Quantum Information Theory
Théorie de l'information quantique
(Org: **Richard Cleve** (Waterloo))

GILAD GOUR, University of Calgary, Department of Mathematics and Statistics, Calgary, Alberta
Quantum Resource Theories and Super Selection Rules

In quantum information theory entanglement arises due to the restriction to local operations and classical communication (LOCC). In particular, entanglement can be considered as a quantum resource with which spatially separated parties can overcome or at least partly overcome the limitation of LOCC. Clearly, different types of restrictions corresponds to different kinds of quantum resource theories (QRTs). In this talk I will discuss the QRTs that emanate from various natural constraints. I will focus on QRTs that follow from the presence of super-selection rules or the absence of shared reference frames. In particular, I will discuss the analogies and distinctions between and among the different QRTs and show that, in general, QRTs in many aspects are very similar to entanglement theory. Such comparisons provide a much broader perspective on all of these resource theories and allow us to use the insights gained from one QRT to solve the problems that arise in the context of another QRT.

Joint work with Rob Spekkens.

PATRICK HAYDEN, McGill University
A reverse Shannon theorem for quantum broadcast channels

A reverse Shannon theorem characterizes the resources required to simulate a given noisy channel. The quantum reverse Shannon theorem for single-sender/single-receiver channels, a joint effort of Bennett, Devetak, Harrow, Shor and Winter, established that a single number can be used to characterize the strength of such channels in the presence of free entanglement. In this talk I'll explain how to prove an optimal reverse Shannon theorem for quantum channels with a single sender but many receivers, known as broadcast channels. Surprisingly, the simulation cost for a broadcast channel can be characterized by a simple, tractable optimization problem even though no such simple solution has been found for the capacity region itself, even in the classical case.

Joint work with Frederic Dupuis.

DEBBIE LEUNG, University of Waterloo
Approximate error correction

We will discuss a construction based on quantum list-codes, and its application to adversarial quantum channels.

Joint work with Graeme Smith.

AIDAN ROY, University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4
Weighted complex projective 2-designs from bases

We introduce the problem of constructing weighted complex projective 2-designs from the union of a family of orthonormal bases. If the weight remains constant across elements of the same basis, then such designs can be interpreted as generalizations of complete sets of mutually unbiased bases, being equivalent whenever the design is composed of $d+1$ bases in dimension d. We show that, for the purpose of quantum state determination, these designs specify an optimal collection of orthogonal

measurements. Using highly nonlinear functions on abelian groups, we construct explicit examples from $d+2$ orthonormal bases whenever $d+1$ is a prime power, covering dimensions $d+d=6$, 10, and 12, for example, where no complete sets of mutually unbiased bases have thus far been found.

This is joint work with Andrew Scott.

BARRY SANDERS, University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4

Information-theoretic security for authenticated long-distance quantum key distribution with partial trust networks

Quantum key distribution must overcome two important hurdles: authentication to avoid the man-in-the-middle attack and relays or repeaters to allow long-distance communication. Current feasible approaches suggest complete trust of intermediate nodes in a network. We show that, in a network of partially trusted nodes (even with a low level of trust), our scheme enables probabilistic information-theoretic secure authentication and long-distance key distribution based on existing quantum key distribution technology, thus making our approach feasible now without reliance on total trust of intermediate nodes.

ALAIN TAPP, Université de Montréal

Anonymous message transmission

Anonymous message transmission is the task by which a sender transmits to a receiver a private message in such a way that the receiver does not know who, within the user group, actually sent the message. Furthermore, the rest of the users do not learn anything. The case involving classical messages has been recently solved by A. Broadbent and A. Tapp. They have proposed an information theoretically secure protocol, based solely on pairwise authentic private channels, that tolerates an arbitrary number of corrupted players. I will present a protocol that accomplishes the same goal, in the same model, but with quantum messages.

This work has been done in collaboration with G. Brassard, A. Broadbent, J. Fitzsimons and S. Gambs.