

# 5th Workshop on Coding and Systems

Dublin, Ireland, September 2-4 2009

## Abstracts

---

### Toward a growth rate for pseudocodeword weights

**Abigail Mitchell**

Results on the growth rate of codeword weights in an LDPC ensemble are well known; we define a growth rate for pseudocodeword weight of regular LDPC codes, and discuss its computation for small graph cover degrees. In particular, we show that the growth rate of  $M$ -cover pseudocodewords can be computed by solving a system of  $M + 1$  simultaneous nonlinear equations.

---

### Proposal of a power-efficient modified 8B/10B coding scheme

**Alicia Roca**

We propose a power-efficient variant of the 8B/10B coding scheme and compare it with the original one (US Patent 4486739, A. X. Widmer, P. A. Franzaszek).

Computer manufacturers are working hard to reduce the power consumption of every computer component. The new coding scheme aims at minimizing the number of transitions during data transmission since every signal change from 0 to 1 implies power consumption. The original 8B/10B coding scheme was proposed in 1983 and aimed at maximizing the number of transitions to make clock recovery easier. After more than 20 years of technological improvement, it is now possible to modify and improve the original coding scheme by minimizing the number of transitions while run length is kept so that clock recovery is not endangered.

---

### Raptor Codes on Symmetric Channels

**Amin Shokrollahi**

Fountain codes are a new class of codes designed for communication over channels with unknown characteristics. Given a set of  $k$  symbols (where a symbol can be a bit, or more generally a vector of bits), a fountain code can produce a limitless stream of output symbols. The goal is the design of such a code such that reconstruction of the original  $k$  symbols is possible from any set of output symbols whose number is close to optimal. On the binary erasure channel, this translates to the reconstruction of the original  $k$  symbols given any set of  $k(1 + \varepsilon)$  output symbols, with high probability, wherein  $\varepsilon$  is a design parameter controlling the proximity to

the channel capacity. On other symmetric channels, such as the binary symmetric channel with crossover probability  $p$  (and unknown  $p$ ) the condition translates to successful recovery of the original  $k$  bits from any set of  $k(1 + \varepsilon)/(1 - h(p))$  output bits, where  $h(\cdot)$  is the binary entropy function.

Raptor codes are a sub-class of fountain codes, designed for linear time encoding and decoding algorithms. We will review the basic theory behind fountain codes, the design and analysis of these codes on the BEC, and the basic theory of these codes on other symmetric channels. The talk will also introduce some of the exciting applications of Raptor codes in the real world.

---

## Network coding with modular lattices

**Andreas Kendziorra**

We introduce a generalisation of the subspace codes for random network coding of Kötter and Kschischang to modular lattices. This generalisation is used to apply submodule-lattices for random network coding, especially subgroup-lattices of finite abelian p-groups.

---

## Bounds and Constructions of Constant Dimension Subspace Codes

**Anna-Lena Trautmann**

Constant dimension subspace codes are of great interest since Kötter and Kschischang developed a theory of subspace codes for application in random network coding. One main subject of research is to find the largest possible constant dimension codes for given parameters and minimum distance. It is helpful to first develop bounds for the size of these codes.

Several upper bounds were found, many of them in accordance with the classical bounds (of linear codes) like the Singleton, the sphere packing, the Johnson I and Johnson II bound. Moreover there is the Wang-Xing-Safavi-Naini bound and the one of the derived binary constant weight code. In general the Johnson type bounds are the tightest upper bounds found so far.

Some lower bounds were derived as well, the sphere covering bound and several constructive ones.

In some cases (for the ambient dimension  $n$ , subspace dimension  $k$ , minimum distance  $2\delta$ ), optimal code constructions have been found already. These cases are

1.  $2\delta = 2$  ,  $n = k$  ,  $n = n - k$  ,  $\delta \geq k + 1$  ,  $\delta \geq n - k + 1$  (trivial cases)
2.  $2\delta = 2k$  and  $k|n$  (spread codes)

There are many different ways for constructing “good” constant dimension codes. Kötter and Kschischang showed that the analogue of Reed-Solomon-codes in projective space is the lifting of maximum rank distance (MRD) codes. A subcase of this is the spread code construction by Manganiello, Gorla and Rosenthal. Etzion and Silberstein used constant-weight binary codes

and the corresponding reduced row echelon forms and Ferrers diagrams for their construction. A third approach has been done by Kohnert and Kurz, who look at subspace codes as  $q$ -analogues of  $t$ -designs.

