Contents

Week 2

Quantum Gates and Circuits

The main idea here is to identify quantum operations in a language more familiar with computation, such as gates and circuits, without worrying about the underlying physical system.
The basic components of a quantum circuit are the gates and the information that flows through the wire and is processed by the gates. Importantly, the gates in a quantum circuit represent *unitary operators*, while the input, output, and general information is given by *pure quantum states.*

1 Single Qubit Gates

Let us start with quantum gates that behave "classically". Consider the unitary operator:

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

acting on the states $|0\rangle$ and $|1\rangle$.

$$X|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

(Classically equivalent to the NOT gate.)
Similarly, the quantum X gate can also act on a superposed state, such that:

$$X(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Importantly, a quantum gate must preserve the normalization of a quantum state and is therefore a unitary operator. This also implies that a quantum gate is reversible.
In general, there exist several single-qubit gates, each given by a 2×2 unitary matrix. Two such important gates are:

$$\sigma_z = \mathcal{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

where σ_z is the Pauli matrix and H is the Hadamard gate. Both these gates are essentially quantum gates with no classical analogue.

$$\mathcal{Z}(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

The circuit can be drawn as follows:

$$\begin{array}{ccc}
\alpha|0\rangle + \beta|1\rangle & -\boxed{X}- & \beta|0\rangle + \alpha|1\rangle \\
\alpha|0\rangle + \beta|1\rangle & -\boxed{Z}- & \alpha|0\rangle - \beta|1\rangle \\
\alpha|0\rangle + \beta|1\rangle & -\boxed{H}- & \alpha|+\rangle + \beta|-\rangle
\end{array}$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A list of other key quantum gates is given below:

$$\text{Pauli } \sigma_y : \quad Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \quad \text{(Gate symbol: } Y\text{)}$$

$$\text{Phase gate} \; : \quad S = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{2}}\end{pmatrix} \quad \text{(Gate symbol: } S\text{)}$$

$$\pi/8 \text{ or T gate} \; : \quad T = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix} \quad \text{(Gate symbol: } T\text{)}$$

1.1 Single Qubit Gates as Rotation in the Bloch Sphere

In general we can write a qubit $|\psi\rangle$ as a vector $\vec{v}$ in the Bloch sphere as shown below:

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle$$

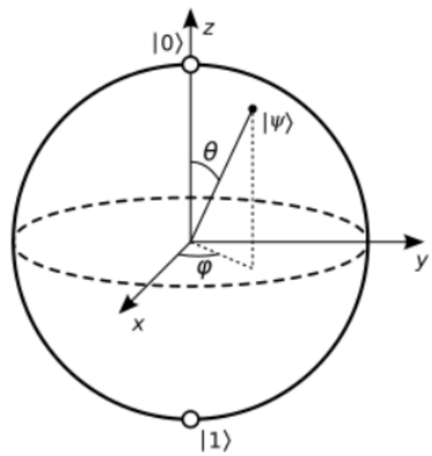
$$\vec{v} = \{cos\phi sin\theta, sin\phi sin\theta, cos\theta\}$$

An important set of single qubit gates is given by rotation operators about the $\hat{x}, \hat{y}$ and $\hat{z}$ axis in the Bloch sphere — defined by the exponentiation of the Pauli matrices.

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

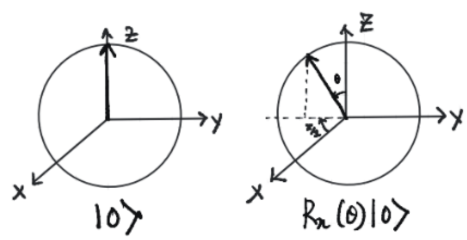
Suppose we have the state; $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$

$$R_x(\theta)|0\rangle = \begin{pmatrix}cos(\frac{\theta}{2})\\ -isin(\frac{\theta}{2})\end{pmatrix} = cos(\frac{\theta}{2})|0\rangle - isin(\frac{\theta}{2})|1\rangle$$



$$= cos(\frac{\theta}{2}) + e^{-i\pi/2}sin(\frac{\theta}{2})\,|1\rangle$$

This results in rotation by an angle θ along the X axis. Similarly, we can have rotations



about the Y and Z axes.

$$R_y(\theta) = \begin{pmatrix} cos(\frac{\theta}{2}) & -sin(\frac{\theta}{2}) \\ sin(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{pmatrix} \quad \text{and} \quad R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

