3 Contributed talks

Towards Fuchsian codes attached to small ramified quaternion algebras

Montserrat Alsina

Universitat Politècnica de Catalunya

(Joint work with Iván Blanco-Chacón, Dionis Remón, Camilla Hollanti)

A new transmission scheme for AWGN, based on Fuchsian groups, was proposed in [2], in such a way that maximal orders in indefinite quaternion algebra are used to generate the constellation.

We deal with embedding theory and quadratic forms to make explicit arithmetic fuchsian groups, specially those attached to small ramified quaternion algebras by using [1], in order to study the performance of derived codes.

References

[1] M. ALSINA AND P. BAYER, *Quaternion orders, quadratic forms, and Shimura curves*, vol. 22 of CRM Monograph Series, American Mathematical Society, Providence, RI, 2004.

[2] I. BLANCO-CHACÓN, C. HOLLANTI, D. REMÓN, M. ALSINA, *Fuchsian codes for AWGN channels* (journal version), (Submitted).

Universitat Politècnica de Catalunya-BarcelonaTech, Dept. Matemàtica Aplicada III, Escola Politècnica Superior d'Enginyeria de Manresa
Av. Bases de Manresa 61-73, 08242 Manresa, CATALONIA
montserrat.alsina@upc.edu

Structure of Linear and Cyclic codes over $\mathbb{F}_q[v]/\langle v^q - v\rangle$

Aysegul Bayram

Yildiz Technical University, Department of Mathematics, Faculty of Arts and Sciences

(Joint work with Irfan Siap)

In [1], we introduced the ring $\mathbb{F}_q[v]/\langle v^q - v\rangle$ where q is a prime power, its algebraic structure, ideals, units, etc. A Gray map which is deduced from the Chinese Remainder Theorem and this map relates the ring R with the ring F_q^q is also introduced. Next linear codes over R are considered. Then by defining an inner product the dual of a linear code is defined and relation to linear code and its dual is also presented. Finally, the algebraic structure of cyclic codes and their duals are presented. In all cases examples that illustrate the theorems and lemmas are provided.

References

[1] T. ABUALRUB AND I. SIAP, *On the construction of cyclic codes over the ring Z_2+uZ_2*, WSEAS Transactions on Mathematics, 5 (2006), pp. 750–755.

[2] A. BAYRAM AND I. SIAP, *Structure of codes over the ring $Z_3[v]/\langle v^3 - v\rangle$*, Appl. Algebra Engrg. Comm. Comput., (accpeted, 2013).

[3] K. BETSUMIYA AND M. HARADA, *Optimal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$ with respect to the hamming weight*, Information Theory, IEEE Transactions on, 50 (2004), pp. 356–358.

[4] A. BONNECAZE AND P. UDAYA, *Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Transactions on Information Theory, 45 (1999), pp. 1250–1255.

[5] S. T. DOUGHERTY, B. YILDIZ, AND S. KARADENIZ, *Codes over R_k, Gray maps and their binary images*, Finite Fields Appl., 17 (2011), pp. 205–219.

Yildiz Technical University, Department of Mathematics, Faculty of Arts and Sciences, Esenler, Istanbul
isiap@yildiz.edu.tr, abayram@yildiz.edu.tr

Fuchsian codes with arbitrary rates

Iván Blanco-Chacón

Aalto University

(Joint work with M. Alsina, C. Hollanti and D. Remón)

Fuchsian codes for additive white Gaussian noisy channels have been recently introduced in [2] and [1]. They are non-linear SISO codes with code rate 3 real dimensions per channel use. The codewords come from the left regular representation of certain orders of indefinite quaternion $\mathbb{Q}$-algebras. A recently discovered point-reduction algorithm in logarithmic time implies that the decoding of these codes has logarithmic complexity. In this talk we present our ongoing work, which is an extension of these results to quaternion algebras over totally real number fields of arbitrary degree. In particular, for a totally real number field of degree n, the associated non-linear code has code rate $3n$.

References

[1] M. ALSINA, I. BLANCO-CHACÓN, C. HOLLANTI, AND D. REMÓN, *Fuchsian codes for AWGN channels (journal version)*. Submitted.

[2] I. BLANCO-CHACÓN, C. HOLLANTI, AND D. REMÓN, *Fuchsian codes for AWGN channels*. PREPROCEEDINGS. The International Workshop on Coding and Cryptography, WCC 2013. p. 496–507. Bergen (2013). ISBN: 978-82-308-2269-2

Aalto University, Finland
ivnblanco@gmail.com

Tables on q-Analogs

Michael Braun

University of Applied Sciences, Darmstadt, Germany

The theory of combinatorial q-analogs has a long history reaching back to the early 19th century. Concepts, theories, and discrete structures based on finite sets and and their subsets turn into a q-analog if they are considered over finite vector spaces over a finite field $\mathbb{F}_q$ with q elements. In this case subsets of a finite set become subspaces of a finite vector space and orders of subsets become dimensions of subspaces.

A very prominent example is the q-analog of a combinatorial t-design: A t-$(n, k, \lambda; q)$ *design* is a set of k-subspaces of $\mathbb{F}_q^n$—called blocks—such that each t-subspace of $\mathbb{F}_q^n$ is contained in exactly λ blocks.

