Module III - Part 1

Quantum computation

PH 534 QIC

Quantum gates and circuits

(A) 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 flowing through the wire and being processed by the gates. Importantly, gates in a quantum circuit represents unitary operations, while the input, output and general information is given by pure quantum states.*

*Mixed states appear probabilistically or as purifications.

Now, an important question that arises is why did we spend so much time studying quantum operations and mixed states if ultimately we are using pure states and unitary operations in designing quantum circuits. The answer here is that the quantum circuits we will look at here will use logical states and gates. However, these logical states require physical components that are governed by quantum operations and are not necessarily pure. So, a large part of research and engineering is spent on creating these logical qubits and unitary gates.

It helps to make an important distinction — what tools here are classical and those that are purely quantum. For example, the states $|0\rangle$ and $|1\rangle$ are states of a quantum system (energy levels of an atom or spin of an electron) but are equivalent to the classical bits as they are perfectly distinguishable. On the other hand states such as $\alpha|0\rangle + \beta|1\rangle$ are essentially quantum. Again, unitary operations given by Pauli matrix σ_x mimics the action of the classical NOT gate but σ_z is quantum. So we always try to focus on these small distinctions.

i) Single qubit gates

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

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

acting on the states $|0\rangle$ and $|1\rangle$. We already know that σ_x is a spin flip operator, i.e.,

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

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

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 an unitary operator.

This also implies that a quantum gate is reversible. In general, unlike the classical case, there can exist several single qubit gates each given by a 2×2 unitary matrix.

Two such important gates are the

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

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

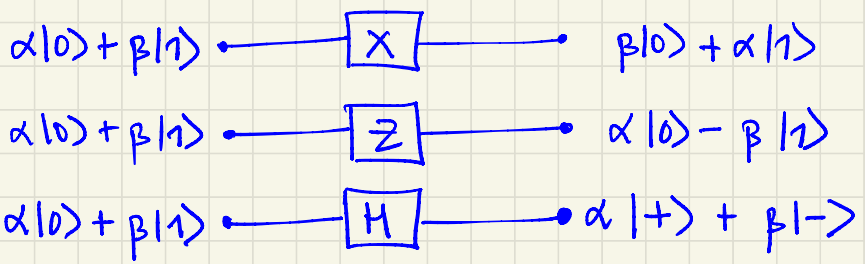
$$Z(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

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

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

creates superposition in the otherwise classical state $|0\rangle$ and $|1\rangle$

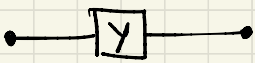
The circuit can be drawn as follows :-



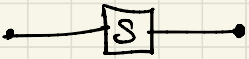
where $|\pm\rangle = \frac{1}{\sqrt{2}}\{|0\rangle \pm |1\rangle\}$

A list of other key quantum gates are given below :-

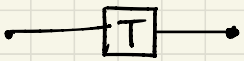
Pauli σ_y : $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$



Phase gate : $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$ → i



$\pi/8$ or T gate : $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

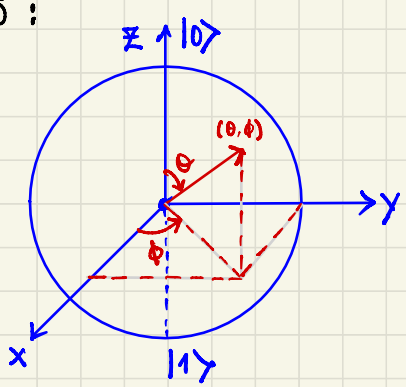


ii) Single qubit gates as rotations in the Bloch sphere

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

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

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



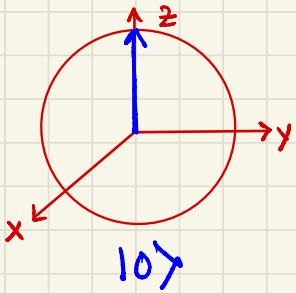
An important set of single qubit gates are given by rotation operators about the $\hat{x}$, $\hat{y}$ and $\hat{z}$ axis in the Bloch sphere — defined by the exponentiation of the Pauli matrices.

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

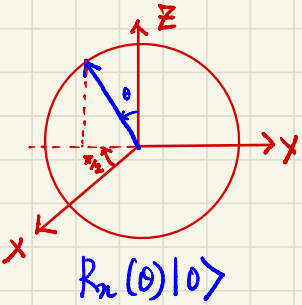
Suppose we have the state; $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$R_x(\theta)|0\rangle = \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta/2 \\ -i\sin\theta/2 \end{pmatrix} = \cos\tfrac{\theta}{2}|0\rangle - i\sin\tfrac{\theta}{2}|1\rangle$$

$$= \cos\tfrac{\theta}{2} + e^{-i\pi/2}\sin\tfrac{\theta}{2}|1\rangle$$



$|0\rangle$



$R_x(\theta)|0\rangle$

So, a rotation like $e^{i\theta/2 X}$, gives rise to rotation by angle θ along the X axis.

* note the factor $\frac{1}{2}$ in $e^{i\theta/2 X}$

Similarly, we can have rotations about the Y and Z axes.

