Matrix Theory in Quantum Information
Théorie des matrices en information quantique
(Org: **David Kribs** (University of Guelph), **Rajesh Pereira** (University of Guelph) and/et **Sarah Plosker** (Brandon University))

ANNE BROADBENT, University of Ottawa
Specious Adversaries and Quantum Private Information Retrieval

Private information retrieval is a cryptographic scheme that allows a client to secretly query a database. We show that information-theoretic single-server quantum private information retrieval requires a linear amount of communication to be secure against specious adversaries, which are the quantum analog of honest-but-curious adversaries. We also stress the importance of adequate comparison between classical and quantum adversaries—unfair comparisons might lead to an unjustified advantage for the quantum case.

JIANXIN CHEN, University of Guelph
symmetric extension of two-qubit states

Quantum key distribution uses public discussion protocols to establish shared secret keys. In the exploration of ultimate limits to such protocols, the property of symmetric extendibility of underlying bipartite states ρ_{AB} plays an important role. A bipartite state ρ_{AB} is symmetric extendible if there exits a tripartite state $\rho_{ABB'}$, such that the AB marginal state is identical to the AB' marginal state, i.e. $\rho_{AB'} = \rho_{AB}$. For a symmetric extendible state ρ_{AB}, the first task of the public discussion protocol is to break this symmetric extendibility. Therefore to characterize all bi-partite quantum states that possess symmetric extensions is of vital importance. We prove a simple analytical formula that a two-qubit state ρ_{AB} admits a symmetric extension if and only if $tr(\rho_B^2) \geq tr(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$. Given the intimate relationship between the symmetric extension problem and the quantum marginal problem, our result also provides the first analytical necessary and sufficient condition for the quantum marginal problem with overlapping marginals.

BENOIT COLLINS, University of Ottawa / AIMR
Free probability and quantum information theory

We are interested in the behavior of typical quantum channels with large input space and small output space. We show that the output set of these quantum channels is almost deterministic, and that it can be described through free probability techniques. We compute the minimum output entropy of these typical quantum channels, and as an application, we obtain new bounds for the violation of the minimum output entropy. This is a report on joint works with S. Belinschi and I. Nechita.

JASON CRANN, Carleton University/University of Lille 1
Manifestations of duality in quantum information

The recent representation theory surrounding locally compact groups has initiated several new connections between harmonic analysis and quantum information. In this talk, we will use this theory to generate two "dual" classes of quantum channels for every locally compact group. Focusing mainly on finite groups we will explore their properties from the point of view of quantum information such as noiseless subsystems, quantum capacities and entanglement preservation. Time permitting, we will present further manifestations of this duality, in particular its connection to the complementarity of private and correctable subsystems. This is joint work with Matthias Neufang.

NICOLAS DELFOSSE, Université de Sherbrooke
Percolation and quantum error correction

Surface codes, introduced by Kitaev, are quantum error-correcting codes defined from a tiling of surface. First, we recall how the parameters of the surface code are related with the properties of the tiling of surface. Then, we observe the similarities between quantum erasures and percolation theory. Using these similarities, we derive an upper bound on the percolation threshold of a family of hyperbolic lattices from results of quantum information theory. This talk is based on joint work in progress with Gilles Zémor.

DOUG FARENICK, University of Regina
Dual matrix systems and Tsirelson's problem

A matrix system $\mathcal{S}$ is a $*$-vector space of complex $n \times n$ matrices that contains the identity matrix. By a theorem of Choi and Effros, the dual space $\mathcal{S}^d$ of a matrix system $\mathcal{S}$ has the structure of an operator system. In this lecture I will report on joint work with A. Kavruk, V. Paulsen, and I.G. Todorov whereby Tsirelson's problem on quantum correlations is cast in terms of states on certain tensor products of dual matrix operator systems.

MARK GIRARD, Institute for Quantum Science and Technology - University of Calgary
On Convex Optimization Problems in Quantum Information

The evaluation of many important quantities in quantum information theory involves finding the solution to a convex optimization problem, usually in the form of minimizing a convex function over a convex subset of hermitian matrices. For example, determination of the relative entropy of entanglement (REE) for an arbitrary quantum state ρ amounts to minimizing the relative entropy of ρ with respect to the convex set of separable states. While finding closed fomulae solutions to such convex optimization problems is usually impossible, solving the converse problem is often instructive and enlightening in regard to the original problem. That is, given a family of convex functions and a state σ on the boundary of a subset of hermitian matrices, we can find all functions whose minimum value is achieved at σ. In particular, this allows us to determine explicit expressions for the REE and its variants, such as the Rains bound. This approach also elucidates interesting facts about these quantities, such as, among others, that the Rains bound reduces to the REE when at least one subsystem is a qubit.

GILAD GOUR, University of Calgary
Towards a complete classification of multipartite entanglement

Multi-particle entanglement is an essential resource for a variety of quantum information processing tasks. Yet, despite an enormous amount of literature dedicated to its study, our current understanding of it is still in its infancy. In this talk I will introduce a systematic classification of multiparticle entanglement in terms of equivalence classes of states under stochastic local operations and classical communication (SLOCC). I will show that such an SLOCC equivalency class of states is characterized by ratios of homogenous polynomials that are invariant under local action of the special linear group. I will then introduce a complete construction of the set of all such SL-invariant polynomials (SLIPs). The construction is based on Schur-Weyl duality and applies to any number of qudits in all (finite) dimensions. In addition, I will introduce an elegant formula for the dimension of the homogenous SLIPs space of a fixed degree as a function of the number of qudits. The expressions for the SLIPs involve in general many terms, but for the case of qubits can be written in a much simpler form.

