The submitted abstracts are not refereed at this stage and
the authors are solely responsible for the claims made in their abstracts.

Invited Talks

How serious is Godel's incompleteness theorem?

Gregory Chaitin
IBM T.J. Watson Research Center
Yorktown Heights, NY
chaitin@us.ibm.com

This year is the centenary of Godel's birth, but we still do not know how seriously we should take his famous 1931 incompleteness theorem, and whether it implies that mathematics should be done somewhat differently. I will review Godel's original "I'm unprovable" proof, Turing's version deriving incompleteness from uncomputability, and my own approach to incompleteness based on notions of information, complexity and randomness, and I'll also discuss a new quasi-empirical approach to mathematics emphasizing the similarities between mathematics and physics rather than the differences.

Some Combinatorial Problems in Statistical Design of Experiments

Ching-Shui Cheng
Department of Statistics, University of California Berkeley
Berkeley, CA 94720-3860
cheng@stat.berkeley.edu

Experimental design is concerned with the planning of experiments to collect valid information as efficiently as possible. Combinatorial design, graph theory, finite geometry and coding theory provide important tools. I will review some of these connections. Examples will be provided to illustrate applications of results from these areas.

Vizings Conjecture on Domination and Related Problems

Bert Hartnell* and Doug Rall
Department of Mathematics & Computing Science, Saint Mary's University
Halifax, Nova Scotia, B3H 3C3 , Canada
Bert.Hartnell@smu.ca

One of the most tantalizing (and frustrating!) open problems in domination is that posed by V. G. Vizing in 1963. Namely, is the domination number of the Cartesian product of any two graphs at least as large as the product of the domination numbers? In 1968 he posed it as a conjecture and it appears as elusive as ever. Some of the attacks on this problem and related questions will be outlined.

Graph Reconstruction by Permutations

William Kocay* and Pierre Ille
Department of Computer Science, University of Manotoba
Winnipeg, MB, Canada R3T 2N2
bkocay@cc.umanitoba.ca

Let G and H be graphs with a common vertex set V, such that $G-i$ is isomorphic to $H-i$, for all $i \in V$. The Graph Reconstruction Conjecture states that G and H must be isomorphic graphs in this situation, whenever $|V| \geq 3$. We study the graph reconstruction problem from the point of view of the isomorphism mappings relating $G-i$ and $H-i$. Let p_i be the permutation of $V-i$ that maps $G-i$ to $H-i$, and let q_i denote the permutation obtained from p_i by mapping i to i. It is shown that certain algebraic relations involving the edges of G and the permutations $q_i q_j^{-1}$ and $q_i q_k^{-1}$, where $i, j, k \in V$ are distinct vertices, often force G and H to be isomorphic. The relations between the algebra and combinatorics of graph reconstruction are investigated.

My Conjectures on Edge-graceful Trees

Sin-Min Lee
Department of Computer Science, San Jose State University
San Jose, California 95192
sin_min_lee@yahoo.com

Given a (p,q)-graph G, an edge graceful labeling of G is a one-to-one map from set of all edges of G to the positive integers $\{1, 2, \cdots, q\}$ such that, for every vertex x of G, the sum of the labels on all edges containing it $\pmod p$ are distinct. These labelings have been constructed for many families of graphs. We give here a survey of theory of edge-graceful graphs. I conjectured that all trees of odd orders admit edge-graceful labelings twenty years ago. The progress of some of my conjectures in these fields will be reported.

More on Decompositions of Edge-Colored Complete Graphs

Richard M. Wilson
Department of Mathematics, California Institute of Technology
Pasadena, CA 91125
rmw@its.caltech.edu

Given a simple graph G with m edges, let d be the greatest common divisor of the degrees of its vertices. With finitely many exceptions, the edge set of the complete graph K_n on n vertices can be partitioned into (edge-disjoint but not necessarily vertex-disjoint) copies of G provided that $n(n-1) \equiv 0 \pmod{2m}$ and $n-1 \equiv 0 \pmod{d}$. This is a result of this writer from 1975.

We are concerned with extensions of this result. Many combinatorial problems can be seen to be equivalent to certain decompositions of edge-colored complete graphs, $K_n^{(\lambda_1,\ldots,\lambda_r)}$ in which any two distinct vertices are joined by λ_i edges of color i, $i = 1, 2, \ldots, r$. In general, we are given a family $\mathcal{G}$ of graphs whose edges are colored with elements of $\{1, 2, \ldots, r\}$ and we wish to find a family of subgraphs of $K_n^{(\lambda_1,\ldots,\lambda_r)}$, each isomorphic to a member of $\mathcal{G}$, so that each edge of the complete graph is in exactly one of the subgraphs.

For the case when the graphs in $\mathcal{G}$ are simple (i.e. have at most one edge of color i joining any two distinct vertices, $i = 1, 2, \ldots, r$), necessary and asymptotically sufficient conditions on n in term of $\mathcal{G}$ were given by E. Lamken and the writer in 2000. At the time, we thought this would be sufficient for all reasonable applications to problems in design theory, but it became apparent that it would be useful to have results for the case when the graphs in $\mathcal{G}$ are not necessarily simple.

We can give an answer (necessary and asymptotically sufficient conditions for the existence of a decomposition) in the general case, but it is much more complex, computationally. This is joint work with Anna Draganova and Yukiyasu Mutoh. Recently, we have extended our results to directed edge-colored graphs.

We will give examples of combinatorial problems that can be put into this framework, give a precise description of the main result, and briefly discuss certain points of the proof.

Contributed Talks

Random Logistic Modeling

Reza Ahangar and Ernest Ballenger*
Department of Mathematics, Kansas Wesleyan University
Salina, Kansas 67401-6196
ballengerern@yahoo.com

It is well known that the environment cannot provide unlimited resources and it is subject to random changes. A discrete dynamical system that can describe a population density in a deterministic environment is

$$P_{n+1} = p_n(1 + A - BP_n) \text{ and } P(0) = P_0, \tag{0.1}$$

where A is the growth rate per individual in the absence of over-population pressures, and BP_n the overcrowded population force factor which reduces the birth rate. If P_n represents the population at stage n then by (0.1) the population can be determined in the $(n+1)$ stage. Suppose, in a simple case, that random variation causing change in the population is linearly proportional to the population

$$W_n = rP_n \tag{0.2}$$

for a random number $0 \leq r \leq 1$. By discrete systems (0.1) and (0.2), we introduce a random logistic model

$$P_{n+1} = p_n(1 + A - BP_n) + W_n \text{ and } P(0) = P_0. \tag{0.3}$$

The solution to this random difference equation will be studied. The stability of the equilibrium point will also be investigated. We will use an algorithmic approach and computer algebra system to introduced a curve fitting method to random logistic data.

