ABSTRACTS

DCCG Workshop
Lethbridge
July 9 – 14, 2001

In multi-author talks "⋆" indicates the speaker.

Vertex-Transitive Graphs

Brian Alspach
University of Regina
alspach@math.uregina.ca

A graph X is said to be *vertex-transitive* when the automorphism group of X acts transitively on the vertex set of X. The three talks will deal with some unsolved problems for vertex-transitive graphs.

Codes and the $(22, 33, 12, 8, 4)$ *Balanced Incomplete Block Design*

R.T. Bilous and G.H.J. van Rees*

University of Manitoba
vanrees@cs.umanitoba.ca

The point code of a $(22, 33, 12, 8, 4)$-BIBD is a binary doubly-even self-orthogonal code of length 33. This code, if it exists, could be embedded into a binary doubly-even self-orthogonal code,C, of length 33 and dimension 16 with no coordinate of all zeroes. Since the enumeration of inequivalent binary doubly-even self-dual codes of length 32 along with their automorphism groups is known, we can enumerate inequivalent such codes with their automorphism groups for length 34. From these, we can enumerate all inequivalent codes like C and their automorphism groups. There are 594 such codes. The number we check by theory.

The problem now is to see if one of these codes contain 22 codewords of weight 16 that could make up the incidence matrix of a $(22, 33, 12, 8, 4)$. Theory has eliminated 116 of these codes. Computing has eliminated a further 156. The talk will show how we did this.

Selected Topics on Sharply-Vertex-Transitive Designs

Marco Buratti
Università di Perugia, ITALY

Given a subgraph B of a graph Γ, a (Γ, B)-design is a collection $\mathcal{D} = \{B_1, ..., B_n\}$ of copies of B (*blocks*) whose edges partition $E(\Gamma)$, i.e., $\bigcup_{i=1}^{n} E(B_i) = E(\Gamma)$. In the case where Γ is a *Cayley graph* on a group G preserving $\mathcal{D}$, we say, for obvious reasons, that $\mathcal{D}$ is *sharply-vertex-transitive under* G. In particular, a design is *cyclic* when it is sharply-vertex-transitive under the cyclic group.

Here, we present some progress on the following problems:

1. Settle the set of pairs (v, k) for which there exists a cyclic k-cycle system of the complete graph on v vertices, i.e., a cyclic (K_v, C_k)-design.
2. Settle the set of values of v for which there exists a cyclic $2-(v, 4, 1)$ design, i.e., a cyclic (K_v, C_4)-design.
3. Settle the groups G for which there exists a sharply-vertex-transitive 1-*factorization* of the complete graph under G, i.e., a sharply-vertex-transitive *resolvable* (K_v, K_2)-design under G.

Special Ramsey Defining Patterns

Collin C. Carbno

Saskatchewan Telecommunications

Classical Ramsey theory proves that for graph with a sufficiently large number of points neither c points of the graph are mutually connected (c-clique) , or s points of the graph are totally unconnected. The smallest number of points that satisfy this criteria is known as the Ramsey number $R(c, s)$. A C-language program was written that used Monte Carlo simulation to estimate what fraction of all possible graphs satisfy the Ramsey condition for a number of points $m, m < n$. The fraction of graphs of m points that violates the Ramsey criteria appears to drop rapidly as m increases and become minute long before m reaches $R(c, s)$. A pattern for the number of points one less than the Ramsey number can therefore be logically called a Ramsey number defining pattern. If these patterns could be understood and predicted it follows that Ramsey numbers could be easily computed. A C-language program was written that searches for Ramsey patterns for $R(3, s)$. The paper develops some theoretical results on these Ramsey defining patterns and gives some observations from this investigation. A possible analytic form is found for Ramsey numbers of the form $R(3, s)$.

