Report from Dagstuhl Seminar 11461

Coding Theory

Edited by

Joachim Rosenthal[1], M. Amin Shokrollahi[2], and Judy Walker[3]

1 **Universität Zürich, CH,** rosenthal@math.uzh.ch
2 **EPFL – Lausanne, CH,** amin.shokrollahi@epfl.ch
3 **University of Nebraska – Lincoln, US,** jwalker7@math.unl.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11461 "Coding Theory". A (channel) code is typically a set of vectors of the same length n over a finite alphabet Σ. By choosing a fixed codebook, binary strings of appropriate length are injectively mapped into the elements of the code. These elements are then transmitted over a communications channel which induces errors on the codeword. Depending on how well the original code is designed, and which algorithms are used, the result of this transmission and attempts to recover the original vector after transmission can be anywhere between disastrous to excellent. Coding theory is all about the design of excellent codes as a function of the communications channel, and the design of efficient algorithms for choosing the codebook vectors, and more importantly, for recovering the original vector after transmission. As such, successful design of codes requires knowledge and tools in a number of areas such as combinatorics, algorithms design, probability theory and complexity theory, to name a few. The purpose of this workshop is to bring together researchers in the field to discuss recent theoretical advances in algebraic coding, codes on graphs, and network coding, as well as new and emerging applications of coding methods to real-world problems.

Seminar 13.–18. November, 2011 – www.dagstuhl.de/11461
1998 ACM Subject Classification E.4 Coding and Information Theory, I.1.2 Algorithms.
Keywords and phrases Algebraic coding theory, complexity theory, cryptography, graph theory, graph based codes, information theory, randomized algorithms, networking, data distribution.
Digital Object Identifier 10.4230/DagRep.1.11.50
Edited in cooperation with Ghid Maatouk, Masoud Alipour

1 Executive Summary

Joachim Rosenthal
M. Amin Shokrollahi
Judy Walker

This workshop brought together 42 researchers in key areas of coding theory. The seminar had a strong emphasis on interaction and collaboration among researchers. This goal was made clear in a series of five-minute talks by all seminar participants, where they briefly described their research interests and/or described a problem that they were currently working on. The rest of the time was dedicated to more in-depth talks by a selected number of researchers, but the lecture time was kept reasonably short so that long stretches of time were available for seminar participants who wished to discuss further and collaborate in small groups.

Coding Theory, *Dagstuhl Reports*, Vol. 1, Issue 11, pp. 50–65
Editors: Joachim Rosenthal, M. Amin Shokrollahi, and Judy Walker
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The talks fell into several broad categories, the most prominent of which was algebraic coding theory. Algebraic coding theory primarily investigates codes obtained from algebraic constructions. Prime examples of this area of coding theory are codes from algebraic geometry and codes obtained from algebraically constructed expander graphs. This discipline is almost as old as coding theory itself, and has attracted (and continues to attract) some of the brightest minds in the field. Among the most exciting advances in this field in recent years has been the invention of list-decoding algorithms for various classes of algebraic codes; this area began with a landmark paper by Sudan that proposed an algebraic list-decoding scheme for Reed-Solomon codes. List decoding algorithms yield for a received word a short list of codewords that have at most a given distance τ to the received word. The size of the list depends on the distance τ. The methods in this field are mostly algebraic and make use of various properties of multivariate polynomials, or more generally, the properties of "well-behaved" functions in the function field of an irreducible variety. Methods from algebraic geometry are very important in this area. On the computational side the field naturally embeds in the theory of Gröbner bases. There are emerging relationships between this area and codes on graphs, the leading question being whether it is possible to match the superior performance of graph-based codes with list-decoding algorithms, or at least with algorithms that are derived from list-decoding algorithms.
Several talks covered recent advances and current research in some of the most notable questions that relate to algebraic constructions of codes, namely, list decoding; Berlekamp-Massey-like algorithms (for decoding, list-decoding, and Gröbner bases computation); elliptic curve methods and bent and hyperbent functions; rank-metric codes; bounds on codes (semidefinite programming bounds, BCH-like bounds); pivot distributions; properties of specific code constructions such as cyclic orbit codes, classes of self-dual codes, and codes obtained from generalized concatenation; and pseudocodewords, which straddle the boundary between algebraic analysis of codes and message-passing decoding of codes on graphs.

