D. Augot - Connections between decoding Reed-Solomon codes and solving discrete logarithms over extension fields

Joint work wih Francois Morain.
A connection between the discrete logarithm problem over Fq^h and the problem of decoding Reed-Solomon codes over Fq has been proposed and studied by Cheng, Wang at FOCS 2004, essentially in a theoretical manner to study the hardness of decoding a Reed-Solomon codes when a large number of errors occurs. We propose to study this reduction in a reverse direction from a practical point of view : how do decoding algorithms help in solving the discrete logarithm problem over finite fields. The first step is to consider a unique decoding algorithm, like Gao's algorithm, and to adapt it to the discrete logarithm problem. We have implemented this approach in Magma and NTL and have made numerical computations. Although the method seems less efficient than the original Adleman index-calculus method, there are some original directions that we will discuss.

C. Bachoc - New geometric applications of the linear programming method

Using the linear programming method combined with Frankl-Wilson intersection theorems we will show how to improve the known asymptotic estimates for the measurable chromatic number of Euclidean space.
We will also discuss the possibility to improve the linear programming bounds using induced subgraphs and other methods in the cases of Johnson and Hamming spaces.

E. Bayer - Ideal lattices in abelian number fields

Ideal lattices are useful in the construction of codes for fading channels. The existing constructions mostly rely on cyclotomic fields and their totally real subfields. The purpose of this talk, based on a joint work with Piotr Maciak, is to describe a family of ideal lattices associated to abelian number fields of prime power conductor. This also has applications to Euclidean minima, in particular Minkowski's conjecture.

M. Bianchi - Disguising the secret code structure in non-Goppa-based McEliece variants

Joint work with Marco Baldi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani.
The talk will aim at describing a variant of the McEliece cryptosystem able to disguise the structure of the secret code, chosen by the authorized user, in such a way that the public key is no longer permutation-equivalent to the secret code. This increases the security level of the public key, thus opening the way for reconsidering the adoption of classical families of codes, like Generalized Reed-Solomon codes (GRS), that have been longly excluded from the McEliece cryptosystem for security reasons. However the framework implementation is not intended only to GRS codes and can be adapted to a number of code families. The talk will highlight how to adopt GRS codes as an example of algebraic codes. This choice is due to their optimum distance properties that could yield a reduction in the key size or, equivalently, an increased level of security against information set decoding. Possible vulnerabilities and attacks related to the considered system will be described; the best design choices aimed to avoid these attacks will be also shown.

M. Borello - Automorphisms of order 2p in binary self-dual extremal codes with an application to the remarkable case of length 72

Let C be a binary self-dual code with an automorphism g of order 2p, where p is an odd prime, such that g^p is a fixed point free involution. If C is extremal of length a multiple of 24 all the involutions are fixed point free, except the Golay Code and eventually putative codes of length 120. Connecting module theoretical properties of a self-dual code C with coding theoretical ones of the subcode C(g^p) which consists of the set of fixed points of g^p, we prove that C is a projective F_2<g>-module if and only if a natural projection of C(g^p) is a self-dual code.
This result has a nice application in the search of an extremal self-dual code of length 72, whose existence is a long-standing open problem. Supposing that such a code has an automorphism g of order 6, we prove that it is a projective F_2<g>-module. We use this fact to do an exhaustive search and we do not find an extremal code. This proves that the automorphism group of an extremal code of length 72 does not contain elements of order 6.

N. Boston - Violations of the Ingleton Inequality

Joint with Ting-Ting Nan.
In network information theory, non-Shannon-type inequalities arise in determining capacity/entropy regions where there are more than three random variables.
The most famous such inequality is the Ingleton inequality, which is satisfied by linear network codes. To produce better network codes raises the question of finding points in the region that violate the Ingleton inequality and this problem can be translated into group theory. Abelian and small groups do not produce violations, and Mao, Thill, and Hassibi computed that the smallest Ingleton-violating group is the symmetric group on five letters, of order 120. They then generalized this example to other matrix groups. In each of their cases, the Ingleton ratio (which is less than or equal to 1 if and only if the inequality holds) is smaller than 4/3.
We go beyond their work to show that examples of Ingleton-violating groups abound, construct explicit examples with arbitrarily large Ingleton ratio, give a systematic approach to finding good examples and a much simplified formula for the Ingleton ratio, and give supporting evidence for the Four-Atom Conjecture of Dougherty, Freiling, and Zeger, which would bound the ratio in terms of the group order.

