Finite Fields in Combinatorics II

(Org: **Daniel Panario** (Carleton University))

AIDEN BRUEN, U of Calgary

Information sets and linear algebra

Modern industrial error correction involves convolutional codes and linear codes over finite fields. For the latter, a data vector of length k is encoded to a codeword w of length n say with n>k. Given just the k entries of w in an information set we can recover w and thus the input data. We announce new results on information sets using a fundamental new result in linear algebra. [Joint with Trevor Bruen]

SUDHIR GHORPADE, Indian Institute of Technology Bombay, India

Coprime polynomial pairs, Hankel matrices, and splitting subspaces

We give a combinatorial proof of the fact that the probability for two randomly chosen monic polynomials in $\mathbb{F}_q[X]$ of degree n to be coprime is identical with the probability for an $n \times n$ Hankel matrix over $\mathbb{F}_q$ to be nonsingular. We will also discuss an open problem of determining the number of the so called splitting subspaces of a given dimension over a finite field, and outline some recent progress.

KAI-UWE SCHMIDT, Simon Fraser University

Sets of symmetric matrices over finite fields

A set of $m \times m$ symmetric matrices over a finite field is called an (m, d)-set if the difference between distinct elements has rank at least d. I will present constructions of (m, d)-sets and use association schemes to prove fundamental combinatorial properties of (m, d)-sets, showing optimality of the constructions in certain cases. These results have applications in the theory of codes over Galois rings and shed new light on the Z_4-linearity of Kerdock and Delsarte-Goethals codes.

BRETT STEVENS, Carleton University

finite field constructions of an imperfect design

A scheduling problem motivates searching for a design on n^2 points with blocks of size n. Such a design exists, of course, but the problem requires double resolvablity, which is impossible. Various notions of "best possible" lead us to three situations where we find finite field constructions meeting the relevant bounds, involving planes, ovals and APN functions.

Joint work with Tim Alderson and Keith Mellinger

QIANG WANG, Carleton University

Ambiguity and Deficiency of Permutations

We introduce the concepts of weighted ambiguity and deficiency, which measures the injectivity and surjectivity of difference mappings respectively, for a given mapping f between two finite Abelian groups of the same size. Then we obtain certain optimal constructions using permutation polynomials over finite fields. Furthermore, we explain their connections with Costas Arrays and Almost Perfect Nonlinear (APN) functions which are employed in some cryptosystems. (joint work with D. Panario, A. Sakzad, and B. Stevens).