Lecture 5: Review of quantum computing
Reading: Kaye Chap 4. Nielsen and Chuang Chap 4.

These topics are also very well covered in the referenced texts so I will just summarize the key points as before.

1 Quantum circuit model

1.1 Generalities

- Logical qubits are represented as wires, boxes are quantum gates (unitary operators)
- A general circuit inputs a density operator in a system register and some ancilla qubits, applies operations to the system and ancillae, and leaves the register in a different state, most generally as $\sum_i A_i \rho_{in} A_i^\dagger$, where A_i are Kraus operators.
- Measurement results in a classical label i and leaves the system in the corresponding state.
- 1-qubit quantum gate U rotates a state, represented by a point in or on the Bloch sphere.
- General rotation gates are formed exponential maps of Pauli gates as discussed previously. Explicit expressions are given in the texts.
- Any 1-qubit unitary can be represented as $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$ where α, β, γ, and δ are real numbers specifying rotation angles. This decomposition can be generalized to any two non-parallel axes l and m.
- A corollary is that U can be decomposed as $U = e^{i\alpha} AXBXC$, with $ABC = I$.
- Controlled U gates are two-qubit gates that apply U if a control is $|1\rangle$ and otherwise do nothing. It can be represented as $c - U = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes U$.
- Controlled U gates followed by measurement is equivalent to classically controlling the gates.
- A 2-qubit gate is defined to be an entangling gate if the input is a product state but the output is not.
- A universal gate set is on for which any n qubit operator can be approximated to arbitrary accuracy by only gates from that set.
- A gate set consisting of any 2-qubit entangling gate and all 1-qubit gates is universal.
- The above set is infinite. A finite universal set of gates is CNOT, H, T.
- Solovay-Kitaev theorem (loosely): Any 1-qubit gate can be implemented with polylog number of gates from the universal set.

1.2 Measurement

A general measurement operator is specified as M_m. Given a state $|\psi\rangle$, the probability to measure label m is $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. A special case of measurement is a projective measurement for which $P_m = P_m^\dagger$ and $P_m^2 = P_m$. In that case we get the familiar measurement postulate from your favorite QM textbook.

A von Neumann measurement is a further special case that all projectors have rank one. Say we have an orthonormal basis $|\phi_j\rangle$ so that $|\psi\rangle = \sum_j \alpha_j |\psi_j\rangle$. A von Neumann measurement uses orthogonal projectors $|\phi_j\rangle\langle\phi_j|$ applied to the quantum state. The probability to get eigenvalue j is $Tr(|\phi_j\rangle\langle\phi_j| |\psi\rangle\langle\psi| = |\alpha_j|^2$.

1.3 Quantum algorithms

- Difference between classical probabilistic and quantum algorithms
- Some quantum circuits can be efficiently simulated on classical computers (Gottesman-Knill Theorem). This group is the Clifford group consisting of CNOT, H, $\pi/2$ phase gates (search for the CHP package by Scott Aaronson).
- Phase kick-back: say we have a control and target register and the target is initialized in the eigenvector of some unitary. Putting the control in $|+\rangle$ by a Hadamard gate and applying $c - U$ will yield the eigenvector and the eigenvalue (which is in general a complex phase), which can then be associated with control register. Since this phase is only generated if U is applied, only $|1\rangle$ gets the phase, and there is now a relative phase between $|0\rangle$ and $|1\rangle$ in the control register. This phase can be determined by applying H again on the control. This idea is the key one underlying many quantum algorithms.
- Deutsch algorithm, Deutsch-Josza algorithm
- Phase estimation, quantum Fourier transform