General Introduction to Spooky Quantum Witchcraft

Presented by Elijah Burns

General overview

- General description of quantum computer and how they differ from classical computers
- Representing & manipulating quantum computational systems
- Example algorithm & quantum runtime improvements
- Potential future applications & theoretical capabilities

My Credentials:

What are quantum computers:

- Classical computation relies on binary bits which are either 1 or 0
- Quantum computers use qubits (quantum bits) which can be 1, 0 or a super position of the 2.
- In addition to superposition, qubits can make use of the quantum properties of entanglement and interference.
- For simplicity, we'll be using Dirac notation and matrix notation to represent systems of qubits going forward.

Superposition:

- Qubits can be 0, 1 or a superposition of the 2 with probability coefficients α & β corresponding to the likely hood that they will collapse to either 0 or 1.
- Example qubits:
- $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ => 100% probability to collapse to 0
- $\begin{pmatrix} 0 \\ -1 \end{pmatrix}$ => 100% probability to collapse to 1
- $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ => 50% probability to collapse to 0, 50% probability to collapse to 1
- $\begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$ => 25% probability to collapse to 0, 75% probability to collapse to 1
- $\begin{pmatrix} \frac{i}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$ => 25% probability to collapse to 0, 75% probability to collapse to 1

Dirac & Matrix Notation

- Dirac notation (Bra-Ket notation) is used to represent quantum systems as a sum of probability states.
- $|\Psi\rangle$ is used to denote a quantum wave function Ψ.
- $\{|\Psi\rangle = \alpha_1 |\Psi_1\rangle + \cdots + \alpha_n |\Psi_n\rangle \mid ||\alpha_1||^2 + \cdots + ||\alpha_n||^2 = 1\}$
- This can also be used to represent classical bit states $|0\rangle$ & $|1\rangle$.
- For a single qubit with possible states $|0\rangle$ & $|1\rangle$ we can denote the system as:
- $\{|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \mid ||\alpha||^2 + ||\beta||^2 = 1\}$
- The same qubit $|\Psi\rangle$ can also be represented as a vector with elements α and β:
- $|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

Representing Multi-Qubit Systems

- A system of multiple qubits can be represented by taking the tensor product of multiple qubit states:

$$|\Psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}$$

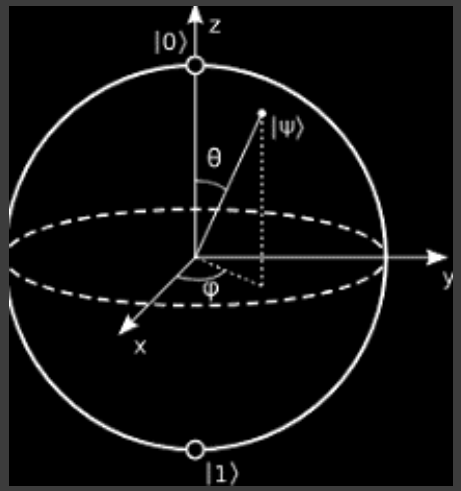
$$|\Psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle = \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}$$

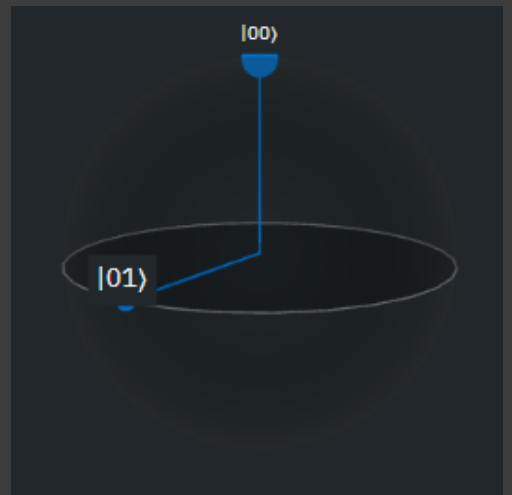
$$|\Psi_{12}\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\\ \beta_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix} \Rightarrow \begin{matrix}|00\rangle\\ |01\rangle\\ |10\rangle\\ |11\rangle\end{matrix}$$

