Mathematisches Forschungsinstitut Oberwolfach

Report No. 56/2007

Coding Theory

Organised by
Joachim Rosenthal, Zürich
Amin Shokrollahi, Lausanne

December 2nd – December 8th, 2007

Abstract. Coding theory lies naturally at the intersection of a large number of disciplines in pure and applied mathematics: algebra and number theory, probability theory and statistics, communication theory, discrete mathematics and combinatorics, complexity theory, and statistical physics. The workshop on coding theory covered many facets of the recent research advances.

Mathematics Subject Classification (2000): 11T71, 14G50, 68P30, 94B27.

Introduction by the Organisers

The workshop on Coding Theory has brought together leading researchers in several key areas of mathematical coding theory. On the side of many mathematicians there were computer scientist and electrical engineers present. Participants came from many countries and the group included both senior and junior researchers.

Ever since its conception in the late 1940's, the theory of error-correcting codes has established itself as one of the central areas in mathematics.

Coding theory lies naturally at the intersection of a large number of disciplines in pure and applied mathematics: algebra and number theory, probability theory and statistics, communication theory, discrete mathematics and combinatorics, complexity theory, and statistical physics, are just but a few areas which have brought about very interesting applications in coding theory in recent years. The multitude of methods and means to construct and analyze codes and their properties suggests that a workshop with the explicit aim of bringing together researchers in different sub-fields of coding theory is necessary for cross-fertilization of ideas and global advancement of the field.

The following topics were covered during the workshop.

Combinatorial and probabilistic coding theory: This area has experienced a huge revival in recent years because of its success in the design of codes with superior performance. Very roughly, in this area combinatorial structures are used to construct error-correcting codes, and properties of these structures are used to design and analyze efficient encoding and decoding algorithms for the codes. One of the most prominent examples in this area is furnished by the class of LDPC codes. These codes are constructed from sparse bipartite graphs. More generally Michael Tanner showed in the 80's how to construct 'general codes on graphs'.

The sparsity of the graph provides methods for construction of low complexity encoders and decoders. The graphs need to be designed in such a way as to facilitate an optimal operation of the algorithms. To achieve this goal researchers have developed and applied methods from probability theory and statistics, algebra, discrete mathematics, number theory, and statistical physics.

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 the 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. Such 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 embedds in the theory of Gröbner bases. There are emerging relationships between this area and codes on graphs, the leading question being whether or not 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.

Theoretical computer science: Theoretical computer science has contributed a large number of ideas to coding theory. The above mentioned analysis and design of LDPC codes, and the conception of list-decoding algorithms are two prime examples of such contributions.

The reader will find it interesting to study in more details the summary of the talks collected in this report.

Workshop: Coding Theory

Table of Contents

Ralf Koetter (joint with Frank R. Kschischang)
Error correction for network coding channels 3185

Gabriele Nebe (joint with Eric Rains and Neil Sloane)
Self-dual codes and invariant theory 3185

Alexander Barg (joint with Dmitry Nogin)
A functional view of upper bounds on codes 3187

Tom Hoeholdt (joint with Jorn Justesen)
Graph codes with Reed-Solomon component codes - I 3188

Jorn Justesen (joint with Tom Hoeholdt)
Graph codes with Reed-Solomon component codes - II 3191

Pascal O. Vontobel
A Factor-Graph Approach to Universal Channel Decoding 3194

Heide Gluesing-Luerssen (joint with Gert Schneider)
Weight Enumeration for Convolutional Codes 3195

Margreta Kuijper (joint with Raquel Pinto)
Minimal trellis realization by inspection for convolutional codes over finite rings 3197

Gary McGuire
Fourier Spectra on Finite Fields and Subspaces of Matrices 3198

Françoise Levy-dit-Vehel
MinRank and Rank Decoding: similarity and cryptographic relevance . . . 3199

Deepak Sridhara (joint with Christine A. Kelley)
Eigenvalue bounds on the pseudocodeword weight of expander codes 3202

Olgica Milenkovic (joint with Wei Dai)
Coding-Theoretic Problems in Genetics: Superimposed Codes for Compressed Sensing DNA Microarrays 3205

Iwan Duursma (joint with Seung Kook Park)
Coset decoding of two-point codes 3207

Christine A. Kelley (joint with Judy L. Walker)
A voltage graph approach to the analysis of LDPC codes 3210

Patrick Solé (joint with San Ling)
Nonadditive Quantum Codes from $\mathbb{Z}_4$-Codes 3213

Jürgen Bierbrauer
A direct approach to LP-bounds 3214

Michele Elia
Some Observations on the Continued Fraction of $\sqrt{N}$ and Factorization 3214

Alfred Wassermann (joint with Michael Kiermaier)
Computing the minimum Lee weight of the $\mathbb{Z}_4$-linear Quadratic Residue Codes of length 72 and 80 3216

Alexander Vardy
Multivariate Interpolation Decoding: Reaching the Ultimate Limit of List Error-Correction 3217

Frank R. Kschischang (joint with Danilo Silva, Ralf Koetter)
A Rank-Metric Approach to Error Control in Random Network Coding . 3219

Marcus Greferath
On a Method to Overcome the Draw-backs of Cycles in the Tanner graph of a Low-Density Parity-Check Code 3221

Gilles Zémor (joint with Alexander Barg)
Hypergraph codes and their decoding 3224

Jürgen Bierbrauer (joint with Gohar Kyureghyan)
Crooked binomials 3226

Daniel Augot
Multivariate generalizations of the Guruswami-Sudan decoding algorithm 3227

Jean-Pierre Tillich (joint with Thomas Camara, Harold Ollivier, David Poulin)
Quantum codes suitable for iterative decoding 3230

Patrick Solé (joint with Dimitrii Zinoviev)
A MacWilliams formula for Convolutional Codes 3231

Wolfgang Willems (joint with S. Bouyuklieva, E. O'Brien, and A. Malevich)
On extremal codes of type II 3232

Emina Soljanin
A Mathematical View of Hybrid ARQ 3233

Vitaly Skachek (joint with Mark F. Flanagan, Eimear Byrne and Marcus Greferath)
Linear-Programming Decoding of Non-Binary Linear Codes 3236

Abstracts

Error correction for network coding channels

Ralf Koetter
(joint work with Frank R. Kschischang)

Random network coding is a powerful and elegant tool for distributing information in networks, distributed storage systems, and peer-to-peer networking. Nevertheless, it typically assumes that all information forwarding devices cooperate in an error free fashion. In fact, without any protection, a single error in one received packet would typically render the entire transmission useless when the erroneous packet is combined with other received packets to deduce the transmitted message.

We derive coding schemes that are capable of protecting against both erroneous packets as well as incomplete transmissions. The framework considers random network coding as a kind of "non-coherent" transmission over a channel modeled as multiplication with a random matrix over F_q. The information bearing quantity that can be used on such a channel is the choice of subspace to be transmitted, which naturally leads to code design in the Grassmannian graph. We present the above described framework, present a Reed-Solomon code type construction based on rank error correcting codes of Gabidulin, and formulate a number of open algebraic coding questions. Of particular interest in this talk are the connections to error correction in the case of an intelligent and fully informed adversary and, consequently, the list decoding properties of the defined Reed-Solomon type codes. While some aspects of the interpolation based approaches of Sudan can be generalized other require substantially different techniques.

References

[1] R. Koetter and F. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, http://www.citebase.org/abstract?id=oai:arXiv.org:cs/0703061, 2007

Self-dual codes and invariant theory

Gabriele Nebe
(joint work with Eric Rains and Neil Sloane)

In our joint book [2] we formalize the notion of a Type of a self-dual code. This is a quadruple $\rho := (R, V, \beta, \Phi)$ where R is a finite ring, V a left R-module (the alphabet of the code), $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ a nonsingular biadditive form such that the right R-module

$$M := \{\beta^r : (x, y) \mapsto \beta(x, ry) \mid r \in R\}$$

is isomorphic to R_R and closed under the involution $\tau : M \to M, m^\tau(x, y) := m(y, x)$. The finite group Φ is a sub R-qmodule of the set of all quadratic mappings from V to $\mathbb{Q}/\mathbb{Z}$, such that $x \mapsto m(x, x) \in \Phi$ for all $m \in M$ and $(x, y) \mapsto \varphi(x +$

$y) - \varphi(x) - \varphi(y) \in M$ for all $\varphi \in \Phi$. Then a code C of Type ρ and length N is a submodule $C \leq V^N$ such that C is self-dual i.e. $C = C^\perp := \{x \in V^N \mid \sum_{i=1}^N \beta(x_i, c_i) = 0 \text{ for all } c \in C\}$ and C is isotropic, which means that $\sum_{i=1}^N \varphi(c_i) = 0$ for all $\varphi \in \Phi$ and $c \in C$.

For the doubly-even self-dual binary codes, $R = V = \mathbb{Z}/2\mathbb{Z}$, $\beta(x, y) = \frac{1}{2}xy$ and $\varphi_0(x) := \frac{1}{4}x^2$, so that $\Phi = \{\varphi_0, 2\varphi_0, 3\varphi_0, 0\}$.

The main theorem of our book [2] is

Theorem. Let ρ be a Type such that R is a direct product of matrix rings over chain rings (i.e. the left ideals are linearly ordered by inclusion). Then the $\mathbb{C}$-vectorspace spanned by the complete weight enumerators of codes of Type ρ is the full invariant ring of the associated Clifford-Weil group $\mathcal{C}(\rho)$.
Here

$$\mathcal{C}(\rho) = \langle m_r, d_\varphi, h_e \mid r \in R^*, \varphi \in \Phi, e \text{ symmetric idempotent in } R\rangle \leq \mathrm{GL}_{|\mathrm{V}|}(\mathbb{C})$$

where

generator	cwe invariant since
$m_r : x_v \mapsto x_{rv}$	C is a code
$d_\varphi : x_v \mapsto \exp(2\pi i\varphi(v))x_v$	C is isotropic
$h_e : x_v \mapsto \frac{1}{\sqrt{\lvert eV\rvert}} \sum_{w \in eV} \exp(2\pi i\beta(v, w))x_{w+(1-e)v}$	$C = C^\perp$

Since we allow R to be non-commutative, this theorem includes higher genus weight enumerators. The complete weight enumerator of genus m is $\mathrm{cwe_m(C)} = \mathrm{cwe(R^m \otimes C)}$ and the code $R^m \otimes C \leq (V^m)^N$ is a self-dual code over the alphabet V^m which is an $R^{m\times m}$-module. The associated Clifford-Weil group is $\mathcal{C}(\rho^m) =: \mathcal{C}_m(\rho)$.

We then get a surjective linear mapping $\phi_m : \mathrm{cwe_m(C)} \mapsto \mathrm{cwe_{m-1}(C)}$ from the invariant ring $\mathrm{Inv}(\mathcal{C}_\mathrm{m}(\rho))$ onto $\mathrm{Inv}(\mathcal{C}_{\mathrm{m}-1}(\rho))$, which yields an orthogonal decomposition

$$\star \quad \mathrm{Inv_N}(\mathcal{C}_\mathrm{m}(\rho)) = \mathrm{K_m^{(N)}} \perp \mathrm{K_{m-1}^{(N)}} \perp \ldots \perp \mathrm{K_0^{(N)}}$$

where K_a^N is isomorphic to the kernel of the restriction of ϕ_a to the homogeneous degree N-invariants $\mathrm{Inv_N}(\mathcal{C}_\mathrm{a}(\rho))$.

This is analogous to the decomposition of the space of modular forms into cusp forms, which is invariant under the Hecke algebra. It is hence natural to search for a coding theory analogue of Hecke-operators. The paper [1] generalizes a lattice theoretic construction (see for instance [3]) of Hecke-operators to codes over finite fields. To this aim let $\mathcal{F}_N := \{C \leq \mathbb{F}_q^N \mid C \text{ is of Type } \rho\}$ denote the family of self-dual codes of Type ρ over the finite field $\mathbb{F}_q$. Then $\mathcal{F}_N = [C_1] \cup \ldots \cup [C_h]$ is the disjoint union of permutation equivalence classes. Define a linear operator T on $\mathbb{C}[C_1] \oplus \ldots \oplus \mathbb{C}[C_h] \cong \mathbb{C}^h$ by $T([C]) := \sum_{D \in \mathcal{F}_N, D \sim C} [D]$ where $D \sim C$ iff D and C are neighbors, which means that $D \cap C$ has codimension 1 in C and D.

Theorem. T acts on $\mathrm{Inv_N}(\mathcal{C}_\mathrm{m}(\rho))$ by mapping $\mathrm{cwe_m(C)}$ to $\sum_{D \in \mathcal{F}_N, D \sim C} \mathrm{cwe_m(D)}$. The decomposition $\star$ is exactly the eigenspace decomposition of T.

References

[1] G. Nebe, *Kneser-Hecke operators in coding theory.* Abh. Math. Sem. Univ. Hamburg **76** (2006) 79-90.
[2] G.Nebe, E. Rains, N. Sloane, *Self-dual codes and invariant theory.* Springer (2006).
[3] G. Nebe, B. Venkov, *On Siegel modular forms of weight 12.* J. reine und angew. Math. **531** (2001) 49-60.
[4] B. Runge, *Codes and Siegel modular forms*, Discrete Math. **148** (1996) 175-204.

A functional view of upper bounds on codes

Alexander Barg
(joint work with Dmitry Nogin)

In the problem of bounding the size of codes in compact homogeneous spaces, Delsarte's polynomial method gives rise to the most powerful universal bounds on codes. Many overviews of the method exist in the literature; see for instance Levenshtein (1998). The purpose of this report is to present a functional perspective of this method and give some examples.

Let X be a compact metric space whose isometry group G acts transitively on it. The zonal polynomials associated with this action give rise to a family of orthogonal polynomials $\mathcal{P}(X) = \{P_\kappa\}$ where $\kappa = 0, 1, \dots$ is the total degree. These polynomials are univariate if G acts on X doubly transitively (the well-known examples include the Hamming and Johnson graphs and their q-analogs and other Q-polynomial distance-regular graphs; the sphere $S^{n-1} \in R^n$) and are multivariate otherwise.

Let $\langle f, g\rangle = \int_{-1}^{1} fgd\mu$ be the inner product in $L_2([-1, 1], d\mu)$ where $d\mu(x)$ is a distribution on $[-1, 1]$ induced by the invariant measure on G. By Delsarte's fundamental theorem, the size of the code $C \subset X$ whose distances take values in $[-1, s]$ is bounded above by $|C| \le \inf_{f\in\Phi} f(1)/\hat{f}(0)$ where $\Phi = \{f : f(x) \le 0, x \in [-1, s]; \quad \hat{f}(0) > 0, \ \hat{f}(i) \ge 0, i = 1, 2, \dots\}$, where $\hat{f}(i) = \langle f, P_i\rangle$ are the Fourier coefficients of f.

In the univariate case, the best asymptotic upper bounds on codes in a large class of spaces arise by taking $f(x) = (x - s)(K_k(x, s))^2$, where $K_k(x, s) := \sum_{i=0}^{k} \|P_i\|^{-2} P_i(s)P_i(x)$ is the k-th reproducing kernel ($f(x)$ is called the MRRW polynomial), while for finite parameters better bounds are obtained from the Levensthein polynomials (Levenshtein 1978). We show how the MRRW and Levensthein polynomials arise naturally as stationary points of the moment functional $\mathcal{F}(f) = \int f d\mu$. This enables us to link analytic methods of deriving the bounds to a spectral (linear-algebraic) approach recently introduced in Bachoc (2006) and developed by the authors (Barg and Nogin 2006). The spectral approach is particularly useful in the case of multivariare zonal polynomials (such as infinite Grassmann spaces and the Niederreiter-Rosenbloom-Tsfasman or NRT space). We comment on the derivation of bounds in the NRT space (Barg and Purkayastha 2007) and observe that the link established above enables one to pursue Levenshtein-type bounds in the multivariable case.

References

[1] Levenshtein (1978-1998): V. I. Levenshtein, VIIth Conference on Coding Theory, Vilnius (1978); Problemy Kibernetiki **40** (1983), pp. 43-110; Acta Applicandae Mathematicae **29** (1992), 1–82; Handbook of Coding Theory vol. 1 (1998), pp. 499–648.

Graph codes with Reed-Solomon component codes - I

Tom Hoeholdt

(joint work with Jorn Justesen)

We consider specific cases of the codes based on bipartite expander graphs. The nodes are labeled by the points and lines of a finite geometry, and there is a branch connecting a line node to any node labeled by a point on the line. The code symbols are associated with the branches, and the symbols connected to a given node are restricted to be codewords in a Reed-Solomon (RS) code over the field that is used for constructing the geometry.

These codes were introduced by Tanner in 1981 ([3]) and since then a considerable number of results have been obtained ([1], [2], [4], ans [5]).

Let $G = (V, E)$ be an n- regular bipartite graph, without loops and multiple edges, with vertex set $V = V_1 \cup V_2$. That the bipartite graph is n-regular means that each vertex of V_1 is connected to n vertices of V_2 and each vertex of V_2 is connected to n vertices of V_1. Let $x_1, x_2, \ldots, x_m$ be the vertices in V_1 and $y_1, y_2, \ldots, y_m$ the vertices in V_2 and define the $m \times m$ matrix $M = m_{ij}$ by

$$m_{ij} = \begin{cases} 1 & \text{if } x_i \text{ is connected to } y_j \\ 0 & \text{else} \end{cases}$$

The *adjacency matrix* of the bipartite graph is

$$A = \begin{pmatrix} 0 & M \\ M^T & 0 \end{pmatrix}$$

Thus each row has n 1s and the largest eigenvalue of A is n and the corresponding eigenvector is the all-ones vector. It is known ([6]) that $-n \leq \lambda_i \leq n$ where λ_i is any eigenvalue and that the second largest eigenvalue λ is closely related to the expansion properties of the graph. Let C_1 be a linear n, k_1, d_1 code and C_2 a linear n, k_2, d_2 code both over the finite field $F(q)$.

We now construct a code C of length $N = mn$ over $F(q)$ by associating $F(q)$ symbols with the edges of the graph (with a selected numbering) and demanding that the symbols connected to a vertex of V_1 (in the chosen order) shall be a codeword of C_1 and that the symbols on the edges connected to a vertex of V_2 (in the chosen order) shall be a codeword of C_2. It is clear that C is a linear code.

The rate R of C satisfy

$$R \geq r_1 + r_2 - 1 \quad \text{where} \quad r_1 = \frac{k_1}{n} \quad \text{and} \quad r_2 = \frac{k_2}{n}$$

The minimum distance D of the code C satisfies

$$D \geq m d_1 \frac{d_2 - \lambda\beta}{n - \lambda\beta}$$

where

$$\beta = \frac{\lambda(d_1 - d_2) + \sqrt{\lambda^2(d_1 - d_2)^2 + 4d_1d_2(n - d_1)(n - d_2)}}{2d_1(n - d_2)}$$

If $d_1 = d_2 = d$ we get

$$D \geq dm\frac{d - \lambda}{n - \lambda}$$

For short component codes the bound is not useful, but we can get a simple lower bound by the following consideration: Starting from a vertex in the right set, n vertices in the left set can be reached in one transition, and $n(n-1)$ vertices in the right set can be reached from these vertices. If they are assumed to be distinct, the minimum distance is always lower bounded by

$$D \geq d(d(d - 1) + 1) = d(d^2 - d + 1)$$

Any nonzero vertex on the right side has at least d nonzero branches connecting to vertices in the left set, and these reach $d(d - 1)$ vertices in the right set with nonzero branches.

Certain bipartite graphs derived from generalized polygons have perfect expansion properties.[4]. The generalized polygons are incidence structures consisting of points and lines where any point is incident with the same number of lines and any line is incident with the same number of points. A generalized N-gon defines a bipartite graph G that satisfies the following conditions:

- For all nodes $u, v \in G$, $d(u, v) \leq N$, where $d(u, v)$ is the length of the minimum path connecting u and v.
- If $d(u, v) = h < N$, then there is a unique path of length h connecting u and v.
- Given a node $u \in G$ there exists a node $v \in G$ such that $d(u, v) = N$.

We note that this implies that the girth of the bipartite graph is at least $2N$. Most of this paper is concerned with graphs from finite planes, and in this context the 3-gons are derived from finite projective planes.

Let M be an incidence matrix for a projective plane with $m = q^2 + q + 1$ points, $(x : y : z)$, and $q^2 + q + 1$ lines of the form $ax + by + cz = 0$. The graph is invariant to an interchange of the two sets of variables.

Thus each row has $q + 1$ 1s and the largest eigenvalue of A is $q + 1$ and the corresponding eigenvector is the all-ones vector. The graph may be seen as a simple expander graph: The eigenvalues are $\pm q + 1$ and $\pm\sqrt{q}$ (all real since A is symmetric).

Starting from a node in the right set, $q + 1$ nodes in the left set can be reached in one transition, and $q(q + 1)$ nodes in the right set can be reached from these nodes. The graph can be used to define a code by associating a symbol with each branch and letting all branches that meet in a node satisfy the parity checks of an (n, k, d) RS code where $n = q + 1$. Thus the length of the total code is

$$N = mn = (q^2 + q + 1)(q + 1)$$

It is sometimes more convenient to let M be an incidence matrix for an Euclidean plane with $m = q^2$ points, (x, y), and q^2 lines of the form $y = ax + b$. The

lines of the form $x = c$ are omitted, and in this way the graph is invariant to an interchange of the two sets of variables.

