CS 880: Quantum Algorithms 2/09/2021

Lecture 4: Quantum Circuits

Instructor: Dieter van Melkebeek Scribe: Keith Johnson

In today's lecture, we first reviewed some material from previous lectures, and specifically some notes about partial measurements and how to think of them. We then provided the solution to last lecture's exercise, showing how intermediate measurements of a circuit can be deferred to the end of the computation. However, it was shown that such "copying" of state we used does not work for all pure states. Then, we discussed intermediate measurements in more depth, defining that *mixed states* are a distribution over superpositions. Finally, we discussed the model of quantum circuits that we will be using, along with a definition of *unitary circuits*.

1 Recap

1.1 Quantum Computation

Recall that in a quantum system, a state is described by a superposition

$$|\psi\rangle = \sum_{s \in \{0,1\}^m} \alpha_s |s\rangle$$

with amplitudes $\alpha_s \in \mathbb{R}$ (or $\mathbb{C}$) and $\| \, |\psi\rangle \, \|_2 \doteq \sqrt{\sum_s |\alpha_s|^2} = 1$. Computations on these systems go through an initialization phase, with a basis state (e.g., $|x0^{m-n}\rangle$), proceed through a sequence of quantum gates, and then terminate, where $|\psi\rangle$ is measured. This measurement collapses the superposition into a basis state $|s\rangle$, from which output y is extracted. The probability of obtaining any given basis state $|s\rangle$ is thus

$$\Pr[\text{obtain } s] = |\alpha_s|^2$$

1.2 Simulating Probabilistic Computations and Partial Measurements

Recall that probabilistic computations can be simulated by applying H to $|0\rangle$ and observing the component. This provides a basic coin-flip mechanism. However, this requires a measurement that is partial (just one qubit) and intermediate. We don't want to measure the entire system, because doing that would collapse the system and eliminate interference, losing the power of quantum computations.

Another way to think about partial measurements is in geometric terms. We can project the state to be measured onto two subspaces, with one being all the vectors where the qubit to be measured is in the zero state, and the other being an orthogonal space where the qubit is in the one state. A partial measurement is then a projection of the state onto these two subspaces. Doing this, we know that the 2-norm is maintained because of the Pythagorean theorem (as the two subspaces are orthogonal), so we can collapse one of the vectors and re-normalize.

2 Exercise - Deferring Measurements

Measurement can be deferred to the end of a computation by using ancilla qubits. Consider the following two circuits starting from same state $|\psi\rangle \doteq \sum_{s\in\{0,1\}^m} \alpha_s |s\rangle$.

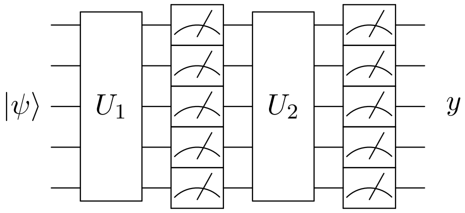

Figure 1: Measurement in the middle of two gates

1. Measure in the middle of two gates (Figure 1).

   Starting from a state $|\psi\rangle$, the state immediately after U_1 is thus $U_1|\psi\rangle$, which can be written as $U_1|\psi\rangle = \sum_s \beta_s |s\rangle$. This intermediate state is then measured to be in state $|s\rangle$ with a probability of $|\beta_s|^2$. Passing through U_2 yields a state $U_2|s\rangle = \sum_t \gamma_{st}|t\rangle$. In this case, the output y is measured to be in state t with probability $|\gamma_{st}|^2$, and the total probability of being in state t from $|\psi\rangle$ is $\sum_s |\beta_s|^2|\gamma_{st}|^2$, summing over all intermediate states s.

