

Coding Theory

Edited by

Hans-Andrea Loeliger¹, Emina Soljanin², and Judy Walker³

1 ETH Zürich, CH, loeliger@isi.ee.ethz.ch

2 Bell Labs, Alcatel-Lucent, Murray Hill, US, emina@research.bell-labs.com

3 University of Nebraska, Lincoln, US, judy.walker@unl.edu

Abstract

Coding theory has become an essential ingredient of contemporary information technology, and it remains a fascinating area of research. The seminar brought together 45 high-caliber researchers with backgrounds and interests in various different parts of coding theory. The new area of codes for cloud applications received much attention, but other key areas such as network codes, codes on graphs, algebraic coding, and polar codes, were also well represented and generated lively discussions.

Seminar 25.–30. August, 2013 – www.dagstuhl.de/13351

1998 ACM Subject Classification E.4 Coding and Information Theory, I.1.2 Algorithms

Keywords and phrases Coding theory, codes on graphs, polar codes, network coding, index coding, data distribution, cloud storage.


Digital Object Identifier 10.4230/DagRep.3.8.136

1 Executive Summary

Hans-Andrea Loeliger

Emina Soljanin

Judy Walker

License  Creative Commons BY 3.0 Unported license
© Hans-Andrea Loeliger, Emina Soljanin, and Judy Walker

While coding theory has evolved into an essential ingredient of contemporary information technology, it remains a fascinating area of research where many fundamental ideas of information theory and mathematics meet. Indeed, the diversity and profundity of recent new ideas in, and new applications of, coding theory is impressive. The following themes were of primary interest at the seminar:

Codes on graphs include turbo codes, low-density parity check codes, and a variety of similar codes. Due to the recent new idea of “spatial coupling”, such codes can now be designed to achieve the Shannon capacity of most communication channels with practical encoders and decoders. Such codes are a perfect nurturing ground for cross-fertilization of ideas between computer science, electrical engineering, and mathematics. The mathematical tools in this area include ideas from graph theory, probability, algebra, discrete mathematics, and statistical physics.

Algebraic coding theory continues to be of supreme theoretical and practical interest. Prime examples of this area are Reed-Solomon codes, codes from algebraic geometry, and codes obtained from algebraically constructed graphs. Recent advances in the field include, in particular, list-decoding algorithms for various classes of algebraic codes. Emerging



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Coding Theory, *Dagstuhl Reports*, Vol. 3, Issue 8, pp. 136–150

Editors: Hans-Andrea Loeliger, Emina Soljanin, and Judy Walker



DAGSTUHL
REPORTS

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

relationships between this area and codes on graphs appear to be promising for future research.

Polar codes (discovered by Arikan in 2008) are a breakthrough of utmost significance. Such codes are provably capacity-achieving on very many channels with very low-complexity (and very practical) encoders and decoders. These codes rely on a new large-system limit that combines information theory and coding theory more smoothly than any prior coding technique. The investigation of such codes, including their combination with other coding techniques (such as codes on graphs and algebraic codes), is an exciting new area of research.

Network coding aims at improving data transmission (throughput, reliability, latency, etc.) in networks. This area is still quite young, but it has begun to influence the design of methods and protocols of content delivery in the internet. There is a diverse set of network coding problem formulations, and network coding can be (and has been) studied within a number of different theoretical frameworks, such as algebraic, combinatorial, information theoretic, and linear programming frameworks.

Codes for cloud applications are about distributed storage of large amounts of data. Diverse requirements on reliability, access latency, updatability, and repairability pose entirely new challenges for coding theory.

In addition, there were also two talks on topics in coding theory inspired by biology.

The seminar brought together 45 high-caliber researchers with backgrounds and interests in these different areas. The seminar was held in the usual Dagstuhl style, with a rather light program of formal presentations and much room for informal interaction. It was interesting and stimulating to hear of developments outside one's own speciality, and (to the best of our knowledge) all attendants greatly enjoyed the seminar.

