Design and Application of Random Network Codes (DARNEC'15)

November 4-6, 2015
Istanbul, Turkey

Conference Abstract Book

Istanbul Technical University
&
Middle East Technical University

Welcome Message

On behalf of the DARNEC'15 organizing committee, we are honored and delighted to welcome you to the "Design and Application of Random Network Codes" conference held at Istanbul Technical University, Istanbul, Turkey.
DARNEC'15 is a meeting of COST Action IC1104. Our technical program is rich and varied with keynote speeches, technical papers and a tutorial, split between mathematics and engineering backgrounds. We expect to numerous opportunities for informal networking during the conference. We also thank our supporters, COST, Istanbul Technical University and Middle East Technical University.

Güneş Karabulut Kurt & Ferruh Özbudak,

Istanbul, November 2015.

Supporters

- European Cooperation in Science and Technology (COST),
- Istanbul Technical University (ITU),
- ITU Faculty of Electrical and Electronics Engineering,
- Middle East Technical University (METU),
- METU Institute of Applied Mathematics (METU IAM).

Website

http://www.thal.itu.edu.tr/darnec/

Committees

Advisory Committee

- Marcus Greferath (Aalto University),
- Mario Osvin Pavčević (University of Zagreb).

Orginizing Team

- Güneş Karabulut Kurt (Istanbul Technical University),
- Ferruh Özbudak (Middle East Technical University),
- İbrahim Altunbaş (Istanbul Technical University),
- Murat Uysal (Özyeğin University),
- Ali Emre Pusane (Bosphorus University),
- Suat Aksu (Istanbul Technical University),
- Eda Tekin (Middle East Technical University),
- Semiha Tedik Başaran (Istanbul Technical University),
- Kamil Otal (Middle East Technical University),
- Selahattin Gökçeli (Istanbul Technical University).

LIST OF PARTICIPANTS

Name	**Surname**	**Afilliation**
Suat	Aksu	Istanbul Technical University
İbrahim	Altunbaş	Istanbul Technical University
Amaro	Barreal	Aalto University
Daniele	Bartoli	Gent University
Eimear	Byrne	University College Dublin
Ioannis	Chatzigeorgiou	Lancaster University
Tuvi	Etzion	Technion - Israel Institute of Technology
Peter	Farkaš	Paneuropean University & Slovak University of Technology
Frank	Fitzek	Dresden University of Technology
Ragnar	Freij	Aalto University
Olav	Geil	Aalborg University
Oliver	Gnilke	Aalto University
Selahattin	Gökceli	Istanbul Technical University
Cem	Güneri	Sabancı University
Daniel	Heinlein	University of Bayreuth
Camilla	Hollanti	Aalto University
Dushantha Nalin	Jayakody Arachchilage	University of Tartu
Relinde	Jurrius	University of Neuchâtel
David	Karpuk	Aalto University
Güneş	Karabulut Kurt	Istanbul Technical University
Vedrana	Mikulić Crnković	University of Rijeka
Francisco A.	Monteiro	University Institute of Lisbon
Kamil	Otal	Middle East Technical University
Ferruh	Özbudak	Middle East Technical University
Mario Osvin	Pavcevic	University of Zagreb
Francesco	Pavese	University of Basilicata
Alberto	Ravagnani	University of Neuchâtel
Cornelia	Roessing	University College Dublin
Joachim	Rosenthal	University of Zurich
Diego	Ruano	Aalborg University
Stefan	Schmidt	Dresden University of Technology
Natalia	Silberstein	Technion - Israel Institute of Technology
Milos	Stojakovic	University of Novi Sad
Leo	Storme	Ghent University
Andrea	Svob	University of Rijeka
Semiha	Tedik Başaran	Istanbul Technical University
Eda	Tekin	Middle East Technical University
Laurence	Um	Universitat Politecnica de Catalunya
Angeles	Vasquez-Castro	Autonomous University of Barcelona
Dejan	Vukobratovic	University of Novi Sad
Alfred	Wassermann	University of Bayreuth
Thomas	Westerbäck	Aalto University
Wolfgang	Willems	University of Magdeburg
Jens	Zumbrägel	École Polytechnique Fédérale de Lausanne

CONFERENCE PROGRAM

Wednesday, November 4

08.45 Registration

09.20 Opening

09.30 Invited Keynote: Tuvi Etzion, ”On the structure of q-Steiner systems”

10.30 Coffee break

11.00 Invited Tutorial: Ioannis Chatzigeorgiou, ”Resource allocation strategies for network-coded service delivery over LTE/LTE-A systems”

12.15 Lunch break

13.30 Invited Keynote: Francisco A. Monteiro, ”Signal processing in the upcoming wireless networks: Untangling signals in space, in spectrum, and network coded”

