

1. Background

Qubits are represented by $|\psi\rangle$, and are defined by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Here, the probability that the qubit is in the $|0\rangle$ state is given by $|\alpha|^2$ and vice versa for $|1\rangle$.

Once a qubit has been measured, the system remains in its measured state, and will always yield the same value, unless some quantum operation has been applied to the qubit - fundamentally, only 1 bit of information can be extracted from the qubit.

It helps to understand that while several values of α, β correspond to the same probabilities of $|0\rangle$ and $|1\rangle$, they refer fundamentally to different states, and will evolve differently. We note the following special states:

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

2 Linear Algebra

2.1 Vector Spaces

Vector spaces need not be vectors. Instead, they can be generalised to the following: A set V is a vector space over \mathbb{K} if:

Addition: If u and v are elements of V then so is $u + v$. This addition must be associative.

Scaling: If u is an element of V , and α is an element of \mathbb{K} , then so is αu . This scaling is distributive.

This gives us a couple of properties:

1. Other mathematical structures can also be a vector space. For instance, the set of all polynomials with complex coefficients of degree 2 are vector spaces over \mathbb{C} .
2. There are also more properties to be checked before deciding if said set is a vector field, but this is often sufficient.

2.2 Relevance to Quantum Computing

States of a quantum system form a vector space and their transformations are described by linear operators. A finite dimension vector space, with a defined inner product (read dot product) is known as a Hilbert space.

2.3 Tensor Multiplication

We can define tensor multiplication on matrices:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{bmatrix}$$

where \otimes denotes the tensor product. For example:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 & 6 \end{bmatrix}$$

In this case, if A is $n \times m$ and B is $a \times b$ then $A \otimes B$ will be $naxmb$.

We further find that the following is true:

$$(A \otimes B)(x \otimes y) = Ax \otimes By$$

given the appropriate dimensions.

2.4 Adjoint / Conjugate Transpose of a Matrix

Adjoint matrix is defined as the conjugate transpose. That is:

$$A^\dagger = (A^*)^T$$

2.5 Unitary and Hermaitan Matrices

Unitary Matrices are defined as such:

$$U^\dagger U = I$$

In other words, U^\dagger is the inverse of U , and the magnitude of the vector remains the same.

Importance: because quantum gates merely rotate / flip a vector, so they must be invertible, so we need our matrices to be unitary.

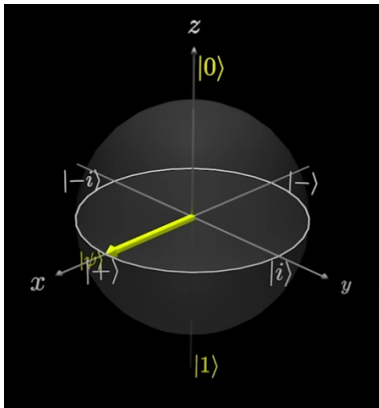
Hermaitan Matrices are defined as:

$$H^\dagger = H$$

3 Quantum Computing Gates

3.1 X, Y, Z Gates

We first note that qubits are often represented in the Bloch Sphere. We define a X, Y, Z axis, and the qubit to be the points on the surface of a unit sphere. Then, along the Z axis, at -1 , we have $|1\rangle$ and at 1 we have $|0\rangle$.



Apparently, the ‘phase’ around the z-axis that the qubit is pointed at is dependent only on the value of β . This is because we consider 2 types of phase: General phase, given by

$$e^{i\phi}(\alpha |0\rangle + \beta |1\rangle)$$

and relative phase

$$\alpha |0\rangle + e^{i\phi}\beta |1\rangle$$

Apparently, general phase is something that is generally not really that important, and we want to consider relative phase in most cases. In general, if both $|0\rangle$ and $|1\rangle$ have some phase associated with it, we can factorise out one of them as a global phase, and ‘discard’ it, leaving us with just the relative phase of one of $|0\rangle$ or $|1\rangle$

We now consider the X, Y, Z gates. They are defined as:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

3.2 Hadamard Gate

We further note the existence of the H gate:

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

The effect of this gate on $|1\rangle$ is to transform it to $|-\rangle$ and for $|0\rangle$ to $|+\rangle$.

