ALGEBRAIC CODING THEORY AND APPLICATIONS DOUBLE INVITED SESSION PROPOSAL MTNS 2024

JULIA LIEB AND CARLOS VELA

Introduction

In mathematics, coding theory plays the main role in designing error-resistant codes, allowing secure and accurate data transmission in telecommunications. Moreover, codes are used to repair failures inside digital storage systems as well as to build post-quantum cryptographic schemes. In the theory of error-correcting codes, there exists three main currents of work: block codes, convolutional codes and subspace codes.

The classical type of codes to correct errors during data transmission via some communication channel have been linear block codes. An (n, k) linear block code $\mathcal{C}$ is defined as a k dimensional subspace of the vector space $\mathbb{F}_q^n$ over some finite field $\mathbb{F}_q$. The parameter n is called the length of the code. Hence, there exists a matrix $G \in \mathbb{F}_q^{k\times n}$, called generator matrix of $\mathcal{C}$, such that $\mathcal{C} = \{uG,\ u \in \mathbb{F}_q^k\}$.

Convolutional codes are a generalization of linear block codes to the polynomial setting. An (n, k) convolutional code is defined as a $\mathbb{F}_q[z]$-submodule with rank k of the module $\mathbb{F}_q[z]^n$. Thus, for an (n, k) convolutional code $\mathcal{C}$, there exists some polynomial generator matrix $G(z) \in \mathbb{F}_q[z]^{k\times n}$ such that $\mathcal{C} = \{u(z)G(z),\ u(z) \in \mathbb{F}_q[z]^k\}$. As the codewords of a convolutional code can be obtained via polynomial multiplication, they possess a convolutional structure, which makes them very suitable for sequential encoding and decoding. Consequently, they are very useful for application in streaming systems where the acceptable delay is rather tight. Since the codewords of a convolutional code are polynomial vectors, they possess a third code parameter called the degree δ of the code. It is defined as the largest degree of all the full-size minors of any generator matrix $G(z)$ of $\mathcal{C}$. One then speaks of an (n, k, δ) convolutional code. A convolutional code of degree $\delta = 0$ is nothing else than a linear block code.

Subspace codes are defined as sets of subsets of $\mathbb{F}_q^n$. In this approach, the codewords of the subspace code are themselves subspaces. This family serves as an efficient means to represent and transmit information reliably. Essentially, instead of individual vectors, the subspace code encodes information using entire subspaces, providing a framework for robust data transmission and storage in various applications, like e.g. network coding.

The space in which a code is constructed is endowed with a metric that gives us a weight $(wt(\cdot))$ for the codewords and distances between them and thus allows us to define the minimum distance of a code, which is a measure for the number of errors this code can correct. For linear codes this minimum distance is equal to $d_{min}(\mathcal{C}) = \min\{wt(v)|v \in \mathcal{C}, v \neq 0\}$. In classical coding theory the Hamming distance is used, that is, the amount of elements in which two codewords differ. Nevertheless, coding theory has been developed by using other metrics such as

subspace distance, Rank distance, Lee distance or chinese euclidean distance. For the last two of these distances, one considers $\mathbb{Z}_p^n$ instead of $\mathbb{F}_q^n$ as ambient space, i.e. one is working over finite rings instead of finite fields.

For convolutional codes, such distance measures can be extended via $wt(v(z)) = \sum_{t=0}^{\deg(v(z))} wt(v_t)$ for the polynomial $v(z) = \sum_{t=0}^{\deg(v(z))} v_t z^t \in \mathbb{F}_q^n[z]$. Moreover, for these codes, one has two main distance measures, namely the free distance $d_{free}(\mathcal{C}) = \min\{wt(v(z))|v(z) \in \mathcal{C}, v(z) \neq 0\}$ and the j-th column distance $d_j^c(\mathcal{C}) := \min\left\{wt(v_{[0,j]}(z)) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq \mathbf{0}\right\}$ where $v_{[0,j]}(z) = v_0 + v_1 z + \cdots + v_j z^j$ for $j \in \mathbb{N}_0$. The second is used if one wants to measure just the number of errors that can be corrected with time-delay j.

When constructing codes it is desirable to do it in an optimal way depending on what feature we want to explode. There exist different bounds for different features, some of them (among many other bounds) are the (generalised) Singleton bound for the minimum distance or the Gilbert-Varshamov and Sphere-packing bounds for the amount of codewords in a code. From the error-correcting capacity point of view, codes that hold bounds on distances are of special interest. Those which have maximum free or minimum distance are called Maximum Distance Separable (MDS) and those which achieve the maximum possible column distances are named Maximum Distance Profile (MDP).

An important value that is related with the amount of codewords in a code, as well as the Gilbert-Varshamov and Sphere-packing bounds previously mentioned, is the covering radius, that is, the minimum natural number r such that every element of the space is contained in at least one ball of radius r centered at each codeword of the code. This value gives an idea on how the elements of the code are spread over the space.