SESSION I

14.30 Leo Storme, ”A geometrical bound for the sunflower property”

14.55 Daniele Bartoli, ”Algebraic curves and random network codes”

15.20 Francesco Pavese, ”Veronese subspace codes”

15.45 Coffee break

16.15 Daniel Heinlein, ”Tables for sizes of largest known codes in network coding”

16.40 Kamil Otal and Ferruh Özbudak, ”Cyclic subspace codes via subspace polynomials”

Thursday, November 5

09.00 Invited Keynote: Joachim Rosenthal, ”Cryptanalyis of McEliece type public key systems based on Gabidulin codes”

10.00 Coffee break

SESSION II

10.30 Wolfgang Willems, ”On self-dual MDS codes”

10.55 Eimear Byrne, ”On the covering radius of rank metric codes”

11.20 Alberto Ravagnani, ”Generalized rank weights”
codes”

11.45 Selahattin Gökceli, ”Network coded cooperation testbed: Implementation and performance results”

12.15 Lunch break

Thursday, November 5

12.15 Lunch break

13.30 Invited Keynote: Natalia Silberstein, "Access-optimal MSR codes with optimal sub-packetization over small fields"

SESSION III

14.55 Vedrana Mikulić Crnković, "On self-orthogonal binary codes invariant under the action of the Held group"

15.20 Ragnar Freij, "Weight enumeration of cooperative locally repairable codes"

15.45 Coffee break

16.15 Nalin D. K Jayakody and Vitaly Skachek, "Network-coded soft forwarding-based distributed LDPC coding scheme"

16.40 David Karpuk, "Strong secrecy in wireless network coding systems from structured interference"

SOCIAL PROGRAM

19.00 Gala dinner

Friday, November 6

09.00 Invited Keynote: Frank Fitzek, "Network coding for the real World!

10.00 Coffee break

SESSION IV

10.30 Alfred Wassermann, "Construction of new large sets of designs over the binary field"

10.55 Andrea Švob, "Designs on which the unitary group U(3;3) acts transitively"

11.20 Oliver Wilhelm Gnilke, "Mosaics and their q-analogues"

11.45 Leo Storme, "Improvement of the sunflower bound for 1-intersecting constant dimension subspace codes"

12.10 Closing remarks and lunch break

13.45 MC Meeting (EHM Department Meeting Room - 2309)

Contents

INVITED TALKS 9

INVITED TUTORIAL 17

CONTRIBUTED TALKS 23

INVITED TALKS

On the structure of q-Steiner systems

Tuvi Etzion

Technion - Israel Institute Of Technology

Abstract

The interest in q-analogs of codes and designs has been increased in the last few years as a consequence of their new application in error-correction for random network coding. One of the most intriguing problems is the existence question of an infinite family of q-analog of Steiner systems in general, and the existence question for q-analog for the Fano plane in particular. We start with a short survey on the motivation and the known results in this area. We exhibit a new method to attack this problem. In the process we define a new family of designs whose existence is implied from the existence of q-analog of Steiner systems, but their existence can be also independent. We present necessary conditions for the existence for such designs, trivial constructions for such designs, and a nontrivial recursive construction. We consider the structure of the q-Fano plane for any given q and conclude that most of its structure is known. Even so, we are unable to determine whether it exists or not. A special attention is given for the case $q = 2$ which was considered by most researchers before.

Network coding for the real world!

Frank Fitzek
Technische Universität Dresden

Abstract

Network coding breaking with old fashioned end to end codes and provides new possibilities for communication systems. Especially for upcoming 5G communication networks, network coding has been identified as key technology as it provides higher throughput, lowedelays, and is able to operate in dynamic settings. This talk will highlight several implementation of network coding targeting transportation and storage use cases based on the world's fastest software library for network coding named KODO. The talk will also show where network coding is becoming part of standardisation activities.

Signal processing in the upcoming wireless networks: Untangling signals in space, in spectrum, and network coded

Francisco A. Monteiro
University Institute Of Lisbon And Institute Of Telecommunications

Abstract

For decades interference was widely considered to be a nuisance to communications links. Nowadays, the existence of signal interference underpins most of the growth of maximum data rates and the overall capacity increase of the future 5th generation of wireless systems. The existence of multipath fading in wireless communications was deemed to make the wireless channels even more challenging. In the past decade or so the advent of multiple-input multiple-output (MIMO) communications turned multipath fading from foe to ally, as multiple virtual independent links could be created in the spatial domain between multi-antenna terminals. Given the orthogonality properties of massive MIMO, the number of antennas at a base station can soon rise to hundreds delivering unprecedented spectral efficiency. Today, most radio engineering textbooks still state that bidirectional links always imply splitting the available bandwidth or slotting the time between the two directions. Signal processing techniques are now contributing to the emergence of in-band full-duplex terminals and relays for wireless networks. Both massive MIMO and in-band full-duplex can therefore be seen along with physical layer network coding as three ways of taking advantage of signals interference. This talk will show that they can all be put together to dramatically increase the re-use of the channel resources in some fundamental networking configurations.