Starting from the definition of such a design over a finite field we describe the connection between several related incidence structures defined on vector spaces as *(partial) large sets of designs*, *t-wise balanced designs*, *packing designs*, *covering designs*, *random network codes*, *arcs*, *caps*, *blocking sets*, *(partial) spreads*, *(partial) parallelisms*, *partitions* etc.

Furthermore, we briefly recall the Kramer-Mesner approach for the construction of designs over finite fields and describe different refinements of this method in order to construct some of the aforementioned related incidence structures.

Finally, we provide some tables on designs and their related incidence structures presenting known and new results on q-analogs.

University of Applied Sciences, Faculty of Computer Science, Schöfferstr. 8b, Bui. D14, D-64295 Darmstadt
michael.braun@h-da.de

Error Correction for Index Coding

Marco Calderini

University of Trento, Italy

(Joint work with Eimear Byrne)

The index coding problem is described in the following scenario. 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. This number is typically lower if coding of data packets is performed by the sender.

Index coding was introduced in [3] and is a topic that has since been studied by many others [2, 5, 4, 1, 6]. Partial equivalences exist between it and the network coding problem [5]. In [4], the authors consider the problem of index coding across a noisy channel. In this generalization, the sender has a vector $x = [x_1, ..., x_n] \in \mathbb{F}_q^n$, each receiver requests a component x_i of x and lets the server know which bits it already has. The sender linearly encodes the vector x as $c = [c_1, ..., c_N] = xL$ using an $n \times N$ matrix L (satisfying certain constraints) over $\mathbb{F}_q$ and transmits the symbols of c using N transmissions. This encoding is referred to as δ-error-correcting if each receiver can retrieve its desired bit after N transmissions, as long as fewer than δ erroneous transmissions have occurred. Syndrome decoding is applied to correct errors and retrieve the required data at each receiver, which is computationally demanding (in fact NP-complete in general).

In [7], the authors describe error correction over matrix channels, which can be applied to network coding. They present a simple capacity-achieving encoding scheme and low complexity decoder based on Gaussian elimination. Here we adapt the ideas of [7] to the index coding problem. We assume the sender has vector $\hat{X} \in \mathbb{F}_{q^k}$ and that each receiver demands a component of $\hat{X}$. $\hat{X}$ is identified with a matrix $X \in \mathbb{F}_q^{n \times k}$ with respect to some fixed basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and each receiver has knowledge of some subset of the rows of X. We write χ_i to denote the indices of the rows of X known to receiver i. The data matrix X is encoded as LX for an $N \times n$ matrix L over $\mathbb{F}_q$. A requirement of L is that for each receiver i there exists $U^i \in \mathbb{F}_q^n$ whose support is contained in χ_i and such that $U^i + E^i$ is contained in the row space of L over $\mathbb{F}_q$, where E^i is the ith vector of the standard basis of $\mathbb{F}_q^n$. The ith decoder solves the equation $LX' = Y$, where X' and X agree at the rows indexed by χ_i, as in the classical index coding scheme. We suggest two decoders, one for which the matrix L is assumed to be known to each receiver, and one for which it is not. In both cases the error-trapping strategy described in [7] is used. For some M, v, the data to be transmitted is embedded in a matrix $Z \in \mathbb{F}_q^{(N+v)\times(M+v)}$ whose first v rows and columns are zero vectors. The rows of Z are sent via $N + v$ transmissions. Errors arise in the form of an $(N+v) \times (M+v)$ matrix W over $\mathbb{F}_q$. Each receiver can recover its required data from $Z+W$, given its own side information, as long as the first t rows of W have rank $t \leq v$.

References

[1] N. ALON, E. LUBETZKY, U. STAV, A. WEINSTEIN, AND A. HASSIDIM, *Broadcasting with side information*, IEEE 49th Annual IEEE Symposium on Foundations of Computer Science, 2008. FOCS '08. 2008, pp. 823–832.

[2] Z. BAR-YOSSEF, Y. BIRK, T. S. JAYRAM, AND T. KOL, *Index coding with side information*, 47th Annual IEEE Symposium on Foundations of Computer Science, 2006. FOCS '06. 2006, pp. 197–206.

[3] Y. BIRK AND T. KOL, *Informed-source coding-on-demand (iscod) over broadcast channels*, in INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3, 1998, pp. 1257–1264 vol.3.

[4] S. H. DAU, V. SKACHEK, AND Y. M. CHEE, *Index coding and error correction*, 2011 IEEE International Symposium on, Information Theory Proceedings (ISIT), 2011, pp. 1787–1791.

[5] S. EL ROUAYHEB, A. SPRINTSON, AND C. GEORGHIADES, *On the index coding problem and its relation to network coding and matroid theory*, IEEE Transactions on Information Theory, 56 (2010), pp. 3187–3195.

[6] K. SHUM, M. DAI, AND C. W. SUNG, *Broadcasting with coded side information*, 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), 2012, pp. 89–94.

[7] D. SILVA, F. KSCHISCHANG, AND R. KÖTTER, *Communication over finite-field matrix channels*, IEEE Transactions on Information Theory, 56 (2010), pp. 1296–1305.

