Banff International Research Station

for Mathematical Innovation and Discovery

BIRS Workshop 09w5103

Applications of Matroid Theory and Combinatorial Optimization to Information and Coding Theory

August 2–7, 2009

Organizers

Navin Kashyap	Department of Mathematics & Statistics, Queen's University, Canada
Emina Soljanin	Mathematics Research Center, Alcatel–Lucent Bell Labs, Murray Hill, NJ, USA
Pascal O. Vontobel	Hewlett–Packard Laboratories, Palo Alto, CA, USA

General Information – Meals

Time	Meal	Details
07:00–09:30	Breakfast (Buffet)*	Sally Borden Building, Monday–Friday
11:30–13:30	Lunch (Buffet)*	Sally Borden Building, Monday–Friday
17:30–19:30	Dinner (Buffet)*	Sally Borden Building, Sunday–Thursday
(see schedule)	Coffee breaks	2nd floor lounge, Corbett Hall

* **Please remember to scan your meal card at the host/hostess station in the dining room for each meal.**

General Information – Meeting Rooms

All lectures will be held in Max Bell 159 (Max Bell Building accessible by walkway on 2nd floor of Corbett Hall). LCD projector, overhead projectors, and blackboards are available for presentations. Please note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155–159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.

General Information – Talks

Long talks are 60 min. long (guideline: 50 min. + 10 min. for questions).
Exception: some long talks on Wednesday are 45 min. long (guideline: 40 min. + 5 min. for question).
Short talks are 30 min. long (guideline: 25 min. + 5 min. for questions).

Sunday, August 2, 2009

Time	Event	Details
16:00	*Check-in begins*	Front Desk – Professional Development Centre – open 24 hours
17:30–19:30	*Buffet dinner*	
20:00	*Informal gathering*	2nd floor lounge, Corbett Hall; beverages and small assortment of snacks available on a cash honour-system

Monday, August 3, 2009

Time	Speaker / Event	Title / Details
07:00–08:45	*Breakfast*	
08:45–09:00	**Brenda Williams**	Introduction and welcome to BIRS
09:00–10:00	**James Oxley**	An Introduction to matroid theory (tutorial)
10:00–10:30	*Coffee break*	
10:30–11:30	**Navin Kashyap**	Applications of matroid methods to coding theory (tutorial)
11:30–13:30	*Lunch*	
13:30–14:30	**Martin Wainwright**	Linear and other conic programming relaxations in combinatorial optimization: graph structure and message-passing
14:30–15:00	*Coffee break*	
15:00–16:00	**Pascal Vontobel**	Pseudo-codewords: fractional vectors in coding theory (tutorial)
16:00–16:30	**Thomas Britz**	From codes to matroids and back
17:30–19:30	*Dinner*	

Tuesday, August 4, 2009

Time	Speaker / Event	Title / Details
07:00–09:00	*Breakfast*	
09:00–10:00	**Bert Gerards**	Binary matroid minors I
10:00–10:30	*Coffee break*	
10:30–11:30	**Jim Geelen**	Binary matroid minors II
11:30–13:00	*Lunch*	
13:00–14:00	*Guided tour*	Guided tour of the Banff Centre Meet in the 2nd floor lounge, Corbett Hall
14:00–14:05	*Group photo*	Meet on the front steps of Corbett Hall
14:05–15:05	**Carles Padro**	On the optimization of secret sharing schemes for general access structures
15:05–15:30	*Coffee break*	
15:30–16:30	**Amos Beimel**	Secret sharing schemes, matroids, and non-Shannon information inequalities
16:30–16:45	*Break*	
16:45–17:45	**P. K. Sarvepalli**	Matroids in quantum computing and quantum cryptography
17:45–19:30	*Dinner*	

Wednesday, August 5, 2009

Time	Speaker / Event	Title / Details
07:00–08:30	*Breakfast*	
08:30–09:30	**Emina Soljanin**	Basics of network coding (tutorial)
09:30–10:15	**Chandra Chekuri**	Combinatorial optimization in routing vs. network coding
10:15–10:45	*Coffee break*	
10:45–11:30	**Alex Sprintson**	Applications of matroid theory to network coding
11:30–12:00	**Randall Dougherty**	Is network coding undecidable?
12:00–13:30	*Lunch*	
	Excursion	
17:30–19:30	*Dinner*	

(The default is to hold these talks on Wednesday morning. Depending on weather conditions, these talks might be held on Wednesday afternoon. The decision will be made at noon-time on Tuesday.)

