WiDS QRL - Quantum Circuits

Nilabha Saha

January 2023

1 Quantum States and Qubits

1.1 Representing Qubit States

A *qubit* can exist in two mutually exclusive states represented by two orthonormal vectors $|0\rangle$ and $|1\rangle$.

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Upon measuring in the *computational basis*, a qubit in state $|0\rangle$ always outputs 0 and a qubit in state $|1\rangle$ always outputs 1.
A qubit's *statevector* can be represented as

$$|q\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

The probability of measuring a state $|\psi\rangle$ to be in the state $|x\rangle$ is given by

$$p(|x\rangle) = |\langle x|\psi\rangle|^2$$

Since probabilities add upto to 1, we must have the statevector to be *normalised*, $\langle\psi|\psi\rangle = 1$. Thus, if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then we must have that $|\alpha|^2 + |\beta|^2 = 1$.
Any overall factor γ on a state for which $|\gamma| = 1$ is referred to as *global phase*. States that differ only by a global phase are physically indistinguishable:

$$|\langle x|\gamma|\alpha\rangle|^2 = |\gamma\langle x|\alpha\rangle|^2 = |\langle x|\alpha\rangle|^2$$

Upon making a measurement, the state of the qubit collapses to the measured value. This is called the *observer effect*.
The general state of a qubit $|q\rangle$ is:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$$

Since the global phase doesn't matter, α and β can be made real and a term representing the relative phase between them can be added:

$$|q\rangle = \alpha|0\rangle + e^{i\phi}\beta|1\rangle \quad \alpha, \beta, \phi \in \mathbb{R}$$

The qubit state has to be normalised, so $\sqrt{\alpha^2 + \beta^2} = 1$ and thus, we can make the substitutions $\alpha = \cos\frac{\theta}{2}$ and $\beta = \sin\frac{\theta}{2}$. The general state of a qubit can thus be represented by:

$$|q\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \quad \theta, \phi \in \mathbb{R}$$

If θ and ϕ are interpreted to be in spherical coordinates (with $r = 1$), then any qubit state can be plotted on the surface of a sphere, called the *Bloch sphere*. The $|0\rangle$ and $|1\rangle$ states lie on the positive and negative ends of the z-axis respectively.

1.2 Single Qubit Gates

Quantum gates are always *reversible* and are represented by unitary matrices. The *X-gate* is represented by the Pauli-X matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

It acts like a NOT gate on the computational basis states:

$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$$

The X-gate acts like a rotation by π radians about the x-axis.

The *Y-gate* and *Z-gate* is represented by the Pauli-Y and the Pauli-Z matrix respectively.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

They Y-gate and Z-gate acts like a rotation by π radians about the y-axis and z-axis respectively.

The computational basis is also called the Z-basis and $|0\rangle$ and $|1\rangle$ form the eigenstates of the Z-gate. Another popular basis used is the X-basis formed by the eigenstates of the X-gate. Those two statevectors are called $|+\rangle$ and $|-\rangle$.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

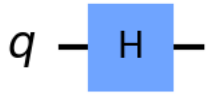
Another less commonly used basis is the Y-basis formed by the eigenstates of the Y-gate. Those two statevectors are called $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$.
The *Hadamard gate* allows us to move away from the poles of the Bloch sphere and create a *superposition* of $|0\rangle$ and $|1\rangle$. It is given by the matrix

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

It performs the following transformations:

$$H|0\rangle = |+\rangle \quad H|1\rangle = |-\rangle$$

This can be thought of as a rotation of π radians about the Bloch vector $\hat{i} + \hat{k}$.



