Coding theory and cryptography

A conference in honor of Joachim Rosenthal's 60th birthday

July 11 - 15, 2022 | University of Zurich

About

This conference is in honor of Joachim Rosenthal on the occasion of his 60th birthday.

Joachim Rosenthal is Professor of Applied Mathematics in the Department of Mathematics at the University of Zurich since 2004. He received the Diplom in Mathematics from the University of Basel in 1986 and the Ph.D. in Mathematics from Arizona State University in 1990. From 1990 until 2004 he has been with the Department of Mathematics at the University of Notre Dame, where he has been last ”The Notre Dame Chair in Applied Mathematics” and Concurrent Professor of Electrical Engineering.

He is one of the pioneers in the field of algebraic coding theory and cryptography.

He is a fellow of IEEE society and honorary professor of Universidad del Norte, Colombia. He also has supervised 30 Ph.D. students, many of them are active researchers in academia. Currently, he serves as Vice President of the Swiss Mathematical Society.

Organizers

Gianira Alfarano, Elisa Gorla, Anna-Lena Horlemann, Karan Khathuria, Roxana Smarandache, Violetta Weger

Conference Location

RAK-08
Archaeological Collection of the University of Zurich
Rämistrasse 73
8006 Zurich, Switzerland.

Contents

Program

	Monday	Tuesday	Wednesday	Thursday	Friday
08:45 - 10:25	Opening Grassl Lieb Abreu	Camps-Moreno Islam López-Permouth Bernal Buitrago	**Excursion**	Persichetti Lobillo Bariffi Almeida	Hieta-aho Sharma Yadav Srivastava
10:25 - 10:55	Coffee Break	Coffee Break		Coffee Break	Coffee Break
10:55 - 12:35	Requena Rocha Pinto Santana Salizzoni	Özbudak Bartz Willenborg Hörmann		Manganiello Ludhani Martínez-Moro Costello	Etzion Wassermann Serban Neri
12:35 - 14:00	Lunch	Lunch		Lunch	Lunch
14:00 - 15:40	Solé Kyureghyan Pelen Mesnager	Anupindi Berardini Iezzi Iglesias Curto		Newman Ke Riet Skachek	Ghorpade Navarro-Pérez Can Panja
15:40 - 16:10	Coffee Break	Coffee Break		Coffee Break	Coffee Break
16:10 - 17:25	Zoo visit and Welcome Apéro (17:00 onwards)	Gluesing-Luerssen Freij-Hollanti Jany		Kohrabaei Battarbee Le Coz	Baldi McMillon Kılıç
Evening		Online Greetings (18:00 onwards)		Dinner	

List of Abstracts

Monday, July 11, 2022

Session 1: 08:45 – 10:25

Chair: Roxana Smarandache

Quantum Convolutional Codes

Markus Grassl
University of Gdansk, Poland

The talk will give a brief introduction to the construction of quantum convolutional codes using classical ones. One particular aspect is the construction of quantum circuits for encoding and their inverses. Some questions that are open to the author will be presented as well.

Erasure decoding of convolutional codes with the help of linear systems

Julia Lieb
University of Zurich, Switzerland

There exist strong connections between convolutional codes and discrete-time linear systems over finite fields, actually they are essentially the same objects. This implies that convolutional codes possess a so-called input-state-output (ISO) representation via a linear system. Such ISO representations have been useful for the analysis, construction and decoding of convolutional codes. In this talk, we will in particular study the decoding of convolutional codes over the erasure channel. We will present an erasure decoding algorithm that makes use of the ISO representation of the corresponding convolutional code. Finally, we will explain the advantages of using ISO representations for the decoding over just using the parity-check matrix of the corresponding convolutional code.

Construction of an Optimal Convolutional Code of Rate 1/2

Zita Abreu
University of Aveiro, Portugal

Joint work with: Raquel Pinto, Rita Simões

Maximum distance separable convolutional codes are described by the property that the free distance reaches the generalized Singleton bound, which makes them optimal for error correction. However, the existing general constructions of such codes are available over fields of large size. In this paper, we consider convolutional codes of rate 1/2 and we derive a novel construction of an MDS convolutional code of rate 1/2 over fields of smaller size than the fields considered in the constructions available in the literature. In order to achieve this result, we consider a generator matrix $G(D)$ of a convolutional code over a field $\mathbb{F}_q$ and construct a generator matrix of a new convolutional code over the same field and of higher degree, by repeating the coeffcients of $G(D)$ of certain degrees.

Supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), references UIDB/04106/2020 and UI/BD/151186/2021.

Keywords: Convolutional codes, free distance, generalized Singleton bound, maximum distance separable (MDS) codes.

References

[1] R. Johannesson, K.S. Zigangirov, *Fundamentals of Convolutional Coding*, Digital and Mobile Communication, Wiley-IEEE Press, New Jersey, 1999.

[2] Lieb, J., Pinto, R., Rosenthal, J.. Convolutional Codes, in "Concise Encyclopedia of Coding Theory" (eds. Huffman, C; Kim, J.; Sole, P.), CRC Press, 2021.

[3] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal, Constructions for MDS-convolutional codes, *IEEE Trans. Inform. Theory*, 47(5), pp. 2045- 2049, 2001.

[4] J. Lieb and R. Pinto, Constructions of MDS convolutional codes using superregular matrices, *Journal of Algebra Combinatorics Discrete Structures and Applications*, 7(1), pp.73-84, 2020.

[5] J. Rosenthal and R. Smarandache, Maximum distance separable convolutional codes, *Appl. Algebra Engrg. Comm. Comput*, 10.1, pp. 15-32, 1999.

[6] J. Justesen, An algebraic construction of rate $1/\nu$ convolutional codes, I*EEE Trans. Inform. Theory*, 21.1, pp. 577-580, 1975.

[7] R. Smarandache and J. Rosenthal, A State Space Approach for Constructing MDS Rate $1/n$ Convolutional Codes, *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory*, pp. 116-117., 1998.

[8] H. Gluesing-Luerssen and B. Langfeld, A Class of one-dimensional MDS convolutional codes, *Journal of Algebra and Its Applications*, 5.4, pp. 505- 520, 2006.

Session 2: 10:55 – 12:35

Chair: Julia Lieb

Computing a Minimal Input-State-Output Representation of Convolutional Codes

Verónica Requena
University of Alicante, Spain

Joint work with: Joan-Josep Climent, Diego Napp

There is a close relation between convolutional codes and linear systems. This connection between both has already been established and analyzed widely by several authors (1; 2; 3; 4). In the literature, we can find different definitions for convolutional codes. In coding theory, convolutional codes can be defined as a $\mathbb{F}(z)$-linear subspace C of $\mathbb{F}^n(z)$ (see (3)), where $\mathbb{F}$ is a finite field and $\mathbb{F}(z)$ is the set of rational functions in the variable z and coefficients in $\mathbb{F}$. However, from a systems theoretic point of view, a convolutional code is a submodule $\mathcal{C}$ of $\mathbb{F}[z]^n$ (see (5)), where $\mathbb{F}[z]$ is the ring of polynomials in the variable z and coefficients in $\mathbb{F}$. In (7), Willems introduces the behavioral approach to linear systems and shows the interconnection with convolutional coding theory. In (2), Kuijper gives a very complete description of the first-order representation theory for linear behaviours. An (n, k) convolutional code $\mathcal{C}$ can be described by a time invariant linear system (see (6))

$$\begin{array}{ll} \mathbf{x}_{t+1} & = A\mathbf{x}_t + B\mathbf{u}_t, \\ \mathbf{y}_t & = C\mathbf{x}_t + D\mathbf{u}_t, \end{array} \quad \mathbf{v}_t = \begin{pmatrix} \mathbf{y}_t \\ \mathbf{u}_t \end{pmatrix}, \quad t = 0, 1, 2, \ldots, \mathbf{x}_0 = 0, \tag{0.1}$$

where $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{m\times k}$, $C \in \mathbb{F}^{(n-k)\times m}$ and $D \in \mathbb{F}^{(n-k)\times k}$. The **degree** or **complexity** of $\mathcal{C}$, denoted by δ, is the internal degree of the generator matrix, that is, the maximum degree of the $k \times k$ minors of $G(z)$. We say that (A, B, C, D) is a realization of $G(z)$ of dimension m. Moreover, it is called **minimal** if it has minimal dimension, that is, when m is equal to δ. The realization (A, B, C, D) of $G(z)$ given in (0.1) is known as the **Input-State-Output (ISO) representation**. Another way to describe a convolutional code is from the first-order representation (see (2))

$$\mathcal{C} = \left\{ \mathbf{v}(z) \in \mathbb{F}[z]^n \mid \exists \mathbf{x}(z) \in \mathbb{F}[z]^\delta : zK\mathbf{x}(z) + L\mathbf{x}(z) + M\mathbf{v}(z) = 0 \right\},$$

where $K, L \in \mathbb{F}^{(\delta+n-k)\times\delta}$ and $M \in \mathbb{F}^{(\delta+n-k)\times n}$. As far as we are aware, obtaining the minimal ISO representation of a convolutional code implies the use of a (K, L, M) first-order representation of the generator matrix in a long process to obtain a minimal ISO representation (A, B, C, D). In this paper, we present a constructive method to build a minimal ISO representation using its generator matrix directly.

References

[1] Jr. G.D. Forney. Convolutional codes I: algebraic structure. In *IEEE Transactions on Information Theory*, 16(6): 720–738, 1970.

[2] M. Kuijper. First-order Representations of Linear Systems. In *Birkhäuser, Boston, MA*, 1994.

[3] J.L. Massey and M.K. Sain. Codes, automata, and continuous systems: explicit interconnections. In *IEEE Transactions on Automatic Control,* 12(6): 644–650, 1967.

[4] J. Rosenthal. Connections between linear systems and convolutional codes. In *Codes, Systems and Graphical Models, volume 123 of The IMA Volumes in Mathematics and its Applications,* 39–66, 2001.

[5] J. Rosenthal, J.M. Schumacher, and E.V. York. On behaviors and convolutional codes. In *IEEE Transactions on Information Theory,* 42(6):1881–1891, 1996.

[6] J. Rosenthal, and E.V. York. BCH convolutional codes. In *IEEE Trans-actions on Information Theory,* 45(6): 1833–1844,1999.

[7] J.C. Willems. From time series to linear system – Part I. finite dimensional linear time invariant systems. In *Automatica,* 22(5): 561–580, 1986.