Thursday, August 6, 2009

Time	Speaker / Event	Title / Details
07:00–09:00	*Breakfast*	
09:00–10:00	**Raymond Yeung**	Facets of entropy
10:00–10:30	*Coffee break*	
10:30–11:30	**Frantisek Matus**	Entropy functions, information inequalities, and polymatroids
11:30–13:00	*Lunch*	
13:00–14:00	**Andreas Winter**	A new inequality for the von Neumann entropy
14:00–15:00	**Randall Dougherty**	Non-Shannon entropy inequalities and linear rank inequalities
15:00–15:30	*Coffee break*	
15:30–16:00	**Alex Grant**	Quasi-uniform codes and their applications
16:00–16:30	**Serap Savari**	A combinatorial study of linear deterministic relay networks
16:30–17:00	**Eimear Byrne**	Upper bounds for error-correcting network codes
17:30–19:30	*Dinner*	
19:30–21:00	Open mike session	Session for open speech and for presenting open problems

Friday, August 7, 2009

Time	Speaker / Event	Title / Details
07:00–09:00	*Breakfast*	
09:00–09:30	**Dillon Mayhew**	Excluded minors for real-representable matroids
09:30–10:00	**Michael Langberg**	Communicating the sum of sources in multiple-unicast networks
10:00–10:30	*Coffee break*	
10:30–11:00	**Olgica Milenkovic**	Sub-linear compressive sensing and support weight enumerators of codes: a matroid theory approach
11:00–11:30	**Alexander Barg**	Linear codes in the ordered Hamming space
11:30–13:30	*Lunch*	
	End of workshop	*Have a safe trip home! (Reminder: check-out time is 12:00 noon)*

Banff International Research Station

for Mathematical Innovation and Discovery

BIRS Workshop 09w5103

Applications of Matroid Theory and Combinatorial Optimization to Information and Coding Theory

August 2–7, 2009

Abstracts

(in alphabetic order by speaker surname)

Speaker **Alexander Barg** (Dept. of ECE, Univ. of Maryland, College Park, USA)

Title *Linear Codes in the Ordered Hamming Space*

Abstract As is well known, the weight distribution of MDS codes in the Hamming metric can be recovered easily from the rank function of a uniform matroid. No such association has been established for the ordered Hamming space (the Niederreiter-Rosenbloom-Tsfasman space), although the weight distribution of MDS codes is also easily found. The question becomes more challenging when one considers codes with distance even one less than the MDS distance. We compute such weight distributions (under some conditions) and discuss the link of MDS codes to uniformly distributed point sets in the unit cube.

This is joint work with Punarbasu Purkayastha.

Speaker **Amos Beimel** (Dept. of CS, Ben-Gurion Univ., Israel)

Title *Secret Sharing Schemes, Matroids, and Non-Shannon Information Inequalities*

Abstract In a secret-sharing scheme, a secret value is distributed among a set of parties by giving each party a share. The requirement is that only predefined subsets of parties can recover the secret from their shares. In this talk, I will discuss the use of non-Shannon information inequalities for proving lower bounds on the size of shares in secret sharing schemes. I will describe two results:

1. Using non-Shannon information inequalities, we prove lower-bounds on the size of the shares in every secret-sharing scheme realizing an access structure induced by the Vamos matroid. This is the first proof that there exists an access structure induced by a matroid which is not nearly ideal.

2. All known proofs on the size of shares in secret-sharing schemes use information inequalities. We show that all the information inequalities known to date cannot prove a lower bound of $\Omega(n)$ on the share size.