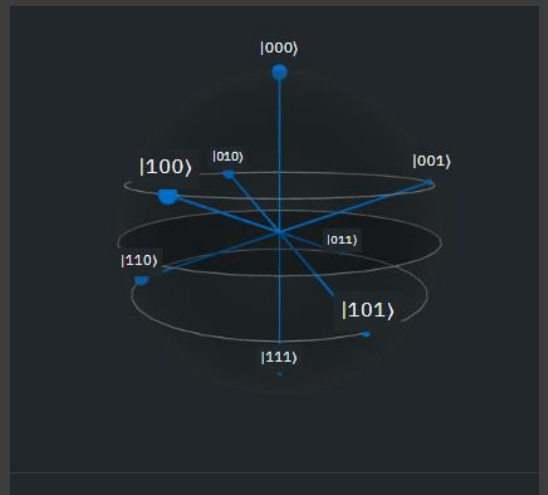
$$|011\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = \begin{pmatrix}1\\ 0\end{pmatrix} \otimes \begin{pmatrix}0\\ 1\end{pmatrix} \otimes \begin{pmatrix}0\\ 1\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}0\begin{pmatrix}0\\ 1\end{pmatrix}\\ 1\begin{pmatrix}0\\ 1\end{pmatrix}\end{pmatrix}\\ 0\begin{pmatrix}0\begin{pmatrix}0\\ 1\end{pmatrix}\\ 1\begin{pmatrix}0\\ 1\end{pmatrix}\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\ 0\\ 0\\ 1\\ 0\\ 0\\ 0\\ 0\end{pmatrix} \Rightarrow \begin{matrix}|000\rangle\\ |001\rangle\\ |010\rangle\\ |011\rangle\\ |100\rangle\\ |101\rangle\\ |110\rangle\\ |111\rangle\end{matrix}$$

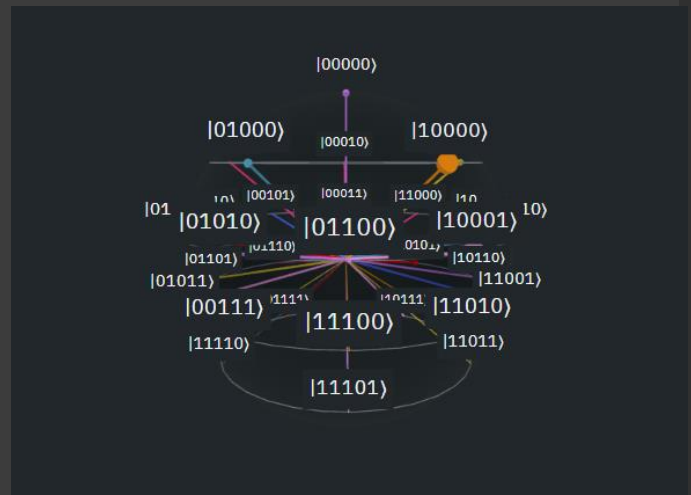
Inner Product and Hilbert Spaces:

- These vectors exist in an inner product space that is restricted and defined by the fact that the squares of all elements must equal 1 (the total probability of something happening must be 1) $\{ ||\alpha_1||^2 + \cdots + ||\alpha_n||^2 = 1 \}$
- In particular, qubits exist in an inner product space known as a Hilbert space whose elements can be infinitely dimensional.
- This allows us to represent multi qubit states in the same vector space, something that becomes especially useful when dealing with entangled qubits.
- This space can be represented geometrically (visually) with a Bloch sphere:









Bit & Qubit Operations

- The four classical single bit operations are identity, negation, constant 0 and constant 1:

$$\text{Identity: } \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \text{ Negation } \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \text{ Constant 0 } \begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}, \text{ Constant 1 } \begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}$$

$$|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix} \Rightarrow negation \Rightarrow X\left(\begin{pmatrix}1\\ 0\end{pmatrix}\right) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix}$$

- Quantum computers can only make use of reversible operations that are their own inverse so the only one we really care about above is negation represented by X:

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

$$\mathrm{X}(|\psi\rangle) = \mathrm{X}\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right) \Rightarrow \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$$

$$\mathrm{X}(\mathrm{X}(|\psi\rangle)) = \mathrm{X}\left(\mathrm{X}\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right)\right) \Rightarrow \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

Hadamard Gate:

- To drop a qubit into equal superposition (equal chance to collapse to $|0\rangle$ or $|1\rangle$) from either the $|0\rangle$ or $|1\rangle$ state you can pass it through the Hadamard gate:

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

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

- Because all quantum operators are also their own inverses this can also take a qubit in equal superposition out of superposition:

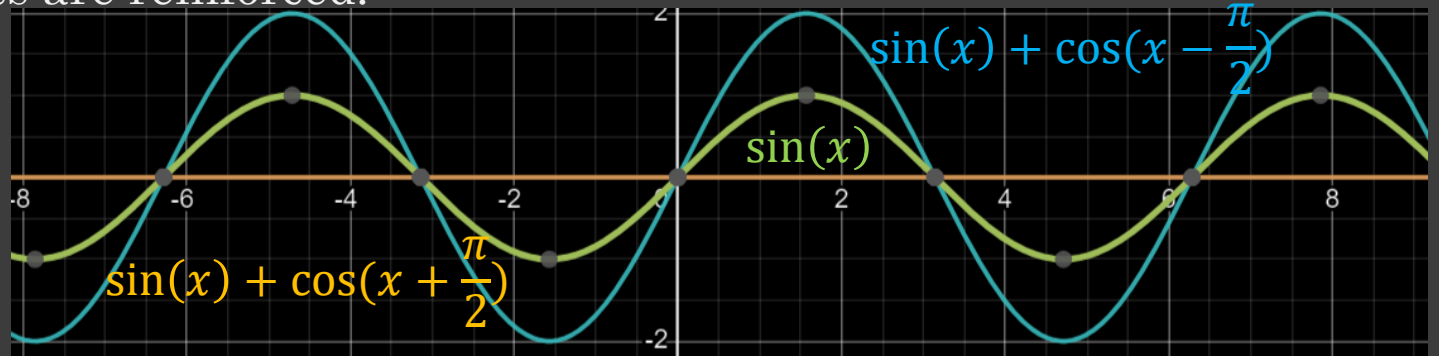
$$H(|\psi\rangle) = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$$

Phase shift:

- We can use phase shift gates like the RX and RZ gates to enact a change to the phase angle of a qubit (complex component):
- RX rotates a single qubit an angle theta about the x-axis, and RZ rotates a qubit an angle theta about the z-axis:

$$RX(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -isin\left(\frac{\theta}{2}\right) \\ -isin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}, RZ(\theta) = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$$

- This allows us to make use of interference within quantum algorithms, allowing unfavorable results to cancel with each other while the desired results are reinforced:



Entanglement:

- We can make the probability state of one qubit dependent on another, correlating their states that they will collapse to when measured.
- This correlation can remain present across vast distances and allowing for faster than light coordination but not communication.
- Mathematically 2 qubits are entangled if they cannot be factored into individual qubit states from the tensored product state:

$$\text{Ex. } |\psi\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}$$

$$\alpha_1\alpha_2 = 0$$

$$\alpha_1\beta_2 = \frac{1}{\sqrt{2}}$$

$$\beta_1\alpha_2 = -\frac{1}{\sqrt{2}}$$

$$\beta_1\beta_2 = 0$$

Entangling Qubits with the Controlled Not Gate (Cnot)

- The CNOT gate operates on 2 bits (or qubits) with one acting as the control bit and one acting as the target bit.
- If the control bit is in state 1, it will negate the target bit, however if the control bit is in state 0 it will leave the target bit as is.

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

$$C(|00\rangle) = |00\rangle \, , \, C(|01\rangle) = |01\rangle$$

$$C(|10\rangle) = |11\rangle \, , \, C(|11\rangle) = |10\rangle$$

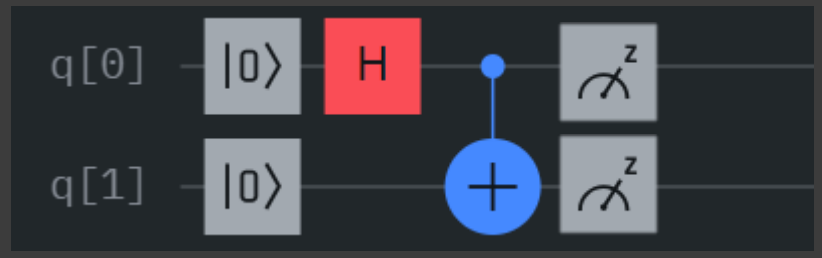
- This allows us to make the state of the target qubit dependent on the state of the control qubit, and if the control qubit is in superposition, then the state of target becomes directly tied to outcome of measuring the control.