Thus each row has q 1s and the eigenvalues are $\pm q$, $\pm\sqrt{q}$ and 0.

All branches that meet in a node satisfy the parity checks of an (n, k, d) RS code with $n = q$. Thus the length of the code is

$$N = q^3$$

The dimension of the graph code derived from a finite plane is lower bounded by

$$K \geq N - 2m(n - k)$$

since the last term is the total number of parity checks in the component codes. However, these checks are not all linearly independent. To find the actual dimension we must specify how the symbols of the component codes are mapped onto the branches. In the Euclidean plane, the node corresponding to a particular pair (a, b) connect to node (x, y) whenever $y = ax + b$.

The codewords can be found by evaluating polynomials in x of degree less than k for all values of x. Since y is a linear function of x, we can also evaluate a polynomial in x and y of degree less than k in the q pairs. With this specification of the code we have:

The dimension of the graph code based on a Euclidean plane over $F(q)$ is

$$\begin{array}{rl} k^3 & \text{for} \quad k \leq \frac{q}{2} \\ m(2k - n) + (n - k)^3 & \text{for} \quad k > \frac{q}{2} \end{array}$$

The number of linearly independent monomials of degree $< k$ is k^3.

Since a graph code is described by the properties of a large parity check matrix, it is not immediately clear how encoding can be performed in a simple way [3]. Here we describe an encoding of codes from Euclidean planes based on evaluations of a suitable set of polynomials.

We represent an edge in the bipartite graph by a quadruple (x, y, a, b) in $F(q)^4$ where $y = ax + b$. A codeword is then obtained by evaluation of a polynomial from (a subset of) $F(q)[X, Y, A, B]$. We therefore have that polynomials which are equivalent modulo the ideal I spanned by $X^q - X, Y^q - Y, A^q - A, B^q - B, Y - AX - B$ evaluate to the same codeword and therefore we only have to consider polynomials in $V = F(q)[X, Y, A, B]/I$. Our first task is to find the dimension of V as a vector space over $F(q)$. This can be done by finding a Groebner basis of I with respect to some monomial order and then finding the leading monomials. The result is

The dimension of V as a vector space over $F(q)$ is q^3.

References

[1] G. Zèmor:"On expander codes" *IEEE Trans.Inform.Theory*(Special Issue on Codes on Graphs and iterative Algorithms) , vol.47, pp.835-837, Feb. 2001.

[2] A. Barg and G. Zèmor:"Error exponents of expander codes" *IEEE Trans.Inform.Theory*, vol.48, pp.1725-1729 , June 2002.

[3] M. Tanner:"A Recursive Approach to Low Complexity Codes" *IEEE Trans.Inform.Theory*, vol.27, pp.533-547, September 1981.

[4] M. Tanner:"Explicit Concentrators from Generalized N-Gons" *SIAM J.Alg.Disc.Meth.* Vol.5 No.3 pp.287-293, September 1984.
[5] M. Tanner:"Minimum-Distance Bounds by Graph Analysis" *IEEE Trans.Inform.Theory*, vol.47, pp.808-821, February 2001.
[6] R. Roth. *Introduction to Coding Theory.* Cambridge University Press, 2006.

Graph codes with Reed-Solomon component codes - II

Jorn Justesen
(joint work with Tom Hoeholdt)

We consider codes based on bipartite expander graphs. The nodes are labeled by the points and lines of a finite geometry, and there is a branch connecting a line node to any node labeled by a point on the line. The code symbols are associated with the branches, and the symbols connected to a given node are restricted to be codewords in a Reed-Solomon (RS) code over the field that is used for constructing the geometry.

The right codes correct all error patterns of weight at most T_1, the left codes correct T_2 errors. Initially we let $T_1 = T_2 = T$. A total of W errors are assumed to occur at randomly chosen positions. Since the decoding is independent of the codeword and the error values, it is sufficient to consider the error graph, a bipartite graph with $N + N$ vertices and W randomly chosen branches. If T is not too small, the probability of decoding errors when more than T errors occur, approximately $1/T!$, is insignificant. The analysis clearly also applies exactly to the case of erasure correction.

If the decoding of the component codes is repeated until a stable result is obtained, a decoding failure occurs if the error graph contains a $T + 1$ core: A k-core in a graph is a subgraph with the property that all vertices have degree at least k.

The existence of cores in random graphs has been a subject of considerable interest in graph theory. In particularly the following result due to Pittel et al. is important [1]: Let G be a random graph with n vertices and w edges. With high probability a k connected core exists when $w > c_k n/2$, but not for smaller w. The core includes a large fraction of the vertices. Here c_k is defined in terms of the Poisson distribution

$$\sigma(j) = e^{-\lambda}\lambda^j/j!$$
$$\pi_k(\lambda) = \textstyle\sum_{j\geq k-1}\sigma(j)$$
$$c_k = min_\lambda[\lambda/\pi_k(\lambda)], \lambda > 0$$

Thus $c_3 = 3.35$, $c_4 = 5.14$, $c_5 = 6.80$, $c_6 = 8.37$, $c_9 = 12.78$. Asymptotically $c_k \approx k + \sqrt{k \log k}$.

The result applies without change to random bipartite graphs. This can be proved by making a small modification in the simplified proof of the basic result, which was given in [2]. The degree of a vertex is initially interpreted as the number of half-edges associated with the vertex. These half-edges are later combined in

pairs to make the actual edges of the graph. The following algorithm simultaneously specifies the random graph and removes edges connected to vertices of low degree:

- Remove a half-edge from a light vertex (degree $< k$)
- Remove a randomly selected half-edge (which becomes the other part of the complete edge)
- Repeat the process as long as there are light vertices

The proof in [2] goes on from here to analyze the evolution of the degree distribution as a stochastic process. For the complete bipartite graph, the only modification is that the steps are:

- Remove a half-edge from a light vertex on the right
- Remove a randomly selected half-edge from the left (to complete the edge)
- Repeat these steps with right and left reversed

If the graph code is based on a random bipartite graph with the given degree, we can continue the selection process from the error graph to the complete code graph (assuming that no vertex has more than N errors). In the bipartite graph derived from a projective plane, a given vertex on the right is connected to $q+1$ vertices on the left, and these have edges connecting to the remaining $q(q+1)$ right vertices. Thus if the vertices are chosen in the relevant subsets, all edges have the same probability of being removed in the last step, and thus the distribution evolves as in the original graph.

Thus for a given error correcting radius, T, the performance is asymptotically the same for product codes, more sparse random graph codes, and codes constructed from geometries. Simulations indicate that although graphs from geometries have smaller second eigenvalues than random graphs, codes based on random graphs have a small advantage in performance.

In the actual decoding of graph codes we remove all light vertices on one side in each step. Initially the number of errors on each side follows a Poisson distribution since N is large compared to T. The average number of errors that are decoded on the left when all component codes are decoded can then be found from this distribution as

$$\sum_{j\le T} j e^{-m} m^j / j!$$

We now introduce the simplifying assumption that these decoded positions are randomly distributed on the right vertices. A similar approach was discussed as an informal introduction in [1]. We prove that if the degrees of the vertices on one side of the graph follow a truncated Poisson distribution, a randomly chosen subset of the branches are removed, and all resulting light vertices are removed, the degree distribution of the remaining vertices is again a truncated Poisson distribution.

The calculation of the mean value of a truncated Poisson distribution is facilitated by the following identity, which is a standard result in traffic theory.

$$\sum_{j>T} j e^{-m} m^j / j! = m \sum_{j\ge T} e^{-m} m^j / j! = m\pi_{T+1}(m)$$

This explains why the summation in the definition of π starts at $k-1$ rather than k. We omit the subscript.

We can now describe the evolution of the degree distribution:

Theorem 1: If the total number of errors in initially $W = MN$, the number of errors in each right code follows a Poisson distribution with mean M. After the first decoding, the number of errors per vertex on the left follows a Poisson distribution with mean

$$m(1) = M\pi(M)$$

The degree distribution after each of the following stages of decoding follow a truncated Poisson distribution with parameters

$$m(j) = M\pi(m(j-1))$$

This simple recursion follows from the independence assumption using the above identity.

If the initial value, M, is less than $min\{m/\pi(m)\}$, $m(j)$ converges to zero, while for M less than this threshold, m converges to the largest value such that $m' = M\pi(m')$.We then have

Theorem 2: In the limit of large N, a graph code with $2N$ nodes and component RS codes correcting a fixed number of errors, T, can be decoded by iterated decoding of the component codes to correct $W = NM$ errors, when

$$M < min_m\{m/\pi(m)\}$$

The iteration can be illustrated graphically as a sequence of points on the line $m = x$ and the graph of $M\pi(x)$.

For small values of T, experiments indicate that the best performance (highest rate for a given fraction of corrected errors), is obtained with different values of T, T_1 and T_2 on the right and left respectively. The original proof of cores in random graphs is not easily modified to work with different values of T in subsets of the vertices. However, in our analysis such a change is easily made. If the definition of the function π is modified to alternate between T_1 and T_2, the parameters are still updated by the same recursion.

The errors are corrected if the initial number of errors is below a certain threshold, but for larger values the decoding process reaches a stationary point with a pair of parameters, $(m', m")$. The iteration can be illustrated graphically (in the form well-known from EXIT graphs) as a staircase line between the graph of $\pi(x)$ for T_1 and a reflected version of the graph of $\pi(x)$ for T_2. The graphic indicates that the decoding threshold is reached when these two curves touch.

Asymptotically the error probability is dominated by the probability of small cores, and it is thus a fairly large negative power of N. For realistic code lengths, the predicted sharp threshold at W errors is observed, but no sufficiently good bound on the probability of a large core is presently available.

References

[1] B. Pittel, J. Spencer, and N. Wormald, *Sudden emergence of a giant k-core in a random graph*, J.Comb.Theory, Series B, **67** (1996), 11–151.

[2] S. Janson and M.J. Luczak, *A simpel solution to the k-core problem*, Random Structures Algorithms, **30** (2007), 50–62.

A Factor-Graph Approach to Universal Channel Decoding

Pascal O. Vontobel

In the last decade it has become more and more clear how one can efficiently achieve reliable communication close to capacity when the channel law is known. A very helpful tool in deriving such codes / decoders has been the factor-graph / message-passing iterative decoding framework [1, 2, 3].

Some work has also been done for formulating decoders when the channel law is not known, see e.g. [4, 5, 6, 7, 8, 9]. However, in these papers the channel law was never totally unknown (the channel was within a very specific class of channels) and / or the decoders could rely on the presence of training sequences or pilot symbols. In this talk we study the case where the channel law is unknown except that it is a discrete memoryless channel (DMC) with known input and output alphabet. Our setup is universal in the sense that no training sequence is allowed, i.e. no position of the channel code is allowed to be fixed to a certain symbol.

We remark that papers and books that discuss universal decoding include [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 18, 20, 21, 22]. However, the practicality of most of the proposed schemes is not quite clear. In this talk, we discuss a variety of approaches for solving this problem efficiently. It turns out that it is worthwhile to design decoders which try to minimize the symbol error probability. This is in contrast to the usual approach where the block error probability is minimized.

For more information, see [23].

References

[1] G. D. Forney, Jr., "Codes on graphs: normal realizations," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 520–548, Feb. 2001.

[2] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 498–519, Feb. 2001.

[3] H.-A. Loeliger, "An introduction to factor graphs," *IEEE Sig. Proc. Mag.*, vol. 21, no. 1, pp. 28–41, Jan. 2004.

[4] A. P. Worthen and W. E. Stark, "Unified design of iterative receivers using factor graphs," *IEEE Trans. on Inform. Theory*, vol. IT–48, no. 2, pp. 843–849, Feb. 2001.

[5] R. Nuriyev and A. Anastasopoulos, "Pilot-symbol-assisted coded transmission over the block-noncoherent AWGN channel," *IEEE Trans. on Comm.*, vol. COM–51, no. 6, pp. 953–963, June 2003.

[6] H. Steendam, N. Noels, and M. Moeneclaey, "Iterative carrier phase synchronization for low-density parity-check coded systems," in *Proc. IEEE Intern. Conf. Communications*, vol. 5, Anchorage, AK, USA, May 11–15 2003, pp. 3120–3124.

[7] J. Dauwels and H.-A. Loeliger, "Joint decoding and phase estimation: an exercise in factor graphs," in *Proc. IEEE Intern. Symp. on Inform. Theory*, Pacifico Yokohama, Japan, June 29 – July 4 2003, p. 231.

[8] ——, "Phase estimation by message passing," in *Proc. IEEE Intern. Conf. Communications*, vol. 1, Paris, France, June 20–24 2004, pp. 523–527.

[9] J. Dauwels, S. Korl, and H.-A. Loeliger, "Expectation maximization for phase estimation," in *Proc. Eighth Intern. Symp. on Comm. Theory and Appl.*, Ambleside, England, 2005.

[10] V. D. Goppa, "Universal decoding for symmetric channels," *Probl. Inform. Transm.*, vol. 11, no. 1, pp. 15–22, 1975.

[11] ——, "Nonprobabilistic mutual information without memory," *Probl. Contr. Inform. Theory*, vol. 4, pp. 97–102, 1975.

[12] I. Csiszár and J. Körner, *Information Theory*. Budapest: Akadémiai Kiadó (Publishing House of the Hungarian Academy of Sciences), 1981, coding theorems for discrete memoryless systems.
[13] J. Ziv, "Universal decoding for finite-state channels," *IEEE Trans. on Inform. Theory*, vol. IT–31, no. 4, pp. 453–460, July 1985.
[14] N. Merhav, "Universal decoding for memoryless Gaussian channels with a deterministic interference," *IEEE Trans. on Inform. Theory*, vol. IT–39, no. 4, pp. 1261–1269, July 1993.
[15] M. Feder and A. Lapidoth, "Universal decoding for channels with memory," *IEEE Trans. on Inform. Theory*, vol. IT–44, no. 5, pp. 1726–1745, Sept. 1998.
[16] A. Lapidoth and J. Ziv, "On the universality of the LZ-based decoding algorithm," *IEEE Trans. on Inform. Theory*, vol. IT–44, no. 5, pp. 1746–1755, Sept. 1998.
[17] ——, "On the decoding of convolutional codes on an unknown channel," *IEEE Trans. on Inform. Theory*, vol. IT–45, no. 7, pp. 2321–2332, Nov. 1999.
[18] M. Feder and N. Merhav, "Universal composite hypothesis testing: a competitive minimax approach," *IEEE Trans. on Inform. Theory*, vol. IT–48, no. 6, pp. 1504–1517, June 2002.
[19] Y. Ephraim and N. Merhav, "Hidden Markov processes," *IEEE Trans. on Inform. Theory*, vol. 48, no. 6, pp. 1518–1569, June 2002.
[20] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. on Inform. Theory*, vol. IT–44, no. 6, pp. 2148–2177, Oct. 1998.
[21] T. P. Coleman, M. Médard, and M. Effros, "Linear complexity universal decoding with exponential error probability decay," in *Proc. 2005 International Conference on Wireless Networks, Communications, and Mobile Computing (Wirelesscom 2005)*, Maui, HI, USA, Jun. 13-16 2005.
[22] T. P. Coleman and M. Médard, "On low complexity decodable universally good linear codes," in *Proc. Inaugural Workshop of the Center for Information Theory and its Applications*, UC San Diego, La Jolla, CA, USA, Feb. 6-10 2006.
[23] P. O. Vontobel, "A factor-graph approach to universal decoding," in *Proc. 44th Allerton Conf. on Communications, Control, and Computing*, Allerton House, Monticello, Illinois, USA, Sep. 27-29, 2006.

Weight Enumeration for Convolutional Codes

Heide Gluesing-Luerssen
(joint work with Gert Schneider)

The weight enumerator of a block code counts the number of codewords of given weight. It turned out to be one of the most important invariants for the performance of a block code. In particular, it is a well-known fact of block code theory that the weight enumerator of a code completely determines that of the dual code. More precisely, they are related by the famous MacWilliams Identity found in 1962. For a k-dimensional code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with weight enumerator $\mathrm{we}(\mathcal{C}) := \sum_{v\in\mathcal{C}} W^{\mathrm{wt}(v)} \in \mathbb{C}[W]$ it reads as $\mathrm{we}(\mathcal{C}^\perp) = q^{-k}\mathbf{H}\big(\mathrm{we}(\mathcal{C})\big)$, where $\mathbf{H}:\ \mathbb{C}[W]_{\le n} \longrightarrow \mathbb{C}[W]_{\le n},\ f(W) \longmapsto (1+(q-1)W)^n f(\frac{1-W}{1+(q-1)W})$. The abundant practical and theoretical applications have been studied ever since.

In this talk I want to discuss possible generalizations of this result to convolutional codes. A convolutional code of length n is a direct summand of the module $\mathbb{F}[z]^n$ endowed with the Hamming weight for polynomial vectors, see, e. g., [5] for details. For these codes the weight enumerator of block code theory can be generalized in a twofold way. A fairly straightforward generalization leads to a formal

power series in two variables with the coefficients being the number of codewords of given weight and length in a meaningful way. In [7] Shearer and McEliece proved that there is no MacWilliams identity for this type of weight enumerator.

A second generalization is given by the weight adjacency matrix. This matrix is defined best by considering state space realizations of the encoder. Thus, let $\mathcal{C} = \operatorname{im} G \subseteq \mathbb{F}[z]^n$ be a convolutional code with minimal and basic encoder matrix $G \in \mathbb{F}[z]^{k\times n}$. From linear systems theory one can deduce that there exist constant matrices A, B, C, D with entries in $\mathbb{F} = \mathbb{F}_q$ such that the encoding identity $\sum_{t\geq 0} u_t z^t G = \sum_{t\geq 0} v_t z^t$ is equivalent to

$$x_{t+1} = x_t A + u_t B, \quad v_t = x_t C + u_t D \ \text{ for all } t \geq 0 \text{ and where } x_0 = 0.$$

Here $u_t \in \mathbb{F}^k$ and $v_t \in \mathbb{F}^n$ for all $t \geq 0$. Moreover, it is known that the length of the internal state vector x_t can be made identical to the degree, say δ, of the code. The system gives rise to the weight adjacency matrix $\Lambda = (\lambda_{X,Y})_{X,Y\in\mathbb{F}^\delta} \in \mathbb{C}[W]^{q^\delta \times q^\delta}$, where

$$\lambda_{X,Y} := \operatorname{we}(\{XC + uD \mid u \in \mathbb{F}^k : Y = XA + uB\}).$$

Thus, at position (X, Y) the weight adjacency matrix is the weight enumerator of the set of all outputs $v = XC + uD$ corresponding to all those inputs $u \in \mathbb{F}^k$ which steer the state X to the next state $Y = XA + uB$. It is well-known that this matrix gives quite detailed information about the performance of the code, see also [4, Sec. 3.10]. Moreover, it can be used to compute the classical weight enumerator of the code mentioned above, see [6, Thm. 3.1] or [2, Thm. 3.8].

Obviously, the weight adjacency matrix is not an invariant of the code since it depends on both the chosen encoder and the minimal realization. However, the non-uniqueness can be nicely described. Indeed, if Λ, $\Lambda' \in \mathbb{C}[W]^{q^\delta \times q^\delta}$ are two weight adjacency matrices for a given code, obtained via possibly different minimal and basic encoders and different minimal state space realizations, then there exists a state space isomorphism $T \in GL_\delta(\mathbb{F})$ such that $\Lambda'_{X,Y} = \Lambda_{XT,YT}$ for all $(X, Y) \in \mathbb{F}^\delta \times \mathbb{F}^\delta$, see [2] for details. In other words, the two matrices differ only by a state space isomorphism. This gives rise to an invariant $\Lambda(\mathcal{C})$ of the code, defined as the orbit under the canonical group action of $GL_\delta(\mathbb{F})$ on Λ. We call $\Lambda(\mathcal{C})$ the generalized weight adjacency matrix of the code.

Now we are in a position to formulate our MacWilliams Identity. Let $\zeta \in \mathbb{C}^*$ be a primitive p-th root of unity, where p is the characteristic of the field $\mathbb{F} = \mathbb{F}_q$ and let $\tau : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ be the usual trace function. We define the MacWilliams matrix

$$\mathcal{H} := q^{-\frac{\delta}{2}} (\zeta^{\tau(XY^\mathsf{T})})_{X,Y\in\mathbb{F}^\delta} \in \mathbb{C}^{q^\delta \times q^\delta}.$$

It is straightforward to show that $\mathcal{H}$ is invertible. Then the generalized weight adjacency matrices of a k-dimensional convolutional code $\mathcal{C} \subseteq \mathbb{F}_q[z]^n$ of degree δ and its dual $\mathcal{C}^\perp := \{w \in \mathbb{F}[z]^n \mid wv^\mathsf{T} = 0 \text{ for all } v \in \mathcal{C}\}$ satisfy

$$\Lambda(\mathcal{C}^\perp) = q^{-k} \mathbf{H}\big(\mathcal{H}\, \Lambda(\mathcal{C})^\mathsf{T}\, \mathcal{H}^{-1}\big).$$

For details see [3]. Thus, just like in the MacWilliams identity for block codes the generalized weight adjacency matrix of the code $\mathcal{C}$ completely determines that

of the dual code, and no representation of the code is needed. The result also generalizes a set of identities developed in [1] for convolutional codes of degree 1.