I will give an overview on the above mentioned constructions and show an improvement on the Reed-Solomon-like construction, which leads to the largest codes such that the decoding algorithm of Kötter and Kschischang (with some modification) can still be used. In the case that  $2\delta = 2k$  and  $n \equiv \frac{\ln(2q^k-1)}{\ln(q)} - 1 \pmod k$ , they are optimal.

---

## Network Codes and $q$ -Analogues of Combinatorial Designs

**Axel Kohnert**

In 2008 Kötter and Kschischang showed how it is possible to use subspace codes for network coding. The codewords of a subspace code are subspaces of a finite dimensional space  $\text{GF}(q)^n$ . The distance between two spaces is given by the distance in the Hasse diagram of the lattice of all subspaces. The construction problem is now to find as many subspaces of pairwise given distance as possible. There is also a connection to the theory of designs over finite fields. We modified an approach of Braun, Kerber and Laue (which they used for the construction of designs over finite fields) to construct constant dimension subspace codes. Using this approach we found many new constant dimension codes with a larger number of codewords than previously known codes.

This is joint work with Sascha Kurz.

---

## On the Roots of a Polynomial connected to Coding and Costas Arrays

**Danny Lynch**

In this talk, we investigate the properties of the polynomial  $F(x) = (1-x)^r + x^s - 1$  over the finite field of  $q$  elements. Occurring naturally in the cross correlation of both m-sequences and Costas arrays, we seek to find cases where the number of roots over the field is maximal. Of particular interest is determining the accuracy of Rickard's Conjecture, which hypothesises an upper bound on the number of roots. Both analytical and numerical techniques are used in this investigation.

---

## Polymatroidal Flows on Two Classes of Information Networks

**Dinkar Vasudevan**

We present inner bounds to the broadcast capacity region of two classes of information networks: Networks of Multiple Access Channels (MACs) and Networks of Deterministic Broadcast Channels (DBC). Our achievability scheme is a separation based scheme consisting of a

physical layer that involves “cleaning up” the constituent channels in the network to create a point-to-point wired overlay, and a network layer that involves routing over this wired overlay. It is shown that finding the optimal way to “clean-up” is equivalent to the problem of finding maximal flows in “polymatroidal” flow networks, an already solved problem. The resulting inner bounds are cut-set bounds evaluated over product input distributions and are tight for Networks of DBCs.

---

## Bounds for Network Error Correcting Codes

**Eimear Byrne**

Information flow in a network is often enhanced if coding is adopted rather than simply routing. In [1] and [2] the authors consider a distance function suitable for coherent network coding with errors and give analogues of the sphere-packing, Singleton and Gilbert-Varshamov bounds in this setting. Here we apply arguments from classical algebraic coding theory to obtain new bounds for network error correcting codes that are the counterparts of the well-known Plotkin and Elias bounds.

- [1] S. Yang, C. K. Ngai, R. Yeung, “Construction of Linear Network Codes that Achieve a Refined Singleton Bound”, IEEE International Symposium on Information Theory, June 2007
  - [2] S. Yang, R. Yeung, “Refined Coding Bounds for Network Error Correction”, IEEE Information Theory Workshop on Information Theory for Wireless Networks, July 2007
- 

## Multidimensional convolutional codes and controllability properties of systems over finite rings

**Eva Zerz**

Using the behavior-code duality pointed out by Rosenthal et al., we study the relations between certain desirable features of a code and the corresponding controllability properties of its behavior. Module-theoretic characterizations are provided as well. The coefficients of the codes and behaviors are taken to be integers modulo  $m$ , where  $m$  is not necessarily prime.

---

## APN and Highly Nonlinear Functions on $\mathbb{Z}_n$ and Applications

**Gary McGuire**

We will give an introduction to the ideas of APN functions and nonlinearity of functions on finite fields and finite rings. In particular we will study the Exponential Welch Costas functions, using the Fourier Transform on  $\mathbb{Z}_n$ . These functions have been proposed for use in non-binary cryptosystems. High nonlinearity is required to ensure resistance to linear cryptanalysis.

We prove some properties of the nonlinearity of these functions, and we suggest a plausible connection of the nonlinearity to the class number of a quadratic field.

