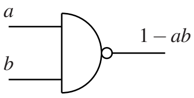
Universal gate sets, Schrödinger Equation, Quantum Teleportation 9/9/03
C/CS/Phys 191 Fall 2003 Lecture 5

1 Universal Gate Sets

1.1 Classical

The NAND gate is universal for classical computation.



For any boolean function $\{0,1\}^n \longrightarrow \{0,1\}$, there is a circuit built of NAND gates (possibly with fan-out) for that function. However the circuit may require an exponential number 2^n of gates. Functions which can be efficiently evaluated require only a polynomial number n^c gates. The distinction between functions which require exponentially large circuits and those which can be computed with polynomial-size circuits does not depend on the chosen set of gates.

1.2 Quantum

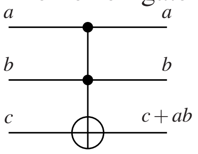
A set G of quantum gates is called universal if for any $\varepsilon > 0$ and any unitary matrix U on n qubits, there is a sequence of gates $g_1, \ldots, g_l$ from G such that $\|U - U_{g_l} \cdots U_{g_2} U_{g_1}\| \leq \varepsilon$.

Here U_g is $V \otimes I$, where V is the unitary transformation on k qubits operated on by the quantum gate g, and I is the identity acting on the remaining $n-k$ qubits. The operator norm is defined by $\|U - U'\| = \max_{|v\rangle \text{unit vector}} \|(U - U')|v\rangle\|$.

Examples of universal gate sets include

- CNOT and all single qubit gates
- CNOT, Hadamard, and suitable phase flips
- Toffoli and Hadamard

The Toffoli gate is a three-qubit gate which complements the third bit iff the first two control bits are each 1.



An n-qubit gate U (a $2^n \times 2^n$ unitary matrix) has exponentially many parameters. So typically in general we need $\exp(n)$ many gates to even approximate U.

The Solovay-Kitaev theorem says that, as a function of ε, the complexity of an approximation is only $\log^2 \frac{1}{\varepsilon}$. This is rather efficient – the complexity as a function of n is the problem.

Quantum computation may be regarded as the study of those unitary transformations on n qubits that can be described by a sequence of polynomial in n quantum gates from a universal family of gates. U is "easy" (implementable) if $U \approx U_{g_k} \cdots U_{g_1}$ for $k = O(\text{poly}(n))$. This definition doesn't depend on our choice of a (finite) universal gate family, since any particular gate in one gate family can be well-approximated with a constant number of gates from another universal gate family. The constant factor does not affect the distinction between polynomial- and exponential-size circuits.

2 Schrödinger's Equation

Shrödinger's equation is the equation of motion which describes the evolution in time of the quantum state.

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi\rangle \quad .$$

Here $\hbar$ is a constant (called Planck's constant – we'll usually assume $\hbar = 1$), and H is a linear *Hamiltonian* which is Hermitian, $H^\dagger = H$. Equivalently, H has an orthonormal set of eigenvectors $|\psi_i\rangle$, all with real eigenvalues λ_i: $H|\phi_i\rangle = \lambda_i|\phi_i\rangle$.

For those of you who are familiar with Shrödinger's equation, the unitarity restriction on quantum gates is simply the time-discrete version of the restriction that the Hamiltonian is Hermitian.

We will now prove that if the system satisfies Shrödinger's equation, then its evolution in discrete time is described by unitary operations. (We will assume that H is time independent.)

