Sharda University

School of Computing Science and Engineering • Department of Computer Science & Engineering

Quantum Computing (CSE063)

Assignment Question Bank (Unit-wise)

Programme: B.Tech, Computer Science & Engineering (CSE) • **Credits:** 3 • **L–T–P:** 3–0–2

Course Instructor: Dr. Gopal Chandra Jana • **Main text:** Kaye, Laflamme & Mosca

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

Instructions

- This question bank is intended for **B.Tech (CSE)** students of the Quantum Computing course.
- Each unit contains **20 questions**. The mark value of every question is shown at the right as **[marks]** and is one of **4, 6, 8, 10, 12, 15**.
- Questions are grouped by the sub-topics **A**, **B**, **C** of each unit; numbering runs Q1–Q20 within a unit.
- **Assignment 1** draws from **Units 1 & 2**; **Assignment 2** draws from **Units 3, 4 & 5** (attempt the questions assigned by the instructor).
- All solutions must be **handwritten**, presented in a clear, **step-by-step** manner, and submitted as a single PDF.
- Indicative **key answers** are given in the **Annexure** at the end — read the important note there before using them.

Unit 1 — Introduction

A. Computers and the Strong Church–Turing Thesis, Circuit Model of Computation

Q1. State the Church–Turing thesis. How does it differ from the *Strong* (Extended) Church–Turing thesis? **[4 marks]**

Q2. Define a *universal* (functionally complete) set of classical logic gates and give two examples. **[4 marks]**

Q3. Show that {NAND} is functionally complete by constructing NOT, AND and OR using only NAND gates. **[6 marks]**

Q4. What is a *model of computation*? Name three models equivalent to the Turing machine and state precisely what "equivalent" means here. **[6 marks]**

Q5. Explain the classical *circuit model* of computation. Define circuit *size* and *depth*, and state how uniform circuit families relate to Turing machines. **[8 marks]**

Q6. Design a half-adder and a full-adder using classical logic gates. Give truth tables and circuit diagrams, and explain how full-adders chain to add two n-bit numbers. **[10 marks]**

Q7. Discuss the Strong Church–Turing thesis and explain, using integer *factoring* as an example, how quantum computing appears to challenge it. Clearly distinguish *computability* from *efficiency* (classes P, BPP, BQP). **[12 marks]**

B. A Linear Algebra Formulation of the Circuit Model, Reversible Computation

Q8. Represent the classical bits 0 and 1 as vectors and write the matrix of the NOT gate. **[4 marks]**

Q9. State Landauer's principle. What is the minimum energy dissipated when one bit of information is erased? **[4 marks]**

Q10. Explain how a deterministic reversible gate corresponds to a *permutation matrix*. Illustrate with CNOT and give its 4×4 matrix. **[6 marks]**

Q11. Using the tensor product, compute $|1\rangle \otimes |0\rangle$ as a vector and state the dimension of the two-bit state space. **[6 marks]**

Q12. Explain why AND and OR are logically *irreversible* while NOT and CNOT are *reversible*. Relate irreversibility to Landauer's principle. **[8 marks]**

Q13. Describe the Toffoli (CCNOT) gate: give its action on $|a, b, c\rangle$ and its truth table. Show that it is *universal for reversible classical computation* (e.g. realise AND / NAND). **[10 marks]**

Q14. Explain reversible computation: state Bennett's result on making any computation reversible, discuss the role of *ancilla* and *garbage* bits, and explain why quantum gates being *unitary* makes reversible classical logic a prerequisite. **[12 marks]**

C. Quantum Physics and Computation

Q15. Define a *qubit*. Write the general single-qubit state and the normalisation condition. **[4 marks]**

Q16. What is *superposition*? How does a qubit differ from a classical bit? **[4 marks]**

Q17. State the Born rule. For $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$, compute the probabilities of measuring 0 and 1. **[6 marks]**

Q18. Explain *superposition*, *measurement* (collapse) and the *no-cloning theorem*. Why can an unknown quantum state not be copied? **[8 marks]**

Q19. Contrast classical and quantum computation across: state representation, composition of systems, evolution and read-out; explain the role of *interference*. **[10 marks]**

Q20. "Quantum physics enables new computational power." Discuss this, covering superposition and the exponential-size state space, entanglement, interference, and the historical motivations (Feynman 1982, Deutsch 1985). Explain why a large state space alone is *not* "free parallelism". **[15 marks]**

Unit 2 — Linear Algebra and the Dirac Notation

A. The Dirac Notation and Hilbert Spaces, Dual Vectors, Operators

Q1. Define a *Hilbert space*. What does "complete" mean, and why is it automatic in finite dimensions? **[4 marks]**

Q2. Write the bra corresponding to $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and state the ket→bra correspondence. **[4 marks]**

Q3. Define the outer product $|\phi\rangle\langle\psi|$ and show that $P = |\psi\rangle\langle\psi|$ (normalised) is a projector ($P^2 = P$). **[4 marks]**

Q4. State the axioms of the inner product (conjugate symmetry, linearity, positive-definiteness) in the physics convention. **[6 marks]**

Q5. Compute $\langle 0|1\rangle$ and $\langle +|+\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; verify orthonormality of $\{|0\rangle, |1\rangle\}$. **[6 marks]**

Q6. Define Hermitian, unitary and normal operators; state one relationship among these classes. **[6 marks]**

