Quantum Information Theory Session
Théorie de l'information quantique

(Org: **Jason Crann** (Carleton University) and/et **Arthur Mehta** (University of Ottawa))

MAHMUD AZAM, University of Saskatchewan
TQFTs and Quantum Computing

Quantum computing is captured in the formalism of the monoidal subcategory M of the category $\mathrm{Vect}_{\mathbb{C}}$ of complex vector spaces generated under tensor products by $\mathbb{C}^2$ — in particular, quantum circuits can be seen as diagrams in this category — while topological quantum field theories, in the sense of Atiyah, are diagrams in $\mathrm{Vect}_{\mathbb{C}}$ indexed by a cobordism category. We outline a program to formalize a connection between these two scenarios. In doing so, we first equip cobordisms with machinery for producing $\mathbb{C}$–linear maps by parallel transport along curves under a connection and then assemble these structures into a higher category. The category M above is also given a suitable higher categorical structure which we call $\mathbb{F}\mathrm{Vect}_{\mathbb{C}}$. Finally, we realize quantum circuits as images of these cobordisms with additional structure under a higher monoidal functor to $\mathbb{F}\mathrm{Vect}_{\mathbb{C}}$, which are computed by taking parallel transports of vectors and then combining the results in a pattern encoded in the domain of the functor. This talk reports on joint work with Steven Rayan.

XIAONING BIAN, Dalhousie University
Generators and relations for 3-qubit Clifford+CS operators

We give a presentation by generators and relations of the group of 3-qubit Clifford+CS operators. The proof roughly consists of two parts: (1) applying the Reidemeister-Schreier theorem repeatedly to an earlier result of ours; and (2) the simplification of thousands of relations into 17 relations. Both (1) and (2) have been formally verified in the proof assistant Agda. The Reidemeister-Schreier theorem gives a constructive method for computing a presentation of a sub-monoid given a presentation of the super-monoid. To achieve (2), we devise an almost-normal form for Clifford+CS operators. Along the way, we also identify several interesting structures within the Clifford+CS group. Specifically, we identify three different finite subgroups for whose elements we can give unique normal forms. We show that the 3-qubit Clifford+CS group, which is of course infinite, is the amalgamated product of these three finite subgroups. This result is analogous to the fact that the 1-qubit Clifford+T group is an amalgamated product of two finite subgroups.

DAVID CUI, Massachusetts Institute of Technology
Sum-of-squares decompositions and nonlocal games

Any nonlocal game has an associated game polynomial representing its winning probability. Exhibiting a sum-of-squares decomposition of this game polynomial gives an upper-bound on the quantum value of the nonlocal game. Such decompositions can be numerically found via a complete hierarchy of semidefinite programs and thus are powerful tools in the theory of nonlocal games. In this talk, we'll discuss how sum-of-squares decompositions can give us self-testing results for nonlocal games and upper-bounds for multipartite games on quantum networks. This is partly based on joint work with Arthur Mehta, Hamoon Mousavi, and Sajjad Nezhadi.

ERIC CULF, University of Waterloo
Coset states in Uncloneable Cryptography

The coset state structure has proven useful on multiple occasions in quantum information, for example in the context of the hidden subgroup problem and stabiliser codes. A basis of coset states exists for every vector subspace of a space of bitstrings, and the elements of the basis are indexed by the coset representatives of the subspace and its orthogonal complement — this provides a large amount of algebraic structure. Recently, Coladangelo, Liu, Liu, and Zhandry [Crypto 2021] introduced a monogamy-of-entanglement (MoE) game based on this structure. We extend this game to construct a variety of uncloneable cryptographic protocols.

First, we show that one of the two cooperating players can learn the other player's answer without significantly affecting the winning probability of the MoE game. This allows to construct a variety of novel cryptographic primitives including a form of uncloneable encryption where decryption uses an interaction between the sender and the receiver, and a stronger form of one-sided device independent quantum key distribution (1S DI QKD) where the receiver's classical device may also be assumed to be untrusted. Our other extension is to show that a comparable MoE property holds for coset states of a wide variety of groups, including infinite-order compact and locally compact abelian groups. This gives rise to an extension of the 1S DI QKD protocol to continuous-variable quantum systems.

This talk is based on joint work with Anne Broadbent (arxiv.org/abs/2303.00048); and with Victor V. Albert and Thomas Vidick (arxiv.org/abs/2212.03935).

