PH 534 Spring 2023
Quantum Information and Computing

Himadri Shekhar Dhar

Room 304, Department of Physics
himadri.dhar@iitb.ac.in
+91 22 2576 **7570**

TENTATIVE OUTLINE OF THE COURSE

Module 1: Foundations – States and operators

1. Basic of QM – linear algebra, quantum state, evolution and measurements.
   Projective measurements vs POVM, distinguishing states, notion of a qubit.
2. Open system – the density matrix, partial trace, purification, Schmidt decomposition.
   Quantum operators – Kraus operators, Stinespring dilation, Choi representation.
   Examples of quantum operators/channels, Choi-Jamiolkowski isomorphism.

Module 2: Quantum information and entanglement

1. Entropy and the notion of information and entanglement – Shannon entropy, data compression, relative entropy, mutual information, conditional entropy, von Neumann entropy, quantum relative entropy, quantum mutual information.

   Encoding information in quantum states, accessible information and Holevo bound.

   Entanglement – LOCC, state transformation, majorization theory, Nielsen's theorem
   Measures of entanglement – maximally entangled states, distillation, von Neumann entropy of entanglement.
2. Convex sets and geometry of state space – mixed state entanglement, separable states, entanglement witness, necessary and sufficient criteria of entanglement, Peres-Horodecki criterion, computable measures of entanglement.

Module 3: Quantum computation

1. Quantum gates and circuits – single qubit gates, universal single qubit gates, controlled gates, basic quantum circuit.
   Toffoli and multi control gates, universal quantum gates, Gray code.
2. Quantum algorithms – functions and an "oracle", costs and notion of complexity.
   Primitives – Phase kickback, preimage states, qubit and n-level Fourier transform.
   Algorithms – Amplitude amplification, Deutsch-Jozsa, Bernstein-Vazirani, Simon's algorithm, period finding (Shor's algorithm).

Module 4: Quantum protocols

1. Quantum communication – Distinguishability between quantum states, fidelity of quantum states, no-cloning theorem, superdense coding, teleportation. Entanglement swapping, teleportation fidelity.

2. Cryptography – Vernam cipher, classical encryption, public key distribution and RSA, Shor's algorithm and attacking the factorisation problem.

   Quantum cryptography, quantum one-time pad, quantum security and entanglement, quantum key distribution, BB84 protocol, EPR/Ekert92 protocol.

Please note that all topics will not be given equal weightage. As this is an introductory course on quantum information theory and quantum computation, our aim will be to focus more on the basic conceptual and mathematical structures and simply touch upon the more complex and finer aspects of the subject. The objective is to familiarise the scholars with different aspects of the subject, which will provide them with a platform to pursue more specialised learning or research if they so desire.

SUGGESTED READING

M. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge)
M. Wilde, Quantum Information Theory (Cambridge)
J. Watrous, The Theory of Quantum Information (Cambridge)
H.-P Breuer and F. Petruccione, The Theory of Open Quantum Systems (Oxford)

EXAMS AND GRADING

Quiz/Assignment – 15%*2 or 10%*3
Mid semester exams – 30% (subject to change)
End semester exams – 40% (subject to change)

All students are required to pass the course to be awarded a credit or audit grade.

Grading will be relative. Pass marks pertain to no more than 30% of the highest grade.

COURSE TIMING/ INTERACTIONS

Class: 13A – Monday 19:00-20:25 hrs. (LT 102)
13B – Thursday 19:00-20:25 hrs. (LT 102)

In-person meeting: **Himadri:** Tuesday 17:00 – 18:00 hrs. (Department office)
TAs: Wednesday 17:00 – 19:00 hrs. (Labs)

Please write an email or message on MS Teams beforehand to schedule the meeting and provide an outline of the problem.

General interaction: We will use MS TEAMS as the primary platform for sharing important information, updates, doubts, and for general discussions about the course.