CS 151 Quantum Computer Science

Lecture 5: Quantum computing

January 31, 2024

Lecturer: Saeed Mehraban *Scribe: Preliminary notes*

1 Logistics

- Problem set 1 is due tonight
- Problem set 2 will be released today

2 Overview

Last time:

- Unitary computation

Today:

- Quantum computing

3 Review: Formulation of three computing theories

	Classical computation	Quantum Computation
States:	$\|v\rangle \in \{0,1\}^m, \sum_i v_i = 1$	$\|\psi\rangle \in \mathbb{C}^m, \sum_i \|\psi_i\|^2 = 1$
Evolutions:	$A \in \{0,1\}^{m\times n}, \sum_i A_{ij} = 1$	$U \in \mathbb{C}^{m\times m}, U^\dagger U = I$
Output:	$\|w\rangle = A\|v\rangle$	$\|\phi\rangle = U\|\psi\rangle$
Measurements:	The nonzero element of $\|w\rangle$	$Pr[i] = \|\langle i\|\phi\rangle\|^2$

To do: a quick review of writing matrices for operations.

3.1 Basic quantum gates

Similar to classical computing, in which we decompose a large computation into a composition of small gates, we can decompose an arbitrary unitary matrix into smaller gates.

- Pauli gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- The T gate. (Becomes important later).

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

- The following is known as the phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- The following relationships hold between these operators

$$\{X, Y\} = \{X, Z\} = \{Y, Z\} = 0$$

$$\frac{1}{2}[X, Y] = iZ, \frac{1}{2}[Y, Z] = iX, \frac{1}{2}[Z, X] = iY$$

$$HXH = Z, HZH = X, S^2 = Z.$$

- Other examples include classical reversible circuits:

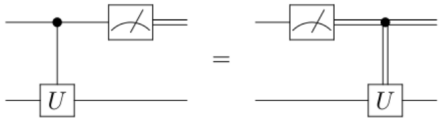
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$Toffoli = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

4 Quantum Computation

Quantum computing consists of three steps: Initialization, applying a quantum circuit, and measurement. The standard model of quantum computing is based on quantum circuits. We start with all zeros states, apply a quantum circuit from a universal gate set, and measure the very first qubit. If it was 1 accept otherwise reject. We say that the given quantum algorithm succeeds in

Figure 1: Principle of deferred measurements



performing reliable computation if it gives the correct answer at least $2/3$ of times. The choice of $2/3$ is arbitrary. We can always amplify the probability of success to any number (e.g., 0.9999) by taking the majority's vote: we repeat the computation multiple times and choose the majority of the answer as the final answer. How does the majority vote help us? Imagine a coin that produces outcome 0, $2/3$ of the time. If we flip this coin n times, it produces k heads with probability $\binom{n}{k}(2/3)^k(1/3)^{n-k}$.

Exercise: Show that the probability that more than $n/2$ of the outcomes is bit 1 is exponentially small.

Lemma 4.1. *We can perform a majority vote by only one measurement in the end.*

Proof. We prepare many copies of the quantum experiment and use a reversible implementation of the majority to store the majority vote in one bit. □

Without loss of generality, we can always assume you start with $|0\ldots0\rangle$.
Similar to classical computing, we can talk about a set of universal gates.

Definition 4.2. A quantum gate set is universal if it can approximate any unitary operation within arbitrary precision.

Recall that there are 2^{2^n} Boolean functions over n bits. We note that the space of n qubit unitary matrices is even more gigantic. So, to approximate an arbitrary unitary matrix, we may need an exponentially long quantum circuit. Can we produce an arbitrary quantum operation exactly? The answer is no. Because arbitrary operations include arbitrary real numbers. But for all plausible applications, an approximation is sufficient.

- CNOT and arbitrary rotation
- Clifford + T; where Clifford = {CNOT, H, S}
- Hadamard, Toffoli

Lemma 4.3 (Deferred measurements)**.** *You can always push the measurements to the end.*

Proof. We can eliminate intermediate measurements using the gadget in Figure 1. □

Lemma 4.4. *We can simulate arbitrary quantum computations with gates composed of real numbers only.*

Proof. Replace i with

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and 1 with the identity I. □

4.0.1 Solovay Kitaev

You can compile a quantum circuit based on one gate set into another gate set without too much overhead.

