
Designs and codes
Dessins et codes
(Org: **David Pike** (Memorial) and/et **Doug Stinson** (Waterloo))

SIMON BLACKBURN, Royal Holloway University of London
Locally block-avoiding orderings of points

This talk is based on joint work with Tuvi Etzion, Technion.

Let n and ℓ be positive integers. Recent papers by Kreher, Stinson and Veitch have explored variants of the problem of ordering the points in a triple system (such as a Steiner triple system, directed triple system or Mendelsohn triple system) on n points so that no block occurs in a segment of ℓ consecutive entries. (Thus the ordering is locally block-avoiding.) I will describe a greedy algorithm which produces such orderings, provided n is sufficiently large when compared to ℓ . I will also talk about some related results and open problems.

Simon R. Blackburn and Tuvi Etzion, 'Block-avoiding point sequencings', *J. Combin. Des.* 29 (2021) 339-366.

ANDREA BURGESS, University of New Brunswick
Cyclic cycle systems of complete equipartite graphs

A *cycle system* of a graph Γ is a partition of the edges of Γ into cycles. For a graph Γ with vertex set \mathbb{Z}_v , we say that a cycle system \mathcal{D} of Γ is *cyclic* if, for any cycle $(c_1, c_2, \dots, c_\ell)$ of \mathcal{D} , we have that $(c_1 + 1, c_2 + 1, \dots, c_\ell + 1)$ is also a cycle of \mathcal{D} .

In this talk, we consider cycle systems of the complete multipartite graph $K_m[n]$ with m parts of size n . We determine necessary and sufficient conditions for the existence of a cyclic ℓ -cycle system of $K_m[n]$ when $2\ell \mid (m-1)n$; this is a natural case to consider, as it allows us to construct cyclic cycle systems with no short-orbit cycles.

This is joint work with Francesca Merola and Tommaso Traetta.

CHARLIE COLBURN, Arizona State University
Covering Perfect Hash Families with Index Greater Than One

Given positive integers N, k, t and a prime power q , let A be an $N \times k$ array whose symbols are column vectors from \mathbb{F}_q^t . The entry in row r and column c of A is denoted by $\mathbf{v}_{r,c}$. Suppose that $\{\gamma_1, \dots, \gamma_t\}$ is a set of distinct column indices. Row r is *covering* (in A) for $\{\gamma_1, \dots, \gamma_t\}$ if the $t \times t$ matrix $[\mathbf{v}_{r,\gamma_1} \cdots \mathbf{v}_{r,\gamma_t}]$ is nonsingular over \mathbb{F}_q . Then A is a *covering perfect hash family*, $\text{CPHF}_\lambda(N; k, q, t)$, if there are at least λ covering rows for each way to choose $\{\gamma_1, \dots, \gamma_t\}$. When $\lambda = 1$, such CPHFs have been explored as a means to generate the smallest known covering arrays of strengths 3 through 6 having hundreds or thousands of columns, when the number of symbols is a (small) prime power. Motivated by applications that require additional coverage in testing, in this talk we explore the construction of CPHFs with $\lambda > 1$.

THAIS BARDINI IDALINO, Universidade Federal de Santa Catarina
Variable cover-free families

Cover-free families have been investigated under different names and as a solution to many problems related to combinatorial group testing. In this presentation, we will review some related objects and constructions found in the literature, as well as some applications in cryptography. Inspired by these applications, we introduce the notion of *variable cover-free families*, which presents variable coverage properties.

This is joint work with Lucia Moura.

HADI KHARAGHANI, University of Lethbridge
The power of prime powers in the building of designs

Assuming the weight p in a weighing matrix $W(n, p)$ is a prime power, it is shown that there is a

$$W\left(\frac{p^{m+1}-1}{p-1}(n-1)+1, p^{m+1}\right)$$

for each positive integer m . The case of $n = p + 1$ reduces to the balanced weighing matrices with classical parameters

$$W\left(\frac{p^{m+2}-1}{p-1}, p^{m+1}\right).$$

DON KREHER, Michigan Technological University
Steiner's problem ... Bussey's solution

A set-system of order N is a pair (X, \mathcal{B}) , where X is N -element set of *points* and \mathcal{B} is a collection of subsets of X called *blocks*.

