Quantum Computation and Information Theory Summary

Mathematical Notes

October 27, 2025

Contents

1 Foundations of Quantum Mechanics **3**
1.1 Postulates . . . 3
1.2 Dirac Notation and Linear Algebra . . . 3
1.3 Density Operators and Partial Trace . . . 3

2 Qubits and Single-Qubit Gates **3**
2.1 Qubit States . . . 3
2.2 Elementary Gates . . . 3

3 Multi-Qubit Systems and Circuits **3**
3.1 Tensor Products and Entanglement . . . 3
3.2 Controlled Gates and Universality . . . 3
3.3 Circuit Model . . . 3

4 Measurement Theory **4**
4.1 Projective Measurements . . . 4
4.2 POVMs and Naimark's Dilation . . . 4

5 Core Phenomena **4**
5.1 No-Cloning Theorem . . . 4
5.2 Bell States and Nonlocality . . . 4
5.3 Entanglement Measures . . . 4

6 Quantum Algorithms **4**
6.1 Fourier Transform . . . 4
6.2 Deutsch-Jozsa and Phase Kickback . . . 4
6.3 Grover's Search . . . 4
6.4 Shor's Algorithm (Outline) . . . 4

7 Noise and Quantum Channels **5**
7.1 CPTP Maps and Kraus Operators . . . 5
7.2 Canonical Noise Models . . . 5
7.3 Distances and Fidelity . . . 5

8 Quantum Error Correction **5**
8.1 Stabilizer Formalism . . . 5
8.2 Simple Codes . . . 5

9 Quantum Information Theory **5**
9.1 Von Neumann Entropy and Mutual Information 5
9.2 Data Processing and Strong Subadditivity 5
9.3 Holevo Bound 5
9.4 Channel Capacities (Overview) 5

10 Quantum Cryptography **6**
10.1 BB84 Protocol 6
10.2 Entanglement-Based QKD 6

11 Computational Complexity (Brief) **6**
11.1 BQP and QMA 6

12 References for Further Study **6**

1 Foundations of Quantum Mechanics

1.1 Postulates

1. States of an isolated system are represented by unit vectors $|\psi\rangle$ in a complex Hilbert space $\mathcal{H}$ (or density operators ρ with $\rho \succeq 0$ and $\operatorname{Tr}\rho = 1$).
2. Evolution is unitary: $|\psi\rangle \mapsto U|\psi\rangle$, or $\rho \mapsto U\rho U^\dagger$.
3. Measurements are described by a set of operators $\{M_m\}$ with $\sum_m M_m^\dagger M_m = I$. Outcome m occurs with probability $p(m) = \|M_m|\psi\rangle\|^2$ and post-measurement state $M_m|\psi\rangle/\sqrt{p(m)}$.
4. Composite systems are represented by the tensor product: $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

1.2 Dirac Notation and Linear Algebra

Let $|\psi\rangle \in \mathcal{H}$, $\langle\psi| = (|\psi\rangle)^\dagger$, and $\langle\phi|\psi\rangle$ the inner product. Observables are Hermitian operators $H = H^\dagger$.

1.3 Density Operators and Partial Trace

Mixed states are $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$. For a bipartite state ρ_{AB}, the reduced state on A is $\rho_A = \operatorname{Tr}_B \rho_{AB}$.

2 Qubits and Single-Qubit Gates

2.1 Qubit States

The computational basis is $\{|0\rangle, |1\rangle\}$. A pure qubit state is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. The Bloch representation uses Pauli matrices $\{X, Y, Z\}$: any state $\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$ with $\|\vec{r}\| \leq 1$.

2.2 Elementary Gates

Common gates: X, Y, Z, H, S, T and rotations $R_{\hat{n}}(\theta) = e^{-i\theta\,\hat{n}\cdot\vec{\sigma}/2}$. Any single-qubit unitary is a rotation on the Bloch sphere.

3 Multi-Qubit Systems and Circuits

3.1 Tensor Products and Entanglement

Composite states live in $\mathcal{H}_A \otimes \mathcal{H}_B$. A pure state $|\psi\rangle_{AB}$ is entangled if it cannot be written as $|\phi\rangle_A \otimes |\chi\rangle_B$. The Schmidt decomposition writes $|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\,|i\rangle_A|i\rangle_B$.

3.2 Controlled Gates and Universality

The CNOT gate together with all single-qubit gates generates a universal set for quantum computation.

3.3 Circuit Model

Algorithms are specified by unitary circuits acting on n qubits followed by measurements in the computational basis.

4 Measurement Theory

4.1 Projective Measurements

Given projectors $\{\Pi_m\}$ with $\Pi_m \Pi_{m'} = \delta_{mm'} \Pi_m$ and $\sum_m \Pi_m = I$, outcome m occurs with probability $p(m) = \mathrm{Tr}(\Pi_m \rho)$ and post-measurement state $\Pi_m \rho \Pi_m / p(m)$.