NATHANIEL JOHNSTON, Institute for Quantum Computing, University of Waterloo
Separability from Spectrum for Qubit-Qudit States

The separability from spectrum problem asks for a characterization of the eigenvalues of the bipartite mixed states ρ with the property that $U^*\rho U$ is separable for all unitary matrices U. This problem has been solved when the local dimensions m and n satisfy $m = 2$ and $n \leq 3$. We solve all remaining qubit-qudit cases (i.e., when $m = 2$ and $n \geq 4$ is arbitrary). In all of these cases we show that a state is separable from spectrum if and only if $U^*\rho U$ has positive partial transpose for all unitary matrices U. This equivalence is in stark contrast with the usual separability problem, where a state having positive partial transpose is a strictly weaker property than it being separable.

JEREMY LEVICK, University of Guelph
The Four-Dimensional Perfect Mirsky Conjecture

A square matrix with non-negative entries, all of whose rows and columns sum to 1 is called a doubly stochastic matrix. The set of such matrices of size $n \times n$ is denoted Ω_n. Doubly stochastic matrices are closely tied to majorization, a partial order on vectors in $\mathbb{R}^n$, a connection made explicit by the Hardy-Littlewood-Polya theorem. Majorization plays an important role in quantum information, where it can be used to compare entanglement of two quantum states. In 1965, Perfect and Mirsky conjectured that the region of all possible eigenvalues of all $n \times n$ doubly stochastic matrices (denoted ω_n) would be the union of the regions Π_k for $k \in \{1, 2, \cdots, n\}$, where Π_k is the convex hull of the k^{th} roots of unity. They proved the conjecture for $n = 1, 2, 3$. In 2007, Rivard and Mashreghi exhibited a counterexample for $n = 5$. We prove the Perfect-Mirsky conjecture for $n = 4$, and provide a new conjecture for which Rivard and Mashreghi's example is not a counterexample. We also discuss some geometric interpretations of the problem of characterizing ω_n.

CHI-KWONG LI, College of William and Mary
Decomposition of unitary gates

In quantum information science, quantum gates acting on vector states are unitary transformations. It is desirable from the theoretical as well as practical point of view to decompose a general unitary transformation into simple ones that are easy to control and implement. In this talk, we will describe some current research on this topic.

MARCO MERKLI, Mathematics, Memorial University
Repeated Quantum Measurement Processes

We consider a sequence of probes, sent to interact one by one with a fixed scatterer. Before interaction, the probes are independent, but they become entangled via the contact with the scatterer. After a probe finishes interacting with the scatterer, a quantum measurement is performed on the probe. The measurement history, i.e., the collection of measurement outcomes, is a stochastic process. We analyze the convergence and fluctuation properties of this process by linking its asymptotic evolution to spectral characteristics of the dynamics.

VARUN NARASIMHACHAR, University of Calgary
Majorization theory and thermodynamics

Majorization is a concept that emerges from the properties of stochastic matrices. The theory of majorization has been identified as an important tool in quantum information since its application to the theory of entanglement by Nielsen. Later works have identified other areas of quantum information where it plays a role, including thermodynamics. In this talk, we describe the connection between majorization theory and thermodynamics, with a summary of our recent results in this area. These include necessary and sufficient conditions for transitions between thermodynamic states of quantum systems, under various conditions (with or without catalysts, costing or yielding work, small or large systems). Notably, our results imply the insufficiency of the traditional formulation of the Second Law to decide the feasibility of state transitions.

Based on the work in http://arxiv.org/abs/1309.6586

MUNEERAH AL NUWAIRAN, University of Ottawa
EPOSIC Channels

In this work, we introduce the EPOSIC channels, a class of SU(2)-irreducibly covariant quantum channels. We show that if H and K are SU(2)-irreducible spaces then the EPOSIC channels from End(H) into End(K) are the extreme points of the convex set of all SU(2)-irreducibly covariant channels from End(H) into End(K). We get a set of Kraus operators, the Choi matrix, a complementary channel, and the dual map of EPOSIC channel. As an application of the EPOSIC channels, we get a new example of a positive map that is not completely positive. We obtain a bound for the minimal output entropy of the tensor product of two SU(2)-irreducibly covariant channels. We also examine the E.B.T property of EPOSIC channels.

SARAH PLOSKER, Brandon University
Dirichlet Polynomials, Majorization, and Trumping

Majorization and trumping are two partial orders that have proved useful in entanglement theory. We show some relations between these two partial orders and generalized Dirichlet polynomials, Mellin transforms, and completely monotone functions. These relations are used to prove a succinct generalization of Turgut's characterization of Trumping. This is joint work with R. Pereira.

RAYMOND SZE, The Hong Kong Polytechnic University
State Transformation Problem in Quantum Information

One of the fundamental problems quantum information scientists concerned with, is whether one can design and construct a quantum device that transforms certain quantum states into other quantum states. This task is physically possible if a specified quantum operation (transformation) of certain prescribed sets of input and output states can be found. The problem then becomes to determine an existence condition of a trace preserving completely positive map sending ρ_j to σ_j for all j, for certain given sets of quantum states $\{\rho_1, \ldots, \rho_k\}$ and $\{\sigma_1, \ldots, \sigma_k\}$. This is called the problem of state transformation. In this talk, recent results on this problem will be presented.