The *P-gate (phase gate)* is parametrised, that is, it needs a number ϕ to tell it exactly what to do. The P-gate performs a rotation of ϕ radians around the z-axis direction. It has the matrix form:

$$P = \begin{bmatrix}1 & 0\\0 & e^{i\phi}\end{bmatrix} \quad \phi \in \mathbb{R}$$

We actually have $Z = P(\pi)$.
The *I-gate* is a gate that does nothing and has the matrix representation

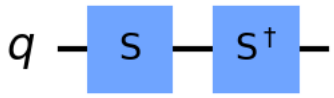
$$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

The *S-gate* (also called the $\sqrt{Z}$-gate) is a $P(\frac{\pi}{2})$-gate and does a quarter turn around the Bloch sphere about the z-axis. The $S^\dagger$*-gate* (also called the $\sqrt{Z}^\dagger$-gate) is a $P(-\frac{\pi}{2})$-gate.

$$S = \begin{bmatrix}1 & 0\\0 & e^{\frac{i\pi}{2}}\end{bmatrix} \quad S^\dagger = \begin{bmatrix}1 & 0\\0 & e^{-\frac{i\pi}{2}}\end{bmatrix}$$

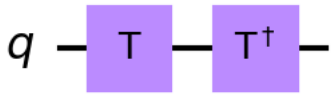
The name "$\sqrt{Z}$-gate" is due to the fact that two successively applied S-gates has the same effect as one Z-gate:

$$SS|q\rangle = Z|q\rangle$$



The *T-gate* is a $P(\frac{\pi}{4})$ gate.

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \quad T^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-\frac{i\pi}{4}} \end{bmatrix}$$

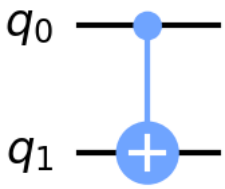


The *U-gate* is the most general of all single-qubit quantum gates. It is a parameterised gate of the form:

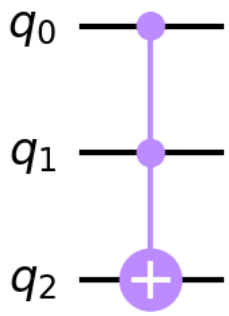
$$U(\theta, \phi, \lambda) = \begin{bmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\phi}{2} & e^{i(\phi+\lambda)\cos\frac{\theta}{2}} \end{bmatrix}$$

1.3 Quantum Half-Adder Circuit

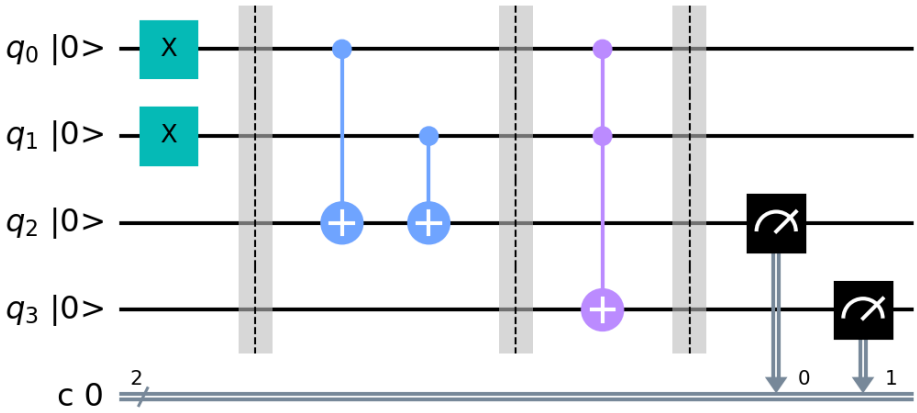
The XOR gate's job is done by the *CNOT (controlled-NOT) gate*.



This is applied to a pair of qubits. One acts as the control qubit (this is the one with the little dot). The other acts as the target qubit. There are multiple ways to explain the effect of the CNOT. One is to say that it looks at its two input bits to see whether they are the same or different. Next, it overwrites the target qubit with the answer. The target becomes 0 if they are the same, and 1 if they are different. Another way of explaining the CNOT is to say that it does a NOT on the target if the control is 1, and does nothing otherwise.
The AND gate's job is done by the *Toffoli gate*.