References

[1] K. A. S. Abdel-Ghaffar. On unit constrained-length convolutional codes. *IEEE Trans. Inform. Theory*, IT-38:200–206, 1992.

[2] H. Gluesing-Luerssen. On the weight distribution of convolutional codes. *Linear Algebra and its Applications*, 408:298–326, 2005.

[3] H. Gluesing-Luerssen and G. Schneider. On the MacWilliams identity for convolutional codes. Preprint 2006. Accepted for publication in IEEE Transactions on Information Theory. Available at http://arxiv.org/pdf/cs.IT/0603013.

[4] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[5] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory, Vol. 1*, pages 1065–1138. Elsevier, Amsterdam, 1998.

[6] R. J. McEliece. How to compute weight enumerators for convolutional codes. In M. Darnell and B. Honory, editors, *Communications and Coding (P. G. Farrell 60th birthday celebration)*, pages 121–141. Wiley, New York, 1998.

[7] J. B. Shearer and R. J. McEliece. There is no MacWilliams identity for convolutional codes. *IEEE Trans. Inform. Theory*, IT-23:775–776, 1977.

Minimal trellis realization by inspection for convolutional codes over finite rings

Margreta Kuijper

(joint work with Raquel Pinto)

In this presentation I consider convolutional codes over finite rings of the type $\mathbb{Z}_{p^r}$. These are motivated by Trellis Coded Modulation systems. I address the open problem of determining the minimal number of trellis states in terms of a polynomial encoder.

In the literature (starting with Forney's early papers in the 70s, [3, 2]) concepts from system theory such as row reducedness have made their way into the algebraic theory of convolutional codes. In the coding community the concept of row reducedness is more commonly known as "predictable degree property". However, until recently, this theory was not fully developed for the ring case. The recent paper [5] develops a concept of row reducedness for polynomial matrices over $\mathbb{Z}_{p^r}$. A central concept is the concept of "p-generator sequence" which was first introduced in [9] for modules in $\mathbb{Z}_{p^r}$. The paper [5] develops this concept further for polynomial modules in $\mathbb{Z}_{p^r}[z]$ and achieves a novel generalization of the predictable degree property for polynomial matrices over $\mathbb{Z}_{p^r}$.

There is a considerable amount of literature concerning minimal trellis construction for convolutional codes over $\mathbb{Z}_{p^r}$, see e.g. [2, 8, 6, 7, 4, 1, 10] In particular, [2] provides a canonical minimal trellis construction from the code sequences. However, the literature does not provide a straightforward method to construct a minimal trellis from a polynomial encoder nor an expression for the minimal number of

trellis states in terms of some kind of McMillan degree ("complexity") as in the field case. In this presentation I present solutions to both of these open problems.

In particular, I present a simple method to construct a minimal trellis from a left prime polynomial encoder. The trellis is in controller canonical form and has a minimal number of trellis states. Also, I express the minimal number of trellis states as p^δ, where δ is the sum of the "p-degrees" from [5] of the associated module, which is an invariant of the code. In the field case δ equals the McMillan degree of the code times r which is the classical formula. I propose a new concept of "minimality" of a polynomial encoder where there is a direct relationship between the sum of the row degrees of the minimal encoder and the minimal number of trellis states, just as in the field case.

References

[1] F. Fagnani and S. Zampieri. Dynamical systems and convolutional codes over finite abelian groups. *IEEE Trans. Inf. Th*, 42:1892–1912, 1996.

[2] G.D. Forney and M.D. Trott. The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders. *IEEE Trans. Inf. Th*, 39:1491–1513, 1993.

[3] G.D. Forney, Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.

[4] R. Johannesson, Z-X. Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Trans. Inf. Th.*, IT-44:839–845, 1998.

[5] M. Kuijper, R. Pinto, and J. W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425:776–796, 2007.

[6] H-A Loeliger, G.D. Forney, T. Mittelholzer, and M.D. Trott. Minimality and observability of group systems. *Linear Algebra and its Applications*, 205-206:937–963, 1994.

[7] H-A Loeliger and T. Mittelholzer. Convolutional codes over groups. *IEEE Trans. Inf. Th.*, IT-42:1660–1686, 1996.

[8] T. Mittelholzer. Minimal encoders for convolutional codes over rings. In B. Honory, M. Darnell, and P.G. Farell, editors, *Communications Theory and Applications*, pages 30–36. HW Comm. Ltd, 1993.

[9] V.V. Vazirani, H. Saran, and B.S. Rajan. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.*, 42:1839–1854, 1996.

[10] E. Wittenmark. Minimal trellises for convolutional codes over rings. *ISIT'98*, 15, 1998.

Fourier Spectra on Finite Fields and Subspaces of Matrices

Gary McGuire

Let V_n denote any n-dimensional vector space over $\mathbb{F}_2$. The Fourier transform of a function $f : V_n \longrightarrow V_m$ is defined by

$$\widehat{f}(a,b) := \sum_{x \in V_n} (-1)^{\langle b, f(x)\rangle + \langle a, x\rangle}$$

for $a \in V_n$ and $b \in V_m$, $b \neq 0$. The angular brackets $\langle\ ,\ \rangle$ denote any inner product on the relevant vector spaces. The Fourier spectrum of f is the subset of $\mathbb{Z}$ consisting of the set of values of $\widehat{f}$, over all a and b ($b \neq 0$), and is independent

of the inner products used. If $m = 1$ then $V_m = V_1 = \mathbb{F}_2$ and any function $f : V_n \longrightarrow \mathbb{F}_2$ is called a Boolean function.

We give a connection between the Fourier spectrum of Boolean functions and subspaces of skew-symmetric subspaces where each nonzero element has a lower bound on its rank. This work is all implicit in Delsarte and Goethals [1].

Let $L(n, k, F)$ denote the maximal dimension of a subspace of $M_{n,n}(F)$ all of whose nonzero elements have rank at least k. Let $L_S(n, k, F)$ denote the maximal dimension of a subspace of $M_{n,n}(F)$ all of whose nonzero elements are skew-symmetric and have rank at least k. We will discuss the calculation of this function in the case of $F = \mathbb{F}_2$ and k large. In particular, we discuss $L_S(n, n-1, \mathbb{F}_2)$ and $L_S(n, n-3, \mathbb{F}_2)$ when n is odd and its relationship to the Fourier spectrum of functions. These methods carry over easily to finite fields of odd characteristic, and are well known [1]. We will discuss carrying over the methods to infinite fields, and proving results on $L(n, k, F)$ and $L_S(n, k, F)$ when F is an infinite field permitting a cyclic extension of degree n. Some results on this can be found in [2] and [3].

Connections have been found between subspaces of matrices with good rank properties and spacetime coding, and also network coding.

References

[1] P. Delsarte, J.-M. Goethals, Alternating Bilinear Forms over GF(q), J. Comb. Th. Ser. A, **19** 26–50 (1975).

[2] R. Gow, R. Quinlan On the Vanishing of subspaces of alternating bilinear forms, Linear and Multilinear Algebra, **54** 415–428 (2006).

[3] G. McGuire, Spectra of Boolean Functions, Subspaces of Matrices, and Going Up versus Going Down, Proceedings of AAECC-17 Bangalore India December 2007, Lecture Notes in Computer Science 4851, S. Boztas and H.-F. Lu eds., Springer 2007.

MinRank and Rank Decoding: similarity and cryptographic relevance

Françoise Levy-dit-Vehel

In this talk, we study a very natural problem in linear algebra called MinRank (MR), that was originally introduced by Buss, Frandsen and Shallit in 96 [10]. We consider matrices M with entries from $R \cup \{x_1, \ldots, x_k\}$, where R is a commutative ring and the x_i are distinct variables. The statement of MR is as follows:

Input: $N, n, r, k \in \mathbb{N}^*,\ M \in \mathcal{M}_{N\times n}(R \cup \{x_1, \ldots, x_k\})$.
Question: decide whether $\min_{(\lambda_1,\ldots,\lambda_k)\in R} \mathrm{rank}(M(\lambda_1, \ldots, \lambda_k)) \leq r$.

Our motivation is cryptographic applications; we thus consider this problem over a finite field $\mathbb{F}_q$. We show here how close MR is to a well-known problem in coding theory, namely the Rank Decoding problem (RD):

Input: $N, n, k \in \mathbb{N}^*$, $G \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^N})$, $c \in \mathbb{F}_{q^N}^n$, $r \in \mathbb{N}^*$.
Question: decide whether there exists a vector $m \in \mathbb{F}_{q^N}^k$, such that $e = c - mG$ has rank $\mathrm{rank}(e \,|\, \mathbb{F}_q) \leq r$?
Here, $\mathrm{rank}(e \,|\, \mathbb{F}_q)$ is the rank of the $(N \times n)$ matrix representing e in a basis of $\mathbb{F}_q^N$

over $\mathbb{F}_q$.
Then we recall some complexity results, in particular a simple reduction of MR from Maximum Likelihood Decoding that shows MR is NP-complete. On the other hand, we show that RD is poly-time many-one reducible to MR; but it is not known whether RD is NP-complete.

Next, we survey methods to address those two problems. Two methods have been proposed to solve MR: the kernel method and the MQ-solving method [3]. The kernel method consists in choosing some vectors of $\mathbb{F}_q^n$ at random, and then tune the x_is - i.e. solve a linear system - so that the matrix $M(x_1, \ldots, x_k)$ admits those vectors in its kernel. Then, with some easy computed probability, this matrix is of rank $\leq r$. Repeating this experiment a sufficient number of times allows to find a matrix with this property. This method works in $O(q^{\lceil \frac{k}{n} \rceil r} k^3)$, and thus is relevant for small r in very small fields.
The MQ-solving method is somehow dual to the previous one. The idea is to express an instance of MR as one of MQ, which is the problem of solving multivariate quadratic equations over a finite field. We try to find a set of independent vectors of a special form in the kernel of matrix $M(x_1, \ldots, x_k)$. Putting the constraints into equations yields a quadratic system with unknowns a subset of coordinates of these vectors, together with the vector $(x_1, \ldots, x_k)$. The results obtained so far are experimental: solving the resulting quadratic system with a Gröbner basis algorithm, we can reach instances of MR with small r.

For general instances of RD, the best algorithm known is due to Ourivski and Johannssson [8], that we explain below: let d be the minimum rank distance of the code. Let $c \in \mathbb{F}_{q^N}^n$ be the received word. Then, if $m \in \mathbb{F}_{q^N}^k$ is such that $e = c - mG$ has smallest rank r - where $r \leq t = \lfloor (d-1)/2 \rfloor$ - then the code $\mathcal{C}_e$ with generator matrix

$$\begin{pmatrix} G \\ c \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ m & 1 \end{pmatrix} \begin{pmatrix} G \\ e \end{pmatrix}$$

has words of rank exactly r. Moreover, the codewords of rank r are exactly the (scalar) multiples of e. Thus, the problem is "reduced" to the one of finding a minimum weight codeword - say $\epsilon e, \epsilon \in \mathbb{F}_{q^N}^*$ - in the code $\mathcal{C}_e$.
Let G_{syst} be the generator matrix of $\mathcal{C}_e$ in systematic form, i.e. $G_{syst} = (I_{k+1}\, R)$, $R \in \mathcal{M}_{(k+1)\times(n-k-1)}(\mathbb{F}_{q^N})$. We have $e = (e_1, e_1 R)$, $e_1 \in \mathbb{F}_{q^N}^{k+1}$. Thus, we need to find e_1 such that $\mathrm{rank}((e1, e1R) \,|\, \mathbb{F}_q) = r$.
We can write e in the form

$$e = XA,$$

where $X = (x_0, \ldots, x_{r-1})$ is an incomplete basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ and $A = (\alpha_{i,j}) \in \mathcal{M}_{r\times n}(\mathbb{F}_q)$ is of full rank r. With obvious notation, letting $A = (A_1\, A_2)$, we get $e = (e_1, e_1 R) = X(A_1, A_2)$, yielding the system over $\mathbb{F}_{q^N}$:

$$(x_0, \ldots, x_{r-1})A_1 R = (x_0, \ldots, x_{r-1})A_2, \tag{1}$$

with unknowns $\alpha_{i,j}$, $x_0, \ldots, x_{r-1}$.

Let $\Omega = (\omega_0, \ldots, \omega_{N-1})$ be a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. We can express each x_i and each coefficient of R with respect to Ω. Doing so, system (1) can be rewritten as a system over $\mathbb{F}_q$. At this point Ourivski and Johannsson propose two strategies. The first one consists in guessing the unknowns $\alpha_{i,j}$ contributing to quadratic terms in the system, and then to solve the resulting linear system. This strategy is of complexity $O((rN)^3 q^{(r-1)(k+1)})$ The other strategy is very similar to the approach proposed by Stern and Chabaud in [1]: it consists in guessing a suitable basis X for e, and then to solve a linear system. The complexity is then $O((k+r)^3 r^3 q^{(N-r)(r-1)})$.

With L. Perret, we have done improvements of this algorithm, by considering a slightly modified system including the equations given by the syndrome of c, and using a Gröbner basis algorithm to solve it [7]. For small values of r, the practical results given by this approach are much better than those of Ourivski and Johannsson.

Finally, we present cryptographic applications of MR and RD: MR can serve as a tool for cryptanalysis in schemes like HFE [6] and TTM [4]; on the designing side, both problems are relevant for constructing authentication schemes [2, 3], but for encryption, the use of RD did not prove successful [9], whereas there has been no proposal for encryption based on MR. We end the talk with some open problems concerning the potential use of MR for solving coding theory problems, as well as about whether one can find a reduction proving the NP-completeness of RD.

References

[1] F. Chabaud, J. Stern, *The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes.* Proceedings of Asiacrypt'96, LNCS 1163, Springer-Verlag, pp.368-381, 1996.

[2] K. Chen, *A new identification algorithm.* Proceedings of the International Conference Cryptography: Policy and Algorithms, LNCS vol. 1029, Springer-Verlag, 1996.

[3] N. Courtois, *Efficient Zero-knowledge Authentication Scheme Based on a Linear Algebra Problem MinRank.* Proceedings of Asiacrypt'01, LNCS 2248, pp.402-421, Springer-Verlag, 2001.

[4] N. Courtois and L. Goubin, *Cryptanalysis of the* TTM *cryptosystem.* Advances in cryptology – Proceedings of Asiacrypt 2000", LNCS 1976, pp.44–57, Springer, 2000.

[5] V. Guruswami, A. Vardy. *Maximum Likelihood Decoding of Reed-Solomon Codes in NP-hard.* IEEE Transactions on Information Theory, Vol.51 No.7, pp-2249-2256, 2005.

[6] A. Kipnis and A. Shamir, *Cryptanalysis of the* HFE *public key cryptosystem by relinearization.* Advances in cryptology – Proceedings of Crypto 99, LNCS 1666, pp.19–30, Springer, 1999.

[7] F. Levy-dit-Vehel (joint work with L. Perret), *Algebraic Decoding of Rank Metric Codes.* Invited talk at the Special Semester on Gröbner Bases (Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics), RICAM, University of Linz, Austria, May 2006.

[8] A.V. Ourivski, T. Johansson, *New Techniques for Decoding Codes in Rank Metric and its Cryptogrphic Applications.* Problems of Information Transmission, vol.38 No.3, 2002, pp.237-246.

[9] R. Overbeck, *Structural attacks for Public-key Cryptosystems based on Gabidulin Codes.* Journal of Cryptology, to appear.

[10] J.O. Shallit, G.S. Frandsen, J.F. Buss, *The Computational Complexity of some Problems of Linear Algebra.* BRICS series report, Aarhus, Denmark, RS-96-33. (also at http://www.brics.dk/RS/96/33).

Eigenvalue bounds on the pseudocodeword weight of expander codes

Deepak Sridhara
(joint work with Christine A. Kelley)

Expander graphs are of fundamental interest in mathematics and engineering and have several applications in computer science, complexity theory, derandomization, designing communication networks, and coding theory [1]. In this talk, we focus on one prominent application of expander graphs – namely, the design of low-density parity-check (LDPC) codes. Low-density parity-check codes are a class of codes that can be represented on sparse graphs and have been shown to achieve record breaking performances with graph-based message-passing decoders. Graphs with good expansion properties are particularly suited for the decoder in dispersing messages to all nodes in the graph as quickly as possible. Expander codes are families of graph-based codes where the underlying graphs are expanders. That is, every element of the family is an expander and gives rise to an expander code. The codes are obtained by imposing code-constraints on the vertices (and possibly, edges) of the underlying expander graphs [2, 3, 4]. It has been observed that graphs with good expansion lead to LDPC codes with minimum distance growing linearly with the block length. In fact, one method of designing asymptotically good linear block codes is from expander graphs [2]. We refer to these expander-based LDPC codes as expander codes.

The popularity of LDPC codes is that they can be decoded with linear time complexity using graph-based message-passing decoders, thereby allowing for the use of large block length codes in several practical applications. In contrast, maximum-likelihood (ML) decoding a generic error-correcting code is known to be NP hard. A parameter that dominates the performance of a graph-based message passing decoder is the minimum pseudocodeword weight, in contrast to the minimum distance for an optimal (or, ML) decoder. The minimum pseudocodeword weight of the graph has been found to be a reasonable predictor of the performance of a finite-length LDPC code under graph-based message-passing decoding and also linear programming (LP) decoding [5, 6, 7].

In this talk, we consider four different ways of obtaining LDPC codes (or, expander codes) from expander graphs. For each case, we first present the known lower bounds on the minimum distance of expander codes based on the expansion properties of the underlying expander graph. We then extend the results to lower bound the minimum pseudocodeword weight on the binary symmetric channel (BSC). These bounds are useful in predicting the performance of expander codes under graph-based iterative decoding and linear programming decoding and also show that expander codes provide a guaranteed level of error-protection with iterative and LP decoding.

Some preliminary definitions followed by our main results on the pseudocodeword weight of expander codes are given below.

Definition 1. A *simple* LDPC code is defined by a bipartite graph G (also called, a Tanner graph) whose left vertices are called *variable* (or, *codebit*) nodes and whose right vertices are called *check* (or, *constraint*) nodes and the set of codewords are all binary assignments to the variable nodes such that at each check node, the modulo-two sum of the variable node assignments connected to the check node is zero, i.e., the parity-check constraint involving the neighboring variable nodes is satisfied.

Equivalently, the LDPC code can be described by a (binary) incidence matrix (or, parity-check matrix) wherein the rows of the matrix correspond to the constraint nodes of G and the columns correspond to variable nodes and there is a one in the matrix at a row-column entry whenever there is an edge between the corresponding constraint node and variable node in G. The LDPC code is in fact the null space of this parity-check matrix.

The above definition can be generalized by introducing more complex constraints instead of simple parity-check constraints at each constraint node, and the resulting LDPC code will be called a *generalized* LDPC code. A pseudocodeword of an LDPC Tanner graph G is defined as follows.

Definition 2. A finite degree ℓ *cover* of $G = (V, W; E)$ is a bipartite graph $\hat{G}$ where for each vertex $x_i \in V \cup W$, there is a *cloud* $\hat{X}_i = \{\hat{x}_{i_1}, \hat{x}_{i_2}, \ldots, \hat{x}_{i_\ell}\}$ of vertices in $\hat{G}$, with $deg(\hat{x}_{i_j}) = deg(x_i)$ for all $1 \leq j \leq \ell$, and for every $(x_i, x_j) \in E$, there are ℓ edges from $\hat{X}_i$ to $\hat{X}_j$ in $\hat{G}$ connected in a $1-1$ manner.

Definition 3. Suppose that $\hat{\mathbf{c}} = (\hat{c}_{1,1}, \hat{c}_{1,2}, \ldots, \hat{c}_{1,\ell}, \hat{c}_{2,1}, \ldots, \hat{c}_{2,\ell}, \ldots)$ is a codeword in the Tanner graph $\hat{G}$ representing a degree ℓ cover of G. Then a *pseudocodeword* $\mathbf{p}$ *of* G is a vector $(p_1, p_2, \ldots, p_n)$ obtained by reducing a codeword $\hat{\mathbf{c}}$, of the code in the cover graph $\hat{G}$, in the following way:

$$\hat{\mathbf{c}} = (\hat{c}_{1,1}, \ldots, \hat{c}_{1,\ell}, \hat{c}_{2,1}, \ldots, \hat{c}_{2,\ell}, \ldots) \rightarrow (\tfrac{\hat{c}_{1,1}+\hat{c}_{1,2}+\cdots+\hat{c}_{1,\ell}}{\ell}, \tfrac{\hat{c}_{2,1}+\hat{c}_{2,2}+\cdots+\hat{c}_{2,\ell}}{\ell}, \ldots) = (p_1, p_2, \ldots, p_n) = \mathbf{p},$$

where $p_i = \frac{\hat{c}_{i,1}+\hat{c}_{i,2}+\cdots+\hat{c}_{i,\ell}}{\ell}$.

