Theory and Application of Sequences and Arrays
Théorie et application des suites et tableaux
(Org: **Jonathan Jedwab** (SFU) and/et **Brett Stevens** (Carleton))

ROBERT BAILEY, University of Regina
Generalized covering and packing designs

Covering designs are a generalization of t-designs, where the requirement that any t-subset of points be contained in *exactly* λ blocks is replaced with the weaker requirement that they be contained in *at least* λ blocks. Covering arrays generalize orthogonal arrays in a similar manner. In this talk, we will present a common generalization of covering designs and covering arrays, as well as some methods of constructing these new designs.

We will also discuss the "dual" problem of packing designs, which are defined by the opposite weakening of the definition, where any t-subset of points may be contained in *at most* λ blocks, and where a similar generalization may be made.

JIM DAVIS, University of Richmond
Association schemes from McFarland Difference Sets

Association schemes can be built by partitioning a group into disjoint subsets all of which are either difference sets or subgroups as long as each difference set is either reversible or the set of inverses for another of the difference sets in the partition. We exhibit partitions for three groups of order 96 into five subsets: four of the subsets are McFarland difference sets and the fifth is a subgroup of order sixteen. The corresponding 5-class association schemes are non-symmetric and imprimitive.

MEGAN DEWAR, Government of Canada
Monotone Gray Codes for vectors of the form $[-m, m]^k$ *and* $[0, m]^k$

We consider ordering k-dimensional vectors having integer coordinates so that consecutive vectors differ by a minimal change. We define a monotone adjacent change Gray code for vectors having integer coordinates to be a listing of the vectors such that consecutive vectors differ in a single position by $+1$ or -1 and such that the vectors appear in order from smallest to largest L_∞ norm. This is a generalization of Savage and Winkler's definition of monotone binary Gray codes. We prove, by construction, the existence of monotone adjacent change Gray codes for $[0, m]^k$, for all $m, k \in \mathbb{N}$, and the existence of monotone adjacent change Gray codes for $[-m, m]^k$, for all $m, k \in \mathbb{N}$, k even. Furthermore, we show that monotone adjacent change Gray codes for $[-m, m]^k$ do not exist when k is odd.

PETER DUKES, University of Victoria
Randomness expansion using orthogonal arrays

Loosely, a pseudo-random number generator (PRNG) turns some short 'random' sequence into a longer sequence which simulates random behavior in some way.

In earlier work, Gopalakrishnan and Stinson demonstrate how a strength two, index one orthogonal array acts as a PRNG. A random row is chosen, requiring two random inputs, and other elements in that row are output as pseudo-random. Although extremely basic by today's standards of PRNGs, some simple and elegant independence bounds exist.

Based on my work with Alan C.H. Ling, this talk explores an extension to higher strength orthogonal arrays. Significantly stronger independence results are possible at the expense of generating a few more initial random inputs.

FRANK FIEDLER, Wesley College
Non-Existence of Golay Sequence Pairs and Vanishing Sums of Roots of Unity

The only known non-existence results for Golay sequence pairs are due to Golay and Eliahou et.al. Golay showed that there are no binary Golay sequences of odd length. Eliahou et.al. proved that if n is the length of a binary Golay sequence pair then n has no prime factor congruent 3 modulo 4.

We present non-existence results for H-phase Golay sequence pairs when $H/2$ is odd.

AARON GULLIVER, University of Victoria
Extended Binary Linear Codes from Legendre Sequences

A construction based on Legendre sequences is presented for a doubly-extended binary linear code of length $2p + 2$ and dimension $p+1$. This code has a double circulant structure. For $p = 4k+3$, we obtain a doubly-even self-dual code. Another construction is given for a class of triply extended rate $1/3$ codes of length $3p+3$ and dimension $p+1$. For $p = 4k+1$, these codes are doubly-even self-orthogonal.

RICHARD HOSHINO, National Institute of Informatics, Tokyo
A Multi-Round Generalization of the Traveling Tournament Problem and its Application to Japanese Baseball

In a double round-robin tournament involving n teams, every team plays $2(n-1)$ games, with one home game and one away game against each of the other $n-1$ teams. Given a symmetric n by n matrix representing the distances between each pair of home cities, the Traveling Tournament Problem (TTP) seeks to construct an optimal schedule that minimizes the sum total of distances traveled by the n teams as they move from city to city, subject to several natural constraints to ensure balance and fairness.

In the TTP, the number of rounds is set at $r = 2$. In this paper, we generalize the TTP to multiple rounds ($r = 2k$, for any $k \geq 1$) and present an algorithm that converts the problem to finding the shortest path in a directed graph, enabling us to apply Dijkstra's algorithm to output the optimal multi-round schedule.

We apply our algorithm to optimize the league schedules for Nippon Professional Baseball (NPB) in Japan, where two leagues of $n = 6$ teams play 40 sets of three intra-league games over $r = 8$ rounds. Our optimal schedules for the Pacific and Central Leagues achieve a 25% reduction in total traveling distance compared to the 2010 NPB schedule, implying the potential for considerable savings in terms of time, money, and greenhouse gas emissions.