Cnot continued & quantum circuit notation:

- If we take 2 qubits in the $|0\rangle$ state and set one (the control) into an equal superposition with the Hadamard gate, we can then pass them both through the Cnot gate causing them to become entangled:

$$C(H(|0\rangle) \otimes |0\rangle) = C\left(\begin{pmatrix} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} \\ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix}\right) = C\left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

- We can also represent this operation using quantum circuit notation for simplicity:

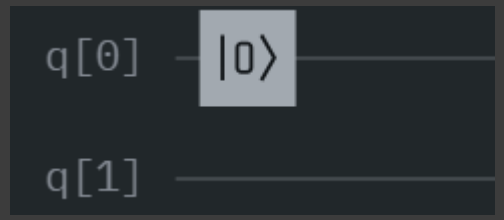


Non-reversible operations:

- Revisiting the four classical bit operators, two were non-reversible operations (constant-0 and constant-1).
- To get around this, input and output qubits are used, allowing us to preserve information while performing the same non-reversible operation:
- Example (constant 0):

Output:

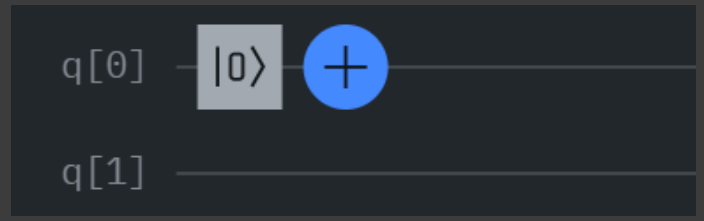
Input:



- No matter what is passed to it in the input qubit, the output qubit will always be |0⟩.
- Constant 1:

Output:

Input:

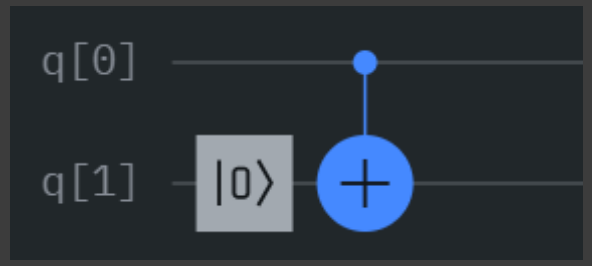


Identity and Negation using input and output bits:

- Identity:

Input:

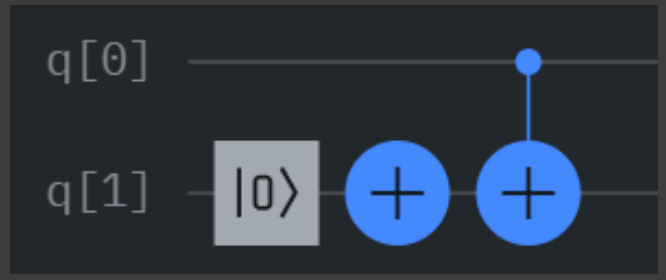
Output:



Negation:

Input:

Output:



Simplest quantum runtime improvement (Deutsch Oracle):

- Imagine you have a black box that performs one of the four bit operations.
- How many queries would it take a classical computer to determine which of the bit operations was performed? How about a quantum computer?
- Both a classical computer and quantum computer require 2 queries because 2 bits of information are required to specify one of four possible states.
- Now consider a different problem, how many queries would it take to simply determine if the operator in the black box was balanced (identity, negation) or constant (constant 0, constant 1)?
- With this problem, there are only 2 outcomes and thus, only 1 bit of information is required to distinguish between the possible outcomes.
- Because of this, a quantum computer can determine whether it was a constant or balanced function in only a single query.

