  \(LS[N](t, k, v)\) for all \(k \in (t, v - t)\) yield \(LS[N](t, \hat{k}, v + l(v - t))\) for all positive integers \(l\) and all \(\hat{k} \mod (v - t) \in (t, v - t)\).

This generalizes earlier results by Khosrovshahi and Ajooodani-Namini [1] from \(k\) to \(\hat{k}\) in the notation of the Theorem.

The Theorem applies to \(LS[2](5, k, 21)\), \(LS[3](4, k, 13)\), \(LS[3](3, k, 30)\), \(LS[3](3, k, 84)\), and \(LS[p](2, k, p + 2)\) for \(p \in \{7, 11, 17, 29\}\).

More complicated strategies deal with less complete assumptions where some Large Sets are known not to exist or their existence is yet undecided. These lead to similar series for example for \(t = 2\) and \(N = 4, 5\), and for \(t > 2\) and \(N = 2, 3, 7\).
On the roots and minimum rank distance of skew cyclic codes

Umberto Martínez-Peñas
Aalborg University, Denmark
Fredrik Bajers Vej 7G, 9220 Aalborg, Denmark

Error correction in the rank metric plays a central role in network coding. In the theory of error-correcting codes in the rank metric [2], the so-called \(q\)-cyclic codes were introduced in [2] for square matrices and have been generalized in [3] for other lengths. Independently, this notion has been generalized to skew or \(q^r\)-cyclic codes by Ulmer et al. (see [1]), where \(r\) may be different from 1.

Some Gabidulin codes are \(q\)-cyclic (see [2] and [3]), which implies that the family of \(q\)-cyclic codes include maximum rank distance (MRD) codes. In [1, 2, 3], it is also shown that these codes can be represented as left ideals in a quotient ring of linearized polynomials. Therefore, this construction of rank-metric codes seems to be the appropriate extension of cyclic codes to the rank metric.

In this work we describe skew cyclic codes using root spaces of linearized polynomials. We prove that the lattice of skew cyclic codes is anti-isomorphic to the lattice of root spaces. We also introduce the concept of cyclotomic spaces and see that they generate the lattice of root spaces, as in the classical case. We also describe cyclotomic spaces generated by elements in a normal basis.

Then we study how root spaces can be used to lower bound the minimum rank distance of skew cyclic codes. We extend the rank version of the BCH bound found in [1] to rank versions of the Hartmann-Tzeng bound and the van Lint-Wilson bound, as they appear in [4].

We conclude by showing that classical cyclic codes equipped with the Hamming metric can be seen as skew cyclic codes equipped with the rank metric, which also shows the relevance of these latter family of codes.

This work corresponds to [5].

References


---

**Rank error-correcting pairs**

**Umberto Martínez-Peñas**  
Aalborg University, Denmark

Fredrik Bajers Vej 7G, 9220 Aalborg, Denmark

Joint work with Ruud Pellikaan, Eindhoven University of Technology.

Error-correcting pairs (ECPs) were introduced independently by Pellikaan in [4] and by Kötter in [3], which define an error-correcting algorithm with respect to the Hamming metric. Linear codes with an ECP include many well-known families, such as (generalized) Reed-Solomon codes, many cyclic codes, Goppa codes and algebraic geometry codes (see [1] and [4]).

In the rank metric, maximum rank distance Gabidulin codes [2] have been widely used, and decoding algorithms using linearized polynomials have been given. However, more general methods of decoding with respect to the rank metric are lacking, specially for codes that are linear over the base field instead of the extension field.

In this work, we introduce some families of vector products, some of which preserve symbolic products of linearized polynomials after evaluation and which are the unique products with this property for some particular sizes.

Then we introduce the concept of rank error-correcting pair (RECP) and give efficient decoding algorithms based on them. We define RECPs for codes that are linear over the extension field and RECPs for codes that are linear over the base field, and prove that the latter type generalize the former type.

Afterwards we derive bounds on the minimum rank distance and give MRD conditions based on RECPs. Finally we study some families of codes that admit RECPs, showing that the given algorithm generalizes the classical algorithm using error-correcting pairs for the Hamming metric.

This work corresponds to [5].

**References**

On self-orthogonal codes generated by orbit matrices of 1-designs

Vedrana Mikulić Crnković
University of Rijeka, Croatia

Radmilj Matejčić 2

Joint work with Dean Crnković.

Lately, some methods for constructing self-orthogonal codes generated by an orbit matrix of a 2-design or a strongly regular graph were developed. We take into consideration linear codes (over some field) generated by the incidence matrices of 1-designs, and by orbit matrices of those structures.

Furthermore, one can construct a binary self-orthogonal code of a self-orthogonal and weakly self-orthogonal 1-design. We analyze under which assumptions is code generated by the incidence matrix or an orbit matrix of a 1-design self-orthogonal and give some examples.
On the density of cyclotomic lattices constructed from codes

Philippe Moustrou
University of Bordeaux, France

Lattices play an important role in communications. It is known that, when the dimension grows, a random lattice behaves well with respect to several related problems, such as sphere packing and covering, channel coding and quantization. It is however desirable to design restricted families of lattices, possibly having additional structure, that retain the benefits of the random. Here we consider this question for the sphere packing problem.