The second area that was covered in the workshop was that of codes on graphs. First proposed by Gallager in the 1950s, the subject of codes on graphs has experienced a huge revival over the past 10–15 years due to the fact that these codes have been shown to have capacity-achieving properties on some channels, and capacity-approaching properties on others. One of the most prominent examples in this area is that of the class of low density parity check (LDPC) codes, which are constructed from sparse bipartite graphs. The sparsity of the graph provides methods for construction of low complexity encoders and decoders. This area is a perfect nurturing ground for cross-fertilization of ideas between computer science, electrical engineering and mathematics. On the engineering side, the amazing simulation results have led some to declare the channel coding problem solved. The main proofs of asymptotic performance of these codes originated in the theoretical computer science community. Despite serious activities in this field many questions remain, related to the performance of graph-based codes and design of good LDPC codes. Several speakers discussed topics related to graph-based codes with applications beyond this field. The topics covered included design of sparse-graph codes for cooperation in communication networks; a new class of iterative decoders for LDPC codes; classes of tail-biting treillises; analysis of treillis pseudocodewords distributions; and bounds on the performance of quantum LDPC codes and their applications to percolations on graphs.

Network coding was another main area covered by the seminar. Network coding theory is concerned with the encoding and transmission of information where there may be many information sources and possibly many receivers. This is a very new area of coding theory and has been around only since 1999. The topic is somewhat far removed from the channel coding problem that Shannon proposed in 1948 and that the other areas of coding theory described in this proposal address. Indeed, there is not yet an agreed-upon formulation of the network coding problem. But there is a notion of linear network coding, and Li, Yeung and Cai showed in 2003 that it is possible to achieve so-called network capacity using linear codes alone. From that basis, much more algebra has been fruitfully introduced into the area. For example, in 2003, Kötter and Médard showed that the linear network codes that achieve a set throughput on a given network are precisely described by the points in a certain algebraic variety associated to the network. The Kötter-Médard approach, of course, relies on knowledge of the network in question. In practice, the network is typically unknown and often continually changing (dynamic). In 2008, Kötter and Kschischang considered random network coding and presented a framework in which the problem of network design is separated from that of code design. The idea is to assume that the network source simultaneously injects k linearly independent vectors from some vector space W into the network. These vectors are combined in various ways and sent through the network, so that the sink receives some linear combinations of them. The mathematical object that is invariant during transmission is the subspace of W spanned by the original k vectors, and so it is natural to consider a code in this context to be a subset of the set $\mathcal{P}(W)$ of all subspaces of W. Since $\mathcal{P}(W)$ is a metric space, the questions of code construction and optimality arise. Some approaches from classical coding theory can therefore be adopted in a fairly straight-forward manner, but deep questions remain, some of which were addressed by seminar speakers. One talk addressed the design and analysis of good end-to-end error-control codes in linear network coding; another topic was the analysis of several strategies for content distribution over network coded systems.

No workshop on such a practical topic as coding theory is complete without the mention of new and emerging applications. Indeed, several of the covered topics had a decidedly practical flavor, as some leading experts in applied coding theory, with an extensive mathematical background, reported about their work and provided insights into the directions the field will be taking in the coming years. Some of the most striking applications of coding-theoretical techniques to practical problems that were discussed included explicit constructions of regenerating codes for distributed storage; using network coding techniques to increase throughput in content distribution; and the design of iterative decoders for LDPC codes with better error floors than the traditional belief propagation decoders.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Coding for Relay Channels

Iryna Andriyanova (Université de Cergy-Pontoise/ENSEA/CNRS, FR)

We present two methods of designing efficient sparse-graph codes for cooperation. The first method is an extension of the design procedure for a point-to-point communication and uses good error-correcting codes (ex. LDPC) both at the source and at the relay ends. The second method takes the advantage of the multi-point transmission model and uses good error-detecting codes (ex. LDGM) along with a block-Markov encoding at the source end. We show that both of the design procedures have comparable performances asymptotically and may achieve the capacity of the relay channel.