From the above definition, it is easy to show that for a simple LDPC constraint graph G, a pseudocodeword $\mathbf{p} = (p_1, p_2, \ldots, p_n)$ is a vector that satisfies the following set of inequalities:

$$0 \leq p_i \leq 1, \quad \text{for } i = 1, 2, \ldots, n, \tag{1}$$

and further, if variable nodes i_1, i_2, …, i_d participate in a check node of degree d, then the pseudocodeword components satisfy

$$p_{i_j} \leq \sum_{k=1,2,..d, k \neq j} p_{i_k}, \text{ for } j = 1, 2, .., d. \tag{2}$$

Extending the above for generalized LDPC codes, it can similarly be shown that on a generalized LDPC constraint graph G, a pseudocodeword $\mathbf{p} = (p_1, p_2, \ldots, p_n)$

is a vector that satisfies the following set of inequalities:

$$0 \leq p_i \leq 1, \quad \text{for } i = 1, 2, \ldots, n, \tag{3}$$

and further, if variable nodes i_1, i_2, ..., i_d participate in a constraint node of degree d and that constraint node represents a subcode $[d, rd, \epsilon d]$, then the pseudocodeword components satisfy

$$(d\epsilon - 1)p_{i_j} \leq \sum_{k=1,2,..d,k\neq j} p_{i_k}, \text{ for } j = 1, 2, .., d. \tag{4}$$

The weight of a pseudocodeword $\mathbf{p}$ on the binary symmetric channel (BSC) is defined as follows [8].

Definition 4. Let e be the smallest number such that the sum of the e largest components of $\mathbf{p}$ is at least the sum of the remaining components of $\mathbf{p}$. Then, the BSC *pseudocodeword weight* of $\mathbf{p}$ is

$$w_{BSC}(\mathbf{p}) = \begin{cases} 2e, & \text{if } \sum_e \text{ largest } p_i = \sum_{\text{remaining}} p_i \\ 2e-1, & \text{if } \sum_e \text{ largest } p_i > \sum_{\text{remaining}} p_i \end{cases}$$

The *minimum BSC pseudocodeword weight* of an LDPC constraint graph G on the BSC is the minimum weight among all pseudocodewords obtainable from all finite-degree lifts of G. This parameter is denoted by $w_{\min}^{BSC}$. In this talk, we present lower bounds on $w_{\min}^{BSC}$ using the expansion properties of the underlying LDPC Tanner graph G for the following cases of expander codes.

Case 1:

Definition 5. Let $0 < \alpha < 1$ and $0 < \delta < 1$. A (c, d)-regular bipartite graph G with n degree c nodes on the left and m degree d nodes on the right is an $(\alpha n, \delta c)$ *expander* if for every subset U of degree c nodes such that $|U| < \alpha n$, the size of the set of neighbors of U, $|\Gamma(U)|$ is at least $\delta c|U|$.

For an LDPC code described by a Tanner graph G that is (c, d)-regular bipartite with n left vertices of degree c and m right vertices of degree d and that is also an $(\alpha n, \delta c)$ expander, we prove the following:

Theorem 1. *If $\delta > 2/3 + 1/3c$ such that δc is an integer, the LDPC code obtained from the $(\alpha n, \delta c)$ expander graph G as above has a pseudocodeword weight*

$$w_{\min}^{BSC} > \frac{2(\alpha n - 1)(3\delta - 2)}{(2\delta - 1)} - 1.$$

The proof involves combinatorial arguments such as Hall's matching theorem and is not a simple extension of the proof for lower bounding the minimum distance.

Case 2:
Suppose G is a d-regular graph and an[1] (n, d, μ) expander. Then, an LDPC code is obtained from G by interpreting the edges in G as variable nodes and the degree d vertices as constraint nodes imposing constraints of an $[d, rd, \epsilon d]$ linear block code. That is, the Tanner graph G' of the LDPC code is the edge-vertex incidence graph of G. The resulting LDPC code has block length $N = nd/2$ and rate $R \geq 2r - 1$. For such an LDPC code, we show the following lower bound on its minimum pseudocodeword weight, using combinatorial arguments as earlier.

Theorem 2. *The LDPC code obtained from an (n, d, μ) expander graph G has a minimum BSC pseudocodeword weight lower bounded as follows:*

$$w_{\min}^{BSC} \geq N\epsilon \frac{(\frac{\epsilon}{2} - \frac{\mu}{d})}{(1 - \frac{\mu}{d})}.$$

References

[1] N. Linial, A. Wigderson, *Expander graphs and their applications*, Lecture notes of a course given at the Hebrew University, 2003, available at *http://www.math.ias.edu/ avi/TALKS/*

[2] M. Sipser, D. A. Spielman, *Expander codes*, IEEE Trans. Inform. Theory, **42** (1996), 1710–1722.

[3] J. Lafferty, D. Rockmore, *Codes and iterative decoding on algebraic expander graphs*, "Proceedings of ISITA 2000," Honolulu, Hawaii, 2000, available at *http://www-2.cs.cmu.edu/afs/cs.cmu.edu/user/lafferty/www/pubs.html*

[4] H. Janwa, A. K. Lal, *On Tanner codes: Minimum distance and decoding*, in "Proceedings of AAECC," **13** (2003), 335–347.

[5] R. Koetter, P. O. Vontobel, *Graph-covers and iterative decoding of finite length codes*, "Proceedings of the 2003 Intl. Symposium on Turbo codes," Brest, France.

[6] C. Kelley, D. Sridhara, *Pseudocodewords of Tanner graphs*, to appear in the IEEE Trans. on Information Theory.

[7] J. Feldman, T. Malkin, R. A. Servedio, C. Stein and M. J. Wainwright, *LP decoding corrects a constant fraction of errors*, IEEE Transactions on Information Theory, **53** (2007) , 82–89.

[8] G. D. Forney, Jr., R. Koetter, F. Kschischang and A. Reznik, *On the effective weights of pseudocodewords for codes defined on graphs with cycles,* in "Codes, Systems and Graphical Models" (eds. B. Marcus and J. Rosenthal), Springer-Verlag, **123** (2001), 101–112.

[9] C. A. Kelley and D. Sridhara, *Eigenvalue bounds on the pseudocodeword weight of expander codes*, Advances in Mathematics of Communications, vol. 1, no. 3, pp. 287–307, Aug. 2007.

Coding-Theoretic Problems in Genetics: Superimposed Codes for Compressed Sensing DNA Microarrays

Olgica Milenkovic

(joint work with Wei Dai)

We consider the problem of algebraic construction of projection matrices for integer-valued compressed sensing DNA microarrays. In this context, we introduce a new family of codes, termed weighted Euclidean superimposed codes (WESCs).

[1] A simple, graph G is said to be a (n, d, μ) *expander* if G has n vertices, is d-regular, and the second largest eigenvalue of G (in absolute value) is μ.

This family generalizes the class of Euclidean superimposed codes, used in multiuser identification systems. WESCs allow for deterministic discrimination of bounded, integer-valued linear combinations of real-valued codewords, and can therefore also be seen as a specialization of compressed sensing schemes. We present lower and upper bounds on the largest size of a member of the WESCs family, and show how to use classical coding-theoretic and new compressed sensing analytical tools to devise low-complexity decoding algorithms for WESCs.

DNA microarrays are two-dimensional arrays of spots containing a large number of unique DNA identifiers placed on a solid substrate. The identifiers are short, single-stranded DNA sequences called *probes*. During the experiment, a solution of single-stranded target DNA sequences is poured over the DNA microarray. The *target* DNA sequences in the solution are labeled with fluorescent tags, and under appropriate experimental conditions, they bond (hybridize) with their complementary probes. Upon removal of the sequences in the solution that did not hybridized with any of the existing probes, and upon measuring the intensity of fluorescence of each spot, one can estimate the concentration of target DNA sequences.

This traditional approach to DNA microarray design and testing has a major shortcoming. Very frequently, the probes are considerably under-utilized - i.e., although the number of potential DNA sequences is very large, the actual number of DNA sequences in a solution is relatively small [1]. Consequently, an efficient microarray design should explore the inherent *sparsity* in target DNA vectors in order to reduce the number of required array spots.

Compressed sensing (CS) is a new sampling method that is suitable for estimation and detection of sparse target signals. A signal is said to be K-sparse if it can be represented by only $K \ll N$ significant coefficients in some space of dimension N, where $N \gg K$ [2, 3]. When the signal is projected onto a properly chosen basis of the transform space, its accurate representation relies only on a small number of coefficients. Encoding of a K-sparse discrete-time signal $\mathbf{x}$ of dimension N is accomplished by computing a measurement vector $\mathbf{y}$ that consists of $m \ll N$ linear projections, $\mathbf{y} = \Phi\mathbf{x}$. Here, Φ represents an $m \times N$ matrix, usually over the field of real numbers. Consequently, the measured vector represents a linear combination of columns of the matrix Φ, with weights prescribed by the non-zero entries of the vector $\mathbf{x}$. Although the reconstruction of the signal $\mathbf{x} \in \mathbb{R}^N$ from the (possibly noisy) projections is an ill-posed problem, the prior knowledge of signal sparsity allows for accurate recovery of $\mathbf{x}$.

CS techniques can be explored for the design of a new DNA microarray technology, termed *compressed sensing (CS) DNA microarrays* [1]. In CS microarray experiments, the integer-valued vector $\mathbf{x}$ is sparse and has entries that correspond to the *number* of different RNA molecules in a cell's cytoplasm. Usually, the number of RNA macromolecules in a wild-type cell is used as the zero-level measurement, and deviations from this value (which can be both positive and negative, integer-valued) represent the actual measurement. Since the number of RNA molecules in a cell at any point in time is upper bounded due to energy constraints, and

due to intracellular space limitations, the deviations are assumed to be finite and relatively small compared to the number of different RNA types.

As a result, the CS DNA microarray probe-target affinity sensing matrix Φ has the following properties. First, its entries $\phi_{i,j}$ are required to lie in the interval $[0, 1]$, and second, its columns are required to have $||\cdot||_1$ or $||\cdot||_2$ norm equal to one. Along with the aforementioned assumption that $\mathbf{x}$ is integer-valued and sparse, the two constraints on Φ give rise to a new coding theoretic paradigm, termed weighted Euclidean Superimposed Codes (WESCs). We present upper and lower bounds on the achievable rates of WESCs that depend on the sparsity of the vector $\mathbf{x}$ and the range of integer-values t that its components can take. We also describe a simple, yet efficient, *correlation decoder* for WESCs and a code-construction method based on spherical codes.

References

[1] M. Sheikh, O. Milenkovic, and R. Baraniuk *Designing Compressive Sensing Microarrays*, Proceedings of the IEEE Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), St. Thomas, U.S. Virgin Islands (2007).

[2] D. Donoho, *Compressed sensing*, IEEE Transactions on Information Theory, **52** (2006), 1289–1306.

[3] E. Candes, J. Romberg, and T. Tao, *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information,* IEEE Transactions on Information Theory, **52** (2006), 489–509.

Coset decoding of two-point codes

Iwan Duursma

(joint work with Seung Kook Park)

Matthews [8] introduced two-point codes as a generalization of one-point codes. In some cases, the parameters of two-point codes are better than those of one-point codes.

Homma and Kim [4, 6, 5, 3] determined the actual minimum distance of two-point codes from Hermitian curves. The full statement of their result contains many cases that are proved in different papers. The proof extends a method for one-point codes introduced by Yang and Kumar [10].

Kirfel and Pellikaan [7] give a different and shorter proof for the minimum distance of Hermitian one-point codes. In his thesis, Seung Kook Park [9] extends that method to Hermitian two-point codes. His result is a one line formula for the actual minimum distance of Hermitian two-point codes and a shorter proof. Moreover, the proof translates into a decoding algorithm for decoding up to half the actual distance.

The method applies to two-point codes in general. For this we introduce the notion of a discrepancy which generalizes the notion of a nongap. Discrepancies are defined for a choice of a curve together with two distinct points on the curve. We illustrate the methods with constructions of linear secret sharing schemes for multi-party computation [2], [1].

1. Discrepancies

In this section, we define the discrepancies of two points on a curve, which is one of the main tools for obtaining our results.

Let X be an algebraic curve (absolutely irreducible, smooth, projective) of genus g over a finite field $\mathbb{F}_3$ and let $\mathbb{F}_3(X)$ be the function field of X over $\mathbb{F}_3$. Let P_∞ and P_0 be two distinct rational points on X. For $f \in \mathbb{F}_3(X)\backslash\{0\}$, $(f)_\infty$ denotes the pole divisor of f, $(f)_0$ the zero divisor of f and $(f) = (f)_0 - (f)_\infty$ the divisor of f. Given a divisor G on X defined over $\mathbb{F}_3$, let $L(G)$ denote the vector space over $\mathbb{F}_3$ consisting of functions $f \in \mathbb{F}_3(X)\backslash\{0\}$ with $(f) + G \geq 0$ and the zero function. Let $l(G)$ denote the dimension of $L(G)$ as an $\mathbb{F}_3$-vector space. When G is of the form $aP_\infty + bP_0$ then the functions in $L(G)$ have poles only at P_∞ or at P_0, of order at most a or b, respectively. For the rational function field $\mathbb{F}_3(x)$ let P_∞ be the simple pole of x and P_0 the simple zero of x. Then, for $a, b \geq 0$, $L(aP_\infty + bP_0) = \langle x^{-b}, \ldots, x^a \rangle$ is of dimension $a + b + 1$. For an arbitrary function field, we aim to describe the dimension of $L(aP_\infty + bP_0)$, for $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. We will do this by defining a permutation $\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $\dim L(aP_\infty + bP_0) = |\{n \in \mathbb{Z} : n \leq a, \sigma(n) \leq b\}|$.

For a given $a \in \mathbb{Z}$, let $b \in \mathbb{Z}$ be minimal such that there exists

$$f \in L(aP_\infty + bP_0)\backslash L((a-1)P_\infty + bP_0).$$

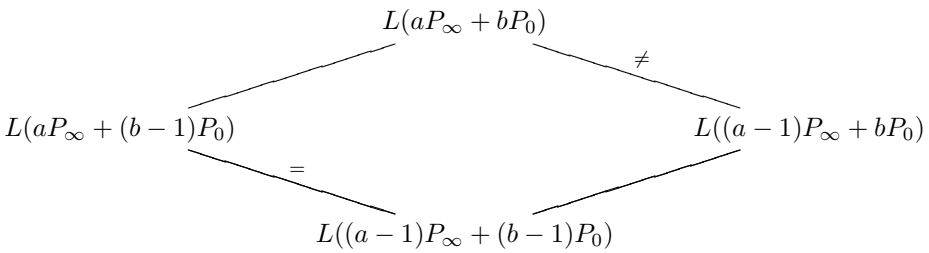
Then

$$L(aP_\infty + bP_0) \neq L((a-1)P_\infty + bP_0) \tag{1}$$

and, by minimality of b,

$$L(aP_\infty + (b-1)P_0) = L((a-1)P_\infty + (b-1)P_0). \tag{2}$$

The number b is uniquely determined by the properties (1) and (2). We have the following diagram:



From the diagram we conclude that

$$L(aP_\infty + bP_0) \neq L(aP_\infty + (b-1)P_0) \tag{3}$$

and

$$L((a-1)P_\infty + bP_0) = L((a-1)P_\infty + (b-1)P_0). \tag{4}$$

Together, properties (3) and (4) are equivalent to the properties (1) and (2). They express that a is minimal such that there exists

$$f \in L(aP_\infty + bP_0) \backslash L(aP_\infty + (b-1)P_0).$$

(Defintion) For a given $a \in \mathbb{Z}$, let $b \in \mathbb{Z}$ be such that

$$L(aP_\infty + bP_0) \neq L((a-1)P_\infty + bP_0)$$

and

$$L(aP_\infty + (b-1)P_0) = L((a-1)P_\infty + (b-1)P_0).$$

We call the ordered pair (a, b) a discrepancy pair. Let $\Gamma \subset \mathbb{Z} \times \mathbb{Z}$ be the set of all the discrepancy pairs.

The uniqueness of a and b in a discrepancy pair (a, b) shows that Γ is the graph of a permutation $\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $\sigma(a) = b$. Let $m > 0$ be minimal such that $m(P_0 - P_\infty)$ is a principal divisor, and let h be a function with $(h) = mP_0 - mP_\infty$. Then $(a, b) \in \Gamma$ if and only if $(a + m, b - m) \in \Gamma$. The permutation σ is completely determined by its images on a set of representatives for the integers modulo m.

References

[1] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *CRYPTO*, pages 521–536, 2006.

[2] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 316–334. Springer, Berlin, 2000.

[3] Masaaki Homma and Seon Jeong Kim. Toward the determination of the minimum distance of two-point codes on a Hermitian curve. *Des. Codes Cryptogr.*, 37(1):111–132, 2005.

[4] Masaaki Homma and Seon Jeong Kim. The complete determination of the minimum distance of two-point codes on a Hermitian curve. *Des. Codes Cryptogr.*, 40(1):5–24, 2006.

[5] Masaaki Homma and Seon Jeong Kim. The two-point codes on a Hermitian curve with the designed minimum distance. *Des. Codes Cryptogr.*, 38(1):55–81, 2006.

[6] Masaaki Homma and Seon Jeong Kim. The two-point codes with the designed distance on a Hermitian curve in even characteristic. *Des. Codes Cryptogr.*, 39(3):375–386, 2006.

[7] Christoph Kirfel and Ruud Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory*, 41(6, part 1):1720–1732, 1995. Special issue on algebraic geometry codes.

[8] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Des. Codes Cryptogr.*, 22(2):107–121, 2001.

[9] Seung Kook Park. Applications of algebraic curves to cryptography, Thesis, University of Illinois at Urbana-Champaign. 2007.

[10] Kyeongcheol Yang and P. Vijay Kumar. On the true minimum distance of Hermitian codes. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 99–107. Springer, Berlin, 1992.

A voltage graph approach to the analysis of LDPC codes

Christine A. Kelley
(joint work with Judy L. Walker)

We consider a voltage graph viewpoint from topological graph theory wherein specific lifts of graphs are determined via "voltage assignments", i.e., assignments of elements of a so-called voltage group, to the edges of a base graph, thus making the lifting entirely algebraic. This algebraic characterization of lifts is a powerful tool for analyzing several graph properties of the resulting lifts using the properties of the base graph. In an entirely different context, various researchers have looked at constructing families of LDPC codes by taking random lifts of a specially chosen base graph, or "protograph", yielding the so-called "protograph codes" [1]. The idea exploited in these constructions is that the properties of the base graph may shed light on the properties of the covering graphs, and therefore on the resulting codes. Indeed, random lifts of graphs have been heavily studied. While these codes have exhibited good performance, many of these constructions appear adhoc and there is a lack of a mathematical theory in designing these graph-based codes. In this work, we aim to bridge this gap by unifying several different families of graph-based codes under one common framework—namely, codes on graphs arising as voltage graphs [2]. By using the tools of topological graph theory, we are able to better understand the properties of such codes.

An algebraic construction of specific covering spaces for graphs was introduced by Gross and Tucker in the 1970s [3]. Given a graph $X = (V_X, E_X)$ where each edge in X has a positive and negative orientation, a function α, called an *ordinary voltage assignment*, maps the positively oriented edges to elements from a chosen finite group G, called the *voltage group*. The negative orientation of each edge is assigned a voltage that is the inverse element of the voltage assigned to its positive orientation. The base graph X, together with the function α, is called an *ordinary voltage graph*. The values of α on the edges are referred to as *voltages*. A new graph X^α, called the *(right) derived graph*, is a degree $|G|$ lift of X and has vertex set $V_X \times G$ and edge set $E_X \times G$, where if (u, v) is a positively oriented edge in X with voltage $h \in G$, then there is an edge from (u, g) to (v, gh) in X^α for each $g \in G$.

In the case that the voltage group is the symmetric group S_n on n elements, one can also view the pair (X, α) as a *permutation voltage graph*. The *permutation derived graph* X^α has vertex set $V_X \times \{1, \ldots, n\}$ and edge set $E_X \times \{1, \ldots, n\}$. If $\pi \in S_n$ is a permutation voltage on the edge $e = (u, v)$ of X, then there is an edge from (u, i) to $(v, \pi(i))$ in X^α for $i = 1, 2, \ldots, n$. Note that X^α is a degree n lift of X rather than a degree $n!$ lift as it would be if viewed as an ordinary derived graph as discussed above.

For an edge e, let e^- and e^+ denote the negative and positive orientations, respectively, of e. A walk in the voltage graph X with voltage assignment α may be represented by the sequence of oriented edges as they are traversed, e.g. $W = e_1^{\sigma_1} e_2^{\sigma_2} \ldots e_n^{\sigma_n}$ where each σ_i is $+$ or $-$ and $e_1, \ldots, e_n$ are edges in G. In this

setting, the *net voltage* of the walk W is defined as the voltage group product of the voltages on the edges of W in the order and direction of the walk.

Voltage graphs have been successfully used to obtain many instances of graphs with extremal properties; see for example [4, 5, 6].