Let $\Delta_n$ denote the supremum of the sphere packing density that can be achieved by a lattice in dimension $n$. Let us recall that Minkowski-Hlawka proved by an averaging argument that asymptotically $\Delta_n \geq \frac{1}{2^{n-1}}$. Later Rogers improved this bound by a linear factor. Gaborit and Zémor in [1] gave an “effective” proof of this result: for infinitely many dimensions $n$, they exhibited a finite (although with exponential size) family of lattices, constructed from linear codes via Construction A, containing lattices achieving this density. Moreover in their construction the lattices afford the action of a cyclic group of order half the dimension.

Recently, Venkatesh [2] showed that for infinitely many dimensions $n$, $\Delta_n \geq \frac{n \log \log n}{2^{n+1}}$, which is the first result improving the linear growth of the numerator. He obtained this result by considering lattices in cyclotomic fields invariant under the action of the group of roots of unity.

Here we use an adaptation of Construction A for cyclotomic fields in order to exhibit finite families of lattices that reach Venkatesh’s density for the same sequence of dimensions. We also provide lattices with density larger than $\frac{cn}{2^n}$ for a set of dimensions which is somewhat larger than that of Gaborit and Zémor. With some slight modifications in our construction, we obtain lattices that are moreover symplectic, a property of interest in the study of principally polarized abelian varieties, thus complementing the result of Autissier [3].

References


On a property of $(n, 2k - 2, k)$-subspace codes

Anamari Nakić
University of Zagreb, Croatia
Unska 3, 10000 Zagreb, Croatia

Joint work with Leo Storme.

We present a result on extendability of specific constant dimension subspace codes [1]. An $(n, M, d, k)$-subspace code over $\mathbb{F}_q$ is a set of $M$ $k$-dimensional subspaces of $\mathbb{F}_q^n$ having minimum distance $d$. We focus on large $(n, M, 2k - 2, k)$-subspace codes over $\mathbb{F}_q$. A well-known upper bound on the maximum size of such a code is

$$M \leq \left\lceil \frac{n}{2} \right\rceil_q / \left\lceil \frac{k}{2} \right\rceil_q. \quad (1)$$

Our main result is the following [1].

**Theorem** Let $n \equiv 0 \pmod{k}$, $(n - 1) \equiv 0 \pmod{k - 1}$ and $1 \leq \delta \leq (q + 1)/2$. Let $\mathcal{C}$ be an $(n, M, 2k - 2, k)$-code, with $M = \left\lceil \frac{n}{2} \right\rceil_q / \left\lceil \frac{k}{2} \right\rceil_q - \delta$. Then $\mathcal{C}$ can be extended to an $(n, \left\lceil \frac{n}{2} \right\rceil_q / \left\lceil \frac{k}{2} \right\rceil_q, 2k - 2, k)$-code $\mathcal{C}'$.

This result implies that if no $(n, \left\lceil \frac{n}{2} \right\rceil_q / \left\lceil \frac{k}{2} \right\rceil_q, 2k - 2, k)$-code exists, then the upper bound (1) can be improved by $(q + 1)/2$.

We give an insight into the technique, coming from finite geometry, that we used to prove this result. We briefly discuss a more general extendability result on some other classes of constant dimension subspace codes whose parameters satisfy specific divisibility conditions. We finally give an application of the mentioned result.

**References**

Contributed talks

Concatenation of convolutional codes and rankmetric codes for multi-shot network coding

Diego Napp
University of Aveiro, Portugal
Joint work with R. Pinto and V. Sidorenko.

In this paper we propose a novel coding approach to deal with the transition of information over network. In particular we make use of the network several times (multi-shot) and decode the information via an inner and an outer code, namely, a convolutional code as an outer code and a rank metric code as an inner code.

Let \( C_O \) be an \((n, k, \delta)\) convolutional code with (Hamming) distance \( d_{\text{free}}(C_O) \), column distance \( d_{cj}(C_O) \) and a minimal basic encoder \( G_O(D) \) and \( C_I \) a rank metric code with (rank) distance \( d_{\text{rank}}(C_I) \) and encoder \( G_I(D) \).

Let \( u(D) = u_0 + u_1 D + u_2 D^2 + \cdots \in \mathbb{F}_q[D]^k \) be the information vector.

Encode it through \( G_O(D) \) to obtain
\[
 v(D) = v_0 + v_1 D + v_2 D^2 + \cdots = u(D)G_O(D) \in C_O \subset \mathbb{F}_q^m.
\]

Finally, the codewords of \( C \) are obtained through the image of the matrix \( G_I(D) \in \mathbb{F}_q^m \times N \)
\[
 x(D) = x_0 + x_1 D + x_2 D^2 + \cdots = v(D)G_I(D) \in \mathbb{F}_q^N.
\]

In this work we shall investigate the distance properties of this concatenated code (we assume throughout the paper that \( m > N \)).