2 Table of Contents

Executive Summary

Hans-Andrea Loeliger, Emina Soljanin, and Judy Walker 136

Overview of Talks


Gabidulin Codes in Characteristic Zero <i>Daniel Augot</i>	140
Some Problems of Coding Theory Motivated by Coding for Memories <i>Alexander Barg</i>	140
Efficient Projection onto the Parity Polytope and its Application to LP Decoding <i>Stark C. Draper</i>	141
Binary Multiplicative Codes <i>Iwan M. Duursma</i>	141
Codes for Secure Distributed Data Storage <i>Salim El Rouayheb</i>	141
Semantic Value of Information: Coding and Decoding Schemes Tailor Made for Image Transmission <i>Marcelo Firer</i>	142
On the MacWilliams Extension Theorem for Poset Codes <i>Heide Gluesing-Luerssen</i>	142
Partial Spread Codes <i>Elisa Gorla</i>	142
A Characterization of All Invariant Weight Functions on a Principal Ideal Ring With the Property That All Code Isometries Allow For Monomial Extension <i>Marcus Greferath</i>	143
Polar Codes: Finite-Length Scaling and Universality <i>Hamed S. Hassani</i>	143
On the Second Largest Eigenvalue of an n-regular Graph <i>Tom Høholdt</i>	143
Graph Codes on Projective and Euclidean Planes <i>Jørn Justesen</i>	144
On the Interior Points of the Storage-Bandwidth Tradeoff <i>P. Vijay Kumar</i>	144
Some Recent Topics in Coding for Secrecy <i>Muriel Medard</i>	144
Linear Codes From Oval Polynomials <i>Sihem Mesnager</i>	145
Gene Prioritization and Rank Aggregation <i>Olgica Milenkovic</i>	145
Neuroscience-inspired Network Decoder <i>Katherine Morrison</i>	146

On the Skew Complexity of Sequences with Applications to Algebraic Decoding <i>Vladimir Sidorenko</i>	146
Optimal Index Codes with Near-extreme Rates <i>Vitaly Skachek</i>	146
On Multiply Constant Weight Codes <i>Patrick Sole</i>	147
Index Coding: Fundamentals, Applications, and Recent Progress <i>Alex Sprintson</i>	147
List Decoding of Subspace Codes <i>Anna-Lena Trautmann</i>	147
Trapping Set Structure of Minimum Weight Codewords in Regular LDPC Codes <i>Bane Vasic</i>	148
Coding for Combined Block-symbol Error Correction <i>Pascal Vontobel</i>	148
On Network Codes and Partial Spreads <i>Wolfgang Willems</i>	149
Participants	150

3 Overview of Talks

3.1 Gabidulin Codes in Characteristic Zero

Daniel Augot (Ecole Polytechnique – Palaiseau & INRIA, FR)

License  Creative Commons BY 3.0 Unported license
© Daniel Augot

Joint work of Augot, Daniel; Loidreau, Pierre; Robert, Gwezheneg

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.

3.2 Some Problems of Coding Theory Motivated by Coding for Memories

Alexander Barg (University of Maryland – College Park, US)

License  Creative Commons BY 3.0 Unported license
© Alexander Barg


Joint work of Barg, Alexander; Mazumdar, Arya; Kashyap, Navin; Zemor, Gilles

We consider several coding problems motivated by writing onto memories. The first part of the talk is devoted to coding in the space of permutations with the Kendall tau metric. We discuss distance-preserving embeddings of the Kendall space and their relation to bounds on the size of optimal codes. A tight asymptotic bound on codes is derived. We also present a construction of codes in permutations that asymptotically meet this bound. The construction relies on codes in the conventional Hamming space and can be decoded based on their decoding algorithms.

In the second part we discuss a noise model motivating by writing on the granular magnetic medium. We discuss several bounds on codes as well as on the capacity of the probabilistic model of the “grains” channel. Finally, we introduce a problem in binary coding that deals with errors that do not affect adjacent bits (this is a simplified version of the previous problem, but it is nontrivial in its own right). We point out that correcting nonadjacent errors is combinatorially equivalent to correcting conventional errors, but at the same time that there are several scenarios in which this restriction helps to construct better codes than in the standard case of Hamming errors.

3.3 Efficient Projection onto the Parity Polytope and its Application to LP Decoding

Stark C. Draper (University of Toronto, CA)

License  Creative Commons BY 3.0 Unported license
© Stark C. Draper


Joint work of Draper, Stark C.; Barman, Siddarth; Liu, Xishuo; Recht, Benjamin

When binary linear error-correcting codes are used over symmetric channels, a relaxed version of the maximum likelihood decoding problem can be stated as a linear program (LP). This LP decoder can be used to decode at bit-error-rates comparable to state-of-the-art belief propagation (BP) decoders, but with significantly stronger theoretical guarantees. However, LP decoding when implemented with standard LP solvers does not easily scale to the block lengths of modern error correcting codes.