This talk is based on joint works with Noam Livne, Carles Padro, and Ilan Orlov.

Speaker **Thomas Britz** (School of Math. and Stat., Univ. of New South Wales, Australia)
Title *From Codes to Matroids and Back*
Abstract Matroid theory generalizes objects and results from many other fields, such as linear algebra, graph theory, and matching theory, to name prominent examples. By applying matroid theory to the generalized objects, it is often possible to achieve good results regarding the original objects.

This talk will present a brief overview on what is presently known about the support and weight connections between coding and matroid theory, and applications of these connections to coding- and graph theory will be given. The newest results include an interesting variation of the Tutte polynomial as well as an interesting but ever-evolving dual identity.

The talk may be seen as an add-on for the workshop tutorial by Navin Kashyap.

Speaker **Eimear Byrne** (School of Math. Sciences, Univ. College Dublin, Ireland)
Title *Upper Bounds for Error-Correcting Network Codes*
Abstract Versions of the Singleton, sphere-packing, and Gilbert-Varshamov bounds for a particular model for error-correcting codes for coherent network coding were given by Yang and Yeung. Here we extend the classical Plotkin and Elias bounds for the same model.

Speaker **Chandra Chekuri** (Dept. of CS, Univ. of Illinois at Urbana-Champaign, USA)
Title *Combinatorial Optimization in Routing vs. Network Coding*
Abstract This talk will survey results that seek to understand the potential benefit that network coding offers over more traditional and simpler transmission schemes such as store and forward routing. This will be examined by asking the following question. What is the maximum ratio (over all networks) between the rate achievable via network coding and via routing? We restrict attention to the wireline setting. This question has been answered to a large extent in the multicast setting in both undirected and directed graphs. In the multiple unicast setting, the benefit is known to be very large in directed graphs while the case of undirected graphs is a wide-open.

Combinatorial optimization plays an important role in understanding the above question. Steiner-tree packings and integrality gaps of linear programming relaxations for Steiner trees are the key tools in the multicast setting. Multicommodity flow-cut gaps play a role in the multiple unicast setting.

Speaker **Randall Dougherty** (IDA Center for Comm. Research, La Jolla, CA, USA)
Title *Is Network Coding Undecidable?*
Abstract I will outline an approach that, if two holes in it can be filled or worked around, will yield a proof that the solvability problem for network coding is undecidable. The idea is to try to represent groups satisfying or not satisfying identities as networks, in order to reduce Rhodes' problem on finite groups to the network coding solvability problem.

Speaker **Randall Dougherty** (IDA Center for Comm. Research, La Jolla, CA, USA)
Title *Non-Shannon Entropy Inequalities and Linear Rank Inequalities*
Abstract Any unconstrained inequality in three or fewer random variables can be written as a linear combination of instances of Shannon's inequality $I(A;B|C) \geq 0$. Such inequalities are sometimes referred to as "Shannon" inequalities. In 1998, Zhang and Yeung gave the first example of a "non-Shannon" information inequality in four variables; their technique was to add two auxiliary variables with special properties and then apply Shannon inequalities to the enlarged list. Here we will show that the Zhang–Yeung inequality can in fact be derived from just one auxiliary variable. Then we use the same basic technique of adding auxiliary variables to give many other non-Shannon inequalities in four variables (which, surprisingly, are all of the same general form). We also derive rules for generating new non-Shannon inequalities from old ones, which can be applied iteratively to generate infinite families of inequalities such as the one used by Matus to show that the closure of the entropic points on four variables is not polytopal.

A variant of this approach (using a different sort of auxiliary variable) allows us to derive inequalities which always hold for ranks of linear subspaces, but need not hold for entropies of random variables. It is known that the Ingleton inequality and the Shannon inequalities give a complete list of the rank inequalities for four variables (subspaces). We derive a list of 24 additional inequalities in five variables which, together with the Shannon inequalities and instances of the Ingleton inequality, are complete for rank inequalities on five subspaces. We also give general many-variable families of rank inequalities.