S. Buzaglo - On the Existence of Perfect Codes for Asymmetric Limited-Magnitude Errors

Joint work with Prof. Tuvi Etzion.
Asymmetric error-correcting codes were subject to extensive research due to their application in coding for computer memories. The advance of technology and the appearance of new nonvolatile memories, such as flash memory, led to a new type of asymmetric errors which have limited-magnitude. Errors in this model are usually in one direction and are not likely to exceed a certain limit. This means that a cell in level i can be raised by an error to level j , such that $i < j$ and $j - i \leq \ell$, where ℓ is the error limited-magnitude.
In this work we mainly consider perfect codes for asymmetric limited-magnitude errors. We consider only linear codes over the ring Z_q . Cassuto et al. showed that every t-error-correcting perfect code in the Hamming scheme, over GF(q), is also a perfect code for error-correction of t asymmetric errors with limited-magnitude $q - 1$. However, there exist many other perfect codes in the asymmetric limited-magnitude errors model that are not perfect Hamming codes. As oppose to the Hamming scheme, in which perfect codes are well known, the existence/nonexistence question of perfect codes in the asymmetric limited-magnitude errors model is far for being solved. We address this question by using two equivalent concepts to perfect linear codes, namely, lattice tiling and group splitting. We present constructions of perfect codes for asymmetric limited-magnitude errors as well as nonexistence result.

I. Duursma - Secure error-correcting codes from nested codes

Secure error-correcting codes add redundancy for reliable error-correction as well as randomness to ensure security. The use of a coset scheme based on nested code pairs C0 containing C1 gives the flexibility to balance the two conflicting demands. Our main result is a decomposition for the weight hierarchies of the codes C0 and C1 and their intermediate codes that describes the information gain and equivocation for the coset scheme.

M. Effros - Reduction as a Tool for Coding and Capacity

Reduction is a central strategy in computer science that is less commonly applied in communications. The reduction strategy yields simple arguments that uncover fundamental properties of networks and enable new approaches for expanding the reach of information theory. A brief introduction to the use of reduction in information theory will be followed by a discussion of some early results and their implications for capacity calculations and for coding.

T. Etzion - Automorphisms of Codes in the Grassmann Scheme

Coding problems in the Grassmannian space have been a sub ject of intensive research in the last five years due to the applications of the related codes in error-correction for random network coding. Two mappings in a finite field, the Frobenius mapping and the cyclic shift mapping, are applied on codes in the Grassmannian, or lines in PG(n, p), to form an automorphisms group in the code. These automorphisms are examined on two classical coding problems in the Grassmannian. The first one is the existence of a Steiner structure. The second one is the existence of a parallelism with lines of the related projective geometry. A new parallelism and a large code which is only slightly short of a Steiner structure, are formed by using a computer search. We also survey the main open problems in this area.

H. Gluesing-Luerssen - About Various MacWilliams Identities for Codes over Finite Commutative Rings

In this talk we will provide a unified approach to MacWilliams identities for various weight enumerators of linear block codes over Frobenius rings. Such enumerators count the number of codewords having a pre-specified property. MacWilliams identities yield a transformation between such an enumerator and the corresponding enumerator of the dual code. All identities can be derived from a MacWilliams identity for the full weight enumerator using the concept of an F-partition, as introduced by Zinoviev and Ericson (1996). With this approach, we recover the MacWilliams identities for the Hamming weight, the symmetrized Lee weight, the support enumerator, the complete and the exact weight enumerator, and the Rosenbloom-Tsfasman weight.

T. Ho - Two network problems and their application to streaming codes

We consider two established problems in networks, whose complete solutions are open. The first is a resource allocation problem that can be posed in a distributed storage context as follows. The problem is to store a unit size data object on a set of storage nodes such that the total amount of storage used does not exceed a given budget, and the probability of successful recovery is maximized under a given probabilistic model for node failure/accessibility. The second is network error correction coding for reliable communication over networks where arbitrary errors can occur on an unknown subset of links. We describe how some of our recent results on these two problems can be combined to design and analyze erasure correction coding for online streaming under probabilistic packet erasures.

C. Hollanti - Geometry of numbers and wiretap channels

The error probability of various coding schemes based on algebraic lattice constellations is evaluated. This is done by using the Dedekind zeta functions of the algebraic number fields involved in the lattice constructions. In particular, it is shown how to upper bound the error performance of a finite constellation on a Raighley fading channel and the probability of eavesdropper's correct

decision on the wiretap channel. As a byproduct, an estimate of the number of elements with a certain algebraic norm is derived.
Joint work with E. Viterbo and D. Karpuk.