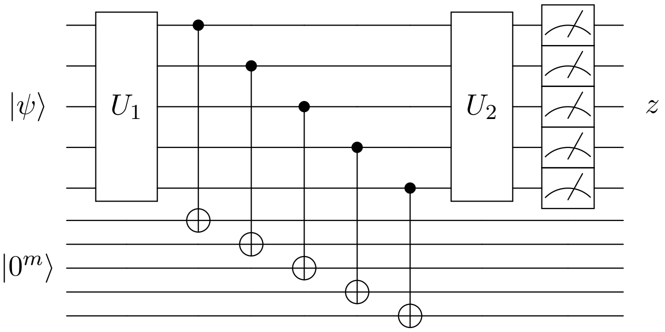

Figure 2: Measurement at the end, after ”copying” intermediate state

2. Use CNOT gates to move measurements to ancilliary qubits (Figure 2).

   The system now starts in a state $|\psi\rangle|0^m\rangle$, and after U_1, is in a state $U_1|\psi\rangle|0^m\rangle$ that, given $U_1|\psi\rangle = \sum_s \beta_s|s\rangle$, equals $\sum_s \beta_s|s\rangle|0^m\rangle$. After the CNOT gates but before U_2, the state becomes $\sum_s \beta_s|s\rangle|s\rangle$. After applying U_2 to the top m qubits, we get that the final state is $\sum_s \beta_s(U_2|s\rangle)|s\rangle = \sum_s \beta_s(\sum_t \gamma_{st}|t\rangle)|s\rangle$, which can be simplified to $\sum_{s,t} \beta_s\gamma_{st}|t\rangle|s\rangle$. Then we can measure the output state $z = t$ with probability $\sum_s |\beta_s\gamma_s t|^2$, which is equivalent to actually performing the intermediate measurement. Thus intermediate measurements can be deferred to the end of the computation.

   Note that this deferring of measurement requires fresh ancilla qubits for each deferral. With current technology, adding these additional qubits is infeasible. However, also note that taking a measurement is a slow process (slower than any quantum gate), so care needs to be taken with that method as well.

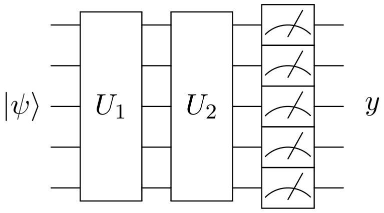

Figure 3: No measurement in the middle of two gates

3. No measurement or CNOT in the middle of U_1 and U_2 (Figure 3).

   If a measurement is not taken in the middle of U_1 and U_2, then the state at the output after U_2 is simply $U_2U_1|\psi\rangle = \sum_s \beta_s(\sum_t \gamma_{st}|t\rangle) = \sum_t(\sum_s \beta_s\gamma_{st})|t\rangle$. Then, the probability of a specific $y = t$ is $|\sum_s \beta_s\gamma_{st}|^2$, which is not equivalent to the previous probabilities.

Note that, when copying the intermediate state with CNOT gates, the resultant state is $\sum_s \beta_s|s\rangle|s\rangle$, not simply $U_1|\psi\rangle U_1|\psi\rangle = \big(\sum_s \beta_s|s\rangle\big)\big(\sum_t \beta_t|t\rangle\big)$, as copying might imply. The issue with this is that the probability of measuring certain states $|s\rangle$ and $|t\rangle$ is not independent—the two states must always be measured the same, as they are copies of each other. Therefore, we get the resultant state of $\sum_s \beta_s|s\rangle|s\rangle$, showing that the copied state and the original state must be the same $|s\rangle$, and the amplitude β_s does not change. Thus specific basis states can be copied, but in general, any arbitrary $|\psi\rangle$ cannot. In the next section, we will prove that this is the case.

3 No Cloning

We have been doing some sort of "copying" with CNOTs. We're copying basis states, and as such, we can transform $|\psi\rangle|0^m\rangle \mapsto |\psi\rangle|\psi\rangle$ for every basis state $|\psi\rangle = |s\rangle$. However, this does not hold in general for all pure states.