Cryptanalyis of McEliece type public key systems based on Gabidulin codes

Joachim Rosenthal
University Of Zurich

Abstract

Assymmetric 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 talk we will study public key ciphers where the public key represents a disguised Gabidulin code. Using geometric ideas we will introduce a new attack which is capable of breaking several variants proposed in the literature.

Access-optimal MSR codes with optimal sub-packetization over small fields

Natalia Silberstein

Technion - Israel Institute Of Technology

Abstract

This work presents a new construction of access-optimal minimum storage regenerating codes which attain the sub-packetization bound. These distributed storage codes provide the minimum storage in a node, and in addition have the following two important properties: first, a helper node accesses the minimum number of its symbols for repair of a failed node; second, given storage l in each node, the entire stored data can be recovered from any $2\log l$ (any $3\log l$) for 2 parity nodes (for 3 parity nodes, respectively). The goal of this work is to provide a construction of such optimal codes over the smallest possible finite fields. Our construction is based on perfect matchings of complete graphs and hypergraphs, and on a rational canonical form of matrices which constitute a generator matrix of the constructed codes. The field size required for our construction is significantly smaller when compared to previously known codes.

INVITED TUTORIAL

Resource allocation strategies for network-coded service delivery over LTE/LTE-A systems

Ioannis Chatzigeorgiou
Lancaster University, United Kingdom

Abstract

Network coding has the potential to significantly improve network reliability by mixing packets at a source node or at intermediate network nodes prior to transmission. In the first part of this talk, the concept of network coding will be quickly reviewed and extended to various cases including systematic, layered and sparse network coding. Performance expressions that describe the decoding probability of each case will be presented and discussed. The second part of the tutorial will use the derived performance expressions in resource allocation models, which can be easily adapted to the Long Term Evolution-Advanced (LTE-A) standard and its 5G features. More specifically, the idea of unequal error protection will form part of a resource allocation framework, whose objective can be either provider-centric or user-centric. In the former case, the provider can optimise the number of transmitted coded packets and the adopted modulation and coding scheme in order to offer a service to a minimum fraction of users without violating an existing service lever agreement. In the latter case, the aim is to maximise the ratio between the number of recoverable layers by the users (user's profit) and the total number of coded packet transmissions (provider's cost). The impact of the adopted network coding method on performance and the effect of sparse network coding on packet transmissions and decoding complexity will also be discussed.

Objectives

The tutorial consists of two parts. The first part will create links between communication theory and random matrix theory over finite fields and present a step-by-step methodology for obtaining theoretical expressions, which describe the performance of various network-coded systems. The objective of the second part is to build on the derived theoretical expressions, develop realistic resource allocation frameworks and consider LTE-A networks as a case of study in order to demonstrate the practical implication of network coding in real-world systems. The tutorial is suitable for graduate students and researchers from both academic and industrial sectors in the area of information theory, communication theory and networking.

Outline

1 Description and Performance Evaluation of Network-Coded Systems

- **Fundamentals of Random Network Coding (RNC):** The concept and terminology of random network coding will be introduced and its two main types, namely inter-session and intra-session network coding, will be presented. Techniques for RNC decoding will be discussed and fundamental performance expressions that characterise the probability of successfully recovering a source message will be analysed.

- **Systematic vs. non-systematic RNC:** This subpart discusses the benefits of transmitting source packets that are not network-coded along with linear combinations of source packets. We derive analytical expressions for the success probability and prove that systematic RNC can both reduce decoding processing and achieve a success probability that is better or at least similar to that of non-systematic RNC, depending on the number of source packets in the original message.

- **RNC for layered services:** If a source message comprises packets of different priority layers or importance levels, the concept of windowing can be used to offer unequal error protection. We will focus on RNC using either non-overlapping windows or expanding windows, discuss their advantages and disadvantages and obtain expressions that accurately describe the decoding probability of each layer as well as the whole source message.

- **Special structures of random linear matrices suitable for network-coded systems:** The structure of random matrices over finite fields of size q plays a pivotal role in the design and performance of network codes. Specific constrained designs will be considered, e.g. block angular matrices as well as matrices having a step structure, the probability of them being full rank will be examined and their application in window-based decoding and relay-aided networks will be presented.

- **Sparse RNC:** The literature usually assumes that network coding selects coefficients from a finite field of size q in a uniformly random fashion when source packets are combined. In this subpart, we consider the case of zero coefficients being selected with a higher probability than the remaining (q-1) coefficients and we present accurate bounds on the decoding probability of sparse RNC. Furthermore, we hint at the possibility of adjusting the sparsity of RNC as a means to trade transmit power for decoding speed. This claim is substantiated in Part II of this tutorial.