In this talk we draw on decomposition methods from optimization theory, specifically the Alternating Direction Method of Multipliers (ADMM), to develop efficient distributed algorithms for LP decoding. The key enabling technical result is a nearly linear time algorithm for two-norm projection onto the “parity polytope”. The parity polytope is formed by taking the convex hull of all codewords of the single parity-check code. Efficient solution of this projection allows us to use LP decoding, with all its theoretical guarantees, to decode large-scale error correcting codes efficiently. We discuss performance results for a number of long LDPC codes, presenting results on error rates and computational complexity. In comparison to BP decoding we observe that the waterfall of the LP decoder initiates at a higher SNR. In conclusion we present a small modification of the LP decoder wherein by slightly penalizing the linear objective of the LP we close the SNR gap between BP and LP.

3.4 Binary Multiplicative Codes

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

License  Creative Commons BY 3.0 Unported license
© Iwan M. Duursma

We describe how binary linear codes with an extra multiplicative structure (to be used for algebraic decoding, secret reconstruction, secure or fast multiplication, etc) are either a Reed-Muller code or the concatenation of an additive subcode over a larger field with a Reed-Muller inner code.

3.5 Codes for Secure Distributed Data Storage

Salim El Rouayheb (Illinois Institute of Technology, US)

License  Creative Commons BY 3.0 Unported license
© Salim El Rouayheb

Distributed storage systems are now a growing paradigm for providing online storage of data and making it accessible anywhere and anytime. In this talk, I will address the problem of achieving information theoretic security of data in these systems to protect it against eavesdropping and malicious attacks. These systems are dynamic due to storage nodes frequently leaving or joining the system. This creates the challenge of safeguarding

the system from an adversary which may come at different time instances to observe and maliciously corrupt the stored data. I will give bounds on the secure capacity, i.e., the maximum amount of information that can be stored safely on the system, and describe secure code constructions that can achieve these bounds in certain cases. An important part of the talk will be dedicated to discussing the numerous problems that remain open in this area.

3.6 Semantic Value of Information: Coding and Decoding Schemes Tailor Made for Image Transmission

Marcelo Firer (State University of Campinas – Brazil, BR)


License  Creative Commons BY 3.0 Unported license
© Marcelo Firer

Joint work of Firer, Marcelo; Panek, Luciano; Ramos Rifo, Laura L.; Pinheiro, Jerry A.

We explore possibilities for coding and decoding considering semantic value for errors, in particular schemes that are tailor made for image transmission. To do so, we introduce a loss function that expresses the overall performance of a coding scheme for discrete channels and exchange the usual goal of minimizing the error probability to that of minimizing the expected loss. In this environment we explore the possibilities of using poset-decoders to make a message-wise unequal error protection (UEP), where using a lexicographic order for encoding. We give explicit examples, done for scale-of-gray images, including visual simulations for the BSMC, exploring the encoding and the decoding possibilities.

3.7 On the MacWilliams Extension Theorem for Poset Codes

Heide Gluesing-Luerssen (University of Kentucky, US)

License  Creative Commons BY 3.0 Unported license
© Heide Gluesing-Luerssen

A weight function on R^n , where R is a finite ring, is said to satisfy the MacWilliams extension property if every weight isometry between codes in R^n extends to an isometry on R^n . After discussing various classes of poset weights we state the main result. It says that a poset weight satisfies the extension property if and only if the poset is hierarchical.

3.8 Partial Spread Codes

Elisa Gorla (Université de Neuchâtel, CH)

License  Creative Commons BY 3.0 Unported license
© Elisa Gorla

Joint work of Gorla, Elisa; Ravagnani, A.

As in the approach by Koetter and Kschischang, we study subspace codes as families of k -dimensional linear spaces over a finite field. Following an idea in finite projective geometry, we introduce a class of constant dimension 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.