N. Kashyap - Coding for "Grains" Channels

Conventional magnetic recording media are composed of tiny fundamental magnetizable units, called "grains", that are random in size and shape. Data are stored on a 2-dimensional recording medium in the form of bits written into evenly spaced bit cells. Writing involves uniformly polarizing all the grains within a bit cell. In the push towards terabit-density magnetic recording, bit cells get smaller and smaller, their size eventually becoming commensurate with the size of an individual grain. At this stage, lack of precise knowledge of grain boundaries becomes a bottleneck. This lack of knowledge manifests itself in the form of an error mechanism in which bits of data get overwritten by their neighbours on the medium. We consider some simplified versions of this error model, and give constructions of codes that can correct this type of error. We also investigate combinatorial and information-theoretic bounds on the rate of optimal codes for such "grains" channels.
This is joint work with Alexander Barg, Arya Mazumdar, and K.M. Shivkumar.

M. Kiermaier - New ring-linear codes of high minimum distance

The Kerdock and Preparata codes contain more codewords than known any linear binary code of the same length and minimum distance. Both series of codes can be constructed as the Gray images of linear codes over the integers modulo 4.
Recently, new infinite series of ring-linear codes have been discovered, whose Gray images outperform all known comparable linear codes over finite fields. In this talk, an overview of these new codes will be given.

F. Kschischang - Coding for Finite-Ring Matrix-Channels

Though network coding is traditionally performed over finite fields, recent work on lattice network coding suggests that, by allowing network coding over finite rings, more efficient lattice network coding schemes can be constructed. This motivates a systematic study of network coding over finite rings. As a starting point, the problem of communication over a finite-ring matrix channel $Y = AX + Z$ is considered; both capacity results and capacity-achieving coding schemes are provided, extending the work of Silva, Kschischang and Koetter (2010), who handled the case of finite fields. A key step in this work is the extension from Gaussian-Jordan elimination to Howell-form reduction.
Joint work with Chen Feng and Roberto W. Nobrega.

V. Kumar - Codes with Local Regeneration

Joint with Govinda M. Kamath, N. Prakash, V. Lalitha.
This talk deals with codes that possess both global and local error-correction properties. The envisaged application is a distributed storage network in which each code symbol is stored in a different node. A second local property of interest in such settings, is the ability to efficiently repair a failed node. In the talk we will provide a bound relating global to local minimum distance and provide several constructions that are optimal with respect to this bound including constructions in which the local codes are regenerating codes.

S. Mesnager - Some recent results on bent and hyper-bent functions

Bent functions are maximally nonlinear Boolean functions with an even number of variables. They were introduced by Rothaus in 1976. For their own sake as interesting combinatorial objects, but also because of their relations to coding theory (Reed-Muller codes) and applications in cryptography (design of stream ciphers), they have attracted a lot of research, specially in the last 15 years. The class of bent functions contains a subclass of functions, introduced by Youssef and Gong in 2001, the so-called hyper-bent functions, whose properties are still stronger and whose elements are still rarer than bent functions. Hyper-bent functions are both of theoretical and practical interest. In fact, they were initially proposed by Golomb and Gong as a component of S-boxes to ensure the security of symmetric cryptosystems. Moreover, there exists a relationship between cyclic codes and hyper-bent functions.
We present some recent results in bent and hyperbent functions including a recent joint work dealing with bent and hyper-bent functions with Dillon like exponents and joint works dealing with bent functions from the class H (introduced in a joint work with Carlet) and o-polynomials.

O. Milenkovic - Permutation Codes in the Ulam Metric

We consider permutation codes in the Ulam metric, suitable for use in flash memories exposed to radiation or experiencing catastrophic charge leakage. Our results include asymptotically tight upper bounds on the size of
the permutation codes, code constructions based on recursive interleaving of permutation arrays and polynomial time decoding algorithms for a special class of permutation codes.
This is joint work with F. Farnoud and V. Skachek.

C. Peters - AG codes for Code-based Cryptography (or How to end a bad reputation)

Higher-genus AG codes are widely thought to be useless for code-based cryptography. This talk will do away with this myth by discussing possible setups.

M. Piva - A new bound on the distance of cyclic codes

Many bounds on the distance of a cyclic code are known. Most of them are based on the defining set of the code. We propose a similar bound, that improves on the Hartmann-Tzeng bound and on the Betti-Sala bound. It is independent of the Roos bound, but it has similar performance.

N. Silberstein - Optimal locally repairable codes via rank-metric codes

Joint work with Ankit Singh Rawat and Sriram Vishwanath.

