Quantum Computing

Unit 3: A Quantum Model of Computation

Dr. Gopal Chandra Jana

Dept. of CSE, Sharda University

Quantum Computing (CSE063) — Unit 3

August 9, 2026

Course Page:

https://www.gcjana.in/courses/shardauniversity/2501/quantum-computing/

Outline

Learning Outcomes of Unit 3

After this unit, a student will be able to...

1. **Describe** the quantum circuit model: qubits, wires, gates and measurement.
2. **Use** common quantum gates (Pauli, H, S, T, rotations, CNOT, CZ, SWAP, Toffoli).
3. **Build** small circuits (e.g. Bell-state preparation) and trace their evolution.
4. **Define** universality and identify exact and discrete universal gate sets.
5. **State** the Solovay–Kitaev theorem and the cost of approximating unitaries.
6. **Implement** measurements with circuits: basis change, deferred and implicit measurement.

Mapping to the Syllabus

A. The quantum circuit model, quantum gates. **B.** Universal sets of gates; efficiency of approximating unitary transformations. **C.** Implementing measurements with quantum circuits.

The Quantum Circuit Model

Ingredients

- **Qubits** on *wires*, usually initialised to $|0\rangle$.
- **Gates**: *unitary* operators applied left-to-right in time.
- **Measurement**: read-out, usually in the computational basis, at the end.

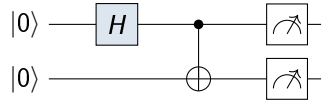


Figure: input → unitary gates → measurement.

- n qubits ⇒ state in $\mathbb{C}^{2^n}$; the whole circuit is one big unitary $U \in U(2^n)$.
- Built from *local* gates (on 1 or 2 qubits).
- Cost: **size** (# gates) and **depth**.

Reading a Quantum Circuit — Conventions

Diagram grammar

- Each *horizontal line* is one qubit; time flows **left** $\rightarrow$ **right**.
- A *box* U applies that unitary to its wire.
- A filled dot $\bullet$ is a **control**; $\oplus$ is a NOT **target**.
- The meter symbol denotes **measurement**; a double line carries a classical bit.

Order matters

The circuit $U_2 U_1$ means "U_1 first, then U_2": drawing is left-to-right, but matrix product reads right-to-left.

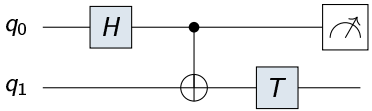


Figure: H on q_0, a CNOT, a T on q_1, then a measurement.

Single-Qubit Gates I — Pauli and Hadamard

Pauli gates

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

X is NOT/bit-flip; Z is phase-flip; $Y = iXZ$. All Hermitian and unitary; $X^2 = Y^2 = Z^2 = I$.

Hadamard

$$H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H|0\rangle = |+\rangle,\ H|1\rangle = |-\rangle.$$

H creates superposition; $H^2 = I$; $HXH = Z$, $HZH = X$.

Effect on the basis

$X : |0\rangle \leftrightarrow |1\rangle$; $Z : |1\rangle \mapsto -|1\rangle$; H rotates between the Z- and X-bases.

Single-Qubit Gates II — Phase and Rotation Gates

Phase gates

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

$S = \sqrt{Z}$, $S = T^2$, $Z = S^2 = T^4$. T is the "$\pi/8$ gate".

Rotations $R_{\hat{n}}(\theta) = e^{-i\theta\,\hat{n}\cdot\vec{\sigma}/2}$

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix},$$

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

Every single-qubit unitary

$U = e^{i\alpha} R_z(\beta)\, R_y(\gamma)\, R_z(\delta)$ (Z–Y decomposition): three rotations plus a global phase.

Multi-Qubit Gates — CNOT, CZ, Controlled-U

Controlled gates

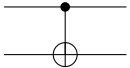
Controlled-U applies U to the target *iff* the control is $|1\rangle$:

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \text{CZ} = \text{diag}(1, 1, 1, -1).$$

Action & facts

CNOT: $|a, b\rangle \mapsto |a,\ a \oplus b\rangle$.
CZ is symmetric in its two qubits and
$\text{CNOT} = (I \otimes H)\,\text{CZ}\,(I \otimes H)$.



CNOT

More Gates — SWAP, Toffoli, Fredkin

SWAP

$$|a, b\rangle \mapsto |b, a\rangle; \quad \text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

SWAP = three CNOTs (alternating direction).