2 Resource Allocation Modelling for Network-Coded Systems

- **3GPPs Long Term Evolution-Advanced (LTE-A):** In the short-term, LTE-A is likely to play a leading role not only in 4G networks but also in the 5G ecosystem. In particular, the ability that LTE-A has of managing broadcast and multicast communications via the eMBMS frameworks are likely to be adopted into next-generation systems. In spite of its natural complexity, we will explain how the resources of the MAC and PHY layers can be mapped onto simple topologies in a bin-packing context and how the systems Service Level Agreements (SLAs) can be mapped onto a constraint set.

- **Optimising with respect to the Internet Service Provider (ISP) or with respect to the users:** ISP-centric optimisation and user-centric optimisation represent two extremes in the Operational Research applied to wireless networks. In this subpart, by referring to a fundamental economic principle, we will clarify how network coding could be integrated into the LTE-A stack and explain how hybrid strategies, which meet the desired SLAs constraints and are fair with respect to the ISP and the users, can be defined.

- **Computationally efficient Sparse RLNC (S-RNC) strategies for ultra-reliable multicast services:** In a network composed by low-end communication devices (e.g. wireless sensors), the optimisation of radio resources should not be our only concern. The computational requirements for the processing of the received information in order to recover the transmitted messages should also play a key role. In this subpart, we will adopt S-RNC and show how to model and optimise both the transmission parameters and the sparsity of the network code in order to minimise the processing footprint in the case of ultra-reliable services.

CONTRIBUTED TALKS

Algebraic curves and random network codes

Daniele Bartoli
GHENT UNIVERSITY
(Joint work with Matteo Bonini and Massimo Giulietti)

Abstract

In their seminal paper [1], Koetter and Kschischang introduced a metric on the set of vector spaces and showed that if the dimension of the intersections of the vector spaces is large enough then a minimal distance decoder for this metric achieves correct decoding. In particular, given an r-dimensional vector space V over $\mathbb{F}_q$, the set $\mathcal{S}(V)$ of all subspaces of V forms a metric space with respect to the subspace distance defined by

$$d(U, U') = \dim(U + U') - \dim(U \cap U').$$

In this context the main problem asks for the determination of the larger size of codes in the space $(\mathcal{S}(V), d)$ with given minimum distance.

Recently, Hansen [2] presented a construction of random network codes based on Riemann-Roch spaces associated to algebraic curves, describing the parameters of these codes.

We generalize this construction and we obtain new infinite families of random network codes from algebraic curves.

[1] R. Koetter, F.R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory* **54**(8), (2008) 3579–3591.

[2] J.P. Hansen. Riemann-Roch spaces and linear network codes, http://arxiv.org/abs/1503.02386.

Keywords: Equidistant codes, Algebraic curves

On the covering radius of rank metric codes

Eimear Byrne
University College Dublin

Abstract

The covering radius of rank metric codes has recently emerged as a significant parameter in network coding problems. For coded-caching problems in particular, it gives a measure of the performance of codes $\{C^{(i)} < \mathbb{F}_q^n : i \in [m]\}$ chosen by the sender to encode data cached in proximity to m different receivers during the placement phase; the existence of an optimal rank-metric covering code for a given set of parameters guarantees that the sender can satisfy all receivers' demands with a minimal number of transmissions during the delivery phase. Such a code is formed by taking a direct sum $C = C^{(1)} \oplus \cdots \oplus C^{(m)}$ of users' codes and can be expressed as

$$C = \left\{ \left[\begin{array}{c} X_1 \\ \vdots \\ X_m \end{array} \right] : X_i \in C^{(i)} < \mathbb{F}_q^n, i \in [m] \right\} \subset \mathbb{F}_q^{m \times n}. \tag{1}$$

While the covering radius for the Hamming distance has been well studied, relatively little has appeared in the literature on this measure with respect to the rank distance. An exception to this is the work of Gadouleau and Zhiyuan Yan, who gave bounds on the $\mathbb{F}_q$-rank distance covering radius of $\mathbb{F}_{q^n}$-linear codes with a focus on maximum rank distance (MRD) codes. However, such codes form a proper subclass of the set of all matrix codes over $\mathbb{F}_q$ and furthermore do not have the form of the code C that arises in coded-caching.

In this work, we give bounds on the rank distance covering radius of the general class of $m \times n$ matrix codes over $\mathbb{F}_q$ and of the subclass of such codes of the form (1). Some of these results can be achieved by using the machinery of association schemes developed by Delsarte.

