The Basics of Quantum Computing

Tyler Burkett


You don't need
Quantum Physics
to do Quantum
Computation
CHANGE MY MIND

What is a Qubit?

- Based on some quantum system with a binary set of states when measured
- Can store 0 and 1 like a regular bit
- Can also be in a *superposition* of 0 and 1
- Measuring a qubit causes it to *collapse* into either a 0 or 1 if its in a superposition

Dirac (Bra-Ket) Notation

Ket

$$|\phi\rangle = \begin{bmatrix} \alpha \\ \beta \\ \vdots \end{bmatrix}$$

Bra

$$\mathbb{R}^N \colon \langle\phi| = |\phi\rangle^T = [\alpha \quad \beta \quad \cdots]$$

$$\mathbb{C}^N \colon \langle\phi| = |\phi\rangle^\dagger = [\alpha^* \quad \beta^* \quad \cdots]$$

Dirac (Bra-Ket) Notation

Inner Product

$$\langle \phi' | \phi \rangle = \begin{bmatrix} \alpha'^* & \beta'^* & \cdots \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \vdots \end{bmatrix} = \alpha'^* \alpha + \beta'^* \beta + \cdots$$

Outer Product

$$|\phi\rangle\langle\phi'| = \begin{bmatrix} \alpha \\ \beta \\ \vdots \end{bmatrix} \begin{bmatrix} \alpha'^* & \beta'^* & \cdots \end{bmatrix} = \begin{bmatrix} \alpha\alpha'^* & \alpha\beta'^* & \cdots \\ \beta\alpha'^* & \beta\beta'^* & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}$$

Tensor Product

$$|\phi\rangle|\phi'\rangle = |\phi\phi'\rangle = \begin{bmatrix} \alpha \\ \beta \\ \vdots \end{bmatrix} \otimes \begin{bmatrix} \alpha' \\ \beta' \\ \vdots \end{bmatrix} = \begin{bmatrix} \alpha\alpha' \\ \alpha\beta' \\ \beta\alpha' \\ \beta\beta' \\ \vdots \end{bmatrix}$$