Toffoli (CCNOT) & Fredkin (CSWAP)

Toffoli: $|a, b, c\rangle \mapsto |a, b, c \oplus ab\rangle$ — reversible AND.
Fredkin: controlled SWAP of two targets.

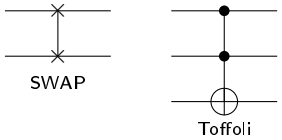


Figure: SWAP and the Toffoli (CCNOT) gate.

Worked Example — Preparing a Bell State

Circuit: H on q_0, then CNOT

$$|00\rangle \xrightarrow{H\otimes I} \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$
$$\xrightarrow{\text{CNOT}} \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle\,.$$

Note

The output is **entangled** (Schmidt rank 2 — Unit 2): a two-gate circuit already exceeds any product state.

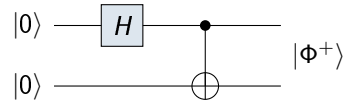


Figure: the standard Bell-state generator.

Quick Check — Round 1 (Circuit Model & Gates)

[Q1]

Write the action of CNOT on $|a, b\rangle$ and give its 4×4 matrix.

[Q2]

Which gates, in what order, create $|\Phi^+\rangle$ from $|00\rangle$?

[Q3]

Give the matrices of S and T. How are they related?

[Q4] True/False

"Every quantum gate is a unitary matrix."

Think for a minute — answers on the next slide.

Answers — Round 1

[A1]

$|a, b\rangle \mapsto |a,\ a \oplus b\rangle$; $\quad \text{CNOT} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$.

[A2]

Apply H to q_0, then CNOT with control q_0 and target q_1.

[A3]

$S = \text{diag}(1, i)$, $T = \text{diag}(1, e^{i\pi/4})$; $\quad S = T^2$ (and $S = \sqrt{Z}$).

[A4]

True — gates are unitary (reversible, norm-preserving). Measurement is the only non-unitary step.

Universality — What Does It Mean?

Definition

A set of gates $\mathcal{G}$ is **universal** if, for every unitary U and every $\varepsilon > 0$, there is a circuit using only gates from $\mathcal{G}$ that approximates U to accuracy ε.

Two flavours

- **Exact universality:** realise every U *exactly* (needs continuously-parametrised gates).
- **Approximate universality:** a *finite* set that approximates every U arbitrarily well.

Error metric

Closeness of U and V is measured by the operator norm

$$E(U, V) = \|U - V\| = \max_{\|\psi\|=1} \|(U - V)\,|\psi\rangle\|.$$

Exact Universality — Single-Qubit Gates + CNOT

Theorem (Barenco et al., 1995)

The set of **all single-qubit unitaries together with CNOT** is *exactly* universal: any n-qubit unitary can be written as a finite product of such gates.

Why it works (sketch)

- Any $U \in U(2^n)$ factors into *two-level* unitaries.
- Each two-level unitary is a controlled single-qubit gate (using CNOTs + Toffoli-style constructions).
- Single-qubit gates supply the "rotation" part.

Cost

A generic n-qubit unitary needs $\Theta(4^n)$ such elementary gates — exponential, but that is the price of an *arbitrary* unitary (most are "hard").

Discrete Universal Sets

Standard finite sets

- $\{ H,\ T,\ \text{CNOT} \}$ — the usual choice.
- $\{ H,\ S,\ T,\ \text{CNOT} \}$ (with $S = T^2$).
- $\{ H,\ \text{Toffoli} \}$ — universal for real amplitudes.

Why $\{H, T, \text{CNOT}\}$?

H and T generate a *dense* subgroup of single-qubit unitaries $SU(2)$; CNOT supplies the entangling two-qubit interaction. Together they are approximately universal on all n qubits.

Key point

A finite set cannot produce *every* unitary exactly (continuum vs. countable), but a universal one gets **arbitrarily close**.

Clifford Gates and Why T Is Needed

The Clifford group

Generated by $\{H, S, \text{CNOT}\}$. It maps Pauli operators to Pauli operators.

Gottesman–Knill theorem

A circuit of *only* Clifford gates (with computational-basis input and measurement) can be **efficiently simulated on a classical computer**.