3.3 S and T gates

We note the following gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\frac{\pi}{2})} \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\frac{\pi}{4})} \end{pmatrix}$$

The adjoint matrix of these 2 gates are its inverse, and their effect is to add a relative phase of 90 and 45 degrees respectively

3.4 Representing multiple qubits, and operations

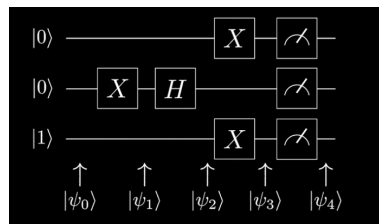
We represent qubits by their tensor product. In other words, we represent the 2 qubits:

$$|00\rangle = |0\rangle \otimes |0\rangle$$

This can be done for any number of qubits. When given 2 arbitrary qubits that are tensor product-ed together, we can expand and write it in the general form. For instance,

$$\alpha |00\rangle + \alpha' |01\rangle + \beta |10\rangle + \beta' |11\rangle$$

Furthermore, we can represent our manipulations to qubits as follows:



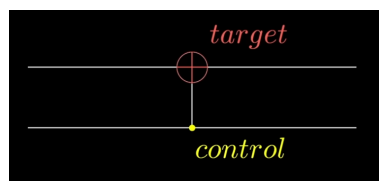
In this case, we will be able to see that the final state is given by:

$$\psi_3 = \frac{1}{\sqrt{2}} (|100\rangle - |110\rangle)$$

so we see that the final state is either of the 2 above states, and measuring the qubits will result in the qubit collapsing into one of the 2 states.

3.5 CNOT, Toffoli

CNOT gates takes one gate as input and manipulates another gate. It applies an X gate to the target qubit if the control qubit is 1, and does nothing otherwise.

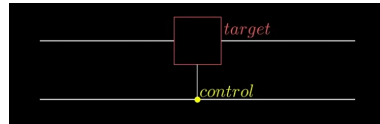


$$\begin{aligned} & CNOT \left(\frac{\sqrt{3}}{4} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle + \frac{1}{4} |11\rangle \right) \\ &= \frac{\sqrt{3}}{4} CNOT |00\rangle + \frac{1}{2} CNOT |01\rangle + \frac{1}{\sqrt{2}} CNOT |10\rangle + \frac{1}{4} CNOT |11\rangle \\ &= \frac{\sqrt{3}}{4} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{\sqrt{2}} |11\rangle + \frac{1}{4} |10\rangle \\ &= \frac{\sqrt{3}}{4} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{4} |10\rangle + \frac{1}{\sqrt{2}} |11\rangle \end{aligned}$$

1st qubit is the **control** 2nd qubit is the **target**

Toffoli Gates operate with 2 control (read input) gates, and 1 target, rather than just 1 control, and require both control bits to be 1 to apply an X-gate to the target qubit.

We can further generalise this to the other existingly known gates; we can have controlled Y, Z, S, T and H gates, giving us some level of conditional logic to be applied.



We represent this in general as seen above.

3.6 Measuring singular qubits

In general, with multiple qubits that are manipulated, the probability of a singular qubit being something in the sum of squares of probabilities of that qubit being the stated value (with all other possible combination of other qubits.)

When we actually measure a given qubit, the state collapses, and we need to normalise the probabilities (just do the obvious, multiple all probabilities by a normalisation constant, and make sure this satisfies that the total probability is 1).

4 Quantum Mechanics

4.1 Entanglement

A state is entangled if it cannot be factored into the tensor product of individual qubits. In other words, qubits depend on each other, and measuring one will determine the others.

Maximally entanglement: If measurement of one of the qubit determines the state of the other qubits

Partially entangled: Measuring one of the qubits affects the amplitudes of the other qubits (i.e. measuring one changes the probability of the other).

Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

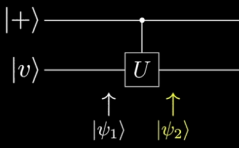
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

4.2 Phase Kickback

In some control circumstances, the control qubit might be affected rather than the target qubit. This seems to happen in the case where the target qubit is a eigenvector of the gate.

