Finite Fields in Combinatorics II

(Chair/Président: **Petr Lisonek** (Simon Fraser University)
Org: **Petr Lisonek** (Simon Fraser University) and/et **David Thomson** (Carleton University))

MARK GIESBRECHT, University of Waterloo
Decomposition of additive polynomials and matrix similarity classes

We explore problems of efficient computations with additive (linearized) polynomials over finite fields, including decomposition/factorization and classifying the number of distinct composition patterns. We connect this to the similarity class of the Frobenius operator of the polynomials.

JING HE, Carleton University
A new class of almost perfect sequences and a new family of Zero Correlation Zone sequences

Using maximal length sequences and multiplicative characters, we construct a class of sequences with almost perfect autocorrelation. Then we interleave two sequences in this class to construct a zero correlation zone (ZCZ) sequence family with large size.

XIANG-DONG HOU, University of South Florida
A Class of Permutation Binomials over Finite Fields

Let q a prime power and $f = ax + x^{2q-1}$, where $a \in \mathbb{F}_q^*$. It was recently conjectured that f is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following holds: (i) $a = 1$, $q \equiv 1 \pmod 4$; (ii) $a = -3$, $q \equiv \pm 1 \pmod{12}$; (iii) $a = 3$, $q \equiv -1 \pmod 6$. We will confirm this conjecture. We will also describe the context from which this conjecture arose.

DANIEL KATZ, California State University, Northridge
Weil Sums of Binomials with Three-Valued Spectra

Weil sums of binomials arise naturally in number theory, and have direct applications in cryptography, digital sequence design, and coding theory. Consider the Weil sum $W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d + ax)$, with ψ_q the canonical additive character of finite field $\mathbb{F}_q$, $\gcd(d, q-1) = 1$, d not a power of p modulo $q-1$, and $a \in \mathbb{F}_q^*$. Fix q and d and consider the spectrum of values obtained as a runs through $\mathbb{F}_q^*$. At least three values must appear, and we discuss recent results about the case where precisely three appear, including our recent proof of the characteristic 3 case of a 1976 conjecture of Helleseth.

DAVID THOMSON, Carleton University
On a conjecture of Golomb and Moreno

A polynomial f over a finite field with $f(0) = 0$ and $f(xd) - f(x)$ being a permutation for all $d \neq 1$ is a *Costas polynomial*. Costas polynomials are semi-multiplicative analogues of *planar functions*. The Golomb-Moreno conjecture states that a Costas polynomial over a prime field is a monomial.

In this talk, we draw connections between Costas polynomials and related combinatorial objects. We also give a partial proof of the Golomb-Moreno conjecture: we show that $3/4$ of the terms of a Costas polynomial must equal 0. We also give an equivalent conjecture in terms of the number of *moved* elements of the field under f.