COMS 6998 - Frontiers of Quantum Complexity and Cryptography (Spring 2022)

Essentials

- Instructor: Henry Yuen (hyuen@cs.columbia.edu)
- Course Website: http://henryyuen.net/classes/spring2022/
- TA: Hamoon Mousavi (h.mousavi@columbia.edu)
- Discussion forum: Slack (invite link: https://join.slack.com/t/coms6998front-mtv5819/shared_invite/zt-11xv641wh-MXAf2smBMe6K65QJ_0I3nA)
- Class time: Thursdays 2 - 4pm
- Zoom link: https://columbiauniversity.zoom.us/j/98981313319 (Passcode: available on CourseWorks, or e-mail me)
- Room: Chandler 401 (when we return to in-person classes)
- Office hours: by appointment

Description

This is an advanced, PhD-level topics class in the theory of quantum computing, focusing in particular on cutting-edge topics in quantum complexity theory and quantum cryptography. The theme of the topics this year will be

Complexity of quantum states and state transformations.

An n-qubit quantum state appears to be exponentially more complex than an n-bit string; a classical description of such a state requires writing down 2^n complex amplitudes in general. Here are some questions that will motivate our explorations:

- How does this complexity manifest itself in different information-processing tasks?
- How can we quantify this complexity?
- Can this complexity be used for cryptographic applications?
- Does the complexity of quantum states relate to traditional concepts in complexity theory such as circuit complexity or space complexity or time complexity?

A list of possible topics:

- Shadow tomography of quantum states
- Quantum state synthesis/unitary synthesis
- Hamiltonian learning
- Quantum key distribution/quantum money
- QMA(2) and the power of unentanglement
- State complexity, AdS/CFT, and quantum gravity
- Quantum state complexity and statistical zero knowledge
- Pseudorandom states and unitaries
- Classical vs. quantum proofs

The following notes from Scott Aaronson will be frequently consulted: https://www.scottaaronson.com/barbados-2016.pdf .

The goal is to explore the results and (more importantly) the questions in this field.

Prerequisites

Must have taken: Basic linear algebra and basic probability theory.

You must have taken at least one of:

- An upper-level CS theory course such as complexity theory/cryptography/algorithms, or
- Quantum computing, or
- Quantum physics.

It is not required that you have taken a course in quantum computing/quantum information before, but it would definitely be helpful. The lectures will introduce the concepts as needed, but will go rather quickly.

The course will expect high levels of mathematical maturity and comfort with proofs. To get a sense of what this course is like, take a look at the lecture notes from this Fall 2020 topics course (http://henryyuen.net/classes/fall2020/).

Grading

10% participation
20% scribe notes
30% problem sets
40% final project

Participation

Participation will be measured by asking questions in class, asking and answering questions on the slack channel, and also participating in the **Class Discussion** sessions that occur every few weeks: before the Q&A session, people should each submit a question/comment about the topics covered recently. During Class Discussion day, we'll have a free-form discussion about the questions/comments posted by folks.

Scribe notes

Each lecture will be scribed by up to 2 people. The scribe notes need to be written up in LaTeX using the provided template, and sent to me within 72 hours of the lecture. These notes will be posted on the course website, and will be a useful resource not only for students in the class, but for other researchers!

Problem sets

There will be approximately 3 problem sets. Collaboration on problem sets is encouraged, but please limit the groups to size three or less. Your writeups should also have the names of your collaborators. Everyone must submit their own solutions.

We will use Gradescope to distribute and mark assignments. All assignments must be turned in via Gradescope. Uploads to Gradescope must be legible.

Final project

In teams of two, you will choose a topic at the frontier of quantum computing related to the theme of the course, read the relevant papers, and write a report of what you have learned. The report can be an in-depth survey, or can be original research. I will separately provide a list of suggested project topics, as well as additional guidelines.

Important dates

- Jan 20- First meeting of the course
- Jan 28 - End of Change of Program period. Online instruction ends.
- March 14 - 18 - Spring Break (no classes)
- April 28 - Last class