These rotation gates can be derived for any unitary $A^2 = \mathbb{I}$:

$$e^{iAx} = 1 + iAx + \frac{i^2}{2!}A^2x^2 + \frac{i^3}{3!}A^3x^3 + \cdots$$

$$= 1 + iAx - \mathbb{I}\frac{x^2}{2!} - iA\frac{x^3}{3!} + \mathbb{I}\frac{x^4}{4!} + \cdots$$

$$= cos(x)\mathbb{I} + iAsin(x)$$

Therefore,

$$R_y(\theta) = e^{-iY\frac{\theta}{2}} = cos(\frac{\theta}{2})\mathbb{I} - isin(\frac{\theta}{2})Y$$

$$R_z(\theta) = e^{-iZ\frac{\theta}{2}} = cos(\frac{\theta}{2})\mathbb{I} - isin(\frac{\theta}{2})\mathcal{Z}$$

(Rotations by angle θ along the Y and Z axes.
For any general rotation about a unit vector $\hat{n} = \{n_x, n_y, n_z\}$:

$$R_{\hat{n}}(\theta) = exp(-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}) = cos(\frac{\theta}{2})\mathbb{I} - isin(\frac{\theta}{2})(n_x X + n_y Y + n_z \mathcal{Z})$$

Importantly, since a unitary operation takes a state on the Bloch sphere to another, any single qubit quantum gate can be written as a product of rotations and a global phase shift, i.e.,

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

where α, θ and $\hat{n}$ are real numbers and vector respectively.
Consider the Hadamard gate :

$$H = \frac{1}{\sqrt{2}}(X + \mathcal{Z}) = exp(i\alpha)R_{\hat{n}}(\theta)$$

$$= \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix} [cos(\frac{\theta}{2})\mathbb{I} - isin(\frac{\theta}{2})(n_x X + n_y Y + n_z \mathcal{Z})]$$

Let $\alpha = \pi/2$, $\theta = \pi$, $\hat{n} = \{\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\}$

$$= i\mathbb{I} \cdot -i(\frac{X}{\sqrt{2}} + \frac{\mathcal{Z}}{\sqrt{2}}) = \frac{1}{\sqrt{2}}(X + \mathcal{Z})$$

Similarly, there exist other such rotations and phase shifts that can represent a universal single qubit unitary operation.

Exercise: Show using rotations in the z and y axes and a phase shift that,

$$U = exp(i\alpha)R_z(\beta)R_y(\gamma)R_z(\delta)$$

$$= \begin{pmatrix} e^{i(\alpha-\frac{\beta}{2})} & 0 \\ 0 & e^{i(\alpha+\frac{\beta}{2})} \end{pmatrix} \begin{pmatrix} cos(\gamma/2) & -sin(\gamma/2) \\ sin(\gamma/2) & cos(\gamma/2) \end{pmatrix} \begin{pmatrix} e^{-i\gamma/2} & 0 \\ 0 & e^{i\gamma/2} \end{pmatrix}$$

Hint: Show that the above relation boils down to the previous relation for an arbitrary single qubit unitary in terms of rotation by about $\hat{n}$ and a global phase shift α.

One can show that the expression can also be written as $U = exp(i\alpha)AXBXC$, where A, B and C are unitary operators such that $ABC = I$ and X is the Pauli matrix.
Say,

$$ABC = R_z(\beta)R_y(\gamma/2)R_y(-\gamma/2)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = \mathbb{I}$$

$$\begin{aligned} A &= R_z(\beta)R_y(\gamma/2) \\ B &= R_y(-\gamma/2)R_z\left(-\frac{\delta+\beta}{2}\right) \quad \Rightarrow \quad ABC = \mathbb{I} \\ C &= R_z\left(\frac{\delta-\beta}{2}\right) \end{aligned}$$

Some general relations we need:

$$X^2 = Y^2 = Z^2 = \mathbb{I} \quad \text{and} \quad \{X, Y\} = \{Y, Z\} = \{Z, X\} = 0$$

$$XYX = -YXX = -YX^2 = -Y$$

$$XR_y(\theta)X = X\left(\cos(\frac{\theta}{2})\,\mathbb{I} - i\sin(\frac{\theta}{2})\,Y\right)X = R_y(-\theta)$$

$$XBX = XR_y(-\gamma/2)R_z\left(-\frac{\delta+\beta}{2}\right)X = XR_y(-\gamma/2)X \cdot XR_z\left(-\frac{\delta+\beta}{2}\right)X$$

$$= R_y(\gamma/2)R_z(\frac{\delta+\beta}{2}) \quad (\text{since } XR_z(\theta)X = R_z(-\theta))$$

$$\therefore A \cdot XBX \cdot C = R_z(\beta)R_y(\gamma/2)R_y(\gamma/2)R_z(\frac{\delta+\beta}{2})R_z\left(\frac{\delta-\beta}{2}\right)$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta)$$

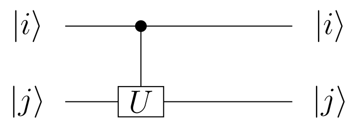
$$\therefore e^{i\alpha}AXBXC = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