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

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

$$\begin{aligned} \exp(iAx) &= 1 + iAx + \frac{i^2}{2!}A^2x^2 + \frac{i^3}{3!}A^3x^3 + \dots \\ &= 1 + iAx - \frac{\mathbb{I}}{2!}x^2 - \frac{i}{3!}Ax^3 + \frac{\mathbb{I}}{4!}x^4 + \dots \\ &= \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \dots\right)\mathbb{I} + iA\left(x - \frac{x^3}{3!} + \dots\right) \\ &= \cos x\,\mathbb{I} + i A \sin x. \end{aligned}$$

Therefore,

$$\left.\begin{aligned} R_y(\theta) = e^{-i\theta/2 Y} &= \cos\theta/2\,\mathbb{I} - i\sin\theta/2\,Y \\ R_z(\theta) = e^{-i\theta/2 X} &= \cos\theta/2\,\mathbb{I} - i\sin\theta/2\,Z \end{aligned}\right\}$$ Rotations by angle θ along the Y and Z axis.

For any general rotation about a unit vector $\hat{n} = \{n_x, n_y, n_z\}$

$$R_{\hat{n}}(\theta) = \exp\left(-i\theta/2\,\hat{n}\cdot\vec{\sigma}\right) = \cos\theta/2\,\mathbb{I} - i\sin\theta/2\left(n_x X + n_y Y + n_z Z\right)$$

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 : $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

$$= \begin{pmatrix} \exp(i\alpha) & 0 \\ 0 & \exp(i\alpha) \end{pmatrix} \left\{ \cos\frac{\theta}{2} \mathbb{I} - i \sin\left(\frac{\theta}{2}\right) \begin{pmatrix} n_x X + n_y Y \\ + n_z Z \end{pmatrix} \right\}$$

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

$$= i\,\mathbb{I} \cdot -i \left(X/\sqrt{2} + Z/\sqrt{2} \right) = \frac{1}{\sqrt{2}} (X + Z)$$

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

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

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

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 $U = \exp(i\alpha) A X B X C$, where A, B and C are are unitary operators such that $ABC = I$ and X is the Pauli matrix.

Say, $ABC = \underbrace{R_z(\beta) R_y(\gamma/2)}_{A} \underbrace{R_y(-\gamma/2) R_z\left(-\frac{\delta-\beta}{2}\right)}_{B} \underbrace{R_z\left(\frac{\delta-\beta}{2}\right)}_{C} = I$

$$A = R_z(\beta) R_y(\gamma/2)$$
$$B = R_y(-\gamma/2) R_z(-\delta/2 - \beta/2)$$
$$C = R_z(\delta/2 - \beta/2)$$

$$ABC = R_z(\beta) R_y(\gamma/2) R_y(-\gamma/2) R_z(-\delta/2 - \beta/2) R_z(\delta/2 - \beta/2)$$
$$= R_z(\beta) R_z(-\beta/2)$$
$$= I$$

Some general relations we need:

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

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

$X R_y(\theta) X = X \cos\theta/2\, I\, X - i X \sin\theta/2\, Y X$

$= \cos\theta/2\, X^2 - i \sin\theta/2\, XYX = \cos\theta/2\, I + i \sin\theta/2\, Y$

$= R_y(-\theta)$

$$XBX = X R_y(-\gamma/2) R_z(-\delta/2 - \beta/2) X = X R_y(-\gamma/2) X X R_z(-\tfrac{\delta}{2} - \beta/2) X$$
$$= R_y(+\gamma/2) R_z(\delta/2 + \beta/2) \quad (\because X R_z(\theta) X = R_z(-\theta))$$

$$\therefore AXBXC = R_z(\beta) R_y(\gamma/2) R_y(\gamma/2) R_z(\delta/2 + \beta/2) R_z(\delta/2 - \beta/2)$$
$$= R_z(\beta) R_y(\gamma) R_z(\delta)$$

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

iii) Two qubit controlled gates

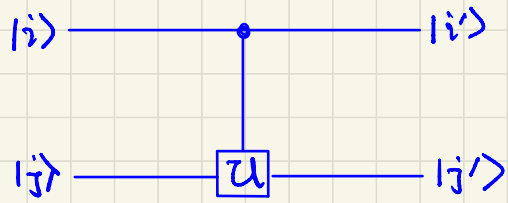
Controlled operations and gates are quite common in classical circuits. When the first qubit (say A) is $|0\rangle$, nothing changes in the second qubit (say B), which means it is operated by identity $\mathbb{I}$). On the other hand if A is $|1\rangle$ the second qubit is acted upon by some unitary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

Here qubit A is the control qubit and B is the target qubit.

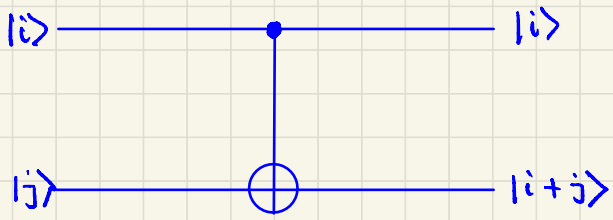
In the computational basis this can be written as follows:

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

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

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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.

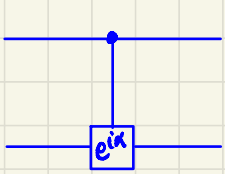
An important difference gates such as CNOT and the classical gates is reversibility. Since quantum gates are nothing but unitary operations they are reversible by definition. On the other hand two input classical gates such as XOR or even the universal NAND are not reversible i.e., given the target state one cannot say what the input states were.