In both cases, we indicate that there are probably new inequalities which cannot be found by these methods and will require different approaches.

Speaker **Jim Geelen** (Dept. of Comb. and Opt., Univ. of Waterloo, Canada)
Title *Binary matroid minors II*
Abstract This talk is on applications of the structure theorem and on open problems concerning minor-closed classes of binary matroids.

This is joint work with Bert Gerards and Geoff Whittle.

Speaker **Bert Gerards** (CWI, Amsterdam, The Netherlands)
Title *Binary matroid minors I*
Abstract In this talk we give an overview of the structure theorem for minor-closed classes of binary matroids. These results extend the graph minors structure theorem of Robertson and Seymour.

This is joint work with Jim Geelen and Geoff Whittle.

Speaker **Alex Grant** (Inst. for Telecommunications Research, Univ. of South Australia)
Title *Quasi-Uniform Codes and their Applications*
Abstract Quasi-uniform random variables have probability distributions that are uniform over their support. They are of fundamental interest because a linear information inequality is valid if and only if it is satisfied by all quasi-uniform random variables. In this paper, we investigate properties of codes induced by quasi-uniform random variables. We prove that quasi-uniform codes (which include linear codes as a special case) are distance-invariant and that Greene's Theorem holds in the setting of quasi-uniform codes. We also show that almost affine codes are a special case of quasi-uniform codes in the sense that quasi-uniform codes are induced by entropic polymatroids while almost affine codes are induced by entropic matroids. Applications of quasi-uniform codes in error correction and secret sharing will also be given.

Joint work with Terence Chan.

Speaker **Navin Kashyap** (Dept. of Math. and Stat., Queen's Univ., Canada)
Title *Applications of Matroid Methods to Coding Theory*
Abstract Matroid theory is a study of a notion of independence that can be abstracted from the usual independence in linear algebra, as well as from trees and forests in graph theory. It is only natural to expect matroid theory to have applications to the theory of error-correcting codes, as matrices over finite fields are objects of fundamental importance in both these theories. An early application can be found in the work of Greene (1976) who (re-)derived the MacWilliams identities as special cases of an identity for the Tutte polynomial of a matroid. More recently, matroid methods have found applications in the study of graphical models for codes, and in the analysis of decoding methods such as the sum-product algorithm, and linear-programming decoding. In this tutorial, we will attempt to give an overview of the applications of matroid methods to coding theory. Among the topics covered will be the use of code/matroid decomposition techniques, and various "width" parameters (treewidth, branchwidth) associated with graphs and matroids, in the analysis of graphical models and decoding algorithms for linear codes.

Speaker **Michael Langberg** (CS Division, The Open Univ. of Israel)
Title *Communicating the Sum of Sources in Multiple-Unicast Networks*
Abstract In this talk we consider the network communication scenario in which a number of sources s_i each holding independent information X_i wish to communicate the sum $\sum_i X_i$ to a set of terminals t_j. The case in which there are only two sources or only two terminals was considered by the work of Ramamoorthy [ISIT 2008] where it was shown that communication is possible if and only if each source terminal pair s_i / t_j is connected by at least a single path.

In this talk we will study the communication problem in general, and show that even for the case of three sources and three terminals, a single path connecting source/terminal pairs does not suffice to communicate $\sum_i X_i$. We then present an efficient encoding scheme which enables the communication of $\sum_i X_i$ for the three sources, three terminals case, given that each source terminal pair is connected by *two* edge disjoint paths. Our encoding scheme includes a structural decomposition of the network at hand which may be found useful for other network coding problems as well.

Joint work with Aditya Ramamoorthy.

Speaker **Frantisek Matus** (Inst. of Inform. Theory and Autom., Acad. of Sciences of the Czech Republic)

Title *Entropy Functions, Information Inequalities, and Polymatroids*

Abstract Shannon entropies of all subvectors of a random vector are considered for the coordinates of an entropic point in a Euclidean space. The problem to find all entropic points will be reviewed and its relation to conditional independence structures discussed. Inequalities for the entropic points and their applications will be presented from the viewpoint of cones of polymatroids.