Slope Covers and Packings in Affine Planes

Mark Chateauneuf* and Doug Stinson
University of Waterloo
mchateau@cacr.math.uwaterloo.ca

We consider a collection of points, T, in an affine plane of prime order, p. Two points determine a slope m if the line which contains them has slope m. A slope m is determined by T if there are at least two points in T which determine m. T is a *slope cover* if all slopes $m \in Z_p$ are determined by T. T is a *slope packing* if for any slope $m \in Z_p$, there are at most two points in T which determine m. We seek small covers and large packings.

Using a BIBD to Develop a Gracefully Degradable Declustered RAID Architecture

Siu-Cheung Chau[1⋆] and Ada Wai-Chee Fu[2]

[1] *Wilfrid Laurier University*
[2] *The Chinese University of Hong Kong*
schau@wlu.ca
adafu@cse.cuhk.edu.hk

A new layout method Prime-groups which is based on a BIBD is proposed to evenly distribute parity groups for declustered RAID. Prime-groups satisfies most of the layout goals for a good declustered RAID layout. For the goals that are not satisfied, it is near optimal. A new layout goal maximal write and reconstruction parallelism is also proposed. If a layout satisfies the new goal, all the surviving disks can be read in parallel and can be rewritten in parallel during reconstruction and reconfiguration. Prime-groups satisfies the new goal when the write request begins in the first disk of the array. It is also near optimal in term of declustering ratio when p is a prime. Prime-groups can compliment the layouts proposed by Alvarez et. el.for the criteria to obtain a good layout is quite different between Prime-groups and those proposed by Alvarez et. el.

Three Applications of Combinatorial Designs

Charles Colbourn
University of Vermont
colbourn@emba.uvm.edu

Recently, combinatorial designs have arisen in a number of interesting applications. In this sequence of talks, three such applications are developed in some detail. The first concerns the design of certain codes used in the manufacture of DNA arrays. The second concerns a wavelength assignment problem in optical networking. The third concerns the detection of defective items in a linearly ordered collection. In each case, a practical problem leads to constraints on a system of sets (or, equivalently, binary matrix), and the optimization relative to these constraints leads to an interesting class of designs. The applications have been selected to reflect a diverse set of problems in design theory, as well as the novelty of their applications.

Complementary Pairs of Sequences

Robert Craigen
University of Manitoba
craigen@server.maths.umanitoba.ca

Complementary sets of sequences (ie sets whose total autocorrelation is zer) have received some attention in recent years, in both the combinatorics the engineering literature, for their connection to codes and designs, and for their applications to communications schemes and range-finding devices.

Known sets are surely sufficient for most engineering applications, but the discovery of more could lead to big inroads in answering questions about orthogonal designs (such as Hadamard matrices and weighing matrices). For all we know, therein lies the final solution to the celebrated Hadamard matrix conjecture.

Yet these sequences are poorly understood; there remain open questions about them that are maddeningly elementary, and known examples are obtained almost exclusively by brute-force computer searches (combined with a couple of elementary recursive constructions).

Over the last few years I have sought to crack open our understanding of complementary sets by aiming at the base: complementary pairs. Aside from sequences with only one nonzero entry, which may be regarded as trivial, no single sequence has zero autocorrelation — this is a property of sets of more than one sequence, which are usually called complementary in this context. Thus, the interesting cases begin with pairs.

Golay pairs, complementary pairs of (1,-1)-sequences, looked very promising when first discovered in the early 50's, but in spite of some determined attacks, only a handful of them have been found, and attempts to find more or show that no more exist have met with failure. Complementary ternary (0,1,-1) pairs initially showed more variation but, until recently, provided few truly new examples.

This talk is about recent work on complementary pairs of various types (binary, Boolean, ternary, complex, dihedral, polyphase,

and integral), starting with the factorization theorem of Eliahou, Kervaire and Saffari. We will introduce new variations on old constructions, discuss the recent (2001) resolution of the question of whether there exist complementary pairs of weight 29, and our attempts to build a coherent theory about these objects.

