Finite Combinatorics
Combinatoire finie
(Org: **Robert Craigen** and/et **David Gunderson** (Manitoba))

WAYNE BROUGHTON, University of British Columbia Okanagan
Systems of Parallel Representatives

In a finite affine plane of order n, a *system of parallel representatives* (SPR) is a set of $n+1$ lines consisting of exactly one line from each parallel class of the plane. An SPR is *tight* if no three of its lines are incident on a common point; this is equivalent to a hyperoval in the dual of the associated projective plane of order n. We describe some basic properties of SPR's and characterize tight SPR's as those on which a certain sum-of-squares function attains the value zero. We then examine some necessary conditions for an SPR to be minimal with respect to this function, and apply our results to SPR's in a hypothetical affine plane of order 12.

ZOLTAN FUREDI, University of Illinois at Urbana–Champaign
Color critical hypergraphs and forbidden configurations

A k-uniform hypergraph (V, E) is 3-color-critical if it is not 2-colorable, but for every edge e the hypergraph $(V, E-e)$ is 2-colorable. Lovász proved in 1976 that

$$|E| \le \binom{n}{k-1}$$

for a 3-color-critical k-uniform hypergraph with n vertices.

Here we give a new algebraic proof and prove a generalization that leads to a sharpening of Sauer's bound for $\mathrm{forb}(m, F)$, where F is a k-by-ℓ $0,1$-matrix.

Joint work with R. Anstee, B. Fleming, and A. Sali.

PENNY HAXELL, University of Waterloo
On stable paths

Let G be a graph with a distinguished vertex d. Suppose that each vertex of G has a preference list of a set of paths joining it to d. A solution to the stable paths problem is a tree T in G rooted at d, with the property that for each vertex x, if x prefers some path P to the path from x to d in T, then some edge of P not incident to x is missing from T. Not every instance of the stable paths problem has a solution, but we show that every instance does have a fractional solution.

JONATHAN JEDWAB, Simon Fraser University, 8888 University Drive, Burnaby, BC, V5A 1S6
Bounds on the growth rate of the peak sidelobe level of binary sequences

The peak sidelobe level of a binary sequence is the largest absolute value of all its nontrivial aperiodic autocorrelations. A classical problem of digital sequence design is to determine how slowly the peak sidelobe level of a length n binary sequence can grow, as n becomes large. Moon and Moser showed in 1968 that the growth rate of the peak sidelobe level of almost all length n binary sequences lies between order $\sqrt{n \log n}$ and $\sqrt{n}$, but in the last forty years no theoretical improvement to these bounds has been found.

I shall present numerical evidence showing how closely these bounds can be approached. A significant algorithmic improvement reveals behaviour that was previously well beyond the range of computation.

Joint work with Denis Dmitriev.

HADI KHARAGHANI, University of Lethbridge

The asymptotic existence of amicable orthogonal designs

An *orthogonal design* A of order n and type $(s_1, s_2, \ldots, s_u)$, in the commuting variables $\pm x_1, \pm x_2, \ldots, \pm x_u$, denoted $\mathrm{OD}(n\,;\, s_1, s_2, \ldots, s_u)$, is a square matrix of order n with entries $\pm x_k$ or 0, where each x_k occurs s_k times in each row and column such that distinct rows are pairwise orthogonal. Two orthogonal designs X and Y are said to be *amicable*, if $XY^t = YX^t$.

Amicable orthogonal designs are instrumental in the construction of orthogonal matrices. Not much is known about the existence or the structure of full (no zeros) amicable orthogonal designs admitting the maximum possible number of variables. An asymptotic existence result for full amicable orthogonal designs with almost maximum number of variables will be presented.

WILLIAM KOCAY, University of Manitoba

Non-Fano Quads in Finite Projective Planes

Given a finite projective plane of order n. A quadrangle consists of four points A, B, C, D, no three collinear. If the diagonal points are non-collinear, the quadrangle is called a non-Fano quad. A general theorem is proved on the distibution of points and lines in a plane of order n, with respect to a non-Fano quad, whenever $n \geq 7$. The theorem implies that the number of possible distributions of points in a plane of order n is limited for all $n \geq 7$.

