EE214/PHYS220 Quantum Computing

Lecture 1: Introduction

Textbook: N. D. Mermin, Quantum computer science (Cambridge Univ. Press, 2007)
(errata at http://www.lassp.cornell.edu/mermin/errata-1-12-12.pdf);
http://www.lassp.cornell.edu/mermin/qcomp/CS483.html (lecture notes)

Other resources:
http://www.theory.caltech.edu/~preskill/ph219/ (lecture notes, Caltech course)
http://inst.eecs.berkeley.edu/~cs191 (lecture notes, UC Berkeley course)
M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, 2000)
G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information*, Vol. I: Basic Concepts (World Scientific, 2005)

Prospects for Quantum Computing (QC): not really clear

Pessimistic view: never, possibly limited to very small QCs as servers for quantum cryptography networks

Optimistic view: in 20-50 years large-scale QCs, capable of factoring large integers

Very optimistic (overoptimistic): will partially or completely replace general-purpose computers

What QC can do efficiently

1) Factoring large integers (exponential speedup)

Best classical: $\sim \exp[(\log N)^{1/3}]$,

more accurately $\sim \exp\left[\left(\frac{64}{9}\log N\right)^{1/3} (\log\log N)^{2/3}\right]$, log base 2

Quantum: $\sim (\log N)^3$ (Shor's algorithm)

2) Search in unsorted database (quadratic speedup)

Classical: $\sim N$ (simply check all)

Quantum: $\sim \sqrt{N}$ (Grover's algorithm)

3) Simulation of quantum systems (for study of materials, etc.)

4) Possibly something else important (still area of active research)

Current status: numbers 15 and 21 "factored" (also 143 with adiabatic QC)

14 well-entangled qubits (trapped ions, 2011), <25 qubits

quantum algorithms with 9 superconducting qubits (2015),

1,000 D-Wave "qubits"

Truly interdisciplinary effort: physics, engineering, computer science, mathematics

Classical vs. quantum computers

Classical: k bits, 2^k states, only one at a time

Evolution: Universal Turing machine (Alan Turing, 1936)

(Universal Turing machine can simulate any other Turing machine, Church-Turing thesis, complexity theory later)

Quantum: k qubits (called Qbits in Mermin's book)

Simply speaking, all 2^k states simultaneously (so as 2^k classical computers); however, not that simple.

State description: $2 \times 2^k - 2$ real numbers (infinite number of states, a point in 2^k-dimensional Hilbert space)

Example: wavefunction (state) for 3 qubits

$$|\psi\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \ \ldots + \alpha_7 |111\rangle$$

α_i are complex numbers (amplitudes, probability amplitudes, etc.)

$\sum_i |\alpha_i|^2 = 1$, overall phase is not important ($|\psi\rangle \to e^{i\varphi}|\psi\rangle$), so 2 degrees of freedom less, $2 \times 2^k - 2$ real numbers

Quantum case (cont.)

State description (cont.)

Actually, a more complex state description by a "density matrix" is needed in real case (decoherence, lost information, probabilistic description).
Then quantum state corresponds to a trace-one Hermitian matrix with dimension $2^k \times 2^k$ (density matrix), described by $2^{2k} - 1$ real numbers.
For simplicity, we will use the wavefunction description.

Evolution

Instead of Turing machine, change in time of coefficients α_i
(not everything is allowed, only unitary transformations in 2^k-dimensional Hilbert space),

In some sense, similar to 2^k classical computers working in parallel (massive parallelization)

Main caveat: This huge information is a "private property" of the quantum system. If we want to extract any information, we should measure; when measure, we get only one of the states (say, 010): only k bits of information (not 2^k bits).

So, the art of quantum algorithms is to somehow convert information in 2^k degrees of freedom into k useful bits. Sometimes possible (factoring, etc.)

Physical realizations of qubits

Qubit realization: any two-level quantum system
(if more than 2 levels, then can reduce space)

Examples of physical realization

(1) Spin 1/2 as a qubit (most usual example, though not important in practice)

Fixed-length vector is real 3D space, but if measure along any direction, then find it either parallel or antiparallel to this direction.