3.2 List decoding and weighted reconstruction

Daniel Augot (École Polytechnique – Palaiseau)

In list decoding, a very important variant of list decoding of Reed-Solomon codes is the weighted polynomial reconstruction problem, as introduced by Guruswami and Sudan, which was later used for soft decoding of Reed-Solomon codes by Koetter and Vardy. In that context, a multiplicity matrix is built, which consists in interpolation constraints for finding the bivariate interpolation polynomial which is such that it admits linear factors corresponding to codewords. We investigate the simple case of a symmetric channel, where we also assume that the interpolation matrix is column symmetric. In that case, we identify the problem as the sum of simple list decoding problems. This can be described in an ideal-theoretical way, where the looked for ideal is the intersection of explicit ideals. We discuss how the linear factors of the simpler interpolation polynomials given by these ideals relate to the solution of the global interpolation problem, in an analogy with ideal-variety correspondence.

3.3 Semidefinite programming bounds for projective codes

Christine Bachoc (Université Bordeaux, FR)

Joint work of Bachoc, Christine; Passuello, Alberto; Vallentin, Frank

A projective code C is a subset of the set $P_q(n)$ of linear subspaces of $\mathbb{F}_q^n$. We consider on $P_q(n)$ the subspace distance defined by $d(U,V) = \dim(U)+\dim(V)-2\dim(U\cap V)$. Following [2], this distance is relevant in the framework of network coding. We consider in this context the classical coding theoretic problem of giving upper estimates for the maximal number $A_q(n,d)$ of elements of a projective code with given minimal distance d. If the classical bounds (anticode, singleton, Johnson, Delsarte, etc..) have been extended in an appropriate way to the case of subspaces of equal dimension, it appears that they cannot apply so easily to general projective codes. This is essentially due to the fact that the Grassmann space $G_q(n,k)$ is homogeneous under the action of the linear group $Gl(n,q)$ while the projective space is not. For general projective codes, only T. Etzion and A. Vardy [4] have provided an interesting bound. Their bound is expressed as the optimal value of a linear program and can be seen as an analog of the sphere packing bound.

In this talk, we present a bound for $A_q(n,d)$ which is the optimal value of a semidefinite program of size polynomial in n, obtained by the symmetrization of a general program, which itself can be viewed as the Lovász theta number of a certain graph [3]. This result is essentially a direct application of the method explained in [1] in a more general context. Numerical computations for $n \leq 13$ show that this bound is slightly better than the Etzion-Vardy bound.

References

1 C. Bachoc, D. Gijswijt, A. Schrijver and F. Vallentin, *Invariant semidefinite programs*, to appear in the Handbook on Semidefinite, Conic and Polynomial Optimization (M.F. Anjos, J.B. Lasserre (ed.)).

2 R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory, Volume 54, Issue 8, August 2008, pp. 3579–3591.

3 L. Lovász, *On the Shannon capacity of a graph*, IEEE Trans. Inform. Theory vol. 25 (1979), pp. 1–5.

4 T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Trans. Inform. Theory, vol. 57, no. 2, pp. 1165–1173, February 2011.

3.4 A Berlekamp-Massey like decoding algorithm

Martin Bossert (Universität Ulm)

An algorithm to determine the error locator polynomial for decoding Reed-Solomon codes is presented. The novel approach uses only properties of linear codes for the proof. The possible extension to the case of list decoding will be explained.