On Integer-Magic Spectra of Trees

Ebrahim Salehi and Patrick Bennett*
Department of Mathematical Sciences, University of Nevada Las Vegas
Las Vegas, NV 89154-4020
pbennett9@gmail.com

For any $h \in \mathbb{N}$, a graph $G = (V, E)$ is said to be h-magic if there exists a labeling $l : E(G) \to \mathbb{Z}_h - \{0\}$ such that the induced vertex set labeling $l^+ : V(G) \to \mathbb{Z}_h$ defined by

$$l^+(v) = \sum_{uv \in E(G)} l(uv)$$

is a constant map. For a given graph G, the set of all $h \in \mathbb{Z}_+$ for which G is h-magic is called the integer-magic spectrum of G and is denoted by $IM(G)$. In this presentation, the integer-magic spectra of trees of diameter five and caterpillars will be discussed.

On Integer-Magic Spectra of the Generalized Theta Grphs

Dharam V. Chopra*, Sin-Min Lee, and Hugo Sun
Department of Mathematics & Statistics, Wichita State University
Wichita, KS 67260-0033
dharam.chopra@wichita.edu

For k>0, we call a graph G=(V,E) as Z_k-magic if there exists a labeling l:E(G)→ Z_k* such that the induced vertex set labeling l^+: V(G)→ Z_k defined by l^+(v)=Σ {l(u,v) : (u,v) in E(G)} is a constant map. We denote the set of all k such that G is k-magic by IM(G). We call this set as the **integer-magic spectrum** of G. The theta graph $\Theta(l_1,l_2,\ldots,l_k)$ is the graph consisting of k pairwise internally disjoint paths with common end vertices and length $l_1,l_2,\ldots,l_k$. We determine the integer-magic spectra of all generalized theta graphs.

Generalized Pseudo-Characteristic of $K_{p,q,r}$

Chao-Chih Chou* and Chin-Mei Fu
St. John's University
Tamsui, Taipei Shien, Taiwan, ROC
chao@mail.sju.edu.tw

Let G be a graph and T be a decomposition of $2G$ into cycles, say $2G = m_1C_{k_1} + m_2C_{k_2} + \cdots + m_tC_{k_t}$. Then the Euler characteritic $\chi_T(G)$corresponding to the decomposition T is given by $\chi_T(G) = |V(G)| - |E(G)| + m_1 + m_2 + \cdots + m_t$.
The generalized pseudo-characteristic of G is given by
$\chi''(G) = max\{\chi_T(G)|T$ is a decomposition of $2G$ into cycles$\}$ Then

$$\chi''(K_{p,q,r}) = \begin{cases} (p+q+r) - [(p+q)r+1]/2 & \text{if } (p+q)r \text{ is odd.} \\ (p+q+r) - (p+q)r/2 & \text{otherwise.} \end{cases}$$

On the Super Edge-Graceful Trees of Even Orders (II)

Ping-Tsai Chung*, Sin-Min Lee, Wen-Ying Gao and Karl Schaffer
Department of Computer Science, Long Island University
Brooklyn, New York 11201
pchung@liu.edu

A (p,q)-graph G is said to be edge graceful if the edges can be labeled by $1, 2, \cdots, q$ so that the vertex sums are distinct $\pmod p$. It is shown that if a tree T is edge-graceful then its order must be odd. Lee conjectured that all trees of odd orders are edge-graceful. J. Mitchem and A. Simoson introduced the concept of super edge-graceful graphs which is a stronger concept than edge-graceful for some classes of graphs. A graph $G = (V, E)$ of order p and size q is said to be super edge-graceful if there exists a bijection
$f : E \to \{0, \pm1, \pm2, \cdots, \pm(q-1)/2\}$ if q is odd
$f : E \to \{\pm1, \pm2, \cdots, \pm q/2\}$ if q is even
such that the induced vertex labeling f^* defined by $f^*(u) = \Sigma\{f(u,v) : (u,v) \in E\}$ has the property:
$f^* : V \to \{0, \pm1, \pm2, \cdots, \pm(q-1)/2\}$ if q is odd
$f^* : V \to \{\pm1, \pm2, \cdots, \pm q/2\}$ if q is even
is a bijection. The conjecture is still unsettled. In this paper we exhibit trees of even orders which are super edge-graceful.

On the Connectivity of Unbordered Words in the N-Cube

Larry J. Cummings
Department of Mathematics, University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1
ljcummin@math.uwaterloo.ca

We consider finite words, or strings, over the binary alphabet. A word w is unbordered if $w = xy = zx$ for non-empty words x, y, z always implies x is empty. No periodic word can be bordered. The set of unbordered binary words of length n form two disjoint subgraphs in the n-cube. A word w is primitive if it is not of the form $w = u^k$ for some integer $k > 1$. A primitive word is a Lyndon word if it is lexicographically least in its cyclic equivalence class. Every Lyndon word is unbordered but the converse is not true. We discuss the conjecture that every unbordered word which is not a Lyndon word is at Hamming distance 1 from at least one Lyndon word in the N-cube.

On the Number of Linear Independent Vectors Over a Finite Field of Prime Order

Steve Damelin*, G. Mullen, V. Reiner, G. Michalski, and J. Taylor
Department of Mathematical Sciences, Georgia Southern University
Statesboro, GA 30460-8093
damelin@ima.umn.edu

Given a set of n vectors over a finite field of prime order (for simplicity one might consider the binary case where we work with vectors with entries 0s and 1's), we are interested in counting the number of vectors from this class which are linear independent $k \leq n$ at a time. Applications to combinatorial designs, graphs, coding and net designs will be discussed.