2 Two Qubit Controlled Gates

Controlled operations and gates are quite common in classical circuits. When the first qubit (say A) is $|0\rangle$, nothing changes in the second qubit (say B), which means it is operated by identity $\mathbb{I}$. On the other hand, if A is $|1\rangle$, the second qubit is acted upon by some unitary U. Here, qubit A is the control qubit, and B is the target qubit.
In the computational basis, this can be written as,

$$|i\rangle\,|j\rangle \longrightarrow |i\rangle\,U^i\,|j\rangle\,, \quad \text{where} \quad U^0 = \mathbb{I}$$

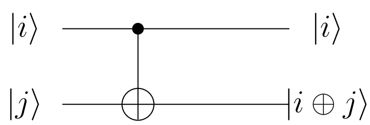
and the circuit representation of such a controlled - U gate would look like:



Let us take the example of the CNOT (controlled NOT) gate, where the target qubit is flipped (NOT or X gate) when the control qubit is $|1\rangle$. In the computational basis this is given by the relation:

$$|i\rangle\,|j\rangle \rightarrow |i\rangle\,|i \oplus j\rangle\,,$$

where $\oplus$ is the classical XOR gate operation, i.e., addition modulo 2.



The matrix representation of the CNOT gate is given by

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

Note that controlled gates are two-qubit unitaries and cannot be written as the product of two single qubit gates, i.e.,

$$\text{Controlled} - U \neq U_1 \otimes U_2 = |0\rangle\,\langle 0| \otimes \mathbb{I} + |1\rangle\,\langle 1| \otimes U$$

$$\therefore \text{CNOT} = |0\rangle\,\langle 0| \otimes \mathbb{I} + |1\rangle\,\langle 1| \otimes \sigma_x = U_{CN}$$
$$\text{Controlled} - \sigma_z = |0\rangle\,\langle 0| \otimes \mathbb{I} + |1\rangle\,\langle 1| \otimes \sigma_z = U_{CZ}$$

Exercise: Show that CNOT can be derived from U_{CZ} and two Hadamard gates.

A significant difference between gates like CNOT and classical gates is their reversibility. Since quantum gates are nothing but unitary operators, they are reversible by definition.

On the other hand, two-input classical gates, such as XOR or the universal NAND, are not reversible; i.e., given the target state, one cannot determine what the input states were.

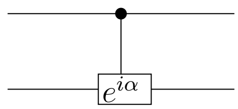
The CNOT gate, along with single qubit gates, are the prototype for all multiple qubit gates and thus forms a universal set.

In an exercise, we wanted to show that any single qubit gate U can be written as:

$$U = exp(i\alpha)AXBXC, \quad \text{where} \quad ABC = \mathbb{I}.$$

Now, we ask **can any controlled-U operator be represented using simply the CNOT and single qubit gate U?**

First, let us consider the controlled-phase operation:

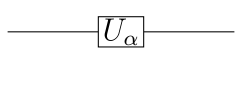


$$\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow e^{i\alpha}\,|10\rangle \\
|11\rangle &\rightarrow e^{i\alpha}\,|11\rangle
\end{aligned}$$

This can also be written as:

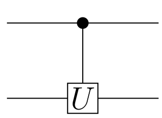
$$\begin{aligned}
|0, j\rangle &\rightarrow |0, j\rangle \\
|1, j\rangle &\rightarrow e^{i\alpha}\,|1, j\rangle
\end{aligned}$$

So, an equivalent circuit for this is given by:

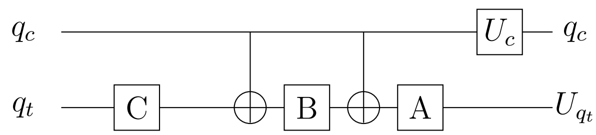


$$U_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$$

Secondly, we know that if the control qubit is $|0\rangle$, then we implement $ABC \cdot \mathbb{I}$ and the target qubit is unchanged, and for control qubit $|1\rangle$, we get $AXBXC$. This is given by the circuit below:



$$\downarrow$$



Therefore, the above circuit creates a two-qubit controlled unitary gate.

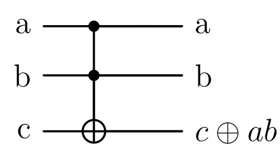
3 Toffoli Gate and Multiple Control Qubits

An important question that one can often ask is whether classical gates can be simulated using quantum circuits. In principle, this should be true as all of the relevant classical physics can be thought of as arising from quantum mechanics. However, we also know that quantum gates are reversible, while universal gates such as NAND and XOR are not.

The reversible three input-output Toffoli gate is a universal gate for classical computation.

The Toffoli gate has two control bits and one target bit that is flipped if both controls are set; i.e.,

$$(a, b, c) \longrightarrow (a, b, ab \oplus c)$$



NOT acts on c *iff* $a = 1$ *and* $b = 1$.