Keywords: rank distance, covering radius

Weight enumeration of cooperative locally repairable codes

Ragnar Freij

Aalto University

(Joint work with Camilla Hollanti and Thomas Westerbäck)

Abstract

Cooperative locally repairable codes have recently gathered wide interest, both for their applications in large scale distributed storage systems, and for their purely mathematical properties. In this talk, we will analyze locally repairable codes from the perspective of the strong connection between linear codes and matroids, and more generally between arbitrary codes and polymatroids. Well known techniques to calculate Tutte and rank polynomials of matroids are applied to the weight enumeration polynomials on locally repairable codes, which in terms give results on the possible field sizes over which given localities can be achieved. We also consider a (to our knowledge) new generalization of locally repairable codes, where the repair can be performed on several different scales, further enhancing the robustness of a storage system.

Keywords: Locally repairable codes, Matroids, Weight enumeration, Tutte polynomial

Mosaics and their q-analogues

Oliver Wilhelm Gnilke
Aalto University
(Joint work with Marcus Greferath and Mario Osvin Pavčević)

Abstract

We will motivate the definition of a new combinatorial object called mosaics. A mosaic is a collection of c $t-$designs of equal sizes (points and blocks) together with an ordering of their blocks such that the blocks partition the point set. A small example stemming from the Fano plane can be described by the following incidence matrix.

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 & 2 & 1 & 2 \\ 2 & 2 & 0 & 1 & 1 & 2 & 1 \\ 1 & 2 & 2 & 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 2 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 & 2 & 0 & 1 \\ 1 & 1 & 2 & 1 & 2 & 2 & 0 \end{bmatrix}$$

Each of the 'colors' $0, 1, 2$ represents a $t-$design on 7 points with 7 blocks.

After presenting a handful of examples and constructions we will outline a few general properties and open questions. The appropriate generalization to the q-analogue case will be presented along with an almost trivial example. We conclude with a version of the famous $S_2(2, 3, 13)$ Steiner Systems by Braun et al., and show that it gives rise to a q-mosaic.

Keywords: Combinatorial Designs, Affine Geometry.

Network coded cooperation testbed: Implementation and performance results

Selahattin Gökceli
Istanbul Technical University
(Joint work with Semiha Tedik Başaran and Güneş Karabulut Kurt)

Abstract

Conventional usage of the network coding mostly covers wired network infrastructures, where transmission errors between nodes are negligible. However, when considering wireless networks, the use of network coding in the conventional case does not fully exploit its potential. Beyond the challenges introduced through the wireless channel impairments, we can exploit the spatial diversity gain provided by the broadcast nature of the wireless channels. In this work, we design and implement a network coded cooperation (NCC) system that operates in real-time through the use of software defined radio nodes. We target wireless networks. Our system is based on orthogonal frequency division multiple access (OFDMA), that provides a practical means to enable high transmission rates through the use of narrowband subcarriers. The developed testbed is composed of three source nodes, a relay node and two destination nodes. The transmission of this NCC-OFDMA system is completed in two phases; the broadcast and the relaying phases. Multiplexing of source nodes' signals is achieved by using OFDMA. In the broadcast phase, OFDMA signal is transmitted to relay and destination nodes. In the relaying phase, the relay node first detects the OFDMA signal, generates network coded symbols and then transmits these symbols to destination nodes. At the end of these two phases, the destination nodes determine the source nodes' signals by using combining detectors. We demonstrate with real-time bit error rate and error vector magnitude measurements that the NCC-OFDMA system can significantly improve the communication quality and robustness, while enabling data transmission between multiple users. Due to the provided benefit of improved radio resource usage efficiency, some features of this implemented NCC-OFDMA system have the potential to be included in future networks.

Keywords: Network coded cooperation, Wireless Networks.

Tables for sizes of largest known codes in network coding

Daniel Heinlein

University of Bayreuth

(Joint work with Michael Kiermaier, Sascha Kurz and Alfred Wassermann)

Abstract

Kötter and Kschischang introduced a new approach of network coding by converting data in subspaces of a common vector space $\mathbb{F}_q^n$. It is possible to define a metric (the so-called subspace metric $d(U, V) := \dim(U+V) - \dim(U \cap V)$) on the set of all subspaces of $\mathbb{F}_q^n$. The topic is therefore accessible for ideas of coding theory.

The maximum size of a code is denoted by $A_q(n, d)$.

In the case of constant dimension codes, all such subspaces have the same dimension k and the maximum size of these codes is called $A_q(n, d; k)$.

In my talk, I present a homepage that contains

- lower bounds on $A_q(n, d)$ and $A_q(n, d; k)$ due to constructions or theoretical arguments,
- upper bounds on them due to theoretical arguments,
- downloadable codes in special cases and
- an API that can be accessed to retrieve the informations in a program

for small parameters.

This project is ongoing work and your contributions are welcome: new or missing results can and should be submitted to increase the strength of the bounds.