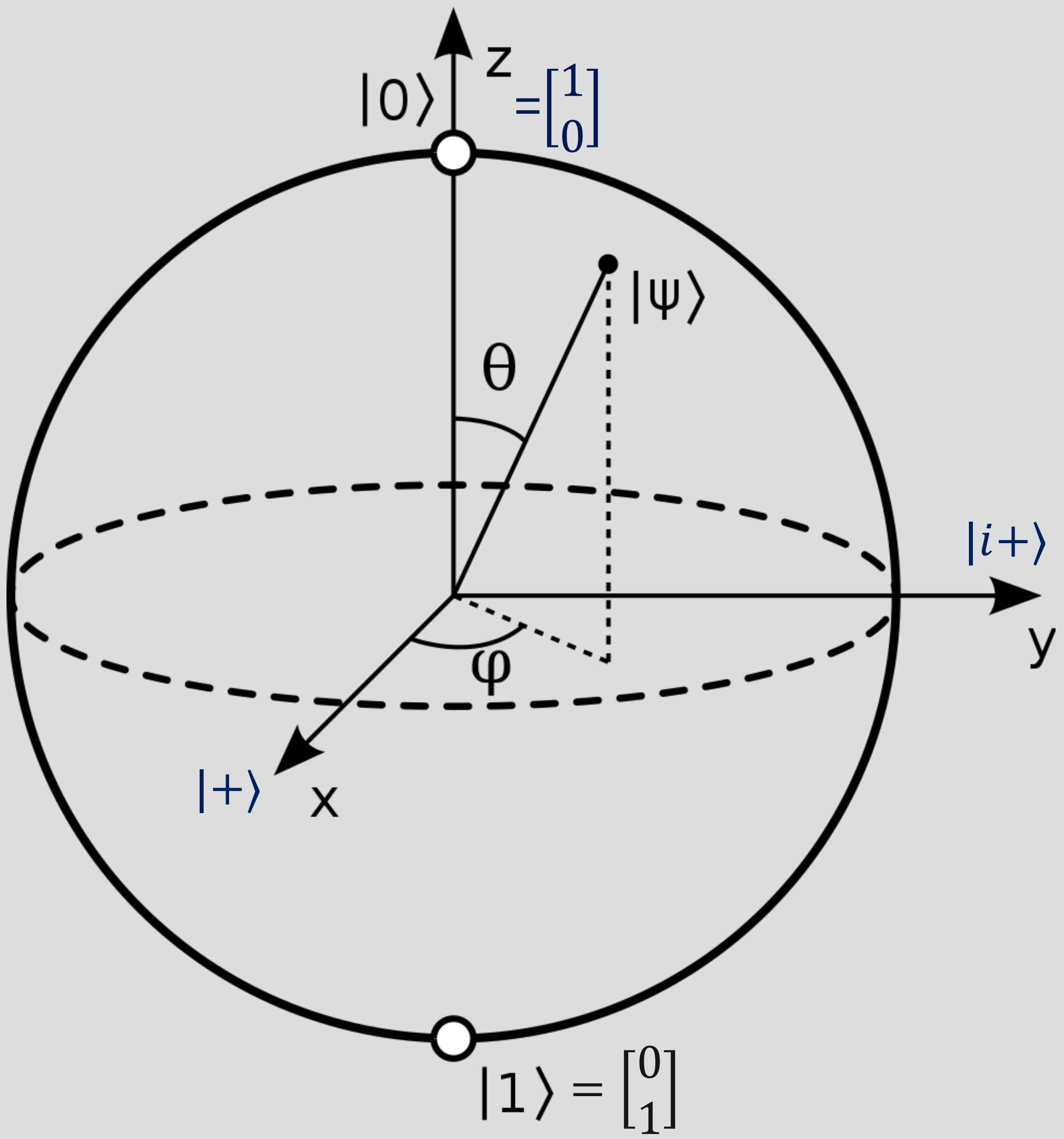
Dirac (Bra-Ket) Notation

$$\langle \psi | A | \phi \rangle = \begin{bmatrix} \gamma & \delta & \cdots \end{bmatrix} \begin{bmatrix} A_{00} & A_{01} & \cdots \\ A_{10} & A_{11} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \vdots \end{bmatrix}$$

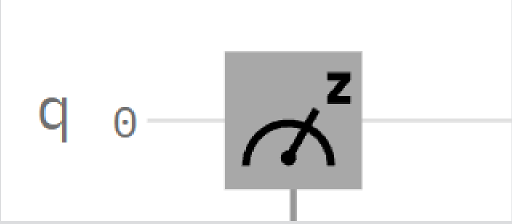
Qubit Representation

- Value represented by a vector in $\mathbb{C}^2$
- Normalized
- First coefficient is always taken to be real

$$|\phi\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle$$



Measuring Qubits



- Measurement is probabilistic
- Probability of measuring 0 or 1 based on coefficients of state

$$p(0) = |\langle 0|\phi\rangle|^2$$

$$p(1) = |\langle 1|\phi\rangle|^2$$

- Superpositions can't be measured; measurements cause the qubit to collapse into $|0\rangle$ or $|1\rangle$

$$p(0x_1x_2) = \sum_{x_1,x_2\in\{0,1\}} |\langle 0x_1x_2|\phi\rangle|^2$$

Qubit Entanglement

Entanglement describes when a set of qubits exist in a state where the state of the whole set cannot be completely separated into the states of its individual qubits.