Department of Mathematics, University of Trento, Italy
marco.calderini@unitn.it

Coding and decoding of MDS $\mathbb{F}_q$-linear codes based on superregular matrices

S. D. Cardell

Departament d'Estadística i Investigació Operativa
Universitat d'Alacant, Spain

(Joint work with J.-J. Climent and V. Requena)

Let $\mathbb{F}_q$ be the Galois field of q elements and consider b a positive integer. If $\mathcal{C}$ is a code of length n over $\mathbb{F}_q^b$, we can consider the codewords of $\mathcal{C}$ as codewords of length nb over $\mathbb{F}_q$. Then, a code $\mathcal{C}$ is said to be an $\mathbb{F}_q$**-linear code** (or a **linear array code**) of length n over $\mathbb{F}_q^b$ if it is a linear code of length nb over $\mathbb{F}_q$ (see [3]). It is worth pointing out that the code symbols of $\mathcal{C}$ can be regarded as elements in the field $\mathbb{F}_{q^b}$; however, linearity over this field is not assumed. The number $k = \log_{q^b} |\mathcal{C}|$ is called the **normalized dimension** (or just dimension) of $\mathcal{C}$ and the minimum distance d is measured over $\mathbb{F}_q^b$.

Let $[n, k, d]$ denote the parameters of the $\mathbb{F}_q$-linear code $\mathcal{C}$ over $\mathbb{F}_q^b$. Although it is not a linear code over $\mathbb{F}_{q^b}$, some properties of the linear codes are maintained for this kind of codes, for example, the Singleton bound

$$d \leq n - k + 1.$$

The $\mathbb{F}_q$-linear codes that achieve equality in the Singleton bound are called, as usual, MDS codes.

Let C be the companion matrix of a primitive polynomial of degree b over $\mathbb{F}_q$. We can define the field isomorphism $\psi : \mathbb{F}_{q^b} \longrightarrow \mathbb{F}_q[C]$, as $\psi(\alpha) = C$, where $\alpha \in \mathbb{F}_{q^b}$ is a primitive element, and we can extend it to a ring isomorphism

$$\Psi : \mathrm{Mat}_{m\times t}(\mathbb{F}_{q^b}) \longrightarrow \mathrm{Mat}_{m\times t}(\mathbb{F}_q[C])$$

in the following way: if $A = \left[\alpha_{ij}\right] \in \mathrm{Mat}_{m\times t}(\mathbb{F}_{q^b})$, then $\Psi(A) = \left[\psi(\alpha_{ij})\right] \in \mathrm{Mat}_{m\times t}(\mathbb{F}_q[C])$.

As a consequence of the properties of isomorphisms, if $A \in \mathrm{Mat}_{(n-k)\times k}(\mathbb{F}_{q^b})$ is a superrregular matrix, then $H = \left[\begin{array}{cc} \Psi(A) & I_{(n-k)b} \end{array}\right]$ is the parity check-matrix of an $[n, k, n - k + 1]$ MDS $\mathbb{F}_q$-linear code $\mathcal{C}$ over $\mathbb{F}_q^b$.

Due to this result, several families of MDS $\mathbb{F}_q$-linear codes can be constructed using known families of superregular matrices such as Vandermonde or Cauchy matrices (see [4, 5, 6]).

For a prime number p, Blaum and some of his coauthors [1, 2], introduce a binary $[p + 2, p, 3]$ MDS array code and provide a decoding algorithm based on the corresponding parity-check matrix. We present a similar algorithm for the codes proposed previously, in the binary case, for the cases $n - k = 2$ and $n - k = 4$ (one symbol in error and two symbols in error). Given an error-corrupted word, we compute the vector of syndromes using the parity-check matrix of the code. Then, we use the properties of the companion matrix of a primitive polynomial in order to find the error vector and recover the sent codeword.

The work of S. D. Cardell and J.-J. Climent was partially supported by Spanish grant MTM2011-24858 of the Ministerio de Economía y Competitividad of the Gobierno de España. The work of S. D. Cardell was also partially supported by a grant for postdoctoral students from the Generalitat Valenciana with reference APOSTD/2013/081. The work of V. Requena was partially supported by the research project UMH-Bancaja with reference IPZS01.

References

[1] M. BLAUM, J. BRADY, J. BRUCK, AND J. MENON, *Evenodd: an efficient scheme for tolerating double disk failures in raid architectures*, IEEE Transactions on Computers, 44 (1995), pp. 192–202.

[2] M. BLAUM, J. BRUCK, AND A. VARDY, *MDS array codes with independent parity symbols*, IEEE Transactions on Information Theory, 42 (1996), pp. 529–542.

[3] M. BLAUM AND R. ROTH, *On lowest density MDS codes*, IEEE Transactions on Information Theory, 45 (1999), pp. 46–59.

[4] J. LACAN AND J. FIMES, *A construction of matrices with no singular square submatrices*, in Finite fields and applications, vol. 2948 of Lecture Notes in Comput. Sci., Springer, Berlin, 2004, pp. 145–147.

[5] R. ROTH AND A. LEMPEL, *On MDS codes via cauchy matrices*, IEEE Transactions on Information Theory, 35 (1989), pp. 1314–1319.