State space Realizations of periodic convolutional codes

Maria Raquel Rocha Pinto
University of Aveiro, Portugal

Joint work with: Ettore Fornasini, Diego Napp, Ricardo Pereira, Paula Rocha

Convolutional codes form a powerful and widely used class of codes which are implemented in a variety of systems including wireless standards and satellite communications. They are the output space of discrete Linear Time-Invariant (LTI) systems over a finite field and can be defined as $\mathbb{F}[d]$-modules, where $\mathbb{F}[d]$ is the ring of polynomials with coefficient in a finite field $\mathbb{F}$. In this talk we focus on periodic convolutional codes, that constitute a class of time-varying convolutional codes more involved than those generated by LTI encoders. Periodic convolutional codes process the information through several different encoders, in contrast to LTI convolutional codes that use one single encoder. This class of codes has attracted much attention after Costello conjectured in 1974 that periodic convolutional codes can attain larger free distance, and therefore better error-correction capabilities, than their time-invariant counterparts. We study the algebraic properties of periodic convolutional codes of period 2 and their representation by means of input-state-output representations. We show that they can be described as $\mathbb{F}[d^2]$-modules and present explicit representation of the set of equivalent encoders. We investigate their state-space representation and present two different but equivalent types of state-space realizations for these codes. These novel representations can be implemented by realizing two linear time-invariant system separately and switching the input (or the output) that is entering (or leaving) the system. We investigate their minimality and provide necessary and also sufficient conditions in terms of the reachability and observability properties of the two linear systems involved. The ideas presented here can be easily generalized for codes with period larger than 2.

Acknowledgments: This work is supported by Portuguese funds through the CIDMA - Center for Research and Development in Mathematics and Applications, and the Portuguese Foundation for Science and Technology (FCT-Fundacão para a Cienciae a Tecnologia), within project UIDB/04106/2020. Moreover, it was also partially supported by Base Funding - UIDB/00147/2020 and Programmatic funding- UIDP/00147/2020 of the Systems and Technologies Center - SYSTEC - fundedby national funds through the FCT/MCTES (PIDDAC). The work of the second author was is partially supported by the Spanish grants PID2019-108668GB-I00 of the Ministerio de Ciencia e Innovación of the Gobierno de España and VIGROB-28 7of the Universitat d'Alacant.

Keywords: Periodic systems, convolutional codes, realizations.

MRD convolutional codes

Filipa Santana
University of Aveiro, Portugal

Joint work with: Diego Napp and Raquel Pinto

The problem of building optimal block codes, such as MDS codes, over small fields has been an active area of research that led to several interesting conjectures. In the context of convolutional codes, optimal constructions, such as MDS or MDP, are very rare and all require very large finite fields. In this work, we focus on the problem of constructing optimal convolutional codes with respect to the rank distance, i.e., we study the construction of Maximum Rank Distance (MRD) convolutional codes. Considering convolutional codes within a very general framework, we present concrete novel classes of MRD convolutional codes for a large set of given parameters.

Generalized weights of convolutional codes

Flavio Salizzoni
University of Neuchatel, Switzerland

In 1997, Rosenthal and York gave a first definition of generalized Hamming weights of convolutional codes. Inspired by their work, in this talk, we propose a new class of generalized weights that takes into account the underlying module structure. We derive their basic properties and we discuss the relation with the other preexisting definitions. We also prove an upper bound on the weight hierarchy of MDS codes.

Session 3: 14:00 – 15:40

Chair: Urs Wagner

A notion of bent sequences based on Hadamard matrices

Patrick Solé
Institut de Mathématiques de Marseille, France

Joint work with: Wei Cheng, D. Crnkovićc, Yaya Li, Denis Krotov, Minjia Shi

A new notion of bent sequence related to Hadamard matrices was introduced recently, motivated by a security application (Solé et al, 2021). We study the self dual class in length at most 196. We use three competing methods of generation: Exhaustion, Linear Algebra and Groebner bases. Regular Hadamard matrices and Bush-type Hadamard matrices provide many examples. We conjecture that if v is an even perfect square, a self-dual bent sequence of length v always exist. We introduce the strong automorphism group of Hadamard matrices, which acts on their associated self-dual bent sequences. We give an efficient algorithm to compute that group. A generalization to complex Hadamard matrices is sketched out.

Keywords: PUF functions, Bent sequences, Hadamard matrices, regular Hadamard matrices, Bush-type Hadamard matrices

On image sets and the univariate representation of APN maps

Gohar Kyureghyan
University of Rostock, Germany

An APN map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by the property that for every non-zero $a \in \mathbb{F}_{2^n}$ the set $\{f(x+a) + f(x) | x \in \mathbb{F}_{2^n}\}$ contains exactly 2^{n-1} elements. The APN maps provide optimal resistance against differential attacks in cryptological applications, and they yield constructions for special codes. In this talk we show a generalisation of a well known result on monomial APN maps by Hans Dobbertin. Further we present some unexpected facts on the image sets of APN maps.

On the relationship between irreducible cyclic codes, finite projective planes and non-weakly regular bent functions

Rumi Melih Pelen
Erzurum Technical University, Turkey

It is known that there is a one-to-one correspondence between irreducible cyclic codes over finite fields and multiplicative subgroups of finite fields. Namely, q being a prime power, and choosing a multiplicative subgroup of order n of a finite field of order q^m as a defining set, one can obtain an irreducible cyclic $[n, m_0]$ code over $\mathbb{F}_q$ based on the generic construction method introduced by C. Ding, where m_0 divides m. The main problem is to evaluate the weight distribution of these codes, which depends on the Gaussian periods of the cyclotomic classes of order N in $\mathbb{F}_{q^m}$, where $q^m - 1 = nN$. In our paper "Strongly regular graphs arising from non-weakly regular bent functions" we observed that two disjoint subsets, $B_+(f)$ and $B_-(f)$, of the finite field of order 3^6 obtained by partitioning the field with respect to the signs of the Walsh spectrum of a sporadic example of ternary non-weakly regular bent function f could be written as a union of certain cosets of the cyclotomic classes of order 13 in $\mathbb{F}_{3^6}$. Furthermore, we observe that irreducible cyclic code obtained by using the multiplicative subgroup of order 56 in $\mathbb{F}_{3^6}$ as a defining set is three-weight. As a union of certain cosets of this defining set in $\mathbb{F}_{3^6}$, $B_+(f)$ and $B_-(f)$ give rise to fusion schemes of class 2 (strongly regular graphs), and so two-weight projective linear codes. In this talk, after reviewing the general features, I will survey our further observations on the relationship between those structures and finite projective planes.

Resolution of an equation over finite fields and its impacts

Sihem Mesnager
University of Paris VIII, France

Joint work with: Kwang Ho Kim

In this talk, we present an overview of some results coming from a very recent (2020-2022) selection, which are realizations and collections of published articles obtained in (3; 4; 6). Finding the number of solutions of equations over finite fields becomes a crucial and unavoidable task that we often encounter when we solve problems algebraically in the domain of protection information theory, basically represented by cryptography and coding theory. More importantly, solving equations over finite fields is a much more important problem from both theoretical and practice points of view. Until recently, we could get satisfied with the number of solutions and not with the complete resolutions of the equations (that is to say, by explicitly finding the set of solutions). This contentment with these shreds of information on the equations that come to us from the problems of the algebraic theory of linear codes or the theory of cryptographic functions in symmetric cryptography becomes more and more unsatisfactory, and it becomes important in +2022 to seek to develop tools and implement methods to perform the resolution of as many equations over finite fields as possible and make them available to theorists, cryptographers and from coding theory.

We discuss solving equations over finite fields. Precisely we shall focus on one equation and namely be interested in the problem of solving explicitly the equation $P_a(X) = 0$ over the finite field $\mathbb{F}_Q$, where $P_a(X) := X^{q+1} + X + a$, $Q = p^n$, $q = p^k$, $a \in \mathbb{F}_Q^*$ and p is a prime. This problem arises in many different contexts, including correcting codes and cryptographic functions. The resolution of $P_a(X) = 0$ was a long research open problem for over half of a century. The research on this specific problem has a long history of more than a half-century from the year 1967 when Berlekamp, Rumsey and Solomon firstly considered a very particular case with $k = 1$ and $p = 2$. After that, many efforts were made by several researchers (Helleseth and Kholosha in 2008 and 2010, Bracken, Tan and Tan in 2014) toward identifying all the $\mathbb{F}_Q$-zeros of $P_a(X)$ specifically for a particular problem instance over binary fields, i.e. $p = 2$. Let N_a denote the number of zeros in $\mathbb{F}_Q$ of the polynomial $P_a(X)$ and M_i denote the number of $a \in \mathbb{F}_Q^*$ such that $P_a(X)$ has exactly i zeros in $\mathbb{F}_Q$. In 2004, Bluher (1) proved that N_a equals 0, 1, 2 or $p^d + 1$ where $d = \gcd(k, n)$ and computed M_i for every i. She also stated some criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(X)$.

In this talk, we shall restrict ourselves to the even characteristic. In the first part of this talk, we will see that the resolution of $P_a(X) := X^{2^k+1} + X + a = 0$ was like a puzzle where almost all the ingredients have been introduced in the literature, and almost all had to be put together using new ideas and appropriate algebraic techniques. Specifically, we first show how we have very recently, (5) completely solved the equation $P_a(X) := X^{2^k+1} + X + a = 0$ over $\mathbb{F}_{2^n}$ when $d = 1$. We will show, in particular, using a new Identity of Dickson polynomials given by Bluher (2), that the problem of finding zeros in $\mathbb{F}_{2^n}$ of $P_a(X)$ can be divided into two problems with odd k: to find the unique preimage of an element in $\mathbb{F}_{2^n}$ under a M*ü*ller-Cohen-Matthews polynomial and to find preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial. By completely solving these two independent problems, they explicitly calculated all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(X)$, with new criteria for which N_a is equal to 0, 1 or 3 as a by-product. We highlight some of the latest important achievements listed above that could not be found without the precious advances made by Bluher (1; 2). Also, the resolution of the equation $P_a(X) = 0$ was done later in two papers in any characteristic p without any restriction on p and $\gcd(n, k)$. Thus now the equation $X^{p^k+1} + X + a = 0$ over $\mathbb{F}_{p^n}$ is completely solved for any prime p, any integers n and k.

In the second part of this talk, we shall present two applications where our was crucial. The first one is to provide in (3) a direct proof of the APN-ness of the Kasami functions. And the second one was to provide ((6)) a complete characterization of quadrinomials permutations on the finite field $\mathbb{F}_{4^m}$ of shape $f_{\underline{\epsilon}}(X) := \epsilon_1 \overline{X}^{q+1} + \epsilon_2 \overline{X}^q X + \epsilon_3 \overline{X} X^q + \epsilon_4 X^{q+1}$, definitively (where $q = 2^k$, $Q = 2^m$, m is odd, $\gcd(m, k) = 1$, $\overline{X} = X^Q$). As a direct application, we derive a complete proof of the conjecture proposed in (8) and confirm its validity by presenting a complete proof of the bijectivity of $f_{\underline{\epsilon}}$ over $\mathbb{F}_Q$ without any restriction. Solving this conjecture gives rise to a family of promising candidates with excellent cryptographic properties as S-boxes in designing block ciphers in symmetric cryptography, namely, permutations having boomerang uniformity 4 and the best-known nonlinearity. The considered conjecture proved in (6) has attracted much attention in recent years (2019-2021). As seen in the very recent literature, more than 7 papers published in IEEE-IT and DCC journals appeared proposing exciting approaches to solve this conjecture, but unfortunately, despite these efforts, the conjecture remains unsolved on its whole. However, it is the first time that we have offered an approach that solves the enter conjecture by handling both sides involving equivalence simultaneously. Very recently (7) we presented a complete proof of the bijectivity of $f_{\underline{\epsilon}}$ over $\mathbb{F}_{Q^2}$ without any restriction.