SAM HARRIS, Northern Arizona University
Quantum reductions of synchronous games to graph games

Synchronous games that are equivalent, in some sense, preserve certain properties about winning strategies. In this talk, we will see how one can transform any synchronous game into a graph homomorphism game. More specifically, we'll see that every synchronous game is equivalent, in some weak sense, to a three-coloring game for an associated undirected graph, and we'll give an upper bound on the number of vertices required for the graph. As a result, we will obtain a quantum version of Lovasz's reduction theorem of the k-coloring problem of a graph to the 3-coloring problem of a graph that holds in all quantum models, extending and simplifying the work of Z. Ji in the finite-dimensional model. This work uses a weak *-equivalence of games that we will describe.

NATHANIEL JOHNSTON, Mount Allison University
Absolute k-Incoherence and Antidistinguishability

We explore the quantum resource theory of k-incoherence, in which the free states are those that can be written as a convex combination of pure states with at most k non-zero entries. In particular, we investigate the set of quantum states that can be shown to be k-incoherent based only on their eigenvalues. In analogy with the absolute separability problem, we call these states "absolutely k-incoherent", and we derive several necessary and sufficient conditions for membership in this set. As an application of our results, we derive a correct version of a recently-disproved conjecture about antidistinguishability of quantum states.

NICHOLAS LARACUENTE, University of Chicago
Information Fragility or Robustness of Quantum States and Processes

How quickly can weak noise destroy information in a quantum system? Several forms of this question can be phrased in terms of the ratio between initial and decayed quantum relative entropy. We consider relevant analytic properties of relative entropy, including how it relates to positive semidefinite order and von Neumann algebra inclusion indices. We emphasize regimes of extremely fast or slow decay, including when non-classical features enable such extremes.

DEBBIE LEUNG, University of Waterloo
Rate-Distortion Theory for Mixed States Ensembles

Consider the compression of asymptotically many i.i.d. copies of ensembles of mixed quantum states where the encoder has access to a general side information system. The figure of merit is per-copy error. Rate-distortion theory studies the trade-off between the compression rate and the per-copy error. The rate-distortion function is the best compression rate given a certain distortion. In this talk, we derive the rate-distortion functions of mixed-state compression in the entanglement-assisted and unassisted scenarios, and also for the general setting where the consumption of both communication and entanglement are considered. We will discuss consequences of our results and open problems. Joint work with Zahra Baghali Khanian and Kohdai Kuroiwa.

SÉBASTIEN LORD, University of Ottawa
Uncloneable Quantum Advice

In this work, we initiate the study of the computational complexity of cloning fixed sequences of quantum states. This is in contrast to prior studies of the no-cloning principle where the states to be copied are not fixed, but rather selected at random from some larger set.

We frame our main results as the instantiation of uncloneable quantum advice for certain specific promise problems and languages. A quantum advice state can be understood as a quantum program which is run by a user to solve a given problem instance. Thus, uncloneable quantum advice can be viewed as a contribution to the larger ongoing quest in quantum cryptography to construct copy-protection schemes for interesting functionalities. Indeed, existing quantum copy-protection schemes only offer security if the program to be copy-protected is chosen at random from some larger family. Our work establishes a proof-of-principle that a version of copy-protection for fixed and specific programs is achievable.

Joint work with Anne Broadbent and Martti Karvonen.

HERMIE MONTERDE, University of Manitoba
Low fidelity quantum transmission

A quantum spin network is modelled by an undirected graph X, where the vertices and edges of X represent the qubits in the network and their interactions, respectively. The fidelity (probability) of quantum state transfer from vertex u to vertex v at time t is given by the modulus of the (u, v) entry of the unitary operator $U(t) = \exp(itH)$, where H is the Hamiltonian of the quantum system. Most studies focus on high fidelity quantum transmission between distinct vertices in a graph (such as perfect state transfer and pretty good state transfer). In this talk, we discuss low fidelity quantum transmission and provide several infinite families of graphs that exhibit such a property. This talk is based on the paper *https://arxiv.org/abs/2303.06297*.

ASHWIN NAYAK, University of Waterloo
Optimal lower bounds for Quantum Learning via Information Theory

We revisit two problems in learning theory, in which the goal is to learn some property given copies ("samples") of the same quantum state. We derive optimal lower bounds on the number of samples required to solve these problems, using a combination of algebraic and information-theoretic techniques. The resulting proofs are both simpler and shorter than those given before.