4.2 POVMs and Naimark's Dilation

General measurements are POVMs $\{E_m\}$ with $E_m \succeq 0$ and $\sum_m E_m = I$. Any POVM can be realized as a projective measurement on a larger Hilbert space.

5 Core Phenomena

5.1 No-Cloning Theorem

Theorem 5.1. There is no unitary U and fixed blank state $|0\rangle$ such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ for all $|\psi\rangle$.

5.2 Bell States and Nonlocality

The Bell basis: $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. Violations of CHSH inequalities witness nonclassical correlations.

5.3 Entanglement Measures

For a bipartite pure state, the entanglement entropy is $E(|\psi\rangle_{AB}) = S(\rho_A)$ where $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$ is the von Neumann entropy.

6 Quantum Algorithms

6.1 Fourier Transform

The Quantum Fourier Transform (QFT) on $N = 2^n$ basis states is $\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle$.

6.2 Deutsch-Jozsa and Phase Kickback

Using interference to distinguish constant vs balanced oracles in a single query for promise problems.

6.3 Grover's Search

Amplitude amplification finds a marked item in $O(\sqrt{N})$ queries using reflections about the uniform superposition and the solution subspace.

6.4 Shor's Algorithm (Outline)

Reduces integer factoring to period-finding via QFT, achieving polynomial time in the input length on a fault-tolerant quantum computer.

7 Noise and Quantum Channels

7.1 CPTP Maps and Kraus Operators

Quantum channels are completely positive trace-preserving maps with Kraus form $\mathcal{E}(\rho) = \sum_k K_k \rho K_k^\dagger$, $\sum_k K_k^\dagger K_k = I$.

7.2 Canonical Noise Models

Depolarizing: $\mathcal{D}_p(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$. Dephasing: $\mathcal{Z}_p(\rho) = (1-p)\rho + p\, Z\rho Z$. Amplitude damping with Kraus operators $K_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$, $K_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$.

7.3 Distances and Fidelity

Trace distance $\frac{1}{2}\|\rho - \sigma\|_1$ bounds state discrimination advantage; Uhlmann fidelity $F(\rho, \sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\,\sqrt{\rho}}\right)^2$ quantifies similarity.

8 Quantum Error Correction

8.1 Stabilizer Formalism

An $[[n, k, d]]$ stabilizer code is the common $+1$ eigenspace of an abelian subgroup $\mathcal{S}$ of the n-qubit Pauli group. Errors are detected via syndrome measurement.

8.2 Simple Codes

Bit-flip code encodes $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as $\alpha|000\rangle + \beta|111\rangle$. CSS construction combines classical linear codes to correct bit- and phase-flip errors.

9 Quantum Information Theory

9.1 Von Neumann Entropy and Mutual Information

$S(\rho) = -\mathrm{Tr}(\rho \log \rho)$, quantum mutual information $I(A : B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$.

9.2 Data Processing and Strong Subadditivity

For a channel $\mathcal{E}$, relative entropy contracts: $D(\rho \,\|\, \sigma) \geq D(\mathcal{E}(\rho) \,\|\, \mathcal{E}(\sigma))$. Strong subadditivity: $S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$.

9.3 Holevo Bound

For ensemble $\{p_x, \rho_x\}$ and measurement outcome Y, the accessible classical information satisfies $I(X : Y) \leq \chi := S(\sum_x p_x \rho_x) - \sum_x p_x S(\rho_x)$.

9.4 Channel Capacities (Overview)

Classical capacity C given by regularized Holevo information (HSW theorem). Quantum capacity Q given by regularized coherent information $I_c(\rho, \mathcal{N}) = S(\mathcal{N}(\rho)) - S((\mathrm{id} \otimes \mathcal{N})(|\psi\rangle\langle\psi|))$. Entanglement-assisted capacity $C_E = \max_\rho I(A : B)$ for the channel's Choi state.

10 Quantum Cryptography

10.1 BB84 Protocol

Encoding random bits in two conjugate bases, sifting, error estimation, information reconciliation, and privacy amplification yield a secret key; security from no-cloning and disturbance of nonorthogonal states.

10.2 Entanglement-Based QKD

E91 uses entangled pairs and Bell tests to certify security under device assumptions.

11 Computational Complexity (Brief)

11.1 BQP and QMA

BQP contains decision problems solvable by polynomial-size quantum circuits with bounded error. **QMA** is the quantum analogue of NP with a quantum proof and verifier.

12 References for Further Study

Nielsen and Chuang, "Quantum Computation and Quantum Information"; Watrous, "The Theory of Quantum Information"; Wilde, "Quantum Information Theory".