# MAT3420 (2022 SPRING) EXAM PREPARATION

MAKOTO YAMASHITA

## What to expect in the exam

The exam will roughly have two parts: the first part to mainly decide if you pass the course or not, and the second part to mainly decide your score.

To get enough points in the first part, I want you to have basic but precise understanding of the principles behind quantum computation. For example, you want to know how to mathematically model various concepts, but "pop-sci" style explanation in plain words would not be enough. On the other hand, you do not have to give precise estimate of algorithms, etc. for this.

The second part is more advanced, so you are expected to give quantitative estimate of algorithms and such. However, you do not have to memorize various algorithms. It is more important that, given a description of a quantum algorithm, you can identify what contributes to benefit over classical algorithms and provide some estimate about the benefit.

Below is a list of topics we covered in the course. Try answering the questions to see if you understand them. You do not have to memorize algorithms, but I still expect you to know claims of important theorems for better grade.

## Topics

**Foundation of quantum mechanics.** Mathematical model of states of a quantum mechanical system; and how to model measurement. probability of outcomes for measurement (Born rule)

Transformation of states; geometric picture of unitary transform on qubit states (Bloch sphere)

How to model combination of smaller parts, e.g., multiple qubits; and mathematical model of partial measurement of composite system.

**Measurement and collapse of states.** What is the claim of Turing's paradox? How does Elitzer–Vaidman bomb detection work?

**Entangled state.** What are separable states and entangled states? Give an example of entangled state.

**Density matrix.** How to model: mixed states; measurement of mixed states; partial measurement. What does the no-communication theorem say? How do we make sense of entropy?

**No-cloning theorem.** What is its mathematical claim?

**Authentication / detection of eavesdropping.** How does the quantum money scheme work? How does the BB84 scheme work?

**Superdense coding.** How does it work?

**Quantum teleportation.** How does this work?

**Nonlocal game.** How does a quantum strategy for the Clauser-Horne-Shimony-Holt game work? What does it say about hidden variable theory?

---

*Date*: 05.04.2021.

**Quantum algorithms.** How does Deutsch's algorithm work? What is the benefit of quantum algorithm for Bernstein-Vazirani problem? Can you see the difference of circuit complexity and query complexity from this problem?

Simon's problem: what is the benefit?

Shor's algorithm: how do we reduce the problem of solving RSA encryption to period finding? What is the Fourier transform, and why does Fourier transform help to solve the period finding problem?

Grover's algorithm: how does it work? How better is it against classical algorithms, and what does the Bennett-Bernstein-Brassard-Zazirani theorem say?

**Universality.** Give a collection of classical gates that is (classically-)universal, and give a collection that is not. How do you relate subgroups of $U(2)$ and universality of quantum gates acting on multiple qubits? What does the Solovay-Kitaev theorem say?

**Error correction.** How do we implement error correction classically? What is a quantum analogue? (Shor's 9-bit code)