In this talk we explain how some popular families of quasi-cyclic LDPC codes can be interpreted as permutation voltage graphs in a straightforward manner, using the constructions in [7, 8] as examples. The Tanner graph of a TSF code [7] may be viewed as the derived graph arising from a permutation voltage assignment on the complete bipartite graph $K_{\ell,k}$ on ℓ right and k left nodes, where the voltage assignments come from the symmetric group S_m on m elements, and the voltages are permutation elements that yield the shifts as given in the construction. For example, the entry $I_{a^i b^j}$ in the parity-check matrix corresponds to the edge between the ith left node, $i = 0, \ldots, k-1$, and the jth right node, $j = 0, \ldots, \ell - 1$ in the base graph $K_{\ell,k}$ and has a voltage equal to a permutation element that yields a circulant shift of $a^i b^j \pmod m$. In a similar way, the array-based codes of [8] may be interpreted in this light.

In the following, we completely classify all submatrices, or equivalently, subgraphs, that generate cycles that must exist in the derived graph based on the structure of the base graph. We start by formalizing this notion of inevitable cycles suggested in [10] by introducing the term *abelian-forcing walk*.

A backtrackless, tailless closed walk W is *abelian-forcing* if for each edge in W, the number of traversals in the positive direction is the same as those in the negative direction.

Lemma 1. An abelian-forcing walk W on X has net voltage 0 for any voltage assignment α to any abelian voltage group G. Hence each lift W_g of W in X^α, for $g \in G$, is a cycle of length $|W|$.

We define U to be an *abelian-forcing graph* if there is an abelian-forcing walk on U which uses every edge of U.

For a graph X, we define a positive integer n to be an *abelian-inevitable cycle length* for X if, for every abelian group G and every voltage assignment α of G on X, the derived graph X^α must have a simple cycle of length n.

For the classification, we will need terminology for two main types of subgraphs. Define an (a, b, c)-*theta-graph*, denoted by $T(a, b, c)$, to be a graph consisting of two vertices v and w, each of degree three, that are connected to each other via three disjoint paths of (edge) lengths $a \geq 1$,$b \geq 1$, and $c \geq 1$, and define a $(a_1, a_2; b)$-*dumbbell graph*, denoted $D(a_1, a_2; b)$ to be a connected graph comprised of two edge-disjoint cycles of lengths $a_1 \geq 1$ and $a_2 \geq 1$ that are connected by a path of length $b \geq 0$. In the case that $b = 0$, we get a bouquet of two circles, which we refer to as a *degenerate* dumbbell graph.

The next result classifies the subgraphs that give rise to abelian inevitable cycles, namely the abelian-forcing graphs.

Theorem 1. If X has an abelian-forcing walk of length n, then n is an abelian-inevitable cycle length for X. In particular,

(1) if X has a subgraph isomorphic to $T(a, b, c)$ then $2(a+b+c)$ is an abelian-inevitable cycle length for X.
(2) If X has a subgraph isomorphic to $D(a_1, a_2; b)$ then $2(a_1 + a_2) + 4b$ is an abelian-inevitable cycle length for X.

Moreover, every abelian forcing walk arises from either a theta graph or a (possibly degenerate) dumbbell graph.

We can now generalize the observation by Exoo in [4] by the following:

Proposition 1. If there is an abelian-forcing walk of length n on X, then n is an abelian-inevitable cycle length for X. In particular, for every abelian voltage assignment α, the girth of X^α is at most

- $2(a + b + c)$ if X contains an (a, b, c)-theta graph.
- $2(a_1 + a_2) + 4b$ if X contains an $(a_1, a_2; b)$-dumbbell graph.

The utility of this voltage graph viewpoint may been seen when one analyzes the girth g of the Tanner graph of the TSF codes. The girth is the length of the smallest cycle in the graph, and is important as it measures the number of iterations of decoding for which the messages passed along the graph remain independent. Indeed, iterative decoding is optimal on cycle-free graphs. It was shown in [7] that the $[155, 64, 20]$ TSF code in Section III has girth 8 and, more generally, all codes in the family have girth at most 12. The base graphs in the TSF construction all contain the complete bipartite graph $K_{2,3}$ as a subgraph, and $K_{2,3}$ is the theta graph $T(2, 2, 2)$. Thus, Proposition 1 immediately gives that the girth of the Tanner graphs of the TSF codes is at most 12.

We note that Theorem 4 in [9] is incorrect; the proof assumes the overlaps are consecutive although the statement does not. Since Theorems 1 and 3 in [10] rely on this result, they are incorrect as well. We now give a correct version of Theorem 3 of [10]:

Theorem 2. Let X be a graph of girth g. Then every abelian-inevitable cycle length for X is at least $3g$.

We are currently applying this voltage-graph analysis to understand other properties of the derived graphs and their implications for the resulting graph-based codes. Simultaneously, we are investigating constructions of LDPC codes by specific voltage assignments. We are considering both the application of one voltage group to a sequence of base graphs and also the use of a tower of groups as voltage groups applied to a specific base graph to generate these families of LDPC codes. The techniques may yield new codes as well as improve existing constructions. Our preliminary results suggest that using appropriate non-abelian groups for the voltage assignments may yield superior codes. This novel voltage graph approach is not limited to LDPC codes; rather, it can be applied in the algebraic design

of other graph-based codes such as turbo codes, repeat-accumulate codes, serial-concatenated codes, etc. Indeed, some constructions of repeat accumulate codes have offset functions that can be related to the voltage assignment function.

References

[1] J. Thorpe, "LDPC codes constructed from protographs", *IPN progress report*, pp. 42-154, JPL, August 2003.

[2] C. Kelley and J. Walker, "On LDPC codes from voltage graphs", in *Special Session on Algebraic Coding Theory, AMS meeting,* Oct. 2007.

[3] J.L. Gross and T.W. Tucker, *Topological graph theory*, Wiley, NY, 1987.

[4] G. Exoo, "Voltage graphs, group presentations, and cages", *The Electronic Journal of Combinatorics*, vol. 11(1), 2004.

[5] L. Brankovic, M. Miller, J. Plesnik, J. Ryan, and J. Siran, "Large graphs with small degree and diameter: A voltage assignment approach", *Jrnl. of Combinatorial Math. and Combinatorial Computing*, vol. 24, pp. 161-176, 1997.

[6] L. Brankovic, M. Miller, J. Plesnik, J. Ryan, and J. Siran, "A note on constructing large Cayley graphs of given degree and diameter by voltage assignments", *Elec. Jrnl. of Combinatorics*, vol. 5, no. 1, R9, 1998.

[7] R. M. Tanner, D. Sridhara, and T. E. Fuja, "A class of group-structured LDPC codes", in *Proc. of Intl. Symp. on Communication Theory and Applications*, Ambleside, U.K., pp. 365–370, July 2001.

[8] J. L. Fan, "Array codes as low-density parity-check codes", in *Proceedings of the 2nd International Symposium on Turbo Codes and their applications*, Brest, France, Sept. 2000, pp. 543–546.

[9] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding", *IEEE Trans. on Info. Theory*, vol. 51, no. 8, pp. 2894-2901, Aug. 2005.

[10] S. Kim, J-S. No, H. Chung, and D-J. Shin, "Construction of protographs for QC-LDPC codes with girth larger than 12", *Proc. of IEEE Intl. Symp. on Info. Theory*, pp.2256-2260, June 2007.

Nonadditive Quantum Codes from $\mathbb{Z}_4$-Codes

Patrick Solé

(joint work with San Ling)

In the present work, we construct binary non additive quantum codes from binary $\mathbb{Z}_4$-linear codes. The argument is based on a description of quantum codes in terms of orthogonal arrays [1],combined with Delsarte celebrated theorem on the equivalence of unrestricted (viz not necessarily linear) codes with given dual distance and orthogonal arrays of given strength [2].

References

[1] K. Feng, S. Ling & C. Xing, Asymptotic bounds on quantum codes from algebraic geometry codes, *IEEE Trans. Inform. Theory*, **5**2, no. 3 (2006), 986 – 991

[2] Delsarte, Philippe, *Four fundamental parameters of a code and their combinatorial significance*. Information and Control **23** (1973), 407–438.

A direct approach to LP-bounds

Jürgen Bierbrauer

Based on a self-contained account of the classical linear programming bounds for codes and orthogonal arrays we give an elementary description of the linear programming bounds for ordered codes, ordered orthogonal arrays (OOA) and tms-nets. The latter were introduced by Niederreiter in the context of uniform distribution and numerical integration. They live in an association scheme (Niederreiter-Rosenbloom-Tsfasman space) which generalizes the Hamming scheme. The main result is a description in terms of a family of polynomials which generalize the Krawtchouk polynomials of coding theory. The Plotkin bound and the sphere packing (Rao) bound for ordered codes are consequences. We also derive a quadratic bound and illustrate by giving some improvements on the parameter bounds for tms-nets. Now that a polynomial description of the LP-bound in NRT-space is available one may attack various problems, for example the classification of perfect codes (the case of equality in the sphere packing bound is described by a Lloyd polynomial) and MDS-codes. Further parameters of tms-nets may be excluded by using polynomials of small constant degree.

References

[1] J. Bierbrauer, *A direct approach to linear programming bounds for codes and tms-nets*, Designs, Codes and Cryptography **42** (2007), 127–143.

Some Observations on the Continued Fraction of $\sqrt{N}$ and Factorization

Michele Elia

The factorization of a composite integer N is a problem of great importance for many theoretical and practical reasons. Several factoring methods are based on properties of the continued fraction of $\sqrt{N}$, a subject-matter that has received great attention, although many properties are still unproved, and many more may remain to be discovered.

The continued fraction expansion of $\sqrt{N}$ is periodic with period τ, and is denoted as

$$\sqrt{N} = \{a_0, \overline{a_1, a_2, \cdots, a_{\tau-2}, a_{\tau-1}, 2a_0}\}$$

where the overbar identifies the periodic part. Within a period, the coefficients a_j satisfy a condition of symmetry $a_i = a_{\tau-i}$ for $1 \le i \le t-1$. The fractions of the sequence

$$\frac{A_0}{B_0} = \frac{a_0}{1}, \frac{A_1}{B_1} = \frac{a_0a_1+1}{a_1}, \frac{A_2}{B_2} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1}, \ldots, \frac{A_n}{B_n}, \ldots$$

are called convergents; numerators and denominators satisfy the recurrences

$$\begin{cases} A_j = a_jA_{j-1} + A_{j-2} \\ B_j = a_jB_{j-1} + B_{j-2} \quad \forall j \ge 2\ , \end{cases}$$

with initial conditions $A_0 = a_0$, $B_0 = 1$, and $A_1 = a_0a_1 + 1$, $B_1 = a_1$. Given a sequence of convergent, we may define two sequences, $\Delta_j = A_j^2 - NB_j^2$ and $\Omega_j = A_jA_{j-1} - NB_jB_{j-1}$, which have the following properties:

(1) Δ_j is a norm element in $\mathbb{Q}(\sqrt{N})$.
(2) $|\Delta_j| < 2\sqrt{N}$ and $|\Omega_j| < \sqrt{N}$ for every $j \geq 1$.
(3) For a given $|a| < \sqrt{N}$, the Diophantine equation $X^2 - NY^2 = a$ is solvable if and only if $a = \Delta_j$ for some j, [1, 3].
(4) The sequence Δ_j is periodic with with period τ, and within a period it satisfies the symmetry condition $\Delta_{\tau-j-2} = \Delta_j$ for $1 \leq j \leq \tau - 3$.
(5) The sequence Ω_j is periodic with period τ, and within a period it satisfies the symmetry condition $\Omega_{\tau-j-1} = (-1)^{\tau-1}\Omega_j$ for $1 \leq j \leq \tau - 2$.
(6) $\Delta_{\tau-1} = (-1)^{\tau}$, thus $A_{\tau-1} + \sqrt{N}B_{\tau-1}$ is a unit in $\mathbb{Q}(\sqrt{N})$.
(7) The matrix
$$M_{\tau-1} = \begin{bmatrix} -A_{\tau-1} & NB_{\tau-1} \\ -B_{\tau-1} & A_{\tau-1} \end{bmatrix}$$
is involutory, that is $M_{\tau-1}^2 = I$, with eigenvalues ± 1 if $\Delta_{\tau-1} = 1$, or neg-involutory, that is $M_{\tau-1}^2 = -I$, with eigenvalues $\pm i$ if $\Delta_{\tau-1} = -1$.
(8) The sequences Δ_m and Ω_m satisfy the following recurrent relations
$$\begin{cases} \Delta_{m+1} = \Delta_{m-1} + a_{m+1}(\Omega_{m+1} + \Omega_m) \\ \Omega_{m+1} = \Omega_m + a_{m+1}\Delta_m \end{cases}$$

Assuming $\Delta_{\tau-1} = 1$, thus τ is even, an eigenvector of $M_{\tau-1}$ associated to the eigenvalue 1 is $[A_{\tau-1} - 1, B_{\tau-1}]^T$, and denoting with d the greatest common divisor of $A_{\tau-1} - 1$ and $B_{\tau-1}$, it is immediately clear that numerator and denominator of the $(\frac{\tau}{2} - 1)$-th convergent are $A_{\tau/2-1} = \frac{A_{\tau-1}-1}{d}$ and $B_{\tau/2-1} = \frac{B_{\tau-1}}{d}$.
Let N be a square-free composite integer, and let $\mathfrak{u} = u_0 + \sqrt{N}u_1$ be the fundamental unit in $\mathbb{Q}(\sqrt{N})$ of positive norm 1. We say that $\mathfrak{u}$ splits N whenever $u_0 + 1$ and $u_0 - 1$ are divisible by some proper factors m_1 and m_2 of $N = m_1m_2$. In particular, $\mathfrak{u}$ splits $N = pq$, when p is a factor of $u_0 + 1$ and q is a factor of $u_0 - 1$, or conversely. The following theorem is thus proved [4].

Theorem 1. *If the norm of the fundamental unit $\mathfrak{u} \in \mathbb{Q}(\sqrt{N})$ is 1, and some factor of N is a square of a principal integral ideal in $Q(\sqrt{N})$, then $\mathfrak{u}$ splits N.*

Corollary 1. *Under the same assumptions as the Theorem, the smaller of the two factors of $N = pq$ is a factor of $\Delta_{\tau/2-1} = A_{\tau/2-1}^2 - NB_{\tau/2-1}^2$. In particular, if p and q are congruent* 3 mod 4*, with $p < q$, then $\Delta_{\tau/2-1} = (q|p)p$, where $(q|p)$ is the Legendre symbol.*

Using properties of convergent and related sequences, it is possible to show that the infrastructure method of Shanks [2] can be applied to the sequence Δ_j. Thus big and small jumps can be made up and down along the sequence. Therefore, if the period τ is known, the element $\Delta_{\tau/2-1}$ can be reached with a number of steps of the order $O(\log N)$, a result that implies the factorization of N in deterministic polynomial time.

In conclusion, two interesting problems arise naturally:

1), (old): *Is it possible to compute exactly or approximately, with an imprecision of the order $O((\log \tau)^{\alpha_1})$, the period τ from N in deterministic polynomial time $O((\log \tau)^{\alpha_2})$?*

2), (possibly new): *Given an ordered set $\mathcal{A}_t$ of $t+1$ pairs*

$$(\Delta_m, \Omega_m)\ , (\Delta_{m+1}, \Omega_{m+1})\ , \ldots , (\Delta_{m+t}, \Omega_{m+t})\ ,$$

with t small, is there any criterion for deciding whether $\mathcal{A}_t$ lies either in the first or in the second middle part of the period in deterministic polynomial time $O((\log N)^{\alpha_3})$?

References

[1] Hua Loo Keng, *Introduction to Number Theory*, New York: Springer, 1981.
[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, Berlin, 1993.
[3] W. Sierpinski, *Elementary Theory of Numbers*, North Holland, New York, 1988.
[4] M. Elia, *Relative Densities of Ramified Primes in* $\mathbb{Q}(\sqrt{pq})$, to appear on International Mathematical Forum, 2008.

Computing the minimum Lee weight of the $\mathbb{Z}_4$-linear Quadratic Residue Codes of length 72 and 80

Alfred Wassermann
(joint work with Michael Kiermaier)

The quadratic residue codes over the integers modulo 4 contain codes of high minimum Lee distance [3]. Via the Gray map, these codes can be transformed into nonlinear binary codes of double length. So it is possible to compare the Gray images with classical binary linear codes.

By computer search we revealed that the Lee weight of the quadratic residue code $QR(72)$ of length 72 and dimension 36 over the ring $\mathbb{Z}_4$ is equal to 22 and the Lee weight of the quadratic residue code $QR(80)$ of length 80 and dimension 40 over the ring $\mathbb{Z}_4$ is equal to 26.

The currently best known binary linear $[144, 72]$ code has minimum Hamming distance 22 and the best known self-dual binary linear code has minimum Hamming distance 20, see [6]. The currently best known binary linear $[160, 80]$ code is a self-dual code with minimum Hamming distance 24, see [5].

	$\mathbb{Z}_4$-code		Best known binary code	
	n	Lee weight	n	Hamming weight
$\mathbb{Z}_4$-QR-code:	72	22	144	22
$\mathbb{Z}_4$-QR-code:	80	26	160	24

We computed the minimum Lee weight of these codes by an adaption of the well known algorithm for the binary case, see [2] and [1, pp. 70–77]. In order to compute the Lee weight, the $\mathbb{Z}_4$-code is projected to its binary image. For this

projected code we enumerate all necessary codewords as described in [1, pp. 70–77], and compute their Hamming weight. Further, for each of these codewords the possible liftings of the coordinates to $\mathbb{Z}_4$ has to be tested.

The running time on a standard computer of the algorithm was below 5 minutes on the QR-code of length 72 and below 4 hours for the QR-code of length 80. For the code of length 72 the computation of the minimum Lee weight with the computer algebra system MAGMA, version 2.13, [4], was stopped after 10 hours without producing a result.

References

[1] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-correcting linear codes*, Heidelberg: Springer-Verlag, (2006).

[2] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann, *Codierungstheorie – Konstruktion und Anwendung linearer Codes*. Heidelberg: Springer-Verlag, (1998).

[3] A. Bonnecaze, P. Solé, A. R. Calderbank, *Quaternary Quadratic Residue Codes and Unimodular Lattices*, IEEE Transactions on Information Theory, **41**, 2 (1995), 366–377.

[4] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput., 24(3-4):235-265, (1997).

[5] M. van Dijk, S. Egner, M. Greferath, and A. Wassermann, *On two doubly even self-dual binary codes of length 160 and minimum weight 24*, IEEE Transactions on Information Theory, **51**, 1 (2005), 408–410.

[6] M. Grassl, *http://www.codetables.de*

Multivariate Interpolation Decoding: Reaching the Ultimate Limit of List Error-Correction

Alexander Vardy

One of the central questions in coding theory is this: what is the largest possible fraction of errors that a code of rate R can correct? We consider the case of adversarial errors, with error-correction defined in the list-decoding sense. Due to a series of groundbreaking papers in the past decade, we now have a complete answer to this question: the ultimate error-correction radius of $1 - R$ can be reached and, moreover, it can be reached constructively with polynomial-time decoding.

It was recognized early on [4] that decoding Reed-Solomon codes is equivalent to the problem of reconstructing *univariate polynomials* from their noisy evaluations. In the late 1990s, Sudan [6] and Guruswami-Sudan [2] came up with the idea of list-decoding Reed-Solomon codes using *bivariate polynomial interpolation*. List decoding means that a decoder produces a small (often, constant-size) list of codewords that, hopefully, contains the codeword that was transmitted. Guruswami and Sudan [2] proved that this will always happen if the fraction of errors is bounded by $\tau_{\rm GS} = 1 - \sqrt{R}$. This is strictly more than the classical decoding radius $\tau_{\rm RS} = (1 - R)/2$, for all rates. The algorithm of [2] was further extended to *algebraic soft-decision decoding* of Reed-Solomon codes by Koetter and Vardy [3].

For a number of years, it was widely believed that the Guruswami-Sudan [2] decoding radius $\tau_{\rm GS} = 1 - \sqrt{R}$ might be the best possible. However, Parvaresh and

Vardy [5] showed that even more errors can be corrected. The work of [5] is based upon two key ideas: transition from bivariate to *multivariate interpolation* and encoding two or more *correlated polynomials* in each transmitted symbol. Specifically, while conventional Reed-Solomon codes can be described by the mapping $f(X) \mapsto \big(f(x_1), f(x_2), \ldots, f(x_n)\big)$, where $f(X) \in \mathbb{F}_q[X]$ is the message polynomial of degree $< k$, the (trivariate) Parvaresh-Vardy codes of [5] are described by the mapping:

$$(1) \qquad f(X) \;\longmapsto\; g(X) = \big(f(X)\big)^a \bmod e(X) \;\longmapsto\; \begin{array}{|c|c|c|c|} \hline f(x_1) & f(x_2) & \cdots & f(x_n) \\ \hline g(x_1) & g(x_2) & \cdots & g(x_n) \\ \hline \end{array}$$

where $e(X)$ is an arbitrary irreducible polynomial of degree k and a is a sufficiently large integer. The mapping (1) incurs a loss in rate, since of the two transmitted polynomials $f(X)$ and $g(X)$, only $f(X)$ carries information. Recently, Guruswami and Rudra [1] showed that $e(X)$ and a in (1) can be chosen in such a way that $g(X) = f(\gamma X)$, where γ is a primitive element of $\mathbb{F}_q$. This makes it possible to "fold" the Parvaresh-Vardy codes back into Reed-Solomon codes, and thereby recover the rate-loss inherent in (1). The final outcome of all this is the result claimed in the first paragraph: using the "folded Reed-Solomon" codes of [1], the error-correction radius of $1 - R$ can be reached. This achieves the information-theoretic limits on list error-correction for the entire range of rates $R \in [0, 1]$. This furthermore yields an improvement by a factor of two over conventional decoding algorithms for Reed-Solomon codes.

