Mathematisches Forschungsinstitut Oberwolfach

Report No. 13/2019

DOI: 10.4171/OWR/2019/13

Contemporary Coding Theory

Organized by
Marcus Greferath, Aalto
Camilla Hollanti, Aalto
Joachim Rosenthal, Zürich

17 March – 23 March 2019

Abstract. Coding Theory naturally lies at the intersection of a large number of disciplines in pure and applied mathematics. A multitude of methods and means has been designed to construct, analyze, and decode the resulting codes for communication. This has suggested to bring together researchers in a variety of disciplines within Mathematics, Computer Science, and Electrical Engineering, in order to cross-fertilize generation of new ideas and force global advancement of the field. Areas to be covered are Network Coding, Subspace Designs, General Algebraic Coding Theory, Distributed Storage and Private Information Retrieval (PIR), as well as Code-Based Cryptography.

Mathematics Subject Classification (2010): 94Bxx, 94Axx, 05Bxx, 51Exx, 11T71, 14G50.

Introduction by the Organizers

Coding theory has developed for a long time since its introduction in the late 1940's as a tool for the realization of Shannon's fundamental limits of communication on unreliable channels. Its rich inter-dependency with other areas of mathematics such as algebra, combinatorics, and probability theory, and its applications to a number of areas such as cryptography, electrical engineering, and theoretical computer science have brought forward coding theory as a highly important area of applicable discrete mathematics. As a matter of fact, most papers submitted to *arXiv* under the area of `math.IT` belong to coding theory, and `math.IT` is one of the most active mathematical areas in entire arXiv, as the reader may wish to verify on `http://front.math.ucdavis.edu/math`.

The above organizers proposed an Oberwolfach workshop on coding theory for this reason, and it was clear at the outset that it would bring together leading

researchers in several key areas of mathematical coding theory. In addition to the many mathematicians, there were a number of computer scientists and electrical engineers present. Participants came from many countries and the group included both senior and junior researchers. This workshop was preceded by several events in Dagstuhl (Seminar 11452 in November 2011, Seminar 13351 in August 2013, and Seminar 16101 in March 2016), in particularly the latter of which the prominent role of coding theory for contemporary challenges (*Big Data*) was emphasized and proven. The organizers of the present workshop are positive that this workshop, along with its predecessors, helps to increase the interaction between mathematicians and researchers in applied areas of communications technology.

In the following paragraphs we briefly sketch the areas of research covered, together with their relationships.

(1) **Network Coding.** Network coding theory is concerned with the encoding and transmission of information in the situation where there may be many information sources and possibly many receivers in a communication network. This is a comparably fresh area of coding theory and was established around 1999. The technical kernel of this topic is still sufficiently close to the channel coding problem posed by Shannon in 1948, and differs from it in that a *network* takes the role of the traditional single-link communication.

As this specific area of coding theory is comparably new, numerous classically educated coding theorists have not yet been intensively exposed to it. Thus, we included leading researchers in the workshop, in the hope that they attract others to the field.

(2) **Subspace Designs.** In various areas of combinatorics, a q-analog of a structure or statement is a generalization involving a new parameter q that returns the original entity or expression in the limit as $q \to 1$ (where this limit is often misleading, as the generalized entity may only be defined for discrete values of q).

Subspace designs form the q-analogs of designs in the sense of traditional design theory. Here, such a q-analog of a t-design is a selection of k-subspaces of $\mathbb{F}_q^n$ such that each t-subspace is contained in the same number λ of subspaces in the collection. A number of recent papers have successfully approached the construction question by adopting the so-called Kramer-Mesner method which prescribes a group of automorphisms in order to reduce the complexity of the search tree that contains subspace designs with reasonable parameters.

The theory of subspace designs has received full attention only recently. It is however of utter importance, because q-analogs of designs are sources of (optimal) subspace codes, that play a prominent role in the above-discussed field of random network coding. We therefore included leading researchers into the workshop, hoping for mutual inspiration between coding theory and this challenging field in combinatorial theory.

(3) **Algebraic Coding Theory.** Algebraic coding theory primarily investigates codes obtained from algebraic constructions. Important examples of this area of coding theory are codes from algebraic geometry, and also codes over rings, as they were more intensively studied since the nineties of the previous century. This discipline is almost as old as coding theory itself, and has attracted many of the brightest minds in the field.

Methods from many distinct mathematical sciences, but also of computer science and electrical engineering are very important in this area. There are emerging relationships between this area and Gröbner bases, graphs, and q-analogs of designs, to mention only a few, and our plan was to bring together top experts in these fields to facilitate an exchange of ideas pertaining to this and other interesting questions between the fields.

(4) **Distributed Storage and Private Information Retrieval.** A key task of any data storage system is to protect large volumes of stored data in the case of server failure, subject to severe constraints in terms of physical storage space, energy consumption, bandwidth, and security.

Private Information Retrieval (PIR) protocols make it possible for users to retrieve data items from a (distributed) database without disclosing information about the identity of the data items retrieved.

Distributed Storage and Private Information Retrieval challenge both coding theory and cryptography, while they seek to solve the most prominent problems of current and future communication scenarios. This area in contemporary coding theory has been introduced rather recently, and hence, many traditional methods from coding theory have not yet been adapted in full extent to it. It is subject to further modelling and faces a good number of unsolved or even yet unposed problems. We invited leading researchers to the workshop, hoping to further inspire this challenging field in mathematical coding theory.

(5) **Code-Based Cryptography.** Traditional public-key cryptography is in practice implemented by the RSA encryption scheme or with a Diffie-Hellman key exchange where one uses the group law of an elliptic curve over a finite field. In 1994 Peter Shor demonstrated that the underlying mathematical problems, namely the factorization of integers and the discrete logarithm problem over an elliptic curve are both polynomial time problems if one has a powerful quantum computer available.

As quantum computers have had real progress in recent years it became paramount to come up with public-key cryptographic schemes that resist attacks by quantum computers. As a matter of fact the National Institute of Standards and Technology (NIST) made a call for the development of a standard. For above reasons there is an active research going on in so-called post-quantum cryptography.

Among the promising candidates in post-quantum cryptography are the systems based on coding theory. The idea goes back to a 1978 paper of

Robert McEliece where the subject was introduced, and has opened the nowadays well-established field of code-based cryptography.

It was the firm believe of the organizers that in a workshop on coding theory some time should naturally be devoted to presentations and discussions on how coding theory can contribute to the area of post-quantum cryptography.

The Oberwolfach workshop 1912, that took place from March 17 till March 23, 2019, was well attended and attracted 57 researchers (20 female) from all scholarly disciplines relevant to contemporary coding theory. The researchers came from 17 countries (Belgium, Croatia, Denmark, Estonia, Finland, France, Germany, Hong Kong, Ireland, Israel, Netherlands, Norway, Portugal, Spain, Switzerland, Turkey, USA), and the program provided 29 talks and presentations that were requested to be highly accessible in light of the presence of a good number of early career researchers.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1641185, "US Junior Oberwolfach Fellows". Moreover, the MFO and the workshop organizers would like to thank the Simons Foundation for supporting Christine A. Kelley, Felice Manganiello and Heide Gluesing-Luerssen in the "Simons Visiting Professors" program at the MFO.

Workshop: Contemporary Coding Theory

Table of Contents

Abstracts

Guessing Random Additive Noise Decoding (GRAND)

Muriel Médard
(joint work with Ken R. Duffy)

We revisit the classical coding theorem of Shannon by considering an alternate means of performing maximum a posteriori decoding, which, under the usual assumption of a uniformly distributed input codebook, is maximum likelihood (ML). Our approach considers a model where a channel output, say Y^n, of n symbols, is created by the addition, over some finite field, of a codeword C^n of n symbols and a noise N^n. The Shannon coding theorem for, say, binary symbols, says that the maximum rate, that we denote R, is $1-H$, where H is the Shannon entropy rate of N, and the rate R is such that the cardinality of the set of codewords (the codebook) is 2^{nR}. The complexity of performing ML decoding by examining all possible 2^{nR} codewords is prohibitive, leading to the search for readily decodable codes, and motivating much of the work in coding theory.

Assume now that we instead guess the noise, N^n, from most likely to least likely, and that we query whether $Y^n - N^n$ is a member of the codebook, i.e. whether $Y^n - N^n$ is a valid codeword. Such an investigation would also lead to a ML decoding. By using recent results on large deviations by Christiansen and Duffy, which use results from Massey, Arikan and others on moments of guesswork (the number of guesses until the correct query occurs), we can re-establish the coding theorem, along with error exponents and success exponents, which are quite new. We show that this seemingly naïve approach leads to low complexity decoding and, surprisingly, to a complexity that decreases as R, the code rate, increases. We also show that we can readily account for non-memoryless noise distributions, such as Markov models of noise yield. We show preliminary results that indicate that the best usual decoding approaches for certain common codes can be outperformed by orders of magnitude by using GRAND.

Network Coding with flags

Gabriele Nebe
(joint work with Dirk Liebhold, Angeles Vazques-Castro)

In Random Linear Network Coding the nodes in the network forward random linear combinations of the input vectors. So the information travelling through the network is the subspace generated by all the input vectors. Networks like the internet keep track of the package sequence number. Network Coding with Flags allows the nodes to compute linear combinations only with vectors having a smaller sequence number. So the information that is preserved by the network is a nested sequence of subspaces, a so called **flag**.

The set of all flags in K^n forms a simplicial complex, where the maximal simplices are the fine flags $\{0\} < V_1 < \ldots < V_n = K^n$ with $\dim(V_i) = i$. This simplicial complex is well known in mathematics as the **spherical building** of $\mathrm{GL}_n(K)$. The **Type** of a flag

$$W_* : \quad \{0\} < W_1 < \ldots < W_\ell < K^n$$

is the set $\mathrm{type}(W_*) := \{\dim(W_i) \mid 1 \leq i \leq \ell\}$ of dimensions of the spaces in the flag. It parametrises the orbits of $\mathrm{GL}_n(K)$ on the set of all flags in K^n. Subspace codes can be recovered by taking $\ell = 1$. Together with Angeles Vazquez-Castro (Barcelona) and my PhD student Dirk Liebhold we developed a theory how to use flags for network coding [1].

In analogy with constant dimension codes we look at codes as subsets of the set of flags of a given type. The distance to measure transmission errors is the generalization of the Grassmann distance

$$d(W_*, W'_*) = \sum_{i=1}^{\ell} d_G(W_i, W'_i), \text{where } d_G(W, W') = \frac{1}{2}(\dim(W + W') - \dim(W \cap W')).$$

This distance is $\mathrm{GL}_n(K)$-invariant. The orbit of flags of a given type decomposes further into cells, according to the pivot positions of the subspaces. Each cell is a regular orbit of the unipotent radical U of a parabolic subgroup of $\mathrm{GL}_n(K)$. The $\mathrm{GL}_n(K)$-invariant distance hence can be seen as a distance function on U. In the subspace case ($\ell = 1$) the group U is abelian, more precisely isomorphic to a full matrix space, turning the cells into affine metric spaces and allowing for linear rank metric codes in U. This fails to be true in the general case. For example if $n = r(\ell + 1)$ and $\dim(W_i) = ri$, then the largest cell is a regular orbit for the group

$$U = \left\{ u_A := \begin{pmatrix} I & A_{11} & A_{12} & \ldots & A_{1\ell} \\ 0 & I & A_{22} & \ldots & A_{2\ell} \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & I & A_{\ell\ell} \\ 0 & \ldots & \ldots & 0 & I \end{pmatrix} \;\middle|\; A_{ij} \in K^{r \times r}, 1 \leq i \leq j \leq \ell \right\}.$$

The distance of u_A and the unit element u_0 is

$$d(u_A, u_0) = \sum_{i=1}^{\ell} r_i, \text{ where } r_i = \mathrm{rk} \begin{pmatrix} A_{1,i} & \ldots & A_{1\ell} \\ \vdots & \vdots & \vdots \\ A_{i,i} & \ldots & A_{i\ell} \end{pmatrix}.$$

In general $d(u_A, u_B) = d(u_A u_B^{-1}, u_0) \neq d(u_{A-B}, u_0)$. The paper [1] describes good flag codes, e.g. the checkerboard codes consisting of fine flags in K^n for $n = 2^{t+1}$, which are $n - 1$-dimensional linear codes with minimum distance 2^t. Other interesting examples for flag codes as well as encoding and decoding algorithms are given in Dirk Liebhold's thesis [2].

References

[1] Dirk Liebhold, Gabriele Nebe, Angeles Vazquez-Castro, *Network coding with flags.* Des. Codes Cryptogr. 86 (2018), 269–284.

[2] Dirk Liebhold, *Flag Codes with Application to Network Coding.* Thesis, RWTH Aachen University (2019).

Subspace codes consisting of k-spaces pairwise intersecting in at least $(k-2)$-spaces

Leo Storme

(joint work with Daniele Bartoli, Jozefien D'haeseleer, Ago-Erik Riet, Peter Vandendriessche)

Consider a vector space V and a set of k-spaces $\mathcal{C} = \{\pi_1, \ldots, \pi_n\}$. If these k-spaces pairwise intersect in $(k-t)$-spaces, then $\mathcal{C}$ is called a $(k, k-t)$-*SCID* (*set of Subspaces with Constant Intersection Dimension*). When we identify the elements of $\mathcal{C}$ with codewords, this gives us in fact an equidistant subspace code.

The classical example of a $(k, k-t)$-SCID is a $(k-t)$-*sunflower*. This is a set of k-spaces which pairwise intersect in the same $(k-t)$-space.

An important theorem on $(k, k-t)$-SCID states that every $(k, k-t)$-SCID $\mathcal{C}$ of size

$$|\mathcal{C}| > \left(\frac{q^k - q^{k-t}}{q-1}\right)^2 + \left(\frac{q^k - q^{k-t}}{q-1}\right) + 1$$

is equal to a $(k-t)$-sunflower.

The general belief is that this lower bound is too large. Most likely, for general q, k, t, smaller $(k, k-t)$-SCID are already equal to $(k-t)$-sunflowers. There is first of all a complete classification of $(k, k-1)$-SCID.

A $(k, k-1)$-SCID is either:

- a $(k-1)$-sunflower,
- a set of k-spaces contained in a $(k+1)$-space.

In recent research, improvements to this sunflower bound have been found for $(k, k-2)$-SCID.

There is the important result of Beutelspacher, Eisfeld and Müller [1] which states that every $(3, 1)$-SCID $\mathcal{S}$, with $|\mathcal{S}| \geq 3(q^2+q+1)$, is contained in

- a hyperbolic quadric in $V(6, q)$,
- a dual partial 2-spread of $V(5, q)$,
- a 1-sunflower.

The following examples are classical examples of $(k, k-2)$-SCID.

- $(k-2)$-sunflower: k-spaces through given $(k-2)$-space.
- Dual of a set of 2-spaces in $V(k+2, q)$, pairwise intersecting in the zero vector, is a set of k-spaces in $V(k+2, q)$, pairwise intersecting in a $(k-2)$-space.

(Size at most $q^k + q^{k-2} + \cdots + q^2 + 1$, when k even, and size at most $q^k + q^{k-2} + \cdots + q$, when k odd)

- *star*: set of k-spaces intersecting a given other k-space Ω in distinct $(k-1)$-spaces.
  (Size at most $q^{k-1} + q^{k-2} + \cdots + q + 1$)

To characterize the largest $(k, k-2)$-SCID, the concept of a configuration was used. Consider a $(k, k-2)$-SCID $\mathcal{S}$. A *configuration* is a set of three codewords A, B, C of $\mathcal{S}$, such that $A \cap B \cap C$ is a $(k-4)$-space π_{ABC}.

This then led to the following characterization results.

The three largest $(k, k-2)$-SCID, $k \geq 4$, are either:

- a $(k-2)$-sunflower,
- the dual of a set of 2-spaces in $V(k+2, q)$, pairwise intersecting in the zero vector,
- a star.

As a corollary, the following sharp sunflower bound was proven.

Let $\mathcal{S}$ be a $(k, k-2)$-SCID, with $k \geq 4$.

If

- $|\mathcal{S}| > q^k + q^{k-2} + \cdots + q^2 + 1$, for k even,
- $|\mathcal{S}| > q^k + q^{k-2} + \cdots + q$, for k odd,

then $\mathcal{S}$ is a $(k-2)$-sunflower.

The arguments which were used to prove the preceding characterization results on the largest $(k, k-2)$-SCID, made us believe that also the largest sets of k-spaces, pairwise intersecting in at least $(k-2)$-spaces could be classified.

There was already the major classification result of 3-spaces pairwise intersecting in at least a 1-space, by M. De Boeck [2], which states that in $V(n, q)$, $n \geq 7$, maximal sets of 3-spaces pairwise intersecting in at least a 1-space, are one of 11 types, and also the Erdös-Ko-Rado results by Frankl and Wilson [3]:

Let $\mathcal{S}$ be a set of k-spaces in $V(n, q)$, pairwise intersecting in at least a $(k-2)$-space.

(i) If $n \geq 2k$, then $|\mathcal{S}| \leq \begin{bmatrix} n-k+2 \\ 2 \end{bmatrix}$. Equality holds if and only if $\mathcal{S}$ is the set of all the k-spaces, containing a fixed $(k-2)$-space of $V(n, q)$, or $n = 2k$ and $\mathcal{S}$ is the set of all the k-spaces in a fixed $(k+2)$-space.

(ii) If $k+2 \leq n \leq 2k-1$, then $|\mathcal{S}| \leq \begin{bmatrix} k+2 \\ k \end{bmatrix}$. Equality holds if and only if $\mathcal{S}$ is the set of all the k-spaces in a fixed $(k+2)$-space.

By using ideas involving again the notion of configuration, large sets of k-spaces pairwise intersecting in at least $(k-2)$-spaces were investigated, under the condition that no non-zero vector lies in all the k-spaces. This led to upper bounds on the sizes of such sets of k-spaces pairwise intersecting in at least $(k-2)$-spaces.

As a consequence, we know that larger examples of such sets of k-spaces are cone examples: they have a vertex Ω of a certain dimension $k - k' > 0$, and these examples are then described by this vertex Ω and a base example $\mathcal{S}$ which is a set of k'-spaces pairwise intersecting in at least $(k' - 2)$-spaces.

References

[1] A. Beutelspacher, J. Eisfeld, and J. Müller, *On sets of planes in projective spaces intersecting mutually in one point.* Geom. Dedicata **78** (1999), 143–159.
[2] M. De Boeck, *The largest Erdős-Ko-Rado sets of planes in finite projective and finite classical polar spaces.* Des. Codes Cryptogr. **72** (2014), 77–117.
[3] P. Frankl and R.M. Wilson, *The Erdős-Ko-Rado theorem for vector spaces.* J. Combin. Theory Ser. A **43** (1986), 228–236.

Channel Resolvability Codes for Secrecy and Stealth

Gerhard Kramer
(joint work with Rana Ali Amjad)

Resolvability refers to generating random strings of symbols whose (joint) probability distribution is "close" to a product distribution. The problem of resolvability *coding* is to determine the smallest number of bits needed to generate such strings. *Channel* resolvability adds a channel after the encoder (the bits-to-string mapping) and considers the distribution of the channel output strings. Channel resolvability plays an important role for secrecy and stealth communication, e.g., for the wiretap channel.

A basic paper on the topic is by Wyner (1975) who developed information theory for a problem with two output strings. Wyner measured "closeness" by using a normalized informational divergence. Han-Verdú (1993) refined the theory by using variational distance, and generalized the theory to channels with memory. We describe a coding scheme for channel resolvability on binary-input channels that can approach the information-theoretic limits. The scheme uses a sparse linear code as an inner code, and any code with large minimum distance as an outer code. We show that the inner code generator matrix sparsity can be on the order of $n \log n$ for a code with blocklength n. This matches the encoding complexity of other existing schemes such as polar codes. One question posed is whether one can design "optimal" resolvability codes with less complexity, especially linear complexity.

Combinatorial Aspects of Rank Metric Codes

Eimear Byrne
(joint work with Alessandro Neri, Alberto Ravagnani, John Sheekey)

Rank metric codes were first introduced to the coding theory community by Delsarte [7] in the framework of association schemes. He also gave a construction of a class of extremal rank metric codes, called *maximum rank distance*, or MRD code, which by definition meet the rank metric Singleton bound. They were later studied by Gabidulin [8] and Roth [11] in the context of error-correction. In more recent times, they have seen a formidable resurgence of interest, due to their connections to subspace codes, network coding and as possible candidates for code-based cryptosystems and signature schemes.

Rank metric codes may be vector spaces in $\mathbb{F}_{q^m}^n$, or may be linear spaces of matrices. We discuss three different aspects of rank metric codes and in doing so highlight some fundamental difference between the theories of these two classes.

Definition 1. Let $m \geq n$. An $\mathbb{F}_q$-$[n \times m, k, d]$ matrix code $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$ of minimum rank distance

$$d = \mathrm{rk}(\mathcal{C}) := \min\{\mathrm{rk(X)} : 0 \neq \mathrm{X} \in \mathcal{C}\}.$$

It is called MRD if $k = m(n - d + 1)$. An $\mathbb{F}_{q^m}$-$[n, k, d]$ vector rank metric code is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ of minimum rank distance

$$d = \mathrm{rk}(C) := \min\{\dim_{\mathbb{F}_q}(c_1, c_2, ..., c_n) : 0 \neq c \in C\}.$$

It is called MRD if $k = n - d + 1$.

MRD codes exists for all choices of q, n, d in the form of Delsarte-Gabidulin codes, or the larger family of twisted Gabidulin codes. Any $\mathbb{F}_{q^m}$-$[n, k]$ code in $\mathbb{F}_{q^m}^n$ can be realised as an $\mathbb{F}_q$-$[n \times m, km]$ matrix code in $\mathbb{F}_q^{n\times m}$ by expanding each coefficient with respect to a basis Γ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

In the case of Hamming metric codes, the support of a word is its set of non-zero coordinates. In the case of rank metric codes, the support of $X \in \mathbb{F}_q^{n\times m}$ is the column-space of X. If $x \in \mathbb{F}_{q^m}^n$ its support is the column space of $\Gamma(x)$ for some basis Γ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Density of MRD Codes. It can be shown by an application of the Schwartz-Zippel Lemma [12], combined with a criterion of Gabidulin [8], that the vector linear MRD rank metric codes are *dense* in the family of all vector linear rank metric codes of the same dimension. Explicitly, if $F(q)$ denotes the family of all $\mathbb{F}_{q^m}$-$[n, k]$ vector rank metric codes and $G(q)$ denotes the family of all $\mathbb{F}_{q^m}$-$[n, k, n - k + 1]$ vector rank metric codes then $\lim_{q\to\infty} \frac{G(q)}{F(q)} = 1$. However, as the following theorem shows, the matrix MRD codes are not dense in the family of all matrix codes of the same dimension. This result is achieved in [5] by counting techniques, using the notion of a *partition balanced family*. Several other density problems can be solved using these methods. A different approach (see [1]) yields the same conclusion.