Keywords: Equation · M*ü*ller-Cohen-Matthews (MCM) polynomials · Dickson polynomial · Zeros of polynomials ·

References

[1] A.W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3), pp. 285 – 305, 2004.

[2] A.W. Bluher. A New Identity of Dickson Polynomials. *ArXiv:1610.05853 [math.NT]*, 2016.

[3] C. Carlet, K.H. Kim, and S. Mesnager. A direct proof of APN-ness of the Kasami functions. *Des. Codes Cryptogr.*, 89(3), pp. 441-446, 2021.

[4] K.H. Kim, J. Choe and S. Mesnager. Solving $X^{q+1} + X + a = 0$ over finite fields. *Finite Fields and Their Applications*, 70 : 101797, 2021.

[5] K.H. Kim and S. Mesnager. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$. *Finite Fields and Their Applications*, 63 : 101630, 2020.

[6] K.H. Kim, S. Mesnager, J.H. Choe, D.N. Lee, S. Lee, and M.C. Jo. On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. Des. Codes Cryptogr. 90(6), 1437-1461, 2022.

[7] K.H. Kim, S. Mesnager, C. H. Kim, and M.C. Jo. Completely Characterizing a Class of Permutation Quadrinomials. Submitted to *Finite Fields and Their Applications*, April 2022.

[8] K. Li, C. Li, T. Helleseth, and L. Qu. Cryptographically strong permutations from the butterfly structure. *Designs, Codes and Cryptography*, 89, pp. 737-761, 2021.

Tuesday, July 12, 2022

Session 1: 08:45 – 10:25

Chair: Felice Manganiello

Non-Special Divisors of Small Degrees and LCD Codes from Hermitian curves

Eduardo Camps-Moreno
Instituto Politécnico Nacional, Mexico

Joint work with: Gretchen Matthews, Hiram H. López

We consider the hull of an algebraic geometry code, meaning the intersection of the code and its dual. We demonstrate how LCD codes from Hermitian curves may be defined using only rational points. Our primary tool is the explicit construction of non-special divisors of degrees g and $g-1$.

k-Galois Hull of Constacyclic Codes

Habibul Islam
University of St. Gallen, Switzerland

Joint work with: Indibar Debnath, Om Prakash

The hull of a linear code is defined as the intersection of the code with its dual. It helps to classify self-dual, self-orthogonal, and linear complementary dual (LCD) codes. On the other hand, the concept of hull has been applied for constructing good entanglement-assisted quantum error-correcting codes. Due to their wide interest in the application, they have been extensively studied in several contexts. For an integer $k \geq 0$, k-Galois inner product which generalizes both Euclidean and Hermitian inner products has introduced in 2017. Under this product here, we investigate the hull of constacyclic codes over finite fields $\mathbb{F}_q$, where q is a prime power. For a unit $\lambda \in \mathbb{F}_q^*$, we first rearrange the irreducible factors of $x^n - \lambda$ in the desired form, and then by utilizing this factorization we formulate the hull dimension of λ-constacyclic codes of length n. Moreover, under certain restrictions on q, we enumerate the number of such constacyclic codes for a given hull dimension.

A Monoid structure on the set of all binary operations over a fixed set

Sergio López-Permouth
Ohio University, United States of America

In recent years, the word magma has been used to designate a pair of the form $(S, *)$ where $*$ is a binary operation on the set S. Inspired by that terminology, we use the notation $M(S)$ (the magma of S) to denote the set of all binary operations on the set S (i.e. all magmas with underlying set S.) In [1], distributivity hierarchy graphs of a set are introduced. Given a set S, its hierarchy graph has $M(S)$ as vertices and there is an edge from one operation, $*$, to another one, $\circ$, if $*$ distributes over $\circ$. Given $* \in M(S)$, the set $\text{out}(*) = \{\circ \in M(S) | * \text{ distributes over } \circ\}$ is called the outset of $*$. We define an operation that make $M(S)$ a monoid in such a way that each outset is a submonoid. This endowment gives us a possibility to compare the various elements of $M(S)$ with respect to the monoid structure of their outsets. Various properties of the operation mentioned above are considered, including multiple additive structures on $M(S)$ that have it as the multiplicative part of a nearring.

References

[1] López-Permouth and L. H. Rowen, "Distributive hierarchies of binary operations", Advances in rings and modules, 225–242, Contemp. Math., 715, Amer. Math. Soc., [Providence], RI, [2018].

[2] López-Permouth, Rafieipour, and Owusu Mensah, "Distributivity relations on the binary operations over a fixed set", Comm. Algebra 49 (2021), no. 12, 5093–5108.

[3] López-Permouth, Rafieipour, and Owusu Mensah, "A monoid structure on the set of all binary operations over a fixed set", to appear in Semigroup Forum.

New advances in permutation decoding of first-order Reed-Muller codes

José Joaquín Bernal
Universidad de Murcia, Spain

Joint work with: Juan Jacobo Simón

In this work we define a variation of the classical permutation decoding algorithm which is valid for any affine-invariant code with respect to a specific kind of information sets (we refer to it as Algorithm II). In particular, it can be used successfully for first-order Reed-Muller codes, R(1, m), with respect to the information sets introduced in [1]. Then, under some simple conditions, we show that this algorithm improves notably the number of errors we can correct in comparison with the known results. Fixed an information set for a given linear code, the permutation decoding algorithm (e.g. [2]) uses a special set of its permutation automorphisms called s-PD-set, where s represents the number of errors it is able to correct. Then, the idea of permutation decoding is to apply the elements of the PD-set to the received vector until the errors are moved out of the fixed information set. The existence of PD-sets relies on the information set previously taken as reference. Many authors have studied families of codes for which it is possible to develop methods to find PD-sets with respect to certain types of information sets. In this paper, our interest is the family of Reed-Muller codes. The problem of applying permutation decoding to Reed-Muller codes has been addressed for many authors earlier, see for instance [3], [6], [7]. We present a slight modification of the notion of PD-set that allows us to apply the procedure with respect to certain type of information sets, in particular, it can be applied taking as reference the information sets given in [1]. Then, we use these new sets to define a new algorithm that relies on their properties and the algebraic structure of affine-invariant codes. We can achieve this main result:

Theorem 1. *Let $R(1,m)$ be the first-order Reed-Muller code of length 2^m, $(m \in \mathbb{N}, m > 2)$. Let $n = 2^m - 1 = r_1 \cdot r_2$ with $\gcd(r_1, r_2) = 1$, $r_1, r_2 > 1$ and $\mathrm{Ord}_{r_1}(2) = m$. Then we can correct up to s errors by using Algorithm II where*

$$s = (\lambda_0 + 1) \cdot r_2 - 1$$

and $\lambda_0 = \max\left\{\lambda \mid m < \left\lceil \frac{r_1}{\lambda} \right\rceil\right\}$.

m	r_1	r_2	A	$B1$	$B2$	Algorithm II		m	r_1	r_2	A	$B1$	$B2$	Algorithm II
4	5	3	3	1	2	5		11	23	89	170	128	169	266
6	9	7	5	3	8	13		12	13	315	315	256	314	629
8	17	15	28	16	27	44		14	43	381	1092	1024	1091	1523
9	73	7	51	32	50	62		15	151	217	2047	2048	2047	2386
10	11	93	93	64	92	185		16	257	255	3855	2048	3854	4334

Table 0.1: Number of corrected errors

By using Theorem 1 we obtain the results contained in Table 0.1. We compare them we the best known results on this topic. Specifically: Column A refers to [4] and Columns B1, B2 refer to two different results in [5].

This work was supported by the Spanish Government under Grant PID2020-113206GB-100 funded by MCIN/AEI/10.13039/501100011033.

References

[1] J. J. Bernal and J. J. Simón, “Information sets from defining sets for Reed-Muller codes of first and second order”, IEEE Trans. Inform. Theory, vol. 64 , no. 10 , pp. $6484-6497, 2018$.

[2] W. C. Huffman, “Codes and Groups”, in Handbook of Coding Theory, vol II, V. S. Pless, W. C. Huffman and R. A. Brualdi Eds. Amsterdam. NorthHolland, 1998

[3] J. D. Key, T. P. McDonough, V. C. Mavron, “Information sets and partial permutation decoding for codes from finite geometries”, Finite Fields Appl. vol 12, pp. 232-247, 2006.

[4] J. D. Key, T. P. McDonough, V. C. Mavron, “Reed-Muller codes and permutation decoding”, Discrete Mathematics vol 310 , pp. $3114-3119, 2010$.

[5] J. D. Key, T. P. McDonough, V. C. Mavron, “Improved partial permutation decoding for Reed-Muller codes”, Discrete Mathematics vol 340, no. 4 pp. $665-682, 2016$.

[6] H-J Kroll, R. Vincenti, “PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of PG(5,2)”, Discrete Mathematics vol 308, pp. 408-414, 2006.

[7] P. Seneviratne. ”Partial permuation decoding for the first-order Reed-Muller codes”, Discrete Mathematics vol 309, pp. 1967-1970, 2009.

Session 2: 10:55 – 12:35

Chair: Elisa Gorla

Rank Metric Codes, Subcodes and Different Notions of Duality

Ferruh Özbudak
Middle East Technical University, Turkey

Joint work with: Javier de la Cruz

In this paper we study rank metric codes in certain ambient spaces together with different inner products. Using some properties of subcodes and the different notions of duality in the ambient spaces we obtain some new extremal rank metric codes. In particular we observe some differences in between the codes based on Hamming schemes and rank metric schemes.