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

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

$$U = \exp(i\alpha) A X B X C, \text{ where } ABC = \mathbb{I}.$$

Now, we ask can any controlled-U operator be represented using simply the CNOT and single qubit gate U above. First, let us consider the controlled-phase operation:

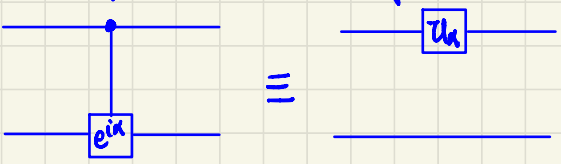


$|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$
$|10\rangle \to e^{i\alpha}|10\rangle$
$|11\rangle \to e^{i\alpha}|11\rangle$

This can also be written as follows:

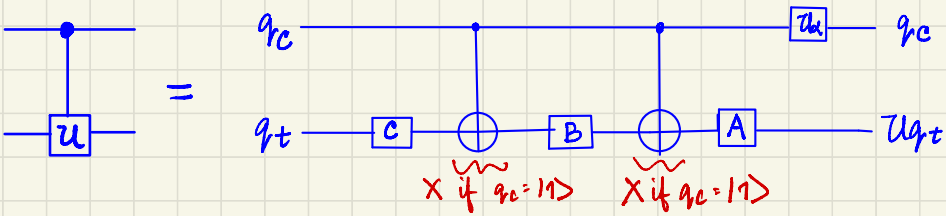
$|0, j\rangle \to |0, j\rangle$
$|1, j\rangle \to e^{i\alpha}|1, j\rangle$

So, an equivalent circuit for this is given by:



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

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:



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

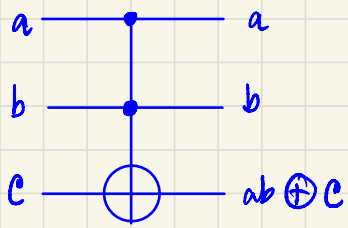
iv) Toffoli gate and multiple control qubits

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 to arise 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.,

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



So NOT acts on c iff $a = 1$ and $b = 1$

- Show that the Toffoli gate is reversible.

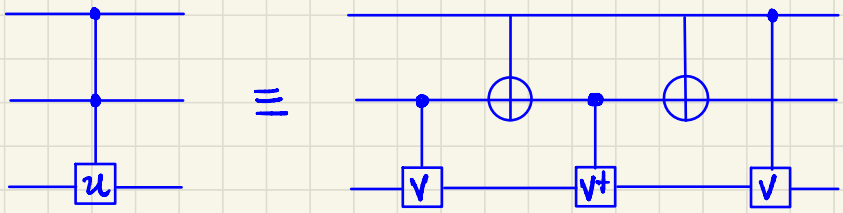
Truth table :

Input	Output
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 1
1 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, $(a=1, b=x, c=0) = (a=1, b=x, c=x)$

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

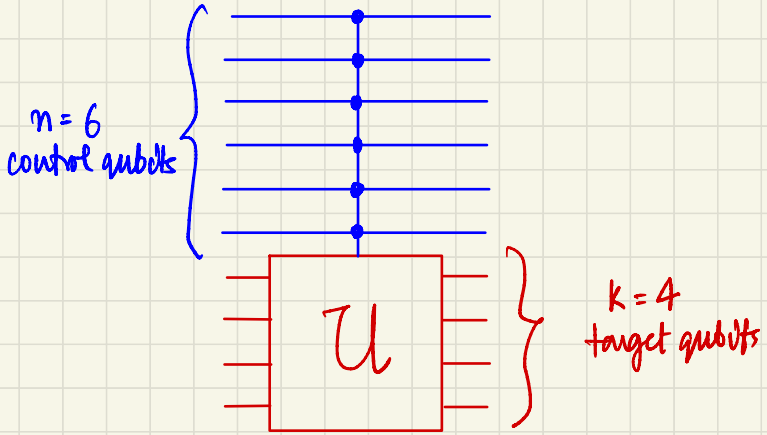


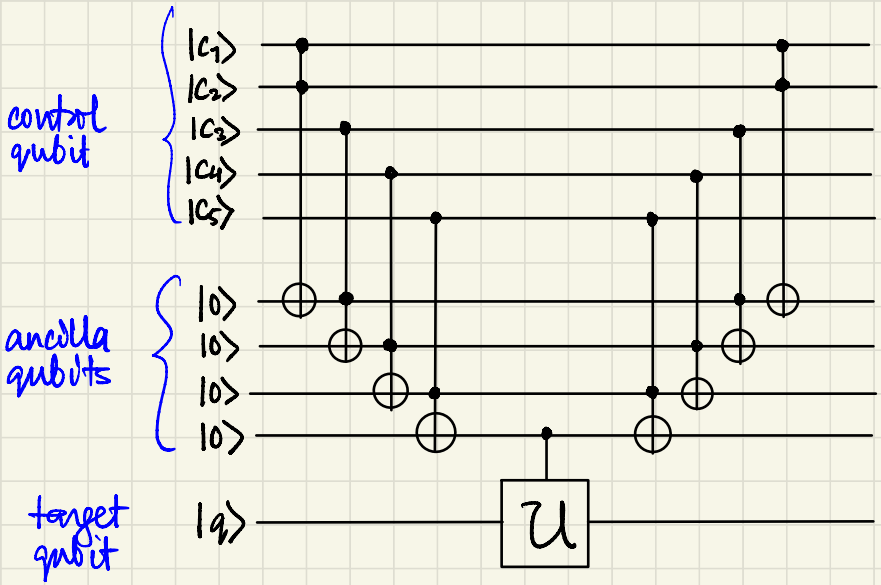
Exercise: Show the above circuit is true for unitary V, where $V^2 = \mathbb{I}$.