3.5 Trellises and Pseudocodewords

David Conti (University College – Dublin)

Joint work of Conti, David; Boston, Nigel

A central paradigm in modern coding theory is to represent codes by special graphs that allow for efficient iterative decoding algorithms. Amongst the most notable of such graphs are *trellises* ([7]). These are dynamical representation of codes that are important both for decoding purposes and for their rich theory which gives combinatorial insight into codes ([2, 6, 7]). Iterative decoding performance on a trellis is affected by *pseudocodewords*, in particular those with low *pseudoweight* ([4, 5]), while decoding complexity grows with trellis size ([7]). To make a trellis smaller one needs to merge vertices, but unfortunately this could create extra cycles yielding bad pseudocodewords. Thus it is important to study trellises along with their pseudocodewords.

In this talk we will first take a stroll through trellises and their pseudocodewords by discussing concretely the basics and some key questions. We will then show how an algebraic framework can be developed to help us studying trellis pseudocodewords distributions, bringing into the picture recurrence sequences, symmetric functions, and invariant theory ([3]). This can then be applied to give a first partial answer to a conjecture on the minimal 16 state trellis for the extended binary Golay code ([1, 2]).

References

1 N. Boston, *A multivariate weight enumerator for tail-biting trellis pseudocodewords*, to appear in Proceedings of "Workshop on Algebra, Combinatorics and Dynamics" Belfast, August 2009, Journal of Mathematical Sciences, Springer

2 A. R. Calderbank, G. D. Forney, Jr., A. Vardy, *Minimal tail-biting trellises: The Golay code and more*, IEEE Trans. Inform. Theory 45 (5) (1999) 1435–1455

3 D. Conti, N. Boston, *Matrix representations of trellises and enumerating trellis pseudocodewords*, Accepted to appear in Allerton 2011 proceedings

4 G. D. Forney Jr., R. Koetter, F. R. Kschischang, A. Reznik, *On the effective weights of pseudocodewords for codes defined on graphs with cycles*, in: Codes, Systems and Graphical Models, Springer, New York, 2001, 101–112

5 G. B. Horn, *Iterative decoding and pseudocodewords*, Ph.D. Thesis, California Institute of Technology, Pasadena, California, 1999

6 R. Koetter, A. Vardy, *The structure of tail-biting trellises: minimality and basic principles*, IEEE Trans. Inform. Theory 49 (9) (2003) 2081–2105

7 A. Vardy, *Trellis structure of codes*, in: Handbook of Coding Theory, Volume 2, Elsevier Science, 1998

3.6 Pivot distributions and Weierstrass nongaps

Iwan M. Duursma (University of Illinois – Urbana-Champaign)

We show how various properties of a linear code are captured by the collection of its dimension-length profiles. The dimension-length profile of a matrix describes the column positions of the pivots after the matrix is brought into row echelon form. The collection of dimension-length profiles describes the distribution of the pivots considered over all possible column permutations of the matrix. A code is MDS if and only if for every permutation of the columns in the generator matrix the pivot columns are the leading columns. The zeta function of a code that we introduced in previous work will be used to describe the deviation from this distribution when the code is not MDS. We will point out how the zeta function is the exact analogue of the zeta function for curves over a finite field and how for curves it describes the distribution of Weierstrass nongaps.

3.7 Classes of Tail-Biting Trellises

Heide Gluesing-Luerssen (University of Kentucky, US)

Joint work of Gluesing-Luerssen, Heide; Forney, G. David Jr.

Tail-biting trellises are – just like the ubiquitous Tanner graphs – instances of normal graphs for codes. More specifically, both form graphs with cycles. While the theory of cycle-free graphs is by now well understood with respect to minimal realization as well as decoding, many questions are still open for graphs with cycles. Yet, these graphs form an important class in coding theory and practice since it has long been known that realizations on graphs with cycles may allow for much more powerful iterative decoding algorithms than cycle-free graphs.

In this talk we will focus on tail-biting trellises: these are graphs in which the constraint codes form a single cycle. We will aim at identifying particularly useful tail-biting trellises. It is well-known that the complexity of decoding algorithms such as the sum-product algorithm depends on the size of the state spaces as well as constraint codes, and thus – not surprisingly – the construction and understanding of minimal trellises is paramount to the theory of tail-biting trellises. However, it turns out that all meaningful concepts of complexity measures for tail-biting trellises lead to different orderings, all of which are only partial, and thus to distinct notions of minimality. In particular, none of these notions leads to a unique minimal trellis realization (in the specified sense) for a given code.