Separable

$$|\phi_1\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$
$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Non-Separable

$$|\phi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Bell States

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

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

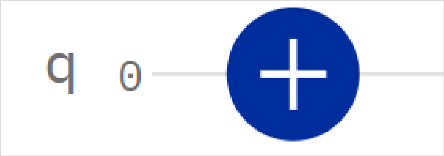
$$|\beta_{11}\rangle = \frac{|10\rangle - |10\rangle}{\sqrt{2}}$$

Operations on Qubits

- Operations on n qubits can be described by $2^{\mathrm{n}} \times 2^{n}$ matrices in $\mathbb{C}$
- Operations must be unitary; $UU^{\dagger} = U^{\dagger}U = I$
- Unitary implies
    - Operations must be reversible
    - Operations preserve norms of vectors they are applied to

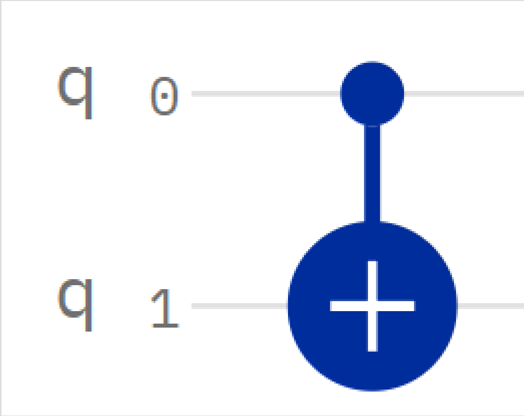
Classical Operations

NOT



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

XOR (CNOT)

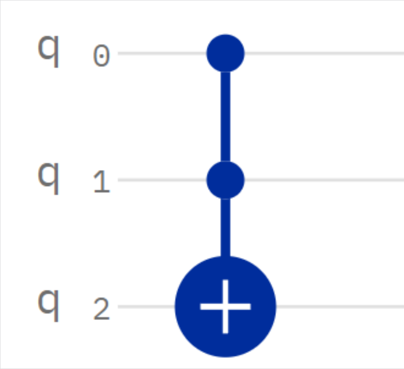


$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \text{NOT}$$

Classical Operations (Cont.)

AND (Toffoli/CCNOT)

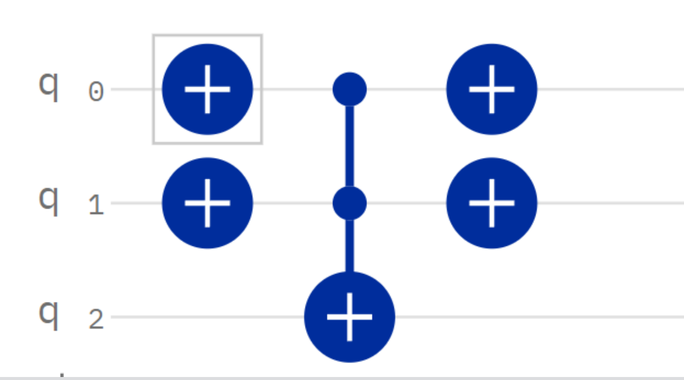
$|0\rangle$



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

OR

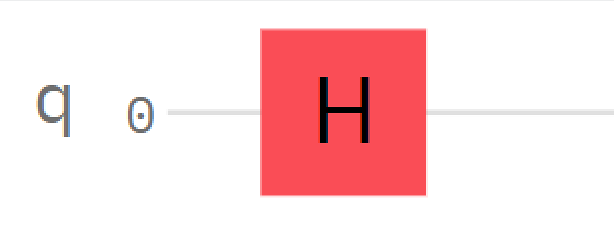
$|1\rangle$



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

Quantum Operations (Cont.)