(Based on joint work with Konstantinos Drakakis, Rod Gow, Veronica Requena)

---

## The LinBox exact linear algebra library and applications to cryptology and codes

**Jean-Guillaume Dumas**

LinBox is a general purpose exact linear algebra library. It consists of a set of highly efficient and generic C++ template algorithms working on different data structures (dense, sparse/structured matrices) with different coefficient domains (finite fields, integer/rationals, polynomials). It uses different packages for finite fields (Givaro), high-speed dense linear algebra over word size finite fields (FFLAS-FFPACK), linear algebra over GF(2) (M4RI), arbitrary precision integers (GMP). Those kernels are used by the special purpose algorithms and its higher level self-management of resources and structured inputs through adaptive schemes. The LinBox library is also usable through classic interpreters such as Maple or SAGE.

We will sketch some LinBox capabilities first through the example of index calculus for DLP resolution over large finite fields (Block iterative methods, structured Gaussian elimination, Chinese remaindering and Hensel lifting of solutions, dense FFT matrix-polynomial linear recurring sequences, ...) and then with the example of LDPC codes (M4RI design of linear algebra over GF(2) with the 4 Russian algorithm, Gray codes, packed arithmetic, ...).

---

## Semilattice endomorphisms

**Jens Zumbrägel**

A semilattice is a partially ordered set such that every pair of elements has a supremum. It can also be described as a commutative idempotent semigroup.

In this talk we consider endomorphisms of a semilattice and explain their relevance in the classification of simple semirings and in the construction of new public-key cryptosystems.

---

## Observing a very noisy state output system and applications to stream ciphers

**Joachim Rosenthal**

Many stream ciphers consist of nonlinear combinations of linear recurrence sequences. Correlation attacks belong to the most powerful methods attacking such systems. The main task consists in finding the state of an associated linear feedback shift register having available a very noisy output sequence.

In this talk we consider the following general problem. Given an autonomous behavior over some finite ring. Assume the elements are faulty with probability  $p$ . How long will it be necessary to observe the sequence in order to compute the state and how can this be efficiently achieved?

The work is done in collaboration with Gérard Maze and Urs Wagner.

---

## Skew Polynomial Ring Codes

**John Sheekey**

In this talk we discuss the concept of codes arising from skew polynomial rings, introduced by Boucher et al. (2007), and show how to obtain an expression for the number of such codes.

---

## A Speculative Approach to Best's (10, 40, 4) Code

**Marcus Greferath**

A non-linear cyclic binary code of length 10 and minimum distance 4 that contains 40 codewords was found by Best at the end of the seventies. It was shown to be unique by Litsyn and Vardy in 1993 and resisted every attempt to be linearized by changing the alphabet structure to a ring like  $\mathbb{Z}_4$ . Conway and Sloane discovered however in 1994 that it is most convenient to rewrite this code as what is called the (cyclic) non-linear (5, 40, 4) pentacode over  $\mathbb{Z}_4$ . This talk briefly revisits Volterra series of non-linear systems and attempts to provide a mathematical preparation to represent this pentacode by a (low-degree polynomial) Volterra series.

---

## Input-state-output representations and construction of finite-support 2D convolutional codes

**Raquel Pinto**

In this talk we use the (2D) systems theory approach to represent and construct (2D) finite support convolutional codes. Concretely, considering the Fornasini-Marchesini first order state space model, we introduce the input-state-output representations of these codes. Taking into account such input-state-output representations, we construct 2D finite-support convolutional codes with a fixed free distance.

---

## Other Construction of Cyclic Low-Density MDS Array Codes

**Sara Díaz**

Let  $\mathbb{F}$  denote a finite field and let  $b$  be a positive integer. Given a code  $\mathcal{C}$  of length  $n$  over  $\mathbb{F}^b$ , the codewords of  $\mathcal{C}$  can be transformed in a one-to-one manner into words of  $\mathbb{F}^{nb}$ . We say that  $\mathcal{C}$  is a linear code of length  $n$  over  $\mathbb{F}^b$  if it is a linear code of length  $nb$  over  $\mathbb{F}$ .

In this work, we use Zech's logarithms over a prime field to provide a parity-check matrix of a cyclic low-density, and sometimes MDS, array code over  $\mathbb{F}_2^b$ .

Let  $p$  be a prime integer and let  $\mathbb{F}_p$  denote the Galois field of  $p$  elements. If  $\alpha \in \mathbb{F}_p$  is a primitive element, then

$$\mathbb{F}_p = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{p-2}\}$$

and  $\mathbb{F}_p^* \approx \mathbb{Z}_{p-1}$  with  $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ . We adopt the convention that  $0 = \alpha^\infty$ . Thus, let us denote by  $\Phi : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_{p-1}^* \cup \{\infty\}$  the application given by  $\Phi(x) = \mathcal{Z}_\alpha(x)$ , where  $\mathcal{Z}_\alpha(x)$  is the exponent of  $\alpha$  such that  $\alpha^x + 1 = \alpha^{\mathcal{Z}_\alpha(x)}$ , that is,  $\mathcal{Z}_\alpha(x)$  is the Zech's logarithm of  $x$ .