The Sum Rank distance of the concatenated code, \( d_{\text{sumrank}}(C) \), of \( C \) is
\[
 d_{\text{sumrank}}(C) = d_{\text{free}}(C_O) \times d_{\text{rank}}(C_I).
\]

**Theorem** The Column Sum Rank distance, \( d_{cj}^C \), of \( C \) is
\[
 d_{cj}^C(C) = d_{cj}^C(C_O) \times d_{\text{rank}}(C_I).
\]

**Theorem** If any sliding window of length \((j_0+1)n\) at most \((d_{cj}^C(C)+1)(n-k)\) packet losses (erasures) occur, then we can completely decode the information sequence.

References


Polynomial approach to construct cyclic subspace codes

Kamil Otal
Middle East Technical University, Turkey

Middle East Technical University
Mathematics Department and Institute of Applied Mathematics
Ankara/Turkey

Joint work with Ferruh Özbudak.

Subspace codes and particularly constant dimensional subspace codes are the main mathematical objects in random network coding due to their error correction capability given in [2]. In particular, cyclic subspace codes are very useful subspace codes with efficient encoding and decoding algorithms. In [1] the authors provided a method to construct cyclic subspace codes using subspace polynomials. They have given explicit constructions of cyclic codes of size \( n \frac{q^N - 1}{q - 1} \) and distance \( 2k - 2 \) where \( N \) is the length, \( k \) is the dimension, \( n \) is a prime dividing \( N \), and \( q \) is the size of the field codewords are over. In this study we improve and generalize their construction by increasing the size up to \( (q^n - 1) \frac{q^N - 1}{q - 1} \). We also give a general condition for the sets of subspace polynomials used to construct these codes and in this way we obtain more diverse sets and more diverse \( N \) values. Later on, we obtain the theorem for the distance not only \( 2k - 2 \) but also \( 2k - 2s \) where \( s \) is a positive integer less than or equal to \( k \).

References


Ensuring data availability in device-to-device caching clusters with regenerating codes

Joonas Pääkkönen
Aalto University, Finland

Joint work with Amaro Barreal, Camilla Hollanti, Olav Tirkkonen.

We consider a cluster of mobile terminals in a wireless cellular network located relatively far away from base stations. The users in the cluster form a caching community where they cache and transmit data through device-to-device (D2D)
communication, thus offloading traffic away from the traditional cellular network. We see how local communication can decrease the total energy consumption due to shorter link distances. However, a natural problem of wireless caching arises as the users are free to roam in and out of the cluster, and therefore cached data can be easily lost.

As the main focus of our work, we investigate under what circumstances modern erasure coding originally developed for distributed storage can be utilized to ensure that data stay available in the cluster despite user mobility. We give analytical expression for choosing optimal coding methods for a given set of system and data parameters. We show that distributed wireless caching leads to considerable energy consumption savings and/or storage space savings over uncoded caching and naive data replication schemes.

---

**On mixed dimension subspace codes**

**Francesco Pavese**

University of Gent, Belgium

Krijgslaan 281, 9000 Ghent

Joint work with A. Cossidente and L. Storme.

Let $V$ be an $n$-dimensional vector space over $GF(q)$, $q$ any prime power. The set $S(V)$ of all subspaces of $V$, or subspaces of the projective space $PG(V)$, forms a metric space with respect to the subspace distance defined by $d_s(U,U') = \dim(U + U') - \dim(U \cap U')$. In the context of subspace codes, the main problem is to determine the largest possible size of codes in the space $(S(V),d_s)$ with a given minimum distance, and to classify the corresponding optimal codes. The interest in these codes is a consequence of the fact that codes in the projective space and codes in the Grassmannian over a finite field referred to as mixed dimension subspace codes and constant dimension subspace codes, respectively, have been proposed for error control in random linear network coding. An $(n,M,d)_q$ mixed dimension subspace code is a set $\mathcal{C}$ of subspaces of $V$ with $|\mathcal{C}| = M$ and minimum subspace distance $d_s(\mathcal{C}) = \min\{d_s(U,U') \mid U,U' \in \mathcal{C}, U \neq U'\} = d$. In this talk I will discuss the mixed dimension case in vector spaces of small dimensions.
Rank metric convolutional codes

Raquel Pinto
University of Aveiro, Portugal

Joint work with J. Rosenthal, D. Napp and P. Vettori.

Most of the theory of Random Linear Network Coding developed so far is concerned with the so-called non-coherent one-shot network coding [1], meaning that the random (i.e., unknown) structure of the net is used just once to propagate information.

However, coding can also be performed over multiple uses of the network, whose internal structure may change at each shot, giving rise to the so-called multi-shot coding. In particular, creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities [2].