References

[1] V. Guruswami and A. Rudra, *Explicit capacity-achieving list-decodable codes*, Proceedings 38-th ACM Symposium on Theory of Computing (STOC), pp. 1–10, Seattle, WA., May 2006.

[2] V. Guruswami and M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometric codes*, IEEE Trans. Inform. Theory, **45** (1999), 1755–1764.

[3] R. Koetter and A. Vardy, *Algebraic soft-decision decoding of Reed-Solomon codes*, IEEE Tran. Inform. Theory, **49** (2003), 2809–2825.

[4] J.L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inform. Theory, **15** (1969), 122–127.

[5] F. Parvaresh and A. Vardy, *Correcting errors beyond the Guruswami-Sudan radius in polynomial time*, Proceedings 46-th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 285–294, Pittsburgh, PA., October 2005.

[6] M. Sudan, *Decoding of Reed-Solomon codes beyond the error correction bound*, J. Complexity, **12** (1997), 180–193.

A Rank-Metric Approach to Error Control in Random Network Coding

Frank R. Kschischang
(joint work with Danilo Silva, Ralf Koetter)

In random linear network coding [1, 2, 3], information is propagated in a communication network as fixed length packets of symbols drawn from a finite field $\mathbb{F}$. The collection of all such packets is a finite-dimensional vector space over $\mathbb{F}$, here called the "ambient space." When an intermediate node between the transmitter and receiver is granted a transmission opportunity, it sends a random $\mathbb{F}$-linear combination of the packets that it has so far received. The receiver collects these randomly combined packets and attempts to infer (e.g., by inversion of a linear system over $\mathbb{F}$) the message selected by the transmitter.

Such a scheme is highly sensitive to the injection of packets containing errors, as such corrupted packets may combine in the network with legitimate packets, causing widespread packet corruption. The problem of error control in random network coding is therefore of great interest.

In [4], a coding scheme was introduced in which the transmitter communicates a message by injecting into the network a basis of a subspace V of the ambient space from some suitable codebook $\mathcal{C}$ of spaces. The receiver gathers packets spanning some space U. A metric between subspaces is defined in which the distance $d(U, V)$ between two subspaces U and V of the ambient space is given as $d(U, V) = \dim(U + V) - \dim(U \cap V)$. Depending on the minimum distance between the distinct codewords of $\mathcal{C}$, correct decoding is possible when $d(U, V)$ is small enough.

Although this approach seems to be the appropriate abstraction of the error control problem in random network coding, one inherent difficulty is the absence of a natural group structure on the set of all subspaces of the ambient space. As a consequence, many of the powerful concepts of classical coding theory such as group codes and linear codes do not naturally extend to codes consisting of subspaces.

In this talk, we described the close relationship between subspace codes and codes for the rank metric. Codewords in rank metric codes are $n \times m$ matrices and the rank distance between two matrices is the rank of their difference. The rank metric was introduced in coding theory by Delsarte [5]. Codes for the rank metric were largely developed by Gabidulin [6] (see also [7]). An important feature of the coding theory for the rank metric is that it supports many of the powerful concepts and techniques of classical coding theory, such as linear and cyclic codes and corresponding decoding algorithms [6, 7, 8, 9].

In the talk we showed that codes in the rank metric can be naturally "lifted" to subspace codes in such a way that the rank distance between two codewords is reflected in the subspace distance between their lifted images. In particular, if u is an $n \times m$ codeword of a rank-metric code C over $\mathbb{F}$, then the "lifting" $\mathcal{I}(u)$ of u is the row space of the matrix $[I|u]$, where I is the $n \times n$ identity matrix. Clearly

$\mathcal{I}(u)$ is an n-dimensional subspace of $\mathbb{F}^{n+m}$. The "lifting" $\mathcal{I}(C)$ of a rank-metric code C is $\mathcal{I}(C) = \{\mathcal{I}(u) : u \in C\}$. Thus $\mathcal{I}(C)$ is a codebook of subspaces of $\mathbb{F}^{n+m}$.

If two matrices u, v are separated by a rank distance d_R, then it is easy to see that $\mathcal{I}(u)$ and $\mathcal{I}(v)$ are separated by a subspace distance $d = 2d_R$, i.e., the lifting construction is distance preserving. From this it immediately follows that the minimum subspace distance between codewords of $\mathcal{I}(C)$ is twice the minimum rank distance between codewords of C. Good rank-metric codes (and in particular, the maximum rank distance codes of Gabidulin) are therefore lifted to good subspace codes.

In the talk we also discussed the problem of decoding, and showed that the decoding problem for the random network coding channel (abstracted as the "operator channel" of [4]) can be reformulated as a (generalized) decoding problem for rank-metric codes, allowing many of the tools from the theory of rank-metric codes to be applied to random network coding. In this generalized decoding problem, the channel may supply partial information about the error in the form of erasures (knowledge of an error location but not its value) and *deviations* (knowledge of an error value but not its location).

For Gabidulin codes, an efficient decoding algorithm is proposed that can fully exploit the correction capability of the code; in particular, it can correct any pattern of ϵ errors, μ erasures and δ deviations provided $2\epsilon + \mu + \delta \leq d - 1$, where d is the minimum rank distance of the code.

The rank-metric approach thus provides a practical means to construct subspace codes and also to decode them.

References

[1] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, 29 June-4 July 2003, p. 442.

[2] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Allerton Conf. on Comm., Control, and Computing*, Monticello, IL, October 2003.

[3] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[4] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, 24-29 June 2007, pp. 791–795.

[5] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. of Comb. Theory. Series A*, vol. 25, pp. 226–241, 1978.

[6] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm*, vol. 21, no. 1, pp. 1–12, 1985.

[7] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inform. Theory*, vol. 37, pp. 328–336, 1991.

[8] G. Richter and S. Plass, "Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm," in *Proc. ITG Conf. on Source and Channel Coding*, Erlangen, Germany, January 2004.

[9] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Proc. 4th Int. Workshop on Coding and Cryptography*, 2005.

On a Method to Overcome the Draw-backs of Cycles in the Tanner graph of a Low-Density Parity-Check Code

Marcus Greferath

Introduction. Low-Density Parity-Check (LDPC) codes, although discovered early in the history of coding theory [2], have attracted the attention of many coding theorists during the recent years due to their rediscovery by MacKay [4]. They form a class of linear block codes that perform close to the Shannon limit and allow for efficient decoding using what are called belief propagation algorithms. The correctness of these algorithms goes back to Pearl [5] for the case that the codes in question possess a parity-check matrix whose Tanner graph is free of cycles. But also for codes not satisfying this requirement belief propagation decoding algorithms are used in spite of their (theoretical) incorrectness. Here they perform tolerably well but certain draw-backs occur that are attributed to cycles in the underlying Tanner graph. It has been shown in [1] that if the Tanner graph contains exactly one cycle, then these draw-backs can be compensated for. This does however not mean that belief propagation is proven to work correctly in the presence of a single cycle.

The project at hand seeks to overcome the effects of cycles by use of random processes that spare the assumption of independence of the distributions passed along the edges of the graph in the decoding algorithm. In the context at hand we focus on what is called the *sum-product* algorithm which allows for a particularly elegant modelling of the operations involved by random processes.

Related approaches, particularly in the framework of what is called *stochastic computing*, have been introduced in [6].

The underlying Algebra. Let R be an arbitrary finite ring with identity, and denote by $\Delta(R)$ the set of all distributions on R, i.e. the set of all function $f : R \longrightarrow [0,1]$ such that $\sum_{r\in R} f(r) = 1$. The operations in R are naturally extended to operations on $\Delta(R)$: in fact we obtain two types of convolutions, the *additive* and the *multiplicative* convolution which we define as follows:

$$(f \oplus g)(x) \;:=\; \sum_{a+b=x} f(a)g(b) \quad \text{and} \quad (f \otimes g)(x) \;:=\; \sum_{ab=x} f(a)g(b).$$

Abbreviating

$$\delta_U(x) \;:=\; \begin{cases} \frac{1}{|U|} & : \text{ if } x \in U, \\ 0 & : \text{ otherwise,} \end{cases}$$

(and allowing for abuses of notation) we find that $(\Delta(R), \oplus, \delta_0)$ and $(\Delta(R), \otimes, \delta_1)$ both form monoids, where the former is abelian. There are no general distributive laws for elements of $\Delta(R)$, however we find that $\delta_r \otimes (f \oplus g) = (\delta_r \otimes f) \oplus (\delta_r \otimes g)$ for all $r \in R$ and $f, g \in \Delta(R)$. An according law holds for multiplication on the right hand side. All in all $\Delta(R)$ turns out to be an *R-bi-semi-module*, by which we summarize the following statements:

(i) $(\Delta(R), \oplus, \delta_0)$ is an abelian monoid.
(ii) There is an action $R \times \Delta(R) \longrightarrow \Delta(R)$ defined by $(r, f) \mapsto rf := \delta_r \otimes f$ such that all $r \in R$ induce an endomorphism $(r, \cdot)$ on $\Delta(R)$.
(iii) The same as **(ii)** on the right hand side of $\Delta(R)$.
(iv) $r(fs) = (rf)s$ for all $r, s \in R$ and $f \in \Delta(R)$.

In addition to what we have observed we introduce the following left division mapping $R \times \Delta(R) \longrightarrow \Delta(R)$. For $r \in R$ and $f \in \Delta(R)$ we set

$$(r, f) \mapsto \frac{1}{r} f, \quad \text{where } (\frac{1}{r} f)(x) := \frac{1}{\sum_{y \in R} f(ry)} f(rx),$$

whenever the right hand side is defined. If not, we set $\frac{1}{r} f := \delta_R$, the uniform distribution. Note that division even by non-units of R is defined in this context.

The Sum-Product-Algorithm. Let C be a set the elements of which are called *checks*, and let S be a set of *sites*. Assume a low-density parity-check code with a $|C| \times |S|$-check matrix H is given. We can define an R-valued edge labelling of the complete bipartite graph on $C \cup S$. With the understanding to omit all zero-labelled edges we then arrive at H being an R-valued edge labelling for the Tanner graph G of the matrix in question.

Belief propagation decoding algorithms for this code proceed in the following fashion. The channel output is given by a vector $y \in \Delta(R)^S$. Two sequences $(\mathrm{c2s}_n)_{n \in \mathbb{N}}$ and $(\mathrm{s2c}_n)_{n \in \mathbb{N}}$ of $\Delta(R)$-valued edge labellings of the graph G are defined according to three basic laws:

(I) $\mathrm{c2s}_0(e) := \delta_R$, the uniform distribution, and $\mathrm{s2c}_0(e) := y_{s(e)}$ for all $e \in E$.

(A) $\mathrm{c2s}_n(e) := \frac{1}{-H_e} \bigoplus_{\substack{f: f \neq e \\ c(e) \in f}} H_f \, \mathrm{s2c}_{n-1}(f)$

(B) $\mathrm{s2c}_n(e) := (1/\Sigma) \cdot y_{s(e)} \cdot \prod_{\substack{f: f \neq e \\ s(e) \in f}} \mathrm{c2s}_{n-1}(f)$. Here $\cdot$ and $\prod$ denote the pointwise product (aka *Hadamard product*), and $(1/\Sigma)$ is a normalisation ensuring $\mathrm{s2c}_n \in \Delta(R)$.

The labellings c2s are called *check-to-site* messages, whereas the labellings s2c are called *site-to-check* messages. If $\mathrm{s2c}_n(e)$ is not defined because of a division by 0, then we set $\mathrm{s2c}_n(e) := \delta_R$. In each step also a vertex labelling $u_n : S \longrightarrow \Delta(R)$ is defined as

$$u_n(s) := (1/\Sigma) \cdot y_s \cdot \prod_{e: s \in e} \mathrm{c2s}_{n-1}(e),$$

where $(1/\Sigma)$ is again a normalising factor. If G is a tree, the sequence of all u_n is known to converge towards an element $u \in \Delta(R)^S$ that under hard decision yields a word $x \in R^S$ minimising the symbol error probability. It is apparent that the tree condition on G ensures independence of the distributions appearing. If we understand these as the distributions of R-valued random variables, then step

(A) computes the distribution of a linear combination of these variables, whereas step **(B)** computes the (conditional) distribution that these variables coincide.

The proposed Random Processes. We propose to exchange passing of distributions by passing of values of the random variables that they represent. For this let the channel output again be given by $y \in \longrightarrow \Delta(R)^S$. Two sequences $(\mathrm{c2s}_n)_{n\in\mathbb{N}}$ and $(\mathrm{s2c}_n)_{n\in\mathbb{N}}$ of R-valued edge labellings of the graph G are defined according to three basic laws:

(I') $\mathrm{c2s}_0(e)$ is sampled according to δ_R, the uniform distribution, and $\mathrm{s2c}_0(e)$ is sampled according to $y_{s(e)}$ for all $e \in E$.

(A') Compute $Q(e) := -\sum_{\substack{f: f\neq e \\ c(e)\in f}} H_f\ \mathrm{s2c}_{n-1}(f)$ and sample $\mathrm{c2s}_n(e)$ from $\frac{1}{H_e}Q(e)$.

(B') Design $\mathrm{c2s}_n$ as follows: For $e \in E$ set $s := s(e)$ and sample $Q(s)$ according to y_s.

$$\mathrm{c2s}_n(e) := \begin{cases} \mathrm{c2s}_{n-1}(e) & : \text{ if } |\{Q(s)\} \cup \{\mathrm{s2c}_{n-1}(f) : f \neq e,\ s \in f\}| > 1 \\ Q(s) & : \text{ otherwise.} \end{cases}$$

Assuming that the $\mathrm{c2s}_n$ form a Markov process is in general weaker than the assumption that G is a tree. Under this assumption however the distribution of the variable c2s converges towards the desired conditional distribution introduced in **(B)**.

Similar to **(B')** an according rule can then be formulated for the update random variables $(u_n)_{n\in\mathbb{N}}$. The limit distribution of u_n is then expected to be an element $\Delta(R)^S$ that under hard decision yields a word R^S minimising the symbol error probability.

Discussion. We have given up the classical parallelism of message passing in order to assure convergence also in cases of graphs containing cycles. This step causes a significant performance loss and is therefore only of theoretical value. Our main idea however is based on the observation that the substituting sampling processes do not hinge on strict independence assumptions on the variables. We therefore envisage that this version of message passing will converge also for graphs that are not trees. It will be a question of further research to explore if a quantum version of this algorithm (i.e. a scheme that passes qudits instead of the original distributions along the edges of the graph) can be proven to work correctly for non-trees.

References

[1] Y. Weiss, *Correctness of local probability propagation in graphical models with loops*, Neural Comput. **12** (2000), 1–41.

[2] R. G. Gallager, *Low density parity check codes*, PhD Thesis, MIT press, Cambridge, MA, 1963.

[3] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, 2004.

[4] D. J. C.MacKay and R. M. Neal, *Good codes based on very sparse matrices*, in: Cryptography and Coding, 5th IMA Conference, 100–111, Dec. 1995.
[5] J. Pearl, *Probabilistic reasoning in intelligent systems: Networks of plausible inference*, Morgan Kaufmann, San Mateo, CA (1988).
[6] A. Rapley, C. Winstead, V. Gaudet, C. Schlegel, *Stochastic iterative decoding on factor graphs*, Proc. 3rd Int. Symp. on Turbo Codes and Related Topics 2003.
[7] N. Wiberg, *Codes and Decoding on General Graphs*, Dissertation, University of Link"oping (1996).

Hypergraph codes and their decoding

Gilles Zémor
(joint work with Alexander Barg)

Let $G = (V, E)$ be a balanced, Δ-regular bipartite graph with vertex set $V = V_1 \cup V_2, |V_1| = |V_2| = n$ and $|E| = N = \Delta n$ edges. Let us choose an arbitrary ordering of edges in E. For a given vertex $v \in V$ this defines an ordering of edges $v(1), v(2), \ldots, v(\Delta)$ incident to it. We denote this subset of edges by $E(v)$. Given a binary vector $x \in \{0,1\}^N$, let us establish a one-to-one correspondence between the coordinates of x and the edges in E. For a given vertex v let $x(v) = (x_e, e \in E(v))$ be the subvector that corresponds to the edges in $E(v)$.

Let $A[\Delta, R_0\Delta, d_0 = \delta_0\Delta]$ be a binary linear code of length Δ and rate $R_0 = \dim(A)/\Delta$. Define a *bipartite-graph code* as follows:

$$C(G; A) = \{x \in \{0,1\}^N : \forall_{v \in V_1 \cup V_2}\ x(v) \in A\}.$$

The rate of the code C is easily seen to satisfy

$$R(C) \geq 2R_0 - 1.$$

This construction (without the requirement that G be bipartite) was first introduced by Tanner [6]. It was shown by Sipser and Spielman [4] that choosing for G graphs with *expanding* properties yields constructive asymptotically good families of binary linear codes. The term "expander codes" was coined to highlight this result. More precisely, the distance of the code $C(G; A)$ can be estimated from below as follows [2]:

$$d/N \geq \delta_0^2\Big(1 - \frac{\lambda}{2d_0}\Big)^2 \tag{1}$$

where λ is the second eigenvalue of the graph G. In particular, if λ is small compared to d_0, then the relative distance $\delta = d/N$ is close to the value δ_0^2. Sipser and Spielman also showed that expander codes can decode adversarial errors up to a fraction of the designed distance with a low complexity iterative decoding algorithm. This fraction was raised to $1/4$ for bipartite-graph codes in [7] and improved again to $1/2$ in [5] and [2].

A number of variations to the bipartite construction have been introduced that yield a better rate/designed distance tradeoff, see [1]. An alternative approach to improve the designed distance was put forward in [3]. It consists of replacing the underlying bipartite graph by a t-partite, t-uniform, Δ-regular hypergraph with

vertex set $V = V_1 \cup \cdots \cup V_t$ where every edge is incident to exactly one vertex in V_i for every i. The definition of the t-partite hypergraph code is then the same as that of a bipartite-graph code. The rate R of the hypergraph code C is readily seen to satisfy

$$R \geq tR_0 - (t-1).$$

In [3], Bilu and Hoory generalize the expansion property to hypergraphs, provide constructions of hypergraphs with this property, and show that when it is satisfied the minimum distance of the corresponding hypergraph code satisfies

$$d/N \geq \delta_0^{\frac{t}{t-1}} - \epsilon \tag{2}$$

where ϵ is a quantity that can be made arbitrarily small by increasing the degree Δ of the hypergraph. Note that when A is a code of large rate and small δ_0, the lower bound (2) for $t > 2$ becomes much better than the bound (1) for bipartite-graph codes.

Decoding hypergraph codes is more challenging than decoding bipartite-graph codes, however. In [3] Bilu and Hoory give an algorithm for even values of t that is guaranteed to decode any pattern of eN errors with e less than

$$\binom{t-1}{t/2}^{-2/t} \left(\frac{\delta_0}{2}\right)^{(t+2)/t} - \epsilon \tag{3}$$

where, again, ϵ is a quantity that can be made arbitrarily small by increasing the degree Δ of the hypergraph. This algorithm consists of $\log N$ iterations, each of which has serial running time linear in the blocklength N.

The object of the present work is to improve on this fraction and get closer to half the designed minimum distance (2) with low-complexity iterative decoding. We obtain, neglecting ϵ-terms:

Theorem. *For any $\alpha > 0$, if the number of errors eN is such that*

$$e \leq (1-\alpha)\delta_0^{t/(t-1)} \min_{\kappa} \max_{\lambda} f(\lambda, \kappa)$$

with

$$f(\lambda, \kappa) = \frac{[1 - t(1-\lambda)/(\kappa - \lambda)]^{1/(t-1)}}{\kappa^{t/(t-1)}[\lambda + (1-\lambda)/(\kappa - 1)]^{t/(t-1)}}$$

they can be corrected in time $O(N \log N)$.

Numerically, the first values of the decoding radius ρ given by the Theorem are

$$\rho \geq \frac{\delta_0^{3/2}}{5.94} \text{ for } t = 3 \qquad \rho \geq \frac{\delta_0^{4/3}}{6.46} \text{ for } t = 4.$$

For fixed values of t, decoding up to half the designed distance efficiently is still an open problem.

References

[1] A. Barg and G. Zémor, *Distance properties of expander codes*, IEEE Trans. Inform. Theory **52** (2006), 78–90.

[2] A. Barg and G. Zémor, *Concatenated codes: serial and parallel*, IEEE Trans. Inform. Theory **51** (2005), 1625–1634.

[3] Y. Bilu and S. Hoory, *On codes from hypergraphs*, European Journal of Combinatorics **25** (2004), 339–354.

[4] M. Sipser and D. A. Spielman, *Expander Codes*, IEEE Trans. Inform. Theory **42** (1996), 1710–1722.