Q7. Define the adjoint $A^\dagger$ of an operator. Prove $(AB)^\dagger = B^\dagger A^\dagger$ and $(|\phi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\phi|$. **[8 marks]**

Q8. Prove that a unitary operator preserves inner products, and hence maps an orthonormal basis to an orthonormal basis. **[8 marks]**

Q9. State the completeness relation (resolution of identity) and use it to expand an arbitrary state in an orthonormal basis. Why is it the "workhorse" of Dirac notation? **[10 marks]**

B. The Spectral Theorem, Functions of Operators

Q10. Define eigenvalues and eigenvectors of an operator and give the characteristic equation. **[4 marks]**

Q11. Define a function $f(A)$ of a normal operator via its spectral decomposition. Compute $\sqrt{A}$ when A has eigenvalues 4 and 9 with projectors P_1, P_2. **[6 marks]**

Q12. Find the spectral decomposition of the Pauli X operator (eigenvalues and eigenvectors), and verify $X = |+\rangle\langle+| - |-\rangle\langle-|$. **[8 marks]**

Q13. State the spectral theorem for a *normal* operator. Explain the special cases for Hermitian and unitary operators (their eigenvalues). **[10 marks]**

Q14. Define the operator exponential e^A. Prove that for an involution ($A^2 = I$), $e^{i\theta A} = \cos\theta\, I + i\sin\theta\, A$, and apply it to compute $e^{i\theta Z}$. **[12 marks]**

C. Tensor Products, The Schmidt Decomposition Theorem

Q15. Define the tensor product of two Hilbert spaces. How does the dimension combine? **[4 marks]**

Q16. Compute $|0\rangle \otimes |1\rangle$ as a 4-vector (Kronecker product) and state the rule $(A \otimes B)(C \otimes D) = AC \otimes BD$. **[6 marks]**

Q17. Distinguish product (separable) from entangled states, with one two-qubit example of each. **[6 marks]**

Q18. State the Schmidt decomposition theorem and explain how the *Schmidt rank* distinguishes product from entangled states. **[10 marks]**

Q19. Give the algorithm to compute a Schmidt decomposition via the singular value decomposition (SVD). Apply it to the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and to a product state. **[12 marks]**

Q20. Develop the linear-algebra foundations of quantum mechanics in Dirac notation: kets, bras, inner/outer products, operators and adjoints; state the spectral theorem; and show how tensor products and the Schmidt decomposition describe composite systems and entanglement. Illustrate with the Bell state. **[15 marks]**

Unit 3 — A Quantum Model of Computation

A. The Quantum Circuit Model, Quantum Gates

Q1. Describe the quantum circuit model. What are its inputs, operations and outputs, and how is cost measured? **[4 marks]**

Q2. Give the matrices of the Pauli gates X, Y, Z and state their key properties. **[4 marks]**

Q3. Give the matrix of the Hadamard gate H. Show $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$ and $H^2 = I$. **[6 marks]**

Q4. Define the phase gates S and T and state the relations among S, T and Z. **[6 marks]**

Q5. Define the SWAP gate and state that SWAP = three CNOTs; give the Toffoli gate action. **[6 marks]**

Q6. Define the CNOT gate: give its action on $|a, b\rangle$ and its 4×4 matrix; define controlled-U and CZ. **[8 marks]**

Q7. Show that the circuit "H on q_0 followed by CNOT" prepares the Bell state $|\Phi^+\rangle$ from $|00\rangle$, tracing the state through each gate. **[8 marks]**

Q8. Define the single-qubit rotations R_x, R_y, R_z and state the Z–Y decomposition of an arbitrary single-qubit unitary. **[10 marks]**

B. Universal Sets of Quantum Gates, Efficiency of Approximating Unitary Transformations

Q9. Define a *universal* set of quantum gates (approximate universality). Why can a finite set not realise every unitary *exactly*? **[4 marks]**

Q10. Name one *exactly* universal gate set and one *discrete* universal set; what role does CNOT play? **[6 marks]**

Q11. Show how to build S, Z and X from $\{H, T\}$ (e.g. $S = T^2$, $Z = T^4$, $X = HZH$). **[6 marks]**

Q12. State the error-composition lemma for a circuit of m gates. If each gate is approximated to accuracy ε, bound the total error and give the per-gate target. **[8 marks]**

Q13. Explain the Clifford group and the Gottesman–Knill theorem. Why is the Clifford group *not* universal, and how does adding T fix this? **[8 marks]**

Q14. State the Solovay–Kitaev theorem. Explain the significance of the poly-logarithmic gate count for approximating a single-qubit unitary. **[10 marks]**

Q15. Discuss the efficiency of approximating unitary transformations: state the Solovay–Kitaev result and the error-composition lemma, and present the *counting argument* showing that almost all n-qubit unitaries need exponentially many gates. **[15 marks]**

C. Implementing Measurements with Quantum Circuits

Q16. Describe computational-basis measurement: the outcome probabilities and the post-measurement (collapse) state. **[4 marks]**

Q17. State the principle of *deferred measurement* and the principle of *implicit measurement*. **[6 marks]**

Q18. Explain how to measure a qubit in an arbitrary orthonormal basis via a unitary basis change; illustrate with measurement in the $\{|+\rangle, |-\rangle\}$ basis. **[8 marks]**

Q19. Describe how to measure a Hermitian observable M with a circuit (diagonalise, rotate, measure) and how expectation values $\langle M \rangle$ are estimated. **[10 marks]**