Discrete Computational Approach for a Lethal Recessive Gene of Cystic Fibrosis

Reza Ahangar and Paul Dierks*
Department of Mathematics, Kansas Wesleyan University
Salina, Kansas 67401-6196
paudie@kwu.edu

Cystic Fibrosis is a genetic disease, which threatens about thirteen million of the U.S population with about 500 deaths every year. A healthy gene {G} will be mutated to a gene {g} which is a recessive gene that causes the disease. The mutant gene initially will appear in the next generation in the form of genotypes GG-normal, Gg-hybrid or carrier, and gg-recessive. A nonlinear difference equation model will be developed. The behavior of the solution of the systems of equations will be studied in several sub-populations of white, black, and Asian carriers. We apply some numerical algorithms to analyze the frequency of the recessive allele of the Cystic Fibrosis gene in population vs. carrier gene. We discuss the behavior of the system by imputing variables of the probability of two carriers mating, the probability of production of carriers, and the probability of diseased infants. The termination of the disease in the population is based on assumptions i) no new mutations of the gene arise, ii) a fraction r of the GG and Gg newborn genotypes survive to the end of the generation, but non of the gg genotypes survive to adulthood. The computational simulation will help us to show how the evolution slowly but surely will clean up the population from this deadly disease.

On the Edge-Magicness of Zykov Sum of Graphs

Dharam Chopra, Rose Dios*, and Sin-Min Lee
Department of Mathematical Sciences, New Jersey Institute of Technology
Newark, New Jersey 07102
dios@adm.njit.edu

A (p,q)-graph G in which the edges are labeled $1, 2, 3, \cdots, q$ so that the vertex sums mod p is a constant, then G is called edge-magic. In this paper, we investigate edge-magic (p,q)-graphs G which are of the form $G_1 + G_2$. Using the Zykov sum construction of graphs we provide infinite families of edge-magic graphs. A conjecture is proposed in this paper.

Judgment Aggregation and the Greedy Algorithm

Christopher Earles
Department of Mathematical Sciences, Bethel College
North Newton, Kansas 67117
cearles@bethelks.edu

The judgment aggregation problem is an extension of the group decision making problem, wherein each voter votes on a set of propositions which may be logically interrelated (such as p, $p \to q$, and q). The simple majority rule can yield an inconsistent set of results, so more complicated rules must be developed. Here I cast the problem in terms of matroids and apply the Greedy Algorithm to obtain a "best" result.

Some Suggestions for Nonabelian Group Based Cryptography

Benjamin Fine*, Gilbert Baumslag, and Gerhard Rosenberegr
Department of Mathematics, Fairfield Unviersity
Fairfield, CT 06840
Ben1902@aol.com

The Anshel-Anshel-Goldfeld and Ko-Lee cryptosystems initiated a broad line of research into cryptosystems based on nonabelian groups. The main source of platforms for such systems are combinatorial group theory and linear groups. In this talk we present three general schemes for using combinatorial group theory to develop encryption protocols. We also mention potential platforms for use with these systems. One first method is a translation to the nonabelian group theoretic setting of the classical Diffie-Hellman protocol. The second is a similar translation but to a noncommutative ring format. Here a power series ring in several noncommuting variables provides a very flexible platform. The final system is based on the difficulty of identifying different free subgroups of a given finitely presented group. Fine-Baumslag and Xu developed a system based on this using the Modular Group as a platform.

Computer Simulation for Mutation and Natural Selection in Tri-Allele Genotypes

Reza Ahangar and Janet A. Franklin*
Department of Mathematics, Kansas Wesleyan University
Salina, Kansas 67401-6196
janfran55@sbcglobal.net

The principles of Darwinian evolution are based on variation and natural selection. Assuming there are three types of alleles $\{G, B, R\}$, the colors green, blue and red will represent G, B, and R respectively. Let $g(n)$, $b(n)$, and $r(n)$ be the proportions of G-, B-, and R-alleles in generation (n). A discrete dynamical system will be developed to find the proportions of $g(n+1)$, $b(n+1)$, and $r(n+1)$ for the next generation. The behavior of the dynamical system and the stability of the equilibrium point of the system will be studied. Numerical simulation and graphical descriptions of the model will be presented. Examples of the evolution of the dynamical system with mutation and natural selection of advantageous genes will be demonstrated

Orthogonal Double Covers of Complete Graphs by Lobsters of Diameter 5

Dalibor Froncek
Department of Mathematics and Statistics University of Minnesota
Duluth, MN 55812-3000
dalibor@d.umn.edu

An orthogonal double cover (ODC) of the complete graph K_n by a graph G is a collection $\mathcal{G} = \{G_i | i = 1, 2, \ldots, n\}$ of spanning subgraphs of K_n, all isomorphic to G, with the property that every edge of K_n belongs to exactly two members of $\mathcal{G}$ and any two distinct members of $\mathcal{G}$ share exactly one edge.

A lobster of diameter five is a tree arising from a double star by attaching any number of pendant vertices to each of its vertices of degree one. We show that for any double star $R(p, q)$ there exists an ODC of K_n by all lobsters of diameter five (with finitely many possible exceptions) arising from $R(p, q)$.

Alliance Partition Number in Graphs

Linda Eroh and Ralucca Gera*
Department of Applied Mathematics, Naval Postgraduate School
Monterey, CA 93943
rgera@nps.edu

Let G be a graph with vertex set $V(G)$ and edge set $E(G)$. A defensive alliance in G is a subset S of $V(G)$ such that for every vertex $v \in S$, $|N[v] \cap S| \geq |(V(G) - N[v]) \cap S|$. A global defensive alliance is an alliance that is also a dominating set. We define the *alliance partition number, ap*(G) *(global alliance partition number, gap*(G)*)*, to be the maximum number of sets in a partition of $V(G)$ such that each set is a defensive alliance (gloabal defensive alliance). In this paper, we give both general bounds and exact results for the alliance partition number and for the global alliance partition number, as well as connection between the two.