Universal Decoding of Interleaved Linearized Reed–SolomonCodes in the Sum-Rank Metric

Hannes Bartz
German Aerospace Center, Germany

Joint work with: Felicitas Hörmann, and Thomas Jerkovits

Linearized Reed–Solomon (LRS) codes achieve the Singleton-like bound in the sum-rank metric and generalize Reed–Solomon codes and Gabidulin codes. They can be defined as evaluation codes with respect to the generalized operator evaluation of skew polynomials, which depends not only on an evaluation point (or code locator) but also on an additional evaluation parameter. Vertically interleaved LRS codes consist of matrices whose rows are codewords of LRS codes. If all codewords are from the same code, the construction is called homogeneous. In contrast to that, inhomogeneous interleaving allows codes with

different code locators, different evaluation parameters,and different code dimensions. So far, homogeneous vertical interleaving of LRS codes has been studied in (1) where an interpolation-based and a Loidreau–Overbeck-like decoder were derived. We use the idea of the universal decoder for inhomogeneous interleaved Gabidulin codes presented in (2) and generalize it to interleaved LRS codes in the sum-rank metric. We show that a decoder $\mathcal{D}$ for homogeneously vertically interleaved LRS codes can be applied to the inhomogeneous setting by means of linear-algebraic transformations in most cases. If the constituent codes have different code locators that span the same space, $\mathcal{D}$ can be applied after multiplying each row of the received matrix with a full-rank block-diagonal matrix over $\mathbb{F}_q$ (for codes over $\mathbb{F}_{q^m}$). The result is then obtained by reversing the transformation after decoding. We show that for certain cases, inhomogeneous interleaving with constituent codes with different evaluation parameters can be seen as homogeneous interleaving with another encoding strategy. $\mathcal{D}$ can thus be directly applied and the resulting codeword only needs to be multiplied with a full-rank $\mathbb{F}_{q^m}$-matrix to account for the different encodings. Note that no transformations are required when using syndrome-based decoders in this case. If the constituent codes have different code dimensions, the interleaved construction can be homogenized by using the LRS code of maximal dimension. Summing up, we provide decoding schemes for more general code classes and hence also contribute to the field of code-based cryptography where security levels strongly depend on the performance of the available decoders and their complexities.

References

[1] H. Bartz, S. Puchinger. Fast Decoding of Interleaved Linearized Reed—Solomon Codes and Variants. arXiv:2201.013392, 2022.

[2] V. Sidorenko, W. Li, G. Kramer. On Interleaved Rank Metric Codes. In *2020 Algebraic and Combinatorial Coding Theory (ACCT).* pages 128–134, 2020.

The Density of Extremal Codes with Sublinearity

Nadja Willenborg
University of St. Gallen, Switzerland

First we will estimate the number of k-dimensional codes in $\mathbb{F}_{q^\ell}^{n\times s}$ with minimum distance bounded from below. Using proof techniques from graph theory we derive a lower and an upper bound for this number. In the following we give a prediction of the asymptotic proportion of codes with respect to sparsity and density as the field size tends to infinity. We conclude that these properties depend on whether or not the cardinality of a code is negligible with respect to an expression depending on the ball of the considered metric. We then apply this theory to calculate the asymptotic proportion of $\mathbb{F}_{q^\ell}$-linear codes in the Hamming-, rank-, and sum-rank metric who meet the Singleton bound with equality. Our results show that $\mathbb{F}_{q^\ell}$-linear MRD codes in the rank metric are sparse for most parameter sets. For the case of $\mathbb{F}_{q^\ell}$-linear MDS codes the behaviour is exactly the opposite. These codes are dense as $q \to \infty$. To study $\mathbb{F}_{q^\ell}$-linear MDS codes we define a row Hamming distance on $\mathbb{F}_{q^\ell}^{n\times s}$ as follows

$$D^{\mathrm{row}}(X,Y) = \omega^{\mathrm{row}}(X-Y),$$

where $X, Y \in \mathbb{F}_{q^\ell}^{n\times s}$ and $\omega^{\mathrm{row}}(X) = |\{i \in [n] : X^\top e_i \neq 0\}|$ describes the row Hamming weight of a matrix. We also investigate the asymptotic proportion of $\mathbb{F}_{q^\ell}$-linear MSRD codes in the sum-rank metric, obtaining results that agree with recent results in the Hamming and rank metric. More precisely MSRD codes are asymptotically dense if and only if they are considered as (n-) sum-rank metric codes, i.e., codes consisting of exactly n matrix blocks. In all other cases, i.e., codes with less than n blocks, MSRD codes are sparse. As an $[n \times s, k, d]_{q^\ell}$-code can only be MDS, MRD or MSRD if s divides the dimension k of the code, we also study families of codes whose dimension is not divisible by s but whose minimum distance is still the largest possible distance for codes of that dimension. We conclude that especially in the rank- and sum-rank metric the asymptotic results of these quasi-optimal codes differ from the usual MRD-, respectively MSRD codes. Depending on the considered subfield linearity, i.e., the degree ℓ of the field extension, these families of codes can become dense.

Speeding up Error-Erasure Decoding of Linearized Reed–Solomon Codes in the Sum-Rank Metric

Felicitas Hörmann
German Aerospace Center, Germany

Joint work with: Hannes Bartz and Sven Puchinger

The sum-rank metric covers the Hamming as well as the rank metric as special cases and has versatile applications in e.g. multishot network coding and code-based cryptography. Linearized Reed–Solomon (LRS) codes are the sum-rank analogs of Reed–Solomon and Gabidulin codes. Several decoders are available for this code class and also interleaved and folded variants have already been studied.The known LRS decoding schemes consider an additive sum-rank channel with errors of bounded sum-rank weight. We extend this error model by allowing three error types: full errors, row erasures,and column erasures. Here, row (column) erasures refer to errors, whose row (column) space is unknown but whose column (row) space is known at the receiver. In (1), we derive an error-erasure decoder for LRS codes by generalizing the syndrome-based error-only decoder from (2). The Berlekamp–Massey-like algorithm can correct t_F full errors, t_R row erasures, and t_C column erasures as long as $2t_F + t_R + t_C \leq n - k$ holds for code length n and dimension k. The decoding scheme has quadratic complexity in the code length and one problem requiring $\mathcal{O}(n^2)$ operations is computing a basis of a skew polynomial's root space with respect to generalized operator evaluation for several evaluation parameters from different conjugacy classes. We achieve a speedup of this task by adapting the probabilistic root-finding algorithm for linearized polynomials, that was presented by Skachek and Roth in (3), to the more general skew-polynomial setting. For a skew polynomial $p \in \mathbb{F}_{q^m}[x;\theta]$ with a finite field $\mathbb{F}_{q^m}$ and an $\mathbb{F}_{q^m}$-automorphism θ and ℓ evaluation parameters from different conjugacy classes of $\mathbb{F}_{q^m}$, the complexity of the computation reduces to $\mathcal{O}(m\ell \deg(p))$ operations in $\mathbb{F}_{q^m}$. The main idea is to iteratively determine a basis of the root space of p with respect to a fixed evaluation parameter a. In each step, we find a second skew polynomial q whose image coincides exactly with the root space of p with respect to a. We then probabilistically compute a basis of the image of q and obtain the overall result as the union of the found bases. Remark that the speedup also applies to error-erasure decoding of interleaved LRS codes. Applications of error-erasure decoding of LRS codes include the decoding of lifted LRS codes in the sum-subspace metric for error control in multishot network coding and randomized decoding algorithms and the resulting attacks on code-based cryptosystems.

References

[1] F. Hörmann, H. Bartz, S. Puchinger. Error-Erasure Decoding of Linearized Reed–Solomon Codes in the Sum-Rank Metric. In *IEEE International Symposium on Information Theory*, 2022.

[2] S. Puchinger, U. Martínez-Peñas. Personal Communication, 2021.

[3] V. Skachek, R.M., Roth. Probabilistic Algorithm for Finding Roots of Linearized Polynomials. In *Designs,Codes and Cryptography.* 46(1):17–23, 2008.

Session 3: 14:00 – 15:40

Chair: Felix Fontein

Pseudorandom sequences from hyperelliptic curves

Vishnupriya Anupindi
RICAM (Johann Radon Institute for Computational and Applied Mathematics), Austria

Joint work with: László Mérai

Pseudorandom sequences, i.e., sequences which are generated with deterministic algorithms but look random, have many applications, for example in cryptography, in wireless communication or in numerical methods. In this work, we are interested in studying the properties of pseudorandomness of sequences derived from hyperelliptic curves of genus 2.

In particular, we will look at two different ways of generating sequences, that is, the linear congruential generator and the Frobenius endomorphism generator. We show that these sequences possess good pseudorandomness properties in terms of linear complexity. In this talk, we will introduce the N-th linear complexity of a sequence, the group structure on hyperelliptic curves of genus 2 and look at the main results.

Computing Riemann-Roch spaces for algebraic geometry codes

Elena Berardini
Eindhoven University of Technology, The Netherlands

Reed–Solomon codes are a well–known technique to represent data in the form of vectors, such that the data can be recovered even if some vector coordinates are corrupted. These codes have many properties. They allow reconstructability of coordinates that have been erased. They ensure the privacy of the data against an adversary learning many coordinates. They are compatible with the addition and multiplication of data. Nevertheless, they suffer from some limitations. For instance, the storage size of vector coordinates grows logarithmically with the number of coordinates. So–called algebraic geometry (AG) codes are a generalization of Reed–Solomon codes that enjoy the same properties, while being free of these limitations. Therefore, the use of AG codes provides complexity gains and turns out to be useful in several applications such as distributed storage [2], distributed computation on secrets [4], and zero-knowledge proofs [3].

Algebraic geometry codes are constructed by evaluating spaces of functions, called Riemann–Roch spaces, at the rational points on a curve. It follows that the computation of these spaces is crucial for the implementation of AG codes. In this talk, I will present a joint work with S. Abelard, A. Couvreur and G. Lecerf [1] on the effective computation of bases of Riemann–Roch spaces of curves. I will discuss the ideas behind our algorithm, including in particular Brill–Noether theory.

The curves used in the construction of AG codes were for the most part limited to those for which the Riemann–Roch bases were already known. This new work and the ones that will follow will allow the construction of AG codes from more general curves.

References

[1] S. Abelard, E. Berardini, A. Couvreur, and G. Lecerf. "Computing Riemann–Roch spaces via Puiseux expansions". In: Journal of Complexity (2022), p. 101666. ISSN: 0885-064X.

[2] A. Barg, K. Haymaker, E. W. Howe, G. L. Matthews, and A. Várilly-Alvarado. "Locally recoverable codes from algebraic curves and surfaces". In: Algebraic geometry for coding theory and cryptography. Vol. 9. Assoc. Women Math. Ser. Springer, Cham, 2017, pp. 95–127.

[3] S. Bordage, M. Lhotel, J. Nardi, and H. Randriam. "Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes". Preprint. 2022.

[4] R. Cramer, M. Rambaud, and C. Xing. "Asymptotically-Good Arithmetic Secret Sharing over $Z/p^{\ell}Z$ with Strong Multiplication and Its Applications to Efficient MPC". In: Springer-Verlag, 2021.

Computing the endomorphism ring of a supersingular elliptic curve

Annamaria Iezzi
Università degli Studi di Napoli Federico II, Italy

Joint work with: Jenny G. Fuselier, Mark Kozek, Travis Morrison, Changningphaabi Namoijam.

In recent years, isogeny-based cryptosystems have captured the attention of the math or crypto community for their potential resistance to quantum attacks. In this context, the most promising protocols have as central objects supersingular elliptic curves defined over a finite field, and their security is therefore based on the mathematical problem of calculating an isogeny between two supersingular elliptic curves E and E'. It has been shown that this problem can be reduced to the calculation of the endomorphism rings of E and E' In this talk, after reviewing the mathematical and cryptographic context, we will then present an improved algorithm for computing the endomorphism ring of a supersingular elliptic curve over a finite field.