To attain this goal, we propose to use rank metric convolutional codes, as this type of codes permits adding complex dependencies to data streams in a quite simple way (see [3] for the particular case of unit memory convolutional codes). In this case, an extension of the standard rank metric over multiple shots, which is analogous to the extended subspace distance defined in [3], will provide the proper measure for the number of rank erasures that a code can tolerate. It is worth mentioning that this approach has been recently used to cope very efficiently with network streaming applications such as video streaming (see [4] and the references therein).

In this contribution, we aim to further explore this direction. Specifically, we introduce a first general definition of rank metric convolutional codes, we propose a suitable concept of distance, and we study the Singleton bound for this class of codes.

References


Equidistant subspace codes

Alberto Ravagnani
Université de Neuchâtel, Switzerland

Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

Joint work with Elisa Gorla.

In the last few years, subspace codes endowed with the subspace distance have received a lot of attention, mostly due to their applications in random linear network coding. A subspace code is defined as a collection of vector spaces of the same dimension over a finite field. According to the subspace distance, two vector spaces of the same dimension are far from each other if their intersection is small.

In this talk we concentrate on equidistant codes, i.e., subspace codes where every two distinct codewords are at the same distance. Equidistant codes were recently proposed by T. Etzion and N. Raviv for use in distributed storage. A very special family of equidistant codes are sunflower, i.e., subspace codes where every two distinct codewords intersect in the same vector space.

We first provide a structural classification of optimal equidistant codes, proving that, for most choices of the parameters, an equidistant code of maximum cardinality is either a sunflower, or the orthogonal of a sunflower. This result shows that most optimal equidistant codes have a very simple structure.

We then propose a structured construction of sunflower codes having asymptotically optimal parameters. Our construction relies on partial spread codes, and represents a sunflower as a family of matrices having a prescribed form.

Finally, we provide an efficient decoding algorithm for our sunflower codes, showing that their decoding procedure can be efficiently reduced to partial spread decoding.
Coding for locality in reconstructing permutations

Netanel Raviv
Technion, Israel

Computer Science Department, Technion – Israel Institute of Technology, Haifa
3200003, Israel

Joint work with Prof. Eitan Yaakobi¹ and Prof. Muriel Méardard².

The problem of storing permutations in a distributed manner arises in several common scenarios, such as efficient updates of a large, encrypted, or compressed data set. This problem may be addressed in either a combinatorial or a coding approach. The former approach boils down to presenting large sets of permutations with locality, that is, any symbol of the permutation can be computed from a small set of other symbols. In the latter approach, a permutation may be coded in order to achieve locality. This work focuses in the combinatorial approach, provides several initial steps in the coding approach, and reveals a connection between the two.

By adapting parallel results from Locally Recoverable Codes (LRCs) [2], we provide an upper bound on the maximum size of a set of permutations with locality. An existential lower bound is also obtained from LRCs by using a counting argument on their cosets. In addition, an equivalent but particularly interesting lower bound may be achieved from sets of transversals in cyclic Latin squares (also known as the non-attacking toroidal semi-queens problem [3]).

For a very low or a very high locality we present sets of permutations which attain the upper bound. In cases where the upper bound is not attained, we provide alternative constructions using a variety of tools, such as Reed-Solomon codes over permutation polynomials, and multi-permutations.

Furthermore, we discuss how addition of redundancy allows efficient computation of any power of the stored permutation, a result which is based on [4], and conclude with a list of open problems for future research.

References


¹Computer Science Department, Technion – Israel Institute of Technology, Haifa 3200003, Israel.
²Research Lab. of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.
Structure of large equidistant Grassmannian codes

Ago-Erik Riet
University of Tartu, Estonia

University of Tartu, J. Liivi 2, 50409 Tartu, Estonia

Joint work with Daniele Bartoli, Leo Storme and Peter Vandendriessche.

We consider vector subspace codes, consisting of $k$-dimensional subspaces of $\mathbb{F}_q^n$, such that each pair of codewords, i.e. $k$-spaces intersects exactly in dimension $t$. Such a code is called a sunflower if there is a $t$-space contained in all codewords. Via a reduction to classical codes, it is known that if a code consists of more than 
\[ \left(\frac{q^k-q^t}{q-1}\right)^2 + \frac{q^k-q^t}{q-1} + 1 \]
codewords, it has to be a sunflower, as noted in [3]. In the case $t = 1$, we right now have an improvement of the bound to
\[ \left(\frac{q^k-q^t}{q-1}\right)^2 + \frac{q^k-q^t}{q-1} + 1 - q^{k-2}. \]

We have also characterized the structure of large enough codes at the other extreme of the spectrum. In the case $t = k - 2$, either the code is “primitive” – a case characterized for large enough codes in [1] and [2] – or, if a code contains at least two “non-primitive”, i.e. “essentially lower-dimensional” codewords, then either 1) the code has size at most $q^2 + 2q + 2$ and is of a very particular structure, or, 2) all codewords are “essentially lower-dimensional” and the code is “essentially” a ball, i.e. a collection of $(k-1)$-spaces contained in a common $k$-space. In the remaining case there could potentially be one exceptional codeword and the rest of the code is “primitive”, which further restricts what the “primitive” part of the code can look like.

