Optimization Techniques in Quantum Information Theory
Techniques d'optimisation en théorie de l'information quantique
(Org: **Nathaniel Johnston** (Mount Allison University), **Rajesh Pereira** (University of Guelph) and/et **Sarah Plosker**
(Brandon University))

ERIC CHITAMBAR, Southern Illinois University
A Classical Analog to Entanglement Reversibility

In this talk I describe intriguing similarities between the quantum theory of entanglement and the classical theory of secret key. Just as entanglement can be shared by two or more quantum systems, secret correlations can be shared by two or more classical systems, whose states are described by probability distributions. Entanglement cannot be increased under local (quantum) operations and classical communication, and likewise secret correlations cannot be increased under local (classical) operations and public communication. Analogous to the tasks of entanglement distillation and formation are the classical tasks of secret key distillation and secrecy formation.

An old open problem in entanglement theory involves characterizing the states that possess reversible entanglement; i.e. states whose rate of entanglement distillation equals its rate of entanglement cost. In this talk, I introduce a similar notion of reversible secrecy. When one of the honest parties holds a binary random variable, the structure of distributions possessing reversible secrecy can be identified exactly. An indispensable tool used in this analysis is a conditional form of the Gacs-Korner common information. Finally, I describe how the structure of distributions possessing reversible secrecy can be related to the structure of quantum states possessing reversible entanglement.

RICHARD CLEVE, University of Waterloo
Efficient Quantum Algorithms for Simulating Lindblad Evolution

The Lindblad equation is the natural generalization to open systems of the Schroedinger equation. We give a quantum algorithm for simulating the evolution of an n-qubit system for time T under the Lindblad equation with local terms. The gate cost of the algorithm is optimal within polylogarithmic factors. A key component of our algorithm is a new "linear combinations of unitaries" construction that pertains to channels which we believe is of independent interest. This is joint work with Chunhao Wang.

HOAN DANG, University of Calgary
Galois-unitary symmetry of mutually unbiased bases as a toy model for SIC-POVMs

Besides applications in quantum information, symmetric informationally-complete (SIC) POVMs have deeply interesting mathematical properties due to their high degree of symmetry. Here we focus on g-unitary symmetry, which is a generalized notion of anti-unitary symmetry. G-unitary operators are defined with respect to a number field extension. For the case of mutually unbiased bases (MUB) where the relevant field extension is simple, we find that g-unitaries help us to solve problems such as MUB-cycling and finding MUB-balanced states.

DOUG FARENICK, University of Regina
Some extremal properties of quantum probability measures

A quantum probability measure is a positive operator-valued measure (POVM) whose value on the entire sample space is the identity operator acting on a Hilbert space H. In the event that H is 1-dimensional, then a quantum probability measure is simply a probability measure in the classical sense. Optimality questions are often linked to the issues of optimisation on a convex set, in which case knowledge of the extreme points of the convex set becomes important. In this lecture, I will discuss the structure of extreme points and C*-extreme points in the space of quantum probability measures, and explain

how quantum probability measures that satisfy a certain norm-theoretic optimality condition are related to the C*-extreme points. In connection with this latter result, the role of operator systems in the analysis of quantum probability measures will be explained. This lecture is drawn from collaborative work with R. Floricel, S. Plosker, and J. Smith.

SEVAG GHARIBIAN, Virginia Commonwealth University

Classical approximation algorithms for quantum constraint satisfaction problems

The study of approximation algorithms for Boolean satisfiability problems such as MAX-k-SAT is a well-established line of research. In the quantum setting, there is a physically motivated generalization of MAX-k-SAT known as the k-Local Hamiltonian problem (k-LH), which is of interest for two reasons: From a complexity theoretic perspective, k-LH is complete for the quantum analogue of NP, and from a physics perspective, k-LH asks one to estimate the energy of a quantum system when cooled to very low temperatures. For the latter reason in particular, the condensed matter physics community has devoted decades to developing heuristic algorithms for k-LH and related problems. However, recent years have witnessed the development of the first classical approximation algorithms for k-LH, which shall be the focus of this talk. We will begin with an introductory overview of some existing results, with no background in quantum computing assumed. We will then discuss recent work in progress on generalizing the celebrated Goemans-Williamson algorithm for MAX-CUT to approximate physically motivated special cases of k-LH. The latter is joint work with Yi-Kai Liu (NIST, USA).

MARK GIRARD, University of Calgary

Conversion witnesses for transforming quantum states under PPT-operations.

