Mathematical Foundations of Quantum Computation

MA591: Lecture Notes

Moody T. Chu
NC State University

Table of Contents

Lecture 1. Historical Context and the Single Qubit

1. The Convergence of Disciplines
2. The Physics Crisis and Quantum Mechanics
3. Defining the Qubit
4. Superposition and Measurement
5. Geometric Representation: The Bloch Sphere

Lecture 2. Linear Algebra Foundations

1. Complex Vector Spaces and Hilbert Space
2. Formal Axioms of the Inner Product
3. Dirac Notation: Kets, Bras, and Duality
4. Riesz Representation and the Dual Space
5. Orthonormality and the Gram-Schmidt Process
6. The Completeness Relation (Resolution of the Identity)
7. Linear Operators, Outer Products and Adjoint
8. Spectral Decomposition

Lecture 3. Quantum Postulates and Entanglement

1. The Axiomatic Foundation: Postulates 1 & 2
2. The Copenhagen Interpretation
3. Postulate 3: Measurement and Observables
4. Pure vs. Mixed States: The Density Operator (ρ)
5. Postulate 4: Composite Systems and Tensor Products
6. Entanglement, Separability, and Bell States
7. The Environment: Partial Trace and Reduced Density Matrices
8. State Purification and Schmidt Decomposition

Lecture 4. Quantum Gates and Protocols

1. Fundamentals: Bits vs. Qubits
2. Thermodynamics of Computation: Landauer's Principle
3. Reversible Logic: XOR, Toffoli, and Ancilla Bits
4. Simulating Classical Logic: Reversible AND and NAND
5. Single-Qubit Operations and Pauli Matrices
6. The Hadamard Transformation and Initialization
7. Multi-Qubit Systems and Entanglement
8. Protocol 1: Superdense Coding
9. Protocol 2: Quantum Teleportation
10. Universality and the Solovay-Kitaev Theorem

Lecture 5. Computational Complexity and Reversibility

1. The Turing Perspective
2. The Strong Church-Turing Thesis
3. Thermodynamics of Computation
4. Reversible Computation

Lecture 6. Decomposition of Unitaries and Gate Synthesis

1. Decomposition of Unitaries
2. The Z-Y Decomposition Theorem
3. Two-Level Unitary Decompositions
4. Universal Gate Sets
5. Approximation and the Solovay-Kitaev Theorem

Lecture 7. Quantum Fourier Transform and Shor's Algorithm

1. Review of Classical Discrete Fourier Transform (DFT)
2. Mathematical Definition and Circuit Architecture of the QFT
3. Quantum Phase Estimation (QPE) and Error Performance Bounds
4. The Quantum Order-Finding Problem and Continued Fractions
5. Shor's Factoring Algorithm and Its Reduction to Order-Finding
6. General Period Finding and Shift Invariance

Lecture 8. RSA Cryptography and the Hidden Subgroup Problem

1. RSA Cryptosystem Vulnerabilities
2. Fermat's Little Theorem Foundations
3. Order-Finding Reduction Mechanics
4. Quantum Phase Oracle Superposition
5. Shift Invariance and Phase Decoupling
6. Blind Case Study: Factoring 15
7. The Hidden Subgroup Problem

Lecture 9. Grover's Search Algorithm

1. The Unstructured Search Problem
2. The Quantum Oracle and Phase Kickback
3. The Grover Iteration Operator (G)
4. Mathematical Analysis: Inversion About the Mean
5. Geometric Interpretation: 2D Subspace Rotations
6. Performance Analysis and Iteration Bounds
7. Generalization: Multiple Target Solutions

Lecture 10. Physical Realization and DiVincenzo Criteria

1. Geometric and Algebraic Constraints on Subspace Control
2. Continuous-Space Resonance and Subspace Leakage
3. Invariant Commutator Blocks in Coupled Dynamics
4. Adjoint Transformations on Traceless Deviation Algebras

Lecture 11. Open Quantum Systems and Noise Models

1. Axiomatic Formulation of Open Quantum Systems
2. The Partial Trace and Environmental Coupling Mechanics
3. The Operator-Sum Representation (Kraus Representation Theorem)
4. Unitary Freedom and Matrix Isomorphisms of Noise Maps
5. Discrete Qubit Noise: Bit-Flip, Phase-Flip, and Depolarization Channels
6. Continuous Dissipative Noise: Amplitude and Phase Damping Models
7. Geometric Characterization of Noise via Bloch Ball Deformations

Lecture 12. Quantum Distance Measures

1. Classical Distance Foundations: Defining Probability Distribution Similarity
2. Quantum Trace Distance: Geometric Interpretation and Physical Contractivity
3. Quantum Fidelity: Operational Overlap Measures and Uhlmann's Theorem
4. Distinguishability Relations: The Fuchs–van de Graaf Inequalities
5. Dynamic Distance Measures: Entanglement Fidelity and Channel Preservation

Lecture 13. Quantum Distance Measures

1. Introduction to Quantum Error-Correction
2. Fundamental Quantum Codes
3. General Theory of Error-Correction
4. Classical Linear and CSS Codes
5. The Stabilizer Formalism
6. Fault-Tolerant Quantum Computation