Consequence

Clifford gates alone are **not universal** (else classical simulation of all quantum computation would follow). Adding a *non-Clifford* gate such as T restores universality:

$$\{H, S, \text{CNOT}\} + T \Rightarrow \text{universal}.$$

Approximating Unitaries — Errors Add Up

Composition lemma

If each gate U_i is replaced by an approximation V_i with $\|U_i - V_i\| \le \varepsilon$, then for the whole circuit

$$\left\| U_m \cdots U_1 - V_m \cdots V_1 \right\| \;\le\; \sum_{i=1}^{m} \|U_i - V_i\| \;\le\; m\,\varepsilon.$$

Design rule

To reach total error ε over m gates, approximate *each* gate to ε/m. Errors accumulate at most **linearly** — very forgiving.

So the real question is

How many gates from a discrete set does it take to reach accuracy ε per unitary? Answered by Solovay–Kitaev (next).

The Solovay–Kitaev Theorem

Statement (single qubit)

Let $\mathcal{G}$ be a universal single-qubit gate set that is *closed under inverses*. Then any single-qubit unitary can be approximated to accuracy ε using

$$\boxed{O\big(\log^{c}(1/\varepsilon)\big) \text{ gates}, \qquad c \text{ a small constant } (c \approx 2)\,.}$$

Why it is wonderful

The overhead is **poly-logarithmic** in $1/\varepsilon$: halving the error costs only a constant factor more gates.
Discrete gate sets are essentially as powerful as continuous ones.

For a whole circuit

A circuit of m ideal gates, each compiled to accuracy ε/m, needs $O\big(m \log^{c}(m/\varepsilon)\big)$ gates from the discrete set — still efficient.

Not Everything Is Efficient (A Counting Argument)

The tension

Universality says every U is *reachable*; it does **not** say cheaply.

- Circuits of g gates from a size-K set on n qubits: at most $\sim (Kn^2)^g$ distinct unitaries.
- The group $U(2^n)$ has real dimension 4^n; covering it to accuracy ε needs $\sim (1/\varepsilon)^{4^n}$ points.
- Matching the two forces $g = \Omega\big(4^n \log(1/\varepsilon)\big)$.

Moral

Almost all n-qubit unitaries require an *exponential* number of gates. The useful ones (algorithms) are the rare, structured exceptions.

Worked Example — Building Gates from $\{H, T\}$

Phase gates from T

$$S = T^2 = \mathrm{diag}(1, i), \qquad Z = T^4 = \mathrm{diag}(1, -1).$$

Bit-flip from H and Z

$$HZH = X: \quad H\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

So $X = H\,T^4\,H$.

And the rest

$Y = iXZ$, so Y also follows from $\{H, T\}$ (up to global phase).

With CNOT added, $\{H, T, \mathrm{CNOT}\}$ approximates *any* multi-qubit unitary.

Takeaway

A handful of primitive gates, composed cleverly, reconstruct the whole gate zoo.

Quick Check — Round 2 (Universality & Approximation)

[Q1]

Define what it means for a set of gates to be *universal*.

[Q2]

Name one *exactly* universal set and one *discrete* universal set.

[Q3]

State the Solovay–Kitaev theorem informally (the gate count to reach accuracy ε).

[Q4]

Why is the Clifford group $\{H, S, \mathrm{CNOT}\}$ *not* universal?

Answers — Round 2

[A1]

Its circuits can approximate *any* unitary to arbitrary accuracy ε (in operator norm).

[A2]

Exact: *all single-qubit gates* + *CNOT*. Discrete: $\{H, T, \mathbf{CNOT}\}$.

[A3]

Any single-qubit unitary can be approximated to accuracy ε using only $O(\log^c(1/\varepsilon))$ gates ($c \approx 2$) from a universal set — poly-logarithmic overhead.

[A4]

By the **Gottesman–Knill theorem**, Clifford circuits are efficiently classically simulable; a universal set would make *all* quantum computation classically efficient. A non-Clifford gate (T) is required.

Measurement in the Computational Basis

Projective (von Neumann) measurement

Measuring $|\psi\rangle = \sum_k c_k |k\rangle$ in $\{|k\rangle\}$ gives outcome k with

$$\Pr[k] = |c_k|^2 = |\langle k|\psi\rangle|^2,$$

after which the state **collapses** to $|k\rangle$.

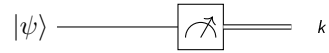


Figure: measurement outputs a classical bit (double line).