Q20. Design and analyse the Bell-basis measurement circuit (CNOT, then H, then measure). Show the mapping of the four Bell states to the computational-basis outcomes. **[12 marks]**

Unit 4 — Introductory Quantum Algorithms

A. Probabilistic Versus Quantum Algorithms, Phase Kick-Back

Q1. Contrast probabilistic and quantum algorithms in state representation and evolution. What phenomenon is unique to quantum? **[4 marks]**

Q2. Using $H{\cdot}H\,|0\rangle = |0\rangle$, explain destructive interference. Why is interference impossible for classical probabilities? **[4 marks]**

Q3. Define the standard (XOR) oracle U_f and show that it is unitary and its own inverse. **[6 marks]**

Q4. Explain the phase kick-back trick: derive $U_f\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle$. **[6 marks]**

Q5. Using the general controlled-U picture, explain how a target eigenstate absorbs the operation while its eigenphase is "kicked back" onto the control; connect to the $(-1)^{f(x)}$ case. **[8 marks]**

B. The Deutsch Algorithm, The Deutsch–Jozsa Algorithm

Q6. State Deutsch's problem. What single bit must be computed, and how many classical queries does it need? **[4 marks]**

Q7. For $f : \{0,1\} \to \{0,1\}$, list the four possible functions and classify each as constant or balanced. **[4 marks]**

Q8. State the Deutsch–Jozsa problem and the measurement rule (which outcome indicates a *constant* function). **[6 marks]**

Q9. Compare the classical and quantum query complexity of Deutsch and Deutsch–Jozsa; state honestly why D–J's exponential gap holds only against *deterministic* classical algorithms. **[6 marks]**

Q10. Using $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_z (-1)^{x\cdot z}|z\rangle$, explain the interference that concentrates (constant) or cancels (balanced) the all-zeros amplitude in Deutsch–Jozsa. **[8 marks]**

Q11. Derive the Deutsch algorithm end-to-end (state after each step) and show that a single query yields $f(0) \oplus f(1)$. **[10 marks]**

Q12. Present the Deutsch–Jozsa circuit and derive the amplitude of $|0\cdots 0\rangle = \frac{1}{2^n}\sum_x (-1)^{f(x)}$; analyse the constant and balanced cases. **[10 marks]**

Q13. Give a complete treatment of Deutsch–Jozsa: problem, circuit, derivation of the output amplitudes, the constant/balanced analysis, and the query-complexity comparison (including the randomised-classical caveat). **[12 marks]**

C. Simon's Algorithm

Q14. Define the inner product $x \cdot z$ over GF(2) used in the Hadamard transform, and compute $101 \cdot 110$. **[4 marks]**

Q15. State Simon's problem (the hidden-string promise). What must the algorithm find? **[6 marks]**

Q16. State the classical and quantum query complexity of Simon's problem. Why is its speed-up "stronger" than Deutsch–Jozsa's? **[6 marks]**

Q17. Explain how repeated runs of Simon's algorithm produce linear equations over GF(2) and how s is recovered by Gaussian elimination; how many runs are needed? **[8 marks]**

Q18. Present Simon's circuit and show that, after the final Hadamards, the measured string z satisfies $s \cdot z = 0 \pmod 2$. **[10 marks]**

Q19. Work a concrete example of Simon's algorithm for $n = 2$ with hidden string $s = 11$: construct a valid two-to-one oracle, describe the measurement outcomes, and recover s. **[12 marks]**

Q20. Discuss how the Deutsch, Deutsch–Jozsa and Simon algorithms illustrate the power of interference. Explain the common template (prepare superposition → query → interfere → measure) and how Simon's hidden-subgroup structure foreshadows Shor's algorithm. **[15 marks]**

Unit 5 — Analysis Tools, Discrete Logarithms & Schmidt Decompositions

A. Tools for Analysing Probabilistic Algorithms

Q1. Define expectation and variance of a random variable and state the linearity of expectation. **[4 marks]**

Q2. State Markov's inequality and its one requirement on X. **[4 marks]**

Q3. State the expected number of independent trials (each succeeding with probability p) until the first success. **[4 marks]**

Q4. State Chebyshev's inequality and show how it follows from Markov's inequality applied to $(X - \mu)^2$. **[6 marks]**

Q5. State the Chernoff/Hoeffding bound for a sum (or mean) of independent bounded variables; how does its decay compare with Chebyshev's? State the union bound. **[6 marks]**

Q6. Explain probability amplification by majority voting: if one run is correct with probability $\frac{1}{2}+\gamma$, bound the error of a k-run majority vote and find k for a target error δ. **[8 marks]**

Q7. A randomised algorithm is correct with probability 2/3. Derive the number of independent repetitions (with majority vote) needed to reduce the error below 1%; show the calculation. **[10 marks]**

B. Solving the Discrete Logarithm Problem When the Order of a Is Composite

Q8. State the discrete logarithm problem (DLP) in a cyclic group of order r. **[4 marks]**

Q9. Describe the setup of Shor's discrete-logarithm algorithm: registers, the function $f(x, y) = a^x b^y$, and the role of the QFT. **[6 marks]**

Q10. Given $t \equiv 2 \pmod 3$ and $t \equiv 1 \pmod 5$, find $t \pmod{15}$ using the Chinese Remainder Theorem.

[6 marks]

Q11. Explain why a *prime* order r makes recovery of t easy (one run), relating to $\mathbb{Z}_r$ being a field.