[6] R. ROTH AND G. SEROUSSI, *On generator matrices of MDS codes (corresp.)*, IEEE Transactions on Information Theory 31 (1985), pp. 826–830.

Departament d'Estadística i Investigació Operativa, Universitat d'Alacant, Campus de Sant Vicent del Raspeig, Apartat de correus 99, E-03080 Alacant, Spain
s.diaz@ua.es, jcliment@ua.es, vrequena@umh.es

Linear codes from orthogonal Grassmannians

Luca Giuzzi

Università di Brescia, Italy

(Joint work with Ilaria Cardinali)

In this talk we shall discuss codes arising from the Grassmann embedding of an orthogonal Grassmannian. These codes can be obtained from the usual linear Grassmann codes by puncturing in a suitable set of components. Here we shall present their parameters as well as discuss some of their properties.

Università degli Studi di Brescia, DICATAM – Section of Mathematics, Via Valotti 9, I-25133 Brescia
giuzzi@ing.unibs.it

Digital Signatures for Network Coding

Oliver Gnilke

Claude Shannon Institute
University College Dublin

The approach of Network Coding generally leads to a single error affecting multiple nodes, since it spreads through the network and is combined with other packages. Error propagation or pollution has been a major disadvantage of network coding, but is inherent to the core idea of this type of coding.

Non-cryptographic network coding relies upon the assumption that all nodes are maintained and under the control of trusted and honest parties and behave exactly according to the given protocol, which is a reasonable approach under the specified assumption. In this case, the only distortions considered are random errors induced by the channels connecting the nodes. These errors are accounted for only at the sinks where they are corrected by designed network decoders.

If a network contains nodes under control of malicious adversaries intending on jamming communication between the sources and the sinks the above approach is entirely ill-suited.

Digital signatures for network coding have been designed to stop errors from spreading throughout the network. Nodes are enabled to verify integrity and authenticity of incoming packages and filter defective ones. The propagation of errors is stopped at the cost of a signature transmitted with every package.

A new class of signatures had to be designed especially for this kind of application since the packages that are sent are modified at every node without the signatory's influence. Therefore a signature had to be created that can verify linear combinations of packages. The advantages gained by using a cryptographic approach will be quantified in this talk. Furthermore we introduce security definitions for this setting, a selection of proposed signatures and the limitations they impose on the network codes to be used. We will give a prospect on future research to overcome several of these restrictions and hope this talk will inspire more research interest in the cryptographic approach to network coding.

Claude Shannon Institute, UCD CASL, 8 Belfield Office Park, Dublin 4
oliver.gnilke@gmail.com

Coding for Wireless Distributed Storage Systems

Camilla Hollanti

Aalto University

(Joint work with David Karpuk (Aalto University))

Cloud storage has emerged in recent years as an inexpensive and scalable solution for storing large amounts of data and making it widely available to users. The growing success of cloud storage has been accompanied by new advances in the theory of erasure codes for such systems, namely the application of network coding techniques for distributed data storage and the theory of regenerating codes introduced by Dimakis et al., followed by a large body of further work in the literature. However, a majority of the results achieved exclusively concern the network layer, assuming either a perfect error-free channel or a simple bit-flip error/bit erasure scenario. Surprisingly few initiatives have been taken towards the physical layer functionality, e.g., how to protect the data transmission following a data reconstruction or node repair request when communication takes place over a wireless channel. Isolated from the storage point of view, on the other hand, wireless communications research has matured over the past two decades. The aim of this talk is to tentatively draw these two aspects together and to encourage a new research direction for coding for wireless distributed and cloud storage systems.

References

[1] A. DIMAKIS, P. GODFREY, Y. WU, M. WAINWRIGHT, AND K. RAMCHANDRAN, *Network coding for distributed storage systems*, IEEE Transactions on Information Theory, 56 (2010), pp. 4539–4551.

[2] H.-F. LU, C. HOLLANTI, R. VEHKALAHTI, AND J. LAHTONEN, *Dmt optimal codes constructions for multiple-access mimo channel*, IEEE Transactions on Information Theory, 57 (2011), pp. 3594–3617.

Department of Mathematics and Systems Analysis, Aalto University, Finland
camilla.hollanti@aalto.fi

The (extended) rank weight enumerator and q-matroids

Relinde Jurrius

Vrije Universiteit Brussel, Belgium

(Joint work with Ruud Pellikaan)

Let C be an $\mathbb{F}_{q^m}$-linear code of length n. With the element $\mathbf{c} = (c_1, \ldots, c_n)$ of C an $m \times n$ matrix $m(\mathbf{c})$ is associated where the j-the column of $m(\mathbf{c})$ consists of the coordinates of c_j with respect to a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The rank weight $\mathrm{wt}_R(\mathbf{c}) = \mathrm{rk}(\mathbf{c})$ of $\mathbf{c}$ is by definition the rank of the matrix $m(\mathbf{c})$. The *rank weight enumerator* is given by

$$W_C^R(X, Y) = \sum_{w=0}^{n} A_w^R X^{n-w} Y^w,$$

where $A_w^R = |\{\mathbf{c} \in C : \mathrm{rk}(\mathbf{c}) = w\}|$. See [1].

