Design Theory
Théorie du design

(Org: **Hadi Kharaghani** (University of Lethbridge) and/et **Doug Stinson** (University of Waterloo))

PETER DANZINGER, Ryerson University

Some recent results on the Hamilton-Waterloo Problem

Given a graph G, a C_n-factor is a spanning subgraph of G each component of which is isomorphic to the n-cycle C_n. A factorization of G is a set of factors that between them partition the edges of G. Let K_v^* be the complete graph on v vertices if v is odd and $K_v - I$, where I is a 1-factor, when v is even.

Given non-negative integers v, m, n, α, β, the Hamilton-Waterloo problem, HWP$(v; m, n; \alpha, \beta)$, asks for a factorization of K_v^*, or, into α C_m-factors and β C_n-factors. Clearly, $v, n, m \geq 3$ must be odd, $m \mid v$, $n \mid v$ and $\alpha + \beta = (v-1)/2$ are necessary conditions. Without loss of generality we may assume that $n \geq m \geq 3$.

Recently we showed that the necessary conditions where (mostly) sufficient when m and n are odd and v is a multiple of n and m. More recently we have considered the case where v is not a multiple of n and m, we also have new results in the case where m and n have opposite parity.

Joint Work with A. Burgess and T. Traetta.

HADI KHARAGHANI, University of Lethbridge

Balancedly splittable Hadamard matrices

A Hadamard matrix of order n is said to be balancedly splittable if by a suitable permutation of the rows it can be splitted in two parts such as

$$\begin{pmatrix} H_1 \\ H_2 \end{pmatrix},$$

where H_1 is an $\ell \times n$ matrix, $\ell < n$, and $H_1^T H_1$ has at most two distinct off diagonal entries.

Feasible parameters and construction methods will be presented. Applications include some symmetric association schemes with five and six classes.

This is a joint work with Sho Suda.

ILIAS KOTSIREAS, Wilfrid Laurier University

Algorithms for difference families in finite abelian groups

Our main objective is to show that the computational methods that we previously developed for difference families in cyclic groups can be fully extended to the more general setting of arbitrary finite abelian groups. In particular the power spectral density (PSD) test and the method of compression can be used to speed up search algorithms.

This is joint work with Dragomir Z. Djokovic (University of Waterloo)

DON KREHER, Michigan Technological University

Uniformly resolvable decompositions of the complete graph: 3-paths and 3-stars.

If X is a connected graph, then an X-factor of a larger graph is a spanning subgraph in which all of its components are isomorphic to X. If a graph can be edge decomposed into X-factors, then we say the graph has an X-factorization. For example a K_2-factor is a one-factor and a K_2-factorization is a one-factorization. An (X, Y)-URD$(G; r, s)$ is an edge decomposition of the graph G into r X-factors and s Y-factors. In this talk we consider the problem when $(X, Y) = (P_3, K_{1,3})$ and $G = K_n$.

PETR LISONEK, Simon Fraser University
Kochen-Specker sets and Hadamard matrices

Kochen-Specker sets (KS sets) demonstrate the contextuality of quantum mechanics, which is one of its properties that may become crucial in quantum information theory. We use generalized Hadamard matrices to construct infinite families of KS sets. We show that the recently discovered simplest KS set is the initial member of one of our infinite families. We introduce a new class of complex Hadamard matrices which have not been studied previously and we show that they can be used to construct KS sets.

LUCIA MOURA, University of Ottawa
Ordered Orthogonal Array Construction Using LFSR Sequences

In this talk, we discuss a new construction of ordered orthogonal arrays (OOA) of strength t with $(q+1)t$ columns over a finite field $\mathbb{F}_q$ using linear feedback shift register sequences (LFSRs). OOAs are naturally related to (t, m, s)-nets, linear codes, and MDS codes. Our construction selects suitable columns from the array formed by all subintervals of length $\frac{q^t-1}{q-1}$ of an LFSR sequence generated by a primitive polynomial of degree t over $\mathbb{F}_q$. The set of parameters of our OOAs are the same as the ones given by Rosenbloom and Tsfasman (1997) and Skriganov (2002), but the constructed arrays are different. We experimentally verify that our OOAs are stronger than the Rosenbloom-Tsfasman-Skriganov OOAs in the sense that ours are "closer" to being a "full" orthogonal array. This is joint work with André Castoldi, Daniel Panario and Brett Stevens.

MIKE NEWMAN, university of ottawa
embedding factorizations in uniform hypergraphs

An old problem of Cameron asks when a partial parallelism can be extended to a complete parallelism. A specific formulation of this asks when a 1-factorization of a complete h-uniform hypergraph can be embedded in a 1-factorization of a (larger) complete h-uniform hypergraph. This was answered by Haagkvist and Hellgren: the "obvious necessary conditions" are sufficient.

We consider a generalization, asking when an r-factorization of a complete h-uniform hypergraph on m vertices can be embedded in an s-factorization of a (larger) complete h-uniform hypergraph on n vertices. While we do not have a complete characterization, we come surprisingly close. For $s = r$, the "obvious necessary conditions", together with $\gcd(m, n, h) = \gcd(n, h)$ are sufficient. For $s > r$ we need some more assumptions, but still we prove existence under a wide range of parameters.