As a consequence, the question of classifying good trellises becomes a crucial yet non-trivial step in the theory of tail-biting trellises. A major tool for identifying structural properties is the normal graph dualization introduced by Forney (2001). Indeed, it turns out that the dual graph may reveal trellis properties that are not immediately identifiable from the primal trellis. In this talk, we will show several such properties and relate them to more obvious properties of the dual trellis. Among other things, we will present system-theoretically meaningful notions of controllability and observability. As to be expected they are mutually dual. The process of investigating a trellis and its dual in parallel will also lead to a constructive reduction procedure for certain trellises.

3.8 A BCH-Bound for Ring-Linear Coding

Marcus Greferath (University College – Dublin, IE)

Joint work of Greferath, Marcus; Conti, David; Walker, Judy; Zumbrägel, Jens

Ring-Linear Coding started enjoying increased attention at the beginning of the last decade of the previous century, when it was discovered that certain non-linear binary block codes of high quality could be linearized by a change of alphabet. These new code versions were linear over a ring, rather than a field, and also the metric on this ring had to be different from the Hamming metric to fully reflect their error correction properties.

Since those days a lot of research has been devoted to ring-linear coding. On the structural side there was a great success settling the question which class of rings (or modules) is the most appropriate for ring-linear coding, and allows for possibly most foundational results of the traditional finite-field based theory.

On the constructional side we observe less success in providing families or sporadic examples of codes which outperform their finite-field siblings. This is in part due to the fact that up to now there have not been proved any assertive bounds like the BCH bound that allows to construct codes of a desired minimum distance.

The present talk's goal is to tackle this problem. We will show that a BCH bound can be shown for *any* finite ring R as long as we observe the expected restriction that the length n of the code in question is an invertible element in R. As a by-product we obtain a very nice new characterization of the class of all Frobenius rings. This is given as follows:

Theorem: For a finite ring R the following are equivalent.

(a) R is a Frobenius ring.

(b) There is a homomorphism $\chi : (R, +) \longrightarrow (\mathbb{C}^\times, \cdot)$, such that

$$\sum_{y\in I} \chi(y) \;=\; \begin{cases} 1 & : \quad I = \{0\}, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

(c) For every ring S there exists an extension T and a homomorphism $\chi : (R, +) \longrightarrow (T^\times \cap Z(T), \cdot)$ that satisfies the condition under **(b)**.

3.9 Linear-algebraic list decoding and subspace-evasive sets

Venkatesan Guruswami (Carnegie Mellon University – Pittsburgh)

Joint work of Guruswami, Venkatesan; Wang, Carol; Xing, Chaoping

This talk described a simple linear-algebraic approach that is surprisingly effective in list decoding variants of Reed-Solomon codes from an error fraction approaching the information-theoretically maximum limit of 1-R where R is the rate of the code.

The algorithm can be thought as a higher-dimensional version of the Welch-Berlekamp decoder. Similar to earlier algebraic list-decoders, the algorithm consists of two steps: multivariate polynomial interpolation (albeit with no need for "multiplicities") followed by a "root-finding" step to determine candidate close-by codewords. Both steps amount to solving (certain structured) linear systems and can be performed efficiently. Further, the candidate solutions are confined to a low-dimensional subspace. Pruning this subspace to find close-by codewords, though polynomial time, is the theoretically most expensive step of the algorithm. However, in practice one expects that the subspace will consist of a unique (or very few) candidate messages.

By pre-coding the messages to belong to a large "subspace-evasive set", i.e., a subset that has small intersection with every low-dimensional subspace, we can reduce the proven bound on list size (after pruning the candidate subspace) to a constant. Such subspace-evasive sets are interesting pseudorandom objects in their own right. I also stated state the outcome of recent generalizations of this approach to folded algebraic-geometric codes, leading to efficiently list-decodable codes with simultaneously near-optimal rate, list size, and alphabet size.