2 degrees of freedom (angles), $2 \times 2^k - 2 = 2$ for $k = 1$.

Sequential measurements: previous information fully lost.

(2) Polarization of a photon

Measurement by a polarizer: yes or no.

Two degrees of freedom (only one in linear polarization, but actually also a phase in elliptic polarization)

(2') Presence or absence of a photon

Beam splitter, "dual-rail"

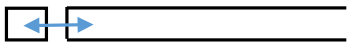
Physical realizations of qubits (cont.)

(3) Two levels of an atom

(4) Semiconductor charge qubit (two quantum dots populated by one electron)

Superposition is most obvious, mathematically the same system as spin

(5) Superconducting charge qubit



1,000,000 or 1,000,001 Cooper pairs on “island”

(6) Superconducting flux qubit

In superconducting loops magnetic flux is quantized, $0, \pm\Phi_0, \pm 2\Phi_0, \ldots, \Phi_0 = \frac{h}{2e}$

With Josephson junctions quantization is not exact, $U(\Phi)$, for double-well potential $U(\Phi)$ we have superposition of different fluxes, i.e. superposition of current going clockwise and counterclockwise.

(7) ”Transmon” qubit

Josephson junction in parallel with a significant capacitance,
slightly anharmonic potential, two lowest levels of a nonlinear oscillator

Main quantum properties used in QC

- Superposition
- Interference (can be negative)
- Entanglement
- Measurement (collapse)

Brief history of Quantum Computing (QC) and Quantum Information (QI)

Late 1920 (1927) development of quantum mechanics

1982 Richard Feynman, difficult to simulate quantum by classical
$\Rightarrow$ need quantum

1982 no-cloning theorem (Wooters-Zurek, Dieks, also Yurke)

1984 Charles Bennett and Gilles Brassard, quantum crtyptography
(actually Stephen Wiesner, late 1960s, paper not accepted)

1985 David Deutsch, Universal quantum computer efficiently simulates arbitrary quantum system, also Deutsch algorithm

1994 Peter Shor, efficient factoring (1995 Kitaev)

1995 Lov Grover, search in unsorted database

1996 Robert Calderbank & Peter Shor, Andrew Steane,
quantum error correction

Since then rapid progress (well funded)

Structure of the course

Overview of quantum mechanics

General structure of a quantum computer, 1-qubit, 2-qubit, and 3-qubit gates

Usual QC protocol for a function calculation and main trick, toy problems (algorithms)

EPR, Bell states, quantum teleportation, quantum cryptography

---

RSA encryption, Shor's algorithm for factoring

Grover algorithm

Quantum error correction

Computational complexity (very briefly)

EE214/PHYS220 Quantum Computing

Lecture 2: Quantum mechanics postulates

Postulate 1. State of a quantum system is represented by a vector in a Hilbert space with the norm ("length") of 1.

number and order of postulates not important

Notation: $|\psi\rangle$ ("ket-vector")

Hilbert space: complete inner-product space

Linear space, can introduce basis, orthonormal basis

In 1D or 3D case $|\psi\rangle \leftrightarrow \psi(x)$ or $\psi(\vec{r})$, so Hilbert space is infinite-dimensional.

In QC much simpler, since Hilbert space is always finite-dimensional.

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ .. \\ .. \\ \alpha_N \end{pmatrix} \qquad |\phi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ .. \\ .. \\ \beta_N \end{pmatrix}$$

α_i , β_i are complex numbers

Inner product is

$$\langle\phi|\psi\rangle = \sum_i \beta_i^* \alpha_i$$

(Dirac notation, bra-ket)

Postulate 1 (cont.)

Different bases are possible (e.g., measurement of spin along different directions)

"Computational basis": $|000\rangle, |001\rangle, |010\rangle, \ldots$

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_7 \end{pmatrix} = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \cdots + \alpha_7|111\rangle$$

superposition $\qquad\qquad \sum_i |\alpha_i|^2 = 1$ (normalization)

Most states are entangled: 1 qubit is characterized by 2 complex numbers, so k separate qubits would be characterized by $2k$ complex numbers, but general k-qubit state is characterized by 2^k complex numbers.