In distributed storage systems data is reliably stored over a network of nodes in such a way that a user (data col lector) can retrieve the stored data even if some system nodes fail. To achieve such a resilience against node failures, distributed storage systems introduce data redundancy based on different coding techniques.
For example, erasures codes are widely used in such systems: when using an (n, k) code, data to be stored is first divided into k blocks and then these k information blocks are encoded into n blocks stored in n different nodes in the system. In addition, when a single node fails, the system reconstructs the data stored in the failed node to keep the required level of redundancy. This process of data reconstruction for a failed node is called node repair process. During a node repair process the node which joins the system instead of the failed node downloads the data from a set of available nodes. When the size r of such a set is smaller than the number of information blocks k, the codes used to store the data are called locally repairable codes and r is called locality.
In this talk we will consider locally repairable codes which have all-symbols locality and have the maximal possible minimum distance, or equivalently, can tolerate the maximum number of node failures. The explicit construction of such codes has been known only for the case when (r + 1) divides n, where r is a given locality and n is the length of a code. We will present a new explicit construction for locally repairable codes with all-symbols locality. This construction is based on rank-metric codes and provides optimal locally repairable codes for larger family of parameters. This is the first explicit construction of optimal locally repairable codes with (r + 1) does not divide n, which has been stated as an open problem. In addition, we will discuss some generalizations of such codes and will show that by using optimal rank-metric codes we can also construct optimal generalized locally repairable codes.

V. Skachek - Hybrid Noncoherent Network Coding

Joint work with Olgica Milenkovic and Angelia Nedich.
We describe a novel extension of subspace codes for noncoherent networks, suitable for use when the network is viewed as a communication system that introduces both dimension and symbol errors. We show that when symbol erasures occur in a significantly large number of different basis vectors transmitted through the network and when the min-cut of the networks is much smaller then the length of the transmitted codewords, the new family of codes outperforms their subspace code counterparts.
For the proposed coding scheme, termed hybrid network coding, we derive two upper bounds on the size of the codes. These bounds represent a variation of the Singleton and of the sphere-packing bound. We show that a simple concatenated scheme that represents a combination of subspace codes and Reed-Solomon codes is asymptotically optimal with respect to the Singleton bound. Finally, we describe two efficient decoding algorithms for concatenated subspace code.

C. Stefanovic - Codes-on-graphs and slotted ALOHA

In this talk we present a novel approach for optimizing distributed ALOHA-like random access schemes that is based on recently introduced analogies between successive interference cancellation and iterative belief propagation decoding on erasure channels. Specifically, we focus on the design of a slotted ALOHA scheme, in which users independently perform random access with a predefined probability on a slot basis, resulting with a rateless-like distribution of user transmissions over slots.
The presented results show that by the proposed approach rather rather high throughputs can be achieved, comparable or even higher to the ones reported in recent literature.

L. Storme - Linear codes arising from finite geometrical structures

In recent years, there have been a large number of results on linear codes arising from finite geometrical structures.
First of all, for many years, the linear codes with generator matrix equal to the incidence matrix of the points and the k-spaces of the finite projective spaces PG(n, q) of dimension n and order q have been of great interest [3].
Geometrical methods were used to determine the minimum weight of these codes and these codes were reciprocally used to obtain new results about substructures of finite projective spaces [1]. Recently, the results on the
small weight codewords of these codes have been improved [4].
Similarly, linear codes linked to the finite generalized quadrangles have been investigated, from the point of view of LDPC codes [5]. This was extended to linear codes linked to finite classical polar spaces [6].
Finally, functional codes linked to quadrics and Hermitian varieties have received a lot of attention [2].
This talk presents a number of these results to give an idea of the great variety of linear codes that are linked to finite geometrical structures, and of the different techniques used to obtain these results.

References:

[1] E.F. Assmus, Jr. and J.D. Key, Designs and their codes. Cambridge University Press, 1992.
[2] F.A.B. Edoukou, A. Hallez, F. Rodier, and L. Storme, On the small weight codewords of the functional codes Cherm(X), X a non-singular Hermitian variety. Des. Codes Cryptogr. 56 (2010), 219-233.
[3] Y. Kou, S. Lin, and M.P.C. Fossorier, Low-density parity check codes based on finite geometries: a rediscovery and new results.

IEEE Trans. Inform. Theory 47 (2001), 2711-2736.
[4] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde, An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of P G(n, q). J. Combin. Theory, Ser. A 116 (2009), 996-1001.
[5] Z. Liu and D.A. Pados, LDPC codes from generalized polygons. IEEE Trans. Inform. Theory 51 (2005), 3890-3898.
[6] V. Pepe, L. Storme, and G. Van de Voorde, On codewords in the dual code of classical generalized quadrangles and classical polar spaces. Discr. Math. 310 (2010), 3132-3148.

P. Vontobel - Analysis of message-passing iterative decoders via zeta functions

During the last decade, a variety of results have been presented on the use of graph-based zeta functions for analyzing graphical models. Some recent advances allow us to connect these disparate results and to provide a more unified framework of this type of graphical-model analysis. In particular, these advances allow us to connect computation tree pseudo-codewords and graph-cover pseudo-codewords, two central objects in the analysis of message-passing iterative decoders of low-density parity-check codes. (Based on joint work with Henry D. Pfister, Texas A&M University).