Speaker **Dillon Mayhew** (School of Math., Stat. and Operations Research, Victoria Univ. of Wellington, New Zealand)

Title *Excluded Minors for Real-Representable Matroids*

Abstract Rota conjectured that if F is a finite field, then there is only a finite number of minor-minimal matroids that are not F-representable. Such matroids are called excluded minors for F-representability. Rota's conjecture contrasts with the long-established fact that there are infinitely many excluded minors for representability over the real numbers. Geelen (2008) conjectured a much stronger fact: if M is any real-representable matroid, then there is an excluded minor, N, for real-representability, such that N contains M as a minor.

We present a proof of Geelen's conjecture. This is joint work with Mike Newman and Geoff Whittle.

Speaker **Olgica Milenkovic** (Dept. of ECE, Univ. of Illinois at Urbana-Champaign, USA)

Title *Sub-linear Compressive Sensing and Support Weight Enumerators of Codes: a Matroid Theory Approach*

Abstract Compressive sensing is a new sampling technique for sparse signals that has the potential to significantly reduce the complexity of many data acquisition techniques. Most compressive sensing reconstruction techniques are still prohibitively time-consuming, narrowing the scope of practical applications of this method. We propose a new method for compressive sensing signal reconstruction of logarithmic complexity that combines iterative decoding methods with greedy subspace pursuit algorithms. The performance of the method depends on certain characteristics of support weight enumerators of the codes used for constructing the sensing matrix, which can be described via matroid theory.

This is joint work with Wei Dai and Vin Pham Hoa.

Speaker **James Oxley** (Dept. of Math., Louisiana State Univ., USA)
Title *An Introduction to Matroid Theory*
Abstract Matroids were introduced by Whitney in 1935 to try to capture abstractly the fundamental properties of dependence common to graphs and matrices. Whitney's definition embraces a surprising diversity of combinatorial structures. A *matroid* $(E, \mathcal{I})$ consists of a finite set E and a non-empty family $\mathcal{I}$ of subsets of E, called *independent sets*, such that every subset of an independent set is independent, and, for every subset X of E, all maximal independent subsets of X have the same number of elements. For example, if E is the set of column labels of a matrix and $\mathcal{I}$ is the collection of linearly independent subsets of E, then $(E, \mathcal{I})$ is a matroid. Moreover, if E is the edge set of a graph G and $\mathcal{I}$ is the collection of edge-sets of forests of G, then $(E, \mathcal{I})$ is also a matroid. These two examples were Whitney's basic classes of matroids and much of what is done in matroid theory, from the terminology used to the types of theorems that are proved, has its origins in linear algebra or graph theory. Immediately from the definition of a matroid, one can see that a matroid is uniquely determined by its minimal dependent sets (*circuits*), its maximal independent sets (*bases*), or its *rank function* r where $r(X)$ is the size of a largest independent subset of X. This talk will introduce the most common ways to define matroids and will then present some fundamental examples, some basic constructions, and some of the main theorems of the subject. A more thorough introduction to matroids is contained in the survey paper "What is a matroid?" available at http://www.math.lsu.edu/˜oxley/survey4.pdf

Speaker **Carles Padro** (Dept. of Applied Math. IV, Univ. Politecnica de Catalunya, Spain)
Title *On the Optimization of Secret Sharing Schemes for General Access Structures*
Abstract In a secret sharing scheme a secret value is distributed into shares among a set of participants in such a way that the qualified subsets of participants can recover the secret value, while the non-qualified ones do not obtain any information about it. In this situation, the size of every share is at least the size of the secret. If all shares have the same size as the secret, which is the best possible situation, the scheme is said to be ideal. Only a few access structures admit an ideal secret sharing scheme. In general, one is interested in finding schemes with optimal share length for every given access structure. This appeared to be a very difficult problem that has attracted the attention of many researchers. Nevertheless, it is far from being solved.