Broken Spectrum for Strict Colourings

Lucia Gionfriddo
University of Catania, Italy
lucia.gionfriddo@dipmat.unict.it

A mixed hypergraph is a triple $\mathcal{H} = (X, \mathcal{C}, \mathcal{D})$, where X is the vertex set and $\mathcal{C}$, $\mathcal{D}$ are both a list of non empty subsets of X: the $\mathcal{C}$-edges and the $\mathcal{D}$-edges. A strict k-colouring of H is a surjection $c: X \mapsto \{1, 2, 3, 4.....k\}$ such that each edge of $\mathcal{C}$ has at least two vertices assigned a common value and each edges of $\mathcal{D}$ has at least two vertices assigned distinct values. The minimum number of colours in a strict-colouring of a mixed-hypergraph $\mathcal{H}$ is called the *lower-chromatic number* of $\mathcal{H}$ and it is denoted by $\chi(\mathcal{H})$, the maximum number of colours is called the *upper-chromatic number*, $\bar{\chi}(H)$. Recently we determined the minimum number of vertices for which there exist hypergraphs with gaps. Further we examined colourings of mixed hypergraphs in the case that H is a P_3-*design* and constructed families of P_3-*design* having the chromatic spectrum with gaps and other particular properties.

On the Upper Chromatic Index of a Graph

M. Gionfriddo[1], L. Milazzo[2⋆] and V. Voloshin[3]

[1,2] *Department of Mathematics and Informatics*
University of Catania
Viale A. Doria, 6 95125 - Catania, Italy
[3] *Institute of Mathematics and Computer Science*
Moldavian Academy of Sciences, Moldova
gionfriddo@dmi.unict.it
milazzo@dmi.unict.it
voloshin@math.md

We consider the coloring of the edges of a graph in such a way that every vertex with a degree of at least two is incident to at least two edges of the same color. The maximum number of colors that can be used is the upper chromatic index of a graph G, denoted as $\bar{\chi}'(G)$. We prove that for a graph G with the maximum number of disjoint cycles c and m edges, n vertices and p pendant vertices respectively, $\bar{\chi}'(G) = c + m - n + p$.

Absorbing Sets in Coloured Tournaments Revisited

Gena Hahn
University of Montreal
hahn@iro.umontreal.ca

A theorem of Sands, Sauer and Woodrow says that in any digraph D whose edges are coloured in two colours so that there is no monochormatic ray (infinite path), there exists a set S of vertices such that from any vertex not in S there is a monochromatic (directed) path to a vertex in S; further, there is no monochromatic path between vertices of S. We say that S is an absorbing set. It follows from the theorem that if D is a tournament, there is an absorbing vertex. What happens if more than two colours are used?

Adding More Runs to Saturated D-Optimal Resolution III Designs

A.S. Hedayat* and Haiyuan Zhu

Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
hedayat@uic.edu

We consider the class of saturated main effect plans for the 2^k factorial. With these saturated designs, the overall mean and all main effects can be unbiasedly estimated provided that there are no interactions. However, there is no way to estimate the error variance with such designs. Because of this, we like to add s more runs to the set of $(k+1)$ runs in the D-optimal design in this class. There are several broad approaches to do this. One approach is to select some of the interior runs in the design and make multiple observations on the chosen runs. In this approach, we have $(k+1)$ choices for each additional run. The second approach is to select s runs from the set of exterior runs, which have not been used in the design. This latter approach allows us (2^k-k-1) choices for each additional run. If $s>1$, we have the third approach which is to select part of s runs from the set of interior runs and part from the set of exterior runs. Clearly we should not make our choice arbitrary no matter which approach we follow. Our goals here are: a. To search for s run so that the resulting design based on $(k+s+1)$ runs yields a D-optimal design; b. Classify all the runs into equivalent classes so that the runs in the same equivalent class give us the same value of the determinant of the information matrix. This allows us to trade-off runs for runs if it becomes necessary. In this paper we shall address these approaches and present some new results.