- Output is a classical bit-string; the process is *irreversible*.
- "Copying" a basis state: $\mathrm{CNOT}\,|x\rangle\,|0\rangle = |x\rangle\,|x\rangle$ for $x \in \{0,1\}$ (*not* cloning of superpositions!).

Measuring in an Arbitrary Orthonormal Basis

Basis change = rotate, then measure

To measure in an orthonormal basis $\{|\varphi_k\rangle\}$, pick a unitary U with $U|\varphi_k\rangle = |k\rangle$, apply U, then measure in the computational basis:

$$\Pr[k] = |\langle\varphi_k|\psi\rangle|^2 = |\langle k|U|\psi\rangle|^2.$$

Recipe

1. Build U that sends the desired basis to $\{|k\rangle\}$.
2. Apply U to the state.
3. Measure in the computational basis; relabel outcome $k \leftrightarrow |\varphi_k\rangle$.

Why this is enough

Hardware measures in one fixed basis; *any* projective measurement is that fixed measurement preceded by a suitable unitary.

Worked Example — Measuring in the X (Hadamard) Basis

Basis $\{|+\rangle, |-\rangle\}$

Since $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, take $U = H$. For $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$H|\psi\rangle = \tfrac{\alpha+\beta}{\sqrt{2}}|0\rangle + \tfrac{\alpha-\beta}{\sqrt{2}}|1\rangle.$$

$$\Pr[+] = \tfrac{|\alpha+\beta|^2}{2}, \qquad \Pr[-] = \tfrac{|\alpha-\beta|^2}{2}.$$

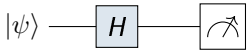
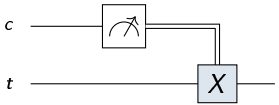


Figure: an X-basis measurement is H then a Z-basis measurement.

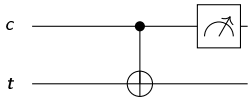
Principle of Deferred Measurement

Statement

Measurements can always be **moved to the end** of a circuit. If a measurement outcome classically controls a later gate, that classical control can be replaced by a *quantum*-controlled gate.



measure, then classical-control



quantum-control (CNOT), then measure

The two circuits give identical output statistics.

Principle of Implicit Measurement

Statement

Any qubits left *unmeasured* at the end of a circuit may be **assumed to be measured** without changing the measurement statistics of the qubits we *do* read.

Why it's useful

Lets us reason about *sub-circuits* and reduced states, and simplifies proofs about garbage / ancilla qubits.

- Discarding a qubit = tracing it out.
- Tracing out = measuring it and ignoring the result.
- So "ignore" and "measure-then-ignore" are indistinguishable to an observer of the rest.

Measuring an Observable

Hermitian observable

An observable $M = M^\dagger$ has spectral form $M = \sum_m m\, P_m$ (Unit 2). Measuring M yields eigenvalue m with

$$\Pr[m] = \langle\psi|\, P_m\, |\psi\rangle\,, \qquad \text{post-state } \frac{P_m\,|\psi\rangle}{\sqrt{\Pr[m]}}.$$

Circuit implementation

Diagonalise $M = UDU^\dagger$. Apply $U^\dagger$, measure in the computational basis to read an eigenvalue, then (if needed) apply U to restore the eigenstate.

Expectation value

Averaging outcomes gives $\langle M\rangle = \langle\psi|\, M\, |\psi\rangle$ — estimated by repeating and averaging, the basis of many quantum algorithms.

Worked Example — Bell-Basis Measurement

Circuit: CNOT, then H on the control

This rotates the Bell basis to the computational basis:

$$|\Phi^+\rangle \mapsto |00\rangle\,, \qquad |\Phi^-\rangle \mapsto |10\rangle\,,$$
$$|\Psi^+\rangle \mapsto |01\rangle\,, \qquad |\Psi^-\rangle \mapsto |11\rangle\,.$$

Measuring both qubits then identifies which Bell state was present.

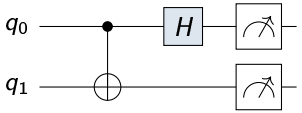


Figure: the inverse of the Bell-generator measures in the Bell basis.

Quick Check — Round 3 (Measurements)

[Q1]

How do you measure a qubit in the $\{|+\rangle, |-\rangle\}$ basis using a circuit?

[Q2]

State the principle of deferred measurement.

[Q3]

State the principle of implicit measurement.