VACLAV LINEK, University of Winnipeg, 515 Portage Ave., Winnipeg, MB, R3B 2E9

Chromatic numbers of Steiner quadruple systems

A Steiner quadruple system of order v, SQS(v), is a pair (X, B), where B is a set of 4-subsets of X such that each 3-subset of X is in a unique member of B. Hanani showed that an SQS(v) exists if and only if $v = 0, 1$ or $v \equiv 2, 4 \pmod 6$. An SQS(v) is commonly described as a S(3,4,v) design, and as a 4-uniform hypergraph each SQS(v) has a chromatic number.

For a given $k \geq 2$, a basic problem is to determine all v for which a k-chromatic SQS(v) exists. We survey recent progress on this problem and point out avenues for future research.

DHRUV MUBAYI, University of Illinois at Chicago

Turan's theorem with colors

We consider a generalization of Turán's theorem for edge-colored graphs. Suppose that R (red) and B (blue) are graphs on the same vertex set of size n. We conjecture that if R and B each have more than $(1-1/k)n^2/2$ edges, and K is a $(k+1)$-clique whose edges are arbitrarily colored with red and blue, then $R \cup B$ contains a colored copy of K, for all $k+1 \notin \{4, 6, 8\}$. If $k+1 \in \{4, 6, 8\}$, then the same conclusion holds except for one specific edge-coloring of K_{k+1}.

We prove this conjecture for all 2-edge-colorings of K_{k+1} that contain a monochromatic K_k. This provides a new proof of Turán's theorem. We also prove the conjecture for $k+1 \in \{3, 4, 5\}$.

This is joint work with Ajit Diwan.

WENDY MYRVOLD, University of Victoria, Victoria, BC
Investigating Conjectures about Fullerenes

Fullerenes are all-carbon molecules whose molecular structures correspond to 3-regular planar graphs that have face sizes equal to five or six. Fuigui (Fullerene Interactive Graphical User Interface) is a java program under development whose goal is to aid the exploration of fullerenes and their parameters. This talk will include a selection of interesting open problems about various fullerene parameters. A demonstration of how Fuigui can be used to attack these will be provided.

This is joint work with Bette Bultena, Sean Daugherty, Bradley Debroni Patrick Fowler, Sameer Girn, Marsha Minchenko, and Jennifer Woodcock.

ORTRUD OELLERMANN, University of Winnipeg
Steiner Trees and Convex Geometries

Let V be a finite set and $\mathcal{M}$ a collection of subsets of V. Then $\mathcal{M}$ is an alignment of V if and only if $\mathcal{M}$ is closed under taking intersections and contains both V and the empty set. If $\mathcal{M}$ is an alignment of V, then the elements of $\mathcal{M}$ are called convex sets and the pair $(V, \mathcal{M})$ is called an aligned space. If $S \subseteq V$, then the convex hull of S is the smallest convex set that contains S. Suppose $X \in \mathcal{M}$. Then $x \in X$ is an extreme point for X if $X \setminus \{x\} \in \mathcal{M}$. A convex geometry on a finite set is an aligned space with the additional property that every convex set is the convex hull of its extreme points. Let G be a connected graph. We define several graph convexities using Steiner distances and trees and characterize those classes of graphs for which these graph convexities are convex geometries.

Joint work with M. Nielsen.

RANGANATHAN PADMANABHAN, University of Manitoba
A group representation for the anti-Pappian design

It was shown by H. Schröter [Nachr. Ges. Wiss. Göttingen 1889, 193–236] that among the ten combinatorially possible $(10, 3)$ designs, only one cannot be realized in a projective plane over any field. In view of this, this D10 is known in the literature as an anti-Pappian design. In 1954, R. Lauffer [Math. Nachrichten, vol. 11] gave a representation of this design over the infinite division ring of quaternions. This proves that the design, viewed as a ternary implicational system, is strictly consistent, meaning that it is impossible to formally derive $x = y$ from the ten defining equations. Here we give a group representation of rank 3 for this configuration and show that 3 is the minimal possible rank for such a representation. Apart from demonstrating the combinatorial consistency of the anti-Pappian design, this gives a new proof of the fact that this design cannot be realized in any finite Desarguesian plane. This is part of an unpublished set of notes on group representations written in collaboration with Barry Wolk and the late Professor Nathan Mendelsohn.