- **Show that the Toffoli gate is reversible.**

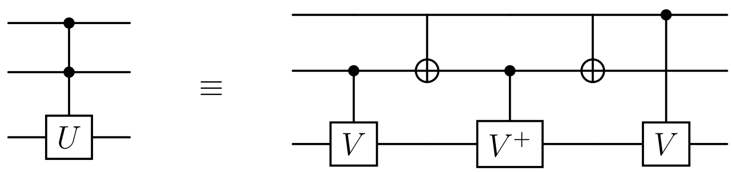
Truth Table

a	b	c	Output
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

If one sets $c = 1$, we get: $(a, b, c = 1) = (ab \oplus 1)$ which is the **NAND** gate.

Also, $(a = 1, b = x, c = 0) \rightarrow (a = 1, b = x, c = x)$

The Toffoli gate or any three-qubit controlled unitary can be created using two-qubit controlled unitaries, similar to how we created a controlled-U gate using CNOT and single qubit gates.

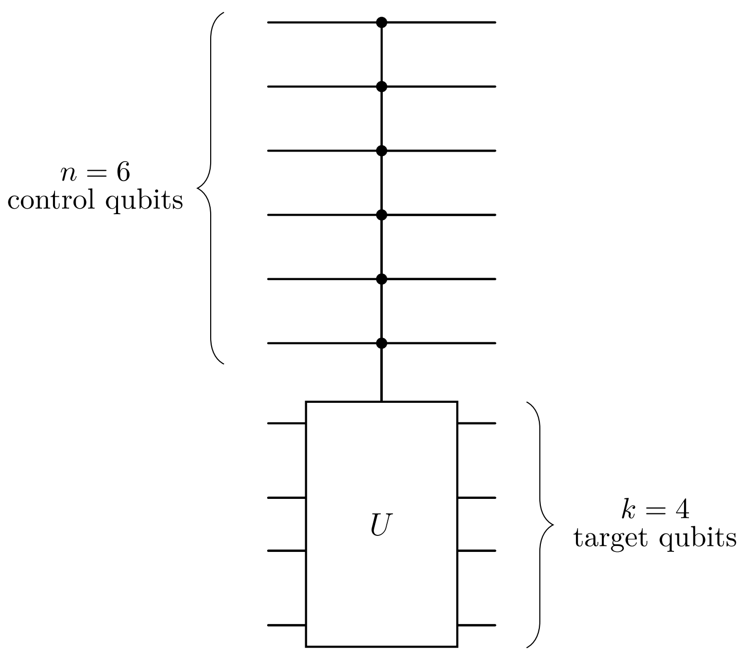


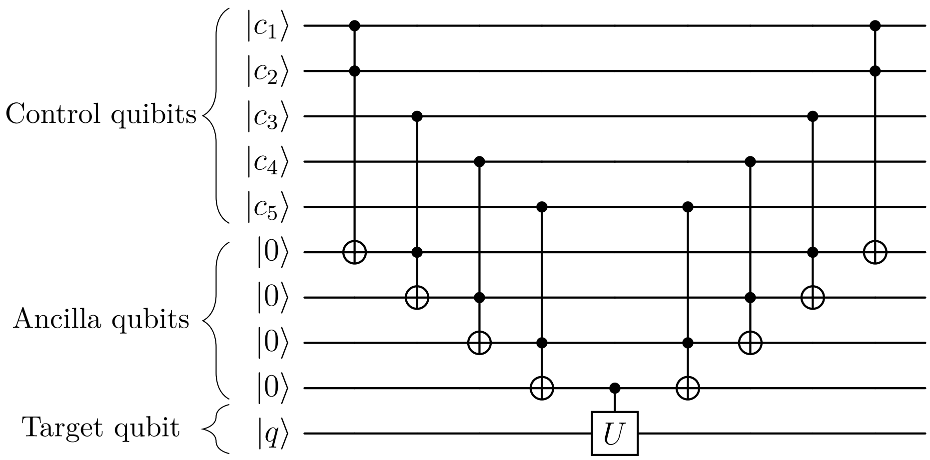
Exercise: *Show the above circuit is true for unitary V, where $V^2 = \mathbb{I}$.*

In general, we can define multi-qubit controlled gates that act on (say) $n+k$ qubits, where the first n qubits are *control qubits* and the operator U acts on the next k *target qubits*. This can be defined as follows:

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

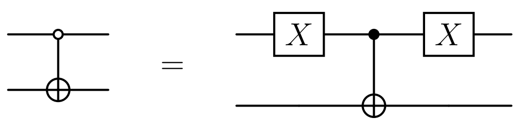
where $x_1x_2\ldots x_n$ is the product of the n bit values. This implies that U acts on the k-qubit $|\psi\rangle$ only if all x_i values are equal to 1 (i.e., all control qubits are set at 1's). The circuit representation of the $n+k$ controlled unitary is given by :



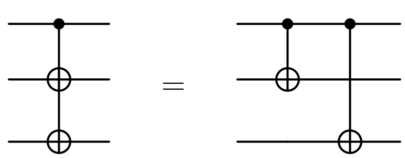


Exercise: *Show that a multi-qubit controlled single-qubit U gate ($C^5(U)$) can be implemented using a series of Toffoli gates.*

An interesting conditional gate is one in which the condition on the control qubit is changed. Think of the CNOT gate which is conditioned such that the target qubit is flipped if and only if the control qubit is $|0\rangle$ (instead of $|1\rangle$).