This will perform a NOT on the target qubit only when both controls are in state 1.
The following is a *quantum half-adder circuit* for adding 1 and 1:



1.4 More Single Qubit Operations

The Pauli matrices, upon exponentiation, give rise to the *rotation operators* about the x, y, and z axes given by:

$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

If $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in three dimensions, then we can perform a rotation by θ about the $\hat{n}$ axis by:

$$R_{\hat{n}}(\theta) = e^{-i\theta\hat{n}\cdot\vec{\sigma}/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(n_xX + n_yY + n_zZ)$$

where $\vec{\sigma}$ denotes the three component vector (X, Y, Z) of Pauli matrices.
An arbitrary single qubit operator can be written in the form

$$U = e^{i\alpha} R_{\hat{n}}(\theta)$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$.

> **Z-Y decomposition for a single qubit:** Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that
> $$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

In fact, suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. An arbitrary single qubit unitary operator U may be written as

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$$

for appropriate choices of α, β, γ and δ.
An important theorem is that for any arbitrary unitary gate U on a single qubit, there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

> **Composition of single qubit operations:** If a rotation through an angle β_1 about the axis $\hat{n}_1$ is followed by a rotation through an angle β_2 about an axis $\hat{n}_2$, then the overall rotation is through an angle β_{12} about an axis $\hat{n}_{12}$ given by
> $$c_{12} = c_1 c_2 - s_1 s_2 \hat{n_1} \cdot \hat{n_2}$$
> $$s_{12} \hat{n}_{12} = s_1 c_2 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \hat{n}_2 \times \hat{n}_1$$
> where $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$, $c_{12} = \cos(\beta_{12}/2)$, and $s_{12} = \sin(\beta_{12}/2)$.

1.5 Multiple Qubits

Two qubits together can be represented by four complex amplitudes stored in a 4-D vector as follows:

$$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

The normalisation condition applies, $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.
For two separated qubits, their collective state can be described using the Kronecker product:

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad |b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

$$|ab\rangle = |a\rangle \otimes |b\rangle = \begin{bmatrix} a_0 \times \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \\ a_1 \times \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

This could similarly be extended to the case of n qubits where we'd have a 2^n dimensional state vector describing the collective state of all the qubits.
An important two qubit state is the *Bell state* or *EPR pair*:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

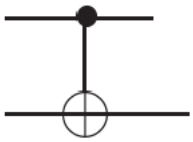
We can represent the action of two single qubit gates on two qubits by the Kronecker product of the respective linear operators of the gates. Suppose U and V are two operators acting on the qubits $|q_0\rangle$ and $|q_1\rangle$ respectively. This simultaneous operation can be represented by

$$U|q_0\rangle \otimes V|q_1\rangle = (U \otimes V)|q_0 q_1\rangle$$

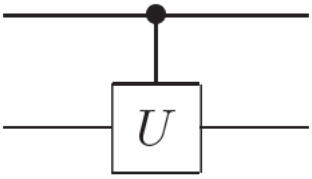
1.6 Controlled Operations

The prototypical controlled operation is the controlled-NOT given by the CNOT gate. It is a quantum gate with two input qubits, known as the *control qubit*control *qubit* and the *target qubit* respectively. In terms of the computational basis, the action of the CNOT is given by $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$. Thus, in the computational basis, the matrix representation of CNOT is

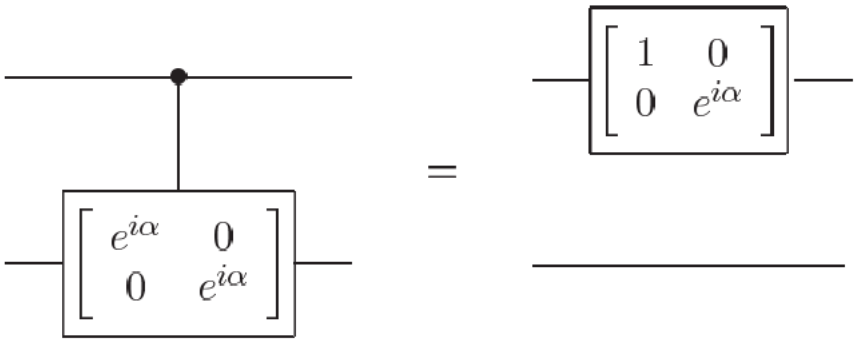
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