Several methods to find both lower and upper bounds on the share length will be discussed in this talk. We present the most important results and techniques that have been obtained about this open problem from combinatorics, specially from the use of matroids and polymatroids. We discuss as well some combinatorial techniques to construct efficient linear secret sharing schemes.

Speaker **Pradeep Kiran Sarvepalli** (Dept. of Phys. and Astr., Univ. of British Columbia, Canada)
Title *Matroids in Quantum Computing and Quantum Cryptography*
Abstract In this talk I will briefly survey the use of matroids in quantum computation and quantum cryptography. I review a recent work by Shepherd and Bremner which claims that even restricted models of quantum computation, such as those consisting of abelian gates, give rise to probability distributions that cannot be sampled efficiently by a classical computer. I will sketch their arguments that use the theory of binary matroids to substantiate their claim.

I next consider an open problem related to the classification of a class of quantum states called the stabilizer states. A restricted version is to classify the equivalence classes of a subclass of stabilizer states (namely, the CSS states) under the action of the local unitary group and a subgroup of the local unitary group, called the local Clifford group. Specifically, we seek necessary and sufficient conditions as to when a CSS stabilizer state has distinct equivalence classes. I show that CSS stabilizer states whose equivalence classes are distinct must arise from binary matroids which are neither graphic nor co-graphic. In the process we also arrive at a class of minor closed matroids (whose excluded minors appear to be uncharacterized).

Finally, I consider applications of matroids to an important cryptographic primitive namely, quantum secret sharing, which deals with the problem of distribution of a quantum state among n players so that only authorized players can reconstruct the secret. I present the first steps toward a matroidal characterization of quantum secret sharing schemes. This characterization allows us to construct efficient schemes from self-dual matroids that are coordinatizable over a finite field. In the process we also provide a connection between a class of quantum stabilizer codes and secret sharing schemes.

Speaker **Serap A. Savari** (Dept. of ECE, Texas A & M Univ., USA)
Title *A Combinatorial Study of Linear Deterministic Relay Networks*
Abstract In the last few years the “linear deterministic” relay network model has gained popularity as a means of studying the flow of information over wireless communication networks. In this model we consider layered directed graphs, and a node in the graph receives a linear transformation of the signals transmitted to it by neighboring nodes. There is recent work extending the celebrated max-flow/min-cut theorem of Ford and Fulkerson to this model. This result was first established by a randomized transmission scheme over large blocks of transmitted signals. We demonstrate the same result with a simple, deterministic, polynomial-time algorithm which takes as input a single transmitted signal instead of a long block of signals. Our capacity-achieving transmission scheme requires the extension of a one-dimensional Rado-Hall transversal theorem on the independent subsets of columns of a column-partitioned matrix into a two-dimensional variation for block matrices. The rank function arising from the study of cuts in our model has an important difference from the rank functions considered in the literature on matroids in that it is submodular but not monotone.

Speaker **Emina Soljanin** (Alcatel–Lucent Bell Laboratories, Murray Hill, NJ, USA)
Title *Basics of Network Coding*
Abstract Network coding is an elegant and novel technique introduced at the turn of the millennium to improve network throughput and performance. Since then, it has attracted significant interest from diverse scientific communities of engineers, computer scientists, and mathematicians at both academia and industry. This talk will try to answer the first most natural questions one would ask about this new technique, namely, what is network coding and how it works, how network codes are designed, how much it costs to deploy networks implementing such codes, and what kind of benefits one should expect.

Speaker **Alex Sprintson** (Dept. of ECE, Texas A & M Univ., USA)
Title *Applications of Matroid Theory to Network Coding*
Abstract In this talk we discuss the connections between the matroid theory and network coding. We present two ways of constructing new classes of coding networks from matroids. These constructions are instrumental for establishing several important properties of coding networks, such as insufficiency of scalar and vector linear network coding and inachievability of network coding capacity. We present recent results in this research area and outline directions for future work.

