ACT21 Graduate Minisymposium

Wednesday, June 9th

15:00-15:25	Benjamin Jany
15:25-15:50	Giuseppe Cotardo
15:50-16:00	Break
16:00-16:25	Paolo Santonastaso
16:25-16:50	Miguel Ángel Navarro-Pérez
16:50-17:00	Break
17:00-17:25	Jessica Bariffi
17:25-17:50	Anina Gruica
17:50-18:30	Get together on Wonder

The time indicated in the schedule is referred to **Central European Summer Time (CEST)**

15.00 **Benjamin Jany**, University of Kentucky

Rank metric code invariants: a q-polymatroid approach

In recent years, understanding algebraic and combinatorial invariants of rank metric codes (subspaces of $\mathbb{F}_q^{n\times m}$ along with the rank metric) has been of interest in coding theory due to their application to error-correcting codes for linear networks. It was found that one can associate a q-polymatroid to a rank metric code and "extract" some of the algebraic and combinatorial structure of the code. In this talk I will define q-polymatroids and show how to determine code-invariants, such as the rank distance or the generalized weights, directly from the q-polymatroid.

15.25 **Giuseppe Cotardo**, University College Dublin

Bilinear Complexity of 3-tensors Linked to Coding Theory

A well studied problem in algebraic complexity theory is the determinination in the non-scalar model of the complexity of a problem relying on evaluation of bilinear maps. The non-scalar complexity of an algorithm is the minimum number of non-scalar operations required to execute it. The bilinear complexity of a 3-tensor, which is a bilinear map, is its complexity in this non-scalar model. This is the same as its tensor rank, which is the minimum number of rank-one matrices whose span contains its first slice space. In 1989, Håstad showed that computing the bilinear complexity of a 3-tensor over a finite field is NP-complete and is NP-hard if the tensor is over the rationals. In this talk, we present upper bounds on the tensor rank of certain classes of 3-tensors and give explicit constructions of sets of rank-one matrices containing their first slice spaces. We then show how these results can be applied in coding theory to derive upper bounds on the tensor rank of some rank-metric codes. In particular, we compute the tensor rank of a family of codes corresponding to a particular 3-tensor and show that its members are extremal with respect to Kruskal's tensor rank bound.

15.50 Break

16.00 **Paolo Santonastaso**, University of Campania

On the list decodability of rank-metric codes

Let q be a prime power. A *code* C is a subset of $\mathbb{F}_q^n$ endowed with a metric on $\mathbb{F}_q^n$. A *list decoding algorithm* for C permits to find all codewords in a ball of a certain radius τ centered in a received word $\mathbf{y}$. Consequently, we say that C is *efficiently τ-list decodable*, if there exists a polynomial-time list decoding algorithm at the radius

τ. The problem of determining whether or not a code equipped with the Hamming metric is (efficiently) list-decodable is intesively studied in the Hamming metric. The problem of list decoding recently attracted a lot of attention for rank-metric codes. Wachter-Zeh in [3] proved that Gabidulin codes in $\mathbb{F}_{q^m}^n$ with minimum distance d cannot be efficiently list decoded at any radius τ such that

$$\tau \geq \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{2} - m(d-\epsilon)}, \qquad (1)$$

where $0 \leq \epsilon < 1$. Watcher-Zeh and Raviv in [1] improved these results showing infinite families of Gabidulin codes which are not efficiently list decodable *at all*. Based on the hardness of list decoding problem for Gabidulin codes, a new cryptosystem, known as LIGA, arises. However, the list decoding of other rank-metric codes still requires further investigations. In this talk we will investigate results on the list decoding of rank-metric codes containing a Gabidulin code, based on [2].

[1] N. Raviv, A. Wachter-Zeh: Some Gabidulin codes cannot be list decoded efficiently at any radius, *IEEE Trans. Inform. Theory* **62(4)** (2016), 1605–1615.

[2] P. Santonastaso and F. Zullo: On the list decodability of rank-metric codes containing Gabidulin codes, arXiv:2103.07547.

[3] A. Wachter-Zeh: Bounds on list decoding of rank-metric codes. *IEEE Trans. Inform. Theory* **59(11)** (2013), 7268–7276.

16.25 **Miguel Ángel Navarro-Pérez**, University of Alicante

An orbital construction of optimum distance Flag codes

In this talk we present a construction of optimum distance full flag code on $\mathbb{F}_q^{2k}$, by using the action of a specific subgroup of the general linear group. We start from a known orbit (subspace) code of dimension k with maximum distance and provide sufficient conditions to extend its orbital structure to full flags, obtaining a flag code with maximum distance and also the largest possible size.

16.50 Break

17.00 **Jessica Bariffi**, German Aerospace Center (DLR) and University of Zurich

Analysis of Low-Density Parity-Check Codes over Finite Integer Rings for the Lee Channel

We study the performance of low-density parity-check (LDPC) codes over finite integer rings, over two channels that arise from the Lee metric. The first channel is a discrete memory-less channel (DMC) matched to the Lee metric. The second channel adds to each codeword an error vector of constant Lee weight, where the error vector is picked uniformly at random from the set of vectors of constant Lee weight. It is shown that the marginal conditional distribution of the two channels coincides, in the limit of large blocklengths. The performance of selected LDPC code ensembles is analyzed by means of density evolution and finite-length simulations, with belief propagation decoding and with a low-complexity symbol message passing algorithm.

17.25 **Anina Gruica**, Technical University of Eindhoven

Codes with good distance properties from a density perspective

In this talk I will discuss the problem of estimating the number of codes with given cardinality and minimum distance bounded from below. I will focus on block codes with the Hamming metric, rank-metric codes and subspace codes with the injection metric. The bounds on these codes are derived from studying isolated vertices in bipartite graphs. From the bounds obtained using this method I will then be able to say what the typical code over a large finite field looks like, and in particular, whether or not it is optimal. When discussing the results on subspace codes with the injection metric, I will show an application to the theory of partial spreads in finite geometry.

17.50 Get together on Wonder