The proof uses amalgamation-detachment, and an approach based on a group action.

This is joint work with Amin Bahmanian.

DANIEL PANARIO, Carleton University
Covering arrays from m-sequences and character sums over finite fields

A covering array of strength t on v symbols is an array with the property that, for every t-combination of column vectors, every one of the possible v^t t-tuples of symbols appears as a row at least once in the subarray defined by these column vectors. Arrays whose rows are cyclic shifts of an m-sequence over a finite field possess many combinatorial properties and have been used to construct various combinatorial objects; see [2].

In this talk we consider covering arrays consisting of discrete logarithms of carefully selected m-sequence elements. Inspired by [1], we connect the covering array definition for this type of arrays to the value of certain character sums over finite fields. Taking advantage of the balanced way in which the m-sequence elements are distributed, we are able to evaluate these sums. This provides new infinite families of covering arrays of arbitrary strength [3].

Joint work with L. Moura, B. Stevens and G. Tzanakis.

References:

[1] C.J. Colbourn, Covering arrays from cyclotomy, Designs, Codes and Cryptography 55 (2010), 201-219.

[2] L. Moura, G. L. Mullen, D. Panario. Finite field constructions of combinatorial arrays, Designs, Codes and Cryptography 78 (2016), 197-219.

[3] G. Tzanakis, L. Moura, D. Panario, B. Stevens. Covering arrays from m-sequences and character sums, Designs, Codes and Cryptography 85 (2017), 437-456.

DAVID PIKE, Memorial University of Newfoundland
A disproof of Tutte's conjecture based on twofold triple systems

In 1984, Colbourn and Johnstone presented a twofold triple system for which the corresponding 2-block-intersection graph was connected but not Hamiltonian. A recent paper by Erzurumluoğlu and Pike established that such a twofold triple system exists for every order $v \equiv 0$ or 1 (mod 3) such that $v \geq 6$, except for $v \in \{7, 9, 10\}$. However, it remained the case that all of the known examples were for twofold triple systems having non-bipartite 2-block-intersection graphs. Bipartite examples (which constitute counterexamples to Tutte's 1971 conjecture that every 3-connected cubic bipartite graph is Hamiltonian) have now been found and will be described in this talk. This is joint work with Rosalind Cameron.

DOUG STINSON, University of Waterloo
Ideal ramp schemes and related combinatorial objects

In 1996, Jackson and Martin proved that a strong ideal ramp scheme is equivalent to an orthogonal array. However, there was no good characterization of ideal ramp schemes that are not strong. Here we show the equivalence of ideal ramp schemes to a new variant of orthogonal arrays that we term *augmented orthogonal arrays*. We give some constructions for these new kinds of arrays, and, as a consequence, we also provide parameter situations where ideal ramp schemes exist but strong ideal ramp schemes do not exist.

TOMMASO TRAETTA, Università degli Studi di Perugia, Italy
Steiner triple systems with well-behaved automorphisms

A design is called f-pyramidal when it has an automorphism group fixing f points and acting sharply transitively on the others.

We consider the problem of determining the set of values of v for which there exists an f-pyramidal Steiner triple system of order v. Although this problem has been deeply investigated when $f = 1$, it remains open for a special class of values of v. For the next admissible value of f, which is $f = 3$, we provide a complete solution. However, for greater values of f this problem remains widely open.

In this talk, we will present the most recent results on this subject. This is joint work with Marco Buratti and Gloria Rinaldi.

STEVE WANG, Carleton University
A matrix approach to the period of a nonlinear congruential pseudorandom sequences over finite fields

We study the period of a nonlinear congruential pseudorandom sequence $\bar{a} = \{a_0, a_1, a_2, ...\}$ generated by $a_n = f^{(n)}(a_0)$ with initial value a_0, where f is a permutation polynomial over a finite field. We explain the connection between the period of the sequence and the order of an associated matrix $A(f)$ defined by the powers of $f(x)$. We also explore the connection between the rank of $A(f)$ and the cardinality of the value set of f.

QING XIANG, University of Delaware
A new infinite family of hemisystems of the Hermitian surface

This is a talk about tight sets and m-ovoids of the classical polar spaces (in particular, quadrics). Tight sets and m-ovoids are important substructures of the classical polar spaces, which are not only interesting in their own right, but also can give rise to many other geometric/combinatorial objects, such as translation planes, strongly regular graphs, two-weight codes. We will talk about a recent construction of hemisystems of the Hermitian surface $H(3, q^2)$ in the case where $q \equiv 3$ (mod 4), or equivalently, a $\frac{(q+1)}{2}$-ovoid of $Q^-(5, q)$, the elliptic quadric in $\mathrm{PG}(5, q)$. The construction uses cyclotomic classes of finite fields, and it depends on rather complicated computations involving Gauss sums. The talk is based on joint work with John Bamberg, Melissa Lee, and Koji Momihara.