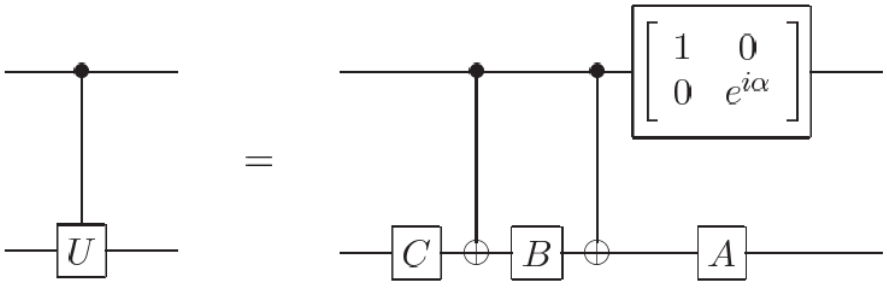
In the above figure, the top line represents the control qubit and the bottom line represents the target qubit.
More generally, suppose U is an arbitrary single qubit unitary operation. A *controlled-U* operation is a two qubit operation with a control and a target qubit. If the control qubit is set, then U is applied to the target qubit, otherwise the target qubit is left alone; that is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$. The controlled-U operation is represented by the following:



The controlled-U operation can be implemented via a two-part procedure based upon the decomposition $U = e^{i\alpha}AXBXC$. The first step would be to apply the phase shit $e^{i\alpha}$ on the target qubit controlled by the control qubit. This can be done by the following:



The construction of the controlled-U operation can now be completed as shown:

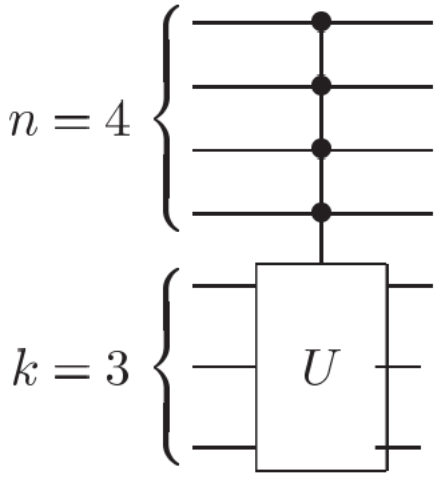


To understand how this works, suppose that the control qubit is set. Then the operation $e^{i\alpha}AXBXC = U$ is applied to the second qubit. If the control qubit is not set, then the operation $ABC = I$ is applied to the second qubit. Thus, the circuit implements the controlled-U operation.
We could also condition on multiple qubits. Generally, suppose we have $n + k$ qubits, and U is a k qubit unitary operator. Then we define the controlled

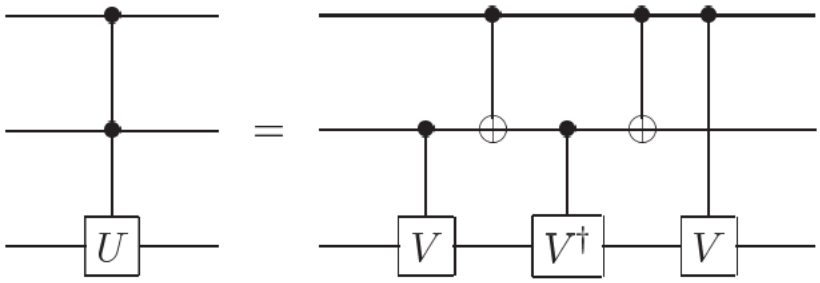
operation $C^n(U)$ by the equation

$$C^n(U)|x_1x_2\ldots x_n\rangle|\psi\rangle = |x_1x_2\ldots x_n\rangle U^{x_1x_2\ldots x_n}|\psi\rangle$$