Theorem 2 ([5]). *Let* $F(q) := \{\mathcal{C} \in \mathbb{F}_q^{n\times m} : \dim(\mathcal{C}) = k\}$ *and* $G(q) := \{\mathcal{C} \in F(q) : \mathcal{C}$ *is not MRD*$\}$. *For every* $\varepsilon > 0$ *there exists* $q_\varepsilon \in \mathbb{N}$ *s.t.* $\forall$ *prime powers* $q \geq q_\varepsilon$,

$$\frac{|G(q)|}{|F(q)|} \geq \frac{1}{2} - \varepsilon.$$

In particular, $\lim_{q\to\infty} \frac{|G(q)|}{|F(q)|} \geq \frac{1}{2}$, *provided the limit exists.*

Similar results hold for these families parametrized by m, that is as $m \longrightarrow \infty$, the vector rank metric codes are dense, while the matrix MRD codes are not.

Codes and Subspace Designs. The notion of a subspace design, or a design over $\mathbb{F}_q$, has been known since the 1970s, with the first non-trivial construction given by Thomas [13]. A t-(n, r, λ) subspace design is a collection B of r-dimensional subspaces of $\mathbb{F}_q^n$ with the property that every t-dimensional subspace of $\mathbb{F}_q^n$ is contained in the same number of elements of B. While it is known that t-subspace designs exist for infinitely many parameter sets [9], relatively few infinite families are known. There is a single known sporadic example of a realizable parameter set of q-Steiner system, which has $\lambda = 1$. These are 2-$(13, 3, 1)$ subspace designs over $\mathbb{F}_2$, found by employing the Kramer-Mesner algorithm. A major open problem concerns the existence of a q-analogue of the Fano plane, which would have parameters 2-$(7, 3, 1)$.

A new approach to the problem is to use coding theory. The celebrated Assmus-Mattson theorem [2], which is an application of the MacWilliams Duality Theorem, identifies criteria under which the Hamming supports of the words of a fixed weight in a linear code form the blocks of a classical t-(n, r, λ) design, which is a collection of r-subsets of $[n]$, such that every t-subset of $[n]$ is contained in λ blocks. We give a rank-metric analogue of this theorem, giving a connection between subspace designs and rank-metric codes.

Theorem 3 ([6]). *Let* C *be an* $\mathbb{F}_{q^m}$-$[n, k, d]$ *rank metric code. Let* $1 \leq t < d$ *be an integer. Suppose that* $C^\perp$ *has at most* $d - t$ *ranks in* $\{1, ..., n - t\}$. *Let* $d^\perp$ *be the minimum distance of* $C^\perp$. *Then*

(1) the d*-dimensional supports of* C *form the blocks of a* t*-design over* $\mathbb{F}_q$,
(2) the $d^\perp$*-dimensional supports of* $C^\perp$ *form the blocks of a* t*-design over* $\mathbb{F}_q$.

We remark that while a version of the theorem exists for matrix codes, it is not true to say that for any d-dimensional support U of an element of a matrix code $\mathcal{C}$ that the number $|\{X \in \mathcal{C} : \sigma(X) = U\}|$ is an invariant of d.

Tensor Representation of Codes. The role of matrices in classical coding theory is fundamental. Efficient encoding and decoding procedures rely on the concepts of generator and parity check matrices. Several properties of a code are characterised by such matrices, including duality, equivalence and its minimum distance. These matrices also yield connections to equivalent objects in finite geometry, and hence many optimal codes have been constructed from sets of points in projective space.

We present rank-metric codes in the framework of 3-tensors. More precisely, we define the generator tensor and parity check tensor of an $\mathbb{F}_q$-linear space of matrices and describe the properties of such codes in relation to these objects.

An important and well-studied parameter of a tensor is given by its *tensor rank*. This aspect of bilinear maps is central to algebraic complexity theory [3]. In terms of rank metric codes, this is a significant parameter. E.g., the storage overhead and the number of symbol operations required by a tensor encoder is a function of the tensor rank. Moreover, the computational/storage costs are lower than those associated with a generator matrix, especially for the matrix rank metric codes.

Let $N_q(k,d) := \min\{N : \exists \text{ an } \mathbb{F}_q\text{-}[N,k,d] \text{ code}\}$. It is well known [3] that any $\mathbb{F}_q$-$[n \times m, k, d]$ code has tensor rank at least $N_q(k,d)$. We say the code is *tensor rank optimal* if its tensor rank meets this lower bound.

Theorem 4 ([4])**.** *Let R, k, d satisfy $R = N_q(k,d)$. Let C be an $\mathbb{F}_q$-$[R,k,d]$ code. Let $V \in \mathbb{F}_q^{n\times R}$ and $W \in \mathbb{F}_q^{m\times R}$ have full rank. The code $\{V\mathrm{diag}(c)W^T : c \in C\}$ is an $\mathbb{F}_q$-$[n \times m, k, d]$ rank metric code of tensor rank R in the following cases.*

(1) $R \leq n$, V has rank n, and W generates an $[R,m]$ MDS code.
(2) $R \leq m$, W has rank m, and V generates an $[R,n]$ MDS code.
(3) $R \leq n + m - d$, V and W both generate MDS codes.
(4) $n = k$, $m = d$, V is the parity-check matrix of an (extended) GRS code, W is the generator matrix of an (extended) GRS code, and C is an (extended) GRS code.

We introduce a new invariant, the list of generalized tensor ranks of an $\mathbb{F}_q$-$[n \times m, k, d]$ rank metric code and use these to obtain a refinement of the tensor rank bound proved by Kruskal [10]. We show that generalized rank weights can be used to distinguish inequivalent MRD codes.

References

[1] J. Antrobus, H. Gluesing-Luerssen, Maximal Ferrers Diagram Codes: Constructions & Genericity Considerations, `https://arxiv.org/abs/1804.00624`.

[2] E. F. Assmus, Jr., H. F. Mattson, Jr., *New 5-Designs*, Jour. Combinatorial Theory **6**, pp. 122–151, 1969.

[3] P. Bürgisser, M. Clausen, M. A. Shokrollahi, Algebraic Complexity Theory, Grundlehren der mathematischen Wissenschraften 315, Springer, 1997.

[4] E. Byrne, A. Neri, A. Ravagnani, J. Sheekey, Tensor Representation of Rank-Metric Codes, preprint, 2019.

[5] E. Byrne, A. Ravagnani, Partition-Balanced Familes of Codes and Asymptotic Enumeration in Coding Theory, `https://arxiv.org/abs/1805.02049`.

[6] E. Byrne, A. Ravagnani, An Assmus-Mattson Theorem for Rank Metric Codes, `https://arxiv.org/abs/1806.00448v2`

[7] P. Delsarte, *Bilinear Forms over a Finite Field with Applications to Coding Theory*, J. Combin. Theory Ser. A **25**, pp. 226–241, 1978.

[8] E. Gabidulin, *Theory of Codes with Maximum Rank Distance*, Problems of Information Transmission **2**, pp. 1–12, 1985.

[9] A. Fazeli, S. Lovett, A. Vardy, *Nontrivial t-Designs Over Finite Fields Exist For All t*, J. Combin. Theory Ser. A **127**, pp. 149–160, 2014.

[10] J. B. Kruskal, *Three-Way Arrays: Rank and Uniqueness of Trilinear Decompositions, with Application to Arithmetic Complexity and Statistics*, Linear Algebra and its Applications **18**, pp. 95–138, 1977.
[11] R. M. Roth, *Maximum-Rank Array Codes and their Application to Criss-cross Error Correction*, IEEE Transactions on Information Theory **37**, 2, pp. 328–336, 1991.
[12] J. Schwartz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities*, Journal of the ACM **27**, pp. 701–717, 1980.
[13] S. Thomas, *Designs over Finite Fields*, Geom. Dedicata **24**, 2, pp. 237–242, 1987.

A Factor-Graph Approach to Quantum Information Processing

Pascal O. Vontobel
(joint work with July X. Li)

Graphical notations like factor graphs [1, 2, 3] have proven to be very useful toward expressing relationships between (random) variables and toward formulating low-complexity algorithms for either exactly or approximately computing quantities of interest. For example, decoding algorithms for low-density parity-check codes, which have recently been selected for the new 5G telecommunications standard, are conveniently expressed in terms of factor graphs.

In this presentation, we have reviewed our factor-graph-based approach to quantum information processing [4, 5]. In particular, we have focused on quantum stabilizer codes (see, e.g., [6]) and discussed a new, factor-graph-transform-based approach to relate various graphical representations of such codes [7, 8]. Our approach allows us not only to express spatial correlations of encoded qubits (as is usually done) but also to conveniently express temporal correlations. Overall, this gives us a means to describe and characterize correlations of encoded qubits in space and time.

References

[1] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.
[2] G. D. Forney, Jr., "Codes on graphs: normal realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, 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] H.-A. Loeliger and P. O. Vontobel, "Factor graphs for quantum probabilities," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5642–5665, Sep. 2017.
[5] ——, "Quantum measurement as marginalization and nested quantum systems," *submitted, available online under* `https://arxiv.org/abs/1902.03607`, Feb. 2019.
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, UK: Cambridge University Press, 2010, 10th Anniversary Edition.
[7] P. O. Vontobel, "Stabilizer quantum codes: a unified view based on Forney-style factor graphs," in *Proc. 5th Intern. Symp. on Turbo Codes and Related Topics*, Lausanne, Switzerland, Sep. 1–5 2008, pp. 215–220.
[8] J. X. Li and P. O. Vontobel, "Factor-graph representations of stabilizer quantum codes," in *Proc. 54th Allerton Conf. on Communication, Control, and Computing*, Allerton House, Monticello, IL, USA, Sep. 28–30 2016, pp. 1046–1053.

On checkable group codes

Wolfgang Willems
(joint work with Martino Borello, Javier de la Cruz)

A *linear code* C is called a *G-code* (*or a group code*) if C is a right ideal in the group algebra $KG = \{a = \sum_{g\in G} a_g g \mid a_g \in G\}$ where G is a finite group and K a finite field. Here the vector space KG with basis $\{g \in G\}$ serves as the ambient space with the weight function $\mathrm{wt}(a) = |\{g \in G \mid a_g \neq 0\}|$ and the non-degenerate symmetric bilinear form $\langle \cdot\,, \cdot \rangle$ which is defined by

$$\langle g, h\rangle = \delta_{g,h} \quad \text{for } g, h \in G.$$

Note that KG carries a K-algebra structure via the multiplication in G. More precisely, if $a = \sum_{g\in G} a_g g$ and $b = \sum_{g\in G} b_g g$ are given, then

$$ab = \sum_{g\in G} (\sum_{h\in G} a_h b_{h^{-1}g}) g.$$

In this sense cyclic codes are group codes for a cyclic group G. Reed Muller codes over prime fields $\mathbb{F}_p$ are group codes for an elementary abelian p-group G [2], [5], and there are many other remarkable optimal codes which have been detected as group codes [8], [6], [4], [11].

We would like to mention here that choosing right ideals as group codes is just done by convention. Everything what we are going to prove holds equally true for group codes which are left ideals.

Theorem. [3] Let C be a linear code over K of length n and let G be a finite group of order n. Then C is a right ideal in KG if and only if G is isomorphic to a transitive subgroup of the permutation automorphism group of C.

Definition. A right ideal I in a finite dimenisonal K-algebra A (denoted by $I \leq A$) is called *checkable* if there exists an element $v \in A$ such that

$$I = \{a \mid a \in A,\, va = 0\} = \mathrm{Ann}_r(v) = \mathrm{Ann}_r(Av).$$

Note that checkable left ideals are defined analogously via the left annihilator of a principal right ideal.

Examples. a) Let $e = e^2$ be an idempotent in A. Then the ideal eA is checkable. This can be seen as follows. Obviously, $eA \leq \mathrm{Ann}_r(A(1-e))$. Since any $0 \neq (1-e)b \in (1-e)A$ is not in $\mathrm{Ann}_r(A(1-e))$ we have $eA = \mathrm{Ann}_r(A(1-e))$.
b) If A is a semisimple algebra, then all right and left ideals are generated by idempotents. Thus all right and left ideals are checkable.
c) All cyclic codes are checkable, since the check equation is given by the check polynomial.
d) LCD group codes C (that is, codes for which $C \cap C^{\perp} = \{0\}$) are checkable since $C = eKG$ with a self-adjoint idempotent e [7].

Examples. a) The binary extended $[24, 12, 8]$ Golay code is a checkable group code in $\mathbb{F}_2\mathrm{S}_4$ [4] and $\mathbb{F}_2 D_{24}$ [11], where S_4 is the symmetric group on 4 letters and D_{24} is a dihedral group of order 24.
b) In [10] the authors point out that in numerous cases the parameters of checkable group codes for an abelian group G are as good as the best known linear codes mentioned in [9]. Even more, there is a checkable $[36, 28, 6]$ group code in $\mathbb{F}_5(C_6 \times C_6)$ and a checkable $[72, 62, 6]$ group code in $\mathbb{F}_5(C_6 \times C_{12})$. In both cases the minimum distance is improved by 1 from an earlier lower bound in [9].

As mentioned in the introduction the group algebra KG carries a non-degenerate symmetric bilinear form $\langle \cdot\,, \cdot \rangle$. Thus, for any group code $C \leq KG$ the orthogonal space $C^\perp \leq KG$ is well defined and also a group code in KG.

Theorem. For any right ideal $C \leq KG$ the following are equivalent.

a) C is checkable.
b) $C^\perp$ is a principal right ideal.

As a main result we have the following Theorem. Note that a proof of the equivalence of b) and c) is already contained in [12].

Theorem. If $\operatorname{char} K = p$, then the following are equivalent.

a) KG is code-checkable.
b) Every right ideal in KG is principal.
c) G is p-nilpotent with cyclic Sylow p-subgroup.
d) Every right ideal in the principal p-block $B_0(G) \leq KG$ is principal.

In the literature there are many papers which prove that particular classes of linear codes are asymptotically good. Already 1966 Assmus, Mattson and Turyn asked the question whether the class of cyclic codes is asymptotically good. The answer is still open. Thus we may ask the more general question

Problem. Is the class of group codes asymptitically good?

So far it has been answered only in characteristic 2.

Theorem. [1] For any finite field of characteristic 2 the class of checkable group codes is asymptotically good.

Using the methods of Bazzi and Mitter we are close to a proof that the above Theorem also holds true if $\operatorname{char} K = p$ with $p \equiv 3 \bmod 4$.

References

[1] L.M.J. Bazzi and S.K. Mitter, *Some randomized code constructions from group actions*, IEEE Trans. Inform. Theory **52** (2006), 3210–3219.
[2] S.D. Berman, *On the theory of group codes*, Kibernetika **3** (1967), 31–39.
[3] J.J. Bernal, A. del Río and J.J. Simón, *An intrinsic description of group codes*, Des. Codes Cryptogr. **51** (2009), 289–300.
[4] F. Bernhardt, P. Landrock and O. Manz, *The extended Golay codes considered as ideals*, J. Comb. Theory, Series A **55** (1990), 235–246.
[5] P. Charpin, *Une généralisation de la construction de Berman des codes de Reed-Muller p-aire*, Comm. Algebra **16** (1988), 2231–2246.

[6] J.H. Conway, S.J. Lomonaco and N.J.A. Sloane, *A* [45, 13] *code with minimal distance 16*, Discrete Math. **83** (1990), 213–217.
[7] J. de la Cruz and W. Willems, *On group codes with complementary duals*, Des. Codes and Cryptogr. **86** (2018), 2065–2073.
[8] A. vom Felde, *A new presentation of Cheng-Sloane's* [32, 17, 8]*-code*, Arch. Math. **60** (1993), 508–511.
[9] M. Grassl, *Bounds on the minimum distance of linear codes*, Online available `http://www.codetables.de`.
[10] S. Jitman, S. Ling, H. Liu and X. Xie, *Checkable codes from group rings*, Online available `arXiv: 1012.5498v1`, 2010.
[11] I. McLoughlin and T. Hurley, *A group ring construction of the extended binary Golay code*, IEEE Trans. Inform. Theory **54** (2008), 4381–4383.
[12] D.S. Passman, *Observations on group rings*, Comm. Algebra **5** (1977), 1119–1162.

Constructions of optimal locally recoverable codes via Dickson polynomials

Sihem Mesnager
(joint work with Jian Liu, Deng Tang)

Locally recoverable codes (LRC codes) have recently been a very attractive subject in the research on coding theory due to their theoretical appeal and applications in large-scale distributed storage systems, where a single storage node erasure is considered as a frequent error-event.

An LRC code is said to have *locality* r if the value at any codeword coordinate can be recovered by accessing at most r other coordinates. We refer to such a code as an (n, k, r) LRC code over finite field $\mathbb{F}_q$, if the code is of length n, which has q^k codewords and locality r. For an LRC code with locality r, if a symbol is lost due to a node failure, its value can be recovered by accessing the value of at most r other symbols.

Problems of constructing LRC codes and bounding their parameters have been the subject of a considerable number of publications. Research on bounds for LRC codes was initiated in [3] which showed that the minimal distance $d(\mathcal{C})$ of an (n, k, r) LRC code is bounded as follows: $d(\mathcal{C}) \leqslant n - k - \lceil k/r \rceil + 2$. LRC codes achieving this bound with equality are called *optimal* LRC codes. Taking into account the size of the code alphabet, another upper bound on the minimum distance of (n, k, r) LRC codes was established by Cadambe and Mazumdar [1].

An ingenious idea in designing optimal LRC codes is due to Tamo and Barg [7]. By generalizing the Reed-Solomon codes, Tamo and Barg [7] constructed a family of optimal (n, k, r) LRC codes over a finite field of size that slightly exceeds the code length n. Their method can provide optimal LRC codes for a lot of feasible triplet of parameters (n, k, r). These optimal LRC codes are obtained from specially constructed polynomials over finite fields, called *r-good polynomials* that is to say, an r-good polynomial yields an optimal (n, k, r) LRC code with n divisible by $r + 1$. However, there are only a few known constructions of r-good polynomials. In their very remarquable paper [7], Tamo and Barg have provided three families of good polynomials. In 2018, Liu, Mesnager and Chen [5] have presented

two general methods of designing r-good polynomials by using function composition, which lead to three new constructions of r-good polynomials. Very recently, Micheli [6] has provided a Galois theoretical framework which allows to produce r-good polynomials and showed that the construction of r-good polynomials can be reduced to a Galois theoretical problem over global function fields. The objection of this talk is to explore more polynomials which could be good candidates for being r-good polynomials. More specifically, we exploit Dickson polynomials to provide more families of r-good polynomials leading to the constructions of optimal LRC codes.

1. Background and notation

Let p be a prime and $q = p^s$ be an s-th power of p with s a positive integer. We denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_q^\star$ the cyclic group $\mathbb{F}_q \backslash \{0\}$.

Dickson polynomials (see e.g. [4]) introduced by Dickson in 1897 form an important class of polynomials. They have been extensively investigated in recent years under different contexts. For $b \in \mathbb{F}_q$ and integer $m \geqslant 1$, let

$$D_{m,b}(x) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-b)^j x^{m-2j} \tag{1}$$

denote the Dickson polynomial (of the first kind) of degree m over $\mathbb{F}_q$.

A polynomial F over $\mathbb{F}_{p^s}$ is said to be an *r-good polynomial* if

(1) the degree of F is $r+1$,
(2) there exist pairwise disjoint subsets $\{A_1, \ldots, A_l\}$ of $\mathbb{F}_{p^s}$ with cardinality $|A_i| = r+1$ for $i = 1, \ldots, l$, $l \geqslant 1$, such that the restriction of F to each subset A_i is constant.

2. Constructions of r-good polynomials via Dickson polynomials

For q odd, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 1$. If $m|(q-1)$, then the Dickson polynomial $D_{m,b}(x)$ is an $(m-1)$-good polynomial. Suppose $b \in \xi^l U_m$ for some $l \in S = \{0, 1, \ldots, (q-1)/m - 1\}$, where ξ is a primitive element of $\mathbb{F}_q$, $\xi^i U_m$ is the multiplicative coset of $U_m = \{x \in \mathbb{F}_q \mid x^m = 1\}$. Then, the only pairwise disjoint subsets of $\mathbb{F}_q$ with cardinality m such that $D_{m,b}$ is constant on each subset include

$$D_i = \left\{ u + b \cdot u^{-1} \;\middle|\; u \in \xi^i U_m \right\}, \text{ for } i \in I \subseteq S, \tag{2}$$

where

(3)

$$I = \begin{cases} \left\{0, 1, \ldots, \frac{l}{2} - 1, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - 1\right\}, & \text{if } l \text{ is even, } \frac{q-1}{m} \text{ is even,} \\ \left\{0, 1, \ldots, \frac{l}{2} - 1, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - \frac{1}{2}\right\}, & \text{if } l \text{ is even, } \frac{q-1}{m} \text{ is odd,} \\ \left\{0, 1, \ldots, \frac{l-1}{2}, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - \frac{1}{2}\right\}, & \text{if } l \text{ is odd, } \frac{q-1}{m} \text{ is even,} \\ \left\{0, 1, \ldots, \frac{l-1}{2}, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - 1\right\}, & \text{if } l \text{ is odd, } \frac{q-1}{m} \text{ is odd.} \end{cases}$$

For q odd, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 3$ satisfying $m|(q-1)$. Suppose $b \in \xi^l U_m$ for some $l \in \{0, 1, \ldots, (q-1)/m - 1\}$, where ξ is a primitive element of $\mathbb{F}_q$. Then, one can deduce that the Dickson polynomial $D_{m,b}(x)$ is constant on exactly $l_{D_{m,b}}$ pairwise disjoint subsets with cardinality m, where

$$l_{D_{m,b}} = \begin{cases} \frac{q-1}{2m} - 1, & \text{if } l \text{ is even, } \frac{q-1}{m} \text{ is even,} \\ \frac{q-1-m}{2m}, & \text{if } l \text{ is even, } \frac{q-1}{m} \text{ is odd,} \\ \frac{q-1}{2m}, & \text{if } l \text{ is odd, } \frac{q-1}{m} \text{ is even,} \\ \frac{q-1-m}{2m}, & \text{if } l \text{ is odd, } \frac{q-1}{m} \text{ is odd.} \end{cases}$$

For q even, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 2$ satisfying $m|(q-1)$. Then, the Dickson polynomial $D_{m,b}(x)$ is an $(m-1)$-good polynomial. Suppose $b \in \xi^l U_m$ for some $l \in S = \{0, 1, \ldots, (q-1)/m - 1\}$, where ξ is a primitive element of $\mathbb{F}_q$, $\xi^i U_m$ is the multiplicative coset of $U_m = \{x \in \mathbb{F}_q \mid x^m = 1\}$. Then, the only pairwise disjoint subsets of $\mathbb{F}_q$ with cardinality m such that $D_{m,b}$ is constant on each subset include

$$D_i = \left\{ u + b \cdot u^{-1} \;\middle|\; u \in \xi^i U_m \right\}, \text{ for } i \in I \subseteq S, \tag{4}$$

where

$$I = \begin{cases} \left\{0, 1, \ldots, \frac{l}{2} - 1, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - \frac{1}{2}\right\}, & \text{if } l \text{ is even,} \\ \left\{0, 1, \ldots, \frac{l-1}{2}, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - 1\right\}, & \text{if } l \text{ is odd.} \end{cases} \tag{5}$$

For q even, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 3$ satisfying $m|(q-1)$. Then, one can show that the Dickson polynomial $D_{m,b}(x)$ is constant on exactly

$$l_{D_{m,b}} = \frac{q-1-m}{2m}$$

pairwise disjoint subsets with cardinality m.