In 1852, Professor Dr. J. Steiner of Berlin, asked for which number N does there exist a set system containing no pairs that has order N and maximum block size k satisfying

1. no block properly contains another block, and
2. for all $t = 2, 3, \dots, k - 1$ every t -set that does not contain a block is contained in exactly one block of size $(t + 1)$.

The only known solution with maximum block size at least 5 was an infinite family exhibited by W.H. Bussey from the University of Minnesota in 1914. He provides a construction for each $k \geq 5$ a set-system of order $N = 2^{k-1} - 1$ and maximum block size k satisfying Steiner's conditions. In 1984, H. Hanani, apparently unaware of Bussey's solution, gives exactly the same solution.

In this talk I will discuss Bussey's solution and report on the progress that Charlie Colbourn, Patric Östegård and I have made in constructing another solution.

TRENT MARBACH, Ryerson University
Balanced equi- n -squares

We define a d -balanced equi- n -square $L = (l_{ij})$, for some divisor d of n , as an $n \times n$ matrix containing symbols from \mathbb{Z}_n in which any symbol that occurs in a row or column, occurs exactly d times in that row or column. We show how to construct a d -balanced equi- n -square from a partition of a Latin square of order n into $d \times (n/d)$ subrectangles. In design theory, L is equivalent to a decomposition of $K_{n,n}$ into d -regular spanning subgraphs of $K_{n/d, n/d}$. We also study when L is diagonally cyclic, defined as when $l_{(i+1)(j+1)} = l_{ij} + 1$ for all $i, j \in \mathbb{Z}_n$, which corresponds to cyclic such decompositions of $K_{n,n}$ (and thus α -labellings).

We identify necessary conditions for the existence of (a) d -balanced equi- n -squares, (b) diagonally cyclic d -balanced equi- n -squares, and (c) Latin squares of order n which partition into $d \times (n/d)$ subrectangles. We prove the necessary conditions are sufficient for arbitrary fixed $d \geq 1$ when n is sufficiently large, and we resolve the existence problem completely when $d \in \{1, 2, 3\}$.

Along the way, we identify a bijection between α -labellings of d -regular bipartite graphs and, what we call, d -starters: matrices with exactly one filled cell in each top-left-to-bottom-right unbroken diagonal, and either d or 0 filled cells in each row and column. We use d -starters to construct diagonally cyclic d -balanced equi- n -squares, but this also gives new constructions of α -labellings.

BILL MARTIN, Worcester Polytechnic Institute
Duelling dragons

This project investigates 3-class Q -antipodal association schemes and related objects. Van Dam proved in 1999 that 3-class Q -antipodal association schemes are equivalent to the linked systems of symmetric designs of Cameron (1972). Kodalen constructed new examples in 2019, exhibiting connections to equiangular lines and real mutually unbiased bases. The dual object, at the parameter level, is a 3-class P -antipodal association scheme; such graphs are known as distance-regular antipodal covers of complete graphs, or DRACKNs. In the special case where the automorphism group contains an abelian subgroup acting regularly on the vertices, we have an explicit duality via character theory and then we are truly challenging DRACKNs to have duals. As we will explain in this talk, this is rare.

KAREN MEAGHER, University of Regina

2-Partially Intersecting Partitions

An ℓ -partition of a set of size $n = k\ell$ can be expressed as a set of ℓ disjoint sets, $P = \{P_1, P_2, \dots, P_\ell\}$. Further, an ℓ -partition is uniform if $|P_i| = k$ for all $i = 1, \dots, \ell$. Two uniform ℓ -partitions $P = \{P_1, P_2, \dots, P_\ell\}$ and $Q = \{Q_1, Q_2, \dots, Q_\ell\}$ are said to be 2-partially intersecting if there exist an i and j such that $|P_i \cap Q_j| \geq 2$. There are many different notions of intersection for partitions, and this particular type of intersection is connected to several different problems in design theory. In this talk I will show how an algebraic approach can be used to determine the size of the largest collection of uniform ℓ -partitions of a $k\ell$ -set in which any two partitions are 2-partially intersecting.

