Lecture 19: How to Build Your Own Quantum Computer

Guest Lecturer: Isaac Chuang
Scribed by: Fen Zhao

Department of Mathematics, MIT

November 13, 2003

1 The DiVicenzo Criteria

The DiVicenzo Criteria list four things required for quantum computing: robust qubits, a universal gate set, a fiducial input state, and projective measurements.

1.1 Robust Qubits

A quantum qubit is based on 2 level quantum systems. One must also remember that a tensor product Hilbert space is needed; for example a harmonic oscillator is not a tensor product space and therefore makes a bad quantum computer. In general, a two level atom would make a good quantum computer.

One must also have a long coherence time. This is characterizes how the environment interacts with your ideal qubit system. The imperfect qubit system will have many states besides the two you are interested in. One can think of decoherence as the effects of all the interactions outside your idea set of interactions.

$$|\Psi(t)\rangle = e^{-iHt}|\Psi(0)\rangle$$

$$H = \begin{bmatrix} \mathbf{a} & \mathbf{b} & g & \cdots \\ \mathbf{c} & \mathbf{d} & h & \\ e & f & i & \\ \vdots & & & \ddots \end{bmatrix}$$

In the Hamiltonian above, the elements in bold represent the your ideal set of interactions, and everything else is the non-ideal part that causes decoherence.

There are many sources of decoherence. Gravity causes decoherence if one states weights more thant the other. There may be stray long range fields, typically associated with charge. There can be leakage into larger Hilbert spaces; a two state atom may have higher energy levels that the state can move to. However, there does exists true finite spaces in nature, such as spin.

There are two measurements of decoherence, T_1 and T_2. T_1 is called the "longitudinal coherence time," or the "spin lattice time," or the "spontaneous emission time," or the"amplitude damping." It measures the loss of energy from the system. One can do an experiment to determine T_1. First

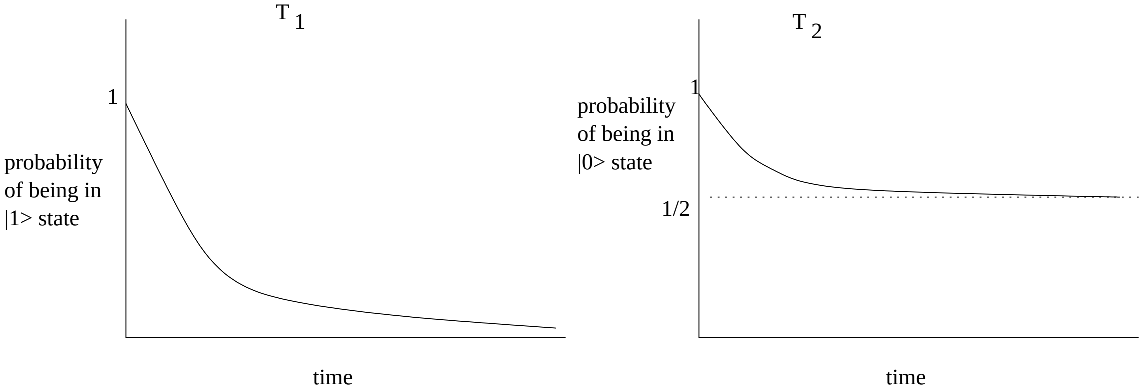

Figure 1: expected results for experiments for T_1 and T_2

initialize the qubit to the ground state $|0\rangle$. Then apply $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, and wait for time t and measure the probability of being in the $|1\rangle$ state. We expect an exponential decay e^{-t/T_i}.

T_2 is called the "transverse coherence time," or the "spin-spin relaxation time," or the "phase coherence time," or the "elastic scattering time," or the "phase damping." One can do an experiment to determine T_2. First initialize the qubit to the ground state $|0\rangle$. Then apply the Hadamard transform H to get the state to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, wait for time t, apply H again, and measure the probability of being in the $|0\rangle$ state. We expect that the measurement goes to 1/2 after a long time because after a long time, most likely something popped the state into either $|0\rangle$ or $|1\rangle$ state, which after the H transform sends the state to $\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$.

In general $T_1 > T_2$.

1.2 Universal Gate Sets

There are many different universal gate sets. We have seen that CNOT and single qubit gates form a universal gate set. CNOT, the Hadamard gate, and $\pi/8$ gate is another universal gate set.

In practice experimentalists use controlled Hamiltonians that they turn on and off for certain time intervals.

$$H = H_{sys} + P_1(t)X + P_2(t)Y...$$

For example, for an NMR setup, we may have

$$H = \frac{\pi\hbar}{2} J\sigma_z \otimes \sigma_z + P_1(t)I \otimes \sigma_x + P_2(t)I \otimes \sigma_y...$$

In the real world, there is no such thing as time dependent Hamiltonians. So how do we perform a sequence of operations? It is a just an approximation; fundemantally we will always have decoherence and will need fault tolerance.

What happens is that our classical controls are actually quantum systems, and we must take into action the back action of the control system on our system. $P_1(t)X$ is just an approximation; in reality, we have a Jaynes-Cumming type interaction Hamiltonian:

$$H = \hbar\omega N + \delta Z + g(a^\dagger \sigma_- + a_+^\sigma)$$

where $\sigma_\mp = \frac{X \pm Y}{2}$. In less abstract terms, there is decoherence that results after a photon interacts with a qubit because the photon will carry away information about the state of the qubit.

2 Implementations

In general, the challenge of quantum computing lies in the fact that quantum systems have short lifetimes, and that we need to control it externally.

System	T (sec)
NMR	10^2 to 10^8
Ion Trap	10^{-3}
Dots	10^{-6}
Microwave Cavity	10^0
Optical Cavity	10^{-5}

Table 1: Some relaxation times for different implementations

2.1 Cavity QED

The Hamiltonian is described by atom, photon, and atom-photon interactions. The qubit is the single photon. Gates for $\pi/8$ and Hadamard are implemented by beam splitter and the like. Turchette managed to achieve a control Z gate.

2.2 Ion Trap

The Hamiltonian is described by spin, photon-phonon (vibrational mode) atom-photon-phonon interactions. The qubit is the atom (spin) and the phonon. The Deutsch-Joza algorithm has been implemented with ion traps. The system has a lifetime of $O(1-100)$ (order of) milliseconds. Pulsed lasers are the universal gate set. The challenge is to get a stable $O(10)$ Hz laser and cooling the ions to absolute zero.

2.3 NMR

The Hamiltonian is described by spins, spin-spin, and external control photon interactions. The spins interact with chemical bonds. The gates are implemented by radio frequency magnetic field pulses. Factoring with 6 qubits has been accomplished. In terms of robustness, ^1H, ^{13}C, ^9F, ^{14}N has coherence times of $O(1)$ seconds.

2.4 All Silicon Quantum Computer

This implementation implants individual atoms into silicon surrounding and controls the atom electronically. It has a coherence of 100 ms at $T = 9.2K$. This implementation is scalable and uses current techniques of classical computer engineering.

3 Quantum Cryptography

Currently two companies make quantum cryptography systems. The purpose of quantum cryptography is to make it more likely to detect an eavesdropper. They are based on the fact that an eavesdropper measuring a quantum system transmitted will collapse the system.

We can relate various techniques of quantum computing to features of it's implementation. Data compression is related to cooling. Error correction is related to control and T_1 and T_2. Noisy coding is related to precision of measurements. Cryptography is related to entanglement and non-locality.