3.9 A Characterization of All Invariant Weight Functions on a Principal Ideal Ring With the Property That All Code Isometries Allow For Monomial Extension

Marcus Greferath (*University College Dublin, IE*)

License © Creative Commons BY 3.0 Unported license
© Marcus Greferath

Joint work of Greferath, Marcus; Honold, Thomas; Mc Fadden, Cathy; Wood, Jay A.; Zumbärgel, Jens

It has been apparent since the end of the foregoing century that finite Frobenius rings (and modules) are the adequate alphabets for ring-linear algebraic coding theory. For these, it was proven early that Hamming isometries and homogeneous isometries allow for MacWilliams' Extension Theorem, which means that linear code isometries that preserve the Hamming and/or homogeneous weight can be monomially extended to the ambient spaces of the codes in question. The talk at hand starts with a question of similar importance: For which subclass of the class of all finite Frobenius rings can we characterize all weight functions that allow for monomial extension of code isometries. Recent years' work has revealed that this question is anything but trivial, however it turned out that we can answer it at least for the class of all finite principal ideal rings.

The talk is dedicated to the memory of Werner Heise, who discovered the homogeneous weight and thereby vastly influenced foundational work in ring-linear coding theory. He died in February 2013.

3.10 Polar Codes: Finite-Length Scaling and Universality

Hamed S. Hassani (*EPFL – Lausanne, CH*)

License © Creative Commons BY 3.0 Unported license
© Hamed S. Hassani

Joint work of Hassani, Hamed S.; Urbanke, Rüdiger

Polar codes achieve the capacity of a wide array of channels under successive decoding. Since the invention of polar codes by Arikan a large body of work has been done to investigate the pros and cons of polar codes in different scenarios. We consider two features of these codes that are central from the practical perspective: finite-length scaling and universality. In this talk, after a brief description of polar codes, we will explain each of these features together with some of the related recent results and open questions.

3.11 On the Second Largest Eigenvalue of an n -regular Graph

Tom Høholdt (*Technical University of Denmark, DK*)


License © Creative Commons BY 3.0 Unported license
© Tom Høholdt

Joint work of Høholdt, Tom; Justesen, Jørn

We give new lower bounds on the second largest eigenvalue of an n -regular connected bipartite graph. This eigenvalue is important for the minimum distance of the graph codes constructed from the graph as well as for the expansion properties of the graph. The proofs involves the quotient matrix and the eigenvalue interlacing theorem. By similar methods we obtain new bounds on the minimum distance of graph codes, in particular in the cases where the previous bounds are useless.

3.12 Graph Codes on Projective and Euclidean Planes

Jørn Justesen (Technical University of Denmark, DK)

License  Creative Commons BY 3.0 Unported license
© Jørn Justesen

Joint work of Justesen, Jørn; Høholdt, Tom

We study codes constructed from Reed-Solomon codes and bipartite graphs coming from projective and Euclidean planes. The code symbols are associated with the edges and the symbols connected to a given vertex are restricted to be codewords in the component Reed-Solomon code. We give exact formulas for the rates and minimum distances of the codes and discuss systematic encoding.

3.13 On the Interior Points of the Storage-Bandwidth Tradeoff

P. Vijay Kumar (IISc – Bangalore, IN)

License  Creative Commons BY 3.0 Unported license
© P. Vijay Kumar

It was shown by Dimakis et al. that in an erasure code designed for distributed storage, there is a tradeoff between amount of data storage and bandwidth for repair of a failed node. While this tradeoff is known to be achievable under functional repair, the same does not hold for exact repair. A recent result by Tian established that there exist code parameters under which exact repair is not achievable even in the limit of large block lengths. In this talk, we will review these developments. We will also provide a normalized tradeoff that explains why code constructions for the interior points are of interest and identify a construction that achieves a single interior point. It also improves upon space-sharing in the interior region.

3.14 Some Recent Topics in Coding for Secrecy

Muriel Medard (MIT, US)

License  Creative Commons BY 3.0 Unported license
© Muriel Medard

In the first part of this talk, we present two examples of recent applications of algebraic codes to secrecy. These codes allow us, under the commonly held assumption of source uniformity, to establish strong information-theoretic guarantees. When encryption is limited to coding coefficients of random linear codes, we show information-theoretic secrecy results for such a construction. In particular, we show that the encoded payload and the encrypted coefficients do not yield information about each other. In our second example, we interpret keys as representing the size of the list over which an adversary would need to generate guesses in order to recover the plaintext, leading to a natural connection between list decoding and secrecy. Under such a model, we show MDS codes can be constructed so that lists satisfy certain secrecy criteria, which we define to generalize common perfect secrecy and weak secrecy notions. In the final part of the talk, we revisit the source uniformity assumption that subtends our analysis, as well as much of information-theoretic treatment of secrecy. In particular, we show that, the common treatment of the elements of the typical set as being essentially uniformly distributed fails when one consider guesswork over the typical set. Such results encourage us to revisit uniformity assumptions in secrecy.