Solving Discrete Logs from Partial Knowledge of the Key

K. Gopalakrishnan*, Nicolas Theriault, and Chui Zhi Yao
Department of Computer Science, East Carolina University
Greenville, NC 27858-4353
GOPAL@ECU.EDU

For Elliptic Curve based Cryptosystems, the discrete logarithm problem must be hard to solve. But even when this is true from a mathematical point of view, there are other aspects to take into account for practical applications. If proper countermeasures are not used, side-channel attacks could be used to reveal information about the key. If the whole key is revealed, then the security problem is obvious. In this talk, we consider the situation when a side channel attack reveals only partial information about the key.

We provide algorithms to solve the discrete log problem for generic groups with partial knowledge of the key, which are considerably better than using a square-root attack on the whole key and an exhaustive search using the extra information, under two different scenarios. In the first case, we assume that a sequence of contiguous bits of the key is revealed. In the second case, we assume that (incomplete) information on the "Square and Multiply Chain" is revealed.

On a Question of Sós About 3-Uniform Friendship Hypergraphs

Stephen G. Hartke* and Jennifer Vandenbussche
Department of Mathematics, University of Illinois
Urbana-Champaign, IL 61801
hartke@math.uiuc.edu

The well-known Friendship Theorem states that if G is a graph in which every pair of vertices has exactly one common neighbor, then G has a single vertex joined to all others (a "universal friend"). This property uniquely defines the graph for a given number of vertices. V. Sós defined an analogous friendship property for 3-uniform hypergraphs, and gave a construction satisfying the friendship property that has a universal friend. She also asked whether any other 3-uniform hypergraphs satisfy the friendship property. We answer this question affirmatively by demonstrating hypergraphs without a universal friend that satisfy the friendship property. These hypergraphs were found using integer programming.

An Anonymous e-Voting Algorithm with Partial PKI solution

Wen-Jung Hsin
Information and Computer Science, Park University
Parkville, MO 64152
wen.hsin@park.edu

In this paper, we propose an Electronic Voting (e-Voting) scheme that provides functionality closely resembling to a paper voting scheme without the need of a global PKI support. Our proposed scheme is efficient in that the computation load for establishing an e-Vote is distributed into off-line and on-line phases, and the on-line signature generation requires only a linear modular computation. The proposed scheme offers many prominent security features, including voter's identity anonymity, unforgeable e-Vote, unlinkable signature, external and internal undeniability, unusable lost or stolen e-Vote, and double casting resolvability.

The number of 4-cycles in 2-factorizations of $K_{n,n}$

Yo-Feng Hsu and Wen-Chung Huang*
Department of Mathematics, Soochow University
Taipei, Taiwan, Republic of China.
wchuang@math.scu.edu.tw

A 2-factor of the complete bipartite graph $K_{n,n}$ is a 2-regular spanning subgraph of $K_{n,n}$. A 2-factorization of $K_{n,n}$ is a partition of the edge set of $K_{n,n}$ into 2-factors. Let $Q(n)$ be the set of all x such that there exists a 2-factorization of $K_{n,n}$ containing exactly x 4-cycles. And we define

$$FC(n) = \begin{cases} \{0, 1, \ldots, n^2/4 - 2, n^2/4\} & \text{if } n \text{ is even,} \\ \{0, 1, \ldots, (n-1)(n-3)/4\} & \text{if } n \text{ is odd.} \end{cases}$$

In this talk, we will discuss the identity $Q(n) = FC(n)$.

Some Results on Total Domination Critical Graphs

Doost Ali Mojdeh and Nader Jafari Rad*
Department of Mathematics, University of Mazandaran
Babolsar, IRAN, P.O. Box 47416-1467
n.jafarirad@umz.ac.ir

A graph G with no isolated vertex is total domination vertex critical if for any vertex v of G that is not adjacent to a vertex of degree one, the total domination number of $G - v$ is less than the total domination number of G. These graphs we call γ_t-critical. If such a graph G has total domination number k, we call it k-γ_t-critical. We verify an open problem of k-γ_t-critical graphs and obtain some results on the characterization of total domination critical graphs of order $\Delta(G) + \gamma_t(G)$.

A-magic Cartesian Products

Dawn M. Jones
Department of Mathematics, SUNY Brockport
Brockport, NY 14420
djones@brockport.edu

In this talk we will discuss certain cartesian products of A-magic and non A-magic graphs. In particular we will focus on cartesian products of trees with regular or nearly-regular graphs.

Exact Maximum Expected Differential and Linear Probability for 2-Round Advanced Encryption Standard

Liam Keliher* and Jiayuan Sui
Department of Mathematics and Computer Science, Mount Allison University
New Brunswick, Canada E4L 1E6
lkeliher@mta.ca

A block cipher is a fundamental cryptographic primitive that is often used for the encryption of large volumes of data. The most powerful attacks against block ciphers are generally considered to be differential cryptanalysis and linear cryptanalysis. Provable security against differential (resp. linear) cryptanalysis requires showing that the maximum expected differential (resp. linear) probability, MEDP (resp. MELP), over 2 or more rounds is sufficiently small. Over the past few years, several papers have provided increasingly tight upper and lower bounds on these values for 2 rounds of the Advanced Encryption Standard (AES), a block cipher standardized by the U.S. government that is one of the most widely used ciphers worldwide. In this work, we determine the exact values of the 2-round MEDP and MELP for the AES. This immediately gives us the best known upper bounds on the AES MEDP and MELP for 4 or more rounds.

The Computational Complexity of Balanced Labelings

M. Kong*, Sin-Min Lee, Eric Seah, and Alfred S. Tang
Department of EE and Computer Science, University of Kansas
Laurence, Kansas 66045
kong@eecs.ku.edu

Let G be a graph with vertex set V(G) and edge set E(G), and let A ={0,1}. A labeling f : V(G) $\rightarrow$ A induces an edge partial labeling f* : E(G) $\rightarrow$ A defined by f*(xy) = f(x),if and only if f(x)=f(y) for each edge xy $\in$ E(G). For i $\in$ A, let v_f(i) = card{v $\in$ V(G) : f(v) = i} and e_f*(i) = card{e $\in$ E(G) : f*(e) = i}. A labeling f of a graph G is said to be friendly if $|$ v_f(0) - v_f(1) $| \leq$ 1. If $|$ e_f(0) - e_f(1) $| \leq 1$ then G is said to be **balanced**. A necessary and sufficient condition for balanced graphs is given. We also show that to decide whether a graph admits a balance labeling is NP-complete.

On Friendly Index Sets of Generalized Books

Harris Kwong* and Sin-Min Lee
Department of Mathematical Sciences, State University of New York at Fredonia
Fredonia, NY 14063
kwong@cs.fredonia.edu

Let G be a graph with vertex set V(G) and edge set E(G). A labeling f : V(G) $\rightarrow$ Z_2 defined by f*(xy) = f(x) + f(y), for each edge xy $\in$ E(G). For i $\in$ Z_2, let v_f(i) = card{v $\in$ V(G) : f(v) = i} and e_f(i) = card{e $\in$ E(G) : f*(e) = i}. A labeling f of a graph G is said to be friendly if | v_f(0) - v_f(1) | $\leq$ 1.The friendly index set of the graph G, The balance index set of the graph G, BI(G), is defined as {| e_f(0) - e_f(1)| : the vertex labeling f is friendly}. We consider the friendly index sets of generalized books.

Spanning Cycles in Regular Matroids Without $M^*(K_5)$ Minors

Hong-Jian Lai*, B. Liu, Y. Liu and Y. Shao
Department of Mathematics, West Virginia University
Morgantown, WV 26506
hjlai@math.wvu.edu

Catlin and Jaeger proved that the cycle matroid of a 4-edge-connected graph has a spanning cycle. This result can not be generalized to regular matroids as there exist infinitely many connected cographic matroids, each of which contains a $M^*(K_5)$ minor and has arbitrarily large cogirth, that do not have spanning cycles. In this paper, we proved that if a connected regular matroid without a $M^*(K_5)$-minor has cogirth at least 4, then it has a spanning cycle. This is a joint work with B. Liu, Y. Liu and Y. Shao.

Combinatorial Methods for the Analysis of Learning Problems

Andrew C. Lee
Computer Science Department, University of Louisiana at Lafayette
Lafayette, LA 70504-1771
cxl9999@louisiana.edu

Let X be a non-empty set and $C \subset 2^X$. One may think of X as the collection of encodings of all instances in a learner's universe. Given some rules of interest, the collections of instances that positively exemplify them are simply subsets of X. Hence, each subset of X is termed as a *concept* and the object C is often referred as a *concept class* in computational learning theory.

It is plausible that some combinatorial properties of C may help the study of learning. One well known example is Vapnik Chervonenkis dimension. It assigns to each concept class a single number which helps to determine the sample size needed to learn the concepts in C. Motivated by these developments, in this talk we will review some notions of computational learning theory and their connections with the combinatorial properties of a set system C.

On Balancedness of Some Graph Products

Suh-Ryung Kim, Sin-Min Lee* and Ho Kuen Ng
Department of Computer Science, San Jose State University
San Jose, California 95192
sin_min_lee@yahoo.com

Balancedness of the Cartesian product and composition of graphs is studied in the paper S-M. Lee, A. Liu and S.K. Tan, On balanced graphs, Congressus Numerantium, **87** (1992), 59-64. We provide some new families of balanced graphs using product constructions. An example is shown that tensor product of two balanced graphs need not be balanced.

Removing Guilt By Association with Additive Homomorphic Encryption Schemes in Symmetric Private Information Retrieval Protocols

Laura Beth Lincoln
Department of Computer Science, Rochester Institute of Technology
Rochester, Rochester, NY 14623
lbl6598@cs.rit.edu

Suppose you are interested in watching pay-per-view, but are scared that the cable company will sell your information, or the association of your name to that purchase could hinder your career, relationships, or increase the amount of time you spend cleaning SPAM out of your mailbox. Private Information Retrieval (PIR) will allow you to retrieve a particular feed without the supplier knowing which feed you actually received, and Symmetric Private Information Retrieval (SPIR) will assure the supplier that you received only the feed you purchased. Now the paranoid buyer can purchase without risking his good name, and the supplier can harvest the cash of the once paranoid customer. This paper will present how additive homomorphic probabilistic encryption schemes, such as Paillier's, can be used in a one round SPIR protocol, and present a protocol that improves upon those that have been previously published.

Weights Modulo a Prime Power in Divisible Codes and a Related Bound

Xiaoyu Liu
Department of Mathematics and Statistics, Wright State University
Dayton, OH 45435-0001
xliu@math.wright.edu

A divisible code is a linear code whose codewords all have weights divisible by some integer larger than 1. In this paper, we generalize the theorem give by R. M. Wilson about weights modulo p^t in linear codes to a divisible code version. Using a similar idea, we give an upper bound for the dimension of a divisible code by some divisibility property of its weight enumerator modulo p^e. We also prove that this bound implies Ward's bound for divisible codes. Moreover, we see that in certain cases, our bound gives better results than Ward's bound.

On the Edge-Graceful Spectra of the Cylinder Graphs

Sin-Min Lee, Claude Levesque, Sheng-Ping Bill Lo* and Karl Schaffer
Cisco Systems, Inc., 170, West Tasman Drive
San Jose, CA 95134
bill_lo1@hotmail.com

Let G be a (p,q)-graph and k≥0. A graph G is said to be ***k-edge graceful*** if the edges can be labeled by k,k+1,...,k+q-1 so that the vertex sums are distinct, mod p. We denote the set of all k such that G is k-edge graceful by egI(G). The set is called the **edge-graceful spectrum** of G. In this paper the problem of what sets of natural numbers are the edge-graceful spectra of cylinder graphs is studied.

The Edge-graceful Spectra of Connected Bicyclic Graphs Without Pendant

W.C. Shiu, M.H. Ling, and Richard M. Low*
Department of Mathematics, San Jose State University
San Jose, CA 95192
low@math.sjsu.edu

Let G be a (p,q)–graph and k a non-negative integer. G is k–edge-graceful if the edges of G can be labeled with $k, k+1, \ldots, k+q-1$ so that the vertex sums are distinct modulo p. The set of all such k where G is k–edge-graceful is called the edge-graceful spectrum of G. We determine the edge-graceful spectra of connected bicyclic graphs without pendant.

Fall Coloring of Cartesian Products of Graphs

Renu Laskar, Jeremy Lyle*
Department of Mathematical Sciences, Clemson University
Clemson, SC 29634-0975
slyle@clemson.edu

The question of whether a graph can be partitioned into k independent dominating sets is considered. For $k = 3$, it is shown that a graph G can be partitioned into three independent dominating sets if and only if the cartesian product $G \Box K_2$ can be partitioned into three independent dominating sets. The graph K_2 can be replaced by any graph H such that $f : Q_n \to H$, where f is a *type-II* graph homomorphism. Included in this set is any cartesian product of any number of paths and stars on any number of vertices.

The cartesian product of two trees is considered, as well as the complexity of partitioning a bipartite graph into three independent dominating sets, which is shown to be NP-complete. For other values of k, repeated cartesian products are considered, leading to a result which gives the possible values of k for which the hypercubes can be partitioned into k independent dominating sets.

Graceful Labelings of Directed Graphs

Alison M. Marr
Department of Mathematics, Southern Illinois University
Carbondale, IL 62901-4408
amarr@siu.edu

A directed graph D with e edges has a graceful labeling if there exists $\theta : V(D) \to \{0, 1, \ldots, e\}$ s.t. $\theta(y) - \theta(x) \bmod (e+1)$ is distinct (and nonzero) for every $(x, y) \in E(D)$. This talk will examine some properties of graceful digraphs and then explore some new results for certain classes of digraphs.

Strong Vertex-Magic and Edge-Magic Total Labelings of 2-Regular Graphs

Dan McQuillan
Department of Mathematics, Norwich University
Northfield VT 05663
dmcquill@norwich.edu

A total labeling of a graph is a bijective assignment of integers $1, 2, \cdots, |V| + |E|$ to the vertices and edges of the graph. The weight of an edge is the sum of its label and its two end vertex labels. The weight of a vertex is the sum of its label and all of its incident edge labels. A total labeling is edge-magic if the weight of every edge is the same. The labeling is vertex-magic if the weight of each vertex is the same. For 2-regular graphs, it is an easy matter to obtain a vertex-magic total labeling from an edge-magic total labeling and vice-versa. A vertex-magic total labeling is said to be strong if the largest labels are on the vertices. We introduce a new method for the construction of strong vertex-magic total labelings for certain disconnected 2-regular graphs. However, there is still much work to be done. We will a highlight a few open problems.

Configurations and Symmetries in Classical Geometry

James M. McQuillan* and Aiden A. Bruen
Department of Computer Science, Western Illinois University
Macomb, IL, 61455
JM-McQuillan@wiu.edu

We investigate various questions relating to configurations in classical planes. One such question is the following: Given two triangles in perspective from a point V, is it possible that V is on the Desargues line?

A Note on Non-Regular Planar Graphs

Nutan Mishra*, Dinesh Sarvate, Adrienne Chisholm, and Jesse J. Raab
Department of Math and Statistics, University of South Alabama
Mobile AL 36688
NMishra@usouthal.edu

We give constructive and combinatorial proofs to decide why certain families of slightly irregular graphs have no planar representation and why certain families have such planar representation. Several non-existence results for infinite families as well as for specific graphs are given, for example the nonexistence of the graphs with $n = 11$ and degree sequence $(4, 5, 5, .., 5)$ and $n = 13$ and degree sequence $(6, 5, 5, ..., 5)$ is shown.

On the Balance Index Sets of Graphs

Alexander Nien-Tsu Lee, Sin-Min Lee, and Ho-Kuen Ng*
Department of Mathematics, San Jose State University
San Jose, CA 95192
ng@math.sjsu.edu

Let G be a graph with vertex set $V(G)$ and edge set $E(G)$, and let $A = \{0, 1\}$. A labeling $f : V(G) \to A$ induces a partial edge labeling $f^* : E(G) \to A$ defined by $f^*(xy) = f(x)$, if and only if $f(x) = f(y)$, for each edge $xy \in E(G)$. For $i \in A$, let $v_f(i) = card\{v \in V(G) : f(v) = i\}$ and $e_{f^*}(i) = card\{e \in E(G) : f^*(e) = i\}$. A labeling f of a graph G is said to be friendly if $|vf(0) - vf(1)| \leq 1$. If, $|e_f(0) - e_f(1)| \leq 1$ then G is said to be balanced. The balance index set of the graph G, BI(G), is defined as $\{|ef(0)ef(1)| :$ the vertex labeling f is friendly$\}$. Results parallel to the concept of friendly index sets are presented.

On the Integer-Magic Spectra of Eulerian Graphs of Odd Sizes

Sin-Min Lee and Kam-Chuen Ng*
Eastman Kodak Company
Rochester, NY 14650-2216
kam.ng@kodak.com

For k>0, we call a graph G=(V,E) as Z_k-magic if there exists a labeling l:E(G)→ Z_k* such that the induced vertex set labeling l^+: V(G)→ Z_k

l^+(v)=Σ {l(u,v) : (u,v) in E(G)}

is a constant map. We denote the set of all k such that G is k-magic by IM(G). We call this set as the **integer-magic spectrum** of G. Low and Lee showed that the integer-magic spectrum for any eulerian graph G of even size is equal to N. In this paper we investigate integer-magic spectra of some eulerian graphs of odd sizes.

Switching Operations for Hadamard Matrices and D-Optimal Designs

William P. Orrick
Department of Mathematics, Indiana University
Bloomington, Indiana 47405
worrick@indiana.edu

I will discuss the creation of new combinatorial designs from old. If one's goal is to produce a design with parameters for which no design was previously known, one strategy is to try to combine known designs with smaller parameters in a clever way so as to produce a new design with the parameters in question. Many constructions along these lines have been discovered over the years. On the other hand, if one wishes to produce many non-equivalent designs with the same parameters, a possible strategy is to try to modify an existing design with those parameters so as to produce a design in a different equivalence class. In this talk, I will describe a number of elementary moves that are very useful for doing exactly this. My main example will be Hadamard matrices, but I will also discuss block designs and D-optimal designs. I expect these moves, called "switching operations" to be very useful in the classification of designs. Applying these to Hadamard matrices of order 36, one can easily produce tens of millions of equivalence classes.