3. Concluding remarks

In this talk we have showed that the well-known Dickson polynomials are good candidates to be r-good polynomials. We have also explored new methods on constructing r-good polynomials via combining Dickson polynomials with linear functions. We found that there exist a large number of such r-good polynomials besides the known ones.

Acknowledgement. We would like to thank Gaojun Luo for the discussion on r-good polynomials via Dickson polynomials in Hangzhou, China.

References

[1] V. R. Cadambe and A. Mazumdar, Bounds on the size of locally recoverable codes, *IEEE Transactions on Information Theory,* vol. 61, no. 11, pp. 5787–5794, 2015.

[2] W. S. Chou, J. Gomez-Calderon, and G. L. Mullen, Value sets of Dickson polynomials over finite fields, *Journal of Number Theory,* vol. 30, no. 3, pp. 334–344, 1988.

[3] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, On the locality of codeword symbols, *IEEE Transactions on Information Theory,* vol. 58, no. 11, pp. 6925–6934, 2012.

[4] R. Lidl, G. L. Mullen, and G. Turnwald, Dickson Polynomials, *Pitman Monographs in Pure and Applied Mathematics*, vol. 65, Addison-Wesley, Reading, MA, 1993.

[5] J. Liu, S. Mesnager, and L. Chen, New constructions of optimal locally recoverable codes via good polynomials, *IEEE Transactions on Information Theory,* vol. 64, no. 2, pp. 889–899, 2018.
[6] G. Micheli, Constructions of locally recoverable codes which are optimal. arXiv:1806.11492 [cs.IT], 2018.
[7] I. Tamo and A. Barg, A family of optimal locally recoverable codes, *IEEE Transactions on Information Theory,* vol. 60, no. 8, pp. 4661–4676, 2014.

Thermal-Management Coding for High-Performance Interconnects

Tuvi Etzion

High temperatures have dramatic negative effects on interconnects performance. We introduce new efficient coding schemes that directly control the peak temperature of a bus by effectively cooling its hottest wires. This is achieved by avoiding state transitions on the hottest wires for as long as necessary until their temperature drops off. At the same time, we reduce the average power consumption by ensuring that the total number of state transitions on all the wires is bounded. Furthermore we are able to correct a number of errors that might occur during the transmission of the information. All these goals are achieved by using some redundancy, we use $n > k$ wires to encode a given k-bit bus. We provide optimal solutions and full analysis in each case.

Applications of nonbinary convolutional codes

Ángela Barbero and Øyvind Ytrehus

Binary convolutional codes were initially attractive for practical applications due to their simple decoding algorithms. Recent years have seen a renewed interest in convolutional codes, this time with a focus on bounds and constructions on *non*binary codes. These codes have better distance properties than their binary counterparts, but are less useful on communication channels that produce errors, since e.g. Viterbi decoding becomes prohibitively complex for all but the simplest codes. However, maximum likelihood decoding is feasible for erasure channels. This makes the codes interesting for several practical modern applications:

Promising applications and research areas

(1) Codes for delay sensitive erasure channels, e.g. transport protocols in the Internet. See Section 1.
(2) Codes for distributed storage. See Section 2.
(3) Codes for distributed computation. See Section 3.
(4) The above examples inherently assume an underlying symbol erasure channel. For channels that introduce errors, sequential decoding was a much used decoding algorithm before the invention of Viterbi decoding. A sequential decoder is less sensitive to the size of the convolutioanal code's

state space than a Viterbi decoder is. Actually, the column distance profile is more important. How do nonbinary codes perform with sequential decoders on a channel which makes errors?

(5) Alternatively, on channels with errors, error *detection* can be achieved quicker in some cases using convolutional codes as opposed to block codes. The idea was patented by Jim Massey in 1967 [1], using binary convolutional codes. Nonbinary codes will offer more rapid detection, since they have a better column distance profile than binary codes. Roughly speaking, a convolutional code possesses an optimum column profile iff the distance between distinct codewords grows as fast as possible (see e.g. [2]), thus allowing a rapid reconstruction of lost information packets.

Potential applications

(1) Block codes have been proposed for Private Information Retrieval (PIR). Is there a way to utilize the sliding window properties of convolutional codes for PIR?
(2) Block codes have been used with success for efficient compressed sensing. What about convolutional codes?
(3) Recently, there have been block subspace codes, or codes designed to have good rank metric properties. What can be achieved in terms of convolutional codes for good rank metric properties?

Potential but *less promising (?)* applications

(1) Convolutional McEliece asymmetric cryptographic schemes: This sounds like a natural idea. However, proposed schemes are either broken or not explained in sufficient detail.

1. Codes for Internet transport

Sequences of IP packets sent over the Internet are traditionally made robust by using TCP's ARQ strategies. For delay sensitive applications, the inherent delay cost of this approach is unacceptable. Hence coded transmission, in particular employing convolutional codes with an optimum column distance profile, offers better delay properties [2].

2. Codes for Distributed storage

In order to protect stored files in distributed storage media against hardware failures, the storage system must offer a reliable scheme for reconstruction of lost content. Early systems used file replication to provide reliability. File replication essentially amounts to storing with a repetition code; for this reason, the use of more advanced codes have become more common, allowing a drastic reduction in the storage requirements compared with file replication for comparable robustness performance. Although Reed-Solomon codes offer optimum code rate, Dimakis *et al.* [3] showed that there is a tradeoff between code rate and reconstruction complexity.

In most cases that have been studied, block codes have been used, with the immediate consequence that files must be static, or encoded in blocks of short length, sacrificing code rate. We show that using convolutional codes instead, files may be extended (as e.g. in blockchain applications), or edited by changing local parts, or inserting or deleting file parts. Direct access to individual records is facilitated by using systematic codes (convolutional or block). If a file is read continuously from start to end, the coding problem is similar to a streaming application. On the other hand, with direct access, locally repairable codes become an advantage. Martnez-Peas and Napp [4] describe locally repairable convolutional codes in a rank distance perspective. In contrast, we describe the storage of files using codes from [2], that may be stored directly but possibly augmented by extra parity checks in order to improve storage reliability and also to facilitate block reconstruction in case of hardware failures.

It follows by definition that a rate $(n-1)/n$ MDP convolutional in which every parity check extends over more than one n-symbol block cannot be locally repairable within one block. Lowering the rate to $(n-1)/(n+1)$ by adding an extra parity symbol (corresponding to a zero-memory parity check!) per block will obviously also make the code 1-erasure-1-block locally repairable. This offers the added possibility of improving the distance properties by optimizing the selection of the other parity checks.

3. Codes for Distributed computation

Distributed computation of certain common operations, often related to linear algebra, can be described in a way similar to distributed storage. Computation in some nodes (stragglers) may take longer to complete than anticipated, thus delaying the result of the entire operation. In the coded approach, the stragglers are considered erasures, and the computational problem is formulated with redundancy an in such a way that the missing straggler results can be recreated based on the rest. Convolutional codes for this problem were considered in [5].

References

[1] James L. Massey, ERROR DETECTION AND CORRECTION SYSTEM FOR CONVOLUTIONAL CODES, US Patent 3,303,333, Feb. 7, 1967, filed July 1962.

[2] Ángela Barbero and Øyvind Ytrehus, "Rate (n-1)/n Systematic Memory Maximum Distance Separable Convolutional Codes," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 3018–3030, Apr. 2018.

[3] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, K. Ramchandran, "Network coding for distributed storage systems", *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[4] Umberto Martnez-Peas and Diego Napp, *Locally Repairable Convolutional Codes with Sliding Window Repair*, arXiv:1901.02073v1 [cs.IT]

[5] Anindya B. Das and Aditya Ramamoorthy, *Distributed Matrix-Vector Multiplication: A Convolutional Coding Approach*, arXiv:1901.08716v1 [cs.IT].

Matrix Codes and Rook Theory

Alberto Ravagnani
(joint work with Heide Gluesing-Luerssen)

1. Introduction and Motivation

Rank-metric codes are linear spaces of matrices over a finite field endowed with the rank distance. They were first studied by Delsarte for combinatorial interest via association schemes [1]. Special classes of rank-metric codes were independently discovered by Gabidulin [2] and Roth [6]. In 2008, Silva, Kschischang and Kœtter [7] proposed rank-metric codes as a solution to the problem of error amplification in adversarial networks. Since then, matrix codes have been the subject of intense mathematical research, and have been studied in connection with several topics in algebra and combinatorics.

In this abstract, we survey some results from a joint work [4] with H. Gluesing-Luerssen, that was presented at the Oberwolfach Workshop on *Contemporary Coding Theory* (ID 1912). The focus of the abstract is on the connection between rank-metric codes and the theory of rook placements.

We start by defining rank-metric codes. In the sequel, we let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. We also work with integers $m \geq n > 0$.

Definition 1. A (**matrix rank-metric**) **code** is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$. Its **dual** is $\mathcal{C}^\perp = \{Y \in \mathbb{F}_q^{n\times m} \mid \langle X, Y\rangle = 0 \ \forall\ X \in \mathcal{C}\}$, where $\langle X, Y\rangle = \mathrm{Tr}(XY^\top)$ is the **trace-product** of X and Y. Note that $\mathcal{C}^\perp$ is also a code, whose dimension is $mn - \dim(\mathcal{C})$. We let $W_i(\mathcal{C})$ denote the number of rank i matrices in a code $\mathcal{C}$.

The starting point of our discussion is an elegant theorem by Delsarte [1] that relates the rank distribution of a code $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ to the rank distribution of its dual code $\mathcal{C}^\perp$. This can be interpreted as the rank-metric analogue of the celerated MacWilliams identities for codes with the Hamming metric.

Theorem 2. *Let $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ be a code and let $0 \leq j \leq n$ be an integer. We have*

$$W_j(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} W_i(\mathcal{C}) \sum_{s=0}^{n}(-1)^{j-s}q^{ms+\binom{j-s}{2}} \begin{bmatrix} n-i \\ s \end{bmatrix}_q \begin{bmatrix} n-s \\ j-s \end{bmatrix}_q .$$

Partitioning the elements of $\mathbb{F}_q^{n\times m}$ according to their rank is not the only way of classifying matrices. Every partition $\mathcal{P}$ of $\mathbb{F}_q^{n\times m}$ yields a notion of $\mathcal{P}$-enumerator of a code $\mathcal{C}$ as follows.

Definition 3. Let $\mathcal{P} = (P_i)_{i\in I}$ be a partition of $\mathbb{F}_q^{n\times m}$. The **$\mathcal{P}$-enumerator** of a code $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ is $(\mathcal{P}(\mathcal{C}, i) \mid i \in I)$, where $\mathcal{P}(\mathcal{C}, i)$ denotes the cardinality of $\mathcal{C} \cap P_i$.

In [4], we address the problem of constructing partition pairs $(\mathcal{P}, \mathcal{Q})$ on $\mathbb{F}_q^{n\times m}$ with the following property: For every code $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$, the $\mathcal{P}$-enumerator of $\mathcal{C}$ and the $\mathcal{Q}$-enumerator of $\mathcal{C}^\perp$ determine each other via an invertible transformation. This problem is an instance of a more general and well-studied question in the context of additive codes in finite abelian groups.

2. The Pivot and Reverse-Pivot Partition

We partition the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form (RREF). This defines a partition on $\mathbb{F}_q^{n\times m}$, denoted by $\mathcal{P}^{\mathrm{piv}}$, which we call the **pivot partition**. We denote by $\mathrm{piv}(X)$ the list of pivots of a matrix $X \in \mathbb{F}_q^{n\times m}$.

Example 4. The matrix

$$X = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

over $\mathbb{F}_3$ has $\mathrm{piv}(X) = (1, 3)$.

Similarly, $\mathcal{P}^{\mathrm{rpiv}}$ partitions the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form *computed from the right*. We call it the **reverse-pivot partition**. The reverse list of pivots of $X \in \mathbb{F}_q^{n\times m}$ is denoted by $\mathrm{rpiv}(X)$. More precisely, we have $\mathrm{rpiv}(X) = (m + 1 - j_r, ..., m + 1 - j_1)$ if $\mathrm{piv}(XS) = (j_1, ..., j_r)$, where

$$S = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \in \mathrm{GL}_m(\mathbb{F}_q).$$

For example, the matrix X in Example 4 has $\mathrm{rpiv}(X) = (2, 3)$. In the sequel, we let $\Pi = \{(j_1, ..., j_r) \mid 1 \le r \le n,\ 1 \le j_1 < j_2 < \cdots < j_r \le m\} \cup \{()\}$ denote the set of admissible pivot lists, where () is the empty list.

3. MacWilliams-Type Identities

In [4], we show that the pair of partitions $(\mathcal{P}^{\mathrm{piv}}, \mathcal{P}^{\mathrm{rpiv}})$ satisfies the property stated right after Definition 3 on page 796. We also compute the coefficients of the corresponding linear transformation in terms of the rank distribution of matrices supported on certain Ferrers diagrams. The latter are defined as follows.

Definition 5. Let $x, y > 0$ be positive integers. An $x \times y$ **Ferrers diagram** is a subset $\mathcal{F} \subseteq \{1, ..., x\} \times \{1, ..., y\}$ such that $(i, j) \in \mathcal{F}$ implies $(i', j') \in \mathcal{F}$ whenever $1 \le i' \le i$ and $j \le j' \le y$. Given an integer r and an $x \times y$ Ferrers diagram $\mathcal{F}$, we denote by $P_r(\mathcal{F}; q)$ the number of rank r matrices $M \in \mathbb{F}_q^{x\times y}$ that are supported on $\mathcal{F}$ (i.e., with $M_{ij} = 0$ whenever $(i, j) \notin \mathcal{F}$).

A Ferrers diagram $\mathcal{F}$ can be visualized as an array of top and right-aligned dots. We write $\mathcal{F} = [c_1, ..., c_y]$ if $c_1, ..., c_y$ are the lengths of the columns of $\mathcal{F}$. For instance, the Ferrers diagram $\mathcal{F} = [1, 1, 3, 4]$ is depicted in Fig. 1. We establish

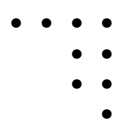

Figure 1. The Ferrers diagram $\mathcal{F} = [1, 1, 3, 4]$.

a MacWilliams-type identity relating the pivot enumerator of a code $\mathcal{C}$ to the reverse-pivot enumerator of $\mathcal{C}^\perp$. The coefficients of the identity are expressed in terms of the rank distribution associated with Ferrers diagrams.

Theorem 6 (Gluesing-Luerssen, R.). *Let $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ be a code and $\lambda, \mu \in \Pi$. Let*

$$\sigma = \widehat{\mu}, \qquad \lambda \cap \sigma = (\lambda_{\alpha_1}, \ldots, \lambda_{\alpha_x}), \qquad \widehat{\sigma} \setminus \lambda = (\hat{\sigma}_{\beta_1}, \ldots, \hat{\sigma}_{\beta_y}).$$

For $j \in [y]$ set $z_j = |\{i \in [x] \mid \lambda_{\alpha_i} < \hat{\sigma}_{\beta_j}\}|$, and let $\mathcal{F}$ be the $x \times y$ Ferrers diagram $\mathcal{F} = [z_1, \ldots, z_y]$. We have

$$\mathcal{P}^{\mathrm{rpiv}}(\mathcal{C}^\perp, \mu) = \frac{1}{|\mathcal{C}|} \sum_{\lambda\in\Pi} \sum_{t=0}^{m} (-1)^{|\lambda|-t} q^{nt+\binom{|\lambda|-t}{2}} \sum_{r=0}^{|\lambda\cap\sigma|} P_r(\mathcal{F}; q) \begin{bmatrix} |\lambda \cap \sigma| - r \\ t \end{bmatrix}_q \mathcal{P}^{\mathrm{piv}}(\mathcal{C}, \lambda).$$

The quantity $P_r(\mathcal{F}; q)$ is well-studied in the context of rook theory. In [5], Haglund establishes an interesting connection between $P_r(\mathcal{F}; q)$ and the q-rook polynomial $R_r(\mathcal{F}; q) \in \mathbb{Z}[q]$ for an arbitrary Ferrers board $\mathcal{F}$. The latter has been introduced by Garsia and Remmel. We refer the reader to [3] for the definitions.

Theorem 7 (Haglund). *For any Ferrers diagram $\mathcal{F}$ and any $r \geq 0$ we have $P_r(\mathcal{F}; q) = (q-1)^r \; q^{|\mathcal{F}|-r} \; R_r(\mathcal{F}; q)_{|q^{-1}}$ in the ring $\mathbb{Z}[q, q^{-1}]$.*

In [4], we give a closed formula for $P_r(\mathcal{F}; q)$, for any Ferrers diagram $\mathcal{F}$, any r, and any q. Using Haglund theorem, we obtain as a simple corollary an explicit expression for the q-rook polynomials associated with an arbitrary Ferrers diagram.

Theorem 8 (Gluesing-Luerssen, R.). *For any $x\times y$ Ferrers diagram $\mathcal{F} = [c_1, ..., c_y]$ and all $1 \leq r \leq \min\{x, y\}$ we have*

$$P_r(\mathcal{F}; q) \;=\; \sum_{1\leq i_1<\cdots<i_r\leq y} q^{ry-\sum_{j=1}^r i_j} \prod_{j=1}^{r} (q^{c_{i_j}-j+1} - 1).$$

In particular, we have

$$(1-q)^r \; R_r(\mathcal{F}; q) \;=\; q^{\sum_{j=1}^y c_j - ry} \sum_{1\leq i_1<\cdots<i_r\leq y} \prod_{j=1}^{r} \left(q^{i_j+j-c_{i_j}-1} - q^{i_j} \right).$$

References

[1] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A*, 25:226–241, 1978.

[2] E. M. Gabidulin. Theory of codes with maximal rank distance. *Probl. Inf. Transm.*, 21:1–12, 1985.

[3] A. M. Garsia and J. B. Remmel. Q-counting rook configurations and a formula of Frobenius. *J. Combin. Theory Ser. A*, 41:246–275, 1986.

[4] H. Gluesing-Luerssen and A. Ravagnani. Partitions of atrix spaces with an application to q-rook polynomials. Preprint: `https://arxiv.org/abs/1811.01282`.

[5] J. Haglund. q-rook polynomials and matrices over finite fields. *Adv. Appl. Math*, 20:450–487, 1998.

[6] R. M. Roth. Maximum-rank array codes and their application to criss-cross error correction. *IEEE Trans. Inform. Theory*, 37:328–336, 1991.

[7] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Trans. Inform. Theory*, 54:3951–3967, 2008.

General Strong Polarization

Madhu Sudan
(joint work with J. Blasiok, V. Guruswami, P. Nakkiran, A. Rudra)

The classical theorem of Shannon [8] asserts that the capacity of the binary symmetric channel with paremeter p is $(1 - h(p))$ where $h(p)$ is the binary entropy function. More elaborately it says that if we choose any $\epsilon > 0$, then for sufficiently large n, there are codes of block length n, rate at least $1 - h(p) - \epsilon$ that can correct random bit flip errors with high probability, where each bit is flipped independently with probability p. Forney [7]'s technique of concatenated codes (from 1966) shows how to do this with polynomial time algorithms, where the algorithms run in time polynomial in n for every fixed $\epsilon > 0$. However the dependence on ϵ remained exponentially high.

Arikan [1]'s introduction of Polar codes in 2008 suggested a possibility that we may have finally found a technique to reduce the dependence to be polynomial in epsilon. Five years later in 2013, Guruswami and Xia [5], and independently Hassani, Alishahi and Urbanke [6] finally confirmed this possibilty thus resolving a major open question in the Shannon theory.

In our work we give clean modular explanations of the main theorem above, which also yields generalizations to a broader class of codes, and broader class of channels (including channels with some memory) and yield exponentially low probabiity of decoding failure (of the form $\exp(-n^{\Omega(1)})$). Based on [2, 3, 4].

References

[1] Erdal Arikan. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Information Theory*, 55(7):3051–3073, 2009.

[2] Jaroslaw Blasiok, Venkatesan Guruswami, Preetum Nakkiran, Atri Rudra, and Madhu Sudan. General strong polarization. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 485–492. ACM, 2018.

[3] Jaroslaw Blasiok, Venkatesan Guruswami, and Madhu Sudan. Polar codes with exponentially small error at finite block length. In Eric Blais, Klaus Jansen, José D. P. Rolim, and David Steurer, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2018, August 20-22, 2018 - Princeton, NJ, USA*, volume 116 of *LIPIcs*, pages 34:1–34:17. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[4] Venkatesan Guruswami, Preetum Nakkiran, and Madhu Sudan. Algorithmic polarization for hidden markov models. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 39:1–39:19. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[5] Venkatesan Guruswami and Patrick Xia. Polar codes: Speed of polarization and polynomial gap to capacity. *IEEE Trans. Information Theory*, 61(1):3–16, 2015.

[6] Seyed Hamed Hassani, Kasra Alishahi, and Rüdiger L. Urbanke. Finite-length scaling for polar codes. *IEEE Trans. Information Theory*, 60(10):5875–5898, 2014.

[7] G. David Forney Jr. *Concatenated Codes*. MIT Press, Cambridge, MA, 1966.

[8] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

Algebraic codes are good

Patrick Solé

We survey the algebraic structure [3], and asymptotic performance of the self-dual and LCD classes of quasi-cyclic [1], quasi-twisted [2], and dihedral codes over finite fields and finite rings. Of special interest is the case of low index: double circulant codes and four circulant codes [4]. We show that additive cyclic codes are good [5], and give an alternative proof that dihedral codes are good [1].

References

[1] Adel Alahmadi, Funda Özdemir, Patrick Solé, *On self-dual double circulant codes*. Des. Codes Cryptography **86(6):** (2018), 1257–1265.
[2] Adel Alahmadi, Cem Güneri, Buket Özkaya, Hatoon Shohaib, Patrick Solé, *On self-dual double negacirculant codes*. Discrete Applied Mathematics **222:** (2017), 205–212.
[3] Cem Güneri, Funda Özdemir, Patrick Solé, *On the additive cyclic structure of quasi-cyclic codes*. Discrete Mathematics **341(10):**, (2018), 2735–2741.
[4] Minjia Shi, Hongwei Zhu, Liqin Qian, Patrick Solé, *On Self-Dual Four Circulant Codes*. Int. J. Found. Comput. Sci. **29(7):**, (2018), 1143–1150.
[5] Minjia Shi, Rongsheng Wu, Patrick Solé, *Asymptotically Good Additive Cyclic Codes Exist*, IEEE Communications Letters **22(10):** (2018), 1980–1983.

Majority logic decoding and subspace designs

Alfred Wassermann

In [6], a simple decoding method based on majority decision for linear codes is presented. Its attraction lies in the easy realization in hardware and it requires that the dual code has to contain the blocks of a t-design, $t \geq 2$, as codewords.

Ever since then, people studied the linear codes generated by the blocks of t-designs. In order to get a good code it is desirable that the rank of the block-point incidence matrix of the design is small over some finite field. The famous Hamada conjecture states that *geometric designs*, which consist of the set of all k-flats in $\mathrm{PG}(v, q)$ or $\mathrm{AG}(v, q)$, minimize the p-rank for a prime power $q = p^s$.