[6 marks]

Q12. State the linear congruence $l_2 \equiv t\, l_1 \pmod r$ produced by each run and show how t is recovered when $\gcd(l_1, r) = 1$. **[8 marks]**

Q13. Explain the subtlety when the order r is *composite*: why l_1 may not be invertible, what partial information $t \bmod (r/d)$ is obtained, and how the CRT completes the recovery. **[10 marks]**

Q14. Work a complete composite-order example ($r = 6$, hidden $t = 4$): from runs giving $l_1 = 2$ and $l_1 = 3$, obtain the partial congruences and combine them by CRT to recover t; explain why the algorithm stays polynomial-time. **[12 marks]**

C. Computing Schmidt Decompositions

Q15. State the Schmidt decomposition theorem, including the constraint on the Schmidt coefficients.

[4 marks]

Q16. Given $|\psi\rangle = \sum_{ij} c_{ij} \, |i\rangle \, |j\rangle$, define the coefficient matrix C and relate the reduced density matrix ρ_A to C. **[6 marks]**

Q17. Describe the SVD method to compute a Schmidt decomposition; how are the Schmidt coefficients and Schmidt rank read off?

[8 marks]

Q18. Describe the reduced-density-matrix method (diagonalise ρ_A) and show it gives the same Schmidt coefficients as the SVD method. **[10 marks]**

Q19. Define the entanglement entropy $S = -\sum_k \lambda_k^2 \log_2 \lambda_k^2$ of a bipartite pure state in terms of its Schmidt coefficients. Compute S for the Bell state and for a product state, and state what each value indicates. **[8 marks]**

Q20. Compute the Schmidt decomposition of the disguised product state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ and of the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ via the SVD; state the Schmidt rank in each case and interpret it. Discuss the classical complexity of computing Schmidt decompositions and its honest limitation for many qubits. **[15 marks]**

Annexure — Key Answers (Indicative)

Important Note.

These key answers are **only an idea / outline**. They convey the core concept, formula or approach expected — they are *not* complete model answers. **Students must read further** (the prescribed textbook by Kaye–Laflamme–Mosca, Nielsen & Chuang, and the lecture slides) and **develop the full, detailed, step-by-step answers themselves**, with all derivations, diagrams and worked numbers shown.

Unit 1 — Key Answers

A1. **Church–Turing thesis:** anything computable by an effective/algorithmic procedure is computable by a Turing machine (about *computability*). **Strong** CT: any realistic model can be simulated by a (probabilistic) TM with only *polynomial* overhead (about *efficiency*).

A2. A gate set from which *every* Boolean function can be built. Examples: $\{\text{AND}, \text{OR}, \text{NOT}\}$; $\{\text{NAND}\}$; $\{\text{NOR}\}$.

A3. $\text{NOT}(a) = a \barwedge a$; $\text{AND}(a,b) = (a \barwedge b) \barwedge (a \barwedge b)$; $\text{OR}(a,b) = (a \barwedge a) \barwedge (b \barwedge b)$ (where $\barwedge$ is NAND). Hence NAND is functionally complete.

A4. A precise notion of allowed states/steps/outputs. Equivalent models: λ-calculus, RAM machine, cellular automata (also Boolean circuits). "Equivalent" = compute the same class of functions, shown by mutual simulation.

A5. An acyclic network of gates on wires computing $f : \{0,1\}^n \to \{0,1\}^m$. *Size* = number of gates; *depth* = longest input-to-output path. *Uniform* circuit families (one circuit per input size, generated by a TM) compute exactly the Turing-computable functions.

A6. Half-adder: $s = a \oplus b$, $c = a \wedge b$. Full-adder: sum $= a \oplus b \oplus c_{\text{in}}$, carry $= ab + bc_{\text{in}} + ac_{\text{in}}$. Chaining n full-adders (ripple carry) adds two n-bit numbers.

A7. Strong CT claims efficient (poly-time) classical simulation of any realistic device. Shor factors integers in poly-time with no known efficient classical algorithm $\Rightarrow$ apparent violation. Computability = what is computable at all; efficiency = resources: P (deterministic poly), BPP (randomised poly), BQP (quantum poly); believed $\text{P} \subseteq \text{BPP} \subseteq \text{BQP}$.

A8. $0 \leftrightarrow |0\rangle = (1,0)^\top$, $1 \leftrightarrow |1\rangle = (0,1)^\top$; NOT $= X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

A9. Erasing one bit dissipates at least $k_B T \ln 2$ of heat: logical irreversibility $\Rightarrow$ physical energy cost.

A10. A reversible gate permutes basis states, so its matrix has a single 1 per row/column (permutation matrix). CNOT: $|a,b\rangle \mapsto |a, a \oplus b\rangle$, matrix $\left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right)$.

A11. $|1\rangle \otimes |0\rangle = (0,0,1,0)^\top = |10\rangle$; dimension $2 \times 2 = 4$.

A12. AND/OR are many-to-one (inputs not recoverable from output) $\Rightarrow$ irreversible $\Rightarrow$ information erased $\Rightarrow$ heat (Landauer). NOT/CNOT are bijections $\Rightarrow$ reversible, no forced erasure.

A13. Toffoli: $|a,b,c\rangle \mapsto |a,b,\, c \oplus (a \wedge b)\rangle$ (flips c iff $a = b = 1$). Setting $c = 0$ gives AND; suitable inputs give NAND $\Rightarrow$ universal for reversible classical computation.