Quantum codes from generalized AG codes

José Ignacio Iglesias Curto
University of Salamanca, Spain

Quantum coding theory is a rising research area, as quantum computers are closer than ever to be a reality. In quantum computing, errors on the information not only may occur while transmission or storage, but also during computation itself. Therefore, quantum error correction is a critical task.

It is well known that classical linear codes may be used to design counterparts in quantum coding, such as BCH codes, Reed-Solomon codes, quasicyclic codes, etc.. In addition, some of the properties of the quantum codes so obtained reflect familiar properties of their classical analogous.

We aim to explore this connection in the case of the family of "Generalized AG codes" in order to construct quantum codes with a recognizable structure, characterize their properties and study how do they improve other known constructions.

Session 4: 16:10 – 17:25

Chair: Gianira Alfarano

Coproducts in Categories of q-Matroids

Heide Gluesing-Luerssen
University of Kentucky, United States of America

Joint work with: Benjamin Jany

A q-matroid is the q-analogue of a (classical) matroid. Its ground space is a finite-dimensional vector space over some finite field $\mathbb{F}_q$, say E, and the rank function is defined on the lattice of subspaces, $\mathcal{L}(E)$. The required properties of the rank functions (boundedness, monotonicity, and submodularity) are the natural generalization of classical matroids. As is well known [6], vector rank-metric codes give rise to q-matroids. Precisely, given an $\mathbb{F}_{q^m}$-linear rank-metric code $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ with generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$, then the map

$$\rho : \mathcal{L}\left(\mathbb{F}_q^n\right) \longrightarrow \mathbb{N}_0, \quad \text{colsp}(Y) \longmapsto \text{rk}(GY)$$

where colsp (Y) denotes the column space of the matrix $Y \in \mathbb{F}_q^{n\times y}$, is a rank function on the subspace lattice of $\mathbb{F}_q^n$. The resulting q-matroid $\mathcal{M} = \left(\mathbb{F}_q^n, \rho\right)$ does not depend on G and is thus uniquely determined by the code $\mathcal{C}$. More generally, $\mathbb{F}_q$-linear rank-metric codes in $\mathbb{F}_q^{n\times m}$ give rise to q-polymatroids, which have been studied in, for instance, [5, 7, 4, 3].

For q-matroids a variety of cryptomorphic definitions have been derived [6, 1]. Yet - compared to classical matroid theory - the theory of q-matroids is still at any early stage. For instance, the notion of direct sum and decomposability into direct summands has not yet been fully understood. Simple examples show that none of the equivalent definitions of a direct sum of classical matroids leads to a well-defined notion for q-matroids. Only recently a very interesting first attempt of defining a direct sum of q-matroids has been put forward in [2].

In this talk we introduce various types of maps between q-matroids and investigate the existence of a coproduct in each of the resulting category. This study is motivated by the fact that the direct sum of classical matroids is a coproduct in the category with strong maps as morphisms.

In order to study categories of q-matroids we first need to introduce maps between these objects. This can be achieved as follows. A map ϕ between q-matroids $\mathcal{M}_1 = (E_1, \rho_1)$

and $\mathcal{M}_2 = (E_2, \rho_2)$ is, first of all, a map from E_1 to E_2. We do not require ϕ to be linear (or semi-linear), but it has to map subspaces of E_1 to subspaces of E_2. In other words, it induces a map from $\mathcal{L}(E_1)$ to $\mathcal{L}(E_2)$. Such maps are called $\mathcal{L}$-maps. There are various options of how an $\mathcal{L}$-map may respect q-matroid structure:

(i) ϕ is strong if for all flats V of $\mathcal{M}_2$ the pre-image $\phi^{-1}(V)$ is a flat of $\mathcal{M}_1$;

(ii) ϕ is weak if $\rho_2(\phi(V)) \leq \rho_1(V)$ for all $V \in \mathcal{L}(E_1)$

(iii) ϕ is rank-preserving if $\rho_2(\phi(V)) = \rho_1(V)$ for all $V \in \mathcal{L}(E_1)$.

In addition, we may require the $\mathcal{L}$-maps to be linear. All of this gives rise to 6 different categories, where the objects are the q-matroids and the morphisms are either linear or arbitrary $\mathcal{L}$-maps of any of the above three types.

Recall that a coproduct of two objects M_1 and M_2 in a category $\mathbf{C}$ is a triple (M, ξ_1, ξ_2) where M is an object in $\mathbf{C}$ and $\xi_i : M_i \longrightarrow M$ are morphisms such that for all objects N in $\mathbf{C}$ and all morphisms $\tau_i : M_i \longrightarrow N$ there exists a unique morphism $\epsilon : M \longrightarrow N$ such that $\epsilon \circ \xi_i = \tau_i$ for $i = 1, 2$.

It turns out that of the above mentioned categories of q-matroids only the category with linear weak maps as morphisms has a coproduct. In that case, the coproduct is the direct sum introduced in [2]. This result stands in contrast to the classical case, where the category with strong maps leads to the direct sum as coproduct.

It remains an open question whether representability is inherited by the direct sum: given q-matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ that are representable by rank-metric codes, is then also $\mathcal{M}_1 \oplus \mathcal{M}_2$ representable by a rank-metric code?

References

[1] E. Byrne, M. Ceria, and R. Jurrius. Constructions of new q-cryptomorphisms. J. Comb. Theory. Ser. $B, 153 : 149 - 194, 2022$.

[2] M. Ceria and R. Jurrius. The direct sum of q-matroids. Preprint 2021. arXiv: 2109.13637.

[3] H. Gluesing-Luerssen and B. Jany. Independent spaces of q-polymatroids. Preprint 2021. arXiv: $2105.01802, 2021$

[4] H. Gluesing-Luerssen and B. Jany. q-Polymatroids and their relation to rank-metric codes. Preprint 2021. arXiv: 2104.06570, 2021

[5] E. Gorla, R. Jurrius, H. López, and A. Ravagnani. Rank-metric codes and q-polymatroids. *J.* Algebraic Combin., 52:1-19, 2020.

[6] R. Jurrius and R. Pellikaan. Defining the q-analogue of a matroid. Electron. J. Combin., 25:P3.2, 2018.

[7] K. Shiromoto. Codes with the rank metric and matroids. Des. Codes Cryptogr., 87:1765-1776, 2019.

Lifting codes and deriving matroids

Ragnar Freij-Hollanti
Aalto University, Finland

Motivated by problems in Private Information Retrieval, we ask how large a linear code $\mathcal{Q}^{\mathcal{T}} \subseteq F^n$ can be, when it is required to agree with a prescribed code $\mathcal{Q} \subseteq F^n$ on a collection $\mathcal{T} \subseteq 2^{[n]}$ of *colluding sets*. We show that the answer to this question is strongly related to the *derived matroid* of the code $\mathcal{Q}$, which is remarkably not a matroid invariant of $\mathcal{Q}$. In order to maximize the *lifted code* $\mathcal{Q}^{\mathcal{T}}$ when the combinatorics, but not the linear structure, of $\mathcal{Q}$ is given, we introduce two novel combinatorial notions. Namely, when $M = ([n], \mathcal{C})$ is a matroid on the ground set $[n]$ and circuits $\mathcal{C}$, we define a *generic derived matroid* δM on the ground set $\mathcal{C}$, and the lift $M^{\mathcal{T}}$ of M over a "collusion pattern" $\mathcal{T} \subseteq 2^{[n]}$.

The Characteristic Polynomial of q-Matroids

Benjamin Jany
University of Kentucky, United States of America

q-Matroids, the q-analogue of matroids, were found useful in studying $\mathbb{F}_{q^m}$-linear rank metric codes. A q-matroid can be defined via a bounded, non-decreasing and submodular integer-valued rank function on the collection of subspaces of $\mathbb{F}_q^n$. Matroids are defined in an analogous way, where a rank function is defined on the collection of subsets of a finite set. It turns out an $\mathbb{F}_{q^m}$-linear rank metric code induces a q-matroid and many of the code's invariants can be determined from the associated q-matroid. In a similar way, a linear block code with the Hamming metric induces a matroid that captures the code's invariants. Given a q-matroid defined over $\mathbb{F}_q^n$, one can associate to it a matroid defined over the projective space $\mathbb{PF}_q^n$ called the projectivization matroid. The latter shares a similar flat structure than the q-matroid and therefore becomes a useful tool to study q-matroids. In this talk I will introduce the construction of the projectivization matroid and show that if the q-matroid arises form a rank metric code, then there exist a linear block code that induces the projectivization matroid. Using this connection, I will then show how one can derive a q-analogue of the critical theorem for q-matroids and $\mathbb{F}_{q^m}$-linear rank metric codes by studying the projectivization matroid.

Thursday, July 14, 2022

Session 1: 08:45 – 10:25

Chair: Giacomo Micheli

Developing Innovative Frameworks for Efficient Code-based Signatures

Edoardo Persichetti
Florida Atlantic University, United States of America

Code-based cryptography is one of the most popular areas of research in the post-quantum family. Yet, while solutions for encryption and key exchange are now recognized to be stable and have reached a good level of performance, the same can't be said for signature schemes. Several protocols have been proposed over the years, the near entirety of which have either been broken, or exhibit very undesirable features, leading to impractical schemes. In this talk, I will discuss a variety of recent approaches based on zero-knowledge, that are able to offer transformative solutions, paving the way for truly practical schemes.

Non Commutative Goppa Codes and their Use in Code-based Cryptography

Francisco Javier Lobillo
Universidad de Granada, Spain

Joint work with: J. Gómez-Torrecillas, G. Navarro

Let $R = L[x; \sigma, \partial]$ be an Ore extension of a field. Let $F \subseteq L$ be a subfield such that $[L : F] = m$. Let $g \in R$ be a nonzero twosided polynomial, $\alpha_0, \dots, \alpha_{n-1} \in L$ be P-independent elements such that $(x - \alpha_i, g)_\ell = 1$ for all $0 \leq i \leq n-1, h_i \in R$ such that

$\deg\left(h_i\right) < \deg(g)$ and $\left(x-\alpha_i\right) h_i - 1 \in Rg$, and $\eta_0, \ldots, \eta_{n-1} \in L^*$. A (generalized) skew differential Goppa code $\mathcal{C} \subseteq F^n$ is defined as

$$\mathcal{C} = \left\{ \left(c_0, \ldots, c_{n-1}\right) \in F^n \mid \sum_{i=0}^{n-1} h_i \eta_i c_i \in Rg \right\}$$

We say that $\{\alpha_0, \ldots, \alpha_{n-1}\}$ are the positional points, g is the skew differential Goppa polynomial and $h_0, \ldots, h_{n-1}$ are the parity check polynomials.