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

$$C^n(U)|x_1 x_2 x_3 \cdots x_n\rangle|\psi\rangle = |x_1 x_2 \cdots x_n\rangle \mathcal{U}^{x_1 x_2 \cdots x_n}|\psi\rangle$$

where $x_1 x_2 \cdots x_n$ is the product of the n bit values. This implies that $\mathcal{U}$ acts on the k-qubit $|\psi\rangle$ only if all x_i values are equal to 1 or all control qubits are set at $|1\rangle$. The circuit representation of the $n+k$ controlled unitary is given by





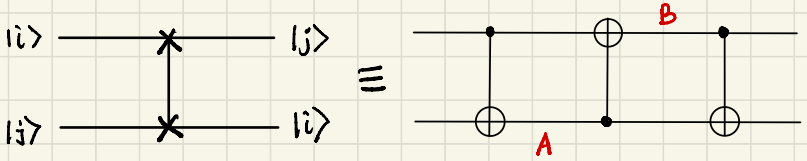
Exercise: Show that a multi qubit control, single qubit U gate ($C^5(U)$) can be implemented using a series of Toffoli gates.

An interesting conditioned 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 $|1\rangle$).

Multiple conditioned gates with two target qubits but a single control qubit.

v) Other interesting gates

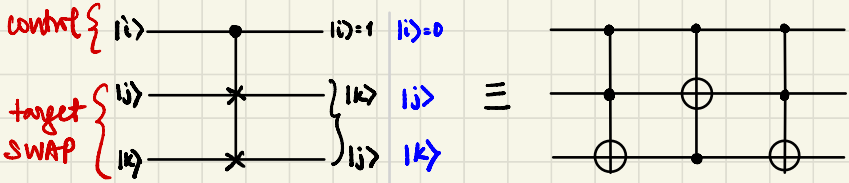
SWAP gate – A two qubit gate the swaps the inputs in the two arms of the quantum circuit.



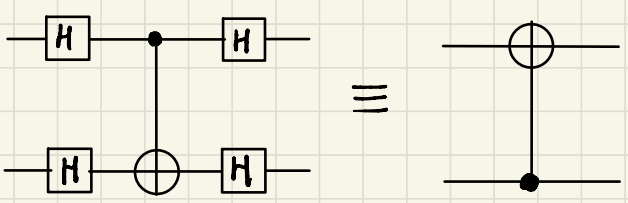
Input		A		B		Output	
|i⟩	|j⟩	|i⟩	|j⟩	|i⟩	|j⟩	|i⟩	|j⟩
0	0	0	0	0	0	0	0
0	1	0	1	1	1	1	0
1	0	1	1	0	1	0	1
1	1	1	0	1	0	1	1

$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FREDKIN gate – A three qubit controlled SWAP gate



CNOT gate in a different basis



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

$|0\rangle|0\rangle \to |0\rangle|0\rangle$; $|0\rangle|1\rangle \to |0\rangle|1\rangle$

$|1\rangle|0\rangle \to |1\rangle|1\rangle$; $|1\rangle|1\rangle \to |1\rangle|0\rangle$

In $\{|+\rangle, |-\rangle\}$ basis :

$|+\rangle|+\rangle \to |+\rangle|+\rangle$

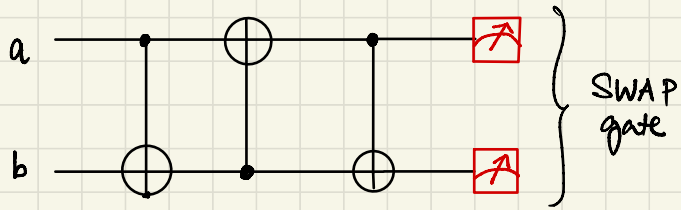
$|-\rangle|+\rangle \to |-\rangle|+\rangle$

$|+\rangle|-\rangle \to |-\rangle|-\rangle$

$|-\rangle|-\rangle \to |+\rangle|-\rangle$

vi) 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.

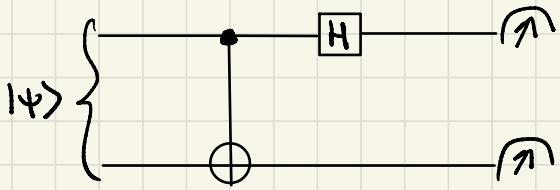


- The circuit is read (as usual) from left to right. The inputs are typically qubits in the computational basis (unless mentioned otherwise) and lines imply the passage of a qubit in time or space. All lines implicitly end in measurement.
- Quantum circuits are typically acyclic i.e., there is no feedback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

and ii) all unterminated 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 are projectors 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 Hadamard gate it becomes $|\psi\rangle = |0\rangle|0\rangle$

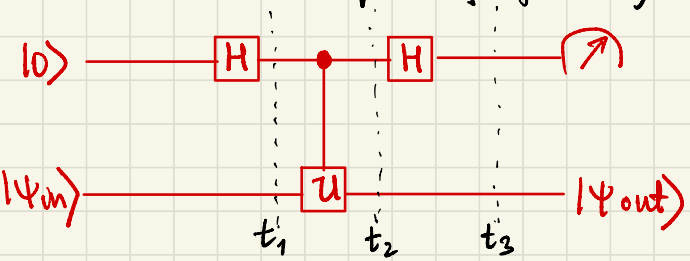
$\therefore |\psi\rangle = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}$ corresponds to measuring 0 and 0.