A14. Bennett: any computation can be made reversible using ancilla bits and *uncomputation* (which clears garbage), with polynomial overhead. Quantum gates are unitary (hence reversible), so reversible classical logic is the classical shadow of quantum computation.

A15. A qubit is a unit vector in $\mathbb{C}^2$: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, $\alpha, \beta \in \mathbb{C}$.

A16. Superposition: a qubit can be a linear combination of $|0\rangle$ and $|1\rangle$; a classical bit is only 0 or 1. Superposition + interference give quantum advantage.

A17. Born rule: $\Pr[k] = |\text{amplitude}_k|^2$. $\Pr[0] = (\sqrt{3}/2)^2 = 3/4$; $\Pr[1] = (1/2)^2 = 1/4$.

A18. Superposition = linear combination of basis states; measurement gives outcome k w.p. $|\text{amplitude}|^2$ and *collapses* the state; no-cloning: no unitary can copy an unknown state (it would break linearity).

A19. State: bit $\in \{0,1\}$ vs unit vector in $\mathbb{C}^2$; composition: cartesian vs tensor product; evolution: Boolean/stochastic vs unitary; read-out: deterministic vs probabilistic (Born). *Interference* (amplitude cancellation) is the key resource.

A20. n qubits carry 2^n complex amplitudes; entanglement gives non-classical correlations; interference lets wrong answers cancel. Feynman: simulating quantum systems is classically hard; Deutsch: a universal quantum computer. A large state space is *not* free parallelism because measurement returns just one string — algorithms must engineer *constructive* interference on the answer.

Unit 2 — Key Answers

A1. A complex vector space with an inner product that is *complete* (Cauchy sequences converge). In finite dimension it is $\mathbb{C}^n$ and completeness is automatic.

A2. $\langle\psi| = \alpha^* \langle 0| + \beta^* \langle 1| = (\alpha^*, \beta^*)$ (conjugate transpose); the ket→bra map is *antilinear*.

A3. $|\phi\rangle\langle\psi|$ is an operator: $(|\phi\rangle\langle\psi|)|\chi\rangle = \langle\psi|\chi\rangle|\phi\rangle$. For $P = |\psi\rangle\langle\psi|$ with $\langle\psi|\psi\rangle = 1$: $P^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = P$; also $P^\dagger = P$.

A4. $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$ (conjugate symmetry); linear in the ket (second) slot; $\langle\psi|\psi\rangle \geq 0$ with equality iff $|\psi\rangle = 0$.

A5. $\langle 0|1\rangle = 0$; $\langle +|+\rangle = \frac{1}{2}(1+0+0+1) = 1$; orthonormal: $\langle i|j\rangle = \delta_{ij}$.

A6. Hermitian $A^\dagger = A$ (real eigenvalues); unitary $U^\dagger U = UU^\dagger = I$ (norm-preserving); normal $A^\dagger A = AA^\dagger$. Hermitian and unitary are both special cases of normal.

A7. $A^\dagger$ satisfies $\langle\phi|A|\psi\rangle^* = \langle\psi|A^\dagger|\phi\rangle$; in coordinates $A^\dagger = (A^*)^\top$. $(AB)^\dagger = B^\dagger A^\dagger$ and $(|\phi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\phi|$ (conjugate transpose / swap).

A8. $\langle U\phi|U\psi\rangle = \langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle$; hence images of an orthonormal basis stay orthonormal.

A9. $\sum_i |i\rangle\langle i| = I$. Then $|\psi\rangle = I|\psi\rangle = \sum_i |i\rangle\langle i|\psi\rangle = \sum_i c_i|i\rangle$ with $c_i = \langle i|\psi\rangle$. Inserting I anywhere expands in a chosen basis.

A10. $A|v\rangle = \lambda|v\rangle$, $|v\rangle \neq 0$; eigenvalues solve $\det(A - \lambda I) = 0$.

A11. $f(A) = \sum_i f(\lambda_i)|v_i\rangle\langle v_i|$. $\sqrt{A} = \sqrt{4}\,P_1 + \sqrt{9}\,P_2 = 2P_1 + 3P_2$.

A12. Eigenvalues ± 1, eigenvectors $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $X = |+\rangle\langle +| - |-\rangle\langle -|$. Check: $|+\rangle\langle +| - |-\rangle\langle -| = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = X$.

A13. A *normal* operator has an orthonormal eigenbasis $\{|v_i\rangle\}$ with $A = \sum_i \lambda_i |v_i\rangle\langle v_i|$ (equivalently $U^\dagger A U$ diagonal). Hermitian $\Rightarrow \lambda_i \in \mathbb{R}$; unitary $\Rightarrow |\lambda_i| = 1$.

A14. $e^A = \sum_k A^k/k!$. For $A^2 = I$, splitting even/odd terms gives $e^{i\theta A} = \cos\theta\, I + i \sin\theta\, A$. Hence $e^{i\theta Z} = \text{diag}(e^{i\theta}, e^{-i\theta})$.

A15. $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim = \dim(A) \cdot \dim(B)$; basis $\{|i\rangle \otimes |j\rangle\}$.

A16. $|0\rangle \otimes |1\rangle = (0,1,0,0)^\top = |01\rangle$; $(A \otimes B)(C \otimes D) = AC \otimes BD$.

A17. Product: $|\psi\rangle = |a\rangle \otimes |b\rangle$ (e.g. $|0\rangle \otimes |+\rangle$). Entangled: no such factorisation, e.g. $(|00\rangle + |11\rangle)/\sqrt{2}$.