Speaker **Pascal O. Vontobel** (Hewlett–Packard Laboratories, Palo Alto, CA, USA)
Title *Pseudo-Codewords: Fractional Vectors in Coding Theory*
Abstract Message-passing iterative decoding has been a very popular decoding algorithm in research and practice for the past fifteen years. Moreover, in the last five years, linear programming decoding has also been a popular topic in coding theory. In both cases, non-zero pseudo-codewords, i.e., certain non-zero fractional vectors, play an important role in the performance characterization of these decoders. This is in contrast to classical coding theory where decoding algorithms were mostly characterized by non-zero codewords.

In this talk we give an overview of results about pseudo-codewords and their influence on message-passing iterative decoding and linear programming decoding. The topics that will be covered include: pseudo-codewords for cycle codes and their relationship to the graph zeta function; pseudo-codewords for finite-geometry-based codes; pseudo-codewords obtained by canonical completion, and how they upper bound the performance of linear programming decoding; the influence of redundant rows in the parity-check matrix on the set of pseudo-codewords; the relationship of pseudo-codewords to other concepts like stopping sets, near-codewords, trapping sets, and absorbing sets.

SPEAKER **Martin Wainwright** (Depts. of EECS and Stat., UC Berkeley, USA)
TITLE *Linear and other Conic Programming Relaxations in Combinatorial Optimization: Graph Structure and Message-Passing*
ABSTRACT There are various hierarchies of linear programming (LP) relaxations, as well as related conic programming relaxations (e.g., SOCP and SDP), that can be applied to a given integer program. We begin with an overview of some of these hierarchies, their on-going applications in coding theory and other areas of applied mathematics, and the connection between such hierarchies and the hypergraph defined by the underlying integer program. We also describe some links between these relaxations, and various types of "message-passing" algorithms that are widely used in communication theory as well as many other domains (e.g., statistical physics, computer vision, machine learning, computational biology).

We then describe some techniques for analysis of LP relaxations in coding theory, including both worst-case and average-case results. In addition, we discuss a line of on-going work on message-passing algorithms that solve LPs and other conic programming relaxations, and some results about convergence rates and rounding techniques.

SPEAKER **Andreas Winter** (Dept. of Math., Univ. of Bristol, UK)
TITLE *A New Inequality for the von Neumann Entropy*
ABSTRACT This talk will be mainly based on a paper with N. Linden. Pippenger has initiated the generalization of the programme to find all the "laws of information theory" to quantum entropy. The standard inequalities derive from strong subadditivity (SSA). SSA of the von Neumann entropy, proved in 1973 by Lieb and Ruskai, is a cornerstone of quantum coding theory. All other known inequalities for entropies of quantum systems may be derived from it. Here we prove a new inequality for the von Neumann entropy which we show is independent of strong subadditivity: it is an inequality which is true for any four party quantum state, provided that it satisfies three linear relations (constraints) on the entropies of certain reduced states. In the talk I will also discuss the possibility of finding an unconstrained inequality (work with N. Linden and B. Ibinson).

SPEAKER **Raymond Yeung** (Dept. of Inform. Engg., The Chinese Univ. of Hong Kong)
TITLE *Facets of Entropy*
ABSTRACT Constraints on the entropy function are sometimes referred to as the laws of information theory. For a long time, the submodular inequalities, or equivalently the nonnegativity of the Shannon information measures, are the only known constraints. Inequalities that are implied by the submodular inequality are categorically referred to as Shannon-type inequalities. If the number of random variables is fixed, a Shannon-type inequality can in principle be verified by a linear program known as ITIP. A non-Shannon-type inequality is a constraint on the entropy function which is not implied by the submodular inequality. In the late 1990s, the discovery of a few such inequalities revealed that Shannon-type inequalities alone do not constitute a complete set of constraints on the entropy function. In the past decade, connections between the entropy function and a number of fields in information science, mathematics, and physics have been established. These fields include probability theory, network coding, combinatorics, group theory, Kolmogorov complexity, matrix theory, and quantum mechanics.

This talk is an attempt to present a picture for the many facets of the entropy function.