Finite Fields in Discrete Mathematics - Part I

(Org: **Petr Lisonek** (Simon Fraser University) and/et **Daniel Panario** (Carleton University))

DANIELE BARTOLI, University of Perugia

More on exceptional scattered polynomials

Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$. If the $\mathbb{F}_q$-subspace $U = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\}$ defines a maximum scattered linear set, then we call f a scattered polynomial of index t. We say a function f is an exceptional scattered polynomial of index t if the subspace U associated with f defines a maximum scattered linear set in $PG(1, q^{mn})$ for infinitely many m. Exceptional scattered monic polynomials of index 0 (for $q > 5$) and of index 1 have been alrady classified (Bartoli-Zhou, Exceptional scattered polynomials, J. Algebra 2018). In this work, we investigate the case $t \geq 2$.

ANNE CANTEAUT, Inria Paris

Searching for APN permutations with the butterfly construction

The existence of APN permutations operating on an even number of variables was a long-standing open problem, until an example with six variables was exhibited by Dillon et al. in 2009. However it is still unknown whether this example can be generalized to any even number of inputs. This talk investigates the cryptographic properties of butterflies: they form a family of involutions operating on (4k+2) variables and with differential uniformity at most 4, which contains the Dillon permutation. We will also prove that this generalized family does not contain any APN permutation besides the Dillon permutation.

THAIS BARDINI IDALINO, University of Ottawa

Embedding cover-free families and cryptographical applications

Cover-free families are set systems used to solve problems where we deal with n elements and want to identify d invalid ones by performing only t tests ($t \leq n$). We are interested in cryptographic problems, and we note that some of those need cover-free families with increasing n. Solutions with increasing n, such as *monotone families* and *nested families*, have been recently considered in the literature. We propose a generalization that we call *embedding families*, which allows us to increase both n and d. We propose constructions of embedding families with good compression ratio using polynomials over finite fields.

DANIEL PANARIO, Carleton University

Finite Fields in Discrete Mathematics

Finite fields are used in many areas of pure and applied mathematics. In this talk we survey several areas of discrete mathematics and combinatorics where finite fields play an important role. We illustrate this usage with some examples. This talk serves as an introduction to the other talks in this minisymposium.

CLAUDIO QURESHI, University of Campinas

Dynamics of Chebyshev polynomials over finite fields

In this talk We completely describe the functional graph associated to iterations of Chebyshev polynomials over finite fields. Then, we use our structural results to obtain estimates for the average rho length, average number of connected components and the expected value for the period and preperiod of iterating Chebyshev polynomials. This is joint work with Daniel Panario.