A18. Any bipartite pure state $|\psi\rangle = \sum_k \lambda_k |u_k\rangle|v_k\rangle$ with orthonormal $\{|u_k\rangle\}, \{|v_k\rangle\}$, $\lambda_k \geq 0$, $\sum_k \lambda_k^2 = 1$. Schmidt rank = number of nonzero λ_k: rank 1 $\Leftrightarrow$ product, rank > 1 $\Leftrightarrow$ entangled.

A19. Form $C = (c_{ij})$; SVD $C = U\Sigma V^\dagger$; then $|\psi\rangle = \sum_k \sigma_k |u_k\rangle|v_k^*\rangle$, coefficients = singular values. Bell: $C = \frac{1}{\sqrt{2}} I \Rightarrow \sigma = \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}$ (rank 2). Product $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$: $C = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\sigma_1 = 1$ (rank 1) $\Rightarrow |0\rangle \otimes |+\rangle$.

A20. Comprehensive: assemble kets/bras/inner-outer products, operators & adjoints, the spectral theorem, tensor products and the Schmidt decomposition; the Bell state (Schmidt rank 2) illustrates entanglement. (Give all definitions and the worked Bell example in full — see notes.)

Unit 3 — Key Answers

A1. Inputs: qubits (usually $|0\rangle$); operations: unitary gates applied left-to-right; output: measurement (usually computational basis). Cost: size (#gates) and depth.

A2. $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$; Hermitian and unitary; $X^2 = Y^2 = Z^2 = I$; X bit-flip, Z phase-flip, $Y = iXZ$.

A3. $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$; $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, $H^2 = I$.

A4. $S = \mathrm{diag}(1, i)$, $T = \mathrm{diag}(1, e^{i\pi/4})$; $S = T^2$, $Z = S^2 = T^4$, $S = \sqrt{Z}$.

A5. SWAP: $|a, b\rangle \mapsto |b, a\rangle = \mathrm{CNOT}_{01}\mathrm{CNOT}_{10}\mathrm{CNOT}_{01}$. Toffoli: $|a, b, c\rangle \mapsto |a, b, c \oplus ab\rangle$.

A6. CNOT: $|a, b\rangle \mapsto |a, a \oplus b\rangle$, matrix $\left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right)$. Controlled-$U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U = \mathrm{diag}(I, U)$. $\mathrm{CZ} = \mathrm{diag}(1, 1, 1, -1)$.

A7. $|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\mathrm{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$.

A8. $R_x(\theta) = e^{-i\theta X/2}$, $R_y(\theta) = e^{-i\theta Y/2}$, $R_z(\theta) = e^{-i\theta Z/2} = \mathrm{diag}(e^{-i\theta/2}, e^{i\theta/2})$. Any $U \in U(2)$: $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

A9. A set whose circuits approximate any unitary to arbitrary accuracy ε. A finite set is countable while unitaries form a continuum, so exact realisation of *all* unitaries is impossible; approximation is not.

A10. Exact: all single-qubit gates + CNOT. Discrete: $\{H, T, \mathrm{CNOT}\}$. CNOT supplies the entangling two-qubit interaction.

A11. $S = T^2$, $Z = T^4$, $X = HZH = HT^4H$; also $Y = iXZ$.

A12. $\|U_m \cdots U_1 - V_m \cdots V_1\| \le \sum_i \|U_i - V_i\| \le m\varepsilon$; approximate each gate to ε/m for total error ε (errors add linearly).

A13. Clifford group $= \langle H, S, \mathrm{CNOT}\rangle$; Gottesman–Knill: Clifford circuits are efficiently classically simulable $\Rightarrow$ not universal. Adding a non-Clifford gate (T) restores universality.

A14. Solovay–Kitaev: any single-qubit unitary is approximable to accuracy ε using $O(\log^c(1/\varepsilon))$ gates ($c \approx 2$) from a universal (inverse-closed) set — poly-logarithmic overhead, so discrete sets are as powerful as continuous ones.

A15. Combine Solovay–Kitaev (poly-log per gate) with error composition (linear); but a counting argument — $\sim (Kn^2)^g$ circuits vs $\sim (1/\varepsilon)^{4^n}$ balls covering $U(2^n)$ — forces $g = \Omega(4^n \log(1/\varepsilon))$: almost all unitaries need exponentially many gates.

A16. $|\psi\rangle = \sum_k c_k |k\rangle \Rightarrow$ outcome k w.p. $|c_k|^2 = |\langle k|\psi\rangle|^2$; state collapses to $|k\rangle$.

A17. *Deferred:* measurements can be pushed to the end; a gate classically controlled by an outcome $\leftrightarrow$ a quantum-controlled gate. *Implicit:* unmeasured qubits at the end may be assumed measured without changing the statistics of measured qubits.

A18. To measure in $\{|\varphi_k\rangle\}$, apply U with $U|\varphi_k\rangle = |k\rangle$, then measure the computational basis. For $\{|+\rangle, |-\rangle\}$: apply H ($H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$), then measure.

A19. $M = \sum_m m P_m$; result m w.p. $\langle\psi| P_m |\psi\rangle$, post-state $P_m|\psi\rangle / \sqrt{\Pr[m]}$. Circuit: diagonalise $M = UDU^\dagger$, apply $U^\dagger$, measure, (optionally apply U). $\langle M\rangle = \langle\psi| M |\psi\rangle$ estimated by repeating and averaging.