Here, a few simple observations on the codes from subspace designs – also known as q-analogs of designs – are reported. These codes have the same length and majority logic decoding capability as the codes from geometric designs, but their decoding complexity is improved.

Rudolph [6] suggested to use the rows of a $b \times v$ block-point incidence matrix $N_{\mathcal{D}}$ of a 2-(v, k, λ) design $\mathcal{D}$ as parity check equations for a linear code $C_{\mathcal{D}}$ over $\mathbb{F}_p$. In [6, 4] it is shown that with *one-step majority logic decoding* the number of errors which can be decoded is equal to $\lfloor (r + \lambda - 1)/2\lambda \rfloor$, with r being the repetition number of the design.

1. Geometric designs and their codes

Let q be a prime power p^m and V be a vector space of finite dimension v over the finite field $\mathbb{F}_q$. For $0 \leq k \leq v$, we denote by $\begin{bmatrix} V \\ k \end{bmatrix}_q = \{U \leq V \mid \dim U = k\}$ the set of k-dimensional subspaces of V. The cardinality of $\begin{bmatrix} V \\ k \end{bmatrix}_q$ can be expressed by the *Gaussian coefficients* $\#\begin{bmatrix} V \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v-1)\cdots(q^{v-k+1}-1)}{(q^k-1)\cdots(q-1)}$.

Taking $\mathcal{P} = \begin{bmatrix} V \\ 1 \end{bmatrix}_q$ as set of points and $\mathcal{B} = \begin{bmatrix} V \\ k \end{bmatrix}_q$ as set of blocks, then it is well known [1, 1§2] that $\mathcal{G} = (\mathcal{P}, \mathcal{B})$ is a 2-$(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q)$ design. $\mathcal{G}$ is called *geometric or classical design*. We note that $r = \begin{bmatrix} v-1 \\ k-1 \end{bmatrix}_q$ and $b = \begin{bmatrix} v \\ k \end{bmatrix}_q$. The p-rank for a geometric design $\mathcal{G}$ has been determined by Hamada [3]. The code $C_{\mathcal{G}}$ is called *Projective Geometry code* (PG code), see e.g. [5].

2. Subspace designs

Subspace designs – also called q-analogs of designs – were introduced independently by Ray-Chaudhuri, Cameron, Delsarte in the early 1970s.

Let q be a prime power p^m and V be a vector space of finite dimension v over the finite field $\mathbb{F}_q$. For integers $0 \leq t \leq k \leq v$ and λ a non-negative integer, a pair $\mathcal{D} = (V, \mathcal{B})$, where $\mathcal{B}$ is a collection of k-dimensional subspaces (*blocks*) of V, is called a t-$(v, k, \lambda)_q$ *subspace design* on V if each t-dimensional subspace of V is contained in exactly λ blocks.

A t-$(v, k, \lambda)_q$ design $\mathcal{D}$ consists of $b = \lambda \begin{bmatrix} v \\ t \end{bmatrix}_q / \begin{bmatrix} k \\ t \end{bmatrix}_q$ blocks and every 1-dimensional subspace appears in $r = \lambda \begin{bmatrix} v-1 \\ t-1 \end{bmatrix}_q / \begin{bmatrix} k-1 \\ t-1 \end{bmatrix}_q$ blocks of $\mathcal{D}$. Moreover, every 2-$(v, k, \lambda)_q$ subspace design is also a 2-$(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \lambda)$ combinatorial design.

As subspace design, the set of blocks of a geometric design with the above parameters is the trivial t-$(v, k, \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q)_q$ (subspace) design for all $0 \leq t \leq k$.

3. Majority logic decoding with subspace designs

Let $\mathcal{D}$ be a t-$(v, k, \lambda)_q$ subspace design. Then, $\mathcal{D}$ can be regarded as combinatorial 2-$(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \lambda_2)$ design. The rows of its block-point incidence matrix $N_{\mathcal{D}}$ are a subset of the rows of the incidence matrix $N_{\mathcal{G}}$ of the 2-$(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q)$ geometric design $\mathcal{G}$. Since if rows are removed from a matrix, its rank can only get smaller or stay constant, it is a simple observation that $\operatorname{rank}_p N_{\mathcal{D}} \leq \operatorname{rank}_p N_{\mathcal{G}}$. Therefore, codes from subspace designs are either the same codes as those from the corresponding geometric designs or contain these codes.

The number of errors ℓ which can be corrected by one-step majority logic decoding is $\ell = \lfloor \frac{r+\lambda-1}{2\lambda} \rfloor$. Thus, ℓ can be bounded by

$$\lfloor (\frac{q^{v-1}-1}{q^{k-1}-1} - 1)/2 \rfloor \leq \ell \leq \lfloor (\frac{q^{v-1}-1}{q^{k-1}-1} - 1)/2 + \frac{1}{2\lambda} \rfloor ,$$

i.e. the choice of λ is irrelevant for the error-correction capability of the code.

The advantage of taking a subspace design with small λ over the trivial design is the reduced complexity of the decoder. For every position of a received word, the decoder runs through those r blocks of the design which contain the corresponding point. Therefore, subspace designs with small values of λ are preferable and the trivial subspace design is the worst choice since it attains the maximal value of λ.

The same can be concluded for the affine designs from subspace designs.

The above considerations lead to the

Generalized Hamada conjecture: A t-$(v,k,\lambda)_q$ subspace design $\mathcal{D}$, regarded as combinatorial design, has parameters 2-$(\begin{bmatrix}v\\1\end{bmatrix}_q, \begin{bmatrix}k\\1\end{bmatrix}_q, \lambda)$. The p-rank of $\mathcal{D}$ is minimal among all combinatorial designs with the same parameters.

References

[1] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*, volume 1,2. Cambridge University Press, second edition, 1999.

[2] M. Braun, M. Kiermaier, and A. Wassermann. q-analogs of designs: Subspace designs. In *Network Coding and Subspace Designs*, pages 171–211. Springer, Cham, 2018.

[3] N. Hamada. The rank of the incidence matrix of points and d-flats in finite geometries. *J. Sci. Hiroshima Univ. Ser. A-I Math.*, 32(2):381–396, 1968.

[4] S. W. Ng. On Rudolph's majority-logic decoding algorithm (corresp.). *IEEE Transactions on Information Theory*, 16(5):651–652, Sep 1970.

[5] W. W. Peterson and E. J. Weldon Jr. *Error-correcting codes*. MIT Press Cambridge, 2nd edition, 1972.

[6] L. D. Rudolph. A class of majority logic decodable codes (corresp.). *IEEE Transactions on Information Theory*, 13(2):305–307, April 1967.

On Soft Decision Decoding of Block Codes

Martin Bossert

A novel decoding scheme for hard and soft decision decoding of cyclic codes is described based on [1] and [2]. Proper cyclic shifts and componentwise counting of components of these shifts are exploited. In the hard decision case the decoding performs better than the binary Johnson radius and, in addition, gives reliability information which can be the basis for various variants of decoding algorithms. Further, soft decision information from the detection can be exploited in the decoding. Since the novel decoding algorithm performes better in case of low rate codes, the Plotkin construction is used to construct and decode codes with higher rate. This construction combines two codes and it is proved that a 3 dB better channel can be obtained for decoding the second code.

BCH Codes. Let α be a primitive element of the field $\mathbb{F}_q$ with $q = 2^m$ and let $n = q - 1$. A BCH(n,k,d) code uses the cyclotomic cosets $K_i = \{i \cdot 2^j, j = 0,1,\ldots,m-1\}$ which are the conjugate roots in order to create polynomials with roots from the base field $\mathbb{F}_2$. For any K_i we can create a monomial

$$m_i(x) = \prod_{j \in K_i} (x - \alpha^{-j}).$$

The generator polynomial of a BCH code of length n is the product of a set of different monomials $m_i(x)$. For the generator polynomial $g(x) = \prod m_i(x)$ the dimension is $k = n - \deg g(x)$. The designed minimum distance is d if $g(x)$ has $d-1$ consecutive roots.

Error Models. In the binary case we transmit n code bits c_i over a binary symmetric channel (BSC). A symbol is corrupted by an error ε_i and the symbol $r_i = c_i + \varepsilon_i$ is received. Thus, if τ errors in the n transmitted symbols at the positions $e_1, e_2, \ldots, e_\tau$ have occured, we denote this error-polynomial by

$$\varepsilon(x) = x^{e_1} + x^{e_2} + \ldots + x^{e_\tau}.$$

For the AWGN channel we use BPSK modulation with $c_i = 0 \leftrightarrow x_i = 1$ and $c_i = 1 \leftrightarrow x_i = -1$. We receive $y_i = x_i + n_i$ were $n_i \in \mathcal{N}(0, \sigma^2)$ is the Gaussian noise.

Basic Idea. Assume we have a dual codeword of weight $d^\perp$ such that $b(x) = x^{b_1} + x^{b_2} + \ldots + x^{b_{d^\perp}}$ with $b_1 = 0$. Since the code is cyclic this is possible. Let the polynomial $w(x)$ be the multiplication of the dual codeword $b(x)$ with the received polynomial $r(x)$. This polynomial $w(x)$ is identical to the multiplication of $b(x)$ with the error $\varepsilon(x)$. Since by definition of the dual code we have $c(x)b(x) = 0 \mod (x^n - 1)$ and therefore,

$$\begin{aligned} w(x) = r(x)b(x) &= (c(x) + \varepsilon(x))b(x) \\ &= c(x)b(x) + \varepsilon(x)b(x) = \varepsilon(x)b(x) \mod (x^n - 1). \end{aligned}$$

We can interpret $w(x)$ as cyclic shifts of the error $\varepsilon(x)$ and add these shifts (coefficients are added in $\mathbb{F}_2$) as follows

$$\begin{aligned} w(x) &= x^{b_1}\varepsilon(x) + \ldots + x^{b_{d^\perp}}\varepsilon(x) \mod (x^n - 1) \\ &= x^{e_1} + x^{e_2} + \ldots + x^{e_\tau} + \\ &\quad x^{e_1+b_2} + x^{e_2+b_2} + \ldots + x^{e_\tau+b_2} + \\ &\quad \vdots \\ &\quad x^{e_1+b_{d^\perp}} + x^{e_2+b_{d^\perp}} + \ldots + x^{e_\tau+b_{d^\perp}}, \end{aligned}$$

where the exponents $e_i + b_j$ are calculated mod n. Note that $w(x) \in \mathcal{C}^\perp$ and therefore, $d^\perp \le \operatorname{wt} w(x) \le \min\{\tau d^\perp, n\}$ for all $\varepsilon(x) \notin \mathcal{C}$. In fact, any non-zero coefficient of $w(x)$ is an error or a shifted error. If an even number of the shifts of $\varepsilon(x)$ will have a 1 at position j then $w_j = 0$. We can shift the non-zero coefficients of $w(x)$ (which are shifted errors) back to their original position by cyclically shifting the polynomial $w(x)$ by the values $b_j \in \{-b_2, -b_3, \ldots, -b_{d^\perp}\}$ and thus, have $d^\perp$ polynomials $x^{b_j} w(x) \mod (x^n - 1)$. Since shifting does not change the weight, every 1 of $w(x)$ is in one of the $d^\perp$ shifts at an original error position. In other words, in the set of all $d^\perp$ shifts we have at least $\operatorname{wt} w(x)$ errors at their original position. That we have at least $\operatorname{wt} w(x)$ errors at their original position is due to the fact that a shifted error (which stays non-zero in w) can be possibly also at another error position in some shift. In each shift of $w(x)$ we have in average at least $\operatorname{wt} w(x)/d^\perp$ errors at the original position of the τ errors while

the remaining $\mathrm{wt}\, w(x) - \mathrm{wt}\, w(x)/d^\perp$ positions are at the $n-\tau$ non-error positions. The summation of the $d^\perp$ shifts of $w(x)$ calculates the frequency of occurrence of ones at the n code positions

$$\Phi = \sum_{j \in \sup\, b(x)} \left(x^{-j} w(x)\right) \mod (x^n - 1),$$

where the summation of the coefficients is done as integer addition. Clearly the value Φ_j is the number of ones at position j in the $d^\perp$ shifts of $w(x)$. The largest values correspond to errors and can be iteratively corrected.

Example. We use the BCH$(63, 24, 15)$ to illustrate several aspects. Note that this code is the best code known with this parameters. The table shows the expected $E[]$ and the simulated $AV[]$ values of Φ depending on the number of errors τ and e denotes error and c non-error positions and $E[\omega]$ is the expected weight of $w(x)$.

τ	5	6	7	8	9
$E[\omega]$	25.2	27.2	28.6	29.6	30.3
$E[\Phi_e(\tau)]$	181.5	163.0	146.9	133.3	121.3
$AV[\Phi_e(\tau)]$	192.2	179.5	169.5	162.3	156.7
$E[\Phi_c(\tau)]$	109.5	118.4	128.6	135.7	153.0
$AV[\Phi_c(\tau)]$	108.6	120.1	125.7	131.3	135.6
$E[\Phi_{max}]$	196.8	188.9	181.6	175.9	141.5

According to the numbers in the table one should expect that decoding above half the minimum distance is possible. Indeed, the decoding of the BCH$(63, 24, 15)$ performes as a decoder which can correct 9 errors which is 2 more than half the minimum distance. Bit flipping decoding of this code can be found in [5].

Plotkin Construction. The construcion [3] combines two codes to construct a code of doubled length. Given $\mathcal{C}^{(1)}(n, k_1, d_1)$ and $\mathcal{C}^{(2)}(n, k_2, d_2)$ both $\subset \mathbb{F}_2^n$ then

$$\mathcal{C}(2n, k_1 + k_2, \min\{2d_1, d_2\}) = \{c = (c^{(1)} \mid c^{(1)} + c^{(2)}),\, c^{(i)} \in \mathcal{C}^{(i)}\}.$$

The length $2n$ and the dimension $k = k_1 + k_2$ are obvious. For the minimum distance we describe a possible decoder for $\mathcal{C}$. After the BSC we receive $r = c + e = (c^{(1)} + e^{(1)} \mid c^{(1)} + c^{(2)} + e^{(2)})$.

The first step is the addition of the right and the left half which gives $c^{(1)} + e^{(1)} + c^{(1)} + c^{(2)} + e^{(2)} = c^{(2)} + e^{(1)} + e^{(2)}$. Since $\mathrm{wt}(e) \geq \mathrm{wt}(e^{(1)} + e^{(2)})$ the $c^{(2)}$ will be correctly decoded if $\tau = \mathrm{wt}(e) \leq \frac{d^{(2)}-1}{2}$.

The second step assumes that $c^{(2)}$ is correct and adds $c^{(2)}$ to the right half which is $c^{(1)} + e^{(2)}$. In addition we have the left half $c^{(1)} + e^{(1)}$. Assume $d^{(1)} - 1$ errors in both halfs. These can be distributed only such that either $c^{(1)} + e^{(1)}$ or $c^{(1)} + e^{(2)}$ contains $\leq \frac{d^{(1)}-1}{2}$ errors. Decoding both and choosing the smaller error weight corrects, thus, the minimum distance is $2d_1$.

Define $x^{(1)} \odot x^{(2)} = (x_0^{(1)} x_0^{(2)}, x_1^{(1)} x_1^{(2)}, \ldots, x_{n-1}^{(1)} x_{n-1}^{(2)})$, where $x_i = (-1)^{c_i}$, then

$$\{c = (c^{(1)} \mid c^{(1)} + c^{(2)})\} \Longleftrightarrow \{x = (x^{(1)} \mid x^{(1)} \odot x^{(2)})\}.$$

For BPSK over AWGN channel we receive $y = x + n = (y^{(1)} \mid y^{(2)}) = (x^{(1)} + n^{(1)} \mid x^{(1)} \odot x^{(2)} + n^{(2)})$. The addition of the left and right half is here $\hat{y}^{(2)} = y^{(1)} \odot y^{(2)}$ or $\hat{y}_i^{(2)} = \text{sign}(y_i^{(1)} y_i^{(2)}) \min\{|y_i^{(1)}|, |y_i^{(2)}|\}$. Soft decoding of $\hat{y}^{(2)}$ gives $x^{(2)}$ and we assume it is correct. Then we have $x^{(1)} + n^{(1)}$ and $x^{(1)} + n^{(2)}$ both $\in \mathcal{N}(1, \sigma^2)$ or $\in \mathcal{N}(-1, \sigma^2)$. The addition of these gives $\in \mathcal{N}(\pm 2, 2\sigma^2)$. The amplitude has factor 2 and thus the signal power has factor 4, however the noise power (variance) is only doubled. Hence, factor 2 gain $\longrightarrow$ 3 dB. The combination $y^{(1)} + x^{(2)} \odot y^{(2)}$ dates back to 1995 and can be found in step 2b on page 376 in [4]. Then it was derived in [6] in 2002 and called equivalent channel. Finally, in [7] it was shown that with this combination channel capacity is achievable.

References

[1] M. Bossert, *An Iterative Hard and Soft Decision Decoding Algorithm for Cyclic Codes*, 12^{th} Intern. ITG Conference on Systems, Communications and Coding, Rostock, February 2019

[2] M. Bossert, *On Hard and Soft Decision Decoding of Block Codes*, Invited Talk, 2019 Joint Workshop on Communications and Coding (JWCC), `https://www.lnt.ei.tum.de/events/2019-joint-workshop-on-communications-and-coding-jwcc`

[3] M. Plotkin, *Binary codes with specific minimum distances*, IEEE Trans. Inf. Theory, vol. 6, pp. 445–450, 1960.

[4] M. Bossert, *Channel Coding for Telecommunications*, John Wiley and Sons Ltd., 1999.

[5] M. Bossert, F. Hergert, *Hard- and soft-decision decoding beyond half the minimum distance – An algorithm for linear codes*, IEEE Trans. Inf. Theory, vol. 32, pp. 709–714, 1986.

[6] N. Stolte, *Rekursive Codes mit der Plotkin-Konstruktion und ihre Decodierung*, Dissertation TU Darmstadt, 2002.

[7] E. Arikan, *Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels*, IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 3051–3073, 2009.

Symbol Erasures in Random Network Coding

Anna-Lena Horlemann-Trautmann

(joint work with Heide Gluesing-Luerssen)

Network coding in general, and random (or non-coherent) network coding in particular, has received much attention during the last 20 years. In random network coding we want to communicate information over a network to several receivers. To increase the information throughput we allow the inner nodes of the network to create random linear combinations of the incoming information and forward this linear combination along the outgoing edges. In the classical setup, as used in [1], the edges of a network are q-ary symmetric channels, i.e., during transmission symbols from $\mathbb{F}_q$ may change into other symbols of $\mathbb{F}_q$. In this talk however, we focus on networks whose edges are erasure channels, i.e., symbols are either unchanged or erased during transmission. A symbol erasure will be denoted by "?". This scenario has been studied significantly less than the classical setup, but some work exists. For instance, in [2] the authors define *hybrid codes* to correct both symbol erasures and classical errors.

Subspace codes, first introduced in [1], are a widely used class of codes well suited for error correction in random network coding. They are defined as sets of subspaces of some given vector space of dimension n over a finite field $\mathbb{F}_q$ with a specified subspace distance, or equivalently, with a prescribed maximal pairwise intersection dimension. One of the most studied families of subspace codes are *spread codes* (or simply *spreads*). It is well known that these codes exist whenever $k|n$. We will use the following construction of (Desarguesian) spread codes: Let $P \in \mathrm{GL}_k(q)$ be the companion matrix of a monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree k. Fix $m \in \mathbb{N}$ and set $n = mk$. Then

$$\mathcal{C} = \left\{ \mathrm{rowspace}(0_{k\times k} \mid \ldots \mid 0_{k\times k} \mid I_k \mid B_{i+1} \mid \ldots \mid B_m) \,\middle|\, i = 1, \ldots, m,\ B_i \in \mathbb{F}_q[P] \right\}$$

is a spread code in $\mathcal{G}_q(k, n)$.

In this work we investigate the performance of spread codes over an erasure-only network channel. More precisely, we compare the symbol erasure correction capability and the probability of decoding success of spread codes in two different network channel models: the *row erasure channel (REC)*, which is modeled as

$$R = AU + E\mathbf{1}_n$$

and the *column erasure channel (CEC)*, modeled as

$$R = AU + \mathbf{1}_k E$$

where $U \in \mathbb{F}_q^{k\times n}$ is a basis matrix of the codeword, $R \in \mathbb{F}_q^{k\times n}$ is the received word, $A \in \mathbb{F}_q^{k\times k}$ represents the linear transformations of the inner nodes, and $E \in \{0, ?\}^{k\times n}$ is the symbol erasure matrix. In the first case, E is multiplied by the all-one matrix on the right, which makes an erasure spread over the whole row, in the latter, E is multiplied by the all-one matrix on the left, which makes an erasure spread over the whole column.

For simplicity we assume that all symbol erasures occur independently and with the same erasure probability p.

When using a spread code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ over these two channels, we get the following results:

- In both, the REC or the CEC, the code $\mathcal{C}$ can correct any erasure pattern $E \in \{0, ?\}^{k\times n}$ with at most $k-1$ nonzero entries. On the other hand, there exist erasure patterns in $\{0, ?\}^{k\times n}$ with k nonzero entries that cannot be corrected. Thus, the symbol erasure correction capability in the classical sense is $k - 1$ for both channels.
- On the REC there are
$$r(n, k) := 2^{kn} - (2^n - 1)^k$$
symbol erasure patterns $E \in \{0, ?\}^{k\times n}$ that can be corrected by $\mathcal{C}$.
- Using $\mathcal{C}$ over the REC, the probability of decoding success is
$$P_{\mathrm{row}} := 1 - \left(1 - (1 - p)^n\right)^k.$$

- Over the CEC the number of correctable erasure patterns depends on the codeword. Overall, the code $\mathcal{C}$ can correct on average (at least)
$$e_{\text{avg}} := \frac{N^m}{q^n-1}\Big(q^n - \Big[\frac{(q^k-1)(N-1)}{N}+1\Big]^m\Big)$$
symbol erasure patterns.
- By averaging over all possible codewords in $\mathcal{C}$, the probability of decoding success over the CEC is
$$\begin{aligned} P_{\text{avg}} &:= \frac{1}{q^n-1}\sum_{\ell=0}^{m-1}\tbinom{m}{\ell+1}(q^k-1)^{\ell+1}P_\ell \\ &= \frac{\pi_0^m}{q^n-1}\Big[q^n - \Big(\frac{(q^k-1)\pi_1}{\pi_0}+1\Big)^m\Big], \end{aligned}$$
where
$$\pi_0 := \sum_{j=0}^{k-1}\binom{k}{j}\pi^j(1-p)^{k(k-j)},$$
$$\pi_1 := \sum_{j=1}^{k-1}\binom{k}{j}\pi^j(1-p)^{k(k-j)} = \pi_0 - (1-p)^{k^2}.$$

To compare the two probabilities of decoding success we show that the one for the CEC grows much faster than the one for the REC:

- For sufficiently large $m = n/k$,
$$\frac{P_{\text{row}}(n,k)}{P_{\text{avg}}(n,k)} \le k(1-p)^{k-k^2}\Big(\frac{(1-p)^k}{\pi_0}\Big)^{m-1}.$$
As a consequence, for any fixed k we have $\lim_{m\to\infty}\frac{P_{\text{row}}(n,k)}{P_{\text{avg}}(n,k)} = 0$.