Write $|\psi(t)\rangle$ in the basis of eigenvectors of H:

$$|\psi(t)\rangle = \sum_j a_i(t)|\phi_j\rangle$$

$$\Downarrow$$

$$i\hbar \frac{d\Sigma a_j|\phi_j\rangle}{dt} = H\Sigma a_j|\phi_j\rangle = \Sigma a_j\lambda_j|\phi_j\rangle$$

$$\Downarrow$$

$$i\hbar \frac{da_j}{dt} = \lambda_j a_j$$

$$\Downarrow$$

$$a_j(t) = e^{-\frac{i}{\hbar}\lambda_j t} a_j(0)$$

$$\Downarrow$$

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar}\lambda_j t} a_j(0)|\phi_j\rangle$$

We get that the change after a discrete time difference is unitary:

$$|\psi(t)\rangle = \begin{pmatrix} e^{-\frac{i}{\hbar}\lambda_1 t} & & 0 \\ & \cdot & \\ & & \cdot \\ 0 & & e^{-\frac{i}{\hbar}\lambda_d t} \end{pmatrix} \begin{pmatrix} a_0 \\ \cdot \\ \cdot \\ a_d \end{pmatrix} = U(t)|\psi(0)\rangle$$

In this basis, $U(t)$ is diagonal.

3 Quantum Teleportation

The *No Cloning Theorem* states that no quantum system can copy a qubit; that is, there is no transform sending $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$. However, if we are willing to destroy the original, we can transmit a qubit, even to a remote location.

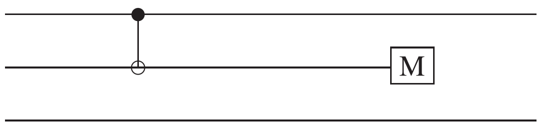
Suppose Alice (A) has access to a quantum state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, which she wants to transmit to a remote party Bob (B). She can accomplish this by transmitting only classical bits of information, provided A and B share the entangled two-qubit state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The technique is known as *quantum teleportation*.

The basic idea is this. A controls $|\psi\rangle$ and the first qubit of $|\phi\rangle$. A's strategy, roughly speaking, is to forcibly entangle $|\psi\rangle$ with the first qubit $|\phi\rangle$. A then measures the first qubit of $|\phi\rangle$, resolving it completely, and hopes this will cause $|\psi\rangle$ to become entangled with the *second* qubit of $|\phi\rangle$. Presumably, B could then transfer $|\psi\rangle$ to the second qubit of $|\phi\rangle$.

As a first try, consider the following diagram. The top line represents $|\psi\rangle$; the bottom two represent the two qubits of $|\phi\rangle$.



That is, A passes $|\psi\rangle$ and the first qubit of $|\phi\rangle$ through a CNOT gate, and then measures the first qubit of $|\phi\rangle$. Now the input into the system as a whole is

$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i|i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}}|j,j\rangle.$$

After passing through the CNOT gate this becomes

$$\sum_{i,j} a_i \big|i, i \oplus j, j\big\rangle.$$

Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j$. The state is now

$$\sum_{j} a_{j\oplus l} \big|j \oplus l, j\big\rangle.$$

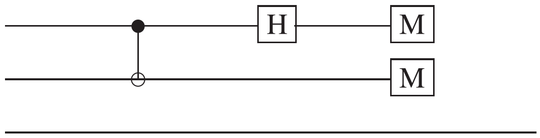
Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Thus we have

$$\sum_{j} a_{j\oplus l} \big|j \oplus l, j \oplus l\big\rangle = \sum_{j} a_j \big|j, j\big\rangle.$$

This is almost exactly what we want. The only problem is that now, the qubit corresponding to $|\psi\rangle$ is entangled with B's qubit. The entanglement that was necessary to get the whole process started is now a liability. One way to disentangle them would be for A to measure her remaining qubit. But this would destroy B's qubit as well.

The ideal solution would be to send the entangle qubits through a CNOT gate—but A controls the first qubit and B controls the second. This would require quantum communication between A and B, which is prohibited.

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now induces the transformation

$$\sum_j a_j |j,j\rangle \longrightarrow \frac{1}{\sqrt{2}} \sum_{ij} a_j (-1)^{ij} |i,j\rangle.$$

Finally A measures i and sends the measurement to B. The state is now:

$$\sum_j a_j (-1)^{ij} |j\rangle.$$

If $i = 0$ then we are done; if $i = 1$ then B applies a phase flip. In either case the state is now $a_0|0\rangle + a_1|1\rangle$.

So A has transported the quantum state to B simply by sending two classical bits.