2 qubits, "separable state"

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \underbrace{\alpha\gamma}_{\alpha_{00}}|00\rangle + \underbrace{\alpha\delta}_{\alpha_{01}}|01\rangle + \underbrace{\beta\gamma}_{\alpha_{10}}|10\rangle + \underbrace{\beta\delta}_{\alpha_{11}}|11\rangle$$

We see that $\alpha_{00}\alpha_{11} = \alpha_{10}\alpha_{01}$, while general 2-qubit wavefunction does not satisfy this condition $\Rightarrow$ most states are not separable (i.e., entangled)

Postulate 2

Postulate 2. Measurable quantities (physical magnitudes, dynamical variables, "observables") are represented by Hermitian operators

Hermitian (self-adjoint) operator: $\hat{B}^\dagger = \hat{B}$

for a matrix, Hermitian conjugate is $B^\dagger_{ij} = B^*_{ji}$

Hermitian matrix: $B_{ij} = B^*_{ji}$ (real on diagonal, complex-conjugate off-diagonal)

Properties of Hermitian operators

- Eigenvalues are real
- Eigenvectors form orthonormal basis (somewhat oversimplified), so each observable defines an orthonormal basis, in which its matrix is diagonal (with real elements)

Postulate 3

Postulate 3. Measurement result is necessarily one of eigenvalues of the corresponding operator (no other results possible).

Measurement result r is generally random, with probability $p_r = |\langle\psi_r|\psi\rangle|^2$, where $|\psi\rangle$ is the state before measurement and $|\psi_r\rangle$ is the normalized eigenvector, corresponding to the eigenvalue r.

If spectrum of the measured operator is degenerate (i.e., a subspace corresponds to the eigenvalue r), then we need to choose a basis $|\psi_{r,j}\rangle$ in this subspace, and $p_r = \sum_j |\langle\psi_{r,j}|\psi\rangle|^2$.

Another way to think: $p_r = \| \hat{\mathbb{P}}_r|\psi\rangle \|^2$

where $\hat{\mathbb{P}}_r$ is operator of projection onto subspace, corresponding to the eigenvalue r
and $\| \ldots \|$ denotes norm ("length") of a vector.

Postulate 3 (cont.)

Example

$$|\psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \cdots + \alpha_7|111\rangle$$

Measure all 3 qubits. 8 possible results.

$$\begin{aligned} 0 &\leftrightarrow 000 \leftrightarrow |000\rangle & P_0 &= |\alpha_0|^2 \\ 1 &\leftrightarrow 001 \leftrightarrow |001\rangle & P_1 &= |\alpha_1|^2 \\ 2 &\leftrightarrow 010 \leftrightarrow |010\rangle & P_2 &= |\alpha_2|^2 \\ &\cdots & &\cdots \\ 7 &\leftrightarrow 111 \leftrightarrow |111\rangle & P_7 &= |\alpha_7|^2 \end{aligned}$$

Measured observable

$$\widehat{M} = \begin{pmatrix} 0 & & & & & & & \\ & 1 & & & & & & \\ & & 2 & & & & & \\ & & & 3 & & & & \\ & & & & 4 & & & \\ & & & & & 5 & & \\ & & & & & & 6 & \\ & & & & & & & 7 \end{pmatrix}$$

eigenvalue for corresp. eigenstate (comp.basis)

Now measure only first qubit, results 0 or 1

$$\widehat{M}_1 = \begin{pmatrix} 0 & & & & & & & \\ & 0 & & & & & & \\ & & 0 & & & & & \\ & & & 0 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}$$

eigenvectors: $\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ for 0 $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{pmatrix}$ for 1

Postulate 3 (cont.)

Measure qubits 2 and 3

$$\widehat{M}_2 = \begin{pmatrix} 0 & & & & & & & \\ & 0 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix} \qquad \widehat{M}_3 = \begin{pmatrix} 0 & & & & & & & \\ & 1 & & & & & & \\ & & 0 & & & & & \\ & & & 1 & & & & \\ & & & & 0 & & & \\ & & & & & 1 & & \\ & & & & & & 0 & \\ & & & & & & & 1 \end{pmatrix}$$

$$\widehat{M} = 4\widehat{M}_1 + 2\widehat{M}_2 + \widehat{M}_3$$

8 eigenvalues: 0, 1, .. 7

Postulate 3’

Postulate 3’. Average (“expectation”) value for measuring operator $\hat{B}$ is $\langle \hat{B} \rangle = \langle \psi | \hat{B} | \psi \rangle$.