Furthermore, we compare the previous results to the erasure correction capability of hybrid codes, as defined in [2], in the CEC. These hybrid codes are defined as compositions of subspace codes with Reed-Solomon codes. Since hybrid codes have different information rate than spread codes for the same k and n, we need to compare the erasure correction capability for codes of approximately the same rate, but different values for k and n. The results depend on the parameters: for (very) small values of $m = n/k$ spread codes have a higher probability of decoding success, whereas for growing m hybrid codes perform better. However, spread codes have the advantage that they can be defined over any underlying field, whereas for hybrid codes we need field sizes in the range of n. Moreover, decoding can be done more efficiently for spread codes than for hybrid codes. Therefore, depending on the application, any of the two codes can be advantageous.

Remark: The results presented in this report and in the corresponding presentation have been published in [3]. In there, the channel models, the erasure correction capabilities of spread and hybrid codes, as well as the corresponding decoding algorithms are described in more detail. Furthermore, the performance of spread

and hybrid codes in a column erasure channel, where also deletions (i.e., row erasures) might occur, is analyzed.

References

[1] R. Kötter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory, **54**(8):3579–3591, 2008.
[2] V. Skachek, O. Milenkovic and A. Nedić, *Hybrid noncoherent network coding*, IEEE Transactions on Information Theory, **59**(6):3317–3331, 2013.
[3] H. Gluesing-Luerssen and A.-L. Horlemann-Trautmann, *Symbol erasure correction in random networks with spread codes*, IEEE Transactions on Information Theory, **65**(4):2075–2091, 2019.

QQR Codes, Points on Hyperelliptic Curves, and Goppa's Conjecture

Nigel Boston
(joint work with Jing Hao)

This extended abstract concerns a fundamental question in coding theory. We are interested in linear codes over the field F of size 2. These are linear subspaces C of F^n. There are 3 important numbers associated to C, namely n, the dimension of C usually denoted k, and its minimum distance d, which is the smallest number of coordinates in which two unequal elements of C differ. Good codes have many well-spaced codewords, and so have both rate $R := k/n$ and relative minimum distance $\delta := d/n$ large.

If we plot points (R, δ) obtained for all linear codes over F, then most of them are clustered near the origin and Manin formalized this by proving that there is a curve $R = \alpha_2(\delta)$ below which the points are dense and above which there are only isolated points. It is therefore of fundamental importance to identify the function α_2 and Goppa conjectured that $\alpha_2(\delta) = 1 - H_2(\delta)$, where $H_2(\delta)$ is the binary entropy function, $-\delta \log_2(\delta) - (1-\delta)\log_2(1-\delta)$.

Quasi-quadratic residue codes are a family of codes that, as we shall see, put Goppa's conjecture to the test. There is one (called QQR(p)) for each odd prime p and the weight (number of nonzero coordinates) of each codeword c_S equals to the number of points on a related hyperelliptic curve, $X_S : y^2 = \prod_{a \in S}(x-a)$, defined over $\mathbf{F}_p$. Here S runs through all 2^p subsets of $\mathbf{F}_p$. This allows for both the injection of ideas from arithmetic statistics into coding theory and the application of coding theory to study the distribution of the number of points as the curve varies.

We focused on $p \equiv 3 \pmod 4$, when QQR(p) is self-dual and has $n = 2p, k = p$. If there are a_i codewords of weight i, then $\sum a_i x^i y^{n-i}$ is called the weight enumerator A of the code. We made some preliminary study of this for QQR(p) and observed (and then proved using the theory of shadows and studying automorphisms of the code) that A is always divisible by $(x^2+y^2)^{d-1}$. In conjunction with Gleason's theorem restricting the form of A for self-dual codes, this allowed us to compute A for p up to 67.

Moreover, we observed and proved a similar result for quadratic residue codes QR(p), namely that their weight enumerators are divisible by $(x+y)^d$. This was then used to discover and correct errors in online tables of weight enumerators of QR codes. We also answered a question of Joyner (in the negative) as to whether the weight enumerators of QQR codes necessarily satisfy Duursma's Riemann Hypothesis.

Next, we used Sidel'nikov's result on the cumulative distribution function of a code to establish that the weight distribution of QQR codes is asymptotically normal as p goes to infinity. This then establishes that, after being symmetrized, the point distribution of the hyperelliptic curves X_S converges to the normal distribution as p goes to infinity, a variant of an unpublished result of Larsen, which was established by very different means.

Finally, back to Goppa's conjecture, where the connection with hyperelliptic curves tells us, as observed by Joyner, that if for infinitely many primes $p \equiv 1 \pmod 4$, $|X_S(\mathbf{F}_p)| < 1.779944271p$ for all $S \subseteq \mathbf{F}_p$, then Goppa's conjecture is false. Letting $M(p) := \max_S |X_S(\mathbf{F}_p)|/p$, by exploiting Hasse-Weil and a study of extremal curves, we computed that for all odd primes $p \leq 61$ except for $p = 41$, $M(p)$ is actually less than this critical value. This gives weak evidence that this approach could lead to a failure of Goppa's conjecture. It was noted that there are curves X_S with 73 points for $p = 41$ and that there exist large p with $M(p)$ as close to 2 as we like by using curves of the form $y^2 = x^d - 1$ for specially chosen d, p.

(Scattered) Linear Sets are to Rank-Metric Codes as Arcs are to Hamming-Metric Codes

John Sheekey
(joint work with Geertrui Van de Voorde)

In this talk we review the classical correspondence between linear codes in the Hamming metric and sets of points in a projective space, and outline the analogous correspondence for codes in the rank metric.

A linear $[n,k]$ code $\mathcal{C}$ over a field $\mathbb{F}_{q^m}$ can be represented by a generator matrix $G \in M_{k\times n}(\mathbb{F}_{q^m})$; the code is then given by $\mathcal{C} = \{xG : x \in (\mathbb{F}_{q^m})^k\}$. The *Hamming weight* of a vector v is defined as $\mathrm{wt}_H(v) = \#\{i : v_i \neq 0\}$, while the *rank weight* is defined as $\mathrm{wt}_R(v) := \dim_{\mathbb{F}_q}\langle v_1, v_2, \ldots, v_n\rangle$.

If $\mathcal{A}$ denotes the set of columns of G, then it is well known that the Hamming weight of a codeword $xG \in \mathcal{C}$ is given by

$$\mathrm{wt}_H(xG) = n - |x^\perp \cap \mathcal{A}|,$$

where $x^\perp := \{y : (\alpha x)\cdot y = 0 \ \forall\ \alpha \in \mathbb{F}_{q^m}\}$, and $|x^\perp \cap \mathcal{A}|$ counts multiplicities. Thus questions regarding the Hamming weight distribution of a code can be translated into questions regarding intersection properties of the set $\mathcal{A}$ with hyperplanes of $(\mathbb{F}_{q^m})^k$. The code $\mathcal{C}$ is MDS if and only if no k of the elements of $\mathcal{A}$ lie on a

common hyperplane; this is precisely the same condition that the set of projective points in $\mathrm{PG}(k-1,q^m)$ defined by $\mathcal{A}$ form an *arc*.

Let us define $\mathcal{L}$ as the $\mathbb{F}_q$-span of the columns of G; $\mathcal{L}$ is then an $\mathbb{F}_q$-subspace of $(\mathbb{F}_{q^m})^k$. Then it is straightforward to show that that

$$\mathrm{wt}_R(xG) = n - \dim_q(x^\perp \cap \mathcal{L}).$$

Thus questions regarding the rank weight distribution of a code can be translated into questions regarding intersection properties of the $\mathbb{F}_q$-subspace $\mathcal{L}$ with the $\mathbb{F}_{q^m}$-subspaces $x^\perp$. Such questions have been studied in finite geometry, where the set of points in $\mathrm{PG}(k-1,q^m)$ defined by $\mathcal{L}$ is referred to as a *linear set*. This correspondence was first noted for the case $k=2$ in [4], and further extended in [5].

Theorem ([5])**.** *Let $\mathcal{C}$ and $\mathcal{C}'$ be two $\mathbb{F}_{q^m}$-linear codes endowed with the rank metric with generator matrices G, G' respectively, and let $\mathcal{L}$ and $\mathcal{L}'$ be the $\mathbb{F}_q$-span of the columns of G and G' respectively.*

(1) The code $\mathcal{C}$ is MRD if and only if the linear set defined by $\mathcal{L}$ is scattered with respect to hyperplanes in $\mathrm{PG}(k-1,q^m)$.
(2) The codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent as rank metric codes if and only if $\mathcal{L}$ and $\mathcal{L}'$ are equivalent under the action of $\Gamma\mathrm{L}(k,q^m)$ on $(\mathbb{F}_{q^m})^k$.

Linear sets have been studied for a variety of reasons; for example blocking sets and two-weight codes. See [2], [3] for background. The above correspondence theorem allows us to translate results from finite geometry into results on rank metric codes, and vice versa. As an example, the following is a corollary of a result in [1]:

If $\mathcal{C}$ is a two-dimensional $\mathbb{F}_{q^m}$-linear rank-metric code in $(\mathbb{F}_{q^m})^m$ with second largest weight $m-e$, then e divides m and all weights in $\mathcal{C}$ are divisible by e. Furthermore, the matrix code in $M_m(\mathbb{F}_q)$ obtained from $\mathcal{C}$ is equivalent to a code in $M_{m/e}(\mathbb{F}_{q^e})$.

There remain many interesting open problems in both rank metric codes and linear sets. This talk is intended to highlight the link between these two areas which proceeded independently for nearly 20 years, and to suggest that researchers in either topic may find useful techniques and interesting open problems in the other.

References

[1] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, T. Szönyi, *On the Number of Slopes of the Graph of a Function Defined on a Finite Field*, J. Combin. Theory Ser. A **86** (1999), 187–196.
[2] M. Lavrauw, *Scattered spaces in Galois geometry*, Contemporary developments in finite fields and applications, 195–216, World Sci. Publ., Hackensack, NJ, 2016.
[3] O. Polverino, *Linear sets in finite projective spaces*, Discrete Math. **310** (2010), 3096–3107.
[4] J. Sheekey, *A new family of linear maximum rank distance codes*, Adv. Math. Commun. **10** (2016), 475–488.
[5] J. Sheekey, G. Van de Voorde, *Rank-metric codes, linear sets, and their duality*, submitted.

Searching for (q-Analogs of) Steiner Triple Systems

Patric R. J. Östergård

Combinatorial designs are well-studied regular discrete structures. An example of a design is the Fano plane, which can be presented as a set system:

$$\{\{0,1,2\},\{0,3,4\},\{0,5,6\},\{1,3,5\},\{1,4,6\},\{2,3,6\},\{2,4,5\}\}.$$

The Fano plane has the property that every 2-subset of the set $\{0,1,2,3,4,5,6\}$ is contained in exactly one of the sets of the set system. The Fano plane is then a 2-$(7,3,1)$ design, when we denote by t-(v,k,λ) a multiset of k-subsets (called blocks) of a v-set (of points) such that each t-subset of the v-set occurs in exactly λ blocks. As we are interested in structural properties of designs, the underlying set of elements is typically irrelevant; we say that two t-designs are isomorphic if there is a bijection between the underlying sets that maps one t-design onto the other. For more information about combinatorial designs in general and various specific types of designs in particular, see [4].

A central problem in design theory is that of determining existence of t-designs with given parameters. If the existence problem can be solved in the positive for some set of parameters, one may proceed and attack the classification problem, which asks for a complete set of representatives from the isomorphism classes. This work has a mathematical as well as a computational flavor [5].

In the framework of vector spaces, one may define analogs of t-(v,k,λ) designs. Let $\mathbb{F}_q^v$ be the v-dimensional vector space over the finite field $\mathbb{F}_q$. A q-analog of a t-(v,k,λ) design is a set S of k-dimensional subspaces of $\mathbb{F}_q^v$, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ elements of S. Whereas the existence problem for 2-$(v,3,1)$ designs—called Steiner triple systems—has been solved, the only known nontrivial existence result for q-analogs of Steiner triple systems is that q-analogs of 2-$(13,3,1)$ designs exist [1].

One big challenge in the study of q-analogs of designs is that the size of the objects is very large already for the smallest admissible parameters. For example, it is a rather straightforward task to manually find and show uniqueness of designs with the parameters of the Fano plane, but so far neither analytical nor computational methods have succeeded in finding a q-analog of the Fano plane or proving that it does not exist. We have seen that the 2-$(7,3,1)$ Fano plane has only 7 blocks, but a q-analog of the Fano plane would consist of as many as 381 3-dimensional subspaces of $\mathbb{F}_2^7$ for $q=2$.

Due to a scarcity of results for q-analogs of Steiner triple systems, the role of bringing known results and concepts from classical designs to the q-analog setting is emphasized. A few such examples will be considered here.

A parallel class of a t-(v,k,λ) design is a set of blocks that partition the set of points. A partition of the blocks of a design into parallel classes is called a resolution and the design is said to be resolvable. A resolvable 2-$(v,3,1)$ design is called a Kirkman triple system. A necessary and sufficient condition for the existence of a Kirkman triple system with v points is that $v \equiv 3 \pmod 6$.

The smallest open case for classifying Kirkman triple systems is $v = 21$. The author and Janne Kokkala have made progress, still unpublished, on the classification of such designs. For example, the case where the designs contain a Fano plane has already been settled. Specifically, in the core of this work are quadrilaterals:

$$\{\{0,1,2\},\{0,3,4\},\{1,3,5\},\{2,4,5\}\}.$$

What would a q-analog of a quadrilateral be? Note that the blocks of the presented quadrilateral intersect each of the sets $\{0,5\}$, $\{1,4\}$, and $\{2,3\}$ in exactly one point and those three pairs of points are precisely the pairs that do not occur in any of the blocks. A (v,g,k,λ) group divisible design (GDD) is a collection of k-subsets (blocks) of a v-set of points and a partition of the points into g-sets (groups), such that each 2-subset of the v-set is contained in either λ blocks or a group but not both. Hence a quadrilateral is a $(6,2,3,1)$ GDD.

In [3], q-analogs of GDDs are studied. A q-analog of a (v,g,k,λ) GDD is a collection of k-dimensional subspaces (blocks) of $\mathbb{F}_q^v$ and a vector space partition into g-dimensional subspaces (groups), such that each 2-dimensional subspace of $\mathbb{F}_q^v$ is contained in either λ blocks or a group but not both.

As a matter of fact, in this setting there is no q-analog of a quadrilateral [3, Lemma 5]. This raises a question about what other substructures could play important roles in the study of q-analogs of Steiner triple systems.

Kirkman triple systems could also be studied in the q-analog setting. Then there has to be a partition of the blocks into sets of blocks that form vector space partitions. Considering such structures at this very moment may sound pointless as already the case of Steiner triple systems is wide open. However, it should be noted that the stronger conditions may be advantageous as they, for example, narrow down and speed up computer searches. The smallest nontrivial case is $v = 9$; in [2] structures "close to" q-analogs of Steiner triple systems with these parameters were found so these may indeed exist (even as Kirkman triple systems).

Finally, by [3] it is possible that there is a q-analog of a $(9,3,3,1)$ GDD. The existence of such a structure would imply the existence of a q-analog of a Steiner triple system with $v = 9$, since the groups can be taken as additional blocks when we have $g = k$. As the groups form a vector space partition (the q-analog of a parallel class), such a system would correspond to a q-analog of a Steiner triple system with (at least) one parallel class.

References

[1] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann, *Existence of q-analogs of Steiner systems*, Forum of Mathematics. Pi **4** (2016), e7.

[2] M. Braun, P. R. J. Östergård, and A. Wassermann, *New lower bounds for binary constant-dimension subspace codes*, Experimental Mathematics **27** (2018), 179–183.

[3] M. Buratti, M. Kiermaier, S. Kurz, A. Nakíc, and A. Wassermann, *q-analogs of group divisible designs*, arXiv:1804.11172.

[4] C. J. Colbourn and J. H. Dinitz (Eds.), *Handbook of Combinatorial Designs*, 2nd ed., Chapman & Hall/CRC, Boca Raton, 2007.

[5] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Springer, Berlin, 2006.

Service rates of codes

Emina Soljanin

Coding has traditionally been used in transmission and storage of data to provide reliability in a more efficient way than simple replication. The traditional performance indicators of codes are the minimum distance and the code rate. More recently, special codes have been developed that also provide efficient maintenance of storage under node failures. In addition to the traditional metrics, the properties of codes that matter in such scenarios are the code locality and availability. Emerging applications, such as distributed learning and fog computing, are adding yet another use for coding. In these applications, the goal is to maximize the number of users that can be simultaneously served by the system. One such service is simultaneous download of different jointly coded data blocks by many users competing for the system's resources. Here, coding affects the rates at which users can be served. Most of the work on data access has been concerned with the download latency (see e.g., [1] and references therein). It has recently been recognized, that another important metric that measures the availability of the stored data is the service rate [2, 3, 4, 5]. Maximizing service rate (or the throughput) of a distributed system helps support a large number of simultaneous system users. This talk introduced the notion of the service rate region of codes and presented some examples where this region is known.

Mathematically, we formulate this problem as follows: There are k files to be stored (redundantly) across n servers. We assume that $n \geq k$ and that files are mathematically elements of some finite field. Each server can store a linear combination of files. We further assume wlog that the time to download a file from server ℓ is exponential with rate μ_ℓ, $1 \leq \ell \leq n$, and that requests to download file i arrive at rate λ_i, $1 \leq i \leq k$. A set of stored symbols that can be used to compute a given file (symbol) is referred to as a recovery set for that file. We denote by $R_{i,1}, \ldots, R_{i,t_i}$ the t_i disjoint recovery sets of file i, and by $\lambda_{i,j}$ the portion of requests for file i that are assigned to the recovery group $R_{i,j}$, $j = 1, \ldots, t_i$. Then the achievable service rate region of such a system is the set of vectors $\lambda = (\lambda_1, \ldots, \lambda_k)$ for which there exist $\lambda_{i,j}$ satisfying the following constraints:

$$\sum_{j=1}^{t_i} \lambda_{i,j} \;=\; \lambda_i \text{ for } 1 \leq i \leq k \quad \text{and} \quad \sum_{i=1}^{k} \sum_{\substack{1 \leq j \leq t_i \\ \ell \in R_{i,j}}} \lambda_{i,j} \;\leq\; \mu_\ell \text{ for } 1 \leq \ell \leq n.$$

The first set of constraints ensures that the demands for all files are served, and the second set ensures that no node is sent requests in excess of its service rate.

Interestingly, the best schemes (those that maximize the achievable service rate region) often combine replication and coding. To see that, we consider an example shown in Fig. 1, which also illustrates an application. The system consists of 2 cameras monitoring two intersecting streets. One of the cameras acquires content a concerning the traffic on one of the streets, and the other content b concerning the other street. Suppose we can store files a and b redundantly on 4 nodes. Fig. 1 (left) shows 3 redundant storage examples: replication, coding, and combined replication

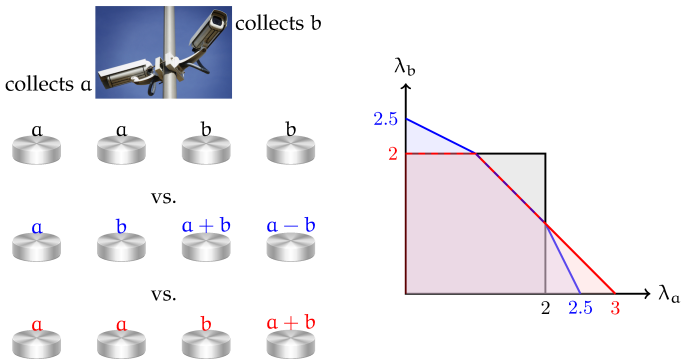

FIGURE 1. (left) Replicated, coded, and hybrid systems with $n = 4$ nodes storing $k = 2$ files. (right) Service capacity regions of the three systems when the service capacity of each node is $\mu = 1$. The regions have the same areas. Coding can handle the skews in request arrival rates λ_a and λ_b for the two stored objects.

and coding. Given that each node can serve $\mu = 1$ requests per second, we want to maximize λ_a and λ_b, the rate of requests for a and b that can be supported. File a can be downloaded from the node storing a, or from two nodes that store combinations of a and b. Fig. 1 (right) shows that coded systems can handle skews in content popularity better than replicated systems. Combined replication and coding can better support asymmetries in demands. This capability is important if the interests in traffic a vs. traffic b change e.g., depending on the time of the day, and if they are high then they are seldom equally likely. Regarding the reliability under node failures, we observe that the coded system preserves data if any two nodes fail, the replication system preserves data if at most one of a nodes and at most one of b nodes fail, and the hybrid system preserves data if any two nodes fail unless both b and $a + b$ nodes fail.

REFERENCES

[1] S. Kadhe, E. Soljanin, and A. Sprintson, "Analyzing download time for availability codes," in *Proceed. 2015 IEEE Internat. Symposium on Information Theory (ISIT'15).*

[2] M. Noori, E. Soljanin, and M. Ardakani, "On storage allocation for maximum service rate in distributed storage systems," *Proceed. 2016 IEEE Internat. Symposium on Information Theory (ISIT'16).*

[3] M. Aktas, S. E. Anderson, A. Johnston, G. Joshi, S. Kadhe, G. L. Matthews, C. Mayer, and E. Soljanin, "On the service capacity region of accessing erasure coded content," *Proceed. 2017 Allerton Conf. on Communica-tion, Control, and Computing.*

[4] P. Peng and E. Soljanin, "On distributed storage allocations of large files for maximum service rate," *Proceed. 2018 Allerton Conf. on Communica-tion, Control, and Computing.*

[5] S. E. Anderson, A. Johnston, G. Joshi, G. L. Matthews, C. Mayer, and E. Soljanin, "Service Rate Region of Content Access from Erasure Coded Storage," *Proceed. 2018 IEEE Internat. Workshop on Information Theory (ITW'18).*

Making McEliece and Regev meet

Gilles Zémor

The McEliece paradigm. For decades, devising a code-based public-key cryptosystem was based on the McEliece paradigm, spelt out in the seminal 1978 paper [1]. The idea is to choose a linear code C that comes with an efficient decoding algorithm, and to publish a *random* generator matrix $\mathbf{G}$. The trapdoor encryption primitive is defined as

$$\begin{aligned} \mathcal{M} = \{0,1\}^m &\rightarrow \{0,1\}^n \\ \mathbf{m} &\mapsto \mathbf{mG} + \mathbf{e} \end{aligned}$$

where $\mathbf{e}$ is a random vector of predetermined small weight t (we speak of an encryption primitive because semantic security needs to be added to it to obtain a genuine cryptosystem). The public matrix $\mathbf{G}$ should "look like" the generator matrix of a random code and it is expected that an attacker who wishes to access $\mathbf{m}$ can do no better than tackle the generic problem of decoding a random linear code. The legitimate receiver has access to the hidden decoding algorithm and can therefore decrypt efficiently. The original McEliece cryptosystem chooses the code C to be a random binary Goppa code. This has proved to be quite successful, but relies upon the assumption that it is not feasible to recover a Goppa code's hidden structure from a random generator matrix. In practice, this is indeed the case, but we do not have a formal assurance that recovering the hidden structure reduces to solving a well-identified problem that fits nicely in present-day complexity theory. This has for long left the McEliece cryptosystem under the suspicion that a method for breaking it exists and is waiting to be discovered.