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

$|\psi\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\}$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}$.

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

If $\hat{O}$ is unitary → it is a gate in the circuit and since $\hat{O}$ is also Hermitian → it is also an observable (say with eigenvalues ± 1 and corresponding eigenstates)



The above circuit allows you to observe the operator $\hat{O}$ upon measurement.

Our initial state is $|0\rangle \otimes |\psi_{in}\rangle$ and at t_1 we have

At t_1 : $|0\rangle \otimes |\psi_{in}\rangle \rightarrow \frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\} \otimes |\psi_{in}\rangle$

t_2 : $\rightarrow \frac{1}{\sqrt{2}}\{|0\rangle|\psi_{in}\rangle + |1\rangle U|\psi_{in}\rangle\}$

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

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

If we measure the first qubit as $|0\rangle$, the $|\psi_{out}\rangle = (\mathbb{I}+U)|\psi_{in}\rangle$

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

eigenstate with ev +1

If first qubit is $|1\rangle$, then $|\psi_{out}\rangle = (\mathbb{I}-U)|\psi_{in}\rangle$

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

eigenstate with ev -1

vii) 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 exist — any unitary operation can be represented using a circuit with only universal gates. These are CNOT, Hadamard, T and phase gates.

The proof for the above set of gates being universal involves three key arguments. These are :

1) 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.

2) All "two-dimensional" or "two-level" unitary operators can be represented CNOT and single qubit gates.

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

We explicitly work out the statements below :

A) Two-level unitary gates are universal

Let us consider an n-dimensional unitary operator U in the Hilbert space. We can find k two-level unitaries V_i, where $k \leq n(n-1)/2$, such that $U = V_1^\dagger V_2^\dagger \dots V_k^\dagger$.

First, let us clarify what we mean by two-level unitaries. In an n-dimensional Hilbert space, a two-level unitary is one that acts on an effective 2×2 dimension. For instance, consider the Hilbert space of four qubits spanned by the computational basis

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

A two-level unitary only acts on the subspace spanned by any two of the above vectors. For instance the unitary v that acts between states $|0000\rangle$ and $|1111\rangle$ would look like,

$$v = \begin{pmatrix} a & 0 & 0 & \cdots & 0 & b \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ c & 0 & \cdots & & 0 & d \end{pmatrix}$$

effective dimension is 2×2

$$v = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Now, we use an example to show how a n-dimensional unitary can be written as a product of two-level unitary operations. Let us assume $n = 3$ and

$$U = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

We can show that there exist three two-level unitaries v_1, v_2 and v_3 such that $v_3 v_2 v_1 U = \mathbb{I}$, which implies that $U = v_1^\dagger v_2^\dagger v_3^\dagger$, where $v_1^\dagger, v_2^\dagger$ and $v_3^\dagger$ are also "two-level" unitaries that gives us the unitary U.

To find the unitaries v_1, v_2 and v_3 we need to reduce the dimensionality of U via successive matrix multiplications.

So, we choose v_1 such that the element in the first column and second row (where d is in U) is equal to zero in the product $v_1 U$.

If $d = 0$, $v_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, else $v_1 = \begin{pmatrix} a^*/N & d^*/N & 0 \\ d/N & -a/N & 0 \\ 0 & 0 & 1 \end{pmatrix}$

where $N = \sqrt{|a|^2 + |d|^2}$ ensures v_1 is unitary.

effective dimension $= 2 \times 2$

$$v_1 U = \begin{pmatrix} a^*/N & d^*/N & 0 \\ d/N & -a/N & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

the idea is to get this term to be 0.

$$= \begin{pmatrix} \frac{|a|^2+|d|^2}{N} & \frac{a^*b}{N} + \frac{d^*e}{N} & \frac{a^*c}{N} + \frac{d^*f}{N} \\ \frac{ad}{N} - \frac{ad}{N} & \frac{bd}{N} - \frac{ae}{N} & \frac{dc}{N} - \frac{af}{N} \\ g & h & i \end{pmatrix} = \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ g' & h' & i' \end{pmatrix}$$

Similarly, one can choose v_2 such that the term in first column and third row (g' in $v_1 U$) is set to zero.

If $g' = 0$, $v_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, else $v_2 = \begin{pmatrix} a'^*/N & 0 & g'^*/N \\ 0 & 1 & 0 \\ g'/N & 0 & -a'/N \end{pmatrix}$

$$v_2 v_1 U = \begin{pmatrix} a'^*/N & 0 & g'^*/N \\ 0 & 1 & 0 \\ g'/N & 0 & -a'/N \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ g' & h' & i' \end{pmatrix}$$

$$= \begin{pmatrix} \frac{|a'|^2+|g'|^2}{N} & \frac{a'^*b'}{N} + \frac{g'^*h'}{N} & \frac{a'^*c'+g'^*i'}{N} \\ d' & e' & f' \\ \frac{a'g'-a'g'}{N} & \frac{bg'-a'h'}{N} & \frac{c'g'-a'i'}{N} \end{pmatrix} = \begin{pmatrix} a'' & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & i'' \end{pmatrix}$$