Keywords: Network coding, tabulated sizes of codes.

Network-coded soft forwarding-based distributed LDPC coding scheme

Nalin D. K Jayakody and Vitaly Skachek
University of Tartu, Tartu, ESTONIA

Abstract

The cooperative communication is an efficient tool to combat channel fading and enhance transmission rate by exploiting spatial degree of freedom. In the wireless relay communication, a relay overhears the source transmissions, performs signal processing on the received signals, and forwards it to the destination.

The main focus of the early literature was on two relaying protocols, namely amplify-and-forward (AF) and decode-and-forward (DF). In the AF, the relay amplifies the signal before forwarding it to the destination. In the DF relaying, the relay makes a decision based on the received signal. AF protocol suffers from noise propagation as the relay forwards noisy signals without processing. In the DF protocol, the relay decodes the sources messages and forwards them to the destination. In the case of erroneous decoding at the relay, these errors will propagate to the destination, causing a loss in diversity gain.

A more advanced relay protocol, based on forwarding of the soft information, is called estimate-and-forward, and it is used to obtain a better error performance. In this relay protocol, the relay estimates and forwards intermediate soft symbols. The term soft symbol generally refers to a continuous-valued estimate of a constellation symbol, usually incorporating probabilistic or reliability information. While the most common mechanism for computing the soft symbol is via the expected value of the constellation symbol based on the (known or estimated) probabilities of the underlying bits.

This paper proposes a novel technique of spatially-coupled low-density parity-check (SC-LDPC) code-based soft forwarding relaying scheme for a multiple access relay system. We introduce an array based optimized SC-LDPC codes in relay channels. We show that the combination of channel coding

and network-coded SIR can be seen as a distributed coding scheme. In order to mitigate the error-propagation due to the erroneous decoding at the relay, we propose a new method for modelling the soft estimated symbols. We also propose a new soft encoding algorithm for this system which overcome the disadvantages of recursive soft encoders proposed in the literature. The calculation of the received Log-Likelihood-Ratios at the destination is derived according to the proposed model. For the SC-LDPC based network coding operation at the relay, we consider two alternative methods, which offer a trade-off between the implementation complexity and the performance, called superposition and soft network coding. Several simulation results show that network-coded SIR-based DCS using the proposed model outperforms those using other well-known relay protocol techniques in terms of the BER performance.

Strong secrecy in wireless network coding systems from structured interference

David Karpuk

Aalto University, Espoo, Finland

(Joint work with Arsenia Chorti)

Abstract

Wireless network coding (WNC) has been proposed for next generation networks. In this contribution, we investigate WNC schemes with embedded strong secrecy by exploiting structured interference in relay networks with two users and a single relay. In a practical scenario where both users employ finite, uniform signal input distributions we compute the corresponding strong secrecy capacity, and make this explicit when PAM modems are used. We then describe a simple triple binning encoder that can provide strong secrecy close to capacity with respect to an untrustworthy relay in the single antenna and single relay setting. An explicit encoder construction is described when M-PAM or M-QAM modulators are employed at the users' transmitters. Lastly we generalize to a MIMO relay channel where the relay has more antennas than the users, and optimal precoding matrices are studied. Our results establish that the design of WNC transmission schemes with enhanced throughput and guaranteed data confidentiality is feasible in next generation systems.

Keywords: Wireless network coding, secrecy capacity, strong secrecy, signal space alinement, triple binning encoder.

On self-orthogonal binary codes invariant under the action of the Held group

Vedrana Mikulić Crnković

University of Rijeka, Croatia

(Joint work with Dean Crnković and Bernardo G. Rodrigues)

Abstract

We construct self-orthogonal 1-designs from the sporadic simple group **He** with large number of points. Furthermore, we define binary codes of the constructed designs and analyse their properties.

Keywords: 1-designs, self-orthogonal codes, Held's group

Cyclic subspace codes via subspace polynomials

Kamil Otal and Ferruh Özbudak
MIDDLE EAST TECHNICAL UNIVERSITY

Abstract

Subspace codes have been intensely studied in the last decade due to their application in random network coding. Cyclic subspace codes are very useful subspace codes with efficient encoding and decoding algorithms. In this study we give some new results and improvements on cyclic subspace codes using subspace polynomials.

In a recent paper (arXiv:1404.7739v3) the authors have studied on subspace codes using their subspace polynomial representations. They give an explicit construction of cyclic codes of size n times the size of a full length orbit where n is a prime dividing the length. In this study we generalize their construction and increase the size up to $q^n - 1$ times the size of a full length orbit, using this generalization we also relax some of their assumptions, for example n does not have to be prime any more. We also use different kind of subspace polynomials, in that way we provide diverse values for the length parameter.