The purpose of this talk is to investigate the rank weight enumerator of a code over $\mathbb{F}_{q^m}$ and its relation with the Tutte polynomial of the *q-matroid* of the code. This can be viewed as the q-analogon of the Hamming weight enumerator of a code over $\mathbb{F}_q$ and its relation with the Tutte polynomial of the matroid of the code, see [2].

The q-matroid will be defined on a vector space $\mathbb{F}_q^n$ instead of a finite set of n elements. We will furthermore define q-rank and the notion of q-independent subspaces of the q-matroid. Finally, we will show the relation between the Tutte polynomial of a q-matroid and the rank weight enumerator of its corresponding code.

References

[1] E. M. GABIDULIN (1985). *Theory of codes with maximal rank distance.* Problems of Information Transmission 21(1), 1–12.

[2] R. JURRIUS AND R. PELLIKAAN (2013). *Codes, arrangements and matroids.* In: Martnez-Moro, E. (Ed.), Algebraic geometry modeling in information theory, (pp. 219–325). London: World Scientific.

Vrije Universiteit Brussel, Vakgroep Wiskunde, Pleinlaan 2, 1050 Elsene
Relinde.Jurrius@vub.ac.be

Intersection numbers for q-analogs of designs

Michael Kiermaier

Universität Bayreuth

(Joint work with Mario Pavčević)

For ordinary t-designs, intersection numbers have been introduced by Mendelsohn in 1971. They have been used successfully for both non-existence proofs and constructions.

In this talk, we will define intersection numbers for q-analogs of designs, and give q-analogs of the Mendelsohn and Köhler equations. As an application, we will get some information on the structure of a putative q-analog of the Fano plane, which is a 2-$(7,3,1)_q$ design. In particular, the existence of a 2-$(7,3,1)_q$ design implies the existence of a 2-$(7,3,q^4)_q$ design.

This research was carried out as part of the short term scientific mission COST-STSM-IC1104-12362 in spring 2013 at the University of Zagreb.

Universität Bayreuth
Lehrstuhl für Mathematik II
D-95440 Bayreuth
Germany
michael.kiermaier@uni-bayreuth.de

Coding for the Permutation Channel

Mladen Kovačević

University of Novi Sad, Serbia

(Joint work with Dejan Vukobratović)

In their seminal paper [4], Kötter and Kschischang proposed *subspace codes* (i.e., codes in projective spaces and Grassmanians) as appropriate constructs for error correction in networks employing random linear network coding (RLNC). The basic idea behind their approach relies on a simple invariance principle. It turns out that this principle can also be applied in some other communication scenarios, such as multipath routed networks, thus providing interesting parallels between the corresponding models.

Permutation channel. A permutation channel over a finite alphabet $\mathcal{A}$ is a communication channel that takes sequences of symbols from $\mathcal{A}$ as inputs, and for any input sequence outputs a random permutation of this sequence. Such channels arise, for example, in some types of packet networks in which the packets comprising a single message are routed separately and are frequently sent over different routes in the network. Consequently, the receiver cannot rely on them being delivered in any particular order. It is interesting to observe that the permutation channel is a special case of the channel induced by RLNC networks, obtained by restricting the set of random matrices that transform the source packets to the set of permutation matrices. In other words, delivering a random permutation of the packets is a special case of delivering multiple linear combinations of the packets.

In addition to random permutations, the channel is assumed to impose other deleterious effects on the transmitted sequence, such as insertions, deletions, and substitutions of symbols. For example, in a networking scenario mentioned above, packet deletions can be caused by network congestion and consequent buffer overflows in the routers.

Coding for the permutation channel. It is clear from the definition of the permutation channel that, when transmitting sequences through it, no information should be encoded in the order of symbols in the sequence because it is impossible to recover this information. The only carrier of information should be the *multiset* of the symbols sent, i.e., the number of occurrences of each symbol from $\mathcal{A}$ in the sequence. The appropriate space in which error-correcting codes for the permutation channel should be defined is therefore the set of all multisets (of certain cardinality) over the channel alphabet [6]. The resulting framework is a generalization of coding in power sets [2, 3, 5], where codewords are taken to be *sets* rather than multisets. Such approaches to coding for the permutation channel are somewhat analogous to the approach of Kötter and Kschischang [4]. Namely, in both cases the guiding idea is to define codes in the space of objects invariant under the channel transformation – (multi)sets are invariant under permutations, whereas vector spaces are invariant (with high probability) under random linear combinations.

We intend to introduce a formal definition of *multiset codes* and their parameters. Their equivalence to the codes in $\mathbb{Z}_+^n$ will be shown, and some geometric and combinatorial properties studied based on this equivalence. In particular, the proof of (non)existence of perfect multiset codes [7] under relevant metrics will be given.

References

[1] M. BRAUN, *On lattices, binary codes, and network codes*, Adv. Math. Commun., vol. 5, no. 2, pp. 225–232, May 2011.

[2] M. GADOULEAU AND A. GOUPIL, *Binary Codes for Packet Error and Packet Loss Correction in Store and Forward*, in: Proc. Int. ITG Conf. on Source and Channel Coding, Siegen, Germany, Jan. 2010.

[3] M. GADOULEAU AND A. GOUPIL, *A Matroid Framework for Noncoherent Random Network Communications*, IEEE Trans. Inf. Theory, vol. 57, no. 2, pp. 1031–1045, Feb. 2011.