[Q4] MCQ

Applying H just before a computational-basis measurement measures in which basis?
(a) Z (b) X (c) Y (d) Bell

Answers — Round 3

[A1]

Apply H, then measure in the computational basis ($H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$).

[A2]

Measurements can be pushed to the end of a circuit; a gate classically controlled by a measurement outcome can be replaced by a *quantum*-controlled gate, with identical statistics.

[A3]

Qubits left unmeasured at the end may be assumed measured without affecting the statistics of the measured qubits.

[A4]

(b) the X basis — H maps $\{|+\rangle, |-\rangle\}$ to $\{|0\rangle, |1\rangle\}$.

Summary of Unit 3

What we covered

1. **Quantum circuit model** — qubits on wires, unitary gates, measurement; size and depth.
2. **Single-qubit gates** — Pauli X, Y, Z; H; phase S, T; rotations R_x, R_y, R_z.
3. **Multi-qubit gates** — CNOT, CZ, controlled-U, SWAP, Toffoli, Fredkin.
4. **Bell-state circuit** — H then CNOT produces entanglement.
5. **Universality** — exact (1-qubit + CNOT) and discrete ($\{H, T, \text{CNOT}\}$); Clifford+T.
6. **Approximation** — errors add linearly; Solovay–Kitaev gives $O(\log^c(1/\varepsilon))$ gates.
7. **Counting** — almost all unitaries still need exponentially many gates.
8. **Measurements** — basis change, deferred and implicit measurement, measuring observables, Bell measurement.

A few reversible gates plus measurement is all a quantum computer needs.

Practice Questions (Exam Oriented)

Short answer (2–5 marks)

1. Draw the quantum circuit model and label its parts.
2. Give the matrices of X, Y, Z, H, S, T and one relation among them.
3. Define a universal gate set; give an exact and a discrete example.
4. State the Solovay–Kitaev theorem and the error-composition lemma.
5. State the principles of deferred and implicit measurement.

Long answer (8–10 marks)

6. Show H then CNOT prepares $|\Phi^+\rangle$; give circuits for all four Bell states.
7. Prove SWAP = three CNOTs; write the SWAP matrix.
8. Explain why the Clifford group is not universal (Gottesman–Knill) and how T fixes it.
9. Design a circuit to measure a qubit in the X basis and in the Y basis; give the probabilities.
10. Describe the Bell-measurement circuit and verify its action on the four Bell states.

Think & Explore (Take-Home)

Mini task (by hand)

- Verify SWAP $= \mathrm{CNOT}_{01}\,\mathrm{CNOT}_{10}\,\mathrm{CNOT}_{01}$.
- Give circuits producing $|\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$.
- Design a circuit to measure in the Y basis (hint: use $S^\dagger$ then H).

Coding (self-learning)

In `Qiskit`: build the Bell circuit, add measurements, run on the simulator; then implement Bell-basis measurement and confirm the $|\Phi^+\rangle \to 00$ mapping.

Reading & reflection

- Nielsen & Chuang, Ch. 4 (quantum circuits; §4.4–4.5).
- Kaye–Laflamme–Mosca, Ch. 4.
- Prepare for **Unit 4**: first quantum algorithms (Deutsch–Jozsa, Grover).

Reminder

Assignment 2 covers Unit 3 — handwritten, step-by-step, submitted as a single PDF via the course page.

References

Textbooks (as per the course page)

1. P. Kaye, R. Laflamme & M. Mosca, *An Introduction to Quantum Computing*, Oxford Univ. Press (Ch. 4). **[Main text]**
2. M. A. Nielsen & I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge (Ch. 4).

Seminal papers

3. A. Barenco *et al.*, "Elementary gates for quantum computation," *Phys. Rev. A*, 1995.
4. D. Gottesman, "The Heisenberg representation of quantum computers," 1998 (Gottesman–Knill).
5. C. M. Dawson & M. A. Nielsen, "The Solovay–Kitaev algorithm," *QIC*, 2006.
6. A. Yu. Kitaev, "Quantum computations: algorithms and error correction," *Russ. Math. Surv.*, 1997.

NPTEL: *Quantum Computing* · Course page: https://www.gcjana.in/courses/shardauniversity/2501/quantum-computing/

Thank You

Any Questions?

"Information is physical."

— Rolf Landauer

Post your doubts on the course page →

https://www.gcjana.in/courses/shardauniversity/2501/quantum-computing/#Post-doubts