Algebraic Design Theory
Théorie de la conception algébrique
(Org: **Hadi Kharigani** (Lethbridge))

ROB CRAIGEN, Manitoba
Synthetic Orthogonality Theory

De Launey and Flannery built their now-canonical field of Algebraic Design Theory upon the base assumption that an $m \times n$ array must have the property that all $2 \times n$ subarrays belong to a collection called an **orthogonality set**, thus abstracting, in an axiomatic fashion, a general category of "orthogonality" pertaining to important classes of designs. This seems an interesting, and inevitable, step in the development of an overarching theory encompassing the disparate objects of design theory: step back, set up axioms and see what worlds those axioms open up for exploration. Those worlds are inhabited, of course, by our old familiar friends in design theory, and many other exotic creatures, as yet unexplored.

The next phase of this work was to develop an algebraic framework that would marry this axiomatic approach with the ongoing questions of conventional design theory. Alternatively, they had an a priori notion of where this path should lead, and deliberately pushed forward in that direction.

But what else might have happened? Backtracking to the axiomatic framework, what dictates that one must follow the path of algebraic development? What might we find by allowing those "ground rules" to inform us what this world looks like? If we are led naturally into algebra, so be it ... but where else might we go?

This talk will summarize an alternative path for exploration, beginning with the De Launey-Flannery approach to orthogonality, and some interesting landscapes of that world that do not lie along their established path.

ILIAS KOTSIREAS, WLU
Cyclic $(v; k_1, k_2, k_3; \lambda)$ difference families with $v = 3 \mod 4$ a prime

We construct several new cyclic difference families $(v; k_1, k_2, k_3; \lambda)$ with $v = 3 \mod 4$ a prime and $\lambda = k_1 + k_2 + k_3 - (3v-1)/4$. The construction is based on the method of orbits, together with an efficient algorithm to solve a corresponding 3-way matching problem. Such families can be used in conjunction with the well-known Paley-Todd difference sets to construct Hadamard and skew Hadamard matrices of order $4v$. In particular, we construct the first example of a skew Hadamard matrix of order $4 \cdot 239$.

Joint work with D. Z. Djokovic.

BILL MARTIN, Worcester Polytechnic Institute
Linked systems of symmetric designs and real mutually unbiased bases

Let Γ be a finite undirected graph with vertex set X partitioned into w subsets each of size v:

$$X = X_1 \dot\cup X_2 \dot\cup \cdots \dot\cup X_w .$$

We say that Γ is a *linked system of symmetric (v, k, λ) designs with w fibres* if Γ satisfies the following three properties:
• no edge of Γ has both ends in the same fibre X_i;
• the subgraph of Γ induced between any two distinct fibres X_i and X_j is the incidence graph of some symmetric (v, k, λ) design;
• for any three distinct indices i, j, k from $\{1, \ldots, w\}$ and for any $a \in X_i$ and any $b \in X_j$ the number of common neighbors of a and b lying in X_k depends only on whether or not (a, b) is an edge of Γ and not on the choice of a and b or on the choice of i, j, k.

A set of w *mutually unbiased bases* in $\mathbb{R}^d$ ("w real MUBs") is a collection of orthogonal bases $\mathcal{B}_1, \ldots, \mathcal{B}_w$ for $\mathbb{R}^d$ enjoying the property that $|\mathbf{x} \cdot \mathbf{y}|$ is constant whenever $\mathbf{x}$ and $\mathbf{y}$ are chosen from distinct bases $\mathcal{B}_i$ and $\mathcal{B}_j$ from our collection.

In this talk we determine when a linked system of symmetric designs can be converted into a set of real MUBs and give partial results in the reverse direction. The talk is based, in part, on joint work with my student Brian Kodalen.

LUCIA MOURA, University of Ottawa
Finite Field Constructions of Combinatorial Arrays

Finite fields play a fundamental role in the construction of combinatorial designs. In an article of the same title with Gary Mullen and Daniel Panario (Designs, Codes and Cryptography, 2016), we survey constructions of combinatorial arrays using finite fields. These combinatorial objects include orthogonal arrays, covering arrays, ordered orthogonal arrays, permutation arrays, frequency permutation arrays, hypercubes and Costas arrays.