Hadamard

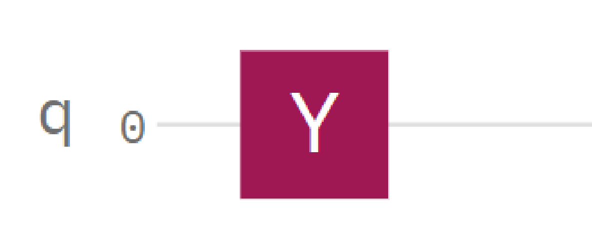


$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$|0\rangle \mapsto |+\rangle$$

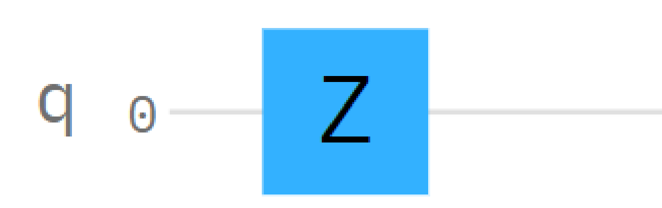
$$|1\rangle \mapsto |-\rangle$$

Y-gate



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

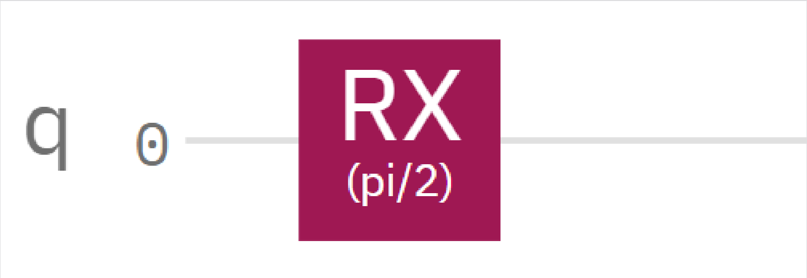
Z-gate



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

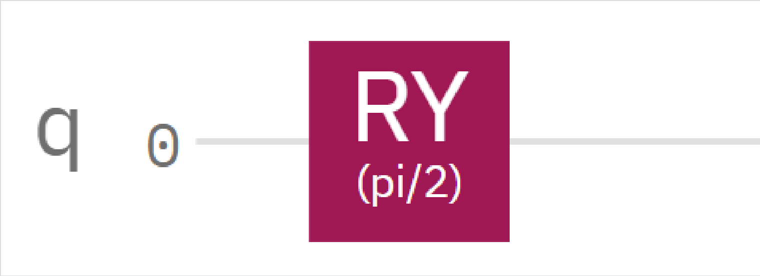
Quantum Operations (Cont.)

Rotate-X



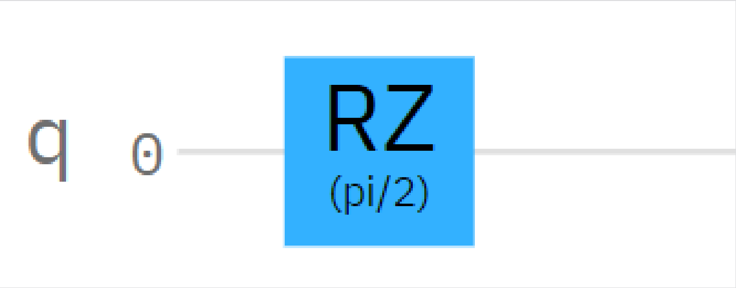
$$\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Rotate-Y



$$\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Rotate-Z



$$\begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Qubits Aren't a Free Lunch

- The fact that operations must be unitary puts restrictions bits don't have
- No cloning/No deleting theorem