The cases with $t$ yet more towards the ends of the interval $[0..k]$ have been solved or are well-known in other contexts. More challenges lie with $t$ towards the middle of the interval.

References


Cameron–Liebler type sets and completely regular codes in Grassmann graphs

Morgan Rodgers
University of Padova, Italy
Stradella S. Nicola 3, 36100 Vicenza VI

Joint work with Leo Storme and Andries Vansweevelt.

A Cameron–Liebler line class in PG(3, q) can be defined as a set $\mathcal{L}$ of lines whose characteristic vector lies in row($A$), where $A$ is the point-line incidence matrix of PG(3, q). These objects are connected to collineation groups of PG($n$, q) having the same number of orbits on points and lines, as well as to symmetric tactical decompositions of the point-line design PG($n$, q). These objects also provide examples of completely regular codes in the Grassmann graph $G_q(4, 2)$; these are sets of vertices that induce an equitable partition in the graph, and provide generalizations of the classical concept of perfect codes.

We generalize the concept of a Cameron–Liebler line class to sets of $k$-spaces in PG($2k+1$, q). After looking at various characterizations of these sets and explaining some of the difficulties that arise in contrast to the known results for line classes, we will give some connections to completely regular codes in $G_q(2k+2, k+1)$, and prove some preliminary results concerning the existence of these objects.

Generalized metrics for network coding

Stefan E. Schmidt
Dresden University of Technology, Germany

We investigate functorial maps and their associated generalized metrics on posets and lattices with respect to their relevance for network coding. In particular, we point out the role of supermodular and submodular functions on lattices, which occur in many different settings such as formal concept analysis, subspace lattices of modules, and matroids.
Binary locally repairable codes with high availability via anticodes

Natalia Silberstein
Technion - Israel Institute of Technology, Israel
Haifa 32000 Israel

Joint work with Alexander Zeh.

Locally repairable codes (LRCs) are a family of erasure codes which allow local correction of erasures, where any code symbol can be recovered by using a small (fixed) number of other code symbols. The concept of LRCs was motivated by application to distributed storage systems (DSSs). DSSs store data across a network of nodes in a redundant form to ensure resilience against node failures. The usage of LRCs in DSSs enables to repair a failed node locally, i.e., by accessing a small number of other nodes in the system. If in addition every symbol of an LRC can be recovered by \( t \) disjoint sets of other code symbols, we say that the code has availability \( t \). High availability is an important property for storage of so called hot data.

LRCs and LRCs with availability were introduced in [2] and [4], respectively. Generalizations of the Singleton bound for such codes and constructions of optimal codes that attain these bounds can be found, e.g., in [2,4]. However, known optimal codes are defined over large finite fields. Codes over small (especially binary) alphabets are of a particular interest due to their implementation ease. Recently, a new bound for LRCs which takes the size of the alphabet into account was established in [1]. Moreover, it was shown in [1] that the family of binary simplex codes attains this bound.

In this paper we propose constructions of new binary LRCs which attain the bound in [1]. All our LRCs have a small locality and a high availability, moreover, most of our codes attain the Griesmer bound. Our constructions use a method of Farrell [3] based on anticodes. In particular, we modify a binary simplex code by deleting certain columns from its generator matrix. These deleted columns form an anticode. We investigate the properties of anticodes which allow constructions of LRCs with small locality and high availability.

References


Contributed talks

46

LDPC codes based on $\mu$-geodetic graphs

Marina Šimac
University of Rijeka, Croatia
Radmile Matejčić 2, 51000 Rijeka, Croatia
Joint work with Dean Crnković and Sanja Rukavina.

The main subject of this talk are low-density parity-check (LDPC) codes spanned by the rows of the adjacency matrix of $\mu$-geodetic graphs obtained from block designs. We will discuss some of the properties of obtained codes.

New bound for batch codes with restricted query size\(^1\)

Vitaly Skachek
University of Tartu, Estonia
J. Liivi 2, Tartu 50409, Estonia
Joint work with Hui Zhang, Technion, Israel.

Batch codes were originally proposed in [2] for load balancing in the distributed server systems. They have a lot of similarities with so-called locally-repairable codes, which are of potential use in the distributed storage systems [1,3,4].

**Definition** A $(k,n,r,t)$ batch code $C$ with restricted query size over an alphabet $\Sigma$ encodes a string $x \in \Sigma^k$ into a string $y = C(x) \in \Sigma^n$, such that for all multisets of indices $\{i_1,i_2,\ldots,i_t\}$, where all $i_j \in [k]$, each of the entries $x_{i_1}, x_{i_2}, \ldots, x_{i_t}$ can be retrieved independently of each other by reading at most $r$ symbols of $y$.