Many alternatives to the use of Goppa codes have been proposed over the years, and many of them have been broken. The modern variant, MDPC-McEliece [2] is interesting in that it replaces Goppa codes with codes with a very weak structure, making it credible that no efficient recovery algorithm exists that exposes the hidden properties. A Moderate Density Parity Check (MDPC) code is defined by a parity-check matrix whose rows all have weight w. It comes with a natural decoding algorithm, the *bit-flipping* algorithm, which consists in deciding, in parallel for every bit position i, to flip its value whenever doing so decreases the syndrome weight: the process is iterated several times. The number t of correctable errors by bit-flipping is approximately n/w. The time-complexity of decoding a random linear code from t errors by Information Set decoding techniques (essentially the best we know) is approximately 2^t, and the time-complexity of recovering the hidden words of weight w is, by similar techniques also of the order 2^w. By choosing $w \approx \sqrt{n}$ one maximises the difficulty of breaking the scheme by known methods, making it of the order $2^{\sqrt{n}}$.

The Alekhnovich paradigm. At the turn of the century, Alekhnovich [3] came up with a radically new way of devising a public-key cryptosystem based on coding theory, by departing from the McEliece approach. Instead of devising a somewhat practical scheme and then doing one's best to evaluate its security, Alekhnovich

devised a scheme specifically so that it came with a proof that breaking it implies the existence of an algorithm that decodes random linear codes. This came at the cost of making the scheme totally impractical, but subsequent variants made the idea more and more efficient and the point we are making in this talk is that these more efficient variants come to closely ressemble MDPC-McEliece. In fact, we can propose a variation that can be seen either as a slightly modified MDPC-McEliece scheme, or a slightly modified Alekhnovich-Regev type scheme. This variation has arguably the best of both worlds in that it is only slightly less efficient than MDPC-McEliece, but breaking it provably reduces to the difficulty of decoding random linear codes.

One of Alekhnovich's core ideas, itself inspired by Ajtai's work on lattices, is to introduce the following decision problem D.

- *Input:* A uniform binary random matrix $\mathbf{H}$, together with a binary vector $\mathbf{y}$ of length n such that:
  (1) $\mathbf{y}$ is either chosen randomly uniformly,
  (2) or $\mathbf{y}$ is of the form $\mathbf{sH} + \boldsymbol{\varepsilon}$ where $\mathbf{s}$ is uniform random and where $\boldsymbol{\varepsilon}$ is a random vector whose weight is some parameter t. In other words $\mathbf{y}$ is at distance t from a random vector in the code generated by the rows of $\mathbf{H}$.
- *Problem:* Decide whether we are in case (1) or (2).

It turns out that any algorithm that solves problem D with a probability of success significantly better than pure guessing can be transformed into an algorithm that decodes random linear codes [4, 6] from random errors of weight t. So if we assume that decoding random linear codes is difficult, it must hold that there is no efficient algorithm that solves problem D better than pure guessing.

The "Regev" version of Alekhnovich's cryptosystem is as follows [5, 7]. The message space is $\{0, 1\}$ (one bit).

- *Public key:* $\mathbf{H}$, $\mathbf{y} = \mathbf{sH} + \boldsymbol{\varepsilon}$.
- *Secret key:* $\mathbf{s}$.
- *Encryption:* $\mathcal{C}(m) = (\mathbf{He}^T, \mathbf{z} = m + \langle \mathbf{e}, \mathbf{y} \rangle)$.
- *Decryption:* $\mathbf{z} + \mathbf{sHe}^T = m + \langle \mathbf{e}, \boldsymbol{\varepsilon} \rangle$.

Both vectors $\mathbf{e}$ and $\boldsymbol{\varepsilon}$ are chosen randomly of weight $t < \sqrt{n}$. Decryption works because the probability that $\langle \mathbf{e}, \boldsymbol{\varepsilon} \rangle \neq 0$ is small. There is a non-zero probability however, that decryption may fail.

Once problem D has been introduced, the security reduction is very simple. If there is an attack against the cryptosystem, it must work just as well when the vector $\mathbf{y}$ is chosen at random uniformly in the whole space, otherwise we would have a distinguishing algorithm that solves problem D. But then, for the same reason, the attack should continue to work just as well when the small-weight vector $\mathbf{e}$ is replaced by a random vector chosen uniformly in the whole space. But after both those transformations, the ciphertext is simply random noise, so nothing can decipher it. Therefore, either it is possible to solve efficiently problem D and hence decode random linear codes, or the cryptosystem is unbreakable.

Consider now the following "vector" version of the above cryptosystem.

- *Public key:* $\mathbf{H}$, $\mathbf{Y} = \mathbf{SH} + \mathbf{E}$. $\mathbf{S}$ and $\mathbf{E}$ are matrices, and every row of $\mathbf{E}$ is chosen to be of weight t. In other words the couple $(\mathbf{s}, \boldsymbol{\varepsilon})$ of the original cryptosystem is replaced by several independent copies of it. Let C be the code whose parity-check matrix is $[\begin{smallmatrix}\mathbf{H}\\ \mathbf{Y}\end{smallmatrix}]$. Let $\mathbf{G}$ be a generator matrix for the code C.
- *Secret key:* $\mathbf{E}$.
- *Encryption:* $\mathbf{m} \mapsto \mathcal{C}(\mathbf{m}) = \mathbf{mG} + \mathbf{e}$. The vector $\mathbf{e}$ is random of weight t as before. The plaintext $\mathbf{m}$ is a vector of length ℓ, the number of rows of the matrix $\mathbf{G}$.
- *Decryption:* compute $\mathbf{E}\mathcal{C}(\mathbf{m})^T = \mathbf{E}\mathbf{e}^T$. This is the syndrome of $\mathbf{e}$ for the (secret) matrix $\mathbf{E}$. *We may use bit-flip (MDPC) decoding to recover* $\mathbf{e}$ *from* $\mathbf{E}$.

Note that when $\mathbf{H} = 0$ we are back to the original MDPC-McEliece encryption primitive. Adding the random matrix $\mathbf{H}$ to the MDPC-McEliece scheme enables us to obtain therefore an Alekhnovich-Regev-type scheme, which has the added value of having a security proof which reduces security to the problem of decoding random linear codes. The McEliece and Alekhnovich paradigms have come together!

These ideas have undergone further developments that appear in the BIKE suite [8].

References

[1] R. J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, Deep Space Network Progress Report, **44** (1978), 114–116.

[2] R. Misoczki, J.-P. Tillich, N. Sendrier, P. Barreto, *MDPC-McEliece: New McEliece variants from moderate density parity-check codes*, 2013 IEEE International Symposium on Information Theory, 2069–2073.

[3] M. Alekhnovich, *More on average case vs approximation complexity*, Comput. Complex. **20** (2011), 755–786. Preliminary version in FOCS 2003.

[4] B. Applebaum, Y. Ishai and E. Kushilevitz, *Cryptography with constant input locality*, *J. Cryptology* **22** (2009), 429–469.

[5] I. Damgård and S. Park, *Is Public-Key Encryption Based on LPN Practical?* `https://eprint.iacr.org/2012/699.pdf`

[6] L. Trevisan, *Some Applications of Coding Theory in Computational Complexity*, Electronic Colloquium on Computational Complexity, Report No. 43 (2004).

[7] C. Aguilar, O. Blazy, J.-C. Deneuville, P. Gaborit and G. Zémor, *Efficient Encryption from Random Quasi-Cyclic Codes*, IEEE Trans. on Information Theory **64**, no. 5 (2018), 3927–3943.

[8] `https://bikesuite.org/`

On the lengths of divisible codes

Michael Kiermaier
(joint work with Thomas Honold, Sascha Kurz, Alfred Wassermann)

1. Divisible Codes

Divisible codes have been introduced by Ward in 1981 [6]. An $\mathbb{F}_q$-linear code is called Δ-*divisible* if all its weights are divisible by Δ. The main case of interest is that Δ is a power of the characteristic of the base field. In this talk, we consider the case $\Delta = q^r$ with $r \in \mathbb{N}_0$.

Divisible codes are interesting for several reasons. Many good codes are divisible. There are connections to self-dual and self-orthogonal codes as well as Griesmer-optimal codes. In this talk, we concentrate on applications in finite geometry and the theory of subspace codes.

Ward's "divisible code bound" [7] gives an upper bound on the dimension of a divisible code, depending on an upper and lower bound on the weights. We follow kind of an orthogonal approach and investigate the lengths of divisible codes, independently of the dimension. As divisible codes can always be extended by all-zero positions, it is natural to look at the *effective length*, which is the number of coordinates which are not all-zero.

For that purpose, we define the numbers $s_q(r,i) = q^i \cdot \frac{q^{r-i+1}-1}{q-1}$, which have the property $q^i \mid s_q(r,i)$, but $q^{i+1} \nmid s_q(r,i)$. This allows us to create kind of a positional system upon the sequence of base numbers $S_q(r) = (s_q(r,0), s_q(r,1), \ldots, s_q(r,r))$. Each integer n has a unique $S_q(r)$-*adic expansion* $n = a_0 s_q(r,0) + a_1 s_q(r,1) + \ldots + a_r s_q(r,r)$ with $a_0, \ldots, a_{r-1} \in \{0, \ldots, q-1\}$ and *leading coefficient* $a_r \in \mathbb{Z}$. The *cross sum* of the $S_q(r)$-adic expansion of n is $a_0 + a_1 + \ldots + a_r$. Now we can state the following characterization of the effective lengths of q^r-divisible codes:

Theorem 1 ([4, Th. 1])**.** *Let $n \in \mathbb{Z}$ and $r \in \mathbb{N}_0$. Then the following are equivalent:*

(i) There exists a q^r-divisible $\mathbb{F}_q$-linear code of effective length n.
(ii) The leading coefficient of the $S_q(r)$-adic expansion of n is non-negative.

As a byproduct of the proof, we get the following bound on the maximum weight of a divisible code.

Theorem 2 ([4, Th. 2])**.** *Let C be a q^r-divisible code of effective length n. Then the maximum weight of C is at most σq^r, where σ denotes the cross-sum of the $S_q(r)$-adic expansion of n.*

2. Partial spreads

Let V be a $\mathbb{F}_q$-vector space of finite dimension v. A set $\mathcal{S}$ of $(k-1)$-flats in $\mathrm{PG}(V)$ is called a *partial spread* if the elements of $\mathcal{S}$ have pairwise trivial intersection. Equivalently, each point of $\mathrm{PG}(V)$ is covered by at most one element in $\mathcal{S}$. The points not covered by any element of $\mathcal{S}$ are called *holes*. An important research question asks for the maximum possible size $A_q(v,k)$ of a partial spread.

In the case $v \mid k$, it is possible to cover all the points of $\mathrm{PG}(V)$ by a *spread* $\mathcal{S}$, showing that $A_q(v,k) = \frac{q^v-1}{q^k-1}$. Otherwise, write $v = tk+r$ with $r \in \{0,\dots,k-1\}$ and assume $t \geq 2$. In 1975, Beutelspacher gave a construction showing that $A_q(v,k) \geq \frac{q^v-q^{k+r}}{q^k-1} + 1$. Furthermore, he proved that the construction is optimal for $r = 1$ [1]. Recently, a considerable progress has been made by Năstase and Sissokho, showing that Beutelspacher's construction is optimal whenever $k > \frac{q^r-1}{q-1}$ [5, Th. 1].

We demonstrate how this result follows as a corollary from Theorem 1, see also [4, Cor. 2]. The crucial observation is that the set $\mathcal{P}$ of holes of a partial $(k-1)$-spread $\mathcal{S}$ describes a q^{k-1}-divisible code of effective length $\#\mathcal{P}$. Assume that $\mathcal{S}$ is a partial $(k-1)$-spread of size $\frac{q^v-q^{k+r}}{q^k-1}+2$. Then $\#\mathcal{P} = \frac{q^{k+r}-1}{q-1} - 2\cdot\frac{q^k-1}{q-1}$. The $S(k-1)$-adic expansion of that number is $\#\mathcal{P} = \sum_{i=0}^{k-1} a_i s_q(k-1,i)$ with $a_0 = a_1 = \ldots = a_{k-2} = q-1$ and leading coefficient $a_{k-1} = q\cdot(\frac{q^r-1}{q-1} - k + 1) - 1$. By Theorem 1, $a_{k-1} \geq 0$ or equivalently, $k \leq \frac{q^r-1}{q-1}$.

3. Projective divisible codes

A linear code C is called *projective* if in a (and then in any) generator matrix of C, any two columns of C are linearly independent and there are no zero columns.[1] The effective length of a projective code is always agrees with its length.

In the above setting of a set of holes of a partial spread, we know more than what was actually used. In fact, the set of holes $\mathcal{P}$ of a partial $(k-1)$-spread $\mathcal{S}$ describes a *projective* q^{k-1}-divisible linear code. The following example shows that this additional restriction may further improve upper bounds on $A_q(v,k)$. Consider a partial 3-spread $\mathcal{S}$ in $\mathrm{PG}(\mathbb{F}_2^{11})$. Its set of holes is of size $2047-15\#\mathcal{S}$. Application of Theorem 1 shows that there exists no binary 8-divisible code of effective length $2047 - 136\cdot 15 = 7$, but there exists one of effective length $2047 - 135\cdot 15 = 22$. Therefore, we get the upper bound $A_2(11,4) \leq 135$. However, there is no *projective* binary 8-divisible code of length $2047 - 133\cdot 15 = 52$ (see Theorem 3 below), improving the upper bound by 3 to 132. The determination of the exact value of $A_2(11,4)$ remains an open problem. So far, the best known construction is the one by Beutelspacher, and the best known upper bound is the one we just derived, so there remains the gap $129 \leq A_2(11,4) \leq 132$.

Motivated by the above example, we study the lengths of projective divisible codes. The question appears to be much harder. No direct characterization as in Theorem 1 is known. There are open cases already for 16-divisible binary, 9-divisible ternary and 5-divisible $\mathbb{F}_5$-linear codes. On the positive side, the lengths of projective even, doubly-even and triply-even binary linear codes are known:

Theorem 3. *(a) The lengths of projective 2-divisible (even) binary codes are*

$$3, 4, 5, 6, \ldots$$

[1] The latter condition is only necessary for linear codes of length 1.

(b) The lengths of projective 4*-divisible (doubly even) binary codes are*

$$7, 8,\ 14, 15, 16, 17, \ldots$$

(c) The lengths of projective 8*-divisible (triply even) binary codes are*

$$15, 16,\ 30, 31, 32,\ 45, 46, 47, 48, 49, 50, 51,\ 60, 61, 62, 63, \ldots$$

Theorem 3 has been shown in [2, Th. 13], with the exception of the hardest single case of projective 8-divisible codes of length 59, whose non-existence has been established only recently in [3].

4. The Johnson bound for subspace codes

Many of the classical coding bounds have been adapted to subspace codes. However, practically everything is covered by the "Johnson type bound II" in [8]. Similar to partial spreads (which are a special case of subspaces codes), subspace codes can be connected to certain divisible codes. Combined with Theorem 1, this yields an improvement of the Johnson bound, see [4, Th. 5].

5. Open problems

We conclude with a list of open problems and ideas for future research.

- Theorem 1 only covers $\mathbb{F}_q$-linear Δ-divisible codes with $\Delta = q^r$, $r \in \mathbb{N}_0$. The more general case that Δ is only a power of the characteristic of $\mathbb{F}_q$ remains open.
- Extend Theorem 3 to more cases, like 16-divisible binary, 9-divisible ternary or 5-divisible $\mathbb{F}_5$-linear codes.
- Investigate the lengths of divisible codes with restrictions on the minimum weight, on the dimension and/or on the point multiplicity.
- Classify divisible codes of parameters which are in some sense extremal.
- Investigate indecomposable divisible codes.
- Investigate the q-analog setting of divisible rank metric codes.

References

[1] Albrecht Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Math. Z. **145** (1975), no. 3, 211–229.
[2] Thomas Honold, Michael Kiermaier and Sascha Kurz, Partial spreads and vector space partitions, in *Network Coding and Subspace Designs*, 131–170, Signals Commun. Technol., Springer, Cham, 2018.
[3] Thomas Honold, Michael Kiermaier, Sascha Kurz and Alfred Wassermann, *The lengths of projective triply-even binary codes*, preprint, 2018, `https://arxiv.org/abs/1812.05957`
[4] Michael Kiermaier and Sascha Kurz, *On the lengths of divisible codes*, preprint, 2019, `http://nbn-resolving.org/urn:nbn:de:bvb:703-epub-4304-1`
[5] Esmeralda L. Năstase and Papa A. Sissokho, *The maximum size of a partial spread in a finite projective space*, J. Combin. Theory Ser. A **152** (2017), 353–362.
[6] Harold N. Ward, *Divisible codes*, Arch. Math. **36** (1981), no. 6, 485–494.
[7] Harold N. Ward, *A bound for divisible codes*, IEEE Trans. Inf. Theory **38** (1992), no. 1, 191–194.
[8] Shu-Tao Xia and Fang-Wei Fu, *Johnson type bounds on constant dimension codes*, Des. Codes Cryptogr. **50** (2009), no. 2, 163–172.

Algebraic Quantum Coding Theory

Markus Grassl

We presented a short introduction to the basic concepts of quantum error-correcting codes, linking quantum mechanics and algebraic coding theory.

Quantum error-correcting codes (QECC) are subspaces of a complex Hilbert space $\mathcal{H}$ which are protected against certain types of "quantum errors" (decoherence). In many cases, the ambient space $\mathcal{H}$ is a tensor product of finite-dimensional spaces $\mathbb{C}^q$, i.e., $\mathcal{H} = \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q = (\mathbb{C}^q)^{\otimes n}$. A quantum code $\mathcal{C}$ of dimension $K = q^k$ and minimum distance d is denoted by $\mathcal{C} = [\![n, k, d]\!]_q$. Similar to the classical case, the distance d describes how many "local" errors can be corrected.

While there is a general theory of quantum error-correcting codes [4], one faces the problem to give an efficient description of the subspace $\mathcal{C}$ in the ambient space $\mathbb{C}^{q^n}$, whose dimension grows exponentially in n. The main solution to this problem is given by so-called stabilizer codes [1, 2, 3].

This allows to construct QECC based on classical linear codes of length n over the fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ which are self-orthogonal with respect to the Euclidian or Hermitian inner product, respectively. The standard metric is the Hamming metric. The properties of the resulting QECC can be derived from the properties of the related codes over finite fields, exploiting methods from algebraic coding theory. Furthermore, quantum mechanics allows to extract information about the error via measurements. The result of the measurement can be interpreted as the error syndrome of the classical code, allowing to essentially use classical decoding algorithms.

References

[1] A. R. Calderbank, E. Rains, P. W. Shor, N. J. A. Sloane, *Quantum error correction via codes over GF(4)*, IEEE Transactions on Information Theory **44** (1998), 1369–1387.

[2] D. Gottesman, *A class of quantum error-correcting codes saturating the quantum Hamming bound*, Physical Review A **54** (1996), 1862–1868.

[3] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Transactions on Information Theory **52** (2006), 4892–4914.

[4] E. Knill, R. Laflamme, *Theory of quantum error-correcting codes*, Physical Review A **55** (1997), 900–911.

Invariants of rank-metric codes and q-polymatroids

Elisa Gorla

(joint work with Relinde Jurrius, Hiram López Valdez, Alberto Ravagnani)

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. Let m, n be positive integers and denote by $\mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ the $\mathbb{F}_q$-vector space of matrices of size $n \times m$ with entries in $\mathbb{F}_q$. Up to a transposition, we assume without loss of generality that $n \leq m$. For a vector subspace $V \subseteq \mathbb{F}_q^n$, we denote by $V^\perp$ the dual of V with respect to the usual scalar product.

Definition 1. The function

$$\begin{array}{rcl} d : \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \times \mathrm{Mat}_{n\times m}(\mathbb{F}_q) & \longrightarrow & \mathbb{N} \\ (A, B) & \longmapsto & \mathrm{rk}(A-B) \end{array}$$

is a **distance** on $\mathrm{Mat}_{n\times m}(\mathbb{F}_q)$. The rank is the corresponding **weight function**. A **rank-metric code** is a vector subspace $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$. The **minimum distance** of a rank-metric code $\mathcal{C} \neq 0$ is the integer

$$d_{\min}(\mathcal{C}) = \min\{\mathrm{rk}(M) \mid M \in \mathcal{C},\ M \neq 0\}.$$

Two rank-metric codes $\mathcal{C}, \mathcal{D} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ are **equivalent** if there is an $\mathbb{F}_q$-linear isometry $\varphi : \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \to \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ such that $\varphi(\mathcal{C}) = \mathcal{D}$.

For brevity, in this extended abstract no proofs are given and references are kept to a minimum. We refer the interested reader to [1] for a comprehensive mathematical introduction to rank-metric codes and a list of references and to [2] for the proofs of the results presented in this note.

We recall the Singleton Bound for rank-metric codes:

$$\dim(\mathcal{C}) \leq m(n - d_{\min}(\mathcal{C}) + 1).$$

Codes that meet the bound are called **Maximum Rank Distance (MRD)**.

The weight distribution and the higher weights are invariants of a rank-metric code, which depend on the weights of the elements of the code and on the dimensions of subspaces satisfying certain rank conditions. They are connected to the decoding properties of the code. The **maximum rank** of a code $\mathcal{C}$ is

$$\max \mathrm{rk}(\mathcal{C}) = \max\{\mathrm{rk}(M) \mid M \in \mathcal{C}\}.$$

It is well known that every rank-metric code satisfies the Anticode Bound:

$$\dim(\mathcal{C}) \leq m \cdot \max \mathrm{rk}(\mathcal{C}).$$

Codes that meet the bound are called **optimal anticodes**.

Definition 2. The **generalized weights** of $\mathcal{C}$ are

$$d_i(\mathcal{C}) = \frac{1}{m} \min\{\dim(\mathcal{A}) \mid \mathcal{A} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \text{ optimal anticode, } \dim(\mathcal{C} \cap \mathcal{A}) \geq i\},$$

for $i = 1, \ldots, \dim(\mathcal{C})$.

It is easy to prove that $d_1(\mathcal{C}) = d_{\min}(\mathcal{C})$.

Definition 3. A **q-polymatroid** is a pair $P = (\mathbb{F}_q^n, \rho)$ where ρ is a function from the set of all subspaces of $\mathbb{F}_q^n$ to $\mathbb{R}$ such that, for all $U, V \subseteq \mathbb{F}_q^n$:

(P1) $0 \leq \rho(V) \leq \dim(V)$,
(P2) if $U \subseteq V$, then $\rho(U) \leq \rho(V)$,
(P3) $\rho(U + V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

A **q-matroid** is a q-polymatroid $(\mathbb{F}_q^n, \rho)$ such that ρ is integer-valued.

Definition 3 is a direct q-analogue of the definition of an ordinary polymatroid, with the extra property that $\rho(V) \leq \dim(V)$ for all $V \subseteq \mathbb{F}_q^n$. It is essentially equivalent to the definition of (q, m)-polymatroid given by Shiromoto in [4].