3.10 Bent functions and related topics

Tor Helleseth (University of Bergen, NO)

Joint work of Helleseth, Tor; Carlet, Claude; Kholosha, Alexander; Mesnager, Sihem

Bent functions are Boolean functions that have maximal distance to all affine functions. In the first part of the talk we gave an overview of classical constructions of bent functions as well as some recent constructions that relates the known families of Niho bent functions to o-polynomials and hyperovals in finite geometry. The corresponding o-polynomials of some of the Niho bent functions were found and the duals of some of these bent functions were given along with some open problems.

The last part of the talk presented an overview of recent results on generalized (nonbinary) bent functions.

3.11 Network Error-Control Coding

Frank R. Kschischang (University of Toronto)

Joint work of Kschischang, Frank R.; Silva, Danilo; Koetter, Ralf

The problem of error-control coding in linear network coding was reviewed. In the case of *coherent* network coding, in which the source-destination transfer matrix is known in advance, it was shown that optimal end-to-end error-control against adversarial errors can be achieved using rank-metric codes. In the case of *noncoherent* network coding, in which the source-destination transfer matrix is random and unknown to transmitter and receiver, it was shown that subspace codes, consisting of codebooks of vector-spaces well-separated according to an appropriate metric, are a good choice for end-to-end error-control against adversarial errors. Simple bounds on such codes were reviewed, and a *lifting* construction described, allowing for the construction of good subspace codes from rank-metric codes. Finally, a random (non-adversarial) noncoherent matrix channel was described. Capacity bounds were given, and a capacity-approaching transmission scheme involving *channel sounding* and *error-trapping* was described, for which the corresponding decoder is simply Gauss-Jordan elimination.

3.12 Interpolation, parametrization and iterative Grobner methods

Margreta Kuijper (The University of Melbourne, AU)

In this talk we consider minimal interpolation and advocate iterative algorithms that construct a minimal Grobner basis at each step. Already in 1995 Fitzpatrick introduced such an algorithm, resembling the Berlekamp-Massey algorithm. In the talk we explicitly use the "predictable leading monomial" property and consider parametric list decoding of Reed-Solomon codes as well as iterative shortest LFSR construction over finite rings.

3.13 Explicit Constructions of Regenerating Codes for Distributed Storage

P. Vijay Kumar (Indian Inst. of Science – Bangalore, IN)

Joint work of Kumar, P. Vijay; Shah, Nihar; Rashmi, K.V.; Ramachandran, K.

Regenerating codes are a class of distributed storage codes that optimally trade the bandwidth needed for repair of a failed node with the amount of data stored per node of the network. An [n; k; d] regenerating code permits the data to be recovered by connecting to any k of the n nodes in the network, while requiring that repair of a failed node be made possible by connecting to any d nodes. The amount of data downloaded for repair is typically much smaller as compared to the size of the source data. In this talk, we present explicit and optimal constructions of regenerating codes.

3.14 Polar codes as generalized concatenation

Simon Litsyn (Tel Aviv University, IL)

Polar construction of codes has attracted a plenty of attention recently since it provides a class of codes provably achieving capacity of symmetric memory-less channels and having low complexity of implementation.

In the talk we show that the original approach due to Arikan can be seen as recursively applied generalized concatenated construction with the inner codes having length 2. This suggests several natural extensions, e.g. using longer inner nested codes and mixed alphabet kernels. These modifications yield a significant improvement in performance of the considered codes.

3.15 Decoding cyclic orbit codes and the discrete logarithm problem

Felice Manganiello (University of Toronto, CA)

Cyclic orbit codes are a subfamily of orbit codes for linear random network codes. Finding a decoding algorithm for these family of codes is still an open problem. In this seminar we show the connection between decoding cyclic orbit codes and a problem called rank discrete logarithm problem. We also present a membership criterion for some particular cyclic orbit codes which is based on solving the rank discrete logarithm problem.