Keywords: Linearized polynomials, subspace polynomials, subspace codes, constant dimension codes, cyclic subspace codes.

Veronese subspace codes

Francesco Pavese
University of Basilicata
(Joint work with A. Cossidente)

Abstract

Let V be an n–dimensional vector space over $\mathrm{GF}(q)$, q any prime power. The set $S(V)$ of all subspaces of V, or subspaces of the projective space $\mathrm{PG}(V)$, 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 subspace codes and constant–dimension codes, respectively, have been proposed for error control in random linear network coding. An $(n, M, d; k)_q$ constant–dimension subspace code (CDC) is a set $\mathcal{C}$ of k–subspaces of V with $|\mathcal{C}| = M$ and minimum subspace distance $d_s(\mathcal{C}) = \min\{d_s(U, U') | U, U' \in \mathcal{C}, U \neq U'\} = d$. The smallest open constant–dimension case occurs when $n = 6$ and $k = 3$. From a projective geometry point of view it translates in the determination of the maximum number of planes in $\mathrm{PG}(5, q)$ mutually intersecting in at most one point.

In this paper I will describe a construction of CDCs obtained by using the correspondence between quadrics of a projective plane $\mathrm{PG}(2, q)$ and points of $\mathrm{PG}(5, q)$. In this setting, a special net of conics (circumscribed bundle) yields a $(6, q^3(q^2-1)(q-1)/3, 4; 3)_q$ CDC admitting the linear group $\mathrm{PGL}(3, q)$ as an automorphism group. Although the size of such a code asymptotically reaches the theoretical upper bound of a $(6, M, 4; 3)_q$ CDC, it turns out that it can be enlarged. This is done by identifying a suitable set of further $(q^2+1)(q^2+q+1)$ planes of $\mathrm{PG}(5, q)$ mutually intersecting in at most one point and extending the previous code. The $(6, q^3(q^2-1)(q-1)/3 + (q^2+1)(q^2+q+1), 4; 3)_q$ CDC so obtained admits the normalizer of a Singer cyclic group of $\mathrm{PGL}(3, q)$ as an automorphism group.

Generalized rank weights

Alberto Ravagnani
University of Neuchâtel

Abstract

Generalized rank weights were introduced by Kurihara, Matsumoto and Uyematsu to evaluate the performance of a Gabidulin code when employed to secure a network communication. Generalized rank weights are defined in terms of the intersection of the Gabidulin code with certain linear spaces, called Frobenius-closed, that satisfy a given algebraic property.

We show that Frobenius-closed spaces coincide with optimal anticodes in the rank metric, giving in particular a convenient test to decide whether a linear space is Frobenius-closed or not. This metric description of Frobenius-closed spaces yields a purely metric characterization of generalized rank weights. In particular, it shows a very close analogy between generalized Hamming weights for classical codes and generalized rank weights for Gabidulin codes. Moreover, it gives a precise link between generalized rank weights and security drops in network communications.

We then propose a definition of generalized rank weights for Delsarte codes, which we call *Delsarte weights*, and establish several properties of the new algebraic invariant. We first prove that Delsarte weights refine generalized rank weights for Gabidulin codes. Then we show that optimal codes and anticodes are characterized by their Delsarte weights, and that the Delsarte weights of a code determine the Delsarte weights of the dual code.

Keywords: generalized rank weights, Gabidulin code, Delsarte code

Equidistant constant dimension subspace codes

Ago-Erik Riet

University of Tartu, Estonia

(Joint work with Daniele Bartoli, Leo Storme and Peter Vandendriessche)

Abstract

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 by Etzion and Raviv [Equidistant Codes in the Grassmannian, 2015]. We are trying to improve this bound for different values of t, this is work in progress. For example in the case $t=1$, we right now have an improvement of the bound to

$$\left(\frac{q^k-q^t}{q-1}\right)^2+\frac{q^k-q^t}{q-1}\ +1-q^{k-2}.$$

Keywords: equidistant code, Grassmannian, sunflower, projective plane.

A geometrical bound for the sunflower property

L. Storme

Ghent University

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

Abstract

Let $\mathcal{S} = \{\pi_1, \ldots, \pi_n\}$ be a collection of k-subspaces in $V(\infty, q)$ for some finite field $\mathbb{F}_q$, and assume that there exists a positive integer t such that $\dim(\pi \cap \pi') = k - t$ for all $\pi, \pi' \in \mathcal{S}$ with $\pi \neq \pi'$, then this set $\mathcal{S}$ is called a *$(k-t)$-intersecting constant dimension code.*

The classical example of a $(k-t)$-intersecting constant dimension code is a *sunflower*. This is a set of k-dimensional subspaces through a common $(k-t)$-dimensional subspace.

It is known that large $(k-t)$-intersecting constant dimension codes are sunflowers.