Follows from postulate 3, but often a separate postulate

Important in standard quantum mechanics, but not important for QC (except NMR)

$$\langle \psi | \hat{B} | \psi \rangle = (\alpha_0^* \; \alpha_1^* \; .. \; \alpha_N^*) \begin{pmatrix} b_{00} & & \\ & b_{ij} & \\ & & b_{NN} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ .. \\ \alpha_N \end{pmatrix}$$

$$\langle \psi | \hat{B} | \psi \rangle = \langle \psi | \; (\hat{B} | \psi \rangle) = (\langle \psi | \hat{B}) \; | \psi \rangle$$

Proof

$\hat{B} = \sum_r r \, \hat{\mathbb{P}}_r$ (since Hermitian)

$$\langle \psi | \hat{B} | \psi \rangle = \sum_r r \, \langle \psi | \, \hat{\mathbb{P}}_r | \psi \rangle = \sum_r r \, \langle \psi | \, \hat{\mathbb{P}}_r \, \hat{\mathbb{P}}_r | \psi \rangle = \sum_r r \, \| \, \hat{\mathbb{P}}_r | \psi \rangle \|^2 = \sum_r r \, p_r$$

QED

Postulate 4

Postulate 4. After measurement of $\hat{B}$ with result r, the state abruptly changes:

$$|\psi\rangle \to \frac{\hat{\mathbb{P}}|\psi\rangle}{\| \hat{\mathbb{P}}|\psi\rangle \|}$$ (projected onto subspace and normalized)

Called wavefunction collapse

Examples

$$|\psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \cdots + \alpha_7|111\rangle$$

(a) Measure all qubits, get result $3 = 011$, then $|\psi\rangle \to |011\rangle$

(Does not matter what was before!
Cannot get more information on α_i.)

(b) Measure only first qubit, get result 0, then

$$|\psi\rangle \to \frac{\alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle}{\sqrt{|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2}}$$

Postulate 4 (cont.)

Remark

We consider the simplest case: "orthodox" measurement ("projective" measurement); this is essentially common sense

More general: "generalized" measurements (POVM, incomplete, partial, weak, continuous, etc.)

Idea: do not know result exactly, partial information $\rightarrow$ partial collapse

Techniques of measurement operators (arbitrary linear operator, replacing projectors $\hat{\mathbb{P}}_r$), quantum trajectory, Bayesian formalism

Will not use in this course because:

- more difficult
- generalized measurement can be reduced to orthodox measurement in an extended Hilbert space (indirect meas.)

Postulate 5

Postulate 5. Evolution of a quantum state is described by

the Schrödinger equation $\frac{d|\psi\rangle}{dt} = -\frac{i}{\hbar}\hat{H}|\psi\rangle$,

where $\hat{H}$ is the operator of energy (Hamiltonian)

We will not really use it, but important that evolution is described by a unitary operator

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar}\hat{H}t}|\psi(0)\rangle = \hat{U}\,|\psi(0)\rangle$$

Since $\hat{H}$ is Hermitian, $\hat{U}$ is unitary, $\hat{U}^\dagger = \hat{U}^{-1}$ $\qquad$ $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{1}$

A unitary operator preserves inner product

$$\langle(\hat{U}\phi)|(\hat{U}\psi)\rangle = \langle\phi|\,\hat{U}^\dagger\hat{U}\psi\rangle = \langle\phi|\psi\rangle$$

Unitary operator transforms an orthonormal basis into an orthonormal basis (rotation of a space)

Quantum computer operation

Evolution in a quantum computer (quantum gates) is described by unitary operators

A quantum computer consists of unitary gates (usually one-qubit and two-qubit gates) and measurement stages

Can be only one measurement at the very end, but for error correction should also be many measurement steps during operation