COL7160 : Quantum Computing

Lecture 6: Quantum Circuit Model

Instructor: Rajendra Kumar **Scribe:** Rishika Garg

1 Quantum Teleportation

We begin by recalling the standard *quantum teleportation* protocol. The goal is to transmit an *unknown quantum state* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ from Alice to Bob using *entanglement* and *classical communication*, without physically sending the qubit itself.

1.1 Initial Setup

Alice and Bob initially share an EPR pair:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Alice possesses two qubits: the unknown state $|\psi\rangle$ and her half of the EPR pair. Bob possesses the remaining qubit. The combined three-qubit state is

$$|\psi\rangle \otimes |\Phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

1.2 Circuit Operations

Alice applies the following operations:

- A CNOT gate with $|\psi\rangle$ as control and her EPR qubit as target.
- A Hadamard gate on $|\psi\rangle$.

After these gates, Alice measures her two qubits in the computational basis. This is a *partial measurement* since Bob's qubit is not measured.

1.3 Partial Measurement

Suppose a general three-qubit state is written as

$$|\Psi\rangle = |0\rangle|\varphi_0\rangle + |1\rangle|\varphi_1\rangle,$$

where $|\varphi_0\rangle, |\varphi_1\rangle$ are states of the remaining qubits. Measuring the first qubit yields:

- Outcome 0 with probability $\| |\varphi_0\rangle \|^2$, post-measurement state $|0\rangle|\varphi_0\rangle / \| |\varphi_0\rangle \|$.
- Outcome 1 with probability $\| |\varphi_1\rangle \|^2$, post-measurement state $|1\rangle|\varphi_1\rangle / \| |\varphi_1\rangle \|$.

In general, whenever a subset of qubits is measured, we first rewrite the global state in the computational basis of the measured qubits. Grouping together all terms consistent with each measurement outcome makes it clear both which outcomes can occur and to which (normalized) state the system collapses after the measurement.

1.4 Classical Communication and Correction

After measuring her two qubits, Alice sends the two classical bits $(m_1, m_2) \in \{0,1\}^2$ to Bob using a classical communication channel. These bits indicate the outcome of her measurement.
Depending on the received bits, Bob applies the following correction to his qubit:

(m_1, m_2)	Operation applied by Bob
$(0,0)$	I
$(0,1)$	X
$(1,0)$	Z
$(1,1)$	XZ

The identity operator I is applied when no correction is needed. The Pauli-X operator corrects a bit-flip error, while the Pauli-Z operator corrects a phase-flip error. When both errors occur, Bob applies XZ. After applying the appropriate operator, Bob's qubit becomes exactly $|\psi\rangle$, completing the teleportation protocol.

2 Quantum Circuit Model

2.1 Classical Circuits

A classical Boolean circuit is a finite directed acyclic graph.

- Nodes correspond to logical gates (AND, OR, NOT).
- Edges represent wires carrying bits.

The *size* of a circuit is the number of gates.
Randomized computation is modeled by allowing random input bits. For a randomized circuit C computing a function f, correctness is required with probability strictly greater than $\frac{1}{2}$:

$$\Pr[C(x) = f(x)] \geq \tfrac{1}{2} + \varepsilon$$

for some constant $\varepsilon > 0$ (commonly $\varepsilon = \frac{1}{6}$, giving success probability at least $\frac{2}{3}$).

2.2 Quantum Circuits

A quantum circuit consists of:

- Qubit wires (horizontal lines).
- Unitary gates acting on 1, 2, or 3 qubits.
- Measurements, typically at the end of the circuit.

Unlike classical circuits:

- Fan-out is restricted: each qubit has fan-out equal to fan-in, since quantum states cannot be copied due to the no-cloning theorem.
- Information flows only along the horizontal qubit wires (time direction) and cannot propagate diagonally between wires.

2.3 Elementary Gates

Common elementary quantum gates include:

- One-qubit gates: X, Y, Z, H.
- Two-qubit gates: CNOT.
- Three-qubit gates: Toffoli.

There are infinitely many one-qubit unitaries, as they correspond to rotations on the Bloch sphere.

3 Randomized Algorithms and Primality Testing

A fundamental application of randomness in algorithms is *primality testing*, where the goal is to decide whether a given integer n is prime.