For a received word $r = c + e \in F^n$, where $c \in \mathcal{C}$ and $e = \sum_{j=1}^{\nu} e_j \varepsilon_{k_j}$ with $e_j \neq 0$ for $1 \leq j \leq \nu$, The syndrome polynomial is defined and computed as

$$s = \sum_{i=0}^{n-1} h_i \eta_i r_i .$$

We define the error locator polynomial as

$$\lambda = \left[\left\{ x - \alpha_{k_j} \mid 1 \leq j \leq \nu \right\}\right]_{\ell} .$$

Then $\deg(\lambda) \leq \nu$ and, for all $1 \leq j \leq \nu$, there exists $\rho_{k_j} \in R$ such that $\deg\left(\rho_{k_j}\right) \leq \nu - 1$ and

$$\lambda = \rho_{k_j}\left(x - \alpha_{k_j}\right) .$$

The error evaluator polynomial is defined as

$$\omega = \sum_{j=1}^{\nu} \rho_{k_j} \eta_{k_j} e_j$$

It follows that $\deg(\omega) < \nu$.

Theorem 1. *The error locator λ and the error evaluator ω polynomials satisfy the non-commutative key equation*

$$\omega = \kappa g + \lambda s,$$

for some $\kappa \in R$. Assume that $\nu \leq t = \left\lfloor \frac{\deg g}{2} \right\rfloor$. Let u_l, v_l and r_l be the Bezout coefficients returned by the left extended Euclidean algorithm (LEEA) with input g and s, where l is the index determined by the conditions $\deg r_{l-1} \geq t$ and $\deg r_l < t$. Then there exists $h \in R$ such that $\kappa = hu_l, \lambda = hv_l$ and $\omega = hr_l$.

This theorem allows to use the LEEA to solve the key equation. Decoding failures, which can appear when $(\lambda, \omega)_{\ell} \neq 1$, are solved in a similar way to [2].

When $\mathbb{F}_q = F \subseteq L = \mathbb{F}_{q^m}$ and $\partial = 0$, we propose a Key Encapsulation Mechanism based in McEliece and Niederreiter's cryptosystems (see [3, 4, 1]), where parameters, key generation algorithms, encapsulation and decapsulation methods are provided.

References

[1] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varum Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlison, and Wen Wang. "Classic McEliece: conservative code-based cryptography". Technical report, NIST's Post-Quantum Cryptography Standardization Project, 102020

[2] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. "A Sugiyama-like decoding algorithm for convolutional codes". IEEE Transactions on Information Theory, 63(10) : 6216 − 6226, 2017. arXiv: 1607.07187

[3] R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory". Technical Report 42-44, National Aeronautics and Space Administration, January and February 1978.

[4] Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory". Problems of Control and Information Theory., 15:159-166, 1986.

The Marginal Distribution of the Lee Channel and its Applications

Jessica Bariffi
German Aerospace Center, Germany and University of Zurich, Switzerland

The syndrome decoding problem lays the foundation for code-based cryptography as it deals with decoding a random linear code over a finite field with respect to some decoding metric by recovering the error term added to the transmitted word. The key size depends on the complexity of the syndrome decoding problem, which in turn depends on the considered metric. The syndrome decoding problem has originally been introduced for the Hamming metric. However, also other metrics have been studied for the use in code-based cryptography, for instance the Lee metric.

In this talk, we consider a random instance of the syndrome decoding problem in the Lee metric over the finite ring of integers modulo q. We assume that a random error term of Lee weight t and length n has been added to the transmitted codeword. For this instance of the syndrome decoding problem in the Lee metric, we are going to derive the marginal distribution for the entries of the additive error term. To do so, we consider the most probable pattern in the error vector, which we refer to as a typical sequence. By the conditional limit theorem, the marginal distribution corresponds then exactly to the distribution of the typical sequence, which is proportional to an exponential function. Depending on the Lee weight t, this exponential function is either decreasing or increasing. Hence, either entries of small weight are more probable or vice versa, respectively.

The fastest algorithms to solve this instance are called information set decoding algorithm. In the Lee metric the best known such algorithm yet is a variant of the binary BJMM-Version. We are going to present two modified version of this algorithm, one for decoding up to the minimum distance and one to decode beyond the minimum distance. In both cases, we use the knowledge of the marginal distribution to assume that with high probability the least probable Lee weights lie outside the information set, where the two algorithms are just the reversed versions of each other. In that way, we are able to reduce the original instance to a smaller instance where the sought-after smaller error vector now only has entries of Lee weights up to a given value r. This reduction yields to a reduction of the cost for the known information set decoding algorithms in the Lee metric.

Smaller Keys for the McEliece Cryptosystem: A convolutional variant with GRS codes

Paulo Almeida
University of Aveiro, Portugal

Joint work with: M. Beltrá, D. Napp, C. Sebastião

We present a new variant of the McEliece cryptosystem that possesses several interesting properties, including a reduction of the public key for a given security level. In contrast to the classical McEliece cryptosystems, where block codes are used, we propose the use of a convolutional encoder to be part of the public key. The secret key is constituted by a Generalized Reed-Solomon code and two Laurent polynomial matrices that contain large parts that are generated completely at random. In this setting the message is a sequence of messages instead of a single block message and the errors are added randomly throughout the sequence. The scheme protection against ISD attacks in the first instants is obtained using codes with distance 1, making list decoding unfeasible. The size of the whole message is adapted such that the full row rank encoder is also protected against ISD attacks. The protection against structural attacks using the square code is also analysed.

Session 2: 10:55 – 12:35

Chair: Henry Chimal-Dzul

CSS-T Codes from Reed-Muller Codes For Quantum Fault-Tolerance

Felice Manganiello
Clemson University, United States of America

Joint work with: Jessalyn Bolkema

Fault-tolerant quantum computation is a critical step in the development of practical quantum computers. Unfortunately, not every quantum error-correcting code can be used for fault-tolerant computation. Rengeswamy et. al. define CSS-T codes, which are CSS codes that admit a physical transversal T-gate. In this talk we give a comprehensive study of CSS-T codes from Reed-Muller codes. These codes allow for the construction of CSS-T code families with non-vanishing asymptotic rate and possibly diverging minimum distance, desirable properties for fault-tolerant quantum computation.

Acknowledgments: This work was partially supported by the National Science Foundation under grant DMS-1547399.

Purity of Free Resolutions of Affine and Projective Reed-Muller Codes

Rati Ludhani
Indian Institute of Technology Bombay, India

Joint work with: Sudhir R. Ghorpade

Following Johnsen and Verdure (2013), we can associate to any linear code C an abstract simplicial complex and in turn, a Stanley-Reisner ring R_C. The ring R_C is a standard graded algebra over a field and its projective dimension is precisely the dimension of C. Thus R_C

admits a graded minimal free resolution and the resulting graded Betti numbers are known to determine the generalized Hamming weights of C. Moreover, the works of Johnsen, Roksvold and Verdure (2016) combined with that of Jurrius and Pellikaan (2009) shows that several classical parameters of a code can be determined by the Betti numbers of the code and its elongations. Thus, explicitly determining the Betti numbers of a code is interesting and useful. However, it is in general, a difficult problem. But this problem becomes easy when the corresponding minimal free resolutions is known to be pure. So we may ask whether the minimal free resolutions of some classical families of codes (or rather, of their Stanley-Reisner rings) are pure. For instance, this is always the case in the case of Reed-Solomon codes.

The question of purity of the minimal free resolution of (generalized or affine) Reed-Muller codes was considered by Ghorpade and Singh (2020). They showed that the resolution is pure in some cases and it is not pure in many other cases. We take up the missing cases and obtain a complete characterization of the purity of graded minimal free resolutions of Stanley-Reisner rings associated to generalized Reed-Muller codes of an arbitrary order. Next, we consider the family of projective Reed-Muller codes, which were introduced by Lachaud (1988) and Sørensen (1991), and have been of considerable interest since then. We shall also give a complete characterization of the purity of minimal free resolutions of projective Reed-Muller codes of an arbitrary order.

Free Resolutions and Generalized Hamming Weights of binary linear codes

Edgar Martínez-Moro
University of Valladolid, Castilla, Spain

Joint work with: I. García-Marco, I. Márquez-Corbella, Y. Pitones

In this work, we explore the relationship between free resolution of some monomial ideals and Generalized Hamming Weights (GHWs) of binary codes. More precisely, we look for a structure smaller than the set of codewords of minimal support that provides us some information about the GHWs. We prove that the first and second generalized Hamming weight of a binary linear code can be computed (by means of a graded free resolution) from a set of monomials associated to a binomial ideal related with the code. Moreover, the remaining weights are bounded by the Betti numbers for that set.

Keywords: Generalized Hamming Weight, Graded free resolution, Second distance, Binary code.

Modeling Sliding Window Decoder Error Propagation Effects for Spatially Coupled LDPC Codes

Daniel Costello
University of Notre Dame, United States of America

Joint work with: Min Zhu, David G. M. Mitchell, Michael Lentmaier

Due to their capacity achieving performance with sliding window decoding (SWD), spatially coupled LDPC (SCLDPC) codes are emerging as candidates for next generation channel coding applications. In this paper we present a general model of SWD of SC-LDPC codes and develop an analysis that allows us to estimate their performance under decoder error propagation conditions that can occur when low latency operation is desired. We also show how the model parameters can be estimated and indicate how the model can be used to predict the performance of code doping techniques used to mitigate the effects of decoder error propagation.

Session 3: 14:00 – 15:40

Chair: Karan Khathuria

Sequential Locally Recoverable Codes for Multiple Erasures from Finite Geometry

Marc Newman
University of St. Gallen, Switzerland

Joint work with: Akram Baghban, Anna-Lena Horlemann, Mehdi Ghiyasvand

A linear locally recoverable code (LRC) with locality r is an $[n, k]$ linear code $\mathcal{C}$ over the field $\mathbb{F}_q$ such that the value of each code symbol can be recovered by accessing the value of at most r other symbols. These codes are capable of simultaneously correcting multiple code symbol erasures using local subsets of symbols and are commonly used for distributed storage systems. They generally come in two flavors: parallel locally recoverable codes and sequential locally recoverable codes (SLRCs); in this work, we focus on the latter. Whereas in the parallel case, erased symbols can only be recovered from the initial unerased symbols, when working sequentially, multiple recursive iterations are possible utilizing recovered code symbols for further recovery.

We provide a method of constructing SLRCs by the application of the code product construction and—in particular—look at this product applied to error correcting codes derived from projective spaces. This lets us define a family of q-ary SLRCs. This construction applied to the projective line provides codes whose parameter sets are (to our knowledge) not previously known and improve the number of recoverable code symbols compared to other known parallel locally recoverable code constructions. Furthermore, we provide bounds on the maximal number of possible recoverable errors which generalize the results in previous work. Additionally, we provide some analysis of possible recovery procedures of these codes.