Coding theory has various relations to algebra and combinatorics. For the construction of good codes, amongst others, finite geometry and design theory as well as group theory have been used. This is in particular true for LDPC codes, which are defined as codes where $\mathcal{C} = \{v \in \mathbb{F}_q^n \mid Hv^\top = 0\}$ with a sparse matrix $H \in \mathbb{F}_q^{(n-k)\times n}$. In a similar way also LDPC convolutional codes can be defined. These codes became important for applications, for error-correction as well as for the development of code-based cryptosystems, as they come with efficient decoding algorithms, like the bit-flipping algorithm.

Invited speakers

In this section we present the titles and abstracts of the proposed talks.

1. Convolutional erasure codes with simplex locality

Margreta Kuijper
The University of Melbourne

Abstract: This work provides a continuation of earlier work on simplex distributed storage block codes over extension fields, presented at MTNS 2014. Instead of a block code we construct a convolutional code with simplex properties and present its easy repair properties for the distributed storage setting. We show how to use a sliding window decoder to do the actual easy repair.

2. Repair schemes using Reed-Muller and Hermitian codes

Hiram López Valdez
Virginia Polytechnic Institute and State University (Virginia Tech)

Abstract: A distributed storage system stores data files over multiple storage nodes. Ideally, the system is set up so if one node fails, the information on that node can be recovered with the information stored on the remaining nodes. An exact repair scheme recovers the info of a failed node by downloading a few pieces of information from the rest of the nodes. In this talk, we describe how to develop exact repair schemes using Reed-Muller and Hermitian codes.

3. Results on b-symbol weights of some codes

Ferruh Özbudak
Sabanci University

Abstract: We explain some details on some recent results on b-symbol weight of codes. This involves some techniques from coding theory, exponential sums and finite geometry.

4. Pseudo-MDP convolutional codes

Raquel Pinto
University of Aveiro

Abstract: In this talk we are going to consider a new construction of convolutional codes and analyze their erasure correction capability. MDP convolutional codes have optimal correction capacity for erasure channels. However, there are not many constructions of MDP convolutional codes and the existing ones consider a large field. We will construct new codes by considering an encoder of an MDP convolutional code and repeating the (matrix) coefficients of the encoder in a certain order. The resulting code is not MDP but its erasure correction capacity will be very near the optimal one for convolutional codes with the same parameters.

This work is in collaboration with Zita Abreu, Julia Lieb and Rita Simões.

5. Spread codes arising from Abelian non-cyclic groups

Verónica Requena
University of Alicante

Abstract: In this talk we present a way of constructing spreads of $\mathbb{F}_q^n$. They will arise as orbits under the action of an Abelian non-cyclic group. First we construct a family of orbit codes of maximum distance using this group and then we complete each of these codes to achieve a spread of the whole space having an orbital structure.

6. MDPC Convolutional Codes having a Quasi-Cyclic structure

Joachim Rosenthal
University of Zurich

Abstract: LDPC convolutional codes have been studied by several authors for about 15 years. They naturally generalize LDPC block codes and they also can be decoded very efficiently.

In the area of code based cryptography Moderate Density Parity Check (MDPC) Codes received prominence, in particular when these codes have also a quasi-cyclic structure as this allows one to keep the public key of the associated crypto system relatively small.

In this paper we will study under what circumstances MDPC convolutional codes can be decoded efficiently.

7. Flag codes generated from constant dimension codes

Xaro Soler
University of Alicante

Abstract: Given a finite field $\mathbb{F}_q$ and a positive integer n, a flag is a sequence of nested $\mathbb{F}_q$-subspaces of a vector space $\mathbb{F}_q^n$ and a flag code is a nonempty collection of flags. Flag codes were introduced in 2018 and, since then, several works have deepened the study of these codes and provided different constructions of them. The list of dimensions of the subspaces in a flag is called its type vector. Constant dimension codes and flag codes are closely related by the notion of projected codes. For each dimension in the type vector of a flag code C, we consider the constant dimension code composed by all the subspaces of this dimension appearing in some flag in C. This list of constant dimension codes is the set of projected codes associated to the flag code C. In this talk we explore the opposite path: we study under which conditions a family of constant dimension codes produces flag codes. In that situation, we realise that different flag codes can come from the same family of constant dimension codes. Then we give a method to obtain the largest flag code generated by a family of constant dimension codes and we determine in which cases such a family gives exactly one flag code. These notions will be crucial to properly connect the (semi)linear equivalence of flag codes with the (semi)linear equivalence of their projected codes. In addition, this study leads to new results concerning the automorphism group of certain families of flag codes.

8. Hadamard matrices and spherical designs

Patrick Solè
Aix-Marseille University

Abstract: Hadamard codes over finite rings are explored wrt their covering radius for the chinese euclidean distance. Generalized bent sequences, when they exist, provide a lower bound. Upper bounds are obtained by considering a spherical code attached to Hadamard matrices of Butson type. Under mild hypotheses, this code is a spherical 2-design, which yields upper bound on its covering radius on the sphere. This bound, in turn, gives an upper bound on the covering radius of the Hadamard codes.

Based on joint work with Minjia Shi, Danni Lu, A. Armario, R. Egan, Ferruh Özbudak.