Therefore, $v_2 v_1 U = \begin{pmatrix} a'' & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & i'' \end{pmatrix}$ } This matrix also has to be unitary

$$\begin{pmatrix} a''^* & 0 & 0 \\ b'' & e'' & h'' \\ c'' & f'' & i'' \end{pmatrix}\begin{pmatrix} a'' & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & i'' \end{pmatrix} = \begin{pmatrix} |a''|^2 & b_1 & c_1 \\ b''a'' & e_1 & f_1 \\ c''a'' & h_1 & i_1 \end{pmatrix} \quad \therefore a'' = 1 \text{ and } b'' = c'' = 0.$$

$v_2 v_1 U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & f'' \\ 0 & h'' & i'' \end{pmatrix}$. Now to satisfy $v_3 v_2 v_1 = \text{II}$

we finally choose $v_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & h''^* \\ 0 & f''^* & i''^* \end{pmatrix}$ and $v_3 v_2 v_1 U = \text{II}$.

Therefore, one can write $U = v_1^\dagger v_2^\dagger v_3^\dagger$, which proves the statement for any 3-dimensional unitary.

Similar to the above case, for an n-dimensional unitary we can look for n "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 $n-1$ dimensional submatrix, we can again select $n-1$ "two-level" unitaries to again set all elements (except the first) to zero.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & a'_{11} & \cdots & a'_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & a''_{11} & \cdots & a''_{1,n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & a''_{n-2,1} & \cdots & a''_{n-2,n-2} \end{pmatrix}$$

(n rows; $n-1$ rows; $n-2$ rows)

So the number of gates needed: $n-1 + n-2 + n-3 + \ldots + 1 = \frac{n(n-1)}{2}$.

B) CNOT and single qubit gates can simulate "two-level" unitary matrices.

In the previous section we showed how a product of "two-level" unitary matrices can be used to represent any arbitrary n-dimensional unitary. Now, we need to show how "two-level" unitary matrices can be represented using the universal set of quantum gates.

The central idea here is how can a "two-level" or an effective two-dimensional unitary be implemented using a quantum gate acting on a single qubit.

$$U = \begin{pmatrix} a & 0 & 0 & \cdots & 0 & b \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c & 0 & \cdots & \cdots & 0 & d \end{pmatrix} \rightarrow \hat{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

effective two-dimensional or two-level matrix

two-dimensional gate acting on a qubit

Let U be a two-level unitary matrix that acts on the subspace spanned by $|s\rangle = |s_1 s_2 s_3 \cdots s_n\rangle$ and $|t\rangle = |t_1 t_2 t_3 \cdots t_n\rangle$. In the above example we have

$|s\rangle = |00\cdots0\rangle$ and $|t\rangle = |11\cdots1\rangle$; $s_i = 0$ and $t_i = 0 \; \forall \; i$.

To implement U we make use of Gray codes, which connect the string of bits $s_1 s_2 s_3 \cdots s_n$ and $t_1 t_2 t_3 \cdots t_n$ by a sequence of strings such that any two subsequent strings are different by a single bit.

Say : $|s\rangle = |1\,0\,0\,1\,1\,0\,0\,1\rangle$ $|g_0\rangle$

$|1\,0\,0\,1\,1\,0\,0\,0\rangle$ $|g_1\rangle$

$|1\,0\,0\,1\,1\,0\,1\,0\rangle$ $|g_2\rangle$

$|1\,0\,\boxed{0}\,1\,0\,0\,1\,0\rangle$ $|g_3\rangle$

$|t\rangle = |1\,0\,\boxed{1}\,1\,0\,0\,1\,0\rangle$ $|g_4\rangle$

Gray code

So, the Gray code connects the states $|s\rangle$ and $|t\rangle$ through a series of gate operations between the states $|g_0\rangle = |s\rangle$ and $|g_m\rangle = |t\rangle$, where $m \leq n$. To implement a quantum circuit for the two-level unitary $\mathcal{U}$ we perform a series of gates that takes us from $|g_0\rangle$ to $|g_{m-1}\rangle$, i.e., $|g_0\rangle \to |g_1\rangle \to |g_2\rangle \to \ldots \to |g_{m-1}\rangle$ and then and then apply a controlled-$\hat{\mathcal{U}}$ on the last bit that differs between $|g_{m-1}\rangle$ and $|g_m\rangle$ (shown in red above). After the controlled-$\hat{\mathcal{U}}$ is applied the reverse operations takes us from $|g_{m-1}\rangle$ to $|g_0\rangle$, i.e., $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \ldots \to |g_0\rangle$.

To reiterate, we want to transform the effective two dimensional or two-level $\mathcal{U}$ to a two-level qubit gate $\hat{\mathcal{U}}$ and this is achieved by bringing $|g_0\rangle$ and $|g_m\rangle$ next to each other by transforming $|g_0\rangle \to |g_1\rangle \to |g_2\rangle \to \ldots \to |g_{m-1}\rangle$.

How can this be done ? First one applies a 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 one can SWAP $|g_1\rangle$ and $|g_2\rangle$ and repeat till the state $|g_0\rangle$ now reaches $|g_{m-1}\rangle$. So, after the series of SWAP operations the states look as shown below :

$|g_1\rangle \to |g_0\rangle$

$|g_2\rangle \to |g_1\rangle$

$|g_3\rangle \to |g_2\rangle$

$\vdots$

$|g_{m-1}\rangle \to |g_{m-2}\rangle$

$|g_0\rangle \to |g_{m-1}\rangle$

Then we apply controlled-$\hat{\mathcal{U}}$ 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.