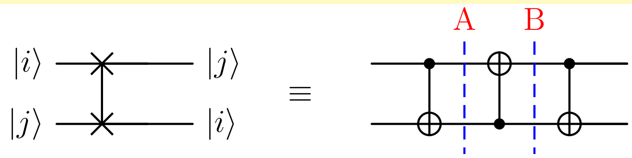


Multiply conditioned gates with two target qubits but a single control qubit:



4 Other Interesting Gates

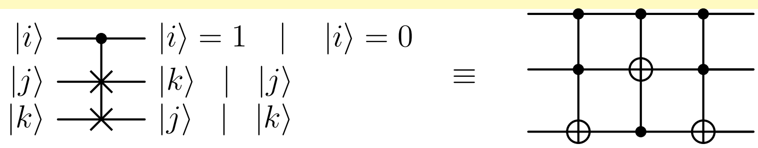
SWAP gate — A two-qubit gate that swaps the inputs in the two arms of the quantum circuit.



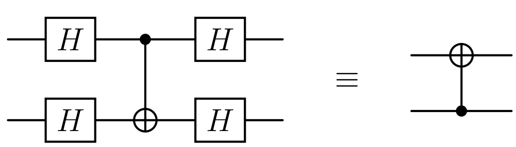
Input		A		B		Output	
$\|i\rangle$	$\|j\rangle$	$\|i\rangle$	$\|j\rangle$	$\|i\rangle$	$\|j\rangle$	$\|i\rangle$	$\|j\rangle$
0	0	0	0	0	0	0	0
0	1	0	1	1	1	1	0
1	0	1	1	0	1	0	1
1	1	1	0	1	0	1	1

$$, U_{\text{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

FREDKIN gate — A three-qubit controlled SWAP gate.



CNOT gate in a different basis



CNOT in the $\{|0\rangle, |1\rangle\}$ basis :

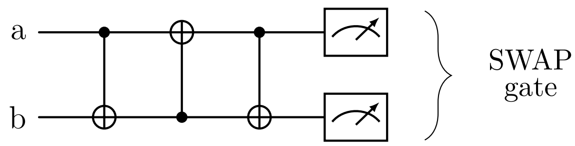
Input	$\rightarrow$	Output
$\|0\rangle\|0\rangle$	$\rightarrow$	$\|0\rangle\|0\rangle$
$\|0\rangle\|1\rangle$	$\rightarrow$	$\|0\rangle\|1\rangle$
$\|1\rangle\|0\rangle$	$\rightarrow$	$\|1\rangle\|1\rangle$
$\|1\rangle\|1\rangle$	$\rightarrow$	$\|1\rangle\|0\rangle$

CNOT in the $\{|+\rangle, |-\rangle\}$ basis :

Input	$\rightarrow$	Output
$\|+\rangle\|+\rangle$	$\rightarrow$	$\|+\rangle\|+\rangle$
$\|-\rangle\|+\rangle$	$\rightarrow$	$\|-\rangle\|+\rangle$
$\|+\rangle\|-\rangle$	$\rightarrow$	$\|-\rangle\|-\rangle$
$\|-\rangle\|-\rangle$	$\rightarrow$	$\|+\rangle\|-\rangle$

5 Quantum Circuits and Measurements

Quantum circuits are a bit different from classical circuits. Some of this results from the unitarity and therefore the reversibility of quantum gates.

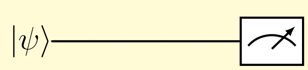


- The circuit is read (as usual) from left to right. The inputs are typically qubits in the computational basis (unless mentioned otherwise) and lines imply the passage of a qubit in time or space. All wires implicitly end in measurement.
- Quantum circuits are typically acyclic, i.e., there is no feedback from one part of the circuit to another.
- Unlike classical circuits, wires in a quantum circuit cannot be joined to achieve irreversible **OR** operation and also several wires cannot emerge from a single point as that would violate the "no cloning" principle.
- Measurements are represented by "meters" and are often projectors in the computational basis. All POVMs can be thought of as projectors with additional qubits.
- All measurements can be performed at the end of the circuit.