BRUCE REED, McGill University, CNRS, and INRIA
The diameter of sparse random graphs

We show that for any p such that pn goes to infinity, the diameter of $G_{n,p}$ is concentrated on two values.

DOUGLAS STINSON, University of Waterloo
Unconditionally secure chaffing and winnowing with short authentication tags

Rivest proposed the idea of a chaffing-and-winnowing scheme, in which confidentiality is achieved through the use of an authentication code. Thus it would still be possible to have confidential communications even if conventional encryption

schemes were outlawed. Hanaoka *et al.* constructed unconditionally secure chaffing-and-winnowing schemes which achieve perfect secrecy in the sense of Shannon. Their schemes are constructed from unconditionally secure authentication codes.

In this talk, we construct unconditionally secure chaffing-and-winnowing schemes from unconditionally secure authentication codes in which the authentication tags are very short. This could be a desirable feature, because certain types of unconditionally secure authentication codes can provide perfect secrecy if the length of an authentication tag is at least as long as the length of the plain text. The use of such a code might be prohibited if encryption schemes are made illegal, so it is of interest to construct chaffing-and-winnowing schemes based on "short" authentication tags.

We use elementary combinatorial techniques for our construction.

JACQUES VERSTRAETE, McGill University, 805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A 2K6
Clique partitions of dense graphs

In this talk I will prove that for any forest $F \subset K_n$, $K_n \backslash E(F)$ is a union of at most roughly $n \log n$ cliques. This result generalizes a number of preceding theorems on clique partitions of complements of paths. In addition, it will be shown that the minimum number of cliques required to partition $K_n \backslash E(G)$ when $G \subset K_n$ has maximum degree $O(n^{1-\epsilon})$, where $\epsilon > 0$ is a constant independent of n, is at most $n^{2-\epsilon/2}(\log n)^2$ and at least $\epsilon^2 n^{2-2\epsilon}$, for n large enough relative to ϵ.

We leave the following two basic open problems. First, to show that if a graph $G \subset K_n$ has maximum degree $o(n)$, then $K_n \backslash E(G)$ can be partitioned into $o(n^2)$ cliques, and second, to exhibit a forest F such that $K_n \backslash E(F)$ cannot be partitioned into any linear number of cliques.

This is joint work with Mike Cavers.

MIEKO YAMADA, Kanazawa University, Kakuma-machi, Kanazawa 920-1192, Japan
Self-dual $\mathbf{Z}_4$ codes generated by Hadamard matrices and conference matices

Active researches on self-dual codes over $\mathbf{Z}_4 = \mathbf{Z}/4\mathbf{Z}$ have been devoted in recent years. A Type II $\mathbf{Z}_4$-code is a self-dual code which has the property that all Euclidean weights are divisible by 8 and contains the all-one vector.

A self-dual $\mathbf{Z}_4$-code which is not a Type II code is called a Type I $\mathbf{Z}_4$-code. A Type IV $\mathbf{Z}_4$-code is a self-dual code with all codewords of even Hamming weight. A type IV code which is also Type I or Type II is called a Type IV-I, or a Type IV-II code respectively. Two infinite families of Type IV codes are known, Klemm's codes and $C_{m,r}$ codes.

The distinct rows of an Hadamard matrix are orthogonal. If we recognize the components 1 and -1 of an Hadamard matrix H_{4m} of order $4m$ as the elements of $\mathbf{Z}_4$, then the $\mathbf{Z}_4$-code generated by H_{4m} is self-orthogonal. In 1999, Charnes proved that if an Hadamard matrix H_{4m} has order $4m$ and m is odd, then the $\mathbf{Z}_4$-code generated by H_{4m} is self-dual and equivalent to Klemm's code. Charnes and Seberry considered the $\mathbf{Z}_4$-code generated by a weighing marix $W(n,4)$ and proved that if it has type $4^{(n-4)/2}2^4$, then it is a self-dual code. In this talk, we give families of self-dual $\mathbf{Z}_4$-codes of Type IV-I and Type IV-II generated by Hadamard matrices and conference matrices.