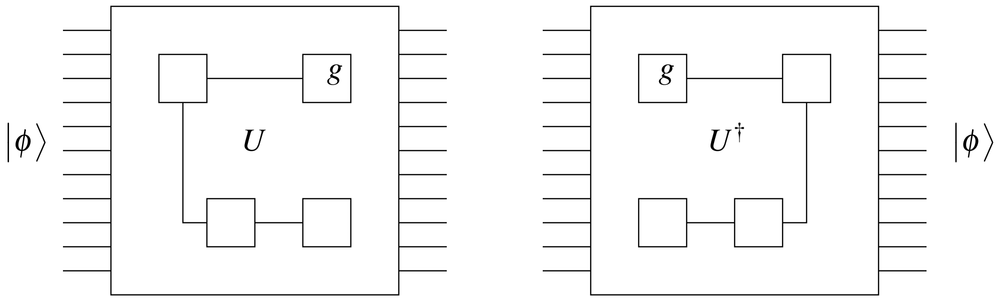
CS 294-2 **BQP vs. P, BPP, Accuracy** 9/14/04
Fall 2004 Lecture 5

1 Reversible Computation

Quantum computation is unitary. A quantum circuit corresponds to a unitary operator U acting on n qubits. Being unitary means $UU^\dagger = U^\dagger U = I$. A quantum circuit which performs a unitary operation U has a mirror image circuit which performs the corresponding operation $U^\dagger$.



The circuits for U and $U^\dagger$ are the same size and have mirror image gates. Examples:

$$\begin{aligned} H &= H^\dagger \\ \text{CNOT} &= \text{CNOT}^\dagger \\ R_\theta &= R^\dagger_{-\theta} \end{aligned}$$

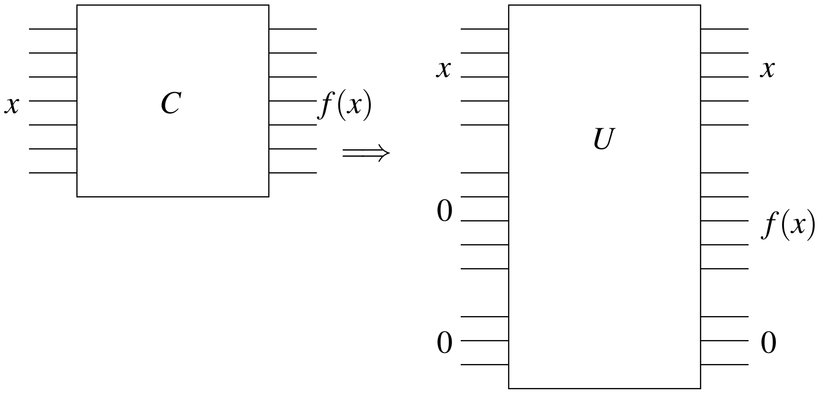
2 P $\subseteq$ BQP

We will show how any classical computation can be simulated by a quantum circuit and then show the specific result that P is contained in BQP.

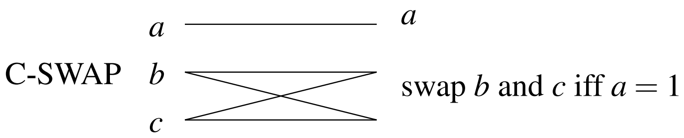
2.1 Simulating Classical Circuits

Quantum computation originally (in the late 70s and early 80s) tried to understand whether unitary constraint on quantum evolution provided limits beyond those explored in classical computation. A unitary transformation taking basis states to basis states must be a permutation. (Indeed, if $U|x\rangle = |u\rangle$ and $U|y\rangle = |u\rangle$, then $|x\rangle = U^{-1}|u\rangle = |y\rangle$.) Therefore quantum mechanics imposes the constraint that classically it must be reversible computation.

How can a classical circuit C which takes an n bit input x and computes $f(x)$ be made into a reversible quantum circuit that computes the same function? We can never lose any information, so in general the circuit must output both the input x and the output $f(x)$. In addition, the quantum circuit may need some additional scratch qubits during the computation since individual gates can't lose any information either. The consequence of these constraints is illustrated below.