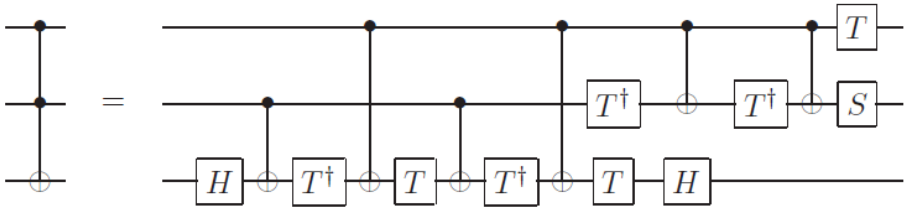
Thus, the operator U is applied to the last k qubits if the first n qubits are all equal to one, otherwise, nothing is done. Such operators can be represented as follows:



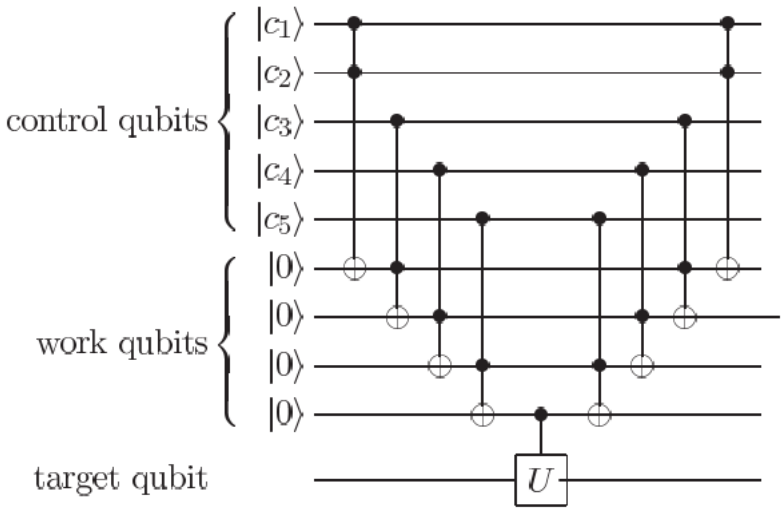
Suppose U is a single qubit unitary operator, and V is a unitary operator chosen so that $V^2 = U$. Then the operations $C^2(U)$ may be implemented by the following circuit:



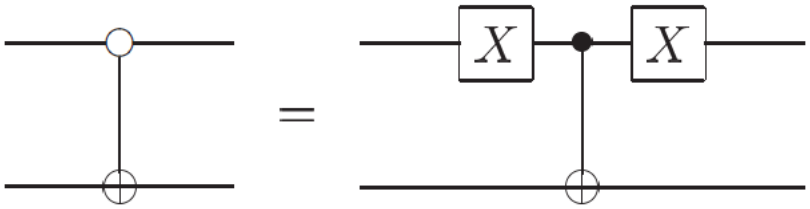
The Toffoli gate can be implemented as follows:



A simple circuit for implementing $C^n(U)$ gates is illustrated in the following:



The circuit divides up into three stages, and makes use of a small number $(n-1)$ of working qubits, which all start and end in the state $|0\rangle$. Suppose the control qubits are in the computational basis state $|c_1, c_2, \ldots, c_n\rangle$. The first stage of the circuit is to reversibly AND all the control bits $|c_1, \ldots, c_n\rangle$ together to produce the product $|c_1 \cdot c_2 \ldots c_n\rangle$. To do this, the first gate in the circuit ANDs c_1 and c_2 together, using a Toffoli gate, changing the state of the first work qubit to $|c_1 \cdot c_2\rangle$. The next Toffoli gate ANDs c_3 with the product $|c_1 \cdot c_2\rangle$, changing the state of the second work qubit to $|c_1 \cdot c_2 \cdot c_3\rangle$. We continue applying Toffoli gates in this fashion, until the final work qubit is in the state $|c_1 \cdot c_2 \ldots c_n\rangle$. Next, a U operation on the target qubit is performed, conditional on the final work qubit being set to one. That is, U is applied if and only if all of c_1 through c_n are set. Finally, the last part of the circuit just reverses the steps of the first stage, returning all the work qubits to their initial state, $|0\rangle$.
If we want to instead implement a two qubit gate in which the target qubit is flipped conditional on the control qubit being set to zero. This can be done as follows:



We can also let a controlled-NOT gate have multiple targets as follows: