

Discrete Math Days 2009

Plenary Talks

Peter J. Cameron

Queen Mary, University of London

Synchronization

This talk will report on a lot of new work on permutation groups, graph homomorphisms, representation theory and other areas motivated by questions about synchronization of finite deterministic automata.

The general question can be phrased as follows. Suppose that G is a given permutation group on a set X of size n . What properties of G guarantee that, if f is a function from X to X which is not a permutation, the transformation monoid generated by G and f necessarily contains an element whose image has size 1? What additional property guarantees that such an element can be represented by a word in f and elements of G in which f is used at most $n - 1$ times?

Groups with the first property are primitive, though not every primitive permutation group satisfies the property. It can be detected by means of graphs: a group fails to have the property if and only if it is contained in the automorphism group of a graph whose clique number and chromatic number are equal. This is the basis of the most practical test we know.

These and other matters will be discussed in the talk.

Rod Canfield

University of Georgia

Problems and results in asymptotic combinatorics

I will divide the talk between two topics. The first is Stirling numbers of the second kind, $S(n, k)$. For each n the maximum $S(n, k)$ is achieved either at a unique $k = K_n$, or is achieved twice consecutively at $k = K_n, K_n + 1$. Call those n of the second kind *exceptional*. Is $n = 2$ the only exceptional integer? The second topic is $m \times n$ nonnegative integer matrices all of whose rows sum to s and all of whose columns sum to t , $ms = nt$. We have an asymptotic formula for the number of these matrices, valid for various ranges of $(m, s; n, t)$. Although obtained by a lengthy calculation, the final formula is succinct and has an interesting probabilistic interpretation. The work presented here is collaborative with Carl Pomerance and Brendan McKay, respectively.

Shuhong Gao

Clemson University

New Directions in Multivariate Public Key Cryptography

In this talk, I will discuss some recent contributions to the field of multivariate public key cryptography (MPKC). I will begin by motivating a need for new public key encryption schemes and then give a brief overview of MPKC. I will introduce a new framework for constructing multivariate public key cryptosystems and propose a new encryption scheme that is secure against known attacks on MPKCs. Joint work with Ray Heindl.

Heather Jordan
Illinois State University

Skolem-type Difference Sets for Cycle Systems

A cyclic m -cycle system of order n is a decomposition of the complete graph of order n into m -cycles that behaves “nicely”. In this talk, we will construct cyclic m -cycle systems of order n for all $m \geq 3$, and all $n \equiv 1 \pmod{2m}$. This result has been settled previously by several authors; however, in this talk, we provide a different solution, as a consequence of a more general result, which handles all cases using similar methods and which also allows us to prove necessary and sufficient conditions for the existence of a cyclic m -cycle system of $K_n - I$ for all $m \geq 3$, and all $n \equiv 2 \pmod{2m}$.

Marni Mishna
Simon Fraser University

The combinatorics of walking around: Strategies for exact lattice path enumeration

Prudent walks, excursions, directed paths and all manner of lattice paths: These objects arise in statistical mechanics to model polymer behaviour, percolation, and other phenomena. Together are a significant advance towards solving the longstanding, elusive problem of exact enumeration of self avoiding walks. Lattice models also appear outside of physics in queuing models, bijective combinatorics and formal language theory. This talk is a survey of objects that arise in combinatorial models within statistical mechanics, through the lens of exact and asymptotic enumeration. Interesting patterns emerge, new techniques arise and truths about the nature of generating functions are revealed.

Patric Östergård
Helsinki University of Technology

Russian Doll Search for Clique-Type Problems

Russian Doll Search (RDS), introduced by Verfaillie, Lemaître, and Schiex in 1996, can in general terms be described as an algorithm for solving a problem with n variables through n subproblems, where the first subproblem includes just the n th variable, the i th subproblem the last i variables, and where the solutions of the subproblems are used for pruning in later subproblems. RDS is for NP-hard problems what dynamic programming is for problems in P.

We shall discuss clique-type problems for graphs, digraphs, and hypergraphs, and see how RDS can be applied to these. It is well known that the problem of finding a maximum clique in a graph is equivalent to finding a maximum independent set and a minimum vertex cover in the complement graph. For digraphs, we consider the problem of finding a maximum transitive subtournament, which is equivalent to finding a maximum induced acyclic subgraph and a minimum feedback vertex set in the complement digraph. Finally, for hypergraphs we consider the problem of finding a maximum independent set (a set including no hyperedge), which is equivalent to finding a minimum hitting set (a set of vertices intersecting all hyperedges) and a minimum set cover.

RDS algorithms can be used, for example, to find the optimal solutions of instances of the Steiner triple covering problem up to 100 times faster than in earlier work. Applications to the study of the capacity of digraphs as well as the problem of finding small tournaments with disjoint Banks and Slater sets (a record-breaking such tournament of order 14 has been found) will also be discussed.

This is joint work with Vesa Vaskelainen.

Contributed Talks

John Arhin

Marlboro College

Some infinite families of non-Trojan SOMA(k, n)s

A SOMA(k, n) is a $n \times n$ array A each of whose entries is a k -subset of a kn -set Ω of symbols, such that every symbol of Ω occurs exactly once in each row and exactly once in each column of A , and every 2-subset of Ω is contained in at most one entry of A . We say that a SOMA(k, n) is Trojan if it can be constructed by the superposition of k mutually orthogonal Latin squares of order n , but not every SOMA(k, n) can be constructed in this way.

Several methods for the construction of SOMA(k, n)s are discussed. Using these methods we can show that a non-Trojan SOMA($2, n$) exists if and only if $n \geq 5$. Note that a non-Trojan SOMA($2, n$) is basically the same thing as a Howell Design $H(n, 2n)$ that does not satisfy the $*$ -condition. In addition, we use these methods to give new examples of non-Trojan SOMA($3, n$)s and of non-Trojan SOMA($4, n$)s.

Robert Bailey

Carleton University

Bases for automorphism groups of graphs

A *base* for a permutation group G is a sequence of points whose pointwise stabiliser is trivial. This means that the action of an element $g \in G$ on a base determines its action on everything (generalising the notion of a basis of a vector space). In the case where G is the automorphism group of a graph, in recent years this concept has been rediscovered by a number of authors under a variety of names.

In this talk, we will pool together some results on this topic, and also mention connections with diverse topics as association schemes, matroids and the metric dimension of graphs.

Anthony Bonato

Ryerson University

Distinguishing Infinite Graphs

The distinguishing number of a graph, introduced by Albertson and Collins, is a measure of how close the graph is to being rigid. More precisely, it is the minimum number of colours needed on vertices so that no non-trivial automorphism preserves the colours. While most research on the distinguishing number has focused on the finite case, recent work considers infinite structures as well. Imrich, Klavžar, and Trofimov recently proved that distinguishing number of the infinite random graph is 2, while Laflamme, Nguyen Van Thé, and Sauer generalized this to certain homogeneous relational structures. We introduce a simple structural condition for infinite graphs and relational structures to have distinguishing number 2, thereby generalizing the above two results.

Dennis D. A. Epple

University of Victoria

The Bichromatic Number of a Graph

A (k, l) -colouring of a graph G is a covering of its vertex set by k independent sets and l cliques, generalizing both the colouring and clique covering of a graph. The bichromatic number of G is defined as the minimum integer r , such that G is (k, l) -colourable for all $k + l = r$. We will investigate some fundamental properties of the bichromatic number and look into some fascinating examples related to designs.

Shonda Gosselin

University of Ottawa

Constructing regular self-complementary uniform hypergraphs

A k -uniform hypergraph is a pair $(\mathcal{V}, \mathcal{E})$ in which \mathcal{V} is a finite set of vertices, and \mathcal{E} is a set of k -subsets of \mathcal{V} called edges. A k -uniform hypergraph $X = (\mathcal{V}, \mathcal{E})$ is called *self-complementary* if it is isomorphic to its complement $(\mathcal{V}, \mathcal{E}^C)$, where \mathcal{E}^C is the complement of \mathcal{E} in the set of all k -subsets of \mathcal{V} , and it is called *t -subset-regular* if there exists a constant c such that every t -subset of \mathcal{V} lies in exactly c edges of \mathcal{E} .

In this talk, we examine the possible orders of t -subset-regular self-complementary k -uniform hypergraphs. We reformulate Khosrovshahi's and Tayfeh-Rezaie's necessary conditions on the order of these structures in terms of the binary representation of the rank k . This gives a more transparent relation between the order n and rank k in the case where k is a sum of consecutive powers of 2. Moreover, we construct 1-subset-regular self-complementary uniform hypergraphs, and prove that our necessary conditions are sufficient for all k , in the case where $t = 1$.

Ilias Kotsireas

Wilfrid Laurier University

Periodic complementary binary sequences and Combinatorial Optimization algorithms

We establish a new formalism for problems pertaining to the periodic and non-periodic autocorrelation functions of finite sequences, which is suitable for Combinatorial Optimization methods. This allows one to bring to bear powerful Combinatorial Optimization methods in a wide array of problems that can be formulated via these two functions. Joint work with C. Koukouvinos, P. M. Pardalos, O. V. Shylo, JOCO, to appear.

