Finite Fields in Discrete Mathematics - Part II
(Org: **Petr Lisonek** (Simon Fraser University) and/et **Daniel Panario** (Carleton University))

DANIEL KATZ, California State University, Northridge
Nonvanishing minors and uncertainty principles for Fourier analysis over finite fields

Chebotarëv's theorem on roots of unity says that every minor of a discrete Fourier transform matrix of prime order is nonzero. We present a generalization of this result that includes analogues for discrete cosine and discrete sine transform matrices as special cases. This leads to a generalization of the Biró-Meshulam-Tao uncertainty principle to functions with symmetries that arise from certain group actions, with some of the simplest examples being even and odd functions. This new uncertainty principle gives a bound that is sharp and, for some classes of functions, stronger than that of Biró-Meshulam-Tao.

PETR LISONEK, Simon Fraser University
Maximally non-associative quasigroups

A quasigroup $(Q, *)$ is an algebraic structure whose multiplication table is a Latin square. We say that $(x, y, z) \in Q^3$ is an associative triple if $(x * y) * z = x * (y * z)$. Let $a(Q)$ denote the number of associative triples in Q. One shows easily that $a(Q) \geq |Q|$, and it was conjectured that $a(Q) = |Q|$ never occurs for $|Q| > 1$. When q is an odd prime power, we give a non-constructive proof of existence of quasigroup Q with $a(Q) = |Q| = q^2$. Our main tools are Dickson nearfields and Weil bound for character sums. This is joint work with Aleš Drápal (Charles University, Prague).

ARIANE MASUDA, City University of New York
Functional Graphs of Rédei Functions

Let $\mathbb{F}_q$ be a finite field of order q and $f : \mathbb{F}_q \to \mathbb{F}_q$ be a mapping. The functional graph associated to f is a directed graph where the vertices are labelled by the elements of $\mathbb{F}_q$ and an edge connects a to $f(a)$ for every $a \in \mathbb{F}_q$. In this talk we discuss the structure of the functional graph of a Rédei function $R_n(x, a)$ over $\mathbb{F}_q$ where $n \in \mathbb{N}$ and $a \in \mathbb{F}_q$. We show conditions for such graphs to be isomorphic for a fixed q, and present families of isomorphic graphs. This is joint work with Juliane Capaverde and Virgínia Rodrigues.

SIHEM MESNAGER, University of Paris VIII
On good polynomials over finite fields for optimal locally recoverable codes

A locally recoverable (LRC) code is a code that enables a simple recovery of an erased symbol by accessing only a small number of other symbols. LRC codes form one of the rapidly developing topics in coding theory because of their applications in distributed and cloud storage systems. Tamo and Barg have presented a family of LRC codes that attain the maximum possible distance. The key ingredient for constructing such optimal LRC codes is the so-called r-good polynomials, where r is the locality of the LRC code. In this talk, we discuss new good polynomials for constructing optimal LRC codes.

LUCAS REIS, University of Sao Paulo
Permutations of finite sets from an arithmetic setting

Let $n, m > 1$ be integers with $\gcd(n, m^2) = m$. We introduce the concept of (n, m)-*piecewise affine permutations*. These are permutations of the finite set

$$[1, n] := \{1, \ldots, n\},$$

defined by m affine-like rules with some generic arithmetic properties. We discuss the existence and number of these permutations. Our main result provides an explicit description on the *cycle decomposition* of such permutations. As a main application,

we obtain (new?) classes of permutation polynomials of finite fields whose cycle decomposition can be explicitly given. We further discuss algebraic properties of these permutation polynomials, including their *weight* and *index*.