In this talk, I briefly discuss finite field constructions of various types of combinatorial arrays. Then, I focus on constructions of orthogonal arrays and related objects such as variable strength orthogonal arrays, ordered orthogonal arrays and covering arrays. An orthogonal array (and its variants) is an array with q^t rows and k columns on an alphabet with q symbols such that its projection into specific t-subsets of columns give subarrays where each t-tuple of the alphabet occurs once as one of its rows. The orthogonal array variants differ in which t-subsets of columns are required to have this "coverage property". A common theme on several of the recent constructions we discuss is the use of linear feedback shift register sequences of maximum period (m-sequences) to build arrays attaining a high number of t-subsets of columns with the "coverage property". The structure of coverage in the arrays built from intervals of length $(q^t - 1)/(q - 1)$ of these sequences reveal interesting relationships with finite geometry. I will mention different constructions I have worked on with André Castoldi, Sebastian Raaphorst, Daniel Panario, Brett Stevens and Georgios Tzanakis.

WILL ORRICK, Indiana University
Maximal determinants, sequence pairs, and cyclotomy

Construction of maximal-determinant matrices using pairs of binary sequences with prescribed autocorrelation properties goes back to the work of Paley and Szekeres in the case of Hadamard matrices, and of Ehlich in the case of matrices of size $n \equiv 2 \pmod 4$. Ehlich's matrices attain the upper bound of Ehlich and Wojtas, which, however, can only be reached under the condition that $n - 1$ be the sum of two integer squares. In certain cases where this condition is not satisfied, new types of sequence pairs discovered about a decade ago produce matrices with determinant approaching the upper bound. We give necessary conditions for the existence of such sequence pairs and describe some methods that have produced solutions up to $n = 106$. Cyclotomic constructions have been fruitful in the search for sequence pairs that generate Hadamard matrices. We describe recent results, some negative, restricting the types of solutions that can be constructed by cyclotomic methods, and some positive, producing infinite families of solutions.

Joint work with Tomas Rokicki, Adam Vollrath, Yancy Liao.

DAVID PIKE, Memorial University of Newfoundland
On the chromatic index of STS block intersection graphs

Given a combinatorial design, its block intersection graph is obtained by creating a vertex for each block and making vertices adjacent when their blocks have non-empty intersection. The chromatic index $\chi'(G)$ of a graph G is the least number of colours with which the edges can be labelled such that adjacent edges are never of the same colour. For any simple graph of maximum degree $\Delta(G)$, Vizing has established that $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$. Here we consider the chromatic index of block intersection graphs of Steiner triple systems. This is joint work with Jonathan Poulin.

ROSTAM SABETI, Olivet College
On classes of periodic parametrized circulant complex Hadamard matrices

This talk is about a novel concept of periodicity for classes of Parametrized Circulant Complex Hadamard (PCCH) matrices associated with solution components of cyclic n-roots. Examples of PCCH matrices of sizes $n = 4, 8, 12, 16$ and 18 with

different periods will be presented. Beside applications of CCH matrices in coding and quantum information, the number of PCCH matrices constructed by this method is an evidence to disprove the problematics (for corresponding versions of CHC) set forth by Teodor Banica, Ion Nechita and Jean-Mark Schlenker. As a result of a reformulated Theory and fundamental Theorems, a Combinatorial-Symbolic search algorithm will be used to construct associated PCCH matrix of size $n = 4k$ for $(k \in \mathbb{N})$. In order to fill some major gaps in derivation of real Hadamard matrices, the impact of this promising method that works very well will be discussed. Using scripts of Mathematica, the construction of PCCH matrix of size $n = 1084$ will be demonstrated.