Theorem 1. *There does not exist a quantum circuit realizing $|\psi\rangle|0^m\rangle \mapsto |\psi\rangle|\psi\rangle$ for every pure state $|\psi\rangle$ on m qubits.*

We prove this by beginning with unitary quantum circuits (see section 5), but we will also need to generalize to general quantum circuits. Suppose there exists a unitary quantum circuit that can realize

$$|\psi\rangle|0^m\rangle \mapsto |\psi\rangle|\psi\rangle \tag{$\star$}$$

for every pure state $|\psi\rangle$ on m qubits.

Consider two arbitrary pure states, $|\psi\rangle = |\psi_1\rangle$ and $|\psi\rangle = |\psi_2\rangle$. We take the inner product of the left-hand side of ($\star$) for these two states. We know that the inner product is preserved for unitary operations, so we set this equal to the inner product of the right-hand side, yielding the equation

$$|\langle\psi_1|\psi_2\rangle \cdot \langle 0^m|0^m\rangle| = |\langle\psi_1|\psi_2\rangle \cdot \langle\psi_1|\psi_2\rangle|$$

Setting $a \doteq |\langle \psi_1 | \psi_2 \rangle|$, we find that $a = a^2$, as $\langle 0^m | 0^m \rangle = 1$. Also note that a must be less than 1, as it is the inner product between two 2-norm 1 vectors. This implies that a can only be either 0 or 1 to satisfy the relationship.

In the case that $a = 0$, this implies that $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, while when $a = 1$, $|\psi_1\rangle$ and $|\psi_2\rangle$ must be parallel. Clearly, two arbitrary pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ are not guaranteed to be orthogonal or parallel to each other, so this is a contradiction.

□

For the general case, we consider a purification of a general circuit (see section 4), since our circuit can now have arbitrary intermediate measurements. A purification with with l extra ancilla qubits allows us to defer these measurements to the end. This purification can realize

$$|\psi\rangle |0^m\rangle |0^l\rangle \mapsto |\psi\rangle |\psi\rangle |g(\psi)\rangle \tag{$\star\star$}$$

where the new ancilla qubits start in the zero state, and at the end are in some garbage state $|g(\psi)\rangle$. We want it to be the case that after observing the ancillas, regardless of their state, we always get the superposition $|\psi\rangle|\psi\rangle$ in the upper qubits. This means that the state $|g(\psi)\rangle$ cannot be entangled with $|\psi\rangle|\psi\rangle$.

Consider again two arbitrary pure states, $|\psi\rangle = |\psi_1\rangle$ and $|\psi\rangle = |\psi_2\rangle$. We take the inner product of the left-hand side of ($\star\star$) for these two states. Since purification of the general circuit yields a unitary circuit, the inner product is preserved, so we again set this equal to the inner product of the right-hand side, this time including the extra ancilla bits.

$$|\langle \psi_1 | \psi_2 \rangle \cdot \langle 0^m | 0^m \rangle \cdot \langle 0^l | 0^l \rangle| = |\langle \psi_1 | \psi_2 \rangle \cdot \langle \psi_1 | \psi_2 \rangle \cdot \langle g(\psi_1) | g(\psi_2) \rangle|$$

Again taking $a \doteq |\langle \psi_1 | \psi_2 \rangle|$, we find that $a = a^2 |\langle g(\psi_1) | g(\psi_2) \rangle|$. Since $|\langle g(\psi_1) | g(\psi_2) \rangle|$ must also be less than one, we again find that a must be either 0 or 1 (and $|\langle g(\psi_1) | g(\psi_2) \rangle|$ must be 1 if $a = 1$). This implies that $|\psi_1\rangle$ and $|\psi_2\rangle$ must be either orthogonal or parallel, which contradicts that they are arbitrary pure states. Therefore, such a general circuit must not exist.

■

4 Intermediate Measurements

So far, we've only been doing measurements at the end to extract some classical information out of the quantum state. However, allowing intermediate measurements increases the size of the system state. Instead of only superpositions of states, we now have to consider a probability distribution over superpositions for 2-norm 1. In probabilistic computing, we can consider probability distributions over probability distributions over deterministic states, which can be collapsed into a single probability distribution. This, however, does not work for quantum computations.