  Two key points:

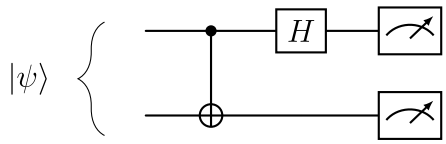
  (i) Measurement outcomes can condition the action of a gate in a circuit.

  (ii) All unmeasured wires can be assumed to be measured.



It is important to note that measurements in quantum circuits (i.e., projective) collapse quantum information to classical information—however, in carefully designed circuits, measurement can be made without revealing the quantum state—as we will see later for quantum teleportation circuit.

Measurement in Bell basis



The above circuit makes a measurement in the Bell basis or projects in the Bell basis.

Suppose $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then after the CNOT, the state becomes $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$, and after the Hadamard gate, it becomes $|\psi\rangle = |0\rangle\,|0\rangle$.

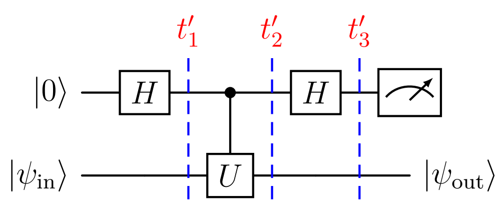
$$\text{Therefore } |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ corresponds to measuring 0 and 0.}$$

Exercise: *Show what the outcome is for the other Bell states.*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad \text{and} \quad |\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Measuring an operator $\hat{O}$ that is unitary and Hermitian

If $\hat{O}$ is unitary $\Rightarrow$ it is a gate in the circuit and since $\hat{O}$ is also *hermitian* $\Rightarrow$ it is an observable (say with eigenvalues ± 1 and corresponding eigenvectors).



The above circuit allows you to observe the operator $\hat{O}$ upon measurement.
Our initial state is $|0\rangle \otimes |\psi_{\text{in}}\rangle$ and at t_1 we have :

$$|0\rangle \otimes |\psi_{\text{in}}\rangle \to \frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\} \otimes |\psi_{\text{in}}\rangle$$

$$\text{at } t_2 : \quad \frac{1}{\sqrt{2}}\{|0\rangle\,|\psi_{\text{in}}\rangle + |1\rangle\,U\,|\psi_{\text{in}}\rangle\}$$

$$\text{at } t_3 : \quad \frac{1}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi_{\text{in}}\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)U\,|\psi_{\text{in}}\rangle\right\}$$

$$= \frac{1}{2}\left\{|0\rangle\left(\mathbb{I}+U\right)|\psi_{\text{in}}\rangle + |1\rangle\left(\mathbb{I}-U\right)|\psi_{\text{in}}\rangle\right\}$$

If we measure the first qubit as $|0\rangle$, then :

$$|\psi_{\text{out}}\rangle = \left(\mathbb{I}+U\right)|\psi_{\text{in}}\rangle$$

$$\text{Now, } U(\mathbb{I}+U)|\psi_{\text{in}}\rangle = (U+U^2)|\psi_{\text{in}}\rangle = +1\cdot(\mathbb{I}+U)|\psi_{\text{in}}\rangle$$

eigenstate with eigenvalue $+1$

If the first qubit is $|1\rangle$, then :

$$|\psi_{\text{out}}\rangle = \left(\mathbb{I}-U\right)|\psi_{\text{in}}\rangle$$

$$\text{and } U(\mathbb{I}-U)|\psi_{\text{in}}\rangle = (U-U^2)|\psi_{\text{in}}\rangle = -1\cdot(\mathbb{I}-U)|\psi_{\text{in}}\rangle$$

eigenstate with eigenvalue -1

6 Universal Quantum Gates

We know that the NAND and NOR gates are universal gates for classical computation and Boolean algebra. But these are irreversible gates. On the other hand, the Toffoli gate is a reversible, three-input gate that is universal for classical computation.
For quantum computation, a similar set of universal gates exists - any unitary operation can be represented using a circuit with only universal gates. These are CNOT, Hadamard, T, and phase gates.
Now, how do you know these gates are universal? The proof involves the following three key arguments-

(a) An arbitrary n-dimensional unitary operation can always be written as a product of effective unitary operators acting on 2-dimensional subspace or "two level" unitary operators.

(b) All two level (or say $2D$) unitary operators can be represented by CNOT and single qubit gates.

(c) All single qubit gates, upto arbitrary accuracy, can be obtained using only Hadamard, T and phase gates.