Decomposable Symmetric Designs

Y. Ionin
Central Michigan University

A decomposition of a symmetric design D is a partition $\mathcal{P}$ of its point set and a partition $\mathcal{B}$ of its block set such that the incidence structure induced by D on each pair (P, B), $P \in \mathcal{P}$, $B \in \mathcal{B}$, is either empty or a symmetric design. If all these symmetric designs have the same parameters, the decomposition is called uniform. We will give examples of infinite families decomposable symmetric designs and explore relations between uniform decompositions of symmetric designs, balanced generalized weighing matrices, and spreads of subspaces in projective spaces.

On a Class of Strongly Regular Graphs

H. Kharaghani
University of Lethbridge
hadi@cs.uleth.ca

Let q be a prime power and n a positive integer with $\frac{q-1}{n}$ being an even integer. It is shown that there is a symmetric $BGW(1+q+\cdots+q^{2m+1}, q^{2m+1}, q^{2m+1}-q^{2m})$ with zero diagonal over the cyclic group C_n of order n, for each nonnegative integer m. The applications include a large class of Strongly Regular Graphs. We also discuss the existence of a class of Doubly Regular Asymmetric Digraphs.

Some Results on the Existence of Large Sets of t-Designs

G.B. Khosrovshahi[1,2*] and B. Tayfeh-Rezaie[2]

[2] *Institute for Studies in Theoretical Physics and Mathematics*
P.O.Box 19395-5746, Tehran, Iran
[1] *Department of Mathematics, University of Tehran, Tehran, Iran*

A set of trivial necessary conditions for the existence of a large set of t-designs, $LS[N](t,k,v)$, is that $N|\binom{v-i}{k-i}$ for $i = 0,\ldots,t$. There are two conjectures due to Hartman and Khosrovshahi which state that the trivial necessary conditions are sufficient in the cases $N = 2$ and $N = 3$, respectively. Ajoodani-Namini has established the truth of Hartman's conjecture for $t = 2$. Apart from this celebrated result, we know the correctness of the conjectures for a few small values of k when $N = 2$ and $t \leq 6$ and also when $N = 3$ and $t \leq 4$. In this talk, we show that the foregoing results are in fact true for infinitely many values of k.

Fixed Parameter Complexity

Ton Kloks

Royal Holloway University of London, UK
ton@cs.rhul.ac.uk

Consider an algorithm for a parameterized problem (I, k) where I is the problem instance and k the parameter. The algorithm is uniformly polynomial if it runs in time $O(f(k)|I|^c)$ where $|I|$ is the problem size $f(k)$ an arbitrary function and c a constant. A parameterized problem is *fixed-parameter tractable* (FPT) if it admits a uniformly polynomial time algorithm. Parameterized complexity was introduced some 10 years ago and there are numerous algorithms known for FPT problems. A breakthrough was made with the discovery of sub-exponential (i.e., $O(c^{\sqrt{k}}n)$) solutions for various domination problems on planar graphs. I will give an outline of the PLANAR DOMINATION algorithm. It was shown that finding subexponential solutions is not possible for all MAX SNP-hard problems unless W[1]=FPT. Furthermore it was shown that PLANAR DOMINATION has no EPTAS running in time $O(2^{o(\sqrt{1/\epsilon}}p(n))$ unless W[1]=FPT. This indicates that the sublinear FPT solution for PLANAR DOMINATION is "close to optimal". I will show some new results on reductions to problem kernels for some problems. I show that PLANAR INDEPENDENT DOMINATION can be solved in time $O(c^{\sqrt{k}}+n)$ time. I show a new algorithm solving the k-LEAF SPANNING TREE problem in time $O(n+p^k)$ for some constant p. Hence also this solution is "close to optimal" since k-LEAF SPANNING TREE is MAX SNP-hard.

A Hole-Size Bound for Incomplete t-Wise Balanced Designs

Donald L. Kreher* and Rolf S. Rees

Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan, U.S.A. 49931-1295
kreher@mtu.edu

An incomplete t-wise balanced design of index λ is a triple $(X, H, \mathcal{B})$ where X is a v–element set, H is a subset of X is called the hole, and $\mathcal{B}$ is a collection of subsets of X called blocks, such that every t-element subset of X is either in H or in exactly λ blocks but not both. If H is a hole in an incomplete t-wise balanced design of order v and index λ, then $|H| \leq v/2$ if t is odd; $(v-1)/2$ if t is even. In particular this result establishes the validity of Kramer's conjecture that: the maximal size of a block in a Steiner t-wise balanced design is at most $v/2$ if t is odd and at most $(v-1)/2$ when t is even.