A20. Circuit CNOT then H on the control then measure both. Mapping: $|\Phi^+\rangle \to 00$, $|\Phi^-\rangle \to 10$, $|\Psi^+\rangle \to 01$, $|\Psi^-\rangle \to 11$ (inverse of the Bell generator).

Unit 4 — Key Answers

A1. Probabilistic: probability vector, stochastic evolution, non-negative entries. Quantum: complex amplitude vector, unitary evolution; unique phenomenon = *interference* (amplitudes can cancel).

A2. $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; a second H makes the two paths to $|1\rangle$ carry $+\frac{1}{2}$ and $-\frac{1}{2}$, which cancel $\Rightarrow |0\rangle$. Classical probabilities are non-negative and cannot cancel.

A3. $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$: it permutes basis states (unitary) and applying it twice restores y ($U_f^2 = I$, self-inverse).

A4. $U_f|x\rangle|-\rangle = |x\rangle \frac{|f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle|-\rangle$ (+ if $f(x)=0$, − if $f(x)=1$).

A5. For controlled-U with target eigenstate $|\psi\rangle$ ($U|\psi\rangle = e^{i\varphi}|\psi\rangle$), the control acquires phase $e^{i\varphi}$. $|-\rangle$ is the (-1)-eigenstate of the bit-flip, giving $(-1)^{f(x)}$.

A6. Decide constant vs balanced = compute $f(0) \oplus f(1)$. Classical: 2 queries.

A7. $f \equiv 0$ (constant), $f \equiv 1$ (constant), $f(x) = x$ (balanced), $f(x) = \neg x$ (balanced).

A8. f is promised constant or balanced; measure the top n qubits — all zeros $\Rightarrow$ constant, otherwise balanced.

A9. Deutsch $2 \to 1$; D–J $2^{n-1}+1$ (deterministic) $\to 1$. D–J's exponential gap is only vs *deterministic* classical algorithms; a randomised one solves it in $O(1)$ queries with high probability.

A10. $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_z (-1)^{x\cdot z}|z\rangle$; the $z=0$ amplitude sums $(-1)^{f(x)}$. Constant $\Rightarrow$ all same sign (reinforce); balanced $\Rightarrow$ equal $\pm$ (cancel).

A11. $|0\rangle|1\rangle \xrightarrow{H\otimes H} |+\rangle|-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}\sum_x (-1)^{f(x)}|x\rangle|-\rangle$; the top qubit is $(\pm)(|0\rangle + (-1)^a|1\rangle)/\sqrt{2}$ with $a = f(0)\oplus f(1)$; a final H gives $|0\rangle$ if $a=0$, $|1\rangle$ if $a=1$. Measure $= a$.

A12. After kick-back and $H^{\otimes n}$, amplitude of $|0\cdots 0\rangle = \frac{1}{2^n}\sum_x (-1)^{f(x)} = \pm 1$ (constant, seen w.p. 1) or 0 (balanced, never seen).

A13. Full D–J: problem, circuit ($H^{\otimes n}\otimes H$, U_f, $H^{\otimes n}$, measure), derivation of the $|0\cdots 0\rangle$ amplitude, constant/balanced analysis, and query comparison with the randomised-classical caveat. (Show all steps.)

A14. $x \cdot z = \bigoplus_i x_i z_i \pmod 2$. $101 \cdot 110 = 1{\cdot}1 \oplus 0{\cdot}1 \oplus 1{\cdot}0 = 1$.

A15. f is two-to-one with a hidden $s \neq 0^n$ such that $f(x) = f(x \oplus s)$; find s.

A16. Classical $\Theta(2^{n/2})$ (even randomised); quantum $O(n)$. Stronger than D–J because the exponential gap holds against *randomised* classical algorithms too.

A17. Each run gives z with $s \cdot z = 0$ — a linear equation over GF(2). Collect $n-1$ independent equations (expected $O(n)$ runs) and solve by Gaussian elimination for the unique nonzero s.

A18. Prepare $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$; measuring the output collapses the input to $(|x_0\rangle + |x_0 \oplus s\rangle)/\sqrt{2}$; $H^{\otimes n}$ then gives amplitudes $\propto 1 + (-1)^{s\cdot z}$, nonzero only when $s \cdot z = 0$.

A19. E.g. $f(00) = f(11) = 00$, $f(01) = f(10) = 11$. Output measurement collapses input to $(|00\rangle + |11\rangle)/\sqrt{2}$ or $(|01\rangle + |10\rangle)/\sqrt{2}$; $H^{\otimes 2}$ yields z with $11 \cdot z = 0 \Rightarrow z \in \{00, 11\}$; the equation $z_1 \oplus z_2 = 0 \Rightarrow s_1 = s_2$, so with $s \neq 0$, $s = 11$.

A20. All three use *prepare superposition → query oracle → interfere (Hadamards) → measure.* Simon's hidden-subgroup (period) structure over $(\mathbb{Z}_2)^n$ generalises to Shor's period-finding over $\mathbb{Z}$ via the QFT.

Unit 5 — Key Answers

A1. $\mathbb{E}[X] = \sum_x x \Pr[X = x]$; $\mathrm{Var}(X) = \mathbb{E}[(X-\mu)^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$; $\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y]$ (always).

A2. For $X \geq 0$ and $a > 0$: $\Pr[X \geq a] \leq \mathbb{E}[X]/a$.