6.1 Two-level Unitary gates are universal

In an n-dimensional Hilbert Space, a two-level unitary acts on an effective 2×2 dimension; it acts only on the subspace spanned by any two of the vectors from the given basis. In simpler terms, a two-level unitary is a special type of quantum operation that only affects two states in a quantum system and leaves all other states unchanged. For instance, consider a hilbert space of four qubits spanned by basis

$$\{|0000\rangle, |0001\rangle, \ldots, |ijkl\rangle, \ldots, |1111\rangle\}$$

Then the unitary ν that acts on states $|0000\rangle$ and $|1111\rangle$ would look like-

$$\nu = \begin{bmatrix} a & 0 & 0 & \cdots & b \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c & 0 & 0 & \cdots & d \end{bmatrix}$$ where the effective dimension is 2×2, $\nu = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the effective unitary.

Theorem 6.1

Let $\mathcal{U}$ be a n-dimensional unitary operator in the Hilbert Space $\mathcal{H}$. There exist k two-level unitaries ν_i, $k \leq \frac{n(n-1)}{2}$, such that $\mathcal{U} = \nu_1^\dagger \nu_2^\dagger \ldots \nu_k^\dagger$.

For an n-dimensional unitary, we can work for $n-1$ *two-level* unitaries that allow us to set the elements of the first column and row to zero, apart from the first element, which is set to unity.

For the $(n-1) \times (n-1)$ dimensional submatrix, we can again select $n-2$ *two-level* unitaries to set all elements (except the first) to zero and so on.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix} \to \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & a'_{1,1} & \cdots & a'_{1,n-1} \\ 0 & a'_{2,1} & \cdots & a''_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{bmatrix} \to \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & a''_{1,1}\cdots & a''_{1,n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a''_{n-2,1}\cdots & a''_{n-2,n-2} \end{bmatrix}$$

So the maximum number of gates needed:

$$(n-1)+(n-2)+(n-3)+\cdots+1 = \frac{n(n-1)}{2}$$

Exercise: Apply this procedure for N=3, and try to find unitaries ν_1, ν_2 and ν_3 such that $\nu_1\nu_2\nu_3\mathcal{U} = \mathbb{I}$

6.2 CNOT and Single Qubit Gates can simulate "Two-Level" Unitary Matrices

From the section 6.1 , we know that product of "two-level" unitary matrices can be used to represent any arbitrary n-dimensional unitary.

How a two-level or an effective two-dimensional unitary (ν) can be implemented using a quantum gate ($\tilde{\nu}$) acting on a single qubit?

$$\nu = \begin{bmatrix} a & 0 & 0 & \cdots & 0 & b \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ c & 0 & 0 & \cdots & 0 & d \end{bmatrix} \quad \Rightarrow \quad \tilde{\nu} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Let ν be a two-level unitary matrix that acts on the subspace spanned by $|s\rangle = |s_1 s_2 \ldots s_n\rangle$ and $|t\rangle = |t_1 t_2 \ldots t_n\rangle$. We make use of **Gray Codes**, which connect the string of bits $s_1 s_2 s_3 \ldots s_n$ and $t_1 t_2 \ldots t_n$ by a sequence of strings such that any two subsequent strings differ by a single bit. For example -

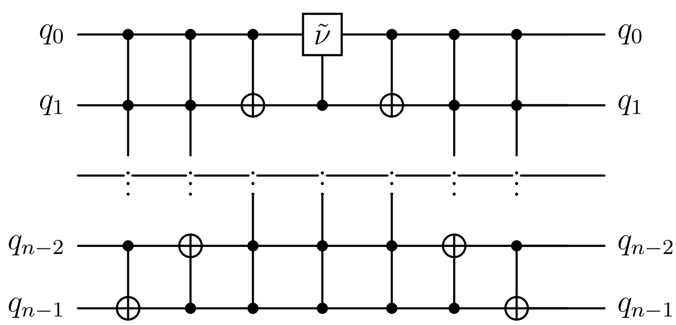
$$\begin{aligned} |s\rangle &= |10011001\rangle \to |g_0\rangle \\ |s\rangle &= |10011000\rangle \to |g_1\rangle \\ |s\rangle &= |10011010\rangle \to |g_2\rangle \\ |s\rangle &= |100\boxed{0}101\rangle \to |g_3\rangle \\ |t\rangle &= |100\boxed{1}101\rangle \to |g_4\rangle \end{aligned}$$

Theorem 6.2

The gray code connects the states $|s\rangle$ and $|t\rangle$ through a series of gate operations between $|g_0\rangle$ and $|g_m\rangle$ where $m \leq n$. We perform a series of gates that takes us from $|g_0\rangle$ to $|g_{m-1}\rangle$, and then apply a controlled $-\tilde{\nu}$ gate on the last bit that is the difference between $|g_{m-1}\rangle$ and $|g_m\rangle$ (shown by the box). After the controlled $-\tilde{\nu}$ is applied, the reverse operations takes us from $|g_{m-1}\rangle$ to $|g_0\rangle$.