3.16 An efficient characterization of a family of hyperbent functions with multiple trace terms

Sihem Mesnager (Université de Paris VIII, FR)

Joint work of Mesnager, Sihem; Flori, Jean-Pierre

Lisonek recently reformulated the characterization of Charpin and Gong of a large class of hyperbent functions in terms of cardinalities of hyperelliptic curves.

In this paper, we show that such a reformulation can be naturally extended to a distinct family of functions proposed by Mesnager. Doing so, a polynomial time and space test is obtained to test the hyperbentness of functions in this family. Finally we show how this reformulation can be transformed to obtain a more efficient test.

3.17 Equivalence and Duality for Rank-Metric Codes

Katherine Morrison (University of Nebraska – Lincoln, US)

Rank-metric codes have garnered significant attention due to their applications in network coding, public-key cryptography, and data storage among other areas.

We focus on characterizing rank-metric codes that are both efficient, i.e. have high dimension, and effective at error correction, i.e. have high minimum distance. With an aim towards finding codes with a perfectly balanced trade-off, we study self-dual rank-metric codes. In particular, we seek to enumerate the equivalence classes of self-dual matrix codes of short lengths over small finite fields. Towards this end, we examine the notion of equivalence for rank-metric codes and use this to characterize the automorphism groups of a particular class of these codes known as Gabidulin codes.

3.18 Pseudocodewords from permanents

Roxana Smarandache (San Diego State University, US)

In this talk, we present some of the directions of research we were led to recently: computing or simplifying the computation of the permanent of 0-1 block matrices, studying if properties that are true for determinants hold also for permanents, defining the notion of quasipermanents for general square matrices over noncommutative rings, similar to the notion of quasideterminants, based on the reduction formulas obtained for the permanent of block matrices, and studying the properties of the "block-cofactor expansion inequality". These questions rise all from the need of information on the class of pseudocodewords with components defined by permanents.

3.19 Double Dixie Cup Unicast

Emina Soljanin (Bell Labs – Murray Hill, US)

Joint work of Soljanin, Emina; Li, Yao; Spasojevic, Predrag

In chunk based content distribution, files are fragmented at the source and the fragments (chunks) are distributed individually throughout the network. In network coded systems, instead of distributing the original file chunks, nodes send out linear combinations of the chunks they hold. This strategy brings about an overall throughput increase. For a number of practical concerns (e.g, computational complexity and synchronization), chunks are grouped into (possibly overlapping) blocks known as generations. Only chunks within the same generation are allowed to be linearly combined. A price to pay for coding only within generations is throughput reduction.

For the purpose of gaining insight into differences among these three distribution strategies, we model them as random allocation protocols, such as the classical coupon collecting and the less known double Dixie cup collecting. Since chunks represent coded information rather than indivisible coupons, we modify these allocation models accordingly. We characterize the throughput behavior in terms of the generation size, and develop strategies to improve the throughput while maintaining the benefits of coding within generations.

3.20 Finite alphabet iterative decoders

Bane Vasic (University of Arizona – Tucson, US)

We introduce a new class of finite alphabet iterative decoders for LDPC codes, and show how to choose nonlinear message update maps for column-weight-three codes so that the decoders with only seven message levels surpass belief propagation (BP) in the error floor region.

3.21 Singly-even self-dual codes with minimal shadow

Wolfgang Willems (Universität Magdeburg, DE)

Joint work of Willems, Wolfgang; Bouyuklieva, S.

There are several reasons why extremal singly-even self-dual codes are of interest. For instance, they provide connections to designs, are proposed for use in secret sharing schemes, and for length 24m+8 they perform better than doubly-even self-dual codes of the same length if the shadow is minimal. In the talk we investigate such codes with minimal shadow. For particular parameters we prove non-existence theorems and state explicit bounds whose existence was proved by Rains.