- **Classical (Deterministic) Algorithms:** The straightforward deterministic approach tests divisibility up to $\sqrt{n}$, which takes time $O(\sqrt{n})$. Since the input size is $\log n$, this is exponential in the input length and hence inefficient for large n.
- **Miller–Rabin Primality Test:** This is a randomized algorithm that runs in time $O(k \log^3 n)$, where k is the number of rounds. Each round has error probability at most $\frac{1}{4}$, so after k independent iterations, the error probability is at most 2^{-2k}, which is exponentially small. This represents a dramatic reduction in time complexity compared to classical methods.
- **AKS Primality Test:** AKS is the first deterministic primality test that runs in polynomial time. The original algorithm had time complexity $(\log n)^6$, which was later improved to $(\log n)^3$. However, the hidden constants in these bounds are very large, making AKS impractical compared to Miller–Rabin in real-world applications.

For more details on the Miller–Rabin primality test, refer to its Wikipedia page: Miller-Rabin.

4 Universality of Gate Sets

A set of gates is *universal* if any unitary operation can be approximated arbitrarily well using only gates from this set.

- The set consisting of all single-qubit gates together with the CNOT gate is universal for quantum computation.
- The gate set $\{\text{CNOT}, H, R_{\pi/4}\}$, where $R_{\pi/4}$ is a phase (rotation) gate, is also universal in the sense that it can approximate any unitary operation to arbitrary precision.
- The Toffoli gate together with the Hadamard gate forms a universal set for unitaries with *real-valued* matrix entries.

The *cost* of implementing a quantum algorithm is typically measured by the number of gates used from a chosen universal gate set. Consequently, the cost can vary depending on which universal set of gates is employed.

5 Quantum Parallelism

Before discussing quantum parallelism, it is useful to view this setting as *classical computation performed using a quantum computer.*

Classical computation using quantum circuits. When implementing classical functions on a quantum computer, we face the following issues:

- All quantum operations must be *reversible*, whereas classical gates such as AND and OR are irreversible.
- Arbitrary copying of data is not allowed due to the *no-cloning theorem*.

Any classical circuit consisting of N NOT gates, A AND gates, and O OR gates can be implemented as a quantum circuit by representing each classical gate using a finite number of Toffoli gates. Since quantum states cannot be freely copied, gates that rely on fan-out must be explicitly repeated.
As a result, the corresponding quantum circuit has complexity

$$poly(N + A + O),$$

with additional overhead due to reversibility requirements and the need to store intermediate results.

Quantum parallelism. Quantum parallelism refers to the ability of a quantum computer to evaluate a classical function on many inputs simultaneously using superposition.
Consider a function

$$f : \{0,1\} \to \{0,1\},$$

implemented via a unitary oracle U_f defined as

$$U_f : |x\rangle\,|b\rangle \mapsto |x\rangle\,|b \oplus f(x)\rangle\,.$$

Notice that applying U_f twice returns the system to the original state.

Exercise 1. Show that U_f is Unitary.

Starting from the state $|0\rangle\,|0\rangle$, applying a Hadamard gate on the first qubit gives

$$\frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} |x\rangle\,|0\rangle\,.$$

Applying U_f once yields

$$\frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} |x\rangle\,|f(x)\rangle\,,$$

which encodes information about both $f(0)$ and $f(1)$ in superposition.

Although a single call to U_f computes the function on all inputs simultaneously, measuring the state collapses it and reveals only one output. Extracting useful global information therefore requires interference and further quantum operations.

Exercise 2. Let

$$f : \{0,1\}^n \to \{0,1\}$$

be a classical Boolean function.

Goal: Construct a quantum circuit that generates the state

$$\frac{1}{\sqrt{2^n}}\Big(\,|00\ldots0\rangle\,|f(00\ldots0)\rangle + |00\ldots1\rangle\,|f(00\ldots1)\rangle + \cdots + |11\ldots1\rangle\,|f(11\ldots1)\rangle\,\Big)$$

using a single invocation of the oracle U_f.

6 Remarks on Computational Models

- Quantum Turing machines exist but are rarely used in practice.
- The quantum circuit model is the standard model for algorithms.

Remark 1. Quantum circuits naturally generalize classical circuits while respecting unitarity and reversibility.