Update and Repair Efficient Storage Codes with Availability via Finite Projective Planes

Junming Ke
University of Tartu, Estonia

The size of datasets is dramatically increasing nowadays, modern distributed storage systems prefer to keep data with redundancy to prevent data loss. A widely adopted technique is erasure coding, where the distributed storage system takes the data as input and generates additional redundant symbols, namely, parity symbols. Any update of a single data symbol will cause the update of several parity symbols. If data symbols and parity symbols are stored in different racks, the update operations will lead the distributed storage systems to a number of data transmissions between racks. Therefore the update performance of storage codes is becoming a common concern in modern distributed storage systems. In this talk, we will introduce a construction of update-efficient storage codes via finite projective planes, also having a short description and efficient local repair with availability.

Batch Code Properties of the Simplex Code

Ago-Erik Reit
University of Tartu, Estonia

Joint work with: Henk D.L. Hollmann, Karan Khathuria, Vitaly Skachek

Batch codes allow for recovery of data from a distributed storage system without putting too much load on individual servers. A primitive multiset linear batch code is given by a generator matrix G of a linear code such that any multiset of t data symbols can be recovered from t disjoint sets of servers/coded symbols. A functional batch code even allows recovering multisets of linear combinations of data symbols.

The binary k-dimensional simplex code is known to be a $t = 2^{k-1}$-batch code and is conjectured to be a $t = 2^{k-1}$-functional batch code. We will give a simple, constructive proof of a result that is “in between” these two properties. For this we will relate the properties to certain old and new additive problems in finite abelian groups. We will also formulate a conjecture for finite abelian groups generalizing the above mentioned conjecture, which we know how to prove for a special case using the combinatorial Nullstellensatz.

Function computation on reconciled data

Vitaly Skachek
University of Tartu, Estonia

Joint work with: Ivo Kubjas

We consider a task of function computation on the reconciled data, which generalizes a set reconciliation problem in the literature. Assume a distributed data storage system with two users A and B. The users possess a collection of binary vectors S_A and S_B, respectively. They are interested in computing a function ϕ of the reconciled data $S_A \cup S_B$. We show that any deterministic protocol, which computes a sum and a product of reconciled sets of binary vectors represented as nonnegative integers, has to communicate at least $2^n + n - 1$ and $2^n + n - 2$ bits in the worst-case scenario, respectively, where n is the length of the binary vectors. Connections to other problems in computer science are established, yielding a variety of additional upper and lower bounds on the communication complexity.

Session 4: 16:10 – 17:25

Chair: Simran Tinani

NP-Complete Problems in Graph Groups and connection to Post-quantum Cryptography

Delaram Kahrobaei
The City University of New York, United States of America

Joint work with: Ramon Flores and Thomas Koberda

Graph groups admit a presentation where the only relations are commutativity relations which are codified in a finite simplicial graph. The fact that these groups are defined by means of a graph imply that there is a tight connection between algorithmic graph theoretic problems and group theoretic problems for graph groups. Since the graph theoretic problems have been of central importance in Complexity Theory, it is natural to consider some of these graph theoretic problems via their equivalent formulation as group theoretic problems about graph groups. Motivated by the fact that some of these group theoretic problems can be used for cryptographic purposes, such as authentication schemes, secret sharing schemes, zero-knowledge proofs, hash functions and key exchange protocols. Flores-Kahrobaei-Koberda, in a series of recent papers in (1; 2; 3; 4) have considered these groups as a promising platform for several cryptographic schemes.

References

[1] R. Flores, D. Kahrobaei, T. Koberda. Expanders and right-angled Artingroups. In *Journal of Topology and Analysis*, pages 1–25, 2021.

[2] R. Flores, D. Kahrobaei, T. Koberda. Hamiltonicity via cohomology of right-angled Artin groups. In *Linear Algebra and its Applications*, 631: 94–110, 2021.

[3] R. Flores, D. Kahrobaei, T. Koberda. An algebraic characterization of k–colorability. In *The Proceedings of the American Mathematical Society*, 149:2249-2255, 2021.

[4] R. Flores, D. Kahrobaei, T. Koberda. Algorithmic Problems in right-angled Artin groups: Complexity and Applications. In *Journal of Algebra*, 519: 111–129, 2019.

Semidirect product key exchange: the state of play

Christopher Battarbee
The City University of New York, United States of America

Joint work with: Delaram Kahrobaei, Siamak F. Shahandashti

In this report we survey the various proposals of the key exchange protocol known as semidirect product key exchange (SDPKE), a generalisation of the famous Diffie-Hellman key exchange believed to be post-quantum. We discuss the various platforms proposed and give an overview of the main cryptanalytic ideas relevant to each scheme, including: matrices over group rings, p-groups of high-dimensional representation, tropical algebras, finite-field entry matrix semigroups, and Boolean algebras. Moreover, we present these ideas chronologically in order to motivate the choice of platform as informed by cryptanalytic work in the area.

Higher dimensional platforms for Tillich-Zéemor hash functions

Corentin Le Coz
Technion, Israel

Joint work with: Christopher Battarbee, Ramón Flores, Thomas Koberda and Delaram Kahrobaei

Group theoretic hash functions are obtained by performing a non backtracking walk in a graph coming from a group. Since the first example by Zéemor in 1991, it has been an active field of research. During my talk, I will introduce the theoretic background of these hash functions, and discuss current existing platforms and attacks. Then, I will speak about a recent joint work with Christopher Battarbee, Ramón Flores, Thomas Koberda and Delaram Kahrobaei. We have constructed hash functions using as platforms higher

dimensional special linear groups over finite fields. This gives many examples of group theoretic hash functions combining quick mixing properties and high girth, which give rise to good preimage and collision resistance.

Friday, July 15, 2022

Session 1: 08:45 – 10:25

Chair: Violetta Weger

Error Correcting Codes in a Frobenius Algebra Ambient

Erik Hieta-aho
Aalto University, Finland

Joint work with: José Gómez-Torrecillas, Javier Lobillo, Sergio R. López-Permouth, Gabriel Navarro

Cyclic codes are among the most studied error-correcting codes. Negacyclic, constacyclic and polycyclic codes are systematic generalizations of cyclic codes. Their underlying common feature is that they can be considered as ideals of certain rings (their Ambient ring.) Cyclic and negacyclic codes share the appealing property that the dual of a cyclic (negacyclic) code is also cyclic (negacyclic) code; in fact the duals are ideals of the same ambient ring. On the other hand, while Constacyclic codes still satisfy that their duals are of the same type, a constacyclic code and its dual are not necessarily ideals of the same ambient ring. The relationship between such pairs of ambient rings has recently been explored in (2). Noting the fact that the duals of polycyclic codes are not polycyclic (3) and observing the alternative of using annihilators in lieu of dual codes proposed and studied in (1) suggests an alternative approach. We extend the results in (1) by assuming only that the ambient ring is a Frobenius algebra. While Frobenius rings in general satisfy the double annihilator condition and that makes it so that an ideal is completely determined by its annihilator, we have only been successful so far in the context of a Frobenius algebra where the additional structure has allowed us to construct an appropriate balanced non-degenerate bilinear form. We have also managed to obtain analogues to the MacWilliams identities in this setting.

References

[1] A. Alahmadi, S. Dougherty, A. Leroy, and P. Solé, On the Duality and the direction of polycyclic codes. In *A*dvances in Mathematics of Communications,10:923-931, 2016.

[2] J. Gómez-Torrecillas, F.J. Lobillo, and G. Navarro. Dual Skew Codes from Annihilators: Transpose Hamming ring extensions. 2017.

[3] S.R. López-Permouth, B.R. Parra-Avila, and S. Szabo. Dual generalizations of the concept of cyclicity of codes. In *Advances in Mathematics of Communications* 3:227-234, 2009.

Multi-twisted additive codes over finite fields

Sandeep Sharma
Indraprastha Institute of Information Technology Delhi, India

Additive codes over the finite field $\mathbb{F}_4$ were introduced and studied by Calderbank *et al.* (1998) as a natural generalization of linear codes. Later, Rains (1999) and Bierbrauer and Edel (2000) defined and studied additive codes over arbitrary finite fields. These codes not only constitute an important family of error-correcting codes, but are also useful in the construction of quantum error-correcting codes. In this talk, we will introduce a new class of additive codes over finite fields, *viz.* multi-twisted (MT) additive codes. We will study their algebraic structures by writing a canonical form decomposition for these codes and provide an enumeration formula for these codes. By placing ordinary, Hermitian and $\star$ trace bilinear forms, we will further study their dual codes and derive necessary and sufficient conditions under which a MT additive code is self-dual, self-orthogonal and MT additive codes with complementary dual. We will also derive a necessary and sufficient condition for the existence of a self-dual MT additive code over a finite field, and provide explicit enumeration formulae for self-dual, self-orthogonal and MT additive complementary dual codes over finite fields with respect to the aforementioned trace bilinear forms. We will also discuss some interesting open problems in this direction.

Enumeration formulae for self-orthogonal, self-dual and LCD codes over finite commutative chain rings

Monika Yadav
Indraprastha Institute of Information Technology Delhi, India

Self-orthogonal, self-dual and linear with complementary dual (LCD) codes constitute the three most important and well-studied classes of linear codes having rich algebraic structures. Self-orthogonal and self-dual codes have nice connections with the theory of modular forms and unimodular lattices, and LCD codes have several applications in cryptography, consumer electronics and data storage. In this talk, we will present explicit enumeration formulae for self-orthogonal, self-dual and LCD codes of an arbitrary length over finite commutative chain rings. These enumeration formulae are useful in classifying these three classes of linear codes over finite commutative chain rings up to equivalence. By applying the classification algorithm and using these enumeration formulae, we will classify all self-orthogonal, self-dual and LCD codes of particular lengths over certain special chain rings. Besides this, we will show that the class of LCD codes over finite commutative chain rings is asymptotically good, and that every free linear $[n, k, d]$-code over a finite commutative chain ring is equivalent to an LCD $[n, k, d]$-code over finite commutative chain ring.

MacWilliams extending conditions and quasi-Frobenius rings

Ashish Srivastava
Saint Louis University, United States of America

Joint work with: Pedro A. Guil Asensio

MacWilliams proved that every finite field has the extension property for Hamming weight which was later extended in a seminal work by Wood who characterized finite Frobenius rings as precisely those rings which satisfy the MacWilliams extension property. We address the question of when is a MacWilliams ring quasi-Frobenius? We prove that a right Artinian left 1-MacWilliams ring is quasi-Frobenius thus answering a question asked by Schneider and Zumbrägel.

Session 2: 10:55 – 12:35

Chair: Anna-Lena Horlemann

Open Problems on Subspace Codes and Designs

Tuvi Etzion
Technion, Israel

Subspace codes and designs were motivated by their application to error-correction in random network coding. We will present in this talk some of the more fascinating open problems in this area as well as some directions for their solutions.

New 2-designs in polar spaces

Alfred Wassermann
University of Bayreuth, Germany

Joint work with: Michael Kiermaier

Combinatorial designs have been studied since nearly 200 years and have many applications in coding theory, e.g. for majority-logic decoding. 50 years ago, Cameron, Delsarte and Ray-Chaudhury introduced subspace designs, also known as q-analogs of designs or designs over finite fields, which recently gained a renewed interest because of their connections to random network coding.