3.22 Percolation and Quantum Erasure Correction

Gilles Zémor (Université Bordeaux, FR)

Joint work of Zémor, Gilles; Delfosse, Nicolas

We show that percolation on graphs, in particular on trees, is closely related to the probability of successful decoding on the erasure channel for the class of cycle codes on graphs. We investigate what information-theoretic bounds on LDPC codes contribute to the determination of critical probabilities for percolation. Transposed to the quantum setting, we find that the same reasoning applies when cycle codes of graphs are replaced by surface codes, quantum codes built on 2-dimensional complexes. We derive new information-theoretic upper bounds on the probability of successful decoding for quantum LDPC (sparse) codes on the quantum erasure channel, and apply these bounds to obtain upper bounds on critical probabilities for percolation on tilings of the hyperbolic plane.

3.23 On the Pseudocodeword Redundancy of Binary Linear Codes

Jens Zumbrägel (University College – Dublin, IE)

Joint work of Zumbrägel, Jens; Boston, Nigel; Flanagan, Mark F.; Skachek, Vitaly

The AWGNC, BSC, and max-fractional pseudocodeword redundancies of a binary linear code are defined to be the smallest number of rows in a parity-check matrix such that the corresponding minimum pseudoweight is equal to the minimum Hamming distance of the code. We show that most codes do not have a finite pseudocodeword redundancy. Also, we provide upper bounds on the pseudocodeword redundancy for some families of codes with t-transitive automorphism group, and we report on our progress of proving bounds for the extended Golay code.

Participants

- Masoud Alipour
EPFL – Lausanne, CH
- Iryna Andriyanova
Univ. de Cergy-Pontoise/ ENSEA/CNRS, FR
- Daniel Augot
Ecole Polytechnique – Palaiseau, FR
- Christine Bachoc
Université Bordeaux, FR
- Martin Bossert
Universität Ulm, DE
- Joan Josep Climent
Universitat d'Alacant, ES
- Gerard Cohen
ENST – Paris, FR
- David Conti
University College – Dublin, IE
- Iwan M. Duursma
Univ. of Illinois – Urbana, US
- Michele Elia
Politecnico di Torino, IT
- Heide Gluesing-Luerssen
University of Kentucky, US
- Elisa Gorla
Universität Basel, CH
- Marcus Greferath
University College – Dublin, IE
- Venkatesan Guruswami
Carnegie Mellon University – Pittsburgh, US
- Kathryn Haymaker
Univ. of Nebraska – Lincoln, US
- Tor Helleseth
University of Bergen, NO
- Tom Hoholdt
Technical University of Denmark – Lyngby, DK
- Christine A. Kelley
Univ. of Nebraska – Lincoln, US
- Axel Kohnert
Universität Bayreuth, DE
- Frank R. Kschischang
University of Toronto, CA
- Margreta Kuijper
The University of Melbourne, AU
- P. Vijay Kumar
Indian Inst. of Science – Bangalore, IN
- Francoise Levy-dit-Vehel
ENSTA – Paris, FR
- Yao Li
Rutgers University – New Brunswick, US
- Simon Litsyn
Tel Aviv University, IL
- Hans-Andrea Loeliger
ETH Zentrum – Zürich, CH
- Ghid Maatouk
EPFL – Lausanne, CH
- Felice Manganiello
University of Toronto, CA
- Sihem Mesnager
Université de Paris VIII, FR
- Katherine Morrison
Univ. of Nebraska – Lincoln, US
- Joachim Rosenthal
Universität Zürich, CH
- Davide Schipani
Universität Zürich, CH
- M. Amin Shokrollahi
EPFL – Lausanne, CH
- Roxana Smarandache
San Diego State University, US
- Emina Soljanin
Bell Labs – Murray Hill, US
- Anna-Lena Trautmann
Universität Zürich, CH
- Bane Vasic
Univ. of Arizona – Tucson, US
- Judy L. Walker
Univ. of Nebraska – Lincoln, US
- Alfred Wassermann
Universität Bayreuth, DE
- Wolfgang Willems
Universität Magdeburg, DE
- Gilles Zémor
Université Bordeaux, FR
- Jens Zumbrägel
University College – Dublin, IE