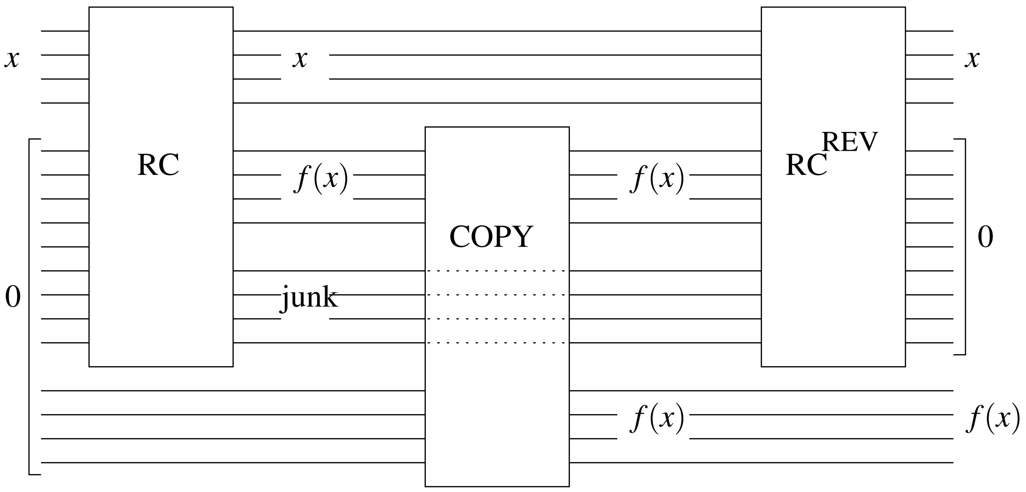
How is this done? Recall that any classical AND and OR gates can be simulated with a C-SWAP gate and some scratch $|0\rangle$ qubits.



If we construct the corresponding reversible circuit RC, we have a small problem. The CSWAP gates end up converting input scratch bits to garbage. How do we restore the scratch bits to 0 on output? We use the fact that RC is a reversible circuit. The sequence of steps for the overall circuit is

$$(x, 0^k, 0^m, 0^k, 1) \xrightarrow{C'} (x, y, \text{garbage}_x, 0^k, 1) \xrightarrow{\text{copy } y} (x, y, \text{garbage}_x, y, 1) \xrightarrow{(C')^{-1}} (x, 0^k, 0^m, y, 1) \ .$$

Overall, this gives us a clean reversible circuit $\hat{C}$ corresponding to C.



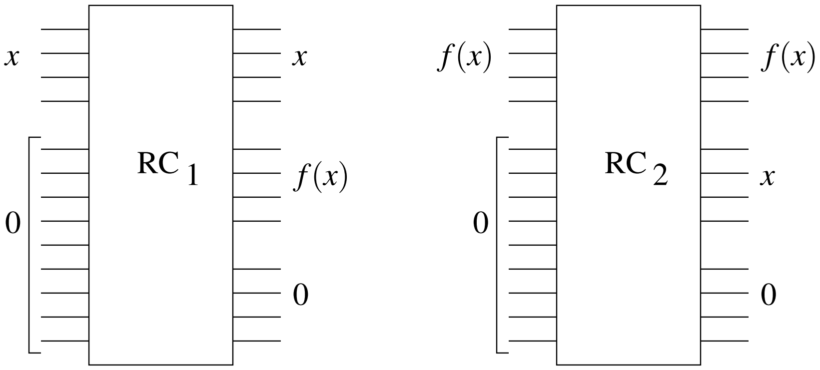
2.2 Proof: P $\subseteq$ BQP

Define a *simple circuit* as a reversible circuit which takes as input x and outputs $f(x)$ and does not generate a copy of x on the output as previously described. Also, roughly define an efficient circuit as one with a small number of total gates.

Theorem 5.1: *There exists a simple circuit for f if and only if f is a bijection and there are efficient circuits for f and f^{-1}.*

Proof:If there is a simple circuit for f, then running that circuit in reverse will compute $f^{-1}(x)$ without knowledge of x. Each y has a unique pre-image under f, thus f is a bijection.

To prove the converse, assume that f is a bijection. An efficient circuit for f implies the existence of an efficient reversible circuit RC_1 which computes $f(x)$. An efficient circuit for f^{-1} implies the existence of an efficient reversible circuit RC_2 which computes $f^{-1}(x)$.



The concatenation RC_1 followed by $\mathrm{RC}_2^{\mathrm{REV}}$ is the desired simple circuit.

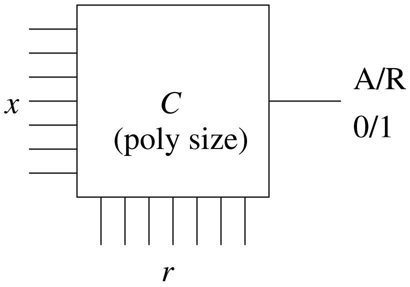
A direct consequence of this theorem is that any polynomial time circuit can be simulated quantumly.

3 BPP ⊆ BQP

We will show that any circuit in BPP can be simulated in BQP by first generating random qubits and then simulating the corresponding polynomial circuit.