New One-way Compression Function for Cryptographic Hash Applications

Dhiren R. Patel
Computer Engineering Department, National Institute of Technology,
Surat Gujarat India 395007
dhiren29p@gmail.com

One-way *hash function* is a transformation (with inherent size reduction) that takes input of arbitrary length and returns a fixed size string h (*usually referred as hash code, hash value, message digest, thumbprint or fingerprint*).

$$H : \{0,1\}^* \to \{0,1\}^n$$

A hash function is chosen such that it is *computationally infeasible* to find an input that produces a given hash output. Further, it is very difficult to modify the input message such that the modified message has the same hash as the original message. This property is crucial for the convenient authentication of large amount of information. Thus hash functions speed up the *data integrity verification process.*

We introduce a new one-way compression function that is useful for design of cryptographic hash function and various cryptographic applications, viz. data and software integrity, RNG, one-way function, entity authentication etc. For core compression, we use C-SAT expressions in a novel CNF matrices form. We apply a variant of the Merkle-Damgard transformation to extend H to arbitrarily long inputs. Due to elegant design and very simple operations; in computation of digest, its efficiency is greater.

Security of this function is directly related to the properties of Clause Satisfiability (C-SAT) Problems. We argue that defeating this function is equivalent to solve instances of NP hard problems. Along with provable security, significant simplicity is maintained due to straight forward computation flow and absence of complex arithmetic operations. Scalable variants of this hash function can be generated to cater applications of different security requirement and levels.

On Distance Two Magicness of Graphs

Ebrahim Salehi
Department of Mathematics, University of Nevada Las Vegas
Las Vegas, NV 89154-4020
salehi@unlv.nevada.edu

Given an abelian group A, a graph $G = (V, E)$ is said to have a distance k magic labeling in A if there exists a labeling $l : E(G) \to A - \{0\}$ such that the induced vertex labeling $l^* : V(G) \to A$ defined by $l^*(v) = \sum_{e \in E_k(v)} l(e)$ is a constant map, where $E_k(v) = \{e \in E(G) : d(v, e) < k\}$. The set of all $h \in \mathbb{Z}_+$ for which G has a distance two magic labeling in $\mathbb{Z}_h$ is called the distance k magic spectrum of G and is denoted by $D_kM(G)$. In this talk, the distance two magic spectra of certain classes of graphs will be discussed.

On the Balance Index Sets of One-point Unions of Graphs

Harris Kwong, Sin-Min Lee, and Dinesh Sarvate*
Department of Mathematics, College of Charleston
Charleston, SC 29424
sarvated@cofc.edu

Let G be a graph with vertex set V(G) and edge set E(G), and let A ={0,1}. A labeling f : V(G) $\to$ A induces an edge partial labeling f* : E(G) $\to$ A defined by f*(xy) = f(x),if and only if f(x)=f(y) for edge xy $\in$ E(G). For i $\in$ A, let v_f(i) = card{v $\in$ V(G) : f(v) = i} and e_{f^*}(i) = card{e $\in$ E(G) : f*(e) = i}. G is said to be a balanced graph or G is balanced, if there is a vertex labeling f of G that satisfies the following conditions :
(i) | v_f(0)-v_f(1)| $\leq$ 1 and
(ii) | e_f(0)-e_f(1) | $\leq$ 1.
The balance index set of the graph G, BI(G), is defined as {| e_f(0) - e_f(1)| : the vertex labeling f is friendly}. In this paper, exact values of the balance index sets of six new families of one-point union of graphs are obtained , all of them form arithmetic progressions .

On H-Matchable Trees

Lane Clark and Andrew Schwartz*
Department of Mathematics, Southern Illinois University
Carbondale, IL 62901-4408

Fix a nontrivial tree H. We call $\{H_1,\ldots,H_n\}$ a perfect H - matching of a tree T if and only if $H_1,\ldots,H_n$ are subtrees of T where each $H_i \simeq H$ and $\{V(H_1),\ldots,V(H_n)\}$ partitions $V(T)$. Then a perfect P_2 - matching of T is a perfect matching of T. A tree is H - matchable if and only if it has a perfect H - matching. We first find the number of labeled H - matchable trees and then find the degree distribution of a random vertex in a random labeled H - matchable tree.

Revisiting Chromatic Polynomials of Some Sequences of Graphs

Amir Barghi and Hossein Shahmohamad*
School of Mathematical Sciences, Rochester Institute of Technology
Rochester, NY 14623
hxssma@rit.edu

The chromatic polynomial of a graph Γ, $C(\Gamma;\lambda)$, is the polynomial in λ which counts the number of distinct proper vertex λ-colorings of Γ, given λ colors. By applying the addition-contraction method, chromatic polynomials of some sequences of 2-connected graphs satisfy a number of recursive relations. We will show that by knowing chromatic polynomial of a few small graphs, chromatic polynomial of each of these sequences can be computed by utilizing either matrices or generating functions.

Pan-Connectedness of Graphs with Large Neighborhood Unions

Yehong Shao
Arts and Science, Ohio University Southern
Ironton, OH 45638
shaoy@ohio.edu

Let G be a simple graph with n vertices. For any $v \in V(G)$, let $N(v) = \{u \in V(G) : uv \in E(G)\}$, $NC(G) = \min\{|N(u) \cup N(v)| : u,v \in V(G) \text{ and } uv \notin E(G)\}$, and $NC_2(G) = \min\{|N(u) \cup N(v)| : u,v \in V(G) \text{ and } u \text{ and } v \text{ has distance 2 in } E(G)\}$. Let $l \geq 1$ be an integer. A graph G on $n \geq l$ vertices is $[l,n]$-pan-connected if for $\forall u,v \in V(G)$, and any integer m with $l \leq m \leq n$, G has a (u,v)-path of length m. In 1998, Wei and Zhu have proved that for a 3-connected graph on $n \geq 7$ vertices, if $NC(G) \geq n - \delta(G) + 1$, then G is $[6,n]$-pan-connected. They conjectured that such graphs should be $[5,n]$-pan-connected. In this paper, we prove that for a 3-connected graph on $n \geq 7$ vertices, if $NC_2(G) \geq n - \delta(G) + 1$, then G is $[5,n]$-pan-connected. Consequently, the conjecture of Wei and Zhu is proved as $NC_2(G) \geq NC(G)$. Furthermore, we show that the lower bound is best possible and characterize all 2-connected graphs with $NC_2(G) \geq n - \delta(G) + 1$ which are not $[4,n]$-pan-connected.