Examples 4. • The simplest example of q-(poly)matroid is $(\mathbb{F}_q^n, \dim(\cdot))$, where $\dim(\cdot)$ denotes the function that associates to a vector space its dimension.
• Let $U \subseteq \mathbb{F}_q^n$. The pair $(\mathbb{F}_q^n, \psi_U)$ with $\psi_U(V) = \dim(V \cap U)$ is not a q-(poly)matroid, since ψ_U does not satisfy property (P3).
• Let $U \subseteq \mathbb{F}_q^n$. The pair $(\mathbb{F}_q^n, \rho_U)$ with $\rho_U(V) = \dim(U) - \dim(U \cap V^\perp)$ is a q-(poly)matroid.

One has the following natural notion of equivalence for q-polymatroids.

Definition 5. Two q-polymatroids $(\mathbb{F}_q^n, \rho_1)$ and $(\mathbb{F}_q^n, \rho_2)$ are **equivalent** if there exists an $\mathbb{F}_q$-linear isomorphism $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\rho_1(V) = \rho_2(\varphi(V))$ for all $V \subseteq \mathbb{F}_q^n$.

One can associate q-polymatroids to rank-metric codes as follows.

Definition 6. Given $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ a rank-metric code, we define the q-polymatroid $P(\mathcal{C}) = \big(\mathbb{F}_q^n, \rho_{\mathcal{C}}\big)$, where

$$\rho_{\mathcal{C}}(V) = \frac{1}{m}(\dim(\mathcal{C}) - \dim(\mathcal{C}(V^\perp)) \in \mathbb{Q}.$$

For $n < m$, we associate to $\mathcal{C}$ the q-polymatroid $P(\mathcal{C})$.
For $n = m$, we associate to $\mathcal{C}$ the q-polymatroids $P(\mathcal{C})$ and $P(\mathcal{C}^\mathsf{T})$.

Here $\mathcal{C}^\mathsf{T}$ denotes the transposed of the code $\mathcal{C} \subseteq \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$, namely

$$\mathcal{C}^\mathsf{T} = \{M^\mathsf{T} \mid M \in \mathcal{C}\} \subseteq \mathrm{Mat}_{n\times n}(\mathbb{F}_q).$$

It is easy to show that equivalent rank-metric codes produce equivalent q-polymatroids. A possible exception is the case $m = n$, where if $\mathcal{C}$ and $\mathcal{D}$ are equivalent rank-metric codes, then either $P(\mathcal{C})$ is equivalent to $P(\mathcal{D})$ and $P(\mathcal{C}^\mathsf{T})$ is equivalent to $P(\mathcal{D}^\mathsf{T})$, or $P(\mathcal{C})$ is equivalent to $P(\mathcal{D}^\mathsf{T})$ and $P(\mathcal{C}^\mathsf{T})$ is equivalent to $P(\mathcal{D})$.

Example 7 (q-polymatroids of MRD codes)**.** Let $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ be a rank-metric code with minimum distance $d_{\min}(\mathcal{C}) = d$. Then $\mathcal{C}$ is MRD if and only if $P(\mathcal{C}) = \big(\mathbb{F}_q^n, \rho_{\mathcal{C}}\big)$ where

$$\rho_{\mathcal{C}}(V) = \begin{cases} n-d+1 & \text{if } \dim(V) > n-d+1, \\ \dim(V) & \text{if } \dim(V) \le n-d+1. \end{cases}$$

Notice that MRD codes of the same dimension have the same associated q-polymatroid, but they are not necessarily equivalent, see [2, Example 5.8].

Example 8 (q-polymatroids of optimal anticodes)**.** Let $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ be a rank-metric code with $r = \max \mathrm{rk}(\mathcal{C})$. Let

$$\rho(V) = \dim(V + \langle e_1, \ldots, e_{n-r}\rangle) - (n-r),$$

where e_i denotes the i-th vector of the standard basis of $\mathbb{F}_q^n$. Then $\mathcal{C}$ is an optimal anticode if and only if either $P(\mathcal{C})$ is equivalent to $(\mathbb{F}_q^n, \rho)$, or $m = n$ and $P(\mathcal{C}^\mathsf{T})$ is equivalent to $(\mathbb{F}_q^n, \rho)$.

Notice that the q-polymatroids of Examples 7 and 8 are q-matroids. Vector rank-metric codes are another example of rank-metric codes whose associated q-polymatroids are q-matroids, see [3]. There are however examples of rank-metric codes, whose associated q-polymatroid is not a q-matroid, see [2, Example 5.10].

The interest in associating q-polymatroids to rank-metric codes comes from the fact that several invariants of rank-metric codes can be computed from the associated q-polymatroids. E.g., it is easy to show that the dimension and minimum distance of a rank-metric code can be computed from the associated q-polymatroid(s). Moreover, in [4] Shiromoto shows that same result holds for the weight distribution. In [2], we prove the same result for the generalized weights.

Theorem 9. *Let $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ be a rank-metric code, $1 \leq i \leq \dim(\mathcal{C})$. Let*

$$d_i(P(\mathcal{C})) = n - \max\left\{\dim(V) \mid V \subseteq \mathbb{F}_q^n,\ \rho_{\mathcal{C}}(V) \leq \frac{\dim(\mathcal{C}) - i}{m}\right\}.$$

If $n < m$, then $d_i(\mathcal{C}) = d_i(P(\mathcal{C}))$.
If $n = m$, then $d_i(\mathcal{C}) = \min\{d_i(P(\mathcal{C})),\ d_i(P(\mathcal{C}^T))\}$.

Finally, there is a natural notion of dual q-polymatroid.

Definition 10. Let $P = (\mathbb{F}_q^n, \rho)$ be a q-polymatroid. For $V \subseteq \mathbb{F}_q^n$ define

$$\rho^*(V) = \dim(V) - \rho(\mathbb{F}_q^n) + \rho(V^\perp).$$

The q-polymatroid $P^* = (\mathbb{F}_q^n, \rho^*)$ is the **dual** of P.

Using standard arguments, one can show that P^* is a q-polymatroid, that the duals of equivalent q-polymatroids are equivalent, and that $P^{**} = P$. Moreover, duality for q-polymatroids is compatible with duality for rank-metric codes.

Theorem 11. *Let $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ be a rank-metric code. Then $P(\mathcal{C})^* = P(\mathcal{C}^\perp)$.*

References

[1] E. Gorla, *Rank-metric codes*, A Concise Encyclopedia of Coding Theory, W.C. Huffman, J.-L. Kim, and P. Solé Eds., CRC Press (to appear).

[2] E. Gorla, R. Jurrius, H. López Valdez, A. Ravagnani, *Rank-metric codes and q-polymatroids*, available at `https://arxiv.org/abs/1803.10844` (submitted).

[3] R. Jurrius, R. Pellikaan, *Defining the q-analogue of a matroid*, Electron. J. Combin. **3** (2018).

[4] K. Shiromoto, *Codes with the rank metric and matroids*, to appear in Des. Codes Cryptogr.

Sub-packetization of Minimum Storage Regenerating Codes: A lower bound and a work-around

Venkatesan Guruswami

Modern cloud storage systems need to store vast amounts of data in a fault tolerant manner, while also preserving data reliability and accessibility in the wake of frequent server failures. Traditional MDS (Maximum Distance Separable) codes provide the optimal trade-off between redundancy and number of worst-case erasures tolerated. However, the applicability of the MDS codes in modern storage systems also depends on their ability to efficiently reconstruct parts of a codeword from the rest of the codeword.

Minimum storage regenerating (MSR) codes are a special sub-class of MDS codes that provide mechanisms for exact regeneration of a single code-block by downloading the minimum amount of information from the remaining code-blocks. As a result, MSR codes are attractive for use in distributed storage systems to ensure node repairs with optimal repair-bandwidth. However, all known constructions of MSR codes require large sub-packetization levels (which is a measure of the granularity to which a single vector codeword symbol needs to be divided into for efficient repair). This restricts the applicability of MSR codes in practice.

In this talk, we presented a near-optimal lower bound that exponentially large sub-packetization is inherent for MSR codes. This lower bound is from [1]. As a way to circumvent this lower bound, we also propose a natural relaxation of MSR codes that allows one to circumvent this lower bound, and present a general approach to construct MDS codes that significantly reduces the required sub-packetization level by incurring slightly higher repair-bandwidth as compared to MSR codes [3].

Let us state the above results a bit more formally. An (n, k, ℓ)-vector MDS code C over the field $\mathbb{F}$ is a subspace (over $\mathbb{F}$) of dimension $k\ell$ of $(\mathbb{F}^\ell)^n$. Its codewords can be viewed as $c = (c_1, c_2, \ldots, c_n)$ where each c_i is a vector of length ℓ over $\mathbb{F}$. The MDS property implies that any codeword $c \in C$ can be uniquely recovered from the components c_i, $i \in T$, for any subset T of k indices. This gives the optimal resilience from worst-case symbol erasures for the given storage overhead of $r := n - k$ redundant/check symbols. In the context of their use in distributed storage, we are interested in bandwidth-efficient repair of an arbitrary symbol c_f (for an index f corresponding to a failed node) by downloading the minimal possible information about c_i, $i \neq f$. A simple argument shows that this minimal amount equals ℓ/r. An MSR code is one that allows for the repair of any failed symbol by downloading exactly ℓ/r symbols about every other codeword symbol. Formally, for every $f \in [n]$, there are $\mathbb{F}$-linear repair functions $R_i^f : \mathbb{F}^\ell \to \mathbb{F}^{\ell/r}$, $i \neq f$, such that c_f can be recovered as an $\mathbb{F}$-linear combination of all the symbols $R_i^f(c_i)$, $i \neq f$. (Here we restrict attention to *linear* repair schemes.) The quantity ℓ is referred to as the sub-packetization of the MSR code.

A long line of work has led to some beautiful constructions of MSR codes, for example in [7, 4]. However, these incur very large sub-packetization of $\ell \approx r^{n/r}$,

which is exponential in n for small values of the redundancy r (which is of most interest in storage applications). There were partial results showing this is inherent: a lower bound of $\ell \gtrsim \exp(\sqrt{k/r})$ was shown in [2], and an exponential bound of $\ell \gtrsim r^{k/r}$ was shown in [5] for the special case when the repair functions are *projections* (i.e., they just return some components of the codeword symbol).

Our main result in [1] that we discussed in the talk is an almost optimal lower bound on sub-packetization of MSR codes. The proof is short and elegant, based on tracking the dimension of the space of some maps that fix a collection of subspaces associated with the MSR code, and was presented in almost full detail in the talk.

Theorem 1. *Suppose an (n, k, ℓ)-vector MDS code with redundancy $r = n - k$ is MSR. Then its sub-packetization ℓ must satisfy $\ell \geq e^{(k-1)/(4r)}$.*

Given the necessity of large sub-packetization for MSR codes, the talk turned to the notion of ϵ-MSR codes put forth in [3]. An ϵ-MSR code relaxes the requirement of optimal repair bandwidth, and allows the download of up to $(1+\epsilon)\ell/r$ symbols from each of the helper nodes $i \neq f$ when recovering the symbol c_f. In other words, the repair functions R_i^f have range $\mathbb{F}^{(1+\epsilon)\ell/r}$. If ϵ is small, this is only a small factor more compared to the optimal ℓ/r bound. Yet, the following theorem from [3] shows that this small elbow room in the repair bandwidth can lead to huge savings in the sub-packetization, by a doubly exponential amount in fact!

Theorem 2. *There is an explicit construction of an (n, k, ℓ)-vector MDS code that is ϵ-MSR over a field $\mathbb{F}$ of size $O(nr)$ and has sub-packetization $\ell \leq O(r^{O(r/\epsilon)} \log n)$.*

The talk discussed the high level strategy for constructing the above codes, which is via a combination of a *short* MSR code of length m and large sub-packetization (say r^m, as in the construction of [6]) with a *long* linear code of large relative distance (of about $1 - \epsilon$) over an alphabet of size $q \leq m$.

References

[1] O. Alrabiah and V. Guruswami. *An exponential lower bound on the sub-packetization of MSR codes*, In Proceedings of the 51st Annual ACM Syposium on Theory of Computing, 2019, to appear.

[2] S. Goparaju, I. Tamo, and R. Calderbank. An improved sub-packetization bound for minimum storage regenerating codes. *IEEE Trans. Information Theory*, 60(5):2770–2779, 2014.

[3] A. S. Rawat, I. Tamo, V. Guruswami, and K. Efremenko. *MDS code constructions with small sub-packetization and near-optimal repair bandwidth*, *IEEE Trans. Information Theory*, 64(10):6506–6525, 2018.

[4] B. Sasidharan, M. Vajha, and P. V. Kumar. An explicit, coupled-layer construction of a high-rate MSR code with low sub-packetization level, small field size and all-node repair. *CoRR*, abs/1607.07335, 2016.

[5] I. Tamo, Z. Wang, and J. Bruck. Access versus bandwidth in codes for storage. *IEEE Trans. Information Theory*, 60(4):2028–2037, 2014.

[6] M. Ye and A. Barg. Explicit constructions of high-rate MDS array codes with optimal repair bandwidth. *IEEE Trans. Information Theory*, 63(4):2001–2014, 2017.

[7] M. Ye and A. Barg. Explicit constructions of optimal-access MDS codes with nearly optimal sub-packetization. *IEEE Trans. Information Theory*, 63(10):6307–6317, 2017.

The covering radius conjecture for Reed-Muller codes

Kai-Uwe Schmidt

The Hamming distance of two Boolean functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ is

$$d(f,g) = \#\{y \in \mathbb{F}_2^n : f(y) \neq g(y)\}.$$

Put

$$\rho_n = \max_f \min_g d(f,g),$$

where the maximum is over all functions f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and the minimum is over all 2^{n+1} affine functions g from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then ρ_n equals the covering radius of the $[2^n, n+1]$ Reed-Muller code, whose determination is one of the oldest and most difficult open problems in coding theory [7]. The determination of ρ_n also answers the question of how well Boolean functions can be approximated by linear functions, which is of significance in cryptography. One can also interpret ρ_n in terms of the Fourier coefficients of Boolean functions. It is convenient to define

$$\mu_n = 2^{n/2} - \rho_n / 2^{n/2-1}.$$

An averaging argument shows that $\mu_n \geq 1$ and a simple recursive construction shows that $\mu_{n+2} \leq \mu_n$. The fact that $\mu_2 = 1$ implies that $\mu_n = 1$ for all even n; the functions attaining the minimum are known as *bent* functions and these have been studied extensively for more than forty years [5].

We are interested in the case that n is odd. Since $\mu_1 = \sqrt{2}$, we have $1 \leq \mu_n \leq \sqrt{2}$. It is known that equality holds in the upper bound for each $n \in \{3, 5, 7\}$. It was suggested in [2] that $\mu_n = \sqrt{2}$ for all odd n, which was disproved by Patterson and Wiedemann [4], by showing that

$$\mu_n \leq \sqrt{729/512} = 1.19\ldots \quad \text{for each } n \geq 15. \tag{1}$$

More recently it was shown by Kavut and Yücel [3] that

$$\mu_n \leq \sqrt{49/32} = 1.23\ldots \quad \text{for each } n \geq 9.$$

Patterson and Wiedemann [4] also conjectured that

$$\lim_{n\to\infty} \mu_n = 1.$$

However no improvement of (1) for large n has been found since this conjecture has been posed in 1983. In [6], I have proved that this conjecture is true and during the talk I explain the ideas behind the proof. The key idea is a semiprobabilistic construction; it mimics the well known partial spread construction for bent functions [1] and is further coupled with some randomness. This allows one to prove that there is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for odd n that looks asymptotically like a bent function.

References

[1] J. F. Dillon. Elementary Hadamard difference sets. Ph.D. Thesis, University of Maryland, College Park. 1974.

[2] T. Helleseth, T. Kløve, and J. Mykkeltveit. On the covering radius of binary codes. *IEEE Trans. Inform. Theory*, 24(5):627–628, 1978.

[3] S. Kavut and M. D. Yücel. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Inform. and Comput.*, 208(4):341–350, 2010.

[4] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16 276. *IEEE Trans. Inform. Theory*, 29(3):354–356, 1983. Corrected in: IEEE Trans. Inform. Theory, 36(2):443, 1990.

[5] O. S. Rothaus. On "bent" functions. *J. Combin. Theory Ser. A*, 20(3):300–305, 1976.

[6] K.-U. Schmidt. Asymptotically optimal Boolean functions. *J. Combin. Theory Ser. A*, 164:50–59, 2019.

[7] N. J. A. Sloane. Unsolved problems related to the covering radius of codes. In T. Cover and B. Gopinath, editors, *Open Problems in Communication and Computation*, pages 51–56. Springer New York, 1987.

Identifying rank-metric codes using Galois group action

Alessandro Neri

(joint work with Sven Puchinger, Anna-Lena Horlemann-Trautmann)

Rank-metric codes have recently become a topic of high interest due to their many applications. They were introduced independently by Delsarte [1], Gabidulin [2] and Roth [7], but only in the last decade they attracted many researchers from different areas of mathematics, computer science and engineering. The framework is explained as follows. One considers a prime power $q = p^r$, a finite field $\mathbb{F}_q$ and an extension field $\mathbb{F}_{q^m}$ of degree m. On the set $\mathbb{F}_{q^m}^n$, the *q-rank* of a vector v is defined as $\mathrm{rk}_q(v) := \dim_{\mathbb{F}_q} \langle v_1, \dots, v_n \rangle_{\mathbb{F}_q}$. The q-rank induces the *rank distance* on the space $\mathbb{F}_{q^m}^n$: the rank distance of two vectors is equal to the q-rank of their difference. In this setting, an $[n,k]_{q^m}$ *rank-metric code* $\mathcal{C}$ is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank distance. The minimum distance d of $\mathcal{C}$ is the minimum q-rank of a non-zero vector in $\mathcal{C}$. The parameters k, n and d are related by a simple and effective relation, namely the Singleton-like bound, which states that $d \leq n - k + 1$. Codes that meet this bound with equality are called *maximum rank distance* codes, or *MRD codes* in short.

The first construction of MRD codes was given by Delsarte, Gabidulin and Roth and is described as follows. Let $1 \leq k \leq n \leq m$ be integers, and θ be a generator of $G := \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Consider the $\mathbb{F}_{q^m}$-subspace $\mathcal{G}_{k,\theta} := \langle \mathrm{id}, \theta, \dots, \theta^{k-1} \rangle_{\mathbb{F}_{q^m}}$ of the group algebra $\mathbb{F}_{q^m}[G]$, and choose a vector $g \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}_q(g) = n$. The $[n,k]_{q^m}$ code $\mathcal{G}_{k,\theta}(g) := \{(f(g_1), \dots, f(g_n)) \mid f \in \mathcal{G}_{k,\theta}\}$ is called *θ-Gabidulin code*. It was proved in [1] that this construction always provides MRD codes.

Very recently, it was shown in [5] that, for a sufficiently large extension field degree m there are plenty of MRD codes that are not θ-Gabidulin codes. Motivated by this result, it has been a research problem of high interest to construct new families of MRD codes. The most prominent new one was given by Sheekey in [9]. However, when looking for new constructions of rank-metric codes, it is important

to check if the new codes are really new, or are equivalent to any of the already known codes.

Given some integers $0 < s_1 < \ldots < s_r < m$ and two equivalent $[n,k]_{\mathbb{F}_{q^m}}$ rank-metric codes $\mathcal{C}$ and $\mathcal{C}'$, it is easy to check that also the codes $\mathcal{C}+\theta^{s_1}(\mathcal{C})+\ldots+\theta^{s_r}(\mathcal{C})$ and $\mathcal{C}'+\theta^{s_1}(\mathcal{C}')+\ldots+\theta^{s_r}(\mathcal{C}')$ are equivalent, where the addition is the vector space sum. Motivated by this simple observation, we introduce the following setting and definitions. Let $\mathcal{P}_{q^m}(n)$ denote the set of all $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$. For any automorphism $\theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and integer $0 \le i \le n$, we consider the map

$$\begin{array}{rccc} \mathcal{S}_i^\theta : & \mathcal{P}_{q^m}(n) & \longrightarrow & \mathcal{P}_{q^m}(n) \\ & \mathcal{C} & \longmapsto & \sum_{j=0}^{i} \theta^j(\mathcal{C}) \end{array}$$

and the integers

$$s_i^\theta(\mathcal{C}) := \dim(\mathcal{S}_i^\theta(\mathcal{C})) \quad \text{and} \quad \Delta_i^\theta(\mathcal{C}) := s_{i+1}^\theta(\mathcal{C}) - s_i^\theta(\mathcal{C}).$$

With this notation, $s_i^\theta(\mathcal{C})$ is called the *i-th θ-dimension of $\mathcal{C}$*, and $\Delta_i^\theta(\mathcal{C})$ the *i-th θ-increment of $\mathcal{C}$*. These sequences of integers are invariants of rank-metric codes under code equivalence, and provide an easy checkable criterion to determine inequivalence of codes. In addition, these sequences and the maps $\mathcal{S}_i^\theta$ have some interesting properties. For a given $[n,k]_{q^m}$ rank-metric code $\mathcal{C}$, we have

$$k = s_0^\theta(\mathcal{C}) \le \ldots \le s_{n-k}^\theta(\mathcal{C}) \le n, \qquad k \ge \Delta_0^\theta(\mathcal{C}) \ge \ldots \ge \Delta_{n-k}^\theta(\mathcal{C}) = 0.$$

These very simple sequences not only provide a tool for checking code inequivalence, but they also have some important applications. Indeed, they yield an elementary way to prove the following result, which is an improvement of a result in [8] for some sets of parameters. In the next theorem, $\phi(m)$ denotes the Euler's totient function, while $\Phi(a,b) = |\{1 \le s \le b \mid \gcd(s,a) = 1\}|$.

Theorem 1. *Let k, n, m be positive integers with $2 \le k \le n-2$, and let $N_q(k,m,n)$ be the number of inequivalent Gabidulin codes of dimension k in $\mathbb{F}_{q^m}^n$.*

(a) *If $m = n$ then*

$$N_q(k,m,m) = \frac{\phi(m)}{2}.$$

(b) *If $m > n$, then*

$$\frac{\Phi(m,n)}{2m[\mathbb{F}_q : \mathbb{F}_p]} \prod_{i=2}^{n} \frac{q^{m-i+1}-1}{q^i-1} \le N_q(k,m,n) \le \frac{\phi(m)}{2} \prod_{i=2}^{n} \frac{q^{m-i+1}-1}{q^i-1}.$$

The second application concerns a characterization result for the special family of Gabidulin codes.

Theorem 2 (Characterization of θ-Gabidulin codes)**.** *Let $\mathcal{C}$ be an $[n,k]_{q^m}$ rank-metric code with minimum distance $d > 1$ and let θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. The following are equivalent:*

1. *$\mathcal{C}$ is a θ-Gabidulin code.*
2. *$\mathcal{C}$ is MRD and $s_1^\theta(\mathcal{C}) = k+1$ ([3]).*

3. $(s_i^\theta(\mathcal{C}))_i = (k, k+1, \ldots, n)$.
4. $(\Delta_i^\theta(\mathcal{C}))_i = (1, 1, \ldots, 1)$.
5. $\mathcal{C} = \mathrm{rowsp}(I_k \mid X)$, *where:*
   (a) $\mathrm{rk}(\theta(X) - X) = 1$,
   (b) *the q-rank of the first row of* $\theta(X) - X$ *is* $n - k$,
   (c) *the q-rank of the first column of* $\theta(X) - X$ *is* k ([4]).