A3. Expected number of trials until the first success $= 1/p$.

A4. $\Pr[|X - \mu| \geq a] \leq \sigma^2/a^2$; follows by applying Markov to $(X-\mu)^2 \geq 0$ with threshold a^2.

A5. For independent bounded X_i, tails decay exponentially, e.g. Hoeffding $\Pr[|\bar{X} - \mathbb{E}\bar{X}| \geq \varepsilon] \leq 2e^{-2n\varepsilon^2}$ — far stronger than Chebyshev's $1/a^2$. Union bound: $\Pr[\bigcup_i A_i] \leq \sum_i \Pr[A_i]$.

A6. One run correct w.p. $\frac{1}{2}+\gamma$; k-run majority error $\le e^{-2\gamma^2 k}$; for error $\le \delta$ take $k \ge \ln(1/\delta)/(2\gamma^2)$.

A7. $\gamma = \frac{2}{3} - \frac{1}{2} = \frac{1}{6}$; error $\le e^{-2(1/6)^2 k} = e^{-k/18} \le 0.01 \Rightarrow k \ge 18 \ln 100 \approx 82.9 \Rightarrow k = 83$.

A8. In $\langle a \rangle$ of order r, given $b \in \langle a \rangle$, find t with $a^t = b$ (i.e. $t = \log_a b$).

A9. Two $\mathbb{Z}_r$ index registers + a value register; compute $f(x,y) = a^x b^y = a^{x+ty}$; apply QFT_r to both index registers; measure.

A10. $t \equiv 2 \pmod 3$, $t \equiv 1 \pmod 5 \Rightarrow t \equiv 11 \pmod{15}$ (since $11 \bmod 3 = 2$, $11 \bmod 5 = 1$).

A11. $\mathbb{Z}_r$ is a field when r is prime, so every $l_1 \neq 0$ is invertible $\Rightarrow t \equiv l_2 l_1^{-1}$ recovered in a single run.

A12. Each run gives (l_1, l_2) with $l_2 \equiv t\, l_1 \pmod r$, $l_1 \approx$ uniform. If $\gcd(l_1, r) = 1$: $t \equiv l_2\, l_1^{-1} \pmod r$.

A13. If $d = \gcd(l_1, r) > 1$, l_1 is not invertible; one learns only $t \equiv (l_2/d)(l_1/d)^{-1} \pmod{r/d}$. Combine several partial congruences by CRT; a poly-log number of runs suffices $\Rightarrow$ still polynomial.

A14. $r = 6$, $t = 4$: $l_1 = 2 \Rightarrow l_2 = 2$, $d = 2 \Rightarrow t \equiv 1 \pmod 3$; $l_1 = 3 \Rightarrow l_2 = 0$, $d = 3 \Rightarrow t \equiv 0 \pmod 2$. CRT $\Rightarrow t \equiv 4 \pmod 6$. Runs are poly-log and CRT is polynomial $\Rightarrow$ poly-time overall.

A15. $|\psi\rangle = \sum_k \lambda_k |u_k\rangle_A |v_k\rangle_B$ with orthonormal $\{|u_k\rangle\}, \{|v_k\rangle\}$, $\lambda_k \ge 0$, $\sum_k \lambda_k^2 = 1$; nonzero count = Schmidt rank.

A16. $C = (c_{ij})$ from $|\psi\rangle = \sum_{ij} c_{ij} |i\rangle |j\rangle$; $\rho_A = \mathrm{Tr}_B |\psi\rangle\langle\psi| = CC^\dagger$, whose eigenvalues are the λ_k^2.

A17. $C = U\Sigma V^\dagger$; $|\psi\rangle = \sum_k \sigma_k |u_k\rangle |v_k^*\rangle$; Schmidt coefficients = singular values σ_k; Schmidt rank = number of nonzero $\sigma_k = \mathrm{rank}(C)$.

A18. Diagonalise $\rho_A = \sum_k \lambda_k |u_k\rangle\langle u_k|$; set $\sigma_k = \sqrt{\lambda_k}$, $|v_k\rangle = \frac{1}{\sigma_k}(\langle u_k| \otimes I)|\psi\rangle$. Since singular values of C equal $\sqrt{\text{eigenvalues of } CC^\dagger} = \sqrt{\lambda_k}$, both methods give the same σ_k.

A19. $S = -\sum_k \lambda_k^2 \log_2 \lambda_k^2$. Bell: $\lambda_k^2 = \frac{1}{2}, \frac{1}{2} \Rightarrow S = -2 \cdot \frac{1}{2}\log_2 \frac{1}{2} = 1$ bit (maximal for one qubit). Product: one $\lambda = 1 \Rightarrow S = 0$. $S > 0$ signals entanglement; $S = 0$ means separable.

A20. $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$: $C = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 0 & 0\end{smallmatrix}\right)$, rank 1, $\sigma_1 = 1 \Rightarrow |0\rangle \otimes |+\rangle$ (product). Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$: $C = \frac{1}{\sqrt{2}} I$, $\sigma = \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}$, rank 2 (maximally entangled). SVD costs $O(d_A d_B \min(d_A, d_B))$ — polynomial in the matrix dimension, but $d = 2^n$, so efficient only when one subsystem is small.

Read the prescribed text and lecture notes; write your own complete, step-by-step solutions.
— Dr. Gopal Chandra Jana, Department of CSE, Sharda University