Let $d$ be the minimum Hamming distance of $C$. If the code alphabet $\Sigma$ is a finite field $F$, and for all $x \in F^k$, $C(x)$ is a linear transformation, then the corresponding batch code is linear. Denote:

$$A = A(k,r,d,\beta,\epsilon) \triangleq (\beta - 1) \left( \left\lceil \frac{k + \epsilon}{r\beta - \beta + 1} \right\rceil - 1 \right) + k + d - 1,$$

$$B = B(k,r,d,\beta,\lambda) \triangleq (\beta - 1) \left( \left\lceil \frac{k + \lambda}{r\beta - \beta + 1} \right\rceil - 1 \right) + k + d - 1,$$

$$C = C(k,r,\beta,\lambda,\epsilon) \triangleq (r\beta - \lambda + 1)k - \binom{k}{2}(\epsilon - 1).$$

**Theorem** Let $C$ be a linear $(k,n,r,t)$ batch code as above. Then,

$$n \geq \max_{\beta \in \mathbb{N}^\lceil 1, \min\{t, \left\lfloor \frac{k-3}{r-1} \right\rfloor \rceil \rceil} \left\{ \max_{\epsilon, \lambda \in \mathbb{N}^{[1,r\beta-\beta]}} \{ \min \{ A, B, C \} \} \right\}.$$

\(^1\)This work is supported in part by the grants PUT405 and IUT2-1.
Random access via sign-compute-resolve on graphs

čedomir Stefanović
Aalborg University, Denmark
Fredrik Bajers Vej 7, 9220 Aalborg, Denmark
Joint work with Dejan Vukobratović, University of Novi Sad.

We consider a scenario in which a large number of users are associated to a common access point (AP), but only a random subset of them is activated in a batch, such that neither the identities nor the number of active users are known. For the resolution of the active users, we propose a random access solution that combines the principles of interference cancellation enabled slotted ALOHA [1] and sign-compute-resolve frameworks [2]. Specifically, we assume that the resolution takes place during a contention period, consisting of equal-length slots, whose start and termination are signalled by the AP. Each user is assigned with (i) a unique signature, derived using a $K$-out-of-$N$ signature code, and (ii) a predefined transmission schedule that defines slots of the contention period in which the user may contend. Only the active users actually contend by transmitting physical-layer network-coded (PLNC) representation of their respective signatures. If up to $K$ user packets collide in a slot, their PLNC-decoded sum is directly resolvable into constituent signatures. When there are more than $K$ packets colliding in a slot, the PLNC-decoded sum can not be resolved and is stored for later use. A resolution of a signature in any of the slots, enables its cancellation from all other slots in which it appears and which contain more than $K$ packets. In this way, previously unresolved sums may be resolved, propelling new iterations of signature resolutions and cancellations. The contention period is terminated when the AP decides that the target performance is reached, which may be when the predefined fraction of users has been resolved.
and/or throughput is maximised. As the number of active users is unknown, the AP has also to obtain its estimate in order to decide whether the target performance has been reached. In this talk we analyse the proposed random access method and evaluate it both in the asymptotic and non-asymptotic settings, for a simple instance of the scheme in which the transmission schedules of the users are defined such that each slot has the same number of potentially active users. We also develop an estimator for the proposed framework, allowing for the termination that adapts to the actual number of active users.

References


---

**Primitive $t$-intersection constant dimension codes**

**Leo Storme**

Ghent University, Belgium

Department of Mathematics, Krijgslaan 281, 9000 Ghent

Joint work with R. Barrolleta, M. De Boeck, E. Suárez-Canedo, and P. Vandendriessche.

A $(k, m)$-SCID $C$ is a set of $k$-dimensional vector subspaces of a vector space $V = V(n, q)$ of dimension $n$ over the finite field of order $q$ such that any two distinct elements of $C$ pairwise intersect in an $m$-dimensional space (SCID: Subspaces with Constant Intersection Dimension).

The classical example of a $(k, m)$-SCID $S$ is a *sunflower*, i.e., a set of $k$-dimensional vector subspaces through a common $m$-dimensional subspace.

In [3], J. Eisfeld defined *primitive* $(k, m)$-SCIDs. These are $(k, m)$-SCIDs satisfying the following properties:

1. $\langle S \rangle = V$;
2. no nonzero vector is contained in all the elements of $S$;
3. each element $\pi$ of $S$ is spanned by $\{ \pi \cap \sigma : \sigma \in S \setminus \{ \pi \} \}$;
4. $\dim(V) \geq 2k$. 
In [2, 3], J. Eisfeld et al discussed primitive (3, 1)-SCIDs and primitive \((k, k - 2)\)-SCIDs.

In this talk, we present a general construction method for primitive \((k, m)\)-SCIDs [1].

References


The Cameron-Liebler problem for sets

**Andrea Švob**

University of Rijeka, Croatia

Radmile Matejčić 2, Rijeka, Croatia

Joint work with Maarten De Boeck and Leo Storme.

In this talk we will introduce the problem on Cameron-Liebler classes of sets and show how we solved this problem completely, by making links to the classical Erdős-Ko-Rado result on sets. We will also present a characterisation theorem for the Cameron-Liebler classes of sets. The talk is based on the work presented in [1].