The primary goal in entanglement theory is to find conditions that determine whether one quantum state can be converted into another under the restriction to local operations and classical communication (LOCC). This is typically done by considering entanglement monotones, but this analysis is difficult due to the fact that the LOCC operations are difficult to describe. It is common to instead consider the larger, yet easier to describe mathematically, class of operations that preserve positivity under partial transpose (PPT). I consider the problem of finding conditions for PPT-conversion of bipartite states in the single-shot regime. In this talk, I will present a family of PPT-conversion witnesses and a new entanglement monotone that are based on the binegativity. I'll finish by presenting a new complete witness for PPT-conversion that is derived using duality properties of semidefinite programs.

GILAD GOUR, University of Calgary

Semidefinite Programming and Quantum Resource Theories

One of the main goals of any resource theory such as entanglement, quantum thermodynamics, quantum coherence, and asymmetry, is to find necessary and sufficient conditions (NSC) that determine whether one resource can be converted to another by the set of free operations. In this talk I will present such NSC for a large class of quantum resource theories which we call affine resource theories (ARTs). ARTs include the resource theories of athermality, asymmetry, and coherence, but not entanglement. Remarkably, the NSC can be expressed as a family of inequalities between resource monotones (quantifiers) that are given in terms of the conditional min entropy. The set of free operations is taken to be (1) the maximal set (i.e. consists of all resource non-generating (RNG) quantum channels) or (2) the self-dual set of free operations (i.e. consists of all RNG maps for which the dual map is also RNG). As an example, I will discuss the applications of the results to quantum thermodynamics with Gibbs preserving operations, and several other ARTs. Finally, I will discuss the applications of these results to resource theories that are not affine.

DAVID KRIBS, University of Guelph

Private Algebras, Private Quantum Channels, etc

In this talk, I will discuss my ongoing work with collaborators on the development of a structure theory for a fundamental notion in quantum privacy; known in different settings as private quantum channels, private quantum codes, quantum secret sharing, private subsystems, decoherence-full subsystems, and private algebras. I'll also discuss connections with quantum error

correction. Based on joint works with Jason Crann, Tomas Jochym-O'Connor, Raymond Laflamme, Rupert Levene, Jeremy Levick, Rajesh Pereira, Sarah Plosker, and Ivan Todorov.

JEREMY LEVICK, University of Guelph
An Uncertainty Principle for Quantum Channels

We present an "uncertainty principle" for quantum channels, showing a relationship between the dimension of the range of a channel and the dimension of the range of its complement. We examine some interesting specific cases, and discuss consequences for privacy of quantum channels.

CHI-KWONG LI, College of William and Mary
Quantum states with prescribed reduced states, and special Quantum channels

We consider the set of quantum states with prescribed reduced states, and the set of quantum channels with special properties. In particular, we study the geometrical properties of these sets, and special elements attaining optimal values of certain functions.

SAEID MOLLADAVOUDI, University of Ottawa
Symmetry Reduction in Multiparty Quantum States

Symmetries are ubiquitous in natural phenomena and also in their mathematical descriptions and according to a general principle in Mathematics, one should exploit a symmetry to simplify a problem whenever possible. In this talk, we focus on elimination of continuous symmetries from multi-particle quantum systems and discuss that the existing methods equip us with a powerful set of tools to compute geometrical and topological invariants of the resulting reduced spaces. As an intermediate step, we consider the maximal torus subgroup T of the compact Lie group of Local Unitary operations K and elaborate on the symmetry reduction procedure and use methods from symplectic geometry and algebraic topology to obtain some of the topological invariants of these relatively well-behaving quotients for multi-particle systems containing r qubits. We elaborate on an explicit example with two qubits and discuss further implications in quantum information theory.

SARAH PLOSKER, Brandon University
Optimal bounds on fidelity of quantum state transfer with respect to errors

Quantum state transfer within a quantum computer can be achieved through the use of a quantum spin chain as a "data bus" for quantum states. More generic graphs besides a chain can also be used to perform this important task. The fidelity, which measures the closeness between two quantum states, is used to determine the accuracy of the state transfer. Ideally the fidelity is 1, representing perfect state transfer. We analyse the sensitivity of the fidelity of a graph exhibiting perfect state transfer to small perturbations in readout time and edge weight in order to obtain physically relevant bounds on the fidelity.

Joint work with Whitney Gordon, Steve Kirkland, Chi-Kwong Li, and Xiaohong Zhang

---

ZBIGNIEW PUCHALA, Institute of Theoretical and Applied Informatics, Polish Academy of Sciences
Asymptotic properties of random quantum channels

We consider random quantum channels, especially the limiting behaviour of the diamond norm for two independent random quantum operations. In order to define random channels we use the Choi-Jamiołkowski isomorphism and consider Wishart matrices with normalized partial trace. Next, we derive an asymptotic behaviour of empirical eigenvalue distribution for this ensemble and, using free probability theory, we derive the eigenvalue distribution for the difference of two random Choi-Jamiołkowski matrices. We show the concentration of measure occurs for the diamond norm. In the case of flat measure on random channels, the limiting value of the diamond norm is equal to $\frac{1}{2} + \frac{2}{\pi}$.