LUCIA MOURA, University of Ottawa

Ordered Covering Arrays and NRT-metric Covering Codes

Ordered covering arrays generalize both ordered orthogonal arrays and covering arrays, which are well-studied combinatorial designs. Classical codes using the Hamming metric can be generalized to codes with a poset metric. The Niederreiter-Rosenbloom-Tsfasman (NRT) metric corresponds to posets that are the disjoint union of chains of the same size. In this talk, we discuss ordered covering arrays and their use in upper bounds for NRT-metric covering codes. This talk is based on joint work with André Guerino Castoldi, Emerson Luiz do Monte Carmelo, Daniel Panario, and Brett Stevens.

SIBEL ÖZKAN, Gebze Technical University

On The Directed Hamilton-Waterloo Problem

Cycle decomposition is an important branch of graph decomposition problems. There are two well-known resolvable cycle decomposition problems where cycles can be partitioned into parallel classes, namely, 2-factors. One problem is the Oberwolfach problem where each 2-factor in the decomposition is isomorphic to a given 2-factor. Another problem is the Hamilton-Waterloo problem where each 2-factor can be isomorphic to one of the given two 2-factors. Both Oberwolfach and the Hamilton-Waterloo problems are mostly studied for uniform cycle factors so far.

Directed version of the Oberwolfach problem has started to gain more interest recently. Here, the decomposed graph is the complete symmetric directed graph K_v^* . Factors with uniform -directed- cycle size 3, with uniform cycle size 4, and with uniform cycle size m where $v \equiv 0 \pmod{2m}$, m is odd with $5 \leq m \leq 49$ are among the results on this version of the problem (see [1], [2], and [3] respectively). Here we carry this directed generalization to the Hamilton-Waterloo problem and present our first results on small cycle sizes. This is joint work with Ugur Odabasi and Fatih Yetgin.

[1] Bermond J. C., Germa A., and Sotteau D. 1979, Resolvable decomposition of K_n^* , Journal of Combinatorial Theory, Series A, 26(2), 179-185.

[2] Bennett F. E., Zhang X., 1990, Resolvable Mendelsohn designs with block size 4, Aequationes mathematicae, 40(1), 248-260.

[3] Burgess A., Francetic N., Sajna M., 2018, On the directed Oberwolfach Problem with equal cycle lengths: the odd case. Australas. J. Combin., 71(2), 272-292.

MAURA PATERSON, Birkbeck, University of London

Reciprocally-weighted external difference families and unconditionally secure authentication

Let G be a finite abelian group of order n . An (n, k, λ) m -External Difference Family (EDF) is a collection of m disjoint subsets of G each of size k , with the property that each nonzero group element occurs precisely λ times as a difference between group elements in two different subsets from the collection. These have use as Algebraic Manipulation Detection (AMD) codes that can be viewed as a special case of an authentication code, which are structures which have long been studied as a tool for authenticating the sender of a message in an unconditionally secure setting. The AMD codes arising from EDFs have the nice feature that the success probability of an adversary in the worst case is equal to the average case success probability.

It is possible to generalise the notation of an EDF to allow subsets of different sizes. However, if we wish to keep the worst case=average case property, then we need to count the number of times that group elements arise as external differences using a weighted sum. Specifically, a reciprocally-weight EDF (RWEDF) is defined to be a generalisation of an EDF in which the subsets may have different sizes, and the differences are counted with a weighting given by the reciprocal of the set sizes. In this talk I will describe a construction of an infinite families of nontrivial RWEDFs, and discuss some open problems relating to these structures.