References

Contributed talks

Normalized difference sets tiling in $\mathbb{Z}_p$

Kristijan Tabak
Rochester Institute of Technology, Zagreb campus, Croatia

D.T. Gavrana 15, 10000 Zagreb, Croatia

We use normalized difference set tiling with parameters $(31, 6, 1)$ in $\mathbb{Z}_{31}$ as a motivation to develop applicable description of possible tiling in bigger groups $\mathbb{Z}_p$. Using multipliers we describe general shape of putative normalized tiling and difference sets as presented in Theorem below.

**Theorem** Let $G = \langle a \rangle \cong \mathbb{Z}_{31}$ and $D \in G(31, 6, 1)_{DS}$. Let $\psi \in \text{Aut}(G)$ be of order 3. There is $\beta \in \mathbb{Z}_{31}$ such that $D^\psi = a^\beta D$ where $a^\beta \neq 1$ and $D = \sum_{j=1}^{6} a^{d_j}$ for which $a^\beta a^{d_1} (a^\beta)^{h^2} = (a^{d_1})^\psi$ and $(a^{d_1})^\psi \in D \cap D^\psi$. Then for any $j_1 \in \{3, 4, 5\}$ following holds:

$$D = a^{d_1} + (a^{d_1})^\psi + (a^{-2d_1})^{h^2} + a^{d_{j_1}} + a^{2d_1} (a^{d_{j_1}})^\psi + (a^{2d_1})^\psi a^{d_1} (a^{d_{j_1}})^{h^2}.$$ 

---

On MDS convolutional codes over $\mathbb{Z}_{p^r}$

Marisa Toste
Polytechnic Institute of Coimbra, Portugal

Joint work with Raquel Pinto and Diego Napp.

Maximum Distance Separable (MDS) convolutional codes are characterized through the property that the free distance meets the generalized Singleton bound. The existence of free MDS convolutional codes over $\mathbb{Z}_{p^r}$ was recently discovered in [1] via the Hensel lift of a cyclic code. In this paper we further investigate this important class of convolutional codes over $\mathbb{Z}_{p^r}$ from a new perspective. We introduce the notions of p-standard form and r-optimal parameters to derive a novel upper bound of Singleton type on the free distance. Moreover, we present a constructive method for building general (non necessarily free) MDS convolutional codes over $\mathbb{Z}_{p^r}$ for any given set of parameters.
References


Applications of algebraic combinatorics to codes and distributed storage systems

Thomas Westerbäck  
Aalto University, Finland

Joint work with Ragnar Freij-Hollanti and Camilla Hollanti.

Matroid theory, a branch of algebraic combinatorics, can be used to analyze many interesting properties of linear codes over fields. Recent research on distributed storage has proven matroid theory to be a valuable tool for analyzing and constructing linear locally repairable codes. In this talk we will present how tools from algebraic combinatorics can be used in connection with codes that not necessarily are linear codes over fields. Especially polymatroids, a generalization of matroids, can be associated with any code $C \subseteq A^n$, where $A$ is an arbitrary finite set. Results on (not necessarily linear) locally repairable codes, using algebraic combinatorics, will also be presented.

On linear codes with complementary duals

Wolfgang Willems  
University of Magdeburg, Germany

A linear subspace $C$ of $K^n$ is called a code with complementary dual or to be brief an LCD code if $C \cap C^\perp = 0$, which is obviously equivalent to the direct decomposition $K^n = C \oplus C^\perp$. Such codes are of particular interest since they are asymptotically good, achieve the Gilbert-Varshamov bound and have applications in cryptoanalysis. In the talk we investigate properties of optimal LCD codes in classical and network coding as well. Using methods from representation theory we characterize LCD group codes which generalizes earlier results of Yang and Massey.
Designs in affine geometry

Jens Zumbrägel
EPFL, Switzerland
Station 14, 1015 Lausanne

Classical designs and their (projective) $q$-analogs can both be viewed as designs in matroids [1], using the matroid of all subsets of a set and the matroid of linearly independent subsets of a vector space, respectively. Another natural matroid is given by the point sets in general position of an affine space, leading to the following concept.

For a prime power $q$ and a positive integer $n$, let $\text{AG}(n, q)$ be the affine geometry given as the incidence geometry $(P, L)$ with set of points $P := \mathbb{F}_q^n$ and set of lines $L := \{AB = \{A + t(B - A) \mid t \in \mathbb{F}_q\} \mid A, B \in P, A \neq B\}$.

An affine $t$-$(v, k, \lambda)$ design is a collection $B$ of $(k - 1)$-dimensional spaces in $A = \text{AG}(v - 1, q)$ such that each $(t - 1)$-dimensional space in $A$ is contained in exactly $\lambda$ spaces of $B$. In the case $\lambda = 1$ one also refers to an affine Steiner system $S(t, k, v)$. In particular, an affine Steiner triple system $S(2, 3, v)$ is a collection of planes in $\text{AG}(v - 1, q)$ such that each line is contained in exactly one of these planes.

In this work we examine the relationship between the affine and the projective $q$-analogs of designs. We show the existence of affine Steiner systems with various parameters, including the “affine $q$-analog” $S(2, 3, 7)$ of the Fano plane. The approach also offers a new viewpoint on some of the results in [2].