Let us fix  $n = p - 1$  and write  $n = br$ . We will consider the following sets of  $\mathbb{Z}_n$ :

$$\begin{aligned} E_0 &= \{0, b, 2b, \dots, (r-1)b\} \\ E_i &= \{x + i \mid x \in E_0\}, \quad \text{for } i = 1, 2, \dots, b-1 \end{aligned}$$

It is evident that these sets define a partition of  $\mathbb{Z}_n$  and  $\frac{n}{2} \in E_{\frac{n}{2} \bmod b}$ .

Now, if  $D_i = \Phi(E_i)$  for  $i = 0, 1, \dots, b-1$  but  $i \neq \frac{n}{2} \bmod b$ , we can construct an  $rb \times nb$  matrix  $H$ , with elements in  $\mathbb{Z}_2$ , whose non-zero elements are located, for  $j = 0, 1, \dots, n-1$ , in the positions:

- $(j, jb)$ ,
- $(k, jb + i + 1)$  if  $k \in D_i + j$  for  $0 \leq i < \frac{n}{2} \bmod b$ ,
- $(k, jb + i)$  if  $k \in D_i + j$  for  $\frac{n}{2} \bmod b < i \leq b-1$ .

The matrix  $H$  is then a parity-check matrix of an  $[n, n-r]$  cyclic low-density, and sometimes MDS, array code over  $\mathbb{F}_2^b$ .

## Metrics on Lattices

**Stefan Schmidt**

We propose a general method to derive partial metrics on finite lattices and discuss under which conditions these partial metrics can be extended to metrics.

Then we investigate super- and submodular maps on lattices and derive via the previous several promising lattice metrics.

On the construction of bent functions of  $2k$  variables from a primitive polynomial of degree  $k$

**Verónica Requena**

In this paper we use a basis of  $\mathbb{F}_2^{2k}$  and a primitive polynomial of degree  $k$  in  $\mathbb{F}_2[X]$  to construct the support of a bent function of  $2k$  variables.

# The Rate-Distortion Function of a Poisson Process with a Queueing Distortion Measure

**Vijay Subramanian**

This paper characterizes the rate distortion function of a Poisson process with a queueing distortion measure that is in complete analogy with the proofs associated with the rate distortion functions of a Bernoulli source with Hamming distortion measure and a Gaussian source with squared-error distortion measure. Analogous to those problems, the distortion measure that we consider is related to the logarithm of the conditional distribution relating the input to the output of a well-known channel coding problem, specifically the Anantharam and Verdu “Bits through Queues” coding problem. We show this problem is equivalent to a standard rate-distortion problem due to: i) the independent increments property of the Poisson process ii) the numerical entropy rate of any finite-rate point process tending to 0, iii) the existence of a reproduction with finite expected distortion, iv) the additive structure of the distortion measure. Our Shannon lower bound involves a number of mutual information inequalities, one of which exploits the maximum-entropy property of the exponential distribution. We also show that the rate distortion functions pertaining to expected distortion and deviation probability are equivalent. We conclude with a comparison to other rate-distortion formulations of the Poisson process in the literature.

Joint work with Todd Coleman and Negar Kiyavash at UIUC.

---

## On convolutional codes over the erasure channel

**Virtudes Tomás**

This paper studies the decoding capabilities of convolutional codes over the erasure channel, more concretely, of maximum distance profile (MDP) convolutional codes, and compares them with the decoding capabilities of MDS block codes over the same channel. The erasure channel involving large alphabets is an important practical channel model when studying packet transmissions over a network, e.g, the Internet.

This is a joint work with Joachim Rosenthal and Roxana Smarandache.

---

## Correcting a Fraction of Errors in Nonbinary Expander Codes with Linear Programming

**Vitaly Skachek**

A linear-programming (LP) decoder for *nonbinary* expander codes is presented. It is shown that this decoder corrects any pattern of errors of a relative weight up to approximately  $\frac{1}{4} \delta_A \delta_B$  (where  $\delta_A$  and  $\delta_B$  are the relative minimum distances of the constituent codes).