The investigation on the θ-dimensions and θ-increments is ongoing. They have nice properties and they seem to represent a natural invariant that needs to be studied, which provides new characterization results. Moreover, using this tool, one can prove results such as [8] in an elementary way. It is still an open problem to understand whether they can characterize other families of MRD codes, or they can even provide new constructions of codes.

References

[1] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, Journal of Combinatorial Theory, Series A **25**(3) (1978), 226–241.

[2] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21**(1) (1985), 3–16.

[3] A.-L. Horlemann-Trautmann and K. Marshall, *New criteria for MRD and Gabidulin codes and some rank-metric code constructions*, Advances in Mathematics of Communications **11**(3) (2017), 533–548.

[4] A. Neri, *Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices*, arXiv preprint (2018), arXiv:1805.06706.

[5] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal, *On the genericity of maximum rank distance and Gabidulin codes*, Designs, Codes and Cryptography **86**(2) (2018), 341–363.

[6] A. Neri, S. Puchinger, and A.-L. Horlemann-Trautmann, *Invariants and inequivalence of linear rank-metric codes*, in: IEEE International Symposium on Information Theory (2019), to appear.

[7] R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction*, IEEE Transactions on Information Theory **37**(2) (1991), 328–336.

[8] K.-U. Schmidt and Y. Zhou, *On the number of inequivalent Gabidulin codes*, Designs, Codes and Cryptography **86**(9) (2018), 1973–1982.

[9] J. Sheekey, *A new family of linear maximum rank distance codes*, Advances in Mathematics of Communications **10**(3) (2016), 475–488.

Constructing asynchronous batch codes using hypergraphs

Vitaly Skachek

(joint work with Ago-Erik Riet and Eldho K. Thomas)

Batch codes were first proposed in [3] as means for balancing load in distributed storage systems. They are also of potential use in private information retrieval (PIR). Batch codes can be viewed as a special case of so-called PIR codes [2]. Both batch and PIR codes were extensively studied in the last years. For a survey of the known results on these two families of codes, the reader can refer to [6].

Definition. [7] An (n, k, t) batch code $\mathcal{C}$ over a finite alphabet Σ is defined by an encoding mapping $\mathsf{C} : \Sigma^k \to \Sigma^n$, and a decoding mapping $\mathsf{D} : \Sigma^n \times [k]^t \to \Sigma^t$, such that

(1) For any $\boldsymbol{x} \in \Sigma^k$ and $i_1, i_2, \cdots, i_t \in [k]$,

$$\mathsf{D}\left(\boldsymbol{y} = \mathsf{C}(\boldsymbol{x}), i_1, i_2, \cdots, i_t\right) = (x_{i_1}, x_{i_2}, \cdots, x_{i_t}).$$

(2) The symbols in the query $(x_{i_1}, x_{i_2}, \cdots, x_{i_t})$ can be reconstructed from t respective pairwise disjoint recovery sets of symbols of $\boldsymbol{y}$ (the symbol x_{i_ℓ} is reconstructed from the ℓ-th recovery set for each ℓ, $1 \leq \ell \leq t$).

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements, where q is a prime power, and $\mathcal{C}$ be a linear $[n, k]$ code over $\mathbb{F}$. Denote the redundancy by $\rho = n - k$. For a *linear batch code*, the encoding of C is given as a multiplication by a $k \times n$ generator matrix $\boldsymbol{G}$ over $\mathbb{F}$ of an information vector $\boldsymbol{x} \in \mathbb{F}^k$,

$$\boldsymbol{y} = \boldsymbol{x} \cdot \boldsymbol{G}\ ; \quad \boldsymbol{y} \in \mathbb{F}^n\ .$$

A *linear batch code* with the parameters n, k and t over $\mathbb{F}_q$, where t is a number of queried symbols, is denoted as an $[n, k, t]_q$-*batch code*.

In this work, we present a new variant of batch codes termed "*asynchronous* batch codes", which are designed for parallel recovery of information symbols from the coded database, where different requests take different service time (i.e. the requests are served in an asynchronous manner).

Definition. An asynchronous $[n, k, t]_q$-batch code $\mathcal{C}$ is an $[n, k, t]_q$-batch code with the additional property that for any legal query $(x_{\ell_1}, x_{\ell_2}, \cdots, x_{\ell_t})$, for all $\ell_i \in [k]$, it is always possible to replace x_{ℓ_j} by some $x_{\ell_{t+1}}$, $\ell_{t+1} \in [k]$, such that $x_{\ell_{t+1}}$ is retrieved from the servers not used for retrieval of $x_{\ell_1}, x_{\ell_2}, \cdots, x_{\ell_{j-1}}, x_{\ell_{j+1}}, \cdots, x_{\ell_t}$, without reading more than one symbol from each server.

It turns out that the graph-based batch codes studied in [4] are asynchronous. By building on the ideas in [4], we show that hypergraphs of Berge girth at least four yield graph-based asynchronous batch codes. We prove the hypergraph-theoretic proposition that the maximum number of hyperedges in a hypergraph of a fixed Berge girth equals the quantity in a certain generalization of the hypergraph-theoretic (6,3)-problem. We then apply the constructions and bounds in [1] to obtain batch code constructions and bounds on the optimal redundancy of the graph-based asynchronous batch codes.

We show that the optimal redundancy $\rho(k)$ of graph-based asynchronous batch codes with the query size $t = 3$ is $2\sqrt{k}$. Moreover, for a general fixed value of $t \geq 4$, $\rho(k) = O\left(k^{1/(2-\epsilon)}\right)$ for any small $\epsilon > 0$. For a general value of $t \geq 4$, $\lim_{k\to\infty} \rho(k)/\sqrt{k} = \infty$.

This talk is based on a work [5], where the settings and proofs are presented in more detail.

References

[1] P. Erdös, P. Frankl, and V. Rödl, *The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent*, Graphs and Combinatorics, vol. 2, no. 1, pp. 113–121, 1986.

[2] A. Fazeli, A. Vardy, and E. Yaakobi, *PIR with low storage overhead: coding instead of replication*, arXiv:1505.06241, May 2015.

[3] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, *Batch codes and their applications*, *Proc. 36th ACM Symp. on Theory of Computing*, Chicago, IL, 2004.

[4] A. S. Rawat, Z. Song, A. G. Dimakis, and A. Gál, *Batch codes through dense graphs without short cycles*, *IEEE Trans. Information Theory*, vol. 62, no. 4, pp. 1592–1604, 2016.

[5] A.-E. Riet, V. Skachek, and E. K. Thomas, *Asynchronous batch and PIR codes from hypergraphs*, *Proc. IEEE Inform. Theory Workshop (ITW)*, Guangzhou, China, 2018.

[6] V. Skachek, *Batch and PIR codes and their connections to locally-repairable codes*, in: Network Coding and Subspace Designs (Eds. M. Greferath, M. O. Pavčević, N. Silberstein, M. Á. Vázquez-Castro), pp. 427–442, 2018.

[7] A. Vardy and E. Yaakobi, *Constructions of batch codes with near-optimal redundancy*, *Proc. IEEE Intern. Symp. on Inform. Theory (ISIT)*, Barcelona, July 2016.

Bounding the number of affine roots

Olav Geil

In this survey we consider the problem of bounding the number of affine roots of multivariate polynomials including briefly mentioning applications in communication theory and function field theory. For univariate polynomials it is well-known that a polynomial of degree s can have at most s roots over any given field, even when counted with multiplicity. This is in contrast to multivariate polynomials which often have infinitely many roots. However, under certain natural restrictions the number is finite and estimating it becomes of interest.

The simplest case to consider is that of counting roots over some finite Cartesian product point set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$, $i = 1, \ldots, m$. Here, $\mathbb{F}$ can be any field, one particular case of interest being when $S_i = \mathbb{F} = \mathbb{F}_q$, $i = 1, \ldots, m$, where the latter notation means the finite field with q elements. The natural extension of the previous mentioned result to the case of multivariate polynomials then is that a polynomial with leading monomial $X_1^{i_1} \cdots X_m^{i_m}$, $i_j < s_j = \#S_j$, $j = 1, \ldots, m$, can have at most

$$s_1 \cdots s_m - \prod_{j=1}^{m} (s_j - i_j) \tag{1}$$

affine roots. This result holds for arbitrary monomial ordering.

Example: *Consider the polynomial* $F(X, Y) = X^2Y + Y^2 + 2$ *over* $\mathbb{F}_5$. *To give an upper bound on the number of affine roots over* $\mathbb{F}_5$ *we consider two different monomial orderings. Namely, as indicated in Figure 1, one for which* $lm(F) = X^2Y$ *and another for which* $lm(F) = Y^2$. *From the first choice we see that there can at most be* 13 *roots. The second choice, however, reveals that actually there cannot be more than* 10 *roots.*

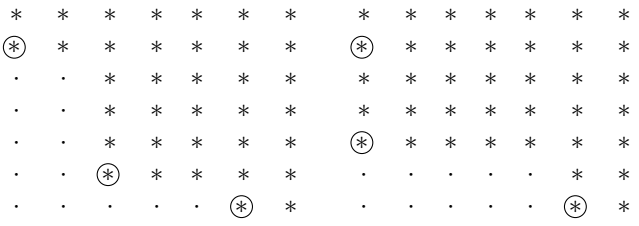

FIGURE 1. Two choices: $\mathrm{lm}(F) = X^2Y$ or $\mathrm{lm}(F) = Y^2$. Number of roots at most $\min\{13, 10\} = 10$

The powerful – yet not very well-known – result (1) has as an easy corollary the famous Schwartz-Zippel bound which states that a polynomial in m variables and of total degree $s < q$ has at least $(q - s)q^{m-1}$ non-roots over $\mathbb{F}_q$.

Considering common roots of more polynomials one may without loss of generality assume that the leading monomials are pairwise different. Plugging these monomials into a figure like Figure 1 one obtains in a very natural way a generalization of (1) by counting again the monomials not marked with $*$.

So far we did not treat roots with multiplicity. For multivariate polynomials there are many different ways of defining the concept typically using Hasse derivatives. The classical definition used in papers like [2, 8] is sometimes called the standard multiplicity. It is possible to formulate a generalization of (1) to estimate the number of roots with at least some prescribed multiplicity for a range of different types of multiplicity [6], but for the standard multiplicity one obtains better information from Dvir et al.'s generalization of the Schwartz-Zippel bound [2]. Employing the lemmas in [2] one further obtains a method to obtain refined information from the leading monomial with respect to a lexicographic ordering.

Example: *In this example we estimate the maximal number of roots of multiplicity at least* 3 *over* $\mathbb{F}_5$ *when given information on the leading monomial with respect to a lexicographic ordering, see Figure 2. The results are derived by employing the lemmas in* [2]*. Observe that the figure is not symmetric.*

In the following we return to not considering multiplicity. The theorem behind (1) is the result below which can be found in many textbooks on commutative algebra, e.g. [1].

Theorem:
Consider an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$. For any monomial ordering the set of monomials that are not leading monomial of any polynomial in I constitutes a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$.

From this one obtains an upper bound on the number of roots of any zero-dimensional ideal. This result is known as the footprint bound [5, 9]. Actually, when restricting to the case of perfect fields (e.g. finite fields) and assuming that I contains a univariate square-free polynomial in each variable one obtains a way to

20	21	22	23	24										
20	20	21	21	23										
20	20	20	21	22										
15	16	17	19	21										
15	15	16	17	20										
15	15	15	17	18	22	23	23	24	24					
10	11	12	15	17	21	22	22	23	23					
10	10	11	13	15	18	20	20	22	22					
10	10	10	13	14	17	19	19	21	21					
5	6	7	11	12	14	17	17	20	20					
5	5	6	9	11	13	16	16	18	19	23	23	24	24	24
5	5	5	9	9	10	14	14	16	18	21	21	23	23	23
0	1	2	7	8	9	13	13	14	17	19	19	22	22	22
0	0	1	5	6	6	11	11	12	16	17	17	21	21	21
0	0	0	5	5	5	10	10	10	15	15	15	20	20	20

FIGURE 2

establish the actual number of roots by employing Buchberger's algorithm. This for instance can be used at a theoretical level to determine the second highest number of roots that a polynomial of total degree s can have over a finite field. See [4, 12].

Another application is to consider rather than Cartesian product point sets – as we did at the beginning of the survey – instead points on curves over $\mathbb{F}_q$. Employing results by Miura [10] and Pellikaan [11] we are able to reproduce the Goppa bound on one-point algebraic geometric codes and to often improve upon it. Furthermore, we can show [7] that the number of rational places of a function field over $\mathbb{F}_q$ having $\Lambda = \langle w_1, \ldots, w_m \rangle$ as a Weierstrass semigroup can at most be

$$\#\Big(\Lambda \setminus \bigcup_{i=1}^{m} \left(qw_i + \Lambda\right)\Big) + 1.$$

There are many other applications besides the ones we listed above. This for instance includes estimating the information leakage and recovery numbers in secret sharing and the ability to correct phase-shift errors and qudit-flip errors when using quantum codes from the CSS construction [3].

REFERENCES

[1] D. A. Cox, J. Little and D. O'Shea, Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra, Springer (1997).

[2] Z. Dvir, S. Kopparty, S. Saraf and M. Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, SIAM J. Comput. **42** (2013), 2305–2328.

[3] C. Galindo, O. Geil, F. Hernando and D. Ruano, *Improved constructions of nested code pairs*, IEEE Trans. Inform. Theory **64** (2018), 2444–2459.

[4] O. Geil, *On the second weight of generalized Reed-Muller codes*, Des. Codes Cryptogr. **48** (2008), 323–330.

[5] O. Geil and T. Høholdt, *Footprints or generalized Bezout's theorem*, IEEE Trans. Inform. Theory **46** (2000), 635–641.

[6] O. Geil and U. Martinez-Penas, *Bounding the number of common zeros of multivariate polynomials and their consecutive derivatives*, Comb. Probab. Comput. **28** (2019), 253–279.

[7] O. Geil and R. Matsumoto, *Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups*, J. Pure Appl. Algebra **213** (2009), 1152–1156.
[8] V. Guruswami and M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometric codes*, Proc. 39th FOCS (1998), 28–37.
[9] T. Høholdt, *On (or in) Dick Blahut's footprint*, Codes, Curves and Signals (1998), 3–9.
[10] S. Miura, *Linear codes on affine algebraic curves*, Trans. IEICE **J81-A(10)** (1998), 1398–1421.
[11] R. Pellikaan, *On the existence of order functions*, J. Statist. Plann. Inference **94** (2001), 287–301.
[12] R. Rolland, *The second weight of generalized Reed-Muller codes in most cases*, Cryptogr. Commun. **2** (2010), 19–40.

Reporter: Jens Zumbrägel

Participants

Gianira N. Alfarano
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
8057 Zürich
SWITZERLAND

Prof. Dr. Ángela I. Barbero
Departamento Matemática Aplicada
Escuela de Ingenierias Industriales
Universidad de Valladolid
C. Paseo de Belén, 7
47011 Valladolid
SPAIN

Prof. Dr. Martin Bossert
Institut für Nachrichtentechnik
Universität Ulm
Albert-Einstein-Allee 43
89081 Ulm
GERMANY

Prof. Dr. Nigel Boston
Department of Mathematics
University of Wisconsin-Madison
303 Van Vleck Hall
480 Lincoln Drive
Madison WI 53706
UNITED STATES

Prof. Dr. Michael Braun
Department of Informatics
Hochschule Darmstadt
Haardtring 100
64295 Darmstadt
GERMANY

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

Prof. Dr. Joan Josep Climent
Departamento de Matemáticas
Universidad de Alicante
Campus de Sant Vicent
03080 Alicante
SPAIN

Prof. Dr. Tuvi Etzion
Computer Science Department
TECHNION
Israel Institute of Technology
Haifa 32000
ISRAEL

Prof. Dr. Olav Geil
Department of Mathematical Sciences
University of Aalborg
Skjernvej 4A
9220 Aalborg
DENMARK

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

Prof. Dr. Oliver W. Gnilke
Department of Mathematics and
Systems Analysis
Aalto University
P.O. Box 11000
00076 Aalto
FINLAND

Prof. Dr. Elisa Gorla
Institut de Mathématiques
Université de Neuchatel
Rue Emile Argand 11
2000 Neuchâtel
SWITZERLAND

Dr. Markus Grassl
Max-Planck-Institut für die Physik des Lichts
Staudtstraße 2
91058 Erlangen
GERMANY

Prof. Dr. Marcus Greferath
Department of Mathematics and Systems Analysis
Aalto University
P.O. Box 11000
00076 Aalto
FINLAND

Prof. Dr. Venkatesan Guruswami
Department of Computer Science
Carnegie Mellon University
GHC 7211
5000 Forbes Avenue
Pittsburgh PA 15213-3890
UNITED STATES

Prof. Dr. Tor Helleseth
Department of Informatics
University of Bergen
Hoyteknologisenteret
5020 Bergen
NORWAY

Prof. Dr. Camilla Hollanti
Department of Mathematics and Systems Analysis
Aalto University
P.O. Box 11000
00076 Aalto
FINLAND

Lukas Holzbaur
Department of Electrical Engineering
Ludwig-Maximilians-Universität München
Theresienstrasse 90/II
80333 München
GERMANY

Prof. Dr. Anna-Lena Horlemann-Trautmann
Fakultät für Mathematik und Statistik
Universität St. Gallen
Bodanstrasse 6
9000 St. Gallen
SWITZERLAND

Dr. Sihuang Hu
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14/16
52062 Aachen
GERMANY

Dr. Relinde Jurrius
Defensie Academie
Faculteit Militaire Wetenschappen
Enys House
Het Nieuwe Diep 8
1781 AC Den Helder
NETHERLANDS

Dr. Christine A. Kelley
Department of Mathematics
University of Nebraska-Lincoln
203 Avery Hall
Lincoln NE 68588-0130
UNITED STATES

Prof. Dr. Michael Kiermaier
Mathematisches Institut
Universität Bayreuth
Universitätsstrasse 30
95447 Bayreuth
GERMANY

Prof. Dr. Gerhard Kramer
Lehrstuhl für Nachrichtentechnik
Technische Universität München
Theresienstrasse 90
80333 München
GERMANY

Dr. Julia Lieb
Departamento de Matematica
Universidade de Aveiro
Campus Universitário de Santiago
3810-193 Aveiro
PORTUGAL

Prof. Dr. Francisco Javier Lobillo Borrero
Departamento de Álgebra
E.T.S.I.
Informática y de Telecomunicación
Universidad de Granada
c/ Periodista Daniel Saucedo Aranda s/n
18071 Granada
SPAIN

Prof. Dr. Felice Manganiello
School of Mathematical and Statistical Sciences
Clemson University
Clemson, SC 29634-0975
UNITED STATES

Prof. Dr. Muriel Médard
Department of EECS
MIT
Rm 36-512
77 Massachusetts Avenue
Cambridge, MA 02139
UNITED STATES

Prof. Dr. Sihem Mesnager
Department of Mathematics
University of Paris VIII
2, rue de la Liberté
93526 Saint-Denis Cedex 02
FRANCE

Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Rm 117
Pontdriesch 14/16
52062 Aachen
GERMANY

Alessandro Neri
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
8057 Zürich
SWITZERLAND

Prof. Dr. Patric R. J. Östergård
Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 15400
00076 Aalto
FINLAND

Prof. Dr. Ferruh Özbudak
Department of Mathematics
Middle East Technical University
06531 Ankara
TURKEY

Dr. Mario O. Pavčević
Department of Applied Mathematics
Faculty of Electrical Engineering and Computing
Unska 3
10000 Zagreb
CROATIA

Dr. Raquel Pinto
Departamento de Matematica
Universidade de Aveiro
Campus Universitario de Santiago
3810-193 Aveiro
PORTUGAL

Dr. Alberto Ravagnani
School of Mathematical Sciences
University College Dublin
Belfield
Dublin 4
IRELAND

Dr. Cornelia Roessing
School of Mathematical Sciences
University College Dublin
Belfield
Dublin 4
IRELAND

Prof. Dr. Joachim Rosenthal
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
8057 Zürich
SWITZERLAND

Prof. Dr. Ronny Roth
Computer Science Department
TECHNION
Israel Institute of Technology
Haifa 32000
ISRAEL

Dr. Elif Sacikara
Department of Mathematics
Sabanci University
Orta Mahalle
Sabanci Ünv. No: 27
34956 Tuzla/Istanbul
TURKEY

Prof. Dr. Kai Uwe Schmidt
Institut für Mathematik
Universität Paderborn
Warburger Strasse 100
33098 Paderborn
GERMANY

Dr. John Sheekey
School of Mathematics and Statistics
University College Dublin
Belfield
Dublin 4
IRELAND

Dr. Vitaly Skachek
Institute of Computer Science
University of Tartu
Ulikooli 17-224
50409 Tartu
ESTONIA

Prof. Dr. Patrick Solé
CNRS
Université Aix Marseille
Centrale Marseille, I2M
Campus de Luminy
Case 907
13288 Marseille Cedex 9
FRANCE

Dr. Emina Soljanin
Department of Electrical Computer Engineering
Rutgers University
94 Brett Road
Piscataway, NJ 08854
UNITED STATES

Prof. Dr. Leo Storme
Department of Mathematics, Analysis, Logic
and Discrete Structures
Ghent University
Krijgslaan 281
9000 Gent
BELGIUM

Prof. Dr. Madhu Sudan
John A. Paulson School of Engineering and Applied Sciences
Harvard University
33 Oxford Street
Cambridge, MA 02138
UNITED STATES

Razane Tajeddine
Department of Mathematics and
Systems Analysis
Aalto University
P.O. Box 11000
00076 Aalto
FINLAND

Prof. Dr. Alexander Vardy
Department of Mathematics
UCSD
MC 0407
9500 Gilman Drive
La Jolla CA 92093
UNITED STATES

Prof. Dr. Pascal O. Vontobel
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T.
Hong Kong
CHINA

Dr. Alfred Wassermann
Mathematisches Institut
Universität Bayreuth
Universitätsstrasse 30
95440 Bayreuth
GERMANY

Violetta Weger
Institut für Mathematik
Universität Zürich
Winterthurerstrasse 190
8057 Zürich
SWITZERLAND

Charlene Weiss
Institut für Mathematik
Universität Paderborn
Warburger Strasse 100
33098 Paderborn
GERMANY

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

Prof. Dr. Øyvind Ytrehus
Simula Research Laboratory
University of Bergen
Hoyteknologisenteret
5020 Bergen
NORWAY

Prof. Dr. Gilles Zemor
Institut de Mathématiques
Université de Bordeaux I
351 Cours de la Liberation
33405 Talence Cedex
FRANCE

Prof. Dr. Jens Zumbrägel
Fakultät für Informatik und Mathematik
Universität Passau
Innstrasse 33
94032 Passau
GERMANY