Proposed Syllabus for CO681/CS667/PHYS767/AM871 (R. Cleve, 2009)

There are 24 lectures of 75 minutes each. The timing information below is approximate.

1. **Introduction to the quantum information framework** (3 lectures). Qubits, unitary operations, and simple projective measurements. State distinguishing problems. Multi-qubit systems and structure among subsystems. Examples of entangled states. Quantum circuits. Controlled-U and CNOT gates. Superdense coding. Incomplete measurements. Teleportation.

2. **Quantum algorithms and complexity theory** (8 lectures).
   Simulations between quantum and classical circuits. Basic complexity classes: P, BPP, BQP, NP, PSPACE, EXP. Simple algorithms in the query model, such as Deutsch, 1-out-of-4 search, or Deutsch-Jozsa. Simon's problem. Quantum Fourier transform. Eigenvalue estimation problem. Quantum algorithms for order-finding and for integer factoring. Grover's search algorithm. Lower bound for quantum searching.

3. **Density matrices and quantum operations on them** (3 lectures).
   Density matrix formalism: pure states, mixtures of pure states, unitary operations and measurements. Normal matrices, and taxonomy of various kinds of normal matrices. Bloch sphere for qubits. Definition and properties of trace and partial trace. POVMs and completely positive trace preserving maps. Converting between Krauss form and Stinespring form. Definition of separable state.

4. **Distance measures between quantum states** (1 lecture).
   Fidelity and trace distance. Holevo-Helstrom theorem.

5. **Entropy and noiseless coding** (1 lecture).
   Overview of classical entropy and noiseless compression. Quantum entropy. Schumacher's compression.

6. **Error-correcting codes and fault-tolerance** (3 lectures).
   Overview of error-correction in the classical case. Peter Shor's nine-qubit quantum error-correcting code. CSS codes. Brief overview of the threshold theorem for fault-tolerant quantum computation.

7. **Nonlocality** (2 lectures). Examples of Bell inequality violations, such GHZ and CHSH. (Optional: communication complexity, such as the quantum protocol for equality in the simultaneous message passing model using fingerprint states and the swap test.)

8. **Cryptography** (3 lectures).
   Brief overview of classical cryptography: one-time pad and complexity-based cryptosystems. BB84 protocol: how it works, and heuristic discussion of its security. Some formal analysis of security, such as BB84 with single qubit measurements or Lo-Chau cryptosystems.Schmidt decomposition and its application to breaking proposed scheme for bit commitment.