Quantum Machine Learning Seminars

Week 3: Quantum Gates & Quantum Circuits

Dr. Hassan Alshal

Outline

1. Encoding Data into Quantum States
2. Quantum Cloner
3. Quantum Gates
4. Quantum Oracles

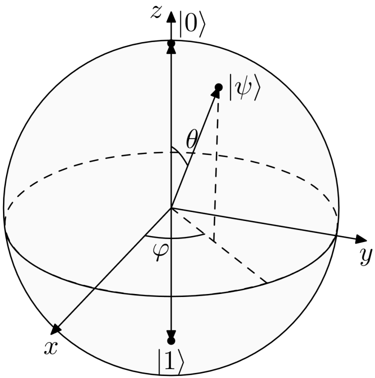
Mapping Classical Data into Quantum States

- Create an orthonormal computational basis from $x \in X \to \{|x_n^{\perp}\rangle\}_{i=1}^{n}$, e.g., $0 \to |0\rangle$ and $1 \to |1\rangle$.
- For a string $(x_1, \cdots, x_n)$ we define n-qubit $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots |x_n\rangle = |x_1 x_2 \cdots x_n\rangle \in \mathtt{H} = \mathbb{C}^{2n}$.
- Register basic encoding: $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$.

  And for n-features string, it requires n qubits.
- Angle encoding:

  $|\psi\rangle = R_y(\theta)|0\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|0\rangle$, where

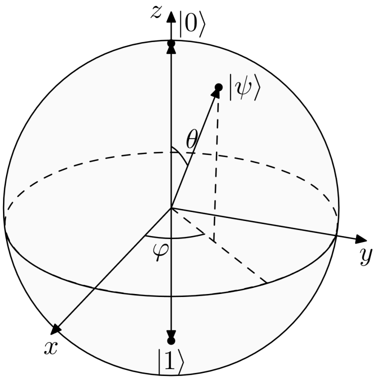
  $$R_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$



https://en.wikipedia.org/wiki/Bloch_sphere

Mapping Classical Data into Quantum States

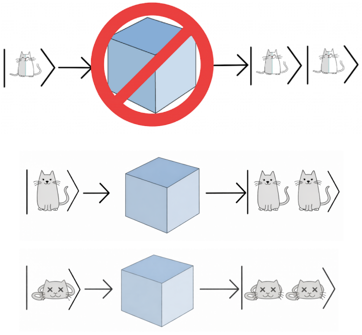
- Amplitude Encoding: for some feature vector $\mathbf{x} \in \mathbb{C}^n$ and some $\{\phi_i\}_{i=1}^n$, define: $|\psi_{\mathbf{x}}\rangle = \sum_{i=1}^{n} x_i |\phi_i\rangle$.
  So, for n-features, it requires $\log_2(n)$ qubits.
  e.g., $\mathbf{x} = (1,\ 2,\ 3,\ 4)$, $||\mathbf{x}|| = \sqrt{30}$ and the encoding is $|\psi_{\mathbf{x}}\rangle = \frac{1}{\sqrt{30}}|00\rangle + \frac{2}{\sqrt{30}}|01\rangle + \frac{3}{\sqrt{30}}|10\rangle + \frac{4}{\sqrt{30}}|11\rangle$.
- If the feature is a matrix $A = \sum_{i,j}^{n} a_{ij}$ with $\sum_{i,j} |a_{ij}|^2 = 1$, define $|\psi_A\rangle = \sum_{i,j} a_{ij} |\phi_i\rangle \otimes |\phi_j\rangle$.
- C.f.: Weigold, M., et al., Encoding patterns for quantum algorithms. IET Quant. Comm. 2(4), 141–152 (2021).



https://en.wikipedia.org/wiki/Bloch_sphere

No-cloning theorem

- Cloning means $\exists|\eta\rangle \in \mathtt{H}_B$ “blank state” and $U^\dagger = U^{-1}$ “a universal” unitary operator such that $\forall|\psi\rangle \in \mathtt{H}_A$, $U|\psi\eta\rangle = |\psi\psi\rangle$.
- There is NO such quantum cloner, i.e., superposition states cannot be copied by “reading”.
- Define $U|\psi\eta\rangle = |\psi\psi\rangle$ and $U|\varphi\eta\rangle = |\varphi\varphi\rangle$.
  Then $\langle\varphi\eta|U^\dagger U|\psi\eta\rangle = \langle\varphi\varphi|\psi\psi\rangle = \langle\varphi|\psi\rangle^2$.
  At the same time $\langle\varphi\eta|U^\dagger U|\psi\eta\rangle = \langle\varphi\eta|\psi\eta\rangle = \langle\varphi|\psi\rangle$.
  Therefore, $\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2 \Leftrightarrow \langle\varphi|\psi\rangle \propto \delta_{ij} \Rightarrow \nexists U$.
- Try to clone $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ using $|\eta\rangle = |0\rangle$.



