6.S979 Final Project

Instructor: Anand Natarajan (anandn@mit.edu)
Released 11/6/2020

Guidelines:

For the final project, the basic requirement is to choose a paper (or two related papers) from the research literature related to topics covered in the class, and write an expository summary of the paper(s). The summary should convey, in your own words, the main results of the paper(s), how they fit into the broader research literature, and some of the key technical ideas involved, with the expected audience being fellow students in the class. You don't need to give full rigorous proofs in your writeup (that's what the original paper is for!) but try to at least give intuition for the ideas in the paper. A reasonable length would be around 4-5 pages, though this is not strict.

You will also have the option of giving a short presentation (10-15 minutes) in class on your project. This is not mandatory but highly encouraged. The presentations will happen during the last week of class.

Below is a list of possible papers. In general I tried to avoid papers that were covered in lecture, and tried to stick to the first paper in a particular line of research. When you are writing your summary, try to check out papers that cite your chosen paper, to get an idea of how the field has progressed since the paper was written. Some of these papers are quite long or technically difficult; for these, it's ok to focus on a manageable chunk (such as a single new technique that the paper introduced).

If there is a paper you'd rather write about that's not on the list, or if you have your own original research you'd like to submit, that's perfectly fine too, but please clear it with me first!

Timeline: Please select a project topic and send me an email with your choice by **Monday, November 16.** If you're choosing something that's not on the list, include a couple of sentences explaining why you think it's a good topic. The final writeups will be due on **Friday, December 11th.** Feel free to send me intermediate drafts or outlines, I will be happy to give you feedback on them!

MIP* odds and ends

Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources
Andrea Coladangelo, Alex Grilo, Stacey Jeffery, Thomas Vidick
https://arxiv.org/abs/1708.07359

Complexity limitations on one-turn quantum refereed games.
Soumik Ghosh and John Watrous.
https://arxiv.org/abs/2002.01509

Perfect zero knowledge for quantum multiprover interactive proofs
Alex B. Grilo, William Slofstra, Henry Yuen
https://arxiv.org/abs/1905.11280

On the complexity of zero gap MIP*
Hamoon Mousavi, Seyed Sajjad Nezhadi, Henry Yuen
https://arxiv.org/abs/2002.10490

Parallel repetition via fortification: analytic view and the quantum case
Mohammad Bavarian, Thomas Vidick, Henry Yuen
https://arxiv.org/abs/1603.05349

Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision
Matthew Coudron, William Slofstra
https://arxiv.org/abs/1905.11635

Nonlocal games, self-testing, and correlations

A generalization of CHSH and the algebraic structure of optimal strategies
David Cui, Arthur Mehta, Hamoon Mousavi, Seyed Sajjad Nezhadi
https://arxiv.org/abs/1911.01593

Geometry of the set of quantum correlations
Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, Valerio Scarani
https://arxiv.org/abs/1710.05892

All Pure Bipartite Entangled States can be Self-Tested
Andrea Coladangelo, Koon Tong Goh, Valerio Scarani
https://arxiv.org/abs/1611.08062

Information Causality as a Physical Principle
M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski
https://arxiv.org/abs/0905.2292

Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH
Mohammad Bavarian, Peter W. Shor
https://arxiv.org/abs/1311.5186

Testing and cryptography with one prover

Note: the first three papers here use ideas from https://arxiv.org/abs/1804.01082, which we will try to cover in class, but probably too late to be useful for the project. This talk https://simons.berkeley.edu/talks/tbd-121 might be a good resource to get some background on the ideas involved.

Computationally-secure and composable remote state preparation
Alexandru Gheorghiu, Thomas Vidick
https://arxiv.org/abs/1904.06320

Self-testing of a single quantum device under computational assumptions
Tony Metger, Thomas Vidick
https://arxiv.org/abs/2001.09161

Simpler Proofs of Quantumness
Zvika Brakerski, Venkata Koppula, Umesh Vazirani, Thomas Vidick
https://arxiv.org/abs/2005.04826

Quantum advantage with shallow circuits
Sergey Bravyi, David Gosset, Robert Koenig
https://arxiv.org/abs/1704.00690

Non-signalling correlations and MIP

How to Delegate Computations: The Power of No-Signaling Proofs
Yael Tauman Kalai, Ran Raz, Ron D. Rothblum
https://eprint.iacr.org/2013/862.pdf

Non-signaling proofs with o(√ log n) provers are in PSPACE
Dhiraj Holden, Yael Tauman Kalai
https://arxiv.org/abs/1910.02590

Testing Linearity against Non-signaling Strategies
Alessandro Chiesa, Peter Manohar, Igor Shinkar
https://eccc.weizmann.ac.il/report/2018/067/download/

Infinite dimensional entanglement

Perfect Embezzlement of Entanglement
Richard Cleve, Li Liu, Vern I. Paulsen
https://arxiv.org/abs/1606.05061

A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations
Andrea Coladangelo
https://arxiv.org/abs/1904.02350

Tsirelson's Problem
V. B. Scholz, R. F. Werner
https://arxiv.org/abs/0812.4305

The works of William Slofstra on this topic are very interesting but probably too technical unless you're comfortable with some group theory. If you are and want to check them out, these recorded talks might help orient you: https://simons.berkeley.edu/talks/tbd-147 and Vern Paulsen's talk here: https://www.birs.ca/events/2019/5-day-workshops/19w5163/videos.