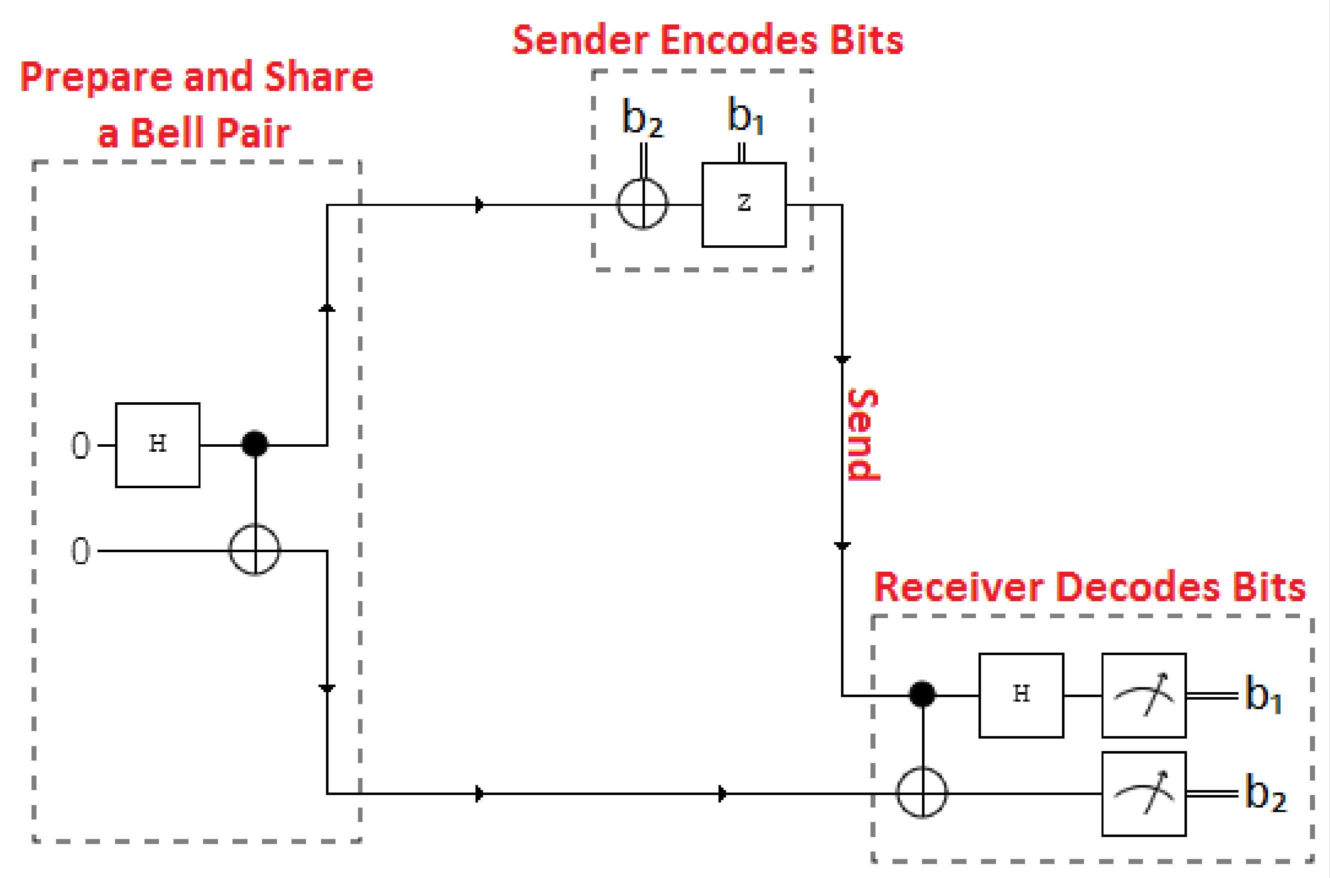
Cloning

$$U(|\phi\rangle|\psi\rangle) = |\phi\rangle|\phi\rangle$$

Deleting

$$U(|\phi\rangle|\phi\rangle) = |\phi\rangle|0\rangle$$

Superdense Coding



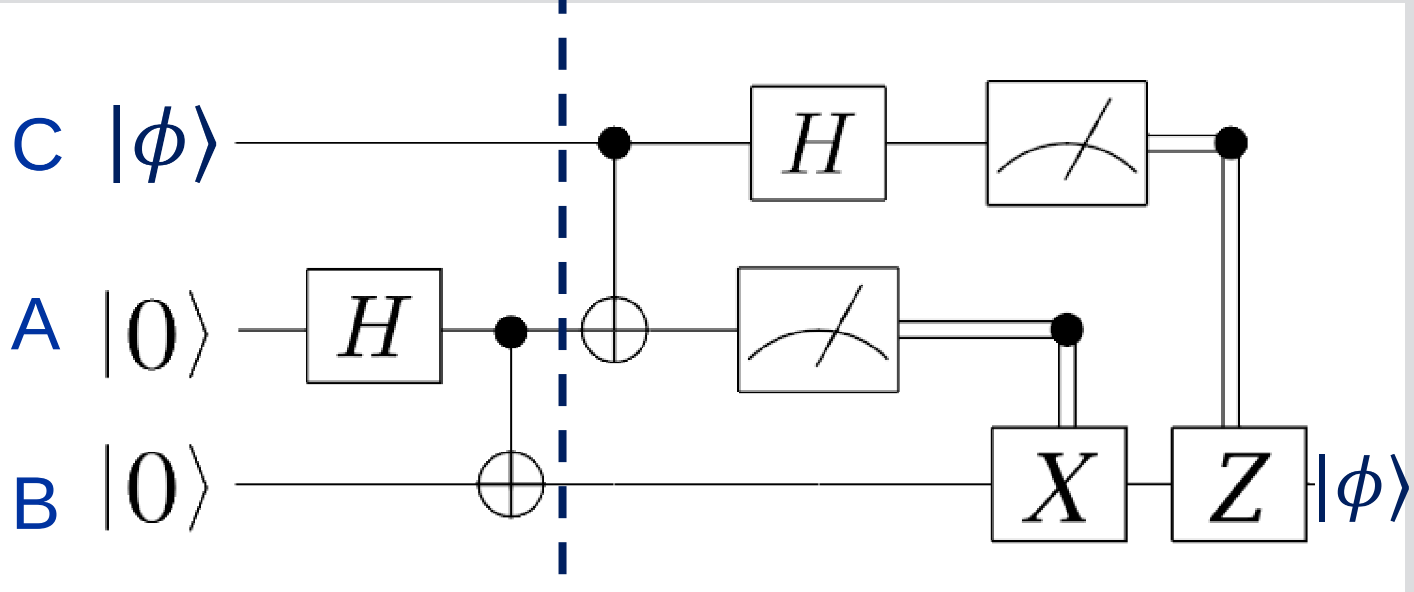
$$(I \otimes I)|\beta_{00}\rangle \Rightarrow |\beta_{00}\rangle$$

$$(X \otimes I)|\beta_{00}\rangle \Rightarrow |\beta_{01}\rangle$$

$$(Z \otimes I)|\beta_{00}\rangle \Rightarrow |\beta_{10}\rangle$$

$$(XZ \otimes I)|\beta_{00}\rangle \Rightarrow |\beta_{11}\rangle$$

Quantum Teleportation



$$|\phi\rangle_C|\beta_{00}\rangle_{AB}$$

$$= |\beta_{00}\rangle_{CA}\left(\frac{\alpha|0\rangle_B + \beta|1\rangle_B}{2}\right) + |\beta_{01}\rangle_{CA}\left(\frac{\beta|0\rangle_B + \alpha|1\rangle_B}{2}\right)$$

$$+ |\beta_{10}\rangle_{CA}\left(\frac{\alpha|0\rangle_B - \beta|1\rangle_B}{2}\right) + |\beta_{11}\rangle_{CA}\left(\frac{-\beta|0\rangle_B + \alpha|1\rangle_B}{2}\right)$$

Other Applications

- Quantum Systems Simulations
- Applications in AI
  - Quantum Random Walks
  - Quantum Support Vector Machines
- Quantum Cryptography
  - Key Distribution
  - Eavesdropping Detection
  - Integer Factoring Algorithms (Shor’s Algorithm)

Recommended Reading & Tools

Quantum Algorithm Implementations For Beginners, Abhijith J. et al.

Quantum Computation and Quantum Information, Michael A. Nielsen & Isaac L. Chuang

A Course in Quantum Computing (for the Community College) Volume 1, Micheal Loceff

IBM Quantum Composer