The Existence of Kirkman Squares – Doubly Resolvable $(v, 3, 1)$-BIBDs

Alan Ling
Michigan Technological University
aling@mtu.edu

A Kirkman square with index λ, latinicity μ, block size k, and v points, $KS_k(v; \mu, \lambda)$, is a $t \times t$ array ($t = \lambda(v-1)/\mu(k-1)$) defined on a v-set V such that (1) every point of V is contained in precisely μ cells of each row and column, (2) each cell of the array is either empty or contains a k-subset of V, and (3) the collection of blocks obtained from the non-empty cells of the array is a $(v, k, \lambda) - BIBD$. For $\mu = 1$, the existence of a $KS_k(v; \mu, \lambda)$ is equivalent to the existence of a doubly resolvable $(v, k, \lambda) - BIBD$. The spectrum of $KS_2(v; 1, 1)$ or Room squares was completed by Mullin and Wallis in 1975. In this talk, we discuss the spectrum for a second class of doubly resolvable designs with $\lambda = 1$. This is a joint work with Colbourn, Lamken and Mills.

Some Graph Partition Problems

Jim Liu
University of Lethbridge
liu@cs.uleth.ca

The index domain alignment for distributed-memory machines is formulated as finding a set of suitable alignment functions that map the index domains of the arrays into a common index domain so as to minimize the cost of data movement due to cross-references between the array. This problem has been formulated as a graph partition problem. We generalize the graph partition problem to four closely related graph partition problems and show that these partition problems are NP-complete. We further present some approximation algorithms. Theoretical analysis and experimental results show that these algorithms produce very good feasible solutions.

A Note on the Structure of Two Dimensional Modulo Metrics

Edgar Martínez-Moro* and F. Javier Galán-Simón

Universidad de Valladolid, Spain
edgar.martinez@ieee.org
javi@emp.uva.es

We shall study the combinatorial structure of sublattices of Gaussian integers and Eisenstein-Jacobi integers. This lattices have been found useful for coding two-dimensional QAM signal constellations (see [3,4]). They can be found also in the theory of self-similar lattices where they are useful for recursive constructions of lattices (see [1,2]). In this work we define an association scheme over the classes in the sublattice which is weakly metric for Mannheim and Hexagonal metrics. This association scheme is defined by the orbitals of a transitive action. This construction have been shown in [5,6] for the case of a p^r (p prime) number of points. In this work we emphasize the relation of the properties of the association scheme with some well known number theoretical facts.

1. J.H. Conway, E.M. Rains, N.J.A. Sloane, On the existence of similar sublattices. Canadian Journal of Mathematics (1999), **6**, 1300–1306
2. J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer Verlag, 3rd. ed, 1998.
3. K. Huber, Codes over Gaussian integers., IEEE Trans. on Inf. Theory, **40**(1) (1994), 207–216.
4. K. Huber, The Mac Williams Theorem for Two-dimensional modulo metrics, AAECC, **8**(1) (1997), 41–48.
5. E. Martínez-Moro, F.J. Galán-Simón, M.A. Borges-Trenard, M. Borges-Quintana, Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics. Cryptography and Coding. Lecture Notes in Computer Science **1746** (1999), Springer Verlag. 45–55
6. E. Martínez-Moro. *Two dimensional lattices with hexagonal metric.* Accepted communication at AAECC14.

The Number of Words in Certain Non-linear Codes

V. Kumar Murty
University of Toronto
murty@math.toronto.edu

We shall investigate the number of words in certain non-linear codes introduced by Elkies.