Quantum Cloner

No-cloning theorem

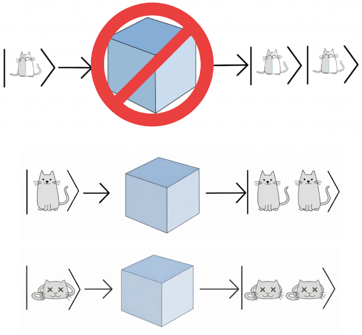
- Classical cloner is `XOR` gate: (x) and $(y) \Rightarrow (x,\ x \oplus y)$.
- The equivalent to `XOR` in the quantum context is `CNOT`: $|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$. Check how it works:

$$|0\rangle|0\rangle \mapsto |0\rangle|0\rangle \quad , \quad |1\rangle|0\rangle \mapsto |1\rangle|1\rangle.$$

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

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \xrightarrow{\texttt{CNOT}} \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle,$$

$$\begin{aligned} |\psi\rangle|\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \beta^2|11\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle. \end{aligned}$$



Quantum Registers and Quantum Gates

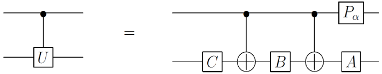
- An n-qubit register is system of n-qubits described as vectors in $\mathtt{H} = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ that can be acted upon by n-qubit gates that are represented by $2n \times 2n$ unitary matrices.
- e.g., check how the matrix
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$
acts on $|0\rangle|0\rangle$ and $|1\rangle|0\rangle$.
- Hadamrd acting on $|0\rangle$ yields basic encoding.

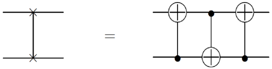
Operator	Gate(s)	Matrix
Pauli-X (X)	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	Z	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

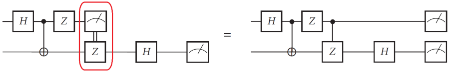
https://en.wikipedia.org/wiki/Quantum_logic_gate

Gate Universality & Deferral

- For any 1-qubit gate U there exist unitary operators A, B, C satisfying $ABC = I$ and $\alpha \in \mathbb{R}$ such that $U = e^{i\alpha} A \sigma_x B \sigma_x C$.
- A set of quantum gates is said to be universal for quantum computation if, any n-qubit gate can be approximated to arbitrary accuracy by a composition of only those gates. $\Rightarrow \{H, S, T, \texttt{CNOT}\}$ is universal.
- Any mid-circuit computational basis measurement can be deferred to the end of the circuit, and a quantum control replaces classical-control conditioned outcome.







Quantum Oracles

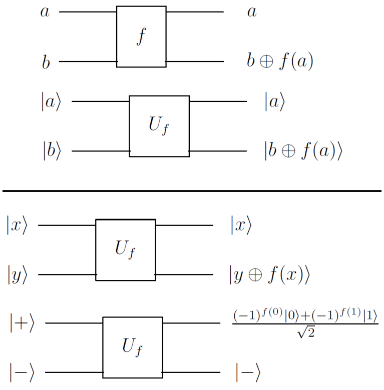
Invertibility

- An oracle is defined as an abstract black box that computes $f : \mathbb{B}^n \to \mathbb{B}^m$ as a single operation.
- f isn't necessarily invertible. So, a reversible computation can be defined as the unitary operator $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$.
- How? $|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{U_f}$ $|x\rangle\big|(y \oplus f(x)) \oplus f(x)\big\rangle = |x\rangle|y\rangle$, i.e., $(U_f)^1 = 1$.
- Phase Oracle: $O_f : \ |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. So for example, prepare $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. $U_f\big(|x\rangle|-\rangle\big) = (-1)^{f(x)}|x\rangle|-\rangle$.

Quantum Oracles

Invertibility

- An oracle is defined as an abstract black box that computes $f : \mathbb{B}^n \to \mathbb{B}^m$ as a single operation.
- f isn't necessarily invertible. So, a reversible computation can be defined as the unitary operator $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$.
- How? $|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{U_f}$ $|x\rangle\big|(y \oplus f(x)) \oplus f(x)\big\rangle = |x\rangle|y\rangle$, i.e., $(U_f)^1 = 1$.
- Phase Oracle: $O_f : \ |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. So for example, prepare $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. $U_f\big(|x\rangle|-\rangle\big) = (-1)^{f(x)}|x\rangle|-\rangle$.



Thank You!