This is joint work with Ken-ichi Kawarabayashi.

HONGGANG HU, University of Waterloo
New Ternary and Quaternary Sequences with Two-Level Autocorrelation

Pseudorandom sequences with good correlation properties are widely used in communications and cryptography. The search of new sequences with two-level autocorrelation has been a very interesting problem for decades. In 2002, Gong and Golomb proposed the iterative decimation-Hadamard transform (DHT) which is an useful tool to study two-level autocorrelation sequences. They showed that for all odd $n \leq 17$, using the second-order decimation-Hadamard transform, and starting with a single binary m-sequence, all known two-level autocorrelation sequences of period $2^n - 1$ which have no subfield factorization can be obtained. Recently, we found many new ternary or quaternary sequences with two-level autocorrelation using the second-order decimation-Hadamard transform. The period of such sequences is $2^n - 1$.

JONATHAN JEDWAB, Simon Fraser University
The asymptotic merit factor of binary sequences

The merit factor of a binary sequence measures the collective smallness of its aperiodic autocorrelation coefficients. Long binary sequences with large merit factor are attractive in digital communications applications, and correspond to high-degree polynomials with $\{+1, -1\}$ coefficients having small L_4 norm on the unit circle. We analyse the behaviour of the merit factor of several classes of binary sequences, as the sequence length increases without bound.

This is joint work with Kai-Uwe Schmidt.

DANIEL KATZ,
Pairs of Maximal Length Sequences with Few Cross-Correlations

We consider pairs of binary maximal length sequences, with one a decimation of the other, and examine the cross-correlations between the one and all the cyclic shifts of the other. We use arithmetic and combinatorial techniques to determine constraints on the number of distinct cross-correlation values that appear and their 2-adic distances from -1 as a function of the length of the sequences and the decimation.

HADI KHARAGHANI, University of Lethbridge
Turyn type sequences

For a given sequence $A = (a_0, a_1, \cdots, a_n)$, let

$$N_A(s) = \sum_{i=0}^{i=n-s} a_i a_{i+s} \text{ for } s = 0, 1, 2, \cdots, n, \text{ and } N_A(s) = 0 \text{ for } s \geq n+1.$$

Four $(-1, 1)$ sequences X, Y, Z, W of lengths n, n, n, $n-1$, are siad to be of *Turyn type* if

$$(N_X + N_Y + 2N_z + 2N_W)(s) = 0, \text{ for } s \geq 1.$$

It is conjectured that Turyn type sequences of lengths n, n, n, $n-1$ exist for all even values of n. A summary of known results on this conjecture will be presented.

MAHDAD KHATIRINEJAD, University of British Columbia
On the Nonexistence of 3-Phase Barker Arrays

A 3-phase Barker array is a matrix of third roots of unity for which all out-of-phase aperiodic autocorrelations have magnitude 0 or 1. The only known truly two-dimensional 3-phase Barker arrays have size 3×3. We prove the nonexistence of $s \times t$ 3-phase Barker arrays for infinitely many values of (s, t). As an example, we show that a 3-phase Barker array of size $s \times 3^k q$, where $k \geq 1$ and $(3, q) = 1$, must satisfy $s \leq 2k + 1$. In the case $q = 1$ and $s > 1$, we completely settle the nonexistence unless $s = 3^k = 3$. Using an exhaustive search, we also rule out the nonexistence of certain small 3-phase Barker arrays.

This is joint work with Jonathan Jedwab and Kai-Uwe Schmidt.

PETR LISONEK, Simon Fraser University
Identities for Kloosterman sums

Kloosterman sums are exponential sums defined on finite fields that are important in Cryptography and Coding Theory. As a motivation example we mention an application in the construction of pseudo-random sequences that are used as key streams in stream ciphers. Identities relating values of Kloosterman sums are thus of interest. We use the theory of elliptic curves to show that an infinite family of such identities can be obtained from the classical modular polynomials. We show that some identities that have been proved earlier by other authors arise as special cases of our result.

DANIEL PANARIO, Carleton University
Divisibility of Polynomials over Finite Fields and Combinatorial Applications

Consider a maximum-length shift-register sequence generated by a primitive polynomial f over a finite field. The set of its subintervals is a linear code whose dual code is formed by all polynomials divisible by f. Since the minimum weight of dual

codes is directly related to the strength of the corresponding orthogonal arrays, we can produce orthogonal arrays by studying divisibility of polynomials. Munemasa (Finite Fields Appl., 4(3):252-260, 1998) uses trinomials over $\mathbb{F}_2$ to construct orthogonal arrays of guaranteed strength 2 (and almost strength 3). That result was extended by Dewar, Moura, Panario, Stevens and Wang (Des. Codes Cryptogr., 45:1-17, 2007) to construct orthogonal arrays of guaranteed strength 3 by considering divisibility of trinomials by pentanomials over $\mathbb{F}_2$.

In this talk we review the above results and we comment on extensions of them. First we simplify the requirement in Munemasa's approach that the characteristic polynomial of the sequence be primitive: we show that the method applies even to the much broader class of polynomials with no repeated factors. Then we give characterizations of divisibility for binomials and trinomials over $\mathbb{F}_3$. Some of our results apply to any finite field $\mathbb{F}_q$ with q elements. We briefly comment on the combinatorial applications of these results.

