Finite Algebraic Combinatorics and Applications
Combinatoire algébrique finie et applications

(Org: **Steven Dougherty** (University of Scranton), **Kenza Guenda** (University of Victoria), **T. Aaron Gulliver** (University of Victoria), **Ilias Kotsireas** (Wilfrid Laurier University) and/et **Edgar Martinez-Moro** (University of Valladoid))

TIM ALDERSON, University of New Brunswick Saint John
Constructions and bounds on 3-D Optical Orthogonal Codes

New constructions of 3-dimensional optical orthogonal codes will be presented. In each case, the codes have ideal off-peak autocorrelation 0, and in all but one case cross correlation 1. All codes produced are optimal with respect to the applicable Johnson bound. All codes are constructed by using a particular automorphism of PG(k, q), the finite projective geometry of dimension k over the field of order q, or by using an affine analogue in AG(k, q).

NUH AYDIN, Kenyon College
Recent Methods of Constructing New Linear Codes over $\mathbb{Z}_4$

Codes over finite rings has been a very active area of research. Among all finite rings, the quaternary ring $\mathbb{Z}_4$ has a special place. A database of best known codes over $\mathbb{Z}_4$ was introduced a few years ago. Recently, there has been an increased research activity on codes over rings that are extensions of $\mathbb{Z}_4$ and many new linear codes obtained from this work have been added to the database. In this talk, we will describe recent methods of constructing quaternary linear codes from codes over various extensions of the quaternary ring.

JONATHAN JEDWAB, Simon Fraser University
Costas cubes

A Costas array is a permutation array for which the vectors joining pairs of 1s are all distinct. We propose a new three-dimensional combinatorial object related to Costas arrays: an order n *Costas cube* is an array $(d_{i,j,k})$ of size $n \times n \times n$ over $\mathbb{Z}_2$ for which each of the three projections of the array onto two dimensions, namely $(\sum_i d_{i,j,k})$ and $(\sum_j d_{i,j,k})$ and $(\sum_k d_{i,j,k})$, is an order n Costas array. We present constructions for two infinite families of Costas cubes. We determine all Costas cubes of order at most 29, showing that Costas cubes exist for all these orders except 18 and 19 and that a significant proportion of the Costas arrays of certain orders occur as projections of Costas cubes. We then present constructions for two infinite families of Costas cubes.

This is joint work with Lily Yen, Capilano University.

FELICE MANGANIELLO, Clemson University
Representations of the Multicast Network Problem

We approach the problem of linear network coding for multicast networks from different perspectives. We introduce the code graph of a network, a simplified directed graph that maintains the information essential to understanding the coding properties of the network. One of the main problems in network coding is to understand when the capacity of a multicast network is achieved with linear network coding over a finite field of size q. We explain how this problem can be interpreted in terms of rational points on certain algebraic varieties.

EDGAR MARTINEZ MORO, University of Valladolid
New Avenues for Test Sets in Coding Theory

Test set decoding was an proposed as an alternative technique for syndrome decoding of linear codes. In this talk we will see how a test set can be also used for non linear codes and for computing the weight hierarchy of a code.

MICHAEL O'SULLIVAN, San Diego State University
Maximal t-path traceable graphs

The problem of characterizing maximal non-Hamiltonian graphs may be naturally extended to characterizing graphs that are maximal with respect to nontraceability and beyond that to t-path traceability. We define a graph to be t-path traceable if the minimal number of paths that can cover it is t, and it is maximal for this property when adding an edge yields a $(t-1)$-path traceable graph. We show how t-path traceability behaves with respect to disjoint union of graphs and the join with a complete graph. Our main result is a decomposition theorem that reduces the problem of characterizing maximal t-path traceable graphs to characterizing those that have no universal vertex. We generalize a construction of maximal non-traceable graphs due to Zelinka to t-path traceable graphs.

CLAUDIO QURESHI, Carleton University
Periods of iterations of mappings over finite fields with restricted preimage sizes

Let $[n] = \{1, \ldots, n\}$ and let Ω_n be the set of all mappings from [n] to itself. Let f be a random uniform element of Ω_n and let $T(f)$ and $B(f)$ denote, respectively, the least common multiple and the product of the length of the cycles of f. Harris proved in 1973 that $\log(T)$ converges in distribution to a standard normal distribution and, in 2011, E. Schmutz obtained an asymptotic estimate on the logarithm of the expectation of T and B over all mappings on n nodes. We obtain analogous results for random uniform mappings on $n = kr$ nodes with preimage sizes restricted to a set of the form $\{0, k\}$, where $k = k(r) \geq 2$. This is motivated by the use of these classes of mappings as heuristic models for the statistics of polynomials of the form $x^k + a$ over the integers modulo p, with $p \equiv 1 \pmod{k}$. We also exhibit and discuss our numerical results on this heuristic. Joint work with R. Martins, D. Panario and E. Schmutz.

ALBERTO RAVAGNANI, University of Toronto
Combinatorics and covering radius of rank-metric error-correcting codes

The covering radius of a rank-metric code is an important parameter that describes its correction capability. It measures the maximum weight of an error matrix than can be corrected by the code.

In this talk we describe combinatorial properties and invariants of matrix codes endowed with the rank metric, and relate them to the covering radius. We introduce new tools for the analysis of rank-metric codes, such as puncturing and shortening constructions. We then discuss upper bounds on the covering radius of a code by applying different combinatorial methods. The various bounds are then applied to the special classes of MRD and quasi-MRD codes.

PADMAPANI SENEVIRATNE, Texas A&M University-Commerce
Paley type bipartite graphs and self-dual codes

We derive an infinite class of binary self-dual codes from Paley type bipartite graphs P(q, k). Many of the codes in this class yield optimal or near optimal parameters. Another class of binary self-orthogonal codes are obtained from the complement of graphs P(q, k). These codes also tend to have optimal parameters. In addition, we find the structure of the automorphism group of these codes.

STEVE SZABO, Eastern Kentucky University
Some Minimal Rings

With no complete classification of finite rings, it may be difficult to identify a minimal ring with respect to cardinality of a particular type. Various minimal rings are given, a few not yet seen in the literature.

ÁNGELES VAZQUEZ-CASTRO, Autonomous University of Barcelona
Wiretap Coset Coding in the Transform Domain

We first describe the mathematical model for secure communications introduced in 1948 by C. Shannon, and how relaxing its assumptions as proposed by A. Wyner in 1975 leads to what is now known as wiretap coset coding for secure communications. We then review known wiretap algebraic linear coset coding constructions and introduce systematic constructions of wiretap codes in the transform/spectral domain.

JAY WOOD, Western Michigan University

Groups of isometries of additive codes over $GF(q)$

When q is a prime p, every additive code C over $GF(p)$ is a linear code, and every linear Hamming isometry of C to itself extends to a monomial transformation. However, when q is a prime power p^ℓ, $\ell \geq 2$, then an additive code C over $GF(q)$ is not necessarily linear, and there can exist additive Hamming isometries from C to itself that are not monomial. In fact, if H_1 and H_2 are any subgroups of $GL(n,p)$ satisfying $H_1 \subseteq H_2 \subseteq GL(n,p)$, together with some natural geometric hypotheses, then there exists an additive code C over $GF(q)$ of dimension n over $GF(p)$ whose group of self-isometries is H_2 while its group of monomial self-maps is H_1.