CO 481/CS 467/PHYS 467, Winter 2019
Introduction to Quantum Information Processing

Syllabus and schedule:

When quantum mechanics meets information processing: [5 lectures]

1. Information is physical and how quantum mechanics affects information processing [0.5 lecture] [NC 1.1, KLM 1.1-1.2]
2. Summary of theory of classical computation [1 lecture]
   (a) Bits, gates, circuits, universality, complexity [NC 3.1.2, KLM 1.3]
   (b) Linear algebra formalism of circuits (vectors, matrices, and tensor products) [KLM 1.4*]
   (c) Models of Computation (Turing machines, probabilistic model) [reading] [NC 3.1.1, KLM 1.2]
   (d) Reversible computation [reading] [KLM 1.5*, NC 3.2.5]
3. Summary of quantum mechanics [1.5 lectures]
   (a) Dirac notations, linear algebra formalism **[Self-study+quiz]** [NC 2.1, KLM 2.1-2.6, 2.8]
   (b) Axioms of quantum mechanics: state space, composite systems, evolution, measurements [NC 2.2.1-2.2.5, 2.2.7, KLM 3.1-3.4]
   (c) Composite systems, entanglement, operations on one of two systems, locality of QM [NC 2.2.8-2.2.9]
4. Immediate information processing consequences of quantum mechanics [2 lectures] [NC 1.3]
   (a) No-cloning theorem [NC 1.3.5, box 12.1]
   (b) Non-distinguishability of non-orthogonal states [NC p56-57 (1st ed)]
   (c) Quantum communication protocols, non-signalling, communication bounds
   (d) Superdense coding and teleportation [NC 2.3, 1.3.7, KLM 5.1-5.2, M 6.4-6.5]
   (e) Bell's inequality and nonlocal games [NC 2.6, M 6.6]

Quantum Computation of Classical Problems in Noiseless Systems: [6 lectures]

5. Quantum circuits [1.5 lectures] [NC 4.2-4.3, 4.5-4.5.4, KLM 4.1-4.4]
   (a) Quantum circuit model [KLM 4.1, NC 1.3.4]
   (b) Quantum gates: Bloch sphere, single-qubit gates and entangling gates [NC 4.2-4.3, KLM 4.2]
   (c) Continuous universal sets of quantum gates [reading] [NC 4.5.1-4.5.2, KLM 4.3]
   (d) Quantum gate approximations [NC Box 4.1, KLM 4.3]
   (e) Finite universal sets of quantum gates [NC 4.5.3, KLM 4.3]
   (f) Efficiency and the Kitaev-Solovay Theorem [NC Appendix 3, KLM 4.4]
   (g) Quantum circuits for measurements [KLM 4.5*]
   (h) Hardness of approximating most unitaries [reading] [NC 4.5.4]

6. Quantum computational complexity [reading] [NC 3.2, KLM 9.1]

7. Quantum algorithms [4.5-5 lectures]
   (a) Quantum query complexity: black box model, phase kick back [KLM 9.2*, 6.2*]
   (b) Grover's search algorithm [NC 6.1, KLM 8.1-8.2, M 4]
   (c) Optimality of Grover's algorithm [reading] [NC 6.6]
   (d) Deutsch-Jozsa algorithm [NC 1.4.2-1.4.5, KLM 6.3-6.4, M 2.2]
   (e) Quantum fourier transform (I) [Quiz cut off] [NC 5.1, M 3.5, KLM p110-117]
   (f) Simon's algorithm [M 2.5, KLM 6.5]
   (g) Shor's factoring algorithm: Quantum fourier transform (II), period finding, classical postprocessing and error analysis, order finding, reduction of factoring to order finding, cryptographic consequences. [M 3.1-3.4, 3.7-3.10, NC 5.3, 5.4.1-5.4.2, KLM 7.1.2-7.1.3, 7.3.1-7.3.2, 7.3.4, 7.4]
   (h) Hidden subgroup framework [NC 5.4.3, KLM 7.5]
   (i) Quantum algorithm for simulating quantum physics (Hamiltonian simulation) [NC 4.7]
   (j) Concluding thoughts: quantum advantage and verification

Quiz (required to pass the course) [Feburary 14, 2018. In class. 1 lecture]

Reading week

Quantum Computation in the presence of noise [7-8 lectures]

8. Modelling noise: mixed state formalism of quantum mechanics [2 lectures]
   (a) Most general quantum states: density matrices (noisy quantum data) [NC 2.4, KLM 3.5.1]
   (b) States on a composite system: partial trace and purification, Schmidt composition [NC 8.3.1, 2.5, KLM 3.5.2]
   (c) Most general quantum dynamics: quantum operations / quantum channels: axiomatic approach [NC 8.2, KLM 3.5.3]
   (d) Characterizations: Stinespring's dilation, Kraus representation, Choi representation [NC 8.2]
   (e) Important quantum channels [NC 8.3]
   (f) Most general measurements: POVM measurements [reading] [NC 2.2.6, KLM A8]
   (g) Trace distance, indistinguishability, Holevo-Helstrom's bound [reading] [NC 9.2, KLM A8, Notes*]

9. Combating noise: Quantum error correcting codes (QECC) [2.5 lectures] [NC 10.1-10.3, 10.5, M 5, KLM 10]
   (a) Motivation: applications of QECC (quantum computation, cryptography, physics)
   (b) Classical 3-bit repetition code
   (c) Linear code, parity checks, and syndrome measurements
   (d) Quantum 3-bit repetition code for bit flip errors
   (e) Quantum 9-bit Shor code for any Pauli error
   (f) Correcting a continuous set of errors via discretization

(g) Sufficient condition for QECC (necessary condition [reading])
(h) Stabilizer formalism – parity checks as compatible observables and discretization
(i) Quantum 9-bit Shor code as a stabilizer code
(j) Sufficient condition for QECC for stabilizer codes
(k) Quantum 5-bit code [reading or assignment]
(l) Quantum 7-bit Steane code
(m) Erasure errors, quantum secret sharing, and modeling the AdS/CFT correspondence

10. Getting an accurate computation out of noisy components [2.5-3 lectures] [NC 10.5-10.6]
    (a) Keeping quantum computation discrete !
    (b) Principles of fault-tolerant quantum computation (don't make a mess)
    (c) The threshold theorem (good enough implies arbitrarily good)
    (d) Fault-tolerant logical Pauli operations for stabilizer codes
    (e) Fault-tolerant logical Clifford operations for stabilizer codes
    (f) Encoded Pauli and Clifford operations on the 7-bit code
    (g) Attaining universality: 1-bit teleportation and the $\frac{\pi}{8}$ gate
    (h) Fault-tolerant measurements
    (i) Overhead, assumptions, where things stand, and is any of this realistic?

Quantum Cryptography in the presence of noise and adversary [2.5-3 lectures]

11. Quantum money
12. Quantum bit commitment [Notes*, M 6.3]
13. Quantum key distribution [NC 12.6, M 6.2]
    (a) Encryption
    (b) Classical one-time pad
    (c) Key distribution problem
    (d) QKD through noiseless insecure channels (BB94 and E91)
    (e) QKD through noisys insecure channels (Lo-Chau proof)

Shorthands:

NC: Nielsen and Chuang

KLM: Kaye, Laflamme, Mosca

M: Mermin

*: available on LEARN