Joint work with Olga Sosnovski, Brett Stevens and Qiang Wang.

ANDREW RECHNITZER, UBC

Some numerical experiments on a very combinatorial group

Richard Thompson's group F is a widely studied group which has provided examples of and counter-examples to a variety of conjectures in group theory. It is also an extremely combinatorially appealing object which has a beautiful description in terms of binary trees.

In this talk I will describe some combinatorial problems associated with F. One of these problems is directly related to the very open problem of the amenability of the group. I will explore this problem using some simple numerical methods that are usually applied to problems in statistical physics.

Joint work with Murray Elder, Eric Fusy, Buks van Rensburg and Thomas Wong will appear in this talk.

KAI-UWE SCHMIDT, Simon Fraser University

From Dirichlet characters to binary sequences with large merit factor

A binary sequence of length n is an n-tuple of elements taking on values $+1$ or -1 and its merit factor is a measure of self-similarity of the sequence. The problem of determining the largest possible merit factor of long binary sequences is related to several classical conjectures due to Littlewood, Erdős, and Turyn. We consider binary sequences of odd square-free length n for which $\phi(n)$ of the n elements are determined by the real nonprincipal Dirichlet character modulo n, while the remaining $n-\phi(n)$ elements can be freely chosen. Subject to mild conditions, we determine the worst-case and best-case behaviour of the merit factor of these sequences, and show that almost all these sequences have the best-case behaviour. We also give explicit examples of such sequences having the best-case behaviour.

This is joint work with Jonathan Jedwab.

BRETT STEVENS, Carleton University

Sequences in Groups: covering arrays, costas arrays and APN permutations

Sequences can be viewed more generally as maps from one group to another, with the standard domain being the Natural numbers or some subset thereof. We survey some common uses of such sequences for constructing orthogonal covering arrays, Costas arrays and APN permutations. The requirements on the sequences in these three cases are similar and lead to two natural definitions: weighted ambiguity and deficiency. We study the optimum lower bounds of these measures for bijections between two groups of the same size and show that optimal ambiguity implies the APN property. We then examine several constructions of mappings which are optimal with respect to these lower bounds.

DOUG STINSON, University of Waterloo

Some new results and conjectures on Costas and honeycomb arrays

An n by n *Costas array* consists of n dots in an n by n array such that there is exactly one dot in each row and each column, and the $n(n-1)$ difference vectors are distinct. A *honeycomb array* with n dots is a set of n dots in the hexagonal grid such that, in each of the three natural directions, the dots occupy exactly n consecutive "rows" of the grid, and the $n(n-1)$ difference vectors are distinct. Costas arrays were defined by Costas in 1975 and honeycomb arrays were defined by Golomb and Taylor in 1984.

We prove that any honeycomb array contains an odd number of dots. The proof makes use of a known result concerning non-attacking queens on a triangular chessboard.

We also consider the problem of finding the maximum number of mutually disjoint n by n Costas arrays. When $n = p-1$ and p is prime, there exist n mutually disjoint n by n Costas arrays. We perform some enumerations for small n and make some conjectures based on the numerical data.

This talk is based on joint work with Simon Blackburn, Jeff Dinitz, Patric Östergård, Anastasia Panoui, and Maura Paterson.

STEPHANIE VAN WILLIGENBURG, University of British Columbia

Composition tableaux

A celebrated type of array is Young tableaux, which arise, for example, in algebraic combinatorics, discrete geometry, representation theory and algebraic geometry. In this talk we generalize Young tableaux, indexed by integer partitions, by introducing composition tableaux, indexed by integer compositions. We then discuss a variety of instances where these new tableaux arise naturally.

STEVEN WANG, Carleton University

On interleaved sequences of Legendre sequences

Families of pseudorandom sequences with low cross correlation and/or high linear complexity have important applications in communications and cryptography. Among several known constructions of sequences with low cross correlations, interleaved constructions proposed by Gong uses two sequences of the same period with two-level autocorrelation. In this talk, we construct some low cross correlation interleaving sequences such that the base sequences may not have the same period, or they may not have two-level autocorrelation. In particular, we present some results on the cross correlation magnitude and linear complexity of the interleaved sequences of Legendre sequences of periods p and q, respectively, where p and q are odd prime numbers.

This talk is based on joint work with J. He, D. Panario, and A. Winterhof.

AMY WIEBE, Simon Fraser University

A new source of seed pairs for Golay sequences of length 2^m

Golay complementary sequence pairs have found application in many areas of digital information processing since their introduction by Golay in 1951. Two of the main questions in the study of Golay sequences are: for what lengths does a Golay sequence pair exist, and how many distinct Golay sequences and Golay sequence pairs of a given length are there? In this talk, we discuss the discovery of new 6-phase length 16 Golay sequences. We explain the origin of these sequences and how they are only the second known nontrivial seed pairs that can be used in the construction of new infinite families of Golay sequences having length a power of 2.