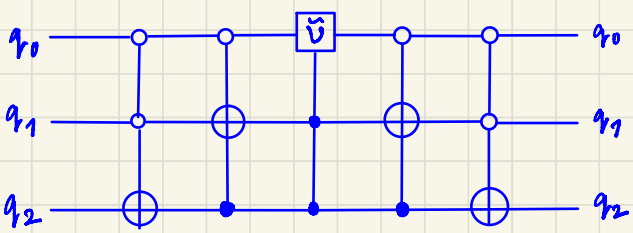
Let us consider the example we used earlier for a three qubit gate. The dimension of this gate is $2^n = 2^3 = 8$.

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

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

The gray code that connects the two-levels on which U acts is given below:

$$|S\rangle = \begin{aligned} |g_0\rangle &= |0\,0\,0\rangle \equiv |q_0\, q_1\, q_2\rangle \\ |g_1\rangle &= |0\,0\,1\rangle \\ |g_2\rangle &= |0\,1\,1\rangle \\ |g_3\rangle &= |1\,1\,1\rangle = |t\rangle \end{aligned}$$



The question now is how many gates are required to implement the above circuit for n qubits. Now, $2(n-1)$ controlled flips are needed before and after implementing the controlled $\tilde{U}$ operation. Now, from Section V, we know that each controlled operation requires $O(n)$ single qubit and CNOT gates. Therefore, $O(n^2)$ gates are needed to implement each effective "two-level" unitary gate.

For n qubits, the unitary matrix can be of the size $N = 2^n$, and we know that one needs $N(N-1)/2$ or $O(N^2)$ which is $O(4^n)$.

However, we know that $O(4^n)$ gates are required to implement an arbitrary n-qubit unitary matrix. Therefore, $O(n^2 4^n)$ single qubit gates are required to implement an arbitrary n-qubit gate.

So, all we need to show that any single qubit unitary can be implemented using a discrete set of universal states.

How/why does the Gray code work?

Let us take a closer look at the Gray code and understand how it reduces an "effective two-level" unitary to a single qubit gate, using a series of controlled gates.

Consider the example we discussed:

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

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

$$v|\psi\rangle = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \begin{matrix} \alpha_0|000\rangle \leftarrow \text{acting on these states} \\ \alpha_1|001\rangle \\ \alpha_2|010\rangle \\ \alpha_3|011\rangle \\ \alpha_4|100\rangle \\ \alpha_5|101\rangle \\ \alpha_6|110\rangle \\ \alpha_7|111\rangle \leftarrow \text{acting on these states} \end{matrix}$$

nothing happens to these 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 v is written in the computational basis $\{|i\rangle\}$ above.

Here is the Gray code →

$$\begin{aligned} |s\rangle = |g_0\rangle &= |0\,0\,0\rangle \equiv |q_0\, q_1\, q_2\rangle \\ |g_1\rangle &= |0\,0\,1\rangle \\ |g_2\rangle &= |0\,1\,1\rangle \\ |g_3\rangle &= |1\,1\,1\rangle = |t\rangle \end{aligned}$$

After the first change $|q_0\rangle \to |q_1\rangle$ i.e., $|000\rangle \to |001\rangle$

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

*See circuit below: Note that the control ensures that $|111\rangle$ does not change

After the second change $|q_1\rangle \to |q_2\rangle$ i.e., $|001\rangle \to |011\rangle$

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

Remains unchanged, so the circuit does not act on these states

So the circuit now acts only on these two states

The above matrix can be written in the operator form as

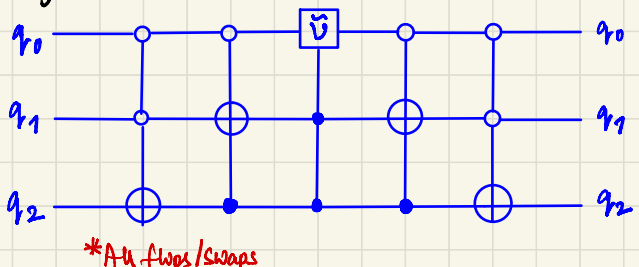
$$\text{So, } U = a|011\rangle\langle 011| + b|011\rangle\langle 111| + c|111\rangle\langle 011| + d|111\rangle\langle 111| + \sum_{|i\rangle \neq \{|011\rangle, |111\rangle\}} |i\rangle\langle i|$$

$\{$ where $\{|i\rangle\}$ is the computational basis – gives us the identity on everything else $\}$

$$= \underbrace{(a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|)}_{\text{Only acts on the qubit } q_0} \otimes \underbrace{|11\rangle\langle 11|}_{\text{Qubit } q_1 \text{ and } q_2 \text{ can then be reversed to original state}} + \sum_{|i\rangle \neq \{|011\rangle, |111\rangle\}} |i\rangle\langle i|$$

This just applies identity everywhere else

The circuit achieves that along with the Gray code – works for any n qubit system.



*All flips/swaps are controlled

* Section C below can be skipped for examination purposes.

C) Universality of Hadamard, T, phase and CNOT gates

We now show how a discrete set of universal gates can be used to implement all single qubit unitaries with sufficient accuracy. It is obvious that arbitrary gates cannot exactly be implemented using only discrete gates, but only upto some approximation. One can define an error between the target unitary U and implemented unitary V.