Deutsch Oracle continued:

- To break down the problem it is important to determine what exactly sets constant and balanced functions apart in this context:

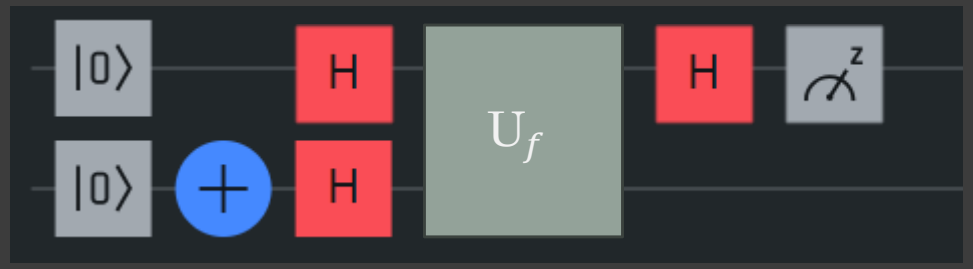
$$\text{Constant: } f(0) = f(1) \text{ , Balanced: } f(0) \neq f(1)$$

- The general approach to solving this is to pass a qubit (technically 2 to keep things reversible) in equal superposition through the black box (represented by the function U_f) and before measurement, compare the probability states of the out put qubit:

- As a quantum circuit this is what that looks like:

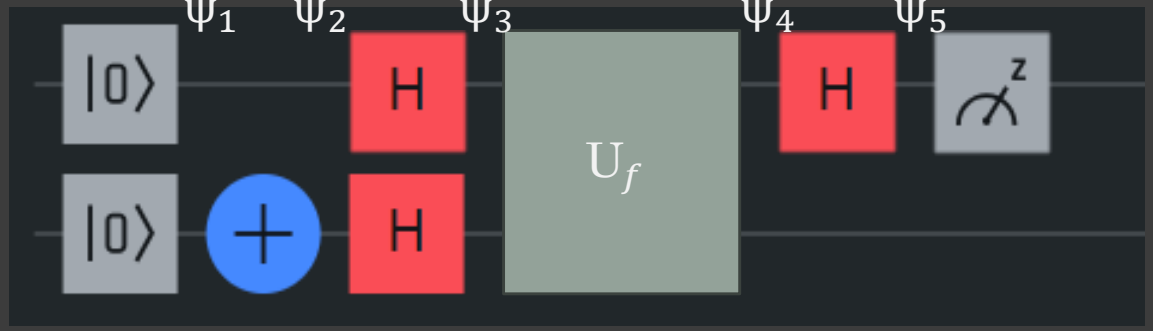
Output:

Input:



Output:

Input:



$$|\psi_1\rangle = |00\rangle \Rightarrow |\psi_2\rangle = |01\rangle$$

$|\psi_3\rangle = |+-\rangle$ ($|+\rangle$ represents H($|0\rangle$) while $|-\rangle$ represents H($|1\rangle$))

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle)$$

$$|\psi_4\rangle = U(|\psi_3\rangle) = \frac{1}{\sqrt{2}}(U(|0\rangle)|-\rangle + U(|1\rangle)|-\rangle)$$

$$|\psi_4\rangle = U(|\psi_3\rangle) = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle$$

- Considering our 2 possible cases; Constant: f(0) = f(1) , Balanced: f(0) ≠ f(1):

$$(-1)^{f(0)} = (-1)^{f(1)} = \pm 1 \Rightarrow |\psi_4\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \pm|+\rangle$$

$$(-1)^{f(0)} = \pm 1 = -(-1)^{f(1)} = -(\mp 1) \Rightarrow |\psi_4\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \pm|-\rangle$$

Constant: $|\psi_5\rangle = \pm H(|\psi_4\rangle) = \pm H(|+\rangle) = \pm|0\rangle$

Balanced: $|\psi_5\rangle = \pm H(|\psi_4\rangle) = \pm H(|-\rangle) = \pm|1\rangle$

Other Quantum Algorithms & Future Capabilities:

- Grover's algorithm, also known as the quantum search algorithm, allows you to search an array in $O(\sqrt{N})$ as a pose to the traditional O(N) run time on a classical computer.
- Shor's algorithm allows you to find the prime factors of extremely large integers in O(log(N)) as a pose to O(N).
- Prime factorization of large integers is very difficult for classical computers which is why it is the backbone of modern data encryption.
- It would take a classical computer somewhere in the range of 300 trillion years to break a 2048-bit rsa private key while a quantum computer with a few million qubits cold break it in a matter of hours.
- A sufficiently large quantum computer would revolutionize our ability to simulate quantum phenomena.
- It would also allow us to develop drugs much faster, potentially allowing us to create personalized treatments in a matter of hours rather than decades.