3.1 Review: BPP

BPP stands for bounded error probabilistic polynomial time. As an example, consider the language PRIMES consisting of prime numbers. There exists a polynomial size circuit C which takes as input x and some random bits r and outputs 1 for ACCEPT and 0 for REJECT.

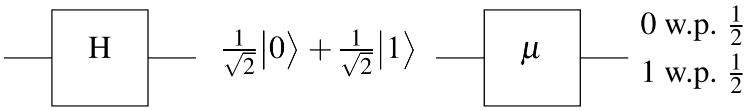


We say PRIMES ∈ BPP if

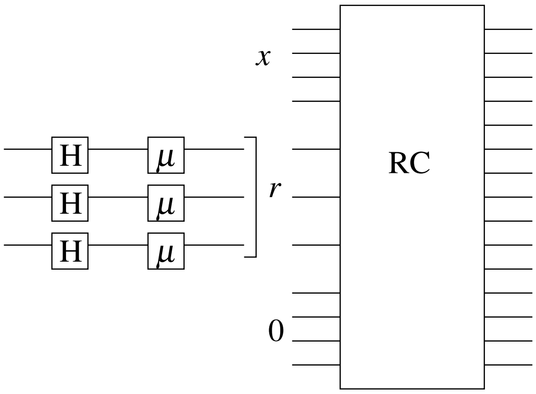
$$\begin{aligned} x \in \text{PRIMES} &\Rightarrow \Pr\{C(x,r)=1\} \geq 2/3, \\ x \notin \text{PRIMES} &\Rightarrow \Pr\{C(x,r)=0\} \geq 2/3. \end{aligned}$$

3.2 Simulating BPP

The main difference between a P circuit and a BPP circuit is the additional input of r random bits. We have already shown that any circuit in P can be simulated in BQP. We want to show that it is possible to generate random qubits from $|0\rangle$ inputs. A simple solution is to apply the Hadamard gate to each $|0\rangle$ and then measure. The Hadamard gate converts $|0\rangle$ to $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Measuring will result is either $|0\rangle$ or $|1\rangle$ with equal probability.



If we generate random bits like this and then run the corresponding quantum circuit to C, we get the straightforward circuit below.



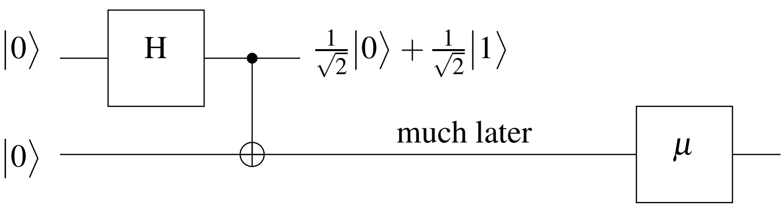
Measurement can be tricky in the intermediate stages of a quantum circuit. Why not skip the measurement and get a superposition of states? Well, if a Hadamard gate occurs in the circuit, we have a problem. The desired outcome is one of these two possibilities with probability $1/2$:

$$|0\rangle \longrightarrow \boxed{\mathrm{H}} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|1\rangle \longrightarrow \boxed{\mathrm{H}} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

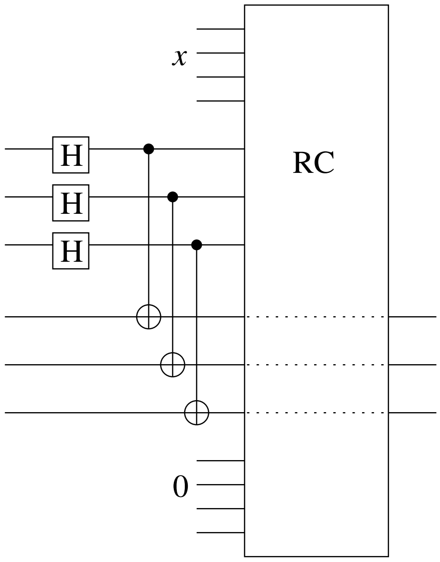
No interference occurs here. Unfortunately, interference can lead to the following undesirable situation in which the randomness disappears:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)\longrightarrow \boxed{\mathrm{H}} \longrightarrow |0\rangle$$

Measurement prevents quantum interference. But, by the principle of deferred measurement, we can postpone the measurement and get the same result. In fact, we can post the measurement indefinitely and not perform it at all.



We now need twice as many qubits as before. Half of them are passed through Hadamard gates and connected by CNOT gates to the other half. This fixes the first half of the qubits to either $|0\rangle$ or $|1\rangle$, even though no measurement was made. It is important to note, however, that since the second half of the qubits are now entangled with the first half, we must be certain not to make any measurements on them either.