[4] R. KÖTTER AND F. R. KSCHISCHANG, *Coding for Errors and Erasures in Random Network Coding*, IEEE Trans. Inf. Theory, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[5] M. KOVAČEVIĆ AND D. VUKOBRATOVIĆ, *Subset Codes for Packet Networks*, IEEE Commun. Lett., vol. 17, no. 4, pp. 729–732, April 2013.

[6] M. KOVAČEVIĆ AND D. VUKOBRATOVIĆ, *Multiset Codes for Permutation Channels*, preprint available at arXiv:1301.7564.

[7] M. KOVAČEVIĆ AND D. VUKOBRATOVIĆ, *Perfect Codes in the Discrete Simplex*, preprint available at arXiv:1307.3142.

University of Novi Sad, Department of Electrical Engineering, Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
kmladen@uns.ac.rs

Derived and Residual q-Designs

Reinhard Laue

Universität Bayreuth

(Joint work with Michael Kiermaier)

A generalization of forming derived and residual designs from t-designs to q-analoga is proposed. The existence of these designs is discussed. If both exist then a new design is constructed, generalizing a construction of Tran van Trung [3], van Leijenhorst [2], Driessen [1] from t-designs to q-analoga. A series of new designs is obtained from this construction. An application to a Large Set construction is derived.

References

[1] LEON M.H.E. DRIESSEN, *t-designs, $t \geq 3$*, Technical Report, Department of Mathematics, Eindhoven University of Technology, (1978).

[2] D. C. VAN LEIJENHORST, *Orbits on the projective line*, J. Combin. Theory Ser. A, 31 (1981), pp. 146–154.

[3] T. VAN TRUNG, *On the construction of t-designs and the existence of some new infinite families of simple 5-designs*, Arch. Math. (Basel), 47 (1986), pp. 187–192.

Universität Bayreuth
95440 Bayreuth
Germany
laue@uni-bayreuth.de

Random network coding, t-designs, and the representation theory of $GL(n, \mathbb{F}_q)$

Cristina Martínez

CSIC-Consejo Superior de Investigaciones Científicas

The encoding of an information word into a $k-$dimensional subspace is usually known as coding for errors and erasures in random network coding. More precisely, let V be an $N-$dimensional vector space over $\mathbb{F}_q$, a code for an operator channel with ambient space V is simply a nonempty collection of subspaces of V. The collection of subspaces is a code for correcting errors that happen to data sent through an operator channel. We can parametrize the matrix coding the information by random variables $a_1, a_2, \ldots, a_n$ which constitute the letters of an alphabet.

Algebraic geometric (AG) codes use as an alphabet a set $\mathcal{P} = \{P_1, \ldots, P_N\}$ of $N - \mathbb{F}_q-$rational points lying on a smooth projective curve C defined over a finite field $\mathbb{F}_q$, that is, in projective coordinates $P_i = [x_i : 1]$ with $x_i \in \mathbb{F}_q$. To each non constant rational function φ on the function field of the curve C defined over $\mathbb{F}_q$ one can associate a matrix with entries in $\mathbb{F}_q$ corresponding to the matrix of an endomorphism of $\mathbb{F}_q-$modules. In several cases, it is possible to count the number of codewords of the code by a simple count of the number of normalized polynomials of degree fixed d over $\mathbb{F}_q$. We will study some examples where these numbers are expresed by closed combinatorial formulas.We will concentrate in the case of cyclic codes also known as Reed-Muller codes, in which the underlying vector space $(\mathbb{F}_q)^n$ is generated by a unique element α over $\mathbb{F}_q$. We study invariant subspaces of $(\mathbb{F}_q)^n$ by finite subgroups of the general linear group $GL(n, \mathbb{F}_q)$ as $t-$designs relating the problem to the representation theory of $GL(n, \mathbb{F}_q)$.

References

[1] A. BESANA, C. MARTÍNEZ, *Codes, Horn's problem and Gromov-Witten invariants*, arXiv: 1202.5221

[2] R. KOETTER AND F. KSCHISCHANG, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory, 54 (2008), pp. 3579–3591.

[3] F. MANGANIELLO, A. TRAUTMANN, AND J. ROSENTHAL, *On conjugacy classes of subgroups of the general linear group and cyclic orbit codes*, in IEEE International Symposium on Information Theory Proceedings (ISIT), 2011 , 2011, pp. 1916–1920.

[4] SUDHIR R. GHORPADE AND SAMRITH RAM, *Enumeration of splitting subspace over finite fields*, math.CO, arxiv: 1203.1849.