Theorem 1. *Every $(k-t)$-intersecting constant dimension code $\mathcal{S}$ of k-subspaces of cardinality larger than $\left(\frac{q^k-q^{k-t}}{q-1}\right)^2 + \left(\frac{q^k-q^{k-t}}{q-1}\right) + 1$ is a sunflower.*

We determined a geometrical variant of this theorem. We found a bound stating that if the dimension of the space generated by the codewords of the $(k-t)$-intersecting constant dimension code $\mathcal{S}$ is large enough, then the code is a sunflower.

Theorem 2. *Let $\mathcal{S} = \{\pi_1, \ldots, \pi_n\}$ be a collection of k-subspaces in $V(\infty, q)$ for some finite field $\mathbb{F}_q$, and assume that there exists a positive integer $t \geq 3$ such that $\dim(\pi \cap \pi') = k - t$ for all $\pi, \pi' \in \mathcal{S}$ with $\pi \neq \pi'$.*

If $\dim\langle\mathcal{S}\rangle \geq k + (t-1)(n-1) + 2$, then $\mathcal{S}$ is a sunflower.

A nice property of the preceding bound is that this bound is sharp. If $\dim\langle\mathcal{S}\rangle = k + (t-1)(n-1) + 1$, then $\mathcal{S}$ is not necessarily a sunflower. We managed to prove that next to the sunflower, there are exactly two types of $(k-t)$-intersecting constant dimension codes $\mathcal{S}$ of k-subspaces, for which $\dim\langle\mathcal{S}\rangle = k + (t-1)(n-1) + 1$.

Keywords: Constant dimension codes, Sunflower property

Designs on which the unitary group $U(3,3)$ acts transitively

Andrea Švob

University of Rijeka

(Joint work with Dean Crnković and Vedrana Mikulić Crnković)

Abstract

In this talk we describe a method for constructing transitive 1-designs from finite groups. We apply this method to construct transitive designs from the simple group $U(3,3)$. Some of the constructed 1-designs are also 2-designs. In this talk, we will discuss 2-designs, obtained using the described method, on which the unitary group $U(3,3)$ acts transitively. The constructed structures will be analysed and described.

Keywords: transitive design, unitary group

Construction of new large sets of designs over the binary field

Alfred Wassermann
University of Bayreuth

Abstract

A simple t-$(v, k, \lambda; q)$ *design over a finite field* is a pair $(\mathcal{V}, \mathcal{B})$ consisting of a vector space $\mathcal{V} = \mathrm{GF}(q)^v$ and a set $\mathcal{B}$ of k-dimensional subspaces of $\mathcal{V}$ such that each t-dimensional subspace of $\mathcal{V}$ is contained in exactly λ members of $\mathcal{B}$.

The set of all k-dimensional subspaces of $\mathcal{V}$, also called the Grassmannian $\mathcal{G}_q(v, k)$, is always a design, the so called trivial design, having parameters t-$(v, k, \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q; q)$.

An $LS_q[N](t, k, v)$ *large set* is a set of N disjoint t-$(v, k, \lambda; q)$ designs which partitions the trivial t-$(v, k, \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q; q)$ design. Large sets of designs over finite fields have been studied for the first time by Ray-Chaudhuri and Schram (1994). There, the authors used non-simple designs.

The first large sets consisting of simple t-designs with $t \geq 2$ have been found recently by Braun, Kohnert, Östergård, Wassermann (2014). Braun, Kiermaier, Kohnert, Laue (in preparation) construct infinite series of large sets based on the known large sets.

We present the construction of a new large set over the binary field having parameters $LS_2[3](2, 4, 8)$, consisting of three disjoint, simple 2-$(8, 4, 217; 2)$ designs. These design parameters were not know to exist, yet. The automorphism group of the designs is generated by $\langle \sigma^5, \phi^2 \rangle$, where σ is the Singer cycle and ϕ is the Frobenius automorphism. The order of the group is 204.

Keywords: Design over finite field, large sets of designs, group of automorphisms.

On self-dual MDS codes

Wolfgang Willems
University of Magdeburg
(Joint work with Gabriele Nebe)

Abstract

On the $\mathbb{F}_q$-vector space $V = \mathbb{F}_q^{m \times n}$ there exists a duality which is defined by $\langle A, B \rangle = \mathrm{trace}(AB^t)$ for $A, B \in V$, where B^t denotes the transpose of B. We call $\mathcal{C} \subseteq V$ self-dual if $\mathcal{C} = \mathcal{C}^\perp$ with respect to the above bilinear form. In the class of MRD codes self-dual codes are hard to find. Surprisingly, they do not exist if q is even. In the talk we characterize for $n = m$ self-dual Gabidulin codes with minimum distance n. The characterization depends on arithmetical conditions of q and n.