4 Is Quantum Computation Digital?

There is an issue as to whether or not quantum computing is digital. We need only look at simple gates such as the Hadamard gate or a rotation gate to find real values.

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

When we implement a gate, how accurate does it need to be? Do we need infinite precision to build this gate properly? A paper by Shamir, "How To Factor On Your Calculator," shows that if we assume infinite precision arithmetic, then some NP complete problems can be solved in polynomial time. However, we obviously cannot have infinite precision, so we must digitize quantum computation in order to approximate values such as $1/\sqrt{2}$. It turns out that $\log n$ bits of precision are necessary.

Suppose we want to build a gate that rotates the input by θ, but the best accuracy we can actually build is rotation by $\theta \pm \Delta\theta$ (finite precision). Let $U_1, \ldots, U_m$ be a set of ideal gates that implement an exact rotation by θ. Let $V_1, \ldots, V_m$ be a set of actual (constructible) gates that implement rotation by $\theta \pm \Delta\theta$. Let $|\phi\rangle$ be the initial state. Let $|\psi\rangle$ be the ideal output

$$|\psi\rangle = U_1 U_2 \cdots U_m |\phi\rangle,$$

and let $|\psi'\rangle$ be the actual output

$$|\psi'\rangle = V_1 V_2 \cdots V_m |\phi\rangle.$$

The closer $|\psi\rangle$ and $|\psi'\rangle$ are to each other, the better the approximation. If we can approximate each gate to within $\varepsilon = O(1/m)$, then we can approximate the entire circuit with small constant error.

Theorem 5.2: *If $\|U_i - V_i\| \leq \frac{\varepsilon}{4m}$ for $1 \leq i \leq m$, then $\| |\psi\rangle - |\psi'\rangle \| \leq \frac{\varepsilon}{4}$.*

Proof:Consider the two hybrid states

$$\begin{aligned} |\psi_k\rangle &= U_1 \cdots U_{k-1} V_k \cdots V_m |\phi\rangle \quad \text{, and} \\ |\psi_{k+1}\rangle &= U_1 \cdots U_k V_{k+1} \cdots V_m |\phi\rangle. \end{aligned}$$

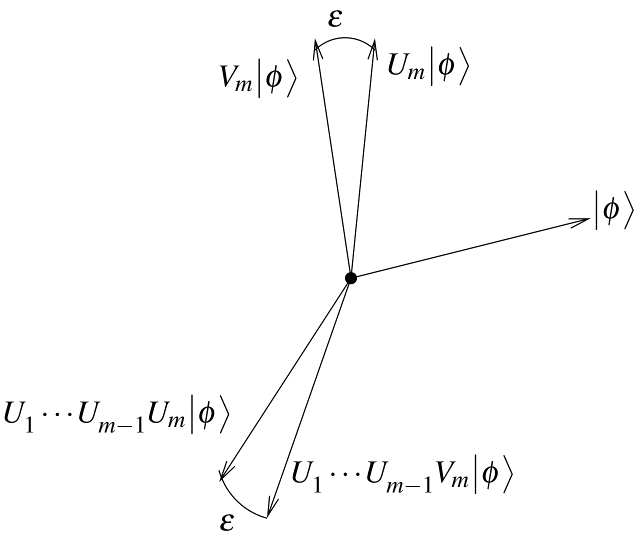
Subtract ϕ_{k+1} from ϕ_k to get

$$\left|\phi_k\right\rangle - \left|\phi_{k+1}\right\rangle = U_1 \cdots U_{k-1}(V_k - U_k)V_{k+1} \cdots V_m\left|\phi\right\rangle$$

Since the unitary transformations don't change the norm of the vector, the only term we need to consider is $U_{k+1} - V_{k+1}$. But we have an upper bound on this, so we can conclude that

$$\|\left|\psi_k\right\rangle - \left|\psi_{k+1}\right\rangle\| \leq \frac{\varepsilon}{4m}.$$

Another way to see this is the following picture. Applying unitary transformations to $U_m\left|\phi\right\rangle$ and $V_m\left|\phi\right\rangle$ preserves the angle between them, which is defined to be the norm.



We use the triangle inequality to finish to proof.

$$\begin{aligned}
\|\left|\psi\right\rangle - \left|\psi'\right\rangle\| &= \|\left|\psi_0\right\rangle - \left|\psi_m\right\rangle\| \\
&\leq \sum_{i=0}^{m-1} \|\left|\phi_i\right\rangle - \left|\phi_{i+1}\right\rangle\| \\
&\leq m \cdot \frac{\varepsilon}{4m} \leq \frac{\varepsilon}{4}.
\end{aligned}$$