CSIC-Consejo Superior de Investigaciones Científicas, Campus UAB s/n, 08193 Bellaterra
cristina@iiia.csic.es

Tactical decomposition of designs over finite fields

Anamari Nakić

University of Zagreb

(Joint work with Mario-Osvin Pavčević)

A t-(v,k,λ_t) design can be generalized as follows. A t-$(v,k,\lambda_t;q)$ design over a finite field $\mathbb{F}_q$ is a set $\mathcal{B}$ of k-dimensional subspaces of a v-dimensional vector space over $\mathbb{F}_q$, called blocks, with the property that any t-dimensional subspace is contained in exactly λ_t blocks. Throughout this talk, 1-dimensional subspaces will be called points. Let Ψ be the set of all points. The motivation to study tactical decompositions of designs over finite fields comes from the fact that for $t = 2$ every design over $\mathbb{F}_q$ gives a 2-design $(\Psi, \mathcal{B})$, where a block is identified with the set of points it contains. A decomposition of a t-$(v,k,\lambda_t;q)$ design $\mathcal{B}$ is any partition of the set $\Psi = \Psi_1 \sqcup \cdots \sqcup \Psi_m$ and of the set $\mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n$. We say that a decomposition is tactical if there are nonnegative integers ρ_{ij} and κ_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$, such that each point of Ψ_i lies in exactly ρ_{ij} blocks of $\mathcal{B}_j$, and each block of $\mathcal{B}_j$ contains exactly κ_{ij} points from Ψ_i. Matrices $[\rho_{ij}]$ and $[\kappa_{ij}]$ are called tactical decomposition matrices. Examples can be constructed by taking the orbits of Ψ and of $\mathcal{B}$ obtained by an action of an automorphism group $G \leq GL(v,q)$ of the design $\mathcal{B}$ over $\mathbb{F}_q$.

In this talk, we present results obtained for tactical decompositions of 2-$(v,k,\lambda_2;q)$ designs. We show that coefficients of tactical decomposition matrices comply an equation system analogous to the one for 2-designs:

$$\sum_{j=1}^{n} \rho_{i_1 j} \kappa_{i_2 j} = \lambda_2 \cdot |\Psi_{i_2}| + \delta_{i_1 i_2} \cdot (\lambda_1 - \lambda_2).$$

The emphasis of the talk is on the additional system of inequations for coefficients of tactical decomposition matrices of designs over $\mathbb{F}_q$. This system is obtained by taking into consideration specific properties of designs over $\mathbb{F}_q$ while using the known proving techniques for t-designs. This system of equations and inequations for coefficients of tactical decomposition matrices represents necessary conditions for the existence of designs over $\mathbb{F}_q$ with an assumed automorphism group. The necessary conditions are implemented in the well-known Kramer-Mesner method for construction of designs over finite fields. Using these additional constraints the adjoined Kramer-Mesner system can be replaced with several smaller systems of linear equations, leading to a reduction of the overall computation time needed for construction of designs over finite fields.

University of Zagreb, Faculty of electrical engineering and computing, Unska 3, 10000 Zagreb, Croatia
anamari.nakic@fer.hr

Partial Spreads in Network Coding

Alberto Ravagnani

Université de Neuchâtel

(Joint work with Elisa Gorla)

Following the approach by R. Kötter and F. R. Kschischang, we study codes for errors and erasures for random network coding as families of k- dimensional linear spaces over a finite field. Following an idea in finite pro- jective geometry, we introduce a class of network codes which we call partial spread codes. Partial spread codes naturally generalize the known family of spread codes. We provide an easy description of such codes, discuss their maximality, and explain how to decode them efficiently.

References

E. GORLA AND A. RAVAGNANI, *Partial Spreads in Random Network Coding*, `http://arxiv.org/abs/1306.5609`.

Institut de Mathématiques, Université de Neuchâtel Emile-Argand 11, CH-2000 Neuchâtel (Switzerland)
alberto.ravagnani@unine.ch

Rank metric and Gabidulin codes in characteristic zero

Gwezheneg Robert

Université de Rennes 1 and INRIA, France

(Joint work with Daniel Augot and Pierre Loidreau)

We transpose the theory of rank metric and Gabidulin codes to the case of fields of characteristic zero. The Frobenius automorphism is then replaced by any element of the Galois group. We derive some conditions on the automorphism to be able to easily transpose the results obtained by Gabidulin as well and a classical polynomial-time decoding algorithm. We also provide various definitions for the rank-metric.

Université de Rennes 1, Rennes, France
INRIA – École Polytechnique, Paris, France
gwezheneg.robert@univ-rennes1.fr

List decoding of subspace codes

Joachim Rosenthal

University of Zurich

(Joint work with Anna-Lena Trautmann)

Important subvarieties of the Grassmann variety are the so called Schubert varieties. We will describe them with their defining equations. Schubert calculus is concerned with the intersection of Schubert varieties. It was first rigorously verified in the 20th century by algebraic means by van der Waerden (1929). The modern approach is via cohomology theory which requires that the base field is algebraically closed. For finite fields the algebraic methods of van der Waerden can still be carried through and we will concentrate on this.

We will show that the list decoding problem subspace codes in network coding can be seen as an intersection problem of a Schubert variety with the set of code words. If the last set has some defining equations one has defining equations for the list decoding problem.