SAROBIDY RAZAFIMAHATRATRA, University of Regina

The Erdős-Ko-Rado theorem for permutation groups

A set of permutations \mathcal{F} of a finite transitive group $G \leq \text{Sym}(\Omega)$ is *intersecting* if any two permutations in \mathcal{F} agree on an element of Ω . The *intersection density* of the intersecting set $\mathcal{F} \subset G$ is the rational number $\rho(\mathcal{F}) := \frac{|\mathcal{F}|}{|G_\omega|}$, where $\omega \in \Omega$. The intersection density of the group G is the number $\rho(G) := \max\{\rho(\mathcal{F}) : \mathcal{F} \subset G \text{ is intersecting}\}$. The permutation group G is said to have the *Erdős-Ko-Rado (EKR) property* if $\rho(G) = 1$.

I will talk about some recent progress on the construction of transitive groups that do not have the EKR property. I will also present some results on the intersection density of transitive groups of certain degrees.

MAHSA SHIRAZI, University of Regina

On a generalization of set-wise intersection of perfect matchings

Two perfect matchings P and Q of a graph on $2k$ vertices are said to be set-wise t -intersecting if there exist edges P_1, \dots, P_t in P and Q_1, \dots, Q_t in Q such that the union of edges P_1, \dots, P_t has the same set of vertices as the union of Q_1, \dots, Q_t has. In this talk I will present an extension of the famous Erdős-Ko-Rado (EKR) Theorem to set-wise t -intersecting families of perfect matching for $t = 2$ and $t = 3$. In particular I will prove the following:

The size of the largest set of set-wise 2 and 3-intersecting perfect matchings in K_{2k} with $k \geq 6$ is $(2k - 5)!!$, and $(2k - 7)!!$, respectively.

BRETT STEVENS, Carleton University

The combinatorial game NOFIL played on Steiner triple systems

We define the impartial combinatorial game NOFIL played on designs. We review some relevant combinatorial game theory. We discuss what is known about optimal play on small Steiner triple systems, exhaustively up to order 15 and for sampled STSs of orders 19, 21 and 25. We show that the complexity of determining the outcome of a game of NOFIL (possibly with moves already made) on Steiner triple systems is PSPACE-complete by reducing the combinatorial game NODE KAYLES on graphs to NOFIL using Barber et al.'s existence theorem of triangle decompositions for sufficiently large triple-divisible graphs. This is joint work with Drs. M. Huggan and S. Huntemann.

RUIZHONG WEI, Lakehead University

On coded caching schemes

Coded caching schemes are used to reduce the network traffic during the peak time by using the local caching to store some information during the off peak time. In this talk, we will introduce two recent results about the construction of coded caching schemes.

ŞULE YAZICI, Koç University

Embedding orthogonal partial Latin squares

In 1960, Evans proved that a partial Latin square of order n can always be embedded in some Latin square of order t for every $t \geq 2n$ and asked if a pair of finite partial Latin squares which are orthogonal can be embedded in a pair of finite orthogonal Latin squares. It is known, that a pair of orthogonal Latin squares of order n can be embedded in a pair of orthogonal Latin squares of order t if $t \geq 3n$, the bound of $3n$ being best possible. Jenkins, considered embedding a single partial Latin square in a Latin square which has an orthogonal mate. His embedding was of order t^2 . In 2014, the first constructive polynomial embedding result for a pair of orthogonal partial Latin squares was given. Recently, the work of Jenkins is generalized and it is shown that any partial Latin square can be embedded in a Latin square which has many orthogonal mates (not just one) that are mutually orthogonal. In this talk, we review results for the embedding of orthogonal partial Latin squares in orthogonal Latin squares, comparing and contrasting these with results for embedding partial Latin squares in Latin squares. We also present a new construction that uses the existence of a set of t mutually orthogonal Latin squares of order n to construct a set of $2t$ mutually orthogonal Latin squares of order n^t .