On Holes in t-Wise Balanced Designs

Rolf Rees
Memorial University of Newfoundland
rolf@math.mun.ca

Kreher and Rees proved that if h is the size of a hole in an incomplete t-wise balanced design of order v and index λ having minimum block size $k \geq t+1$ then

$h \leq (v + (k-t)(t-2) - 1)/(k-t+1)$.

We will show that this bound is sharp infinitely often for every value of $t \geq 2$, viz: for each $t \geq 2$ there exists a constant $C_t \geq 0$ such that whenever $(h-t)(k-t-1) \geq C_t$ there exists an incomplete t-wise balanced design meeting the bound for some $\lambda = \lambda(t,h,k)$. We describe an algorithm by which it appears that one can obtain a reasonable upper bound on C_t for any given value of t, and we present several open problems that we believe are worthy of investigation. This is joint work with Izabela Adamczak, Donald Kreher and Alan Ling.

A Very Basic Intoduction to Error Correcting Codes

Chris Rodger
235 Allison
Auburn University AL
USA 36849-5307
rodgec1@mail.auburn.edu

In this talk the basic ideas behind error correcting codes will be introduced. This will lead on to the introductory ideas used in encoding and decoding, and structures that aid in achieving these goals. The talk will probably reach a description of linear and cyclic codes.

The Graph Theoretical Approach to Convolutional Codes

Chris Rodger

In this second talk, a good introduction to convolutional codes will be given. Several ways of describing the codes will be given, but the main thrust of the talk will focus on a graph theoretical approach. This will provide a good visual method to discuss the decoding of these codes. Convolutional codes are used by NASA.

Encoding on Compact Discs

Chris Rodger

The third and final talk will focus on the use of error correcting codes in compact discs. This will begin with a description of how music is stored on CDs, then will move on to the Reed-Solomon codes, and the technique of interleaving that assists in handling long strings of errors.

Error and Deletion Correcting c-Secure Codes

Reihaneh Safavi-Naini
University of Wollongong, Australia
rei@uow.edu.au

Traceability schemes insert a fingerprint sequence in each copy of the data to provide protection against illegal copying. The aim of a c-traceability scheme is to identify at least one of the colluders if a pirate copy constructed by at most c colluders is found. Previous schemes are based on the assumption that the fingerprint in the pirate copy is of the same length as the original fingerprint. We relax this assumption and show how to trace colluders if the received fingerprint is shorter than the embedded one.

On the Number of Primitive Polynomials over Finite Fields

Peter J-S Shiue
University of Nevada
shiue@nevada.edu

Let F_q denote the finite field of order q, a power of a prime p and m be a positive integer. Denote ${P_q}^a(m)$ the number of primitive polynomials of degree m over F_q with trace a, where $a \in F_q$. The existence of primitive polynomials of arbitrary traces is guaranteed by Cohen [1] except for the cases ${P_4}^0(3) = {P_q}^0(2) = 0$.

Primitive polynomials are also used in the construction of linear feedback shift register sequences having the maximum possible period ([2]). In this paper, we discuss some results on the function ${P_q}^a(m)$. One of the main results is when the degree m is a multiple of $q-1$, ${P_q}^a(m)$ is constant for any nonzero trace a.

This talk is based on joint work with Yaotsu Chang of I-Shou University, Kaohsiung, Taiwan.

References

[1] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, Discrete Math. 83 (1990), 1-7.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, New York (1997).

An Upper Bound on the Chromatic Number of a Graph

Ladislav Stacho
Simon Fraser University

We present a simple upper bound on chromatic number of a graph that is related to the well-known Brook's theorem. As shown, our results is best possible in a sense that it is NP-complete problem to decide whether it can be decreased by one.

The Discrete Logarithm Problem: Theory and Cryptographic Applications

Douglas R. Stinson
University of Waterloo
dstinson@cacr.math.uwaterloo.ca

In this series of instructional lectures, we discuss several aspects of the discrete logarithm problem (DLP) and its applications in cryptography. We begin with an overview of the most important algorithms for the DLP, including the Shanks, Pollard rho, Pohlig-Hellman, and index calculus algorithms.