[5] V. Skachek, R. M. Roth, *Generalized minimum distance iterative decoding of expander codes*, Proceedings IEEE Information Theory Workshop, (2003) Paris, 245–248.

[6] M. Tanner, *A recursive approach to Low-complexity codes*, IEEE Trans. Inform. Theory **27** (1981), 533–547.

[7] G. Zémor, *On expander codes*, IEEE Trans. Inform. Theory **47** (2001), 835–837.

Crooked binomials

Jürgen Bierbrauer

(joint work with Gohar Kyureghyan)

Let $F = GF(q)$, where $q = 2^r$. A function $f : F \longrightarrow F$ is **almost perfectly nonlinear** (APN) if for every $0 \neq a \in F$ the additive derivative $\delta_{f,a}$ defined by $\delta_{f,a}(x) = f(x+a) + f(x)$ is two-to-one: it has $q/2$ different images (equivalently: each image has precisely two preimages).

The APN function f is **crooked** if for every a the image $\delta_{f,a}(F)$ is either a hyperplane or the complement of a hyperplane of F (seen as an r-dimensional vector space over $GF(2)$.

Motivation comes from information transmission (sequences with extremal autocorrelation properties), cryptography (S-boxes) and coding theory (cyclic codes, Preparata codes).

In the long paper [2] we prove that binomial functions $f(x) = x^d + ux^e$ can be crooked only if both exponents d, e have 2-weight ≤ 2. This generalizes the main result of [1] where it is proved that the only crooked power functions are the Gold functions. The proof of [2] uses the projection argument from [1] and makes extensive use of the action of the Galois group.

New crooked binomial functions were constructed in [3, 4, 5, 6]. In [7] succinct constructions are given for the known crooked binomials. They consist of an infinite family and one sporadic example. Here is a description of the infinite family.

Let $F = GF(q^k)$, where $q = 2^s$. Consider the trace and norm $T, N : F \longrightarrow GF(q)$, let $q' = 2^i$. Choose $\mu \in F$ such that $N(\mu) = 1$ and the function $f : F \longrightarrow F$ defined by

$$f(x) = x^{q'+1} + \mu x^{qq'+q^{k-1}}.$$

Theorem 1. The function $f(x)$ above is crooked when the following are satisfied:

- $r = ks, k \in \{3, 4\}$.
- The integers k, s, i are pairwise coprime and $k \mid i + s$.
- $\mu = \epsilon^e$, where ϵ is a primitive element of $F = GF(2^r), e$ is a multiple of $2^s - 1$ and coprime to $2^k - 1$.

The sporadic example is defined on $GF(2^{10})$. We construct it using the properties of a certain projective curve of genus 3 associated to it. There is numerical evidence for the conjecture that this describes all crooked binomial functions.

References

[1] G. M. Kyureghyan, *Crooked maps in $GF(2^n)$,*, Finite Fields and Their Applications, in press.

[2] J. Bierbrauer and Gohar Kyureghyan, *Crooked binomials*, Designs, Codes and Cryptography, in press.

[3] Y. Edel, G. Kyureghyan and A. Pott, *A new APN function which is not equivalent to a power mapping,* IEEE Transactions on Information Theory **52** (2006), 744–747.

[4] L. Budaghyan, C. Carlet, P. Felke, G. Leander, *An infinite class of quadratic APN functions which are not equivalent to power mappings*, Proceedings of the IEEE International Symposium on Information Theory 2006, Seattle.

[5] L. Budaghyan, C. Carlet, G. Leander, *A class of quadratic APN binomials inequivalent to power functions*, submitted.

[6] L. Budaghyan, C. Carlet, G. Leander, *Another class of quadratic APN binomials over $GF(2^n)$: the case n divisible by 4*,, manuscript.

[7] J. Bierbrauer, *A family of crooked functions*, Designs, Codes and Cryptography, submitted.

Multivariate generalizations of the Guruswami-Sudan decoding algorithm

Daniel Augot

It appears that the Guruswami-Sudan list decodign algorithm has not yet been properly analyzed in the multivariate case. By the multivariate case, it is meant that the codes under consideration are obtained by evaluation of multivariate polynomials over the points of the affine space $A^n(\mathbb{F}_q)$. The set of polynomials to be evaluated is either:

$$L = \{f(X_1, \ldots, X_N),\ \deg f(X_1, \ldots, X_N) \leq r\},$$

in which case are obtained the generalized Reed-Muller codes (for simplicity, we assume that $r < q$); or:

$$L = \{f(X_1, \ldots, X_N),\ \deg_{X_i} f(X_1, \ldots, X_N) \leq r; \quad i = 1, \ldots, N\},$$

in which case is obtained the N times product code of the classical Reed-Solomon code. Let us briefly sketch the algorithm for the Reed-Muller codes: Let τ be the number of errors that will be corrected, and $\mu = n^N - \tau$ be the number of positions with no errors. The received word, to be decoded, is a N -dimensional array $y = (y_{i_1,\ldots,i_N})_{(i_1,\ldots,i_N)\in\{1\ldots n\}^N}$. This algortithm is as follows, where wdeg denotes the weighted degree.

input: $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $r, \mu \in \mathbb{N}$, $y = (y_{i_1,\ldots,i_N})$ the received word.
auxiliary parameters: a degree d et s an order of multiplicity.
interpolation: find a polynomial $Q = Q(X_1, \ldots, X_N, Z)$ such that
(1) $Q(X_1, \ldots, X_N, Z) \neq 0$,
(2) $\mathrm{wdeg}_{1,\ldots,1,r} Q(X_1, \ldots, X_N, Z) \leq d$,
(3) $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_N}, y_{i_1,\ldots,i_N})) = s$, $(i_1 \ldots, i_N) \in \{1 \ldots n\}^N$.
factorisation: Compute $List = \{f = f(X_1, \ldots, X_N) \mid Q(X_1, \ldots, X_N, f) = 0\}$.
verification: return all $f \in L$ such that $\deg f \leq r$, et $d(f, y) < \tau$.

This generalization is straightforward, but the analysis can be done in various ways. All analyses are to be done in two steps: first ensuring that the $Q(X_1, \ldots, X_N, Z)$ is zero when evaluated over the solution which is sought for; then writing a sufficient condition for the existence of the $Q(X_1, \ldots, X_N, Z)$ polynomial, regardless of the received word.

Regarding this second condition, we require that, in the interpolation step, the number of unknowns is greater than the number of equations. Indeed, each condition $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_N}, y_{i_1,\ldots,i_N})) = s$ implies $\binom{s+N}{N+1}$ linear equations on the coefficients of Q. On the other hand, the number of unknowns is given by the condition $\mathrm{wdeg}_{1,\ldots,1,r} Q \leq d$. One can shows that this number is $\frac{d^{N+1}}{(N+1)!r}$, and a condition for the existence of the polynomial Q is

$$\frac{d^{N+1}}{(N+1)!r} > \binom{s+N}{N+1} n^N,$$

which can be simplified into

$$d > \sqrt[N+1]{n^N r s(s+1)\ldots(s+N)}. \tag{1}$$

For the first condition, to conclude that the polynomial $Q_f = Q(X_1, \ldots, X_N, f)$ is actually zero, we need to bound the number of zeros of such a polynomial. In the univariate case, this is simply achieved by using the fact that a polynomial can not have more zeroes than its degree. In the multivariate case, things are not as simple. A first analysis has been done by Pellikaan and Wu, using the theory of Groebner bases and the notion of the footprint of an ideal. They end up with the following radius:

$$\frac{\tau}{n^N} \leq \left(1 - \sqrt[N+1]{\frac{r}{n}}\right)^N. \tag{2}$$

However, one can settle a simpler Lemma, which is a generalization of the Schwartz-Zippel Lemma. Note also that it holds over any field.

Lemma 1. *Let $\mathbb{F}$ be an arbitray field. Let $Q(X_1, \ldots, X_N) \in \mathbb{F}[X_1, \ldots, X_N]$ be of total degree less than d. Let $x_1, \ldots, x_n$ be n distinct points in $\mathbb{F}$. The sum of multiplicities of $Q(X_1, \ldots, X_N)$ over the n^N points $\{(x_{i_1}, \ldots, x_{i_N});\ 1 \leq i_1 \leq n, \ldots, 1 \leq i_N \leq n\} \subset \mathbb{F}^N$ is less than or equal to dn^{N-1}.*

Proof. By induction. □

Thus, to ensure that the polynomial Q_f is identically zero, the parameters must be such that Q_f has more than dn^{N-1} zeros, counted with multiplicities. If $\mu = n^N - \tau$ denote the number of positions $(i_1, \ldots, i_n)$ such that $f(x_{i_1}, \ldots, x_{i_N}) = y_{i_1,\ldots,i_N}$, then if

$$s\mu > dn^{N-1}, \tag{3}$$

Q_f is identically zero. Working out the conditions (1) and (3) leads to the following bound for τ:

$$\tau \leq n^N - \sqrt[N+1]{rn^N(1+\frac{1}{s})\ldots(1+\frac{N}{s})}, \tag{4}$$

which gives the following relative decoding radius, when s tends to infinity:

$$\frac{\tau}{n^N} \leq 1 - \sqrt[N+1]{\frac{r}{n}}, \tag{5}$$

an improvement over the Pellikaan and Wu's radius.

But this is not the end of the story. Geil and Matsumoto, using the theory of order domains (which encompasses both algebraic-geometry codes and multivariate codes, as generalized Reed-Muller codes), could provide a Sudan-like algorithm (that is to say, without multiplicities), which, on examples, appears to have a larger decoding radius that what could be obtained using the Schwartz-Zippel Lemma. They appear to use the so-called hyperbolic codes, which are an improvement of the q-ary Reed-Muller codes, when $q > 2$. The remaining open problem is indroduce multiplicities in Geil and Matsumoto approach, which seems a difficult task since such a notion is not taken into consideration in the order domain theory.

To conclude, in the present state of knowledge, the best radius which can obtained is $n^M - \sqrt{n^M(n^M - d_M)}$, where d_M is the minimum distance of the Reed-Muller codes. This achieved by using an old result of Kasami, Lin and Peterson, which relates Generalized Reed-Muller codes to subfield subcodes of Reed-Solomon codes. This enables to decode the generalized Reed-Muller codes as classical Reed-Solomon codes, using the usual Guruswami-Sudan algorithm. Note that this radius coincides with the Johson bound in the q-ary case, when q is large enough.

References

[1] O. Geil and R. Matsumoto. *Generalized Sudan's list decoding algorithm for order domain codes*, in Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC), (2007).

[2] T. Kasami, Shu Lin, and W. Peterson. *New generalizations of the Reed-Muller codes–I: Primitive codes,* IEEE Transactions on Information Theory, **14(2)** (1968), 189–199.

[3] R. Pellikaan and X. W. Wu. *List decoding of q-ary Reed-Muller codes*, 2004, preprint available form authors, extended version of [4]

[4] R. Pellikaan and X. W. Wu. *List decoding of q-ary Reed-Muller codes*, IEEE Transactions on Information Theory, **50(4)** (2004), 679–682.

[5] J. T. Schwartz. *Fast probabilistic algorithms for verification of polynomial identities* Journal of the ACM, **27(4)** (1980), 701–717.

[6] R. Zippel. *Probabilistic algorithms for sparse polynomials* In Edward W. Ng, editor, *Symbolic and Algebraic Computation: EUROSM '79, An International Symposium on Symbolic and Algebraic Manipulation, Marseille, France, Lecture Notes in Computer Science***72** (1979), pages 216–226.

Quantum codes suitable for iterative decoding

Jean-Pierre Tillich
(joint work with Thomas Camara, Harold Ollivier, David Poulin)

The purpose of this talk is to discuss generalizations to the quantum setting of LDPC codes and turbo-codes. These generalizations use a construction of quantum error-correcting codes called "stabilizer codes" or "additive codes over $GF(4)$" [1, 3]. The quantum parity-check matrix of such a quantum code of length n and (quantum) dimension k consists of a $(n-k) \times n$ matrix with entries in $GF(4)$ and rows which are orthogonal with respect to the trace-hermitian inner product. The minimum distance of such a code is the smallest Hamming weight of a row-vector in $GF(4)^n$ which is orthogonal (again with respect to the trace-hermitian inner product) to all the rows of the parity-check matrix but which can not be expressed as a sum of these rows.

A quantum LDPC code is then nothing but a stabilizer code which admits a sparse parity-check matrix of this form. We review the attempts which have been made in this direction (semi-random constructions, quasi-cyclic constructions, group-theoretic constructions, combinatorial constructions using designs) [7, 4, 6, 2]. However, all these quantum LDPC codes have not yielded results as spectacular as their classical counterpart. This is due to several reasons. First there are issues with the code design. Due to the orthogonality constraints imposed on the parity-check matrix, it is much harder to construct quantum LDPC codes than classical ones. In particular, constructing the code at random will certainly not do. In fact, it is still unknown whether there exist families of quantum LDPC codes with non-vanishing rate and unbounded minimum distance and all known constructions seem to suffer from a poor minimum distance for reasons which are not always fully understood. Second, there are issues with the decoder. The Tanner graph associated to a quantum LDPC code necessarily contains many 4-cycles which are well known for their negative effect on the performances of iterative decoding. Moreover, quantum LDPC codes are by definition highly degenerate but their decoder does not exploit this property: rather it is impaired by it.

Generalizing turbo-codes to the quantum setting is a possible way to overcome these problems. In particular, it is possible to define quantum serial turbo-codes [8] in such a way that as for classical turbo-codes, there is complete freedom in choosing the interleaver. This allows to use random constructions as in the classical setting. For instance, it is known by using probabilistic arguments that in a classical serial turbo-code scheme, using an inner convolutional code that is recursive yields turbo-code families with unbounded minimum distance [5]. The generalization of

this result to the quantum setting requires to address encoding issues such that being recursive and not catastrophic for a convolutional encoder. We first recall how a certain binary matrix can be associated to the quantum encoding process and how this enables to define such notions like a quantum convolutional encoder, and properties such as being recursive and non catastrophic for this encoder. We show that despite the fact that both recursive encoders and non catastrophic encoders exist in the quantum setting, there are no encoders which meet these properties at the same time. This hinders obtaining quantum serial turbo-codes with good iterative decoding performances and polynomial minimal distance in the same way as classical serial turbo-codes. However, although it is still possible to construct interesting quantum serial turbo-codes from non-recursive and non-catastrophic encoders. They can be decoded in a similar fashion as classical turbo-codes and display good iterative decoding performance up to moderate block lengths even if they have bounded minimum distance.

References

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, 1997.

[2] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: construction and performances under iterative decoding," in *Proceedings of ISIT 2007*, Nice: IEEE, June 2007, pp. 811–815.

[3] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.

[4] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proceedings of ISIT 2007*, Nice: IEEE, June 2007, pp. 806–811.

[5] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE Int. Symp. Info. Theo. (ISIT'98)*, 1998, p. 31.

[6] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," in *Proceedings of Turbo-coding 2006*, Munich, April 2006.

[7] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse graph codes for quantum error-correction," *IEEE Trans. Info. Theor.*, vol. 50, no. 10, pp. 2315–2330, 2004.

[8] H. Ollivier and J.-P. Tillich, "Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm," in *Proceedings of the 26th Symposium on Information Theory in the Benelux*, Brussels, Belgium, 2005, p. 149.

A MacWilliams formula for Convolutional Codes

Patrick Solé

(joint work with Dimitrii Zinoviev)

The talk introduces the ideas of [1], where, regarding convolutional codes as polynomial analogues of arithmetic lattices, we derive a Poisson Jacobi formula for their trivariate weight enumerator. The proof is based on harmonic analysis on locally compact abelian groups as developed in Tate's thesis to derive the functional equation of the zeta function.

References

[1] P. Solé, D. Zinoviev, *A MacWilliams formula for Convolutional Codes*, Int. J. of Number Theory, **Vol. 3,No. 2**, (2007) 191–206.

On extremal codes of type II

Wolfgang Willems

(joint work with S. Bouyuklieva, E. O'Brien, and A. Malevich)

Among the extremal codes, the self-dual doubly-even codes C with parameters $[24m, 12m, 4m+4]$ are of particular interest, since, by Assmus and Mattson, the code words of a fixed non-trivial weight form a 5-design. By Mallows and Sloane, m can not be arbitrarily long, and by S. Zhang, $m \leq 153$. However, we know only two examples, the $[24, 12, 8]$ Golay code ($m = 1$) and the $[48, 24, 12]$ quadratic residue code ($m = 2$), both with a large simple automorphism group, namely the Mathieu group M_{24} resp. $\mathrm{PSL}(2, 47)$. In order to find larger examples - if anyone exists - the existence of a non-trivial automorphism might be helpful.

Thus we focus on $\mathrm{Aut}(C)$ in this talk. For $m = 3$ and $m = 4$ much has been done over the last years. For instance, if a $[72, 36, 16]$ code exists then its automorphism group is solvable of order smaller or equal to 36; the automorphism group of a putative $[96, 48, 20]$ code has only prime divisors $2, 3$ and 5.

Applying methods from modular representation theory we prove that particular primes can never occur as divisors in the order of the automorphism group. Suppose that p is a prime and $p \mid |\mathrm{Aut}(C)|$. If $12m \leq p \leq 24m$ then $p = 24m - 1$. This observation rules out more than half of the possible 153 cases of m. In the remaining 64 cases it turns out that $\frac{p-1}{2}$ is the order of 2 mod p unless $m = 18, 38, 46, 98, 112, 133$ (exceptional cases). Since $\frac{p-1}{2}$ is in addition odd one can now prove that C is an extended quadratic residue code in all non-exceptional cases. In case $\frac{p-1}{2}$ splits (i.e. $\frac{p-1}{2}$ is not a prime) we finally use an algorithm discovered by Karlin and MacWilliams to show that C is not extremal.

In summary we have proved: *If p is a prime, $m > 2$ and $12m \leq p \leq 24m$ then p does not divide the order of the automorphism group of C unless m is one of 22 cases which we can not decide at the moment.*

To deal with these cases new ideas have to come in since the Karlin-MacWilliams algorithm does not work. However the results we have obtained so far give some evidence to

Conjecture. If C is a binary self-dual doubly even extremal code of length $24m$ with $m > 2$ and p is a prime with $p \mid |\mathrm{Aut}(C)|$ then $p \leq 12m$.

A Mathematical View of Hybrid ARQ

Emina Soljanin

In applications with fluctuating channel conditions within a range of signal-to-noise ratios (SNRs), such as mobile and satellite packet data transmission, the so called *incremental redundancy* (IR) HARQ or *Type II* HARQ schemes achieve higher throughput efficiency by adapting their error correcting code redundancy to varying channel conditions. An IR-HARQ protocol operates as follows: At the transmitter, the information bits are first encoded by an error detecting code (usually cyclic redundancy check (CRC)) code, and then the CRC coded bits are further encoded encoded by a "mother" error correcting code, which is in practice usually systematic. Initially, only the systematic part of the codeword and a selected number of parity bits are transmitted. The selected parity bits together with the systematic bits form a codeword of a punctured mother code. Decoding of this code is performed at the receiving end. If a retransmission is requested, the transmitter sends additional parity bits possibly under different channel conditions or at different power. Decoding is again attempted at the receiving end, where the new parity bits are combined with those previously received. The procedure is repeated after each subsequent retransmission request, until either the CRC test is passed or all the parity bits of the mother code are transmitted.

To be able to mathematically study IR-HARQ, we model it as a scheme with at most m transmissions where a bit is assigned to transmission j with probability α_j. Transmission j takes place if transmission $j-1$ fails. Such random transmission assignment is not only a useful theoretical tool for analysis and performance prediction, but can actually be implemented by an "on-the-fly" dynamic version of the algorithm described in [1], as follows:

Before the IR HARQ protocol starts:

(1) For each bit position i, $i = 1, 2, \ldots, n$, generate a number θ_i independently and uniformly at random over $[0, 1)$.
(2) Compute λ_1 as $\lambda_1 = 1 - \alpha_1$.
(3) If $\theta_i \geq \lambda_1$, assign bit i to transmission 1.

If transmission $j-1$ fails for $2 \leq j < m$:

(1) Determine α_j, if it was not predetermined.
(2) Compute λ_j as $\lambda_j = \lambda_{j-1} - \alpha_j$.
(3) If $\lambda_j \leq \theta_i < \lambda_{j-1}$, assign bit i to transmission j.

If transmission $m-1$ fails:

transmit at most all remaining bits.

We assume that the channel remains constant during a single transmission j, and is described by its Bhattacharyya noise parameter $\gamma(j)$. This parameter is usually a convex function of the SNR determined by the model of the channel.

To operate the protocol transmitter needs to know how many bits and at which power to send in the first transmission, and if transmission $j-1$ fails, how many bits and at which power to send in transmission j for $2 \leq j \leq m-1$. We assume that the transmitter 1) wants to maximize the throughput 2) knows the mother

code and data rates of the past transmissions, and 3) is informed by the receiver of channel information of the past transmissions. The transmitter's strategy is then to send only as many codeword symbols as necessary to ensure a high probability of successful maximum likelihood decoding assuming a high SNR channel during the current transmission.