Goal: We want to transform the effective two dimensional or two-level ν to a two-level qubit gate $\tilde{\nu}$ and this is achieved by bringing $|g_0\rangle$ and $|g_m\rangle$ next to each other by transforming $|g_0\rangle \rightarrow |g_1\rangle \rightarrow \cdots \rightarrow |g_{m-1}\rangle$

To do this, we apply SWAP operation between $|g_0\rangle$ and $|g_1\rangle$ by performing a bit-flip with the target as the qubit that differs (say i) and using the rest of the qubits as control. Next SWAP $|g_1\rangle$ and $|g_2\rangle$ and repeat till the state $|g_0\rangle$ reaches $|g_{m-1}\rangle$. Then we apply controlled $-\tilde{\nu}$ on the j^{th} qubit that differs between $|g_m\rangle$ and $|g_{m-1}\rangle$, before performing the reverse swaps that brings all states to its original state.
The effective circuit can be shown as



A natural question to ask, how many gates are required to implement the above circuit?
$2(n-1)$ controlled flips are needed before and after implementing the controlled $\tilde{\nu}$ operation. Now we know that, each operation requires $\mathcal{O}(n)$ single qubit and CNOT gate. Therefore $\mathcal{O}(n^2)$ gates are needed to implement each effective "two-level" unitary gate. However, $\mathcal{O}(4^n)$ gates are required to implement an arbitrary n-qubit unitary matrix. Therefore, $\mathcal{O}(4^n n^2)$ single qubit gates are required to implement an arbitrary n-qubit gate.

How does the Gray Code works?

The Gray Code reduces an "effective two-level" unitary to a single qubit gate, using a series of controlled gates. Consider the example:

$$\nu = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \quad ; \quad \tilde{\nu} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The basis states for three qubits $\{|i\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$

Then the action of ν on a general state $|\psi\rangle$ -

$$\nu|\psi\rangle = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \begin{pmatrix} \alpha_0 |000\rangle \\ \alpha_1 |001\rangle \\ \alpha_2 |010\rangle \\ \alpha_3 |011\rangle \\ \alpha_4 |100\rangle \\ \alpha_5 |101\rangle \\ \alpha_6 |110\rangle \\ \alpha_7 |111\rangle \end{pmatrix}$$

- Acts non-trivially on: $\alpha_0 |000\rangle, \alpha_7 |111\rangle$
- Nothing happens to the remaining states

Note that our circuit will only act on these states-the blue states. All we need to do is move the elements of the unitary in such a way that the operation is applied only on a single qubit. An important point here is that ν is written in the computational basis $\{|i\rangle\}$ above. The Gray Code Mapping is:

$$\begin{aligned} |s\rangle = |g_0\rangle &= |000\rangle \\ |g_1\rangle &= |001\rangle \\ |g_2\rangle &= |011\rangle \\ |S_3\rangle &= |010\rangle \\ |S_4\rangle &= |110\rangle \\ |S_5\rangle &= |111\rangle = |t\rangle \end{aligned}$$

the First Change $|g_0\rangle \to |g_1\rangle$, i.e., $|000\rangle \to |001\rangle$

$$\nu|\psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & c & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \begin{pmatrix} \alpha_1 |000\rangle \\ \alpha_0 |001\rangle \\ \alpha_2 |010\rangle \\ \alpha_3 |011\rangle \\ \alpha_4 |100\rangle \\ \alpha_5 |101\rangle \\ \alpha_6 |110\rangle \\ \alpha_7 |111\rangle \end{pmatrix}$$

Note that the control on q_1 ensures $|111\rangle$ does not change yet.
After the Second Change $|g_1\rangle \to |g_2\rangle$, i.e., $|001\rangle \to |011\rangle$

$$\nu\,|\psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & d \end{pmatrix} \begin{pmatrix} \alpha_1\,|000\rangle \\ \alpha_2\,|001\rangle \\ \alpha_3\,|010\rangle \\ \alpha_0\,|011\rangle \\ \alpha_4\,|100\rangle \\ \alpha_5\,|101\rangle \\ \alpha_6\,|110\rangle \\ \alpha_7\,|111\rangle \end{pmatrix}$$

The above matrix can be written in operator form as:

$$\nu = a\,|011\rangle\langle 011| + b\,|011\rangle\langle 111| + c\,|111\rangle\langle 011| + d\,|111\rangle\langle 111|$$
$$+ \sum_{|i\rangle \notin \{|011\rangle, |111\rangle\}} |i\rangle\langle i| \quad \text{(where } |i\rangle \text{ are computational basis states)}$$

This simplifies to:

$$\nu = (a\,|0\rangle\langle 0| + b\,|0\rangle\langle 1| + c\,|1\rangle\langle 0| + d\,|1\rangle\langle 1|) \otimes |11\rangle\langle 11| + \sum_{|i\rangle \notin \{|011\rangle, |111\rangle\}} |i\rangle\langle i|$$

Further you can check, the circuit 6.2 achieves this precisely!