(Based on work with Shima Bab Hadiashar and Pulkit Sinha.)

CONNOR PADDOCK, University of Ottawa
Satisfiability problems and algebras of boolean constraint system games

Properties of boolean constraint system (BCS) algebras characterize various types of perfect entangled strategies for BCS nonlocal games. These different types of perfect strategies suggest various generalized notions of satisfiability for constraint systems. We construct a constraint system which is C^*-satisfiable but not tracially satisfiable. We show that reductions between constraint systems can be captured as homomorphisms between BCS algebras, and use this point of view to streamline and strengthen several results of Atserias, Kolaitis, and Severini [AKS'19]. In particular, we show that the question of whether there is a hyperlinear group is linked to proving dichotomy theorems for $\mathcal{R}^{\mathcal{U}}$-satisfiability of constraint systems. We also point out a number of additional open problems with other types of satisfiability.

QUANTUM INFORMATION THEORY TALK AND TUTORIAL: YUMING ZHAO, University of Waterloo
Introduction to quantum self-testing

Suppose we have a physical system consisting of two separate labs, each capable of making a number of different measurements. If the two labs are entangled, then the measurement outcomes can be correlated in surprising ways. In quantum mechanics, we model physical systems like this with a state vector and measurement operators. However, we do not directly see the state vector and measurement operators, only the resulting measurement statistics (which are referred to as a *correlation*). There are typically many different models achieving a given correlation. Hence it is a remarkable fact that some correlations have a unique quantum model. A correlation with this property is called a self-test.

This tutorial will offer an introduction to self-testing and relevant mathematics. Particular focus will be given to the operator-algebraic perspective of understanding self-testing and the use of approximate representation theory in proving robustness.

THOMAS THEURER, University of Calgary
Resource theory of quantum thermodynamics: State convertibility from qubit cooling and heating

Thermodynamics plays an important role both in the foundations of physics and in technological applications. An operational perspective adopted in recent years is to formulate it as a quantum resource theory. I will begin with a quick introduction to the general framework of quantum resource theories, in particular motivating it and explaining why the convertibility of resourceful states is at its core. I will then specialize to the resource theory of quantum thermodynamics and present recent results that I found in collaboration with Elia Zanoni, Carlo Maria Scandolo, and Gilad Gour: We solved the question of how in the quantum limit, thermal non-equilibrium can be used to heat and cool other quantum systems that are initially at thermal equilibrium. We then showed that the convertibility between quasi-classical resources (resources that do not exhibit coherence between different energy eigenstates) is fully characterized by their ability to cool and heat qubits, i.e., by two of the most fundamental thermodynamical tasks on the simplest quantum systems. We, therefore, characterized the core problem of the resource theory of thermodynamics with operationally relevant tasks.

DAVE TOUCHETTE, Université de Sherbrooke

SHERRY WANG, University of Ottawa
Post-quantum Technologies: Password Authentication and Digital Credentials

In a post-quantum world, where attackers may have access to full-scale quantum computers, all public key cryptosystems will be compromised. In this talk, we'll look at two possible post-quantum-secure systems. We'll look at an implementation of a password authentication scheme on a quantum computer. Briefly, we'll also talk about post-quantum digital credentials, which are a privacy technology that allows users to disclose information about an attribute without revealing the attribute itself during transactions.

CUNLU ZHOU, University of New Mexico
A singlet projector based NPA hierarchy for the quantum MAXCUT problem

The QMA-hard quantum MAXCUT (QMC) problem, a quantum analog of the classical MAXCUT problem, studies the maximum eigenvalue of the so-called anti-ferromagnetic Heisenberg model. The quantum Heisenberg model plays a central role in condensed matter physics for understanding quantum magnetism and is one of the simplest models that exhibit genuine quantum computational hardness. The NPA hierarchy is the quantum (noncommutative) analog of the Lasserre hierarchy, which consists of a sequence of converging semidefinite programming (SDP) relaxations and has played an important role in studying combinatorial optimization problems. In this talk, I will introduce an NPA hierarchy for QMC based on the singlet projectors (projectors of the form $h = |\psi^-\rangle\langle\psi^-|$, where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$). The singlet projector follows the $SU(2)$ symmetry naturally, and the obtained NPA hierarchy is conceptually simpler and practically implementable. I will show several analytic and computational results concerning this new hierarchy.

(Based on work with Jun Takahashi, Chaithanya Rayudu, Robbie King, Kevin Thompson, and Ojas Parekh.)