3.15 Linear Codes From Oval Polynomials

Sihem Mesnager (University of Paris VIII, FR)

License © Creative Commons BY 3.0 Unported license
© Sihem Mesnager

The main topics and interconnections arising in this talk are symmetric cryptography (S-boxes), coding theory (linear codes) and finite projective geometry (hyperovals). Bent vectorial functions are maximally nonlinear multi-output Boolean functions. Such functions contribute to an optimal resistance to both linear and differential attacks of those symmetric cryptosystems in which they are involved as substitution boxes (S-boxes). In this talk, we firstly show that the o-polynomials from finite projective geometry give rise to several new classes of optimal vectorial bent functions whose components belong to a certain Reed-Muller code. Secondly, we present a general construction of classes of linear codes from o-polynomials and study their weight distribution proving that all of them are minimal weight codes. The second contribution shows that some hyperovals of the projective plane from finite projective geometry provide the construction of new minimal codes (used in particular in secret sharing schemes, to model the access structures) and give rise to multiple of s -ary (where s is the power of 2 to the r and r being a divisor of m) simplex linear codes (whose the dual are the perfect s -ary Hamming codes) over an extension field.

3.16 Gene Prioritization and Rank Aggregation

Olgica Milenkovic (University of Illinois – Urbana Champaign, US)

License © Creative Commons BY 3.0 Unported license
© Olgica Milenkovic

Joint work of Milenkovic, Olgica; Farnoud, Farzad; Kim, Minji; Raisali, Fardad

We consider the problem of ranking genes according to their likelihood of being implicated in the onset and progression of a disease. Rankings of this form are known as gene prioritizations, and they are used to govern experimental knockout tests. Many software tools exist for prioritizing genes using similarity criteria with respect to genes already known to be involved in the disease, termed disease training genes. Similarity criteria may be as varied as sequence similarity, transcription factor binding sites, expression, and annotation. All individual rankings in one-to-one correspondence with the similarity criteria are aggregated via order statistics methods, which rely on multiple null hypothesis that are hard to test or even potentially accurate.

We propose analyzing the problem via a new combinatorial and information-theoretic approach, based on distance based aggregations. The distances used represent novel extensions of the Kendall distance, used to measure swap distance between two permutations, and the Bregman-Lovasz distance, used to measure distances between rankings and ratings. We also describe integer programming relaxations for the aggregation problems with positional relevance constraints. The distance-based methods outperform order statistics methods in almost all performed tests.

3.17 Neuroscience-inspired Network Decoder

Katherine Morrison (University of Northern Colorado, US)

License © Creative Commons BY 3.0 Unported license
© Katherine Morrison

Joint work of Morrison, Katherine; Curto, Carina

When the brain encounters the same stimulus presented multiple times, different initial neural responses will typically be observed, and yet the brain is still able to determine what stimulus it has encountered. Thus, the brain must be performing some form of error correction. We present a biologically plausible mechanism by which this error correction may be performed. In particular, we show that this decoding algorithm can perform pattern completion, which was previously believed impossible with network models of this form.

3.18 On the Skew Complexity of Sequences with Applications to Algebraic Decoding

Vladimir Sidorenko (Universität Ulm, DE)

License © Creative Commons BY 3.0 Unported license
© Vladimir Sidorenko

Joint work of Sidorenko, Vladimir; Schmidt, Georg; Wachter, Antonia; Bossert, Martin; Li, Wenhui

Linear complexity of a sequence over a field can be efficiently computed using the Berlekamp-Massey algorithm. It will be shown how linear complexity of multiple sequences, which can be described using the language of polynomials over a field, can be generalized to skew complexity for the case of skew (or linearized or twisted) polynomials. We show how the skew complexity can be applied for an efficient algebraic decoding of interleaved Reed-Solomon codes and interleaved Gabidulin codes.