Conrado Martínez

Univ. Politecnica de Catalunya

Combinatorics and the Hiring Problem

The hiring problem has been recently introduced by Broder et al. in ACM-SIAM Symp. on Discrete Algorithms (SODA 2008), as a simple model for decision making under uncertainty. In its simplest formulation, a company interviews candidates in a sequential fashion, with Q_i being the quality or score of the i -th candidate. The Q_i 's are i.i.d. random variables with common distribution $\text{Unif}(0, 1)$. Then, according to the company's hiring strategy, candidate i is either hired or discarded.

We provide an alternative formulation of the hiring problem in combinatorial terms; its main virtue being that it opens the door for the application of a vast and rich array of powerful techniques coming from analytic combinatorics. In particular, we prove several general theorems that apply to large families of hiring strategies, in particular, those we call rank-based. These general results are then applied to the study of particular strategies such as hiring above the maximum, hiring above the m th best and hiring above the median (or above some quantile).

This is joint work with Margaret Archibald.

Shahla Nasserar

College of William and Mary

$TP_2 = \text{Bruhat}$

A matrix is TP_2 if all 1-by-1 and 2-by-2 minors are positive. TP_2 completion problem is described. It is shown that the Bruhat partial order on permutations is equivalent to a certain natural partial order induced by TP_2 matrices and that a positive matrix is TP_2 if (and only if) it satisfies certain inequalities induced by Bruhat order.

Alois Panholzer

Vienna University of Technology

Asymptotic results for the number of unsuccessful parkers in a one-way street

Konheim and Weiss introduced in the Sixties the notion of parking functions during their studies of a linear probing hashing algorithm. Recently Cameron, Johannsen, Prellberg and Schweitzer obtained an exact formula for the number of “defective parking functions with defect k ”. Such defective parking functions can be considered also as sequences $x_1, \dots, x_n \in \{1, \dots, m\}^n$ of addresses, such that, in a one-way street with m parking spaces and n arriving cars, exactly k cars are unsuccessful, i.e., cannot be parked.

Here we focus on asymptotic results and treat the random variable $X_{m,n}$, which denotes the number of unsuccessful cars for a random sequence of addresses for n cars and m parking spaces. We present, depending on the growth of m and n , the limiting behaviour of $X_{m,n}$ by characterizing the limit laws appearing.

Bill Sands

University of Calgary

*On a Problem From *Cruz Mathematicorum**

Suppose you are given four cards, each containing four nonnegative real numbers, written one below the other, so that the sum of the numbers on each card is 1. You are allowed to put the cards in any order you like, then you write down the first number from the first card, the second number from the second card, the third number from the third card, and the fourth number from the fourth card, and you add these four numbers together. What is the smallest interval $[a, b]$ so that, no matter which cards you are given, there is always an ordering of the cards so that the sum will lie in $[a, b]$?

I will give the history of this problem and what I know about it.

Ben Seamone

Carleton University

Edge weightings that induce proper vertex colourings

A graph G permits a *vertex-colouring k -weighting* if each edge of G can be assigned a weight from the set $\{1, \dots, k\}$ such that adjacent vertices have different sums of incident edge weights. Karoński, Łuczak and Thomason have conjectured that the smallest value for which every connected graph (except K_2) has such a weighting is $k = 3$. In joint work with Naserasr, Newman and Stevens, we address this open problem by exploring which graphs permit a vertex-colouring 2-weighting. We present partial results which follow from a classification of bipartite graphs whose cycles satisfy congruency conditions.

Igor Shparlinski
Macquarie University

Sum-Product Problem: New Generalisations and Applications

The celebrated sum-product theorem of Bourgain-Katz-Tao asserts that for any set A in a prime finite field (such that the cardinality $|A|$ is not too small or large) at least one of the sets

$$A + A = \{a_1 + a_2 : a_1, a_2 \in A\}, AA = \{a_1 a_2 : a_1, a_2 \in A\}$$

is of cardinality at least $|A|^{1+\eta}$ for some fixed $\eta > 0$. This result has recently obtained various explicit versions (with an explicit value of η) and has also been extended in various directions including different functions on sets, such as

$$A^{-1} + A^{-1} = \{a_1^{-1} + a_2^{-1} : a_1, a_2 \in A, a_1 a_2 \neq 0\}.$$

We outline some new applications of such results to various number theoretic problems, including estimating the “concentration” of rational points on some curves over finite fields F_p and the number of solutions of congruences of the type $x^x \equiv 1 \pmod{p}$ for a prime p .

We also describe some recent generalisations to the settings of groups of points on elliptic curves and also of matrix rings.

Finally we mention several open problems, some of which are motivated by cryptographic applications.