$|v\rangle$ is an **eigenvector** of U

$$U|v\rangle = e^{i\theta}|v\rangle$$


$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta} |1\rangle \right) |v\rangle$$

If we have a state $|v\rangle$ that is an **eigenvector** of a gate U , by apply a **controlled- U** gate with $|v\rangle$ as the target, we can 'kick' the phase onto the control qubit

4.3 A simple quantum algorithm

Suppose we want to send 2 bits of information by sending on bit. One might do this by entangling 2 states first. If we each take 1 bit, I can perform operations on one qubit, and send it to you. Then, you might be able to perform a step of operations, to get the message I am trying to send.

Superdense Coding

Alice \Rightarrow **Bob**

Alice wants to send 00: Does nothing, Qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice wants to send 01: Applies X to her qubit, Qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$

Alice wants to send 10: Applies Z to her qubit, Qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

Alice wants to send 11: Applies X, Z to her qubit, Qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$

Then Alice sends her qubit to Bob so he now has both

Superdense Coding

Alice \Rightarrow **Bob**

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{H} H|+\rangle|0\rangle = |00\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \xrightarrow{H} H|+\rangle|1\rangle = |01\rangle$$

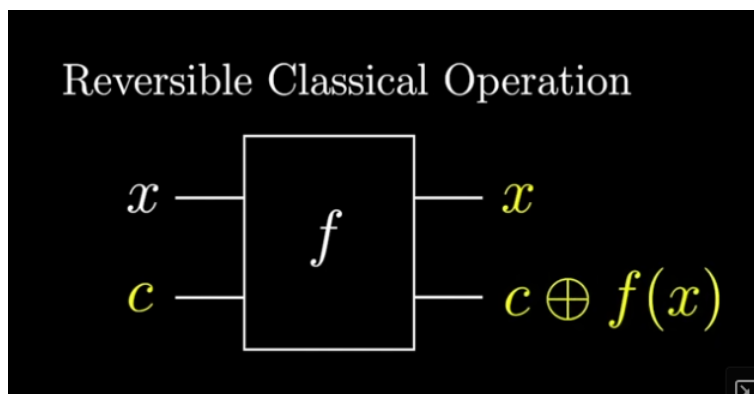
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \xrightarrow{H} H|-\rangle|0\rangle = |10\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|11\rangle - |01\rangle) \xrightarrow{H} H|-\rangle|1\rangle = |11\rangle$$

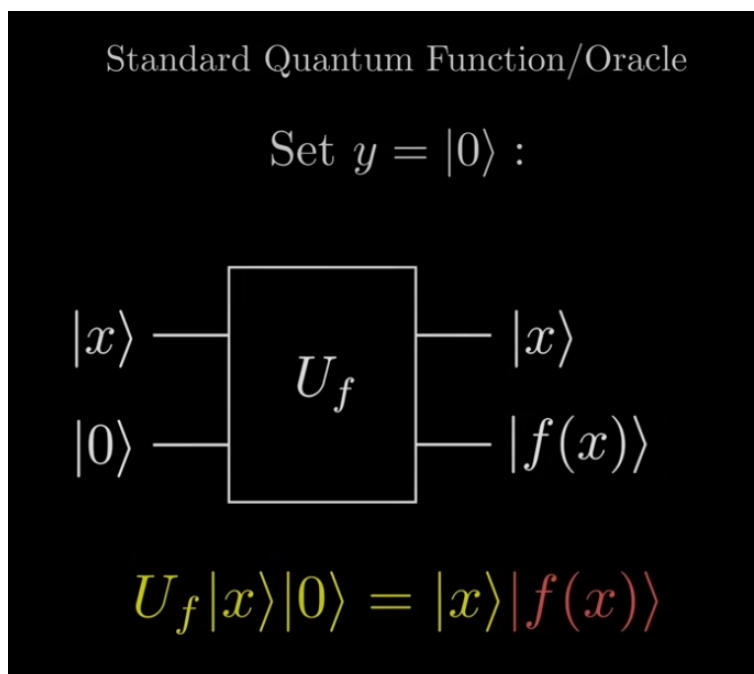
4.4 Functions on Quantum Computers

In general for our classical operations, they are not reversible. In other words, when performing the operation, we usually cannot obtain the input information from just the output information. We often need more information.