3.19 Optimal Index Codes with Near-extreme Rates

Vitaly Skachek (University of Tartu, EE)

License © Creative Commons BY 3.0 Unported license
© Vitaly Skachek

The min-rank of a digraph was shown by Bar-Yossef et al. to represent the length of an optimal scalar linear solution of the corresponding instance of the Index Coding with Side Information (ICSI) problem. In this work, the graphs and digraphs of near-extreme min-ranks are studied. Those graphs and digraphs correspond to the ICSI instances having near-extreme transmission rates when using optimal scalar linear index codes. In particular, it is shown that the decision problem whether a digraph has min-rank two is NP-complete. By contrast, the same question for graphs can be answered in polynomial time.

3.20 On Multiply Constant Weight Codes

Patrick Sole (Télécom Paris Tech, FR)

License © Creative Commons BY 3.0 Unported license
© Patrick Sole

Joint work of Sole, Patrick; Chee, Yeow Meng; Cherif, Zouha; Danger, Jean-Luc; Guilley, Sylvain; Kiah, Han Mao; Kim, Jon-Lark; Zhang, Xiande

Motivated by the security of embarked system a generalization of constant weight codes is introduced and studied. Construction based on parallelism of designs, concatenation of codes, and pseudo-product codes are derived. The asymptotic performance problem is solved completely.

3.21 Index Coding: Fundamentals, Applications, and Recent Progress

Alex Sprintson (Texas A&M University – College Station, US)

License © Creative Commons BY 3.0 Unported license
© Alex Sprintson

Index Coding is one of the central problems in wireless network coding. It has deep connections to many fundamental problems, such as coloring, determining network coding capacity, and interference alignment. This area has been the subject of intensive research and many new insights have been gained over recent years. In this talk, we will survey the fundamentals of index coding, including algorithms for code design, the complexity of such algorithms, and lower and upper bounds on the capacity region of index coding instances. We will also discuss the equivalence between index coding and interference alignment and network coding, as well as the implications of this equivalence. We will also discuss open problems and directions for future research.

3.22 List Decoding of Subspace Codes

Anna-Lena Trautmann (Universität Zürich, CH)

License © Creative Commons BY 3.0 Unported license
© Anna-Lena Trautmann

Joint work of Trautmann, Anna-Lena; Rosenthal, Joachim; Silberstein, Natalia

The finite Grassmannian $\mathcal{G}_q(k, n)$ is defined as the set of all k -dimensional subspaces of the ambient space \mathcal{F}_q^n . Subsets of the finite Grassmannian are called constant dimension codes and have recently found an application in random network coding. In this setting codewords from $\mathcal{G}_q(k, n)$ are sent through a network channel and, since errors may occur during transmission, the received words can possibly lie in $\mathcal{G}_q(k', n)$, where $k' \neq k$.

In this talk, we study the balls in $\mathcal{G}_q(k, n)$ with center that is in $\mathcal{G}_q(k, n)$, for simplicity. We describe the balls with respect to the subspace metric. Moreover, we use two different techniques for describing these balls, one is the Plücker embedding of $\mathcal{G}_q(k, n)$, and the second one is a rank decomposition of the matrix representation of the codewords.

With these results, we consider the problem of list decoding a certain family of constant dimension codes, called lifted Gabidulin codes. We describe a way of representing these codes by linear equations in either the matrix representation or a subset of the Plücker coordinates.

The union of these equations and the equations which arise from the description of the ball of a given radius in the Grassmannian describe the list of codewords with distance less than or equal to the given radius from the received word.

3.23 Trapping Set Structure of Minimum Weight Codewords in Regular LDPC Codes

Bane Vasic (University of Arizona – Tucson, US)

License © Creative Commons BY 3.0 Unported license
© Bane Vasic

Joint work of Vasic, Bane; Khatami, Seyed Mehrdad; Danjen, Ludovic; Nguyen, Dung V.

We present an efficient algorithm for finding all low-weight codewords in a given quasi-cyclic (QC) low-density parity-check (LDPC) code with a fixed column-weight and girth. A low-weight codeword is viewed as an $(a; 0)$ trapping set, and topologically different $(a; 0)$ trapping set are obtained from smaller trapping sets. The method can be used to construct QC codes with given minimum distance and to determine the multiplicity of the low-weight codewords with different trapping set structure.

3.24 Coding for Combined Block-symbol Error Correction

Pascal Vontobel (HP Labs – Paolo Alto, US)

License © Creative Commons BY 3.0 Unported license
© Pascal Vontobel

Joint work of Vontobel, Pascal; Roth, Ron M

Main reference R. M. Roth, P. O. Vontobel, “Coding for Combined Block-Symbol Error Correction,” arXiv:1302.1931v1 [cs.IT], 2013.