Some notes on state terminology:

- A **basis state** is some $|s\rangle$ for $s \in \{0,1\}^m$, which represents some concrete configuration of the system.
- A **pure state** is a superposition $|\psi\rangle = \sum_s \alpha_s |s\rangle$ of basis states $|s\rangle$, each with an amplitude α_s and with $\sum_s |\alpha_s|^2 = 1$.

- A **mixed state** is a probability distribution ρ over superpositions, where $\rho = \{(p_i, |\psi_i\rangle)\}_i$ with $p_i \geq 0$ and $\sum_i p_i = 1$. Each element of ρ is a pair, where p_i is the probability and $|\psi_i\rangle$ is the state.

As an example of a mixed state, consider the measurement of the first component of

$$\frac{1}{\sqrt{3}}(|01\rangle + |10\rangle - |11\rangle)$$

Last lecture, we showed that:

$$\begin{aligned}\Pr[\text{measure } 0] &= \frac{1}{3}, \text{ new state: } |01\rangle \\ \Pr[\text{measure } 1] &= \frac{2}{3}, \text{ new state: } \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)\end{aligned}$$

This measurement thus transforms the pure state:

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle - |11\rangle)$$

into the mixed state:

$$\rho = \left\{ \left(\frac{1}{3}, |01\rangle\right), \left(\frac{2}{3}, \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)\right) \right\}$$

Allowing intermediate measurements is good, but it complicates theoretical analysis. As we have seen, these intermediate measurements can be avoided by ”copying” components into fresh ancillas. This gives a pure state on $m+l$ qubits such that at the end of the computation, measuring and eliminating the last l qubits yields ρ. This operation ensures that, at any point in time, the system is in a pure state. This transformation is referred to as the **purification of** ρ.

Some additional notes on complexity for simulations without intermediate measurements of quantum computations running in time t and space s (to within ϵ):

Time	Space	
$O(t)$	$O(s+t)$	What we are doing with CNOT gates and copying state
poly$(t/\epsilon, 2^s)$	$O(s + \log(t/\epsilon))$	[Girish, Raz, Zhan '20], [Fefferman, Remscrim '20]

The first method is time-optimal, which we have been using by deferring measurements by copying with CNOT gates, and the latter is space-optimal. It is not known if there are any methods with complexity in between these two.

5 Quantum Circuits

In our definition of quantum circuits, we are going to allow intermediate measurements, as they are useful and give additional power to algorithms. We are also going to allow non-classical inputs and outputs to these circuits. While our algorithms as a whole need to start and end in a classical state, we can use circuits with non-classical inputs and outputs like subroutines—bits and pieces of algorithms where some superposition or mixed state is transformed into another. An example of a subroutine like this would be amplitude amplification, which is a procedure transforming one pure state into another.

Definition 1. *A quantum circuit is a system acting on m components (thought of like a register of m qubits) and wires. Operations will be quantum gates acting on a constant number of components, or will be single-component measurements. Operations on disjoint components can act in parallel.*

A special type of quantum circuits are **unitary circuits**, which are circuits with no measurements and only quantum gates. These types of circuits make analysis simpler, as they are reversible and their transition matrices can be combined. With a unitary circuit of k gates, the reverse can also be realized in k gates, where the transition matrix of each gate is simply the complex conjugate transpose of the original circuit.

Additionally, all states in unitary circuits are pure because they contain no measurements. As such, the effect of a circuit is fully specified by the output for each basis state. Each pure state is just a superposition of basis states, and each unitary operation is just a linear operation on these states, so the specification of the circuit is just the transformation from each basis state.

The above properties of unitary circuits are not true in general for all quantum circuits. These circuits can involve measurement, may not be reversible, and may have mixed states.

Exercise 1. *Give an example of two quantum circuits on the same number of qubits that behave the same on all basis states but not on all pure states.*