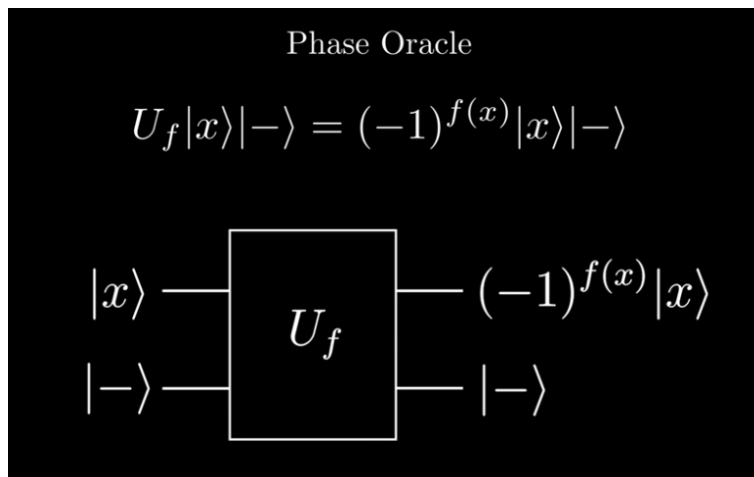
One way that we can help this is by having some control bit c , which we XOR with the output of the function f . If we do this with 0, this just returns our output $f(x)$, and if we also output our input bits, we know for certain what our input was.



We can employ such a strategy to the quantum functions, which as earlier stated due to the unitary nature of the functions, must be reversible. We want to input as the control qubit as $|0\rangle$ so we just get $f(x)$ out.

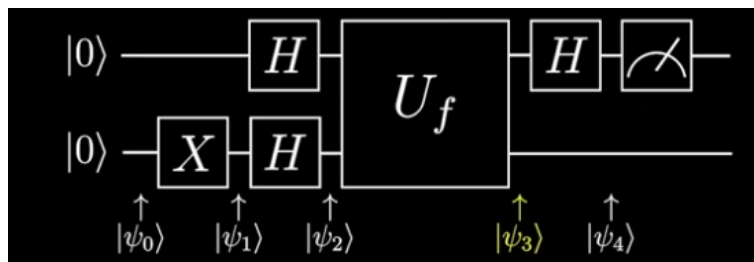


Another special case we might note is if we had instead input the output bit as $|-\rangle$ instead. Our outputs will consist of our input $|x\rangle$ having a phase change, known as a phase oracle.

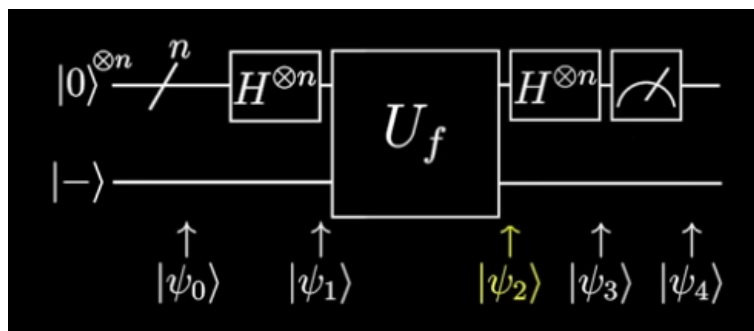


4.5 Deutsch's Algorithm

This algorithm serves to determine if a function is a constant function (in this case, alternative is a 'balanced' function). In classical computers, we have to use 2 inputs, to compare them, but quantum computers allow us to do this once only.



This can be generalised with this other algorithm:



This pattern of applying the H gate, then the function, and the H gate again seems to be a common theme in a lot of algorithms.

What turns out to be really important in these calculations is these 2 identities. In other words, how to apply the H gate to some arbitrary bit string (read: some number of qubits)

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$