Consider the initial state $|\psi\rangle$, where we use the target unitary U and the implemented unitary V. Let us use a POVM measurement M with outcome m and probability p_u and p_v, for the output state $U|\psi\rangle$ and $V|\psi\rangle$. Also, let $|\varepsilon\rangle = (U-V)|\psi\rangle$ and define the error as : $\varepsilon_{u,v} = \max_{\{|\psi\rangle\}} \| (U-V)|\psi\rangle \|$, where $\|\cdot\|$ is the norm.

Now;
$$
\begin{aligned}
|p_u - p_v| &= |\langle\psi|U^\dagger M U|\psi\rangle - \langle\psi|V^\dagger M V|\psi\rangle| \\
&= |\langle\psi|U^\dagger M|\varepsilon\rangle + \langle\psi|U^\dagger M V|\psi\rangle \\
&+ \langle\varepsilon|MV|\psi\rangle - \langle\psi|U^\dagger MV|\psi\rangle| \\
&\leq |\langle\psi|U^\dagger M|\varepsilon\rangle| + |\langle\varepsilon|MV|\psi\rangle| \\
&\leq \||\varepsilon\rangle\| + \||\varepsilon\rangle\| = 2\varepsilon_{u,v}
\end{aligned}
$$

Using the Cauchy Schwarz inequality :
$|\langle\psi|U^\dagger M|\varepsilon\rangle| \leq \|\underbrace{U|\psi\rangle}_{=1}\| \cdot \|M|\varepsilon\rangle\| = \||\varepsilon\rangle\|$

So, one can in principal approximate U with V such that a POVM gives you a difference in probability that is very small.

- Single qubit gates (Hadamard, phase, T) and CNOT gates

The T gate allows for rotation by $\pi/4$ (upto a global phase) around the z-axis, whereas the HTH is a rotation by $\pi/4$ around the x-axis. (Exercise : Show $HZH = X$)

The two operations can be combined and up to an overall phase

gives us the following rotation (see previous section on rotation):

$$e^{-i\pi/8 Z} \cdot e^{-i\pi/8 X} = \left(\cos\frac{\pi}{8}\,\mathbb{1} - i\sin\frac{\pi}{8} Z\right)\left(\cos\frac{\pi}{8}\,\mathbb{1} - i\sin\frac{\pi}{8} X\right)$$

$$= \cos^2\frac{\pi}{8}\,\mathbb{1} - i\left[\cos\frac{\pi}{8}(Z+X) + \sin\frac{\pi}{8} Y\right]\sin\frac{\pi}{8}$$

Exercise: Prove that the above is rotation about the axis $\vec{n} = (\cos\pi/8, \sin\pi/8, \cos\pi/8)$ and an angle θ, such that $\cos(\theta/2) \equiv \cos^2\pi/8$.

Now repeated application of $R_n(\theta)$ can be used to approximate an arbitrary $R_n(\alpha)$ with considerable accuracy. Now θ is known to be an irrational multiple of 2π. Therefore for any accuracy $\epsilon > 0$, one can find an integer $N \geq 2\pi/\epsilon$. Now, let $\theta_k \in [0, 2\pi)$ and $\theta_k = k\theta \bmod 2\pi$. Now, there will exist distinct j and k in the range of natural numbers 1 to N, such that $|\theta_k - \theta_j| \leq 2\pi/N < \epsilon$. This implies that there is $k' = k - j$, such that $|\theta_{k-j}| < \epsilon \neq 0$. It follows that for any $\delta > 0$ there exists an n such that

$$\mathcal{E}(R_n(\alpha), R_n(\theta)^n) < \delta/3.$$

Now from the discussions in Section (ii) it can be shown that any arbitrary unitary (up to a global phase) can be written as:

$$U = R_n(\beta)\, R_m(\gamma)\, R_n(\delta)$$

Consider the rotation $R_n(\alpha)$. Upon applying the Hadamard we get, $H R_n(\alpha) H = R_m(\alpha)$, where m is a vector along $(\cos\pi/8, -\sin\pi/8, \cos\pi/8)$, which also gives us

$$\mathcal{E}(R_m(\alpha), R_m(\theta)^n) < \delta/3$$

Using the two equations above and integers n_1, n_2 and n_3 we get,

$$\mathcal{E}(U, R_n(\theta)^{n_1} H R_n(\theta)^{n_2} H R_n(\theta)^{n_3}) < \delta.$$

Therefore, any single qubit unitary operator U can be approximated using Hadamard and T gates for an arbitrary $\delta > 0$.

To approximate a single qubit unitary to accuracy δ, one needs at least $2^{1/\delta}$ gates from the discrete set and therefore to approximate an m gate circuit one needs $m\,2^{m/\delta}$ gates. However, the rate of convergence upon multiple application of rotations is much better than the exponential growth and intuitively this scales as $1/\delta$ for a single qubit gate and m^2/δ for an m gate circuit, which is quadratic over the circuit size m.

Remarkably, the rate of convergence is much faster. The Solovay - Kitaev theorem implies that an arbitrary single qubit gate may be approximated to an accuracy δ using $O(\log^c(1/\delta))$ gates where $c \approx 2$. Therefore, the theorem states that to approximate a circuit containing m CNOTs and single qubit unitaries to an accuracy δ requires $O(m \log^c(m/\delta))$ gates from the discrete set of universal gates, i.e., the Hadamard, phase, CNOT and T gates.