DANIEL PUZZUOLI, University of Waterloo
Ancilla dimension in quantum channel discrimination

Single-shot quantum channel discrimination is a fundamental task in quantum information theory. It is well known that entanglement with an ancillary system can help in this task. Thus, a fundamental question is: For a given pair of channels with the same input and output spaces, how much entanglement is necessary to optimally discriminate them? I will present results on a specific formulation of this question: Given a pair of channels, what is the minimum ancilla dimension necessary for optimal discrimination? It is known that, in general, an ancilla with dimension equal to that of the input space of the channels is always sufficient (and is sometimes necessary) for optimal discrimination. A natural question to ask is whether the same holds true for the output dimension. That is, in cases when the output dimension of the channels is (possibly much) smaller than the input dimension, is an ancilla with dimension equal to the output dimension always sufficient for optimal discrimination? I will present a family of counterexamples which show that the answer to this question is no. This family contains instances with arbitrary finite gap between the input and output dimensions, and still has the property that in every case, for optimal discrimination, it is necessary to use an ancilla with dimension equal to that of the input.

JAMIE SIKORA, Centre for Quantum Technologies, National University of Singapore
Completely Positive Semidefinite Rank

A matrix X is called completely positive semidefinite (cpsd) if it can be represented as a Gram matrix of positive semidefinite matrices of some finite size d. The cpsd-rank of a cpsd matrix is the smallest integer d for which such a representation is possible. In this work, we initiate the study of the cpsd-rank which we motivate twofold. First, the cpsd-rank is a natural non-commutative analogue of the completely positive rank of a completely positive matrix. Second, we show that the cpsd-rank is physically motivated as it can be used to upper and lower bound the size of a quantum system needed to generate a quantum behavior. Unlike the completely positive rank which is at most quadratic in the size of the matrix, no general upper bound is known on the cpsd-rank. In fact, we show that the cpsd-rank can be exponential in terms of the size. The proof relies crucially on the connection between the cpsd-rank and quantum behaviors. In particular, we use a known lower bound on the size of matrix representations of extremal quantum correlations which we apply to high-rank extreme points of the n-dimensional elliptope.

This is joint work with Anupam Prakash, Antonios Varvitsiotis, and Zhaohui Wei (arXiv:1604.07199).

JOHN WATROUS, University of Waterloo
Semidefinite programming, cone programming, and quantum state discrimination

Semidefinite programming has found many applications in the theory of quantum information. In this talk I will will give a brief introduction to semidefinite programming and its applications to the study of quantum information, and also discuss the more general setting of cone programming and its application to a problem relating to quantum state discrimination by spatially separated parties. The talk will include joint work with Somshubhro Bandyopadhyay, Alessandro Cosentino, Nathaniel Johnston, Vincent Russo, and Nengkun Yu.

XIAOHONG ZHANG, University of Manitoba
Hadamard diagonalizable PST graphs

Our work focuses on Hadamard diagonalizable graphs. For integer-weighted Hadamard diagonalizable graphs, we give an eigenvalue characterization of when such a graph exhibits perfect state transfer (PST) at time $\pi/2$, and then generalize the result to rational-weighted Hadamard diagonalizable graphs. We also define a new binary graph operation, the merge, which keeps the property of being Hadamard diagonalizable, and can be used to produce a lot of PST graphs. We give conditions on two integer-weighted Hadamard diagonalizable graphs for their merge to have PST. Finally we show an intriguing result about the merge operation: if exactly one of the two weights on this operation is an integer, and the other one is an irrational number, then the merge exhibits pretty good state transfer (PGST) from one vertex to several other vertices under certain circumstances.

KAROL ZYCZKOWSKI, Jagiellonian University, Cracow, Poland
Distinguishing generic quantum states

Properties of random mixed states of dimension N distributed uniformly with respect to the Hilbert-Schmidt measure are investigated. We show that for large N, due to the concentration of measure phenomenon, the trace distance between two random states tends to a fixed number $1/4 + 1/\pi$, which yields the Helstrom bound on their distinguishability. To arrive at this result we apply free random calculus and derive the symmetrized Marchenko–Pastur distribution. Asymptotic value for the root fidelity between two random states, $\sqrt{F} = 3/4$, can serve as a universal reference value for further theoretical and experimental studies. Analogous results for quantum relative entropy and Chernoff quantity provide other bounds on the distinguishability of both states in a multiple measurement setup due to the quantum Sanov theorem. Entanglement of a generic mixed state of a bi–partite system is estimated.