References


List of participants

Paulo Almeida, Universidade de Aveiro, Portugal.
Montserrat Alsina, Universitat Politècnica de Catalunya, Spain.
Angela Barbero, Universidad de Valladolid, Spain.
Amaro Barreal, Aalto University, Finland.
Daniele Bartoli, University of Perugia, Italy.
Simon Blackburn, Royal Holloway University of London, United Kingdom.
Michael Braun, University of Applied Sciences Darmstadt, Germany.
Marco Buratti, University of Perugia, Italy.
Eimear Byrne, University College Dublin, Ireland.
Marco Calderini, University of Trento, Italy.
Jessica Claridge, Royal Holloway University of London, United Kingdom.
Gerard Cohen, Telecom ParisTech, France.
Jan De Beule, Vrije Universiteit Brussel, Belgium.
Doris Dumičić Danilović, University of Rijeka, Croatia.
Tuvi Etzion, Technion, Israel.
Peter Farkaš, Slovak University of Technology, Slovakia.
Tobias Gaebel-Hoekenschnieder, Dresden University of Technology, Germany.
Oliver Gnilke, Aalto University, Finland.
Selahattin Gökceli, Istanbul Technical University, Turkey.
Marcus Greferath, Aalto University, Finland.
Harald Gropp, Germany.
Daniel Heinlein, University of Bayreuth, Germany.
Tor Helleseth, University of Bergen, Norway.
Camilla Hollanti, Aalto University, Finland.
Thomas Honold, Zhejiang University, China.
Anna-Lena Horlemann, EPF Lausanne, Switzerland.
Jonathan Jedwab, Simon Fraser University, Canada.
Regina Judák, University of Szeged, Hungary.
Relinde Jurrius, University of Neuchâtel, Switzerland.
David Karpuk, Aalto University, Finland.
Michael Kiermaier, University of Bayreuth, Germany.
Mladen Kovačević, National University of Singapore, Singapore.
Vedran Krčadinac, University of Zagreb, Croatia.
Gunes Kurt, Istanbul Technical University, Turkey.
Sascha Kurz, University of Bayreuth, Germany.
Reinhard Laue, University of Bayreuth, Germany.
Daniel Enrique Lucani Rötter, Aalborg University, Denmark.
Cristina Martínez Ramírez, Maynooth University, Ireland.
Umberto Martínez-Peñas, Aalborg University, Denmark.
Dávid Mezőfi, University of Szeged, Hungary.
Vedrana Mikulić Crnković, University of Rijeka, Croatia.
Francisco Monteiro, University Institute of Lisbon, Portugal.
Philippe Moustrou, Université de Bordeaux, France.
Gabor Nagy, University of Szeged, Hungary.
Anamari Nakić, University of Zagreb, Croatia.
Diego Napp, University of Aveiro, Portugal.
Alessandro Neri, Universität Zürich, Switzerland.
Kamil Otal, Middle East Technical University (Ankara), Turkey.
Ferruh Özbudak, Middle East Technical University (Ankara), Turkey.
Joonas Pääkkönen, Aalto University, Finland.
Mario Osvin Pavčević, University of Zagreb, Croatia.
Francesco Pavese, Ghent University, Belgium.
Raquel Pinto, University of Aveiro, Portugal.
Alberto Ravagnani, University of Neuchâtel, Switzerland.
Netanel Raviv, Technion, Israel.
Ago-Erik Riet, University of Tartu, Estonia.
Morgan Rodgers, University of Padova, Italy.
Cornelia Roessing, University College Dublin, Ireland.
Joachim Rosenthal, University of Zurich, Switzerland.
Vanessa Santana, Aveiro University, Portugal.
Stefan Schmidt, Dresden University of Technology, Germany.
Natalia Silberstein, Technion, Israel.
Vitaly Skachek, University of Tartu, Estonia.
Emina Soljanin, Rutgers, USA.
Čedomir Stefanović, Aalborg Universitet, Denmark.
Miloš Stojaković, University of Novi Sad, Serbia.
Leo Storme, Ghent University, Belgium.
Marina Šimac, University of Rijeka, Croatia.
Andrea Švob, University of Rijeka, Croatia.
Kristijan Tabak, RIT, Croatia.
Marisa Toste, University of Aveiro, Portugal.
Angeles Vazquez-Castro, Autonomous University of Barcelona, Spain.
Hugues Verdure, University of Tromsø, Norway.
Paolo Vettori, University of Aveiro, Portugal.
Renata Vlahović, University of Zagreb, Croatia.
Dejan Vukobratović, University of Novi Sad, Serbia.
Alfred Wassermann, University of Bayreuth, Germany.
Thomas Westerbäck, Aalto University, Finland.
Wolfgang Willems, Otto-von-Guericke University, Germany.
Øyvind Ytrehus, University of Bergen, Norway.
Jens Zumbrägel, EPF Lausanne, Switzerland.