ASIYEH SANAEI, Kwantlen Polytechnic University
Skolem Sequences and Graph Labelling

Skolem sequences were introduced in 1950s and have been used to construct combinatorial designs and to answer set partitioning problems. A Skolem-labeled graph can be assumed as a higher dimensional version of a Skolem sequence and the labelling may be used in testing distance reliability of networks. We survey the known results on graphs Skolem labelling and answer the question of whether a generalized Dutch windmill allows such a labelling. In particular, we show that a Dutch windmill composed of two cycles C_m and C_n, $n \geq m$, with a vertex in common does not have a Skolem labelling if and only if $n - m \equiv 3, 5 \pmod 8$ and m is odd, and thereby introducing a novel technique for proving that a Skolem labelling does not exist. "Joint work with Nancy Clarke"

BRETT STEVENS, Carleton University
Ordered orthognal arrays, LFSRs and hypergraph homomorphisms

We present a new construction of strength-t ordered orthogonal arrays (OOA) with $(q+1)t$ columns over a finite field $\mathbb{F}_q$ using linear feedback shift registers sequences (LFSRs). OOAs are the combinatorial analogue of (t, m, s)-nets. Our construction selects suitable columns from the circulant array formed from an LFSR sequence determined by a primitive polynomial of degree t. We prove properties about the relative positions of runs in the LFSR which establish the OOA properties. 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: our OOAs cover many more t-sets of columns than the Rosenbloom-Tsfasman-Skriganov OOAs. We also discuss this construction from the point of view of hypergraph homomorphisms.

SHO SUDA, Aichi University of Education
Linked systems of symmetric group divisible designs

Symmetric group divisible designs (SGDD) are a generalization of symmetric designs, and are studied by Bose. Inspired by a recent work of uniform association schemes by van-Dam, Martin, and Muzychuk, we introduce a concept of linked systems of SGDD. We will show necessarily conditions for existence, constructions, an equivalence between linked SGDD and association schemes. As a consequence, an upper bound on the number of linked systems of SGDD is obtained.

FERENC SZÖLLŐSI, Aalto University
Classification algorithms for Butson-type Hadamard matrices

A Butson-type complex Hadamard matrix H of order n is an $n \times n$ matrix whose entries are all some q-th root of unity satisfying $HH^* = nI$.

In this talk I will review the methods of orderly generation and (weak) canonical augmentation, and demonstrate how to use these tools to search for Butson-type complex Hadamard matrices of small orders.

These efforts are motivated by two long-standing open problems in harmonic analysis and quantum information theory, namely Fuglede's conjecture and the MUB-6 problem.

STEVE WANG, Carleton University
Some recent progress on Costas arrays

A Costas array of order n is a $n \times n$ permutation array (with exactly one dot in every row and column and blanks elsewhere) such that every vector connecting two dots are distinct. The Costas property ensures that the array has ideal auto-correlation, which makes Costas arrays highly desired for use in RADAR and SONAR communications. We examine two particular constructions of Costas arrays known as the Taylor variant of the Lempel construction, or the T_4 construction, and the variant of the Golomb construction, or the G_4 construction. We connect these constructions with the concept of Fibonacci primitive roots, and show that under the Extended Riemann Hypothesis the T_4 and G_4 constructions are valid infinitely often. We also confirm Golomb and Moreno's conjecture that every ciricular sequence is Costas if and only if it is exponential Welch.

KAROL ZYCZKOWSKI, Jagiellonian University, Cracow
On complex Hadamard matrices with special properties

Two classes of complex Hadamard matrices with certain special properties found recently applications in quantum physics. Consider a four index tensor T_{ijkl} of size M. It can be reshaped into a square matrix $A_{\mu,\nu}$ of size M^2 with three different choices of composed indices e.g. $\mu = (i, j); \nu = (k, l)$ or $\mu = (i, k); \nu = (j, l)$, or $\mu = (i, l); \nu = (j, k)$. A tensor T is called $perfect$ if all three matrices A, A' and A'' generated in this way are unitary. A matrix A is called $multiunitary$ if it remains unitary after suitable reshuffling of their entries. Examples of multiunitary complex Hadamard matrices of size 9 are presented. We discuss also skew complex Hadamard matrices and address the question for which size they exist.