A next natural generalization of subspace designs are designs in finite classical polar spaces. The first non-trivial such designs for $t > 1$ were found by De Bruyn and Vanhove in 2012, some more designs appeared recently in the PhD thesis of Lansdown.

In this talk we will give an overview on the subject and present new parameters of designs in polar spaces found by computer search.

Sphere Packing Lower Bounds: New Developments

Vlad Serban
EPFL, Switzerland

Joint work with: N. Gargava

The search for dense sphere packings in high dimensional Euclidean space is an intriguing quest for structure that strongly relates to optimization problems in coding theory. We show how by lifting suitable codes from prime characteristic to orders $\mathcal{O}$ in $\mathbb{Q}$-division rings and by exploiting the additional symmetries under finite subgroups of $\mathcal{O}^{\times}$, lattices approaching or exceeding the best known effective lower bounds on the packing density Δ_n can be obtained. This joint work with N. Gargava unifies and extends a number of previous constructions.

Explicit constructions of asymptotically good minimal linear codes from graphs

Alessandro Neri
Max Planck Institute for Mathematics in the Sciences, Germany

Joint work with: A. Bishnoi and S. Das

Minimal linear codes were first introduced by Cohen and Lempel over the binary field under the name of *linear intersecting codes* (2). They later gained interest due to their application to secret sharing schemes proposed by Massey (4). Recently, it has been shown that k-dimensional minimal linear codes in $\mathbb{F}_q^n$ are in one-to-one correspondence with strong blocking sets (1; 5), which are special sets of n points in $\mathrm{PG}(k-1, q)$, such that their intersection with each hyperplane generates the hyperplane itself. The notion of strong blocking set was however already known, since they were originally introduced as a tool for deriving covering codes (3).

In this talk we propose a new general method to construct small strong blocking sets – and hence short minimal linear codes – starting from a set of points in $\mathrm{PG}(k-1, q)$ and a graph with special connectivity properties. In particular, we explore how one can get explicit constructions of families of asymptotically good minimal linear codes, by means of expander graphs and families of asymptotically good linear codes.

Keywords: Minimal linear codes, asymptotically good codes, strong blocking sets, expander graphs

References

[1] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Adv. in Math. Commun.*, 2020.

[2] G. Cohen and A. Lempel. Linear intersecting codes. *Discrete Math.*, 56(1):35–43, 1985.

[3] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Adv. in Math. Commun.*, 5(1):119–147, 2011.

[4] J. L. Massey. Minimal codewords and secret sharing. *In Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[5] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Trans. Inform. Theory*, 67(6):3690–3700, 2021.

Session 3: 14:00 – 15:40

Chair: Alessandro Neri

Linear Codes associated to Flag Varieties over Finite Fields

Sudhir R. Ghorpade
Indian Institute of Technology Bombay, India

Joint work with: Fernando Piñero and Prasant Singh

The study of Grassmann codes goes back to Ryan (1987) and it has been of considerable interest in the past three decades. These are linear codes associated to the $\mathbb{F}_q$-rational points of the Grassmann variety $G_\ell(V)$ of ℓ-dimensional subspaces of an m-dimensional vector space V, together with its nondegenerate Plücker embedding in $\mathbb{P}\left(\wedge^\ell V\right)$. It is known that Grassmann codes possess several remarkable properties. Flag varieties are a natural generalization of Grassmann varieties and they may be defined as follows. Let $\underline{\ell} = (\ell_1, \ell_2 \ldots, \ell_s)$ be a sequence of positive integers satisfying $\ell_1 \leq \ell_2 \leq \ldots \leq \ell_s < m$. The corresponding s-step flag variety $\mathcal{F}_{\underline{\ell}}(V)$ consists of ordered tuples $(V_1, \ldots, V_s)$ of subspaces of V such that $V_1 \subseteq V_2 \subseteq \ldots \subseteq V_s$ and $\dim V_i = \ell_i$ for $i = 1, \ldots, s$. We can embed $\mathcal{F}_{\underline{\ell}}(V)$ in a large projective space by considering the product of Plücker projective spaces $\mathbb{P}\left(\wedge^{\ell_i} V\right)$ followed by a Segre embedding. We denote the linear code corresponding to the $\mathbb{F}_q$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$ by $C(\underline{\ell}; m)$ and refer to these as (s-step) flag codes. The study of these codes was initiated by Rodier (2003) who determined the length, the dimension and the minimum distance in the special case when $s = 2$ and $\underline{\ell} = (1, m-1)$. This was continued by Hana (2010) who gave a formula for the length of $C(\underline{\ell}; m)$ and also upper bounds for the dimension and the minimum distance of $C(\underline{\ell}; m)$.

We shall outline an exact formula for the dimension of 2-step flag codes. Further, we show that the upper bound given by Hana for the minimum distance of 2 -step flag codes is attained in several cases. This includes, in particular the case studied by Rodier. We shall also indicate how a general formula for the dimension of arbitrary flag codes can be obtained using a connection with representation theory. This is a joint work with Fernando Piñero and Prasant Singh.

Cyclic orbit flag codes

Miguel-Ángel Navarro-Pérez
Centro Universitario EDEM Escuela de Empresarios, Spain

Joint work with: C. Alonso-González

A flag code is a nonempty collection of flags, i.e, sequences of nested subspaces of $\mathbb{F}_q^n$, with F_q the finite field with q elements. In the network coding setting, these codes were introduced in [3] as a generalization of constant dimension codes. When flag codes are constructed as orbits of (cyclic) subgroups of the general linear group, we speak about *(cyclic) orbit flag codes*. Following the ideas in [2], in this talk we present a study on the parameters and properties of cyclic orbit flag codes by taking into account their *best friend*, that is, the largest subfield over which all the subspaces in the generating flag are vector spaces. We finish the talk by studying two specific families of cyclic orbit flag codes: the one of *Galois cyclic orbit flag codes* and the one of *optimum distance cyclic orbit flag codes*.

References

[1] C. Alonso-González and M.A. Navarro-Pérez, "Cyclic Orbit Flag Codes", Designs, Codes and Cryptography, Vol. 89 (2021), 2331–2356.

[2] H. Gluesing-Luerssen, K. Morrison and C. Troha, "Cyclic Orbit Codes and Stabilizer Subfields", Advances in Mathematics of Communications, 9 (2015), 2, 177-197.

[3] D. Liebhold, G. Nebe and A. Vázquez-Castro, "Network Coding with Flags", Designs, Codes and Cryptography, Vol. 86 (2) (2018) 269-284.

Higher Grassmann Codes

Mahir Bilen Can
Tulane University, United States of America

Joint work with: Roy Joshua, Ravindra Girivaru

The Grassmann codes were originally introduced by Charles Ryan around 1987. The projective Reed-Müller codes are important examples of such algebraic geometric codes. In 1990, Gilles Lachaud computed the parameters of projective Reed-Müller codes under certain bounds on the degrees. In 1996, Dimitrii Yu. Nogin computed the parameters of the Grassmann codes only for the Plücker embeddings. These works motivated so many other important advances in the studies of algebraic geometric codes. In our talk, we will discuss not just the Plücker embeddings, but ALL projective space embeddings of the Grassmann varieties; we will present our results concerning the parameters of all such codes. It turns out that these new codes, which we call the higher Grassmann codes, have better efficiencies compared to the classical Grassmann codes.

Minimum Weight Codewords of Schubert Codes

Avijit Panja
Indian Institute of Technology Bombay, India

Joint work with: Mrinmoy Datta, Sudhir R. Ghorpade

Schubert codes are linear codes associated to the Fq-rational points of Schubert varieties in Grassmannians. These were introduced by Ghorpade and Lachaud around the turn of the last century. A conjecture about the minimum distance of these codes remained open for almost a decade and was eventually proved in the affirmative by Xiang (2008). An alternative proof was given by Ghorpade and Singh (2018) who further analyzed the structure of the minimum weight codewords of Schubert codes. They proposed a conjecture that gives a characterization of the minimum weight codewords of Schubert codes by relating them to the so called "Schubert decomposable" elements in certain exterior powers. In the case when the the Schubert variety is the full Grassmannian, the conjectural characterization is a consequence of a result of Nogin (1996), However, the general case is still open.

We show that this conjecture of Ghorpade and Singh holds in the armative in the case of Schubert divisors, i.e., when the codimension of the Schubert variety in the Grassmannian is 1. We also establish that the conjecture holds in the armative in several other special cases. Further, assuming the validity of the conjecture of Ghorpade and Singh, we give a complete description of Schubert codes that are generated by their minimum weight codewords.

Session 4: 16:10 – 17:25

Chair: Jessica Bariffi

SPANSE: combining sparsity with density for efficient one-time code-based digital signatures

Marco Baldi
Università Politecnica delle Marche, Italy

Joint work with: Franco Chiaraluce and Paolo Santini

The use of codes defined by sparse characteristic matrices, like QC-LDPC and QC-MDPC codes, has become an established solution to design secure and efficient code-based public-key encryption schemes, as also witnessed by the ongoing NIST post-quantum cryptography standardization process. However, similar approaches have been less fortunate in the context of code-based digital signatures, since no secure and efficient signature scheme based on these codes is available to date. The main limitation of previous attempts in this line of research has been the use of sparse signatures, which produces some leakage of information about the private key. In this paper, we propose a new code-based digital signature scheme that overcomes such a problem by publishing signatures that are abnormally dense, rather than sparse. This eliminates the possibility of deducing information from the sparsity of signatures, and follows a recent trend in code-based cryptography exploiting the hardness of the decoding problem for large-weight vectors, instead of its classical version based on small-weight vectors. In this study we focus on one-time use and provide some preliminary instances of the new scheme, showing that it achieves very fast signature generation and verification with reasonably small public keys.

Algebraic Connections Between Absorbing Sets and Cosets

Emily McMillon
University of Nebraska-Lincoln, United States of America

Absorbing sets are combinatorial structures in a code's Tanner graph that have been shown to characterize iterative decoder failure of LDPC codes. In this talk, we will consider the connection between the properties of an absorbing set and the location of the absorbing set's support vector within the code's standard array. In particular, we explore the connection between subspace translates of a code and absorbing set support vectors, and we consider how redundancy in the parity check matrix affects the presence and location of absorbing sets within the standard array.

Network Decoding Against Restricted Adversaries

Altan Kılıç
Eindhoven University of Technology, The Netherlands

Joint work with: Allison Beemer and Alberto Ravagnani

We focus on the one-shot capacity of communication networks with an adversary having access only to a proper subset of network edges. The one-shot capacity measures the maximum number of symbols that can be sent in a single transmission round regardless of the action of the adversary. We provide a method to obtain a unique two-level network from any given network, and show that the one-shot capacity of the original network is upper bounded by the one-shot capacity of the induced two-level network. We then study two-level networks in detail and show that known cut-set bounds are not sharp, where the non-sharpness comes precisely from the fact that the adversary needs to operate on a proper subset of the network edges.

Speaker Index