To derive the transmission rules, we assume that the decoding after transmission $j-1$ failed. On the average, $n\alpha_j$ bits will participate in the j-th transmission, and the remaining $(1-\alpha_1-\cdots-\alpha_j)\cdot n$ bits of the mother code will not be transmitted. The idea is to treat them as if they are transmitted over a really bad channel, *i.e.,* a channel with $\gamma(j+1)=1$, and compute $\overline{\gamma}(j)$, the average Bhattacharyya noise parameter after the j-th transmission, as

$$\overline{\gamma}(j)=\alpha_1\cdot\gamma(1)+\cdots+\alpha_j\cdot\gamma(j)+(1-\alpha_1-\cdots-\alpha_j)\cdot 1.$$

Our goal is to guarantee vanishingly small probability of error. It is shown in [1] that that can be done by choosing α_j or $\gamma(j)$ or both so that

$$\overline{\gamma}(j)<\exp(-c_0^{[\mathcal{C}]}). \tag{1}$$

Here $c_0^{[\mathcal{C}]}$ is a single parameter describing the mother code $\mathcal{C}$, known as the code *noise threshold* [2]. For the turbo code used in the cdma2000 standard and the dominant packet size, this parameter was computed in [1] to be 0.5198.

Condition (1) can be written in a form which clearly shows the tradeoff between the rate of the j-th transmission code and the signal power:

$$\alpha_j(1-\gamma(j))>1-\exp(-c_0^{[\mathcal{C}]})-\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i)). \tag{2}$$

To satisfy the above lower bound on the product of α_j and $1-\gamma(j)$, the transmitter can either increase the code redundancy α_j or increase the signal power which results in a decrease of $\gamma(j)$ and increase of $1-\gamma(j)$. An increase in redundancy results in the lower throughput of the user while an increase in the power results in a higher interference level experienced by other users in the network. Since $\gamma(j)$ is positive, there is a minimum redundancy requirement:

$$\alpha_j>1-\exp(-c_0^{[\mathcal{C}]})-\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i)). \tag{3}$$

This condition ensures that the probability of error of the ML decoding is bounded by $O(n^{-1/2})$ for high SNR. In the case of predetermined α_j (as it is sometimes in practice), the required signal power is specified by

$$\gamma(j)<\frac{\exp\left(-c_0^{[\mathcal{C}]}\right)-(1-\alpha_j)+\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i))}{\alpha_j}. \tag{4}$$

In this protocol, equations (2), (3), and (4) constitute the j-th transmission rules after transmission $j-1$ fails. Note that these equations imply that the transmitter needs to know the channel gains of the previous ARQ transmissions before it could decide how much redundancy or power is required for the current

transmission. Therefore, simple ACK and NACK messaging is not sufficient to meet the need for power allocation or redundancy allocation at the transmitter side. Note that the receiver knows what the transmitter is doing as long as the rules of the transmission have been agreed upon, and the receiver and the transmitter run identical and synchronized random number generators.

In addition punctured mother codes, another family of codes seem to be a natural candidate for use in HARQ schemes. This is the class of Fountain Codes, originally designed for reliable transmission of data over an erasure channel with unknown erasure probability. The first class of efficient Fountain Codes were LT-codes [4]. The codewords of an LT code are generated based on the k information symbols by the means of a probability distribution on the numbers $1, \ldots, k$. Each codeword symbol is obtained independently, by first sampling this distribution to obtain a number d, and then adding the values of d randomly chosen information symbols. Raptor codes are a modified version of LT codes in which the information sequence of k symbols is pre-coded by a high rate, block code, and then the n resulting symbols are used to generate the Raptor codeword symbols in the same manner as for LT codes, [5]. Both, LT and Raptor codes were originally designed for erasure channels, but performance of Raptor codes on arbitrary symmetric channels have been studied in [6]. For a more general description of Fountain codes, we refer the reader to [4], [5], and [6].

The ability of Raptor codes to produce, for a given set of k information symbols, as many codeword symbols as needed for their successful decoding is what makes these codes of interest for use in HARQ schemes. In [3], HARQ based on Raptor codes is examined and compared to HARQ based on LDPC codes. Both theoretical and simulation results showed that both LDPC and Raptor codes are suitable for HARQ schemes. Which codes would make a better choice depends mainly on the width of the signal-to-noise operating range of the HARQ scheme, prior knowledge of that range, and other design parameters and constraints dictated by standards.

References

[1] E. Soljanin, R. Liu, and P. Spasojević. Hybrid ARQ with random transmission assignments. In P. Gupta, G. Kramer, and A. Wijngarden, editors, *Advances in Network Information Theory*, volume 66, pp. 321–334. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, August 2004.

[2] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1451–1461, June 2002.

[3] E. Soljanin, N. Varnica, and P. Whiting, "Incremental redundancy hybrid ARQ with LDPC and raptor codes," *IEEE Trans. Inform. Theory*, submitted for publication, Sept. 2005.

[4] M. Luby, "LT codes," in *Proc. of the 43rd Annual IEEE Symp. on the Foundations of Comp. Science (STOC)*, 2002.

[5] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inform. Theory*, pp. 2551–2567 , June 2006.

[6] O. Etesami and A. Shokrollahi, "Raptor codes on binary memoryless symmetric channels," *IEEE Trans. Inform. Theory*, pp. 2033–2051, May 2006.

Linear-Programming Decoding of Non-Binary Linear Codes

Vitaly Skachek
(joint work with Mark F. Flanagan, Eimear Byrne and Marcus Greferath)

A new approach for analysis of LDPC codes was proposed in [6], and it is based on the consideration of so-called *pseudocodewords* and their *pseudoweights*. The approach was further explored in [3], [5]. In [1] and [2], the decoding of *binary* LDPC codes using linear-programming decoding was proposed, and the connections between linear-programming decoding and classical belief propagation decoding were established. Recently, pseudocodewords of *non-binary* codes were defined and some bounds on the pseudoweights were derived in [4].

In this work, we extend the approach in [2] towards coded modulation, in particular to codes over rings mapped to non-binary modulation signals. As was done in [2], we show that the problem of decoding may be formulated as a linear-programming (LP) problem for the non-binary case.

More specifically, consider codes over finite rings (this includes codes over finite fields, but may be more general). Denote by $\mathfrak{R}$ a ring with q elements, by 0 its additive identity, and let $\mathfrak{R}^- = \mathfrak{R}\backslash\{0\}$. Let $\mathcal{C}$ be a linear $[n,k]$ code with parity-check matrix $\mathcal{H}$ over $\mathfrak{R}$. The parity check matrix $\mathcal{H}$ has $m \geq n-k$ rows.

Denote the set of column indices and the set of row indices of $\mathcal{H}$ by $\mathcal{I} = \{1, 2, \cdots, n\}$ and $\mathcal{J} = \{1, 2, \cdots, m\}$, respectively. The notation $\mathcal{H}_j$ will be used for the j-th row of $\mathcal{H}$. Denote by $\mathrm{supp}(\boldsymbol{c})$ the support of a vector $\boldsymbol{c}$. For each $j \in \mathcal{J}$, let $\mathcal{I}_j = \mathrm{supp}(\mathcal{H}_j)$ and $d_j = |\mathcal{I}_j|$, and let $d = \max_{j\in\mathcal{J}}\{d_j\}$.

For $j \in \mathcal{J}$, define the single parity check code $\mathcal{C}_j$ by

$$\mathcal{C}_j = \{(b_i)_{i\in\mathcal{I}_j} \ : \ \sum_{i\in\mathcal{I}_j} \mathcal{H}_{j,i} \cdot b_i = 0\}$$

Note that while the symbols of the codewords in $\mathcal{C}$ are indexed by $\mathcal{I}$, the symbols of the codewords in $\mathcal{C}_j$ are indexed by $\mathcal{I}_j$.

Assume that the codeword $\bar{\boldsymbol{c}} = (\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_n) \in \mathcal{C}$ has been transmitted over a q-ary input memoryless channel, and a corrupted word $\boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in \Sigma^n$ has been received. Here Σ denotes the set of channel output symbols; assume that this set either has finite cardinality, or is equal to $\mathbb{R}^l$ or $\mathbb{C}^l$ for some integer $l \geq 1$. In addition, assume hereafter that all information words are equally probable, and so all codewords are transmitted with equal probability.

Define the following mapping

$$\xi \ : \ \mathfrak{R} \longrightarrow \{0,1\}^{q-1} \subset \mathbb{R}^{q-1} \ ,$$

by

$$\xi(\alpha) = \boldsymbol{x} = (x^{(\gamma)})_{\gamma\in\mathfrak{R}^-} \ ,$$

such that, for each $\gamma \in \mathfrak{R}^-$,

$$x^{(\gamma)} = \begin{cases} 1 & \text{if } \gamma = \alpha \\ 0 & \text{otherwise.} \end{cases}$$

It can be extended in a natural way to a bijection on $\mathfrak{R}^n$:

$$\Xi \,:\, \mathfrak{R}^n \longrightarrow \{0,1\}^{(q-1)n} \subset \mathbb{R}^{(q-1)n} \,,$$

according to

$$\Xi(\boldsymbol{c}) = (\xi(c_1) \mid \xi(c_2) \mid \cdots \mid \xi(c_n)) \,.$$

For vectors $\boldsymbol{f} \in \mathbb{R}^{(q-1)n}$, the notation

$$\boldsymbol{f} = (\boldsymbol{f}_1 \mid \boldsymbol{f}_2 \mid \cdots \mid \boldsymbol{f}_n)$$

will be used, where

$$\forall i \in \mathcal{I},\ \boldsymbol{f}_i = (f_i^{(\alpha)})_{\alpha \in \mathfrak{R}^-} \,.$$

This notation is used to write the inverse of Ξ as

$$\Xi^{-1}(\boldsymbol{f}) = (\xi^{-1}(\boldsymbol{f}_1), \xi^{-1}(\boldsymbol{f}_2), \cdots, \xi^{-1}(\boldsymbol{f}_n)) \,.$$

We also define a function $\boldsymbol{\lambda} : \Sigma \longrightarrow \mathbb{R} \cup \{\pm\infty\}$ by

$$\boldsymbol{\lambda} = (\lambda^{(\alpha)})_{\alpha \in \mathfrak{R}^-} \,,$$

where, for each $y \in \Sigma$, $\alpha \in \mathfrak{R}^-$,

$$\lambda^{(\alpha)}(y) = \log\left(\frac{p(y|0)}{p(y|\alpha)}\right) \,,$$

and $p(y|c)$ denotes the channel output probability (density) conditioned on the channel input. Extend $\boldsymbol{\lambda}$ to a map on Σ^n by $\boldsymbol{\lambda}(\boldsymbol{y}) = (\boldsymbol{\lambda}(y_1) \mid \boldsymbol{\lambda}(y_2) \mid \ldots \mid \boldsymbol{\lambda}(y_n))$.

The LP decoder is represented by the following objective function

$$\hat{\boldsymbol{c}} = \Xi^{-1}(\hat{\boldsymbol{f}}) \,,$$

where

$$(\hat{\boldsymbol{f}}, \hat{\boldsymbol{w}}) = \arg \min_{(\boldsymbol{f},\boldsymbol{w}) \in \mathcal{Q}} \boldsymbol{\lambda}(\boldsymbol{y}) \boldsymbol{f}^T \,. \tag{1}$$

The polytope $\mathcal{Q}$ is a relaxation of the convex hull of all points $\boldsymbol{f} \in \mathbb{R}^{(q-1)n}$, which correspond to the codewords. This $\mathcal{Q}$ is defined with the help of auxiliary variables

$$w_{j,\boldsymbol{b}} \quad \text{for} \quad j \in \mathcal{J}, \boldsymbol{b} \in \mathcal{C}_j \,.$$

The vector containing these variables will be denoted by

$$\boldsymbol{w} = \left(w_{j,\boldsymbol{b}} \right)_{j \in \mathcal{J}, \boldsymbol{b} \in \mathcal{C}_j} \,,$$

with respect to some ordering on the elements of $\mathcal{C}_j$.

The following constraints are imposed to describe the polytope $\mathcal{Q}$:

$$\forall j \in \mathcal{J},\ \forall \boldsymbol{b} \in \mathcal{C}_j, \quad w_{j,\boldsymbol{b}} \geq 0 \,, \tag{2}$$

$$\forall j \in \mathcal{J}, \quad \sum_{\boldsymbol{b} \in \mathcal{C}_j} w_{j,\boldsymbol{b}} = 1 \,, \tag{3}$$

and

$$\forall j \in \mathcal{J},\ \forall i \in \mathcal{I}_j,\ \forall \alpha \in \mathfrak{R}^-, \qquad f_i^{(\alpha)} = \textstyle\sum_{\boldsymbol{b} \in \mathcal{C}_j,\, b_i = \alpha} w_{j,\boldsymbol{b}} \,. \tag{4}$$

The minimization of the objective function (1) over $\mathcal{Q}$ forms the relaxed LP decoding problem. It is defined by $n(q-1)+mq^{d-1}$ variables and at most $m(q^{d-1}+d(q-1)+1)$ constraints.

The decoding algorithm works as follows. The decoder solves the LP problem of minimizing the objective function (1) subject to the constraints (2)-(4). If $\boldsymbol{f} \in \{0,1\}^{(q-1)n}$, the output is the codeword $\Xi^{-1}(\boldsymbol{f})$. Otherwise, the decoder outputs an 'error'.

In this work, we show that the above relaxation of the LP leads to a solution which has the 'maximum likelihood (ML) certificate' property, i.e. if the LP outputs a codeword, then it must be the ML codeword. Moreover, we show that if the LP output is integral, then it must correspond to the ML codeword. We define the *graph-cover pseudocodewords* of the code, and the *LP pseudocodewords* of the code, and prove the equivalence of these two concepts. This shows that the links between LP decoding on the relaxed polytope and message-passing decoding on the Tanner graph generalize to the non-binary case.

To demonstrate performance, LP decoding of the ternary Golay code is simulated, and the LP decoder is seen to perform approximately as well as codeword-error-rate optimum hard-decision decoding, and approximately 1.5 dB from the union bound for codeword-error-rate optimum soft-decision decoding.

References

[1] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*, Ph.D. Thesis, Massachusetts Institute of Technology, Sep. 2003.

[2] J. Feldman, M.J. Wainwright, D.R. Karger, *Using linear programming to decode binary linear codes*, IEEE Trans. Inform. Theory **51** (2005), 954–972.

[3] G.D. Forney, R. Koetter, F.R. Kschischang, A. Reznik, *On the effective weights of pseudocodewords for codes defined on graphs with cycles*, Codes, systems, and graphical models **123**, IMA Vol. Math. Appl., 101–112, Springer, 2001.

[4] C.A. Kelley, D. Sridhara, J. Rosenthal, *Pseudocodeword weights for non-binary LDPC codes*, Proc. IEEE International Symposium on Information Theory (2006), 1379–1383, Seattle, USA.

[5] R. Koetter, P. Vontobel, *Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes*, to appear in IEEE Trans. Inform. Theory. Also available as Arxiv report arXiv:cs.IT/0512078 (2005).

[6] N. Wiberg, *Codes and Decoding on General Graphs*, Ph.D. Thesis, Linköping University, Sweden, 1996.

Reporters: Ariel Amir and Mahdi Cheraghchi

Participants

Ariel Amir
Institut für Mathematik
Universität Zürich
Winterthurerstr. 190
CH-8057 Zürich

Prof. Dr. Daniel Augot
INRIA Rocquencourt
Domaine de Voluceau
B. P. 105
F-78153 Le Chesnay Cedex

Prof. Dr. Alexander Barg
Department of Electrical and
Computer Engineering
University of Maryland
College Park MD 20742
USA

Prof. Dr. Jürgen Bierbrauer
Dept. of Math. Sciences
Michigan Technological University
1400 Townsend Drive
Houghton , MI 49931
USA

Dr. Kristian Brander
Department of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby

Dr. Eimear Byrne
School of Mathematical Sciences
University College Dublin
Belfield
Dublin 4
IRELAND

Mahdi Cheraghchi
EPFL IC - ALGO
Station 14
CH-1015 Lausanne

Prof. Dr. Joan Josep Climent
Dept. de Ciencia de la Computacio i
Intelligencia Artificial
Universidad de Alicante
Campus de Sant Vicent
E-03080 Alicante

Prof. Dr. Gerard D. Cohen
Dept. Reseaux
ENST
46, rue Barrault
F-75634 Paris Cedex

Prof. Dr. Iwan M. Duursma
Dept. of Mathematics, University of
Illinois at Urbana-Champaign
273 Altgeld Hall MC-382
1409 West Green Street
Urbana , IL 61801-2975
USA

Prof. Dr. Michele Elia
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca degli Abruzzi, 24
I-10129 Torino

Prof. Dr. Gerard van der Geer
Korteweg-de Vries Instituut
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Prof. Dr. Heide Gluesing-Luerssen
Department of Mathematics
University of Kentucky
715 Patterson Office Tower
Lexington , KY 40506-0027
USA

Prof. Dr. Marcus Greferath
School of Mathematical Sciences
University College Dublin
Belfield
Dublin 4
IRELAND

Annika Günther
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Prof. Dr. Tom Hoeholdt
Department of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby

Prof. Dr. Jorn Justesen
COM
Technical University Denmark
DTU-Building 345V
DK-2800 Lyngby

Dr. Christine A. Kelley
Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus , OH 43210-1174
USA

Prof. Dr. Ralf Kötter
Coordinated Science Laboratory
University of Illinois
1308 W. Main Street
Urbana , IL 61801
USA

Satish Babu Korada
EPFL
Communication Theory Lab
EPFL-IC-ISC-Lthc
CH-1015 Lausanne

Prof. Dr. Frank R. Kschischang
University of Toronto
The Edward S. Rogers Sr. Dept. of
Electrical and Computer Engineering
10 King's College Road
Toronto , Ont. M5S 3G4
CANADA

Shrinivas Kudekar
Ecole Polytechnique Federale de
Lausanne (EPFL)
Laboratoire d'algorithmique
Station 14
CH-1015 Lausanne

Prof. Dr. Margreta Kuijper
Dept. of Electrical & Electronic
Engineering
University of Melbourne
Victoria 3010
Melbourne , Victoria
AUSTRALIA

Dr. Francoise Levy-dit-Vehel
ENSTA/UMA
32, Boulevard Victor
F-75739 Paris Cedex 15

Felice Manganiello
Institut für Mathematik
Universität Zürich
Winterthurerstr. 190
CH-8057 Zürich

Prof. Dr. Gary McGuire
School of Mathematical Sciences
University College Dublin
Belfield
Dublin 4
IRELAND

Prof. Dr. Olgica Milenkovic
Engineering Center, ECOT 253
University of Colorado
Boulder , CO 80309
USA

Abigail Mitchell
Dept. of Mathematics
University of Notre Dame
Mail Distribution Center
Notre Dame , IN 46556-5683
USA

Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Dr. Payam Pakzad
3133 College Ave, Apt B
Berkeley , CA 94705
USA

Vishwambhar Rathi
EPFL
Communication Theory Lab
EPFL-IC-ISC-Lthc
CH-1015 Lausanne

Prof. Dr. Joachim Rosenthal
Institut für Mathematik
Universität Zürich
Winterthurerstr. 190
CH-8057 Zürich

Dr. Gert Schneider
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Prof. Dr. Mohammad Amin Shokrollahi
Ecole Polytechnique Federale de Lausanne (EPFL)
Laboratoire d'algorithmique
Station 14
CH-1015 Lausanne

Dr. Vitaly Skachek
Claude Shannon Institute
University College Dublin
8 Belfield Office Park
Beaver Row, Clonskeagh
Dublin 4
IRELAND

Prof. Dr. Roxana Smarandache
San Diego State University
Department of Mathematics and Statistics
5500 Campanile Drive
San Diego , CA 92182-7720
USA

Prof. Dr. Patrick Sole
CNRS; 13S; Leo Algorithms, Euclide B
Universite de Nice
B.P. 145
2000, Route des Colles
F-06903 Sophia Antipolis

Dr. Emina Soljanin
Lucent Technologies
Bell Laboratories
600 Mountain Avenue
Murray Hill , NJ 07974-0636
USA

Dr. Deepak Sridhara
Seagate Technology
1251 Waterfront Place
Pittsburgh , PA 15222
USA

Prof. Dr. Jean-Pierre Tillich
Projet CODES
INRIA Rocqencourt
B.P. 105
F-78153 Le Chesnay Rocquencourt

Deanna Turk
Department of Mathematics
University of Nebraska, Lincoln
Lincoln , NE 68588
USA

Prof. Dr. Alexander Vardy
UCSD
Mail Code 0407
9500 Gilman Drive
La Jolla CA 92093
USA

Dr. Pascal O. Vontobel
Hewlett-Packard Laboratories
1501 Page Mill Road
Palo Alto , CA 94304
USA

Prof. Dr. Judy L. Walker
Department of Mathematics
University of Nebraska, Lincoln
Lincoln , NE 68588
USA

Dr. Alfred Wassermann
Mathematisches Institut
Universität Bayreuth
Universitätsstr. 30
95440 Bayreuth

Prof. Dr. Wolfgang Willems
Fakultät für Mathematik
Otto-von-Guericke-Universität
Magdeburg
Universitätsplatz 2
39106 Magdeburg

Prof. Dr. Gilles Zemor
Institut de Mathematiques
Universite de Bordeaux I
351 Cours de la Liberation
F-33405 Talence Cedex