4.0.2 Uncomputing

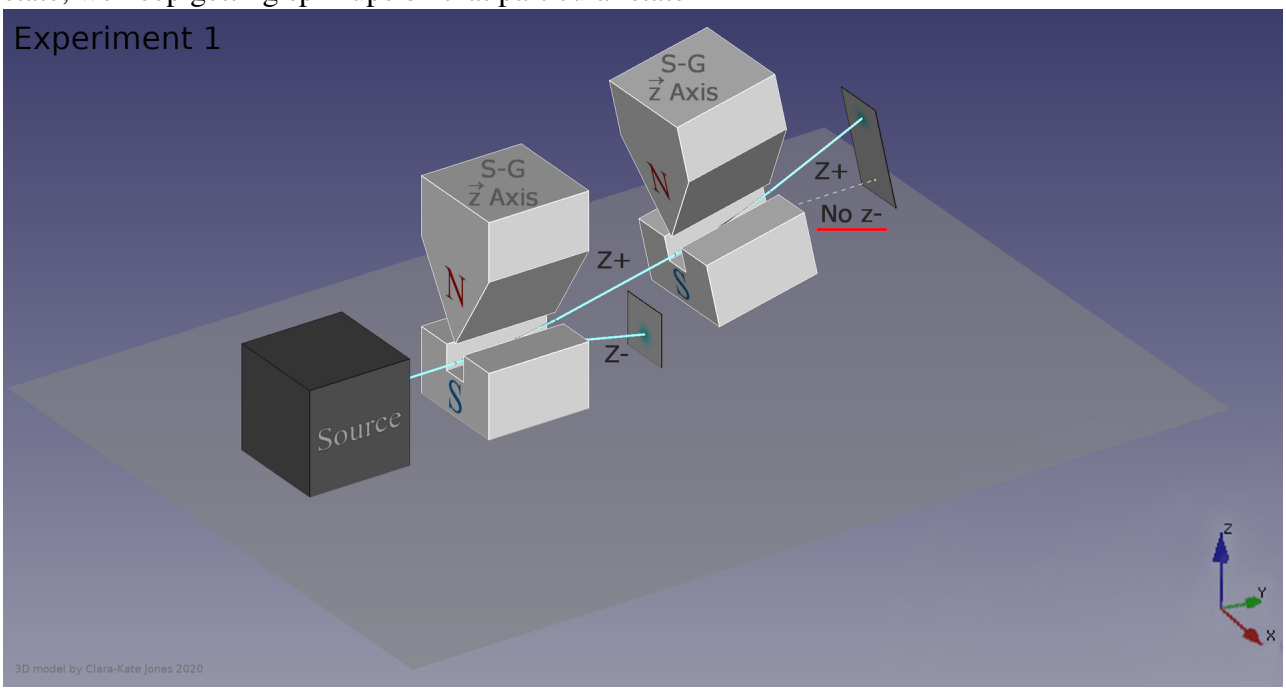
We can always transform a quantum circuit such that the first qubit that contains the answer is 0 or 1, and the rest will be zeros. Here is how: use CNOT to store the answer qubit, then apply the inverse of the computation on the rest. Another important reason why we use uncomputing is for taking quantum computations as subroutines.

Simple example for a universal gate set: Consider 1 dimensional quantum states: all quantum states that are scalar multiple of one vector, e.g., $|0\rangle$. Such a quantum state is only a phase $e^{i\phi}|0\rangle$. Consider a phase quantum gate that simply applies a phase $G = e^{i\theta}$. If θ is a rational multiple of π (e.g., $2\pi, \pi/2, \pi/7$, etc.) by applying G any number of times, we are not able to produce arbitrary phases. Based on a well-known theorem in mathematical analysis called Gibbs equidistribution, if θ is an irrational multiple of π, then we can estimate any angle up to arbitrary precision by repeating G.

5 What happens after a quantum measurement?

Suppose we prepare a quantum state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ in an equal superposition of $|0\rangle$ and $|1\rangle$. If we measure the quantum state in $|0\rangle, |1\rangle$ basis, we obtain a probabilistic outcome, but if we measure the same state in the $|+\rangle, |-\rangle$ basis, we obtain a deterministic result. This suggests that the state of the quantum system was not really $|0\rangle$ or $|1\rangle$, but rather a superposition of the two; it was the state $|+\rangle$. What happens to the quantum state after measurement? Recall the Stern-Gerlach experiment. Suppose we measure the electron spin on an up-down basis and filter out the electrons that have been measured to be down. If we measure the upper beam on an up-down basis one more time, we obtain spin-up one more time. If we continue doing this, we will keep getting spin-ups. See future **??**. In other words, once we measure an arbitrary quantum state on any given basis and obtain a certain outcome, the state of the quantum system collapses to that outcome. Previously, we told you that quantum mechanics is a reversible theory. We have to correct this statement: quantum mechanics is a reversible theory "before measurement." Measurement is an irreversible process. We should note that there are several schools of though regarding interpretations of quantum mechanics. The above interpretation of quantum measurements is based on a school of thought known as the Copenhagen school.

Figure 2: Two consecutive spin up-down measurements. Once we obtain spin-up in a quantum state, we keep getting spin-ups on that particular state



5.1 Schrödinger's cat

Would the above interpretation of quantum measurements lead to paradoxical outcomes? Schrödinger's cat is a thought experiment in quantum mechanics, proposed by the Austrian physicist Erwin Schrödinger in 1935. It illustrates what he saw as the problem of the Copenhagen interpretation of quantum mechanics when applied to everyday objects.

In the thought experiment, a cat is placed in a sealed box with a radioactive atom, a Geiger counter, a hammer, and a vial of poison. If the radioactive atom decays, the Geiger counter triggers the hammer to break the vial, which would kill the cat. As long as the box remains closed, the state o the radioactive atom is in a superpostion of triggering and not triggering the hammer. Hence, the cat is simultaneously alive and dead in a superposition of states. Once the box is opened, the cat is observed to be either alive or dead, not both. Suppose we keep the box closed for many years and open the box and see the cat is dead. When did the cat really die?

This paradox is often used to illustrate the weirdness of quantum mechanics and the concept of superposition, where particles can exist in multiple states at the same time until they are observed. The thought experiment was not intended to be a practical one but rather to illustrate the potential issues and interpretations of quantum mechanics in understanding real-world objects and systems.