Quantum Gates

Week 2

Quantum Gates

Hadamard Gate

- Single qubit gate.
- Represented by matrix,

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

- Has the following effect on computational basis:

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

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

- Creates a superposition.

Pauli Gates

- The Pauli-X gate is represented as

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

  This gate is also known as the quantum NOT gate.

- The Pauli-Y gate is represented as

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

- The Pauli-Z gate is represented as

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

Phase Shift Gates

- This is a family of single-qubit gates that leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$.
- They are represented as

$$\mathsf{R}_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

- The probability of measuring the basis states is unchanged after applying this gate as it just modifies the phase of the quantum state. The Pauli-Z gate is just a special case the the Phase Shift Gates.

C-NOT Gate

- This is a 2-qubit gate.
- It is represented by

$$\begin{bmatrix} I & 0_{2\times 2} \\ 0_{2\times 2} & \sigma_X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- The first qubit acts as the control, and C-NOT performs the NOT operation on the second qubit only if the first qubit is 1.
- This is only a small set of gates we have shown here. There are many others such as the SWAP, C-SWAP and Toffoli gates. The reader is encouraged look up these gates on their own time.

Quantum Wires

Quantum Wires

- A quantum wire is a wire in a quantum circuit. Unlike its classical counterpart, quantum wires need not be actual wires (that conduct electricity). Instead quantum wires can also be thought of as the passage of time, or passage of space.
- Unlike regular wires, quantum wires can't be merged, this is a an OR operation and is non-unitary, nor can they be split as a result of the no-cloning theorem.

Quantum Circuits

Quantum Circuits

- Quantum Circuits are a sequence of quantum gates connected by quantum wires. The physical realization of a quantum algorithm translates to a quantum circuit. Hence quantum circuits are a model of quantum computation.

Quantum Entanglement

- Postulate 4, from last week's lecture material, allows us to define a concept most fundamental to quantum computation – entanglement. Consider,

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

- This state has a remarkable property that their exist no single qubit states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |a\rangle |b\rangle$. The reader is encouraged to prove this an exercise (hint: consider $|a\rangle = \alpha_a |0\rangle + \beta_a |1\rangle$ and $|b\rangle = \alpha_b |0\rangle + \beta_b |1\rangle$).
- Any composite system having this property is an *entangled* state.

Creating an Entanglement

Entangled states play a very important role in quantum computing and quantum information as we will see in the coming weeks. It is only natural for us to ask how create a pair of entangled qubits. The Hadamard and C-NOT gates that we have studied about will help us make the circuit shown in Figure 1.

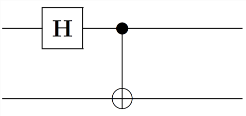

Figure 1: Quantum circuit for entangling two qubits (Credits: John Preskill's lecture notes)

No-cloning theorem

Theorem

There exists no unitary operator U such that for any arbitrary quantum state $|\psi\rangle$ and a random ancilla $|\phi\rangle$, we can perform the following transformation

$$|\psi\rangle \otimes |\phi\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \tag{1}$$

The no-cloning theorem is a very important result which is used throughout quantum computation and quantum information.

Proof of the No-cloning Theorem

We show a proof of Theorem 1 by contradiction. Suppose we can perform the transformation shown in equation 1, and let there be two arbitrary quantum states $|\psi\rangle$ and $|\Psi\rangle$. Then for an appropriate U we would have

$$U|\psi\rangle \otimes |\phi\rangle = e^{i\alpha}|\psi\rangle \otimes |\psi\rangle \tag{2}$$

$$U|\Psi\rangle \otimes |\phi\rangle = e^{i\beta}|\Psi\rangle \otimes |\Psi\rangle \tag{3}$$

where α and β are the phases. Now we take the Hermitian conjugate of (3).

$$\langle\Psi| \otimes \langle\phi|U^\dagger = e^{-i\beta}\langle\Psi| \otimes \langle\Psi| \tag{4}$$

Now multiplying (2) and (4) together we get

$$\begin{aligned}\langle\Psi| \otimes \langle\phi|U^\dagger U|\psi\rangle \otimes |\phi\rangle &= e^{-i\beta}\langle\Psi| \otimes \langle\Psi|e^{i\alpha}|\psi\rangle \otimes |\psi\rangle \\ \langle\Psi|\psi\rangle \otimes \langle\phi|\phi\rangle &= e^{i(\alpha-\beta)}\langle\Psi|\psi\rangle \otimes \langle\Psi|\psi\rangle\end{aligned} \tag{5}$$

Taking absolute value on both sides we get