URL <http://arxiv.org/abs/1302.1931v1>

Many data transmission and storage systems suffer from different types of errors at the same time. For example, in some data storage systems the state of a memory cell might be altered by an alpha particle that hits this memory cell. On the other hand, an entire block of memory cells might become unreliable because of hardware wear-out.

Such data transmission and storage systems can be modeled by channels that introduce symbol errors and block (i.e., phased burst) errors, where block errors encompass several contiguous symbols. Moreover, if some side information is available, say based on previously observed erroneous behavior of a single or of multiple memory cells, this can be modeled as symbol erasures and block erasures.

We present novel error correction coding schemes that can deal with certain setups that include both symbol and block errors and both symbol and block erasures. At the end of the talk, we will pose some open problem w.r.t. the existence of efficient decoders for certain scenarios.

3.25 On Network Codes and Partial Spreads

Wolfgang Willems (*Universität Magdeburg, DE*)

License  Creative Commons BY 3.0 Unported license
 Wolfgang Willems

Let $\mathcal{G}_q(n, \ell)$ denote the Grassmannian (subspaces of dimension ℓ of an n -dimensional vector space over F_q). We discuss bounds of the function

$$A_q(n, d, \ell) = \max\{|C| : C \subset \mathcal{G}_q(n, \ell), d(C) \geq d\}$$

where the distance is the subspace distance. We mainly focus on the case $d = 2\ell$, i.e., on the maximal size of a “partial ℓ -spread” in an n -dimensional space. Moreover, we answer a question posed by Bu in the seventieth and improve an upper bound of Etzion and Vardy.

Participants

- Daniel Augot
Ecole Polytechnique – Palaiseau
& INRIA, FR
- Angela Barbero
University of Valladolid, ES
- Alexander Barg
University of Maryland – College
Park, US
- Eimear Byrne
University College Dublin, IE
- Pascale Charpin
INRIA, FR
- Gerard Cohen
ENST – Paris, FR
- Stark C. Draper
University of Toronto, CA
- Iwan M. Duursma
University of Illinois – Urbana
Champaign, US
- Salim El Rouayheb
Illinois Inst. of Technology, US
- Marcelo Firer
State University of Campinas –
Brazil, BR
- Heide Gluesing-Luerssen
University of Kentucky, US
- Elisa Gorla
Université de Neuchâtel, CH
- Marcus Greferath
University College Dublin, IE
- Hamed S. Hassani
EPFL – Lausanne, CH
- Michael Heindlmaier
TU München, DE
- Tor Helleseth
University of Bergen, NO
- Werner Henkel
Jacobs University – Bremen, DE
- Tracey Ho
CalTech – Pasadena, US
- Tom Høholdt
Technical Univ. of Denmark, DK
- Jørn Justesen
Technical Univ. of Denmark, DK
- Axel Kohnert
Universität Bayreuth, DE
- Margreta Kuijper
The University of Melbourne, AU
- P. Vijay Kumar
IISc – Bangalore, IN
- Michael Lentmaier
Lund University, SE
- Hans-Andrea Loeliger
ETH Zürich, CH
- Felice Manganiello
Clemson University – South
Carolina, US
- Muriel Medard
MIT, US
- Sihem Mesnager
University of Paris VIII, FR
- Olgica Milenkovic
University of Illinois – Urbana
Champaign, US
- Katherine Morrison
Univ. of Northern Colorado, US
- Joachim Rosenthal
Universität Zürich, CH
- Vladimir Sidorenko
Universität Ulm, DE
- Vitaly Skachek
University of Tartu, EE
- Roxana Smarandache
University of Notre Dame, US
- Patrick Solé
Télécom Paris Tech, FR
- Emina Soljanin
Bell Labs – Murray Hill, US
- Alex Sprintson
Texas A&M University – College
Station, US
- Vladimir D. Tonchev
Michigan Tech University –
Houghton, US
- Anna-Lena Trautmann
Universität Zürich, CH
- Bane Vasic
Univ. of Arizona – Tucson, US
- Pascal Vontobel
HP Labs – Paolo Alto, US
- Judy L. Walker
Univ. of Nebraska – Lincoln, US
- Wolfgang Willems
Universität Magdeburg, DE
- Oyvind Ytrehus
University of Bergen, NO
- Jiun-Hung Yu
ETH Zürich, CH

