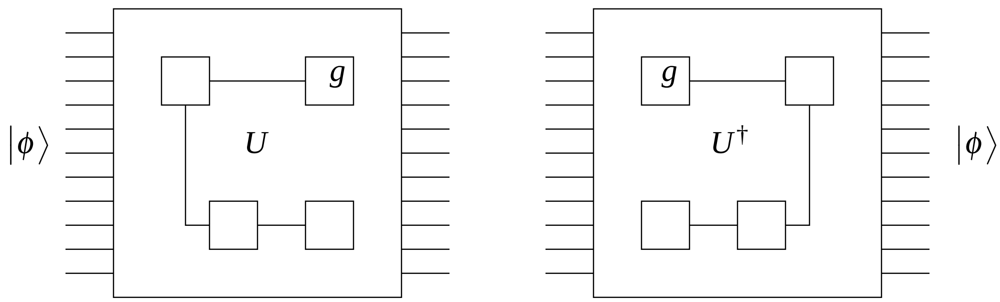
1 Reversible Computation

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 $U^\dagger$.



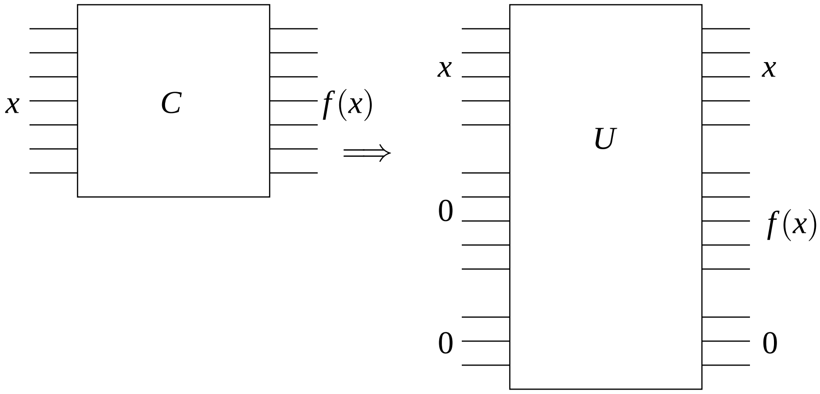
The circuits for U and $U^\dagger$ are the same size and have mirror image gates. Examples:

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

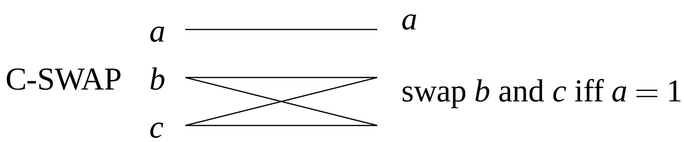
2 Simulating Classical Circuits

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.



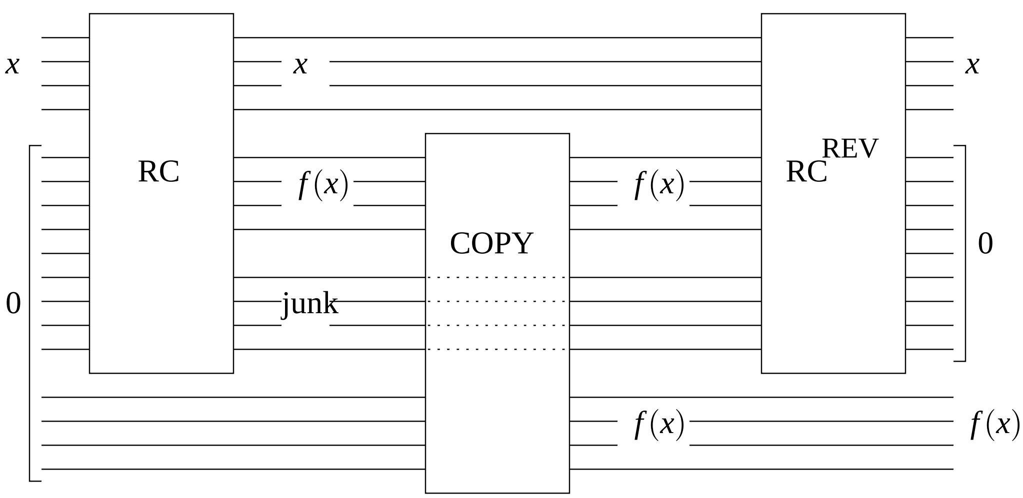
How is this done? Recall that any classical AND and OR gates can be simulated with a C-SWAP gate and some scratch $|0\rangle$ qubits.



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.



3 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 4.1: *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

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

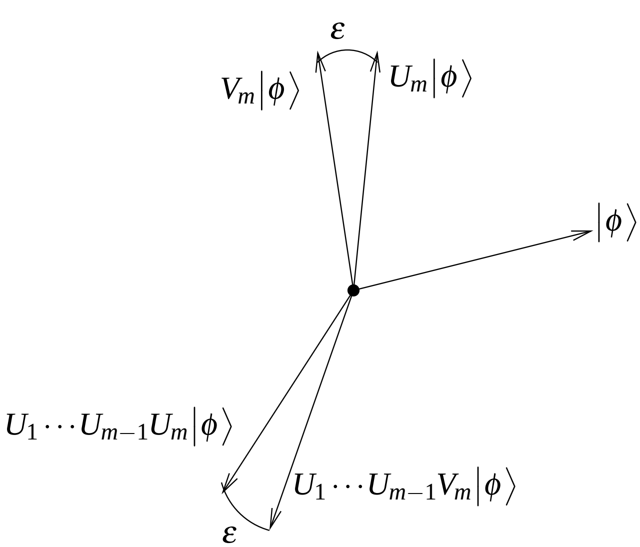
Subtract ϕ_{k+1} from ϕ_k to get

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

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

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

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



We use the triangle inequality to finish to proof.

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