Mathematics Institute, Winterthurerstr 190, CH-8057 Zurich, Switzerland
rosen@math.uzh.ch

Random Network Coding Advantage over MDS Codes for Adaptive Multimedia Communications

Paresh Saxena

Universitat Autònoma de Barcelona

(Joint work with M. A. Vázquez-Castro)

In [2], Ho et al. introduced randomized linear network coding for distributed multisource multicast deriving upper bounds of the error probability. In [1], Balli et al. derive upper bounds for single source multicast on the probability mass function of the minimum distance of the code. In this paper, we focus on the time-variant version of the latter with distributed channel erasures in time instead of distributed link failures in space. Specifically, we focus on systematic random linear network coding (SRNC) over time-variant point-to-point erasure channels. Our contribution is three fold. First, we derive the exact probability mass function of the minimum distance of SRNC (d_{SRNC}) based on the erasure probability. Second, we investigate the potential of SRNC codes to replace MDS codes, specifically Reed-Solomon (RS) codes with minimum distance (d_{RS}). We show that the difference between the minimum distance of the two codes; i.e., $d_{RS} - d_{SRNC}$ tends to zero for practical finite field sizes. Further, we quantify the advantage of SRNC in terms of decoding delay using on-the-fly progressive decoding. Finally, we show the advantage of SRNC over MDS codes in terms of flexibility for adaptive joint source-channel protection in multimedia transmission.

References

[1] H. BALLI, X. YAN, AND Z. ZHANG, *On randomized linear network codes and their error correction capabilities*, IEEE Transactions on Information Theory, 55 (2009), pp. 3148–3160.

[2] T. HO, M. MEDARD, R. KOETTER, D. KARGER, M. EFFROS, J. SHI, AND B. LEONG, *A random linear network coding approach to multicast*, IEEE Transactions on Information Theory, 52 (2006), pp. 4413–4430.

Universitat Autònoma de Barcelona, Barcelona, Spain
paresh.saxena@uab.es

Asymptotic Analysis of Coded Slotted ALOHA

Čedomir Stefanović

Aalborg University, Denmark

(Joint work with Petar Popovski)

Analogies between successive interference cancellation in slotted ALOHA framework and iterative belief-propagation erasure-decoding have been established recently, opening the possibilities to enhance random access protocols by application of theory and tools of erasure-correcting codes [1][2]. The asymptotic performance of erasure-correcting codes is standardly assessed by using the and-or tree evaluation [3]. In this talk we present the application of the and-or tree evaluation for the asymptotic analysis of the slotted ALOHA-based protocols. We generalize it for the case when the contending users and slots are divided into classes. We also include in the analysis the impact of channel conditions, which may vary over user classes, inducing different packet loss probabilities.

References

[1] G. LIVA, *Graph-based analysis and optimization of contention resolution diversity slotted aloha*, IEEE Transactions on Communications, 59 (2011), pp. 477–487.

[2] M. G. LUBY, M. MITZENMACHER, AND M. A. SHOKROLLAHI, *Analysis of random processes via And-Or tree evaluation*, in Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 1998), New York, 1998, ACM, pp. 364–373.

[3] C. STEFANOVIC, P. POPOVSKI, AND D. VUKOBRATOVIC, *Frameless aloha protocol for wireless networks*, Communications Letters, IEEE, 16 (2012), pp. 2087–2090.

Aalborg University, Department of Electronic Systems, Fredrik Bajers Vej 7, 9220 Aalborg, Denmark
cs@es.aau.dk

Unequal Error Protection Random Network Coding for Multimedia Communications

Dejan Vukobratović

University of Novi Sad

Rateless (fountain) codes are a popular class of sparse-graph codes that attracted significant attention in coding-theoretic research over the last decade. In this talk, we focus on random linear coding as a fountain coding solution that underlies most of the practical network coding implementations. In particular, we are interested in the design and the performance limits of a class of Unequal Error Protection (UEP) random linear codes that are particularly suitable for network-coded multimedia communications.

University of Novi Sad, Novi Sad, Trg D. Obradovića 6, 21000 Novi Sad, Serbia
dejanv@uns.ac.rs

Bounds on List Decoding of Rank-Metric Codes

Antonia Wachter-Zeh

Institute of Communications Engineering, University of Ulm, Ulm, Germany and Institut de Recherche Mathémathique de Rennes (IRMAR), Université de Rennes 1, Rennes, France

So far, there is no polynomial-time list decoding algorithm (beyond half the minimum distance) for Gabidulin codes, which can be seen as the rank-metric equivalent of Reed–Solomon codes. This talk provides bounds on the list size of rank-metric codes in order to understand whether polynomial-time list decoding is possible or whether it works only with exponential time complexity.

Three bounds on the list size are proven. The first is a lower exponential bound for Gabidulin codes and shows that for Gabidulin codes no polynomial-time list decoding beyond the Johnson radius exists. Second, an exponential upper bound is derived, which holds for any rank metric code of length n and minimum rank distance d. The third bound proves that there exists a rank metric code over $\mathbb{F}_{q^m}$ of length $n \leq m$ such that the list size is exponential in the length for any radius greater than *half the minimum distance*. This implies that there cannot exist a *polynomial* upper bound depending only on n and d similar to the Johnson bound for Hamming metric. All three bounds reveal significant differences to codes in Hamming metric.

Details on these results can be found in [1].

References

[1] A. WACHTER-ZEH, *Bounds on List Decoding of Rank-Metric Codes*, *preprint*, 2013. [Online]. Available: `http://arxiv.org/abs/1301.4643`

Ulm University, Institute of Communications Engineering, Albert-Einstein-Allee 43, 89081 Ulm, Germany
antonia@codingtheory.eu