On the Security of Stickler's Key Exchange Scheme

Michal Sramka
Center for Cryptology and Information Security, Florida Atlantic University
Boca Raton, Florida 33431
sramka@math.fau.edu

In 2005, Eberhard Stickel proposed a variation of the Diffie-Hellman key exchange scheme based on non-abelian groups. In particular, he described a key exchange scheme that uses exponentiations of two group elements that do not commute. The proposal also contains implementation details for some specific subgroup of a general linear group of prime degree n. Although the proposal lacks a rigorous security analysis, the author claims that the brute-force attack of an instance would require to search through a space of size $(2^n - 1)^2$.

We will present results showing that the proposed key exchange scheme can be in fact successfully attacked with considerably smaller complexity. We will show that the scheme can be in fact broken by searching through a space of cardinality $2^n - 1$. Also, for the general scheme with two non-commuting elements of order n_1 and n_2 ($n_1 \geq n_2$), we show that the time complexity of breaking the scheme in the worst-case is $O(n_1 \cdot \log n_1)$ group operations while requiring storage of $O(n_2)$ group elements. As a result, this attack uses square-root less operations than the previous known attack.

How Can NP Graph Problems be Moved Into P?

George Stacey Staples* and René Schott
Department of Mathematics & Statistics, Southern Illinois University at Edwardsville
Edwardsville, IL 62026-1653
sstaple@siue.edu

A well-known result in graph theory states that the closed k-walks contained in a graph are enumerated along the diagonal of the k^{th} power of the graph's adjacency matrix. By constructing the adjacency matrix over an appropriate nilpotent-generated algebra, the k-cycles are recovered in the same manner.

Using this method, the k-cycles, k-circuits, and k-paths can be enumerated in any finite graph. Applying this approach to random graphs yields expected numbers of these structures. Properties of the algebra can also be used to compute the permanent of an arbitrary matrix.

Moreover, these problems are of polynomial complexity in the number of algebra multiplications performed. In this way, the Hamiltonian cycle problem is among problems moved from class NP into P, while counting the perfect matchings of a bipartite graph is among problems moved from class #P into P.

The Conjecture of El-Zahar

Hong Wang
Department of Mathematics, University of Idaho
Moscow Idaho 83844-1103
hwang@uidaho.edu

Let G be a graph of order $5k$ with minimum degree at least $3k$. Then G contains k disjoint cycles of length 5. This was conjectured by El-Zahar in 1984.

On the Balance Index Sets of the (p,p+1)-Graphs

Sin-Min Lee, Yung-Chin Wang*, and Yihui Wen
Department of Physical Therapy, Tzu-Hui Institute of Technology
Taiwan, Republic of China
jackwang91@hotmail.com

Let G be a graph with vertex set V(G) and edge set E(G), and let A ={0,1}. A labeling $f : V(G) \to A$ induces an edge partial labeling $f^* : E(G) \to A$ defined by $f^*(xy) = f(x)$, if and only if f(x)=f(y) for each edge $xy \in E(G)$. For $i \in A$, let $v_f(i) = card\{v \in V(G) : f(v) = i\}$ and $e_{f^*}(i) = card\{e \in E(G) : f^*(e) = i\}$. A labeling f of a graph G is said to be friendly if $|vf(0) - vf(1)| \leq 1$. If $|e_f(0) - e_f(1)| \leq 1$ then G is said to be balanced. The balance index set of the graph G, BI(G), is defined as $|e_f(0) - e_f(1)|$: the vertex labeling f is friendly. In this paper, exact values of the balance index sets of seven families of (p,p+1)-graphs are obtained.

On the Balancedness of the Galaxies with At Most Four Stars

Sin-Min Lee, Linh Vu, Li Wen*, and Danhong Zhang
Department of Computer Science, San Jose State University
San Jose, CA 95192
iwensdf@yahoo.com

Let G be a graph with vertex set V(G) and edge set E(G), and let A ={0,1}. A labeling f : V(G) → A induces an edge partial labeling f* : E(G) → A defined by f*(xy) = f(x),if and only if f(x)=f(y) for each edge xy ∈ E(G). For i ∈ A, let v_f(i) = card{v ∈ V(G) : f(v) = i} and e_f*(i) = card{e ∈ E(G) : f*(e) = i}. A labeling f of a graph G is said to be friendly if | $v_f(0)$ - $v_f(1)$ | ≤ 1. If | $e_f(0)$ - $e_f(1)$ | ≤ 1 then G is said to be ***balanced***. The ***balance index set*** of the graph G, BI(G), is defined as {| $e_f(0)$ - $e_f(1)$| : the vertex labeling f is friendly}. We show that the conjecture that the numbers in BI(G) for any galaxy G forms an arithmetic progression is true for galaxies with at most four stars.

On Balance Index Sets of Trees with Diameter At Most Four

Yong-Song Ho, Sin-Min Lee, Yihui Wen, and Danhong Zhang*
Department of Mathematics, Utica college
Utica, NY 13502-4892
dzhang@utica.edu

Let G be a graph with vertex set V(G) and edge set E(G), and let A ={0,1}. A labeling f : V(G) → A induces an edge partial labeling f* : E(G) → A defined by f*(xy) = f(x),if and only if f(x)=f(y) for each edge xy ∈ E(G). For i ∈ A, let v_f(i) = card{v ∈ V(G) : f(v) = i} and e_f*(i) = card{e ∈ E(G) : f*(e) = i}. A labeling f of a graph G is said to be friendly if | $v_f(0)$ - $v_f(1)$ | ≤ 1. If | $e_f(0)$ - $e_f(1)$ | ≤ 1 then G is said to be ***balanced***. The ***balance index set*** of the graph G, BI(G), is defined as {| $e_f(0)$ - $e_f(1)$| : the vertex labeling f is friendly}. In this paper we investigate the balance index sets of trees with diameter at most four.