We then discuss the subgroup DLP in Z_p, and the elliptic curve DLP. Then we present several standard cryptographic protocols whose security depends on the intractability of various versions of the DLP. These include signature schemes standardized by NIST (DSA, ECDSA), as well as key exchange protocols (Diffie-Hellman) and public-key cryptosystems (ElGamal).

Two problems related to the DLP are introduced: the computational and decision Diffie-Hellman problems. Connections with the DLP are discussed, as well as the relevance of these problems to the security of the previously mentioned cryptographic protocols.

We give an elementary analysis of the complexity of generic algorithms for the DLP. We provide a simple proof of the lower bound of $\sqrt{n}$ group operations for the generic DLP in a subgroup of order n (a famous result of Nechaev and Shoup).

Finally, we discuss some recent results on the so-called low hamming weight DLP. Efficient algorithms for this problem make use of certain interesting new set systems which can be constructed from error-correcting codes.

A Backtracking Algorithm for Finding t-Designs

B. Tayfeh-Rezaie

Institute for Studies in Theoretical Physics and Mathematics (IPM)
P.O. Box 19395-5746*, Tehran, Iran*

Let t, k, v, and λ be integers such that $0 \leq t \leq k \leq v$ and $\lambda > 0$. Let V be a v-set and $P_k(V)$ be the set of all k-subsets (called *blocks*) of V. A t-(v, k, λ) *design* is a collection $\mathcal{D}$ of blocks of V such that every t-subset of V occurs exactly λ times in $\mathcal{D}$. The most used algorithm for finding t-designs is the backtracking algorithm. We present an improvement of the backtracking algorithm which is much faster than the original algorithm in finding t-designs with almost large t. We also introduce some intersection matrices for t-designs which are useful in the improved backtracking algorithm. For example, we have employed the algorithm to classify all 6-(14,7,4) designs with nontrivial automorphism groups and all 5-(14,6,3) designs admitting an automorphism of order seven.

Perfect Codes and Balanced Generalized Weighing Matrices

Vladimir D. Tonchev
Michigan Technical University
Houghton, MI 49931, USA
tonchev@mtu.edu
http://www.math.mtu.edu/∼tonchev

The 1-dimensional subspaces of the simplex code over $GF(q)$ yield a balanced generalized weighing (**BGW**) matrix over $GF(q)^*$. This matrix is characterized as the unique (up to monomial equivalence) BGW matrix with minimum q-rank. Linear shift register sequences of maximum period provide an explicit description in terms of the trace function. The classical BGW-matrices are discussed for comparison. A general construction that applies group automorphisms of $GF(q)^*$ yields monomially inequivalent BGW-matrices. A formula for the q-rank of these matrices is found.

Combinatorial Designs and Digital Communication

Vladimir D. Tonchev

The subject of this talk are some classes of combinatorial designs that arise naturally as the optimal solutions of problems in computer communication, optical and magnetic recording, and delay-insensitive communication in asynchronous systems.

On Cover-Free Families

R. Wei
Lakehead University
wei@ccc.cs.lakeheadu.ca

Cover-Free families were discussed in several equivalent formulations in subjects such as information theory, combinatorics and group testing by numerous researchers. Recently, cover-free families were also used for some cryptographic problems. In this talk, we will first briefly review known results about cover-free families and compare these results which are from different authors. Then we will define some generalized cover-free families and prove new results about these generalizations. Some open problems will also be mentioned.

Applications of a Numerical Sieving Device

Hugh Williams
University of Manitoba
williams@cs.umanitoba.ca

A numerical sieving device is a machine that finds solutions to systems of single-variable linear congruences with various moduli. The mechanism detects these solutions simply by searching through all the integers up to a certain, preselected bound. While this approach may sound very naive, in fact it is possible to make these devices execute at a very rapid rate. Furthermore, for solving certain problems the use of these machines is the fastest method known. In this talk I will provide a brief history of these devices and then go on to describe two recent applications of them. One of these applications is to an old problem concerning a certain character sum. The other is to the problem of finding quadratic polynomials with a high density of prime values.