Quantum computing basics

February 6, 2026

Quantum bits

- Two possible basis states $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- A *qubit* can also be in a linear combination (superposition) of states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

- Thus, a *qubit* is a vector in a $2D$ vector space over the complex field.
- $|0\rangle$ and $|1\rangle$ are called *computational basis states*. They form an orthonormal basis.
- We cannot examine a *qubit* to determine its state. That is, we cannot measure α and β. **States are unobservable**.
- When we measure we get $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. **Measurement collapses the system to one of the basis states**.
- *qubit*'s are decidedly real? Will revisit the issue.

How much information in a *qubit*?

- Infinite number of points on the surface of a sphere. Representation of a state will require infinite number of bits. Can we store the entire *Mahabharat* in a *qubit*?
- *Misleading*, because measurement will collapse the state to either $|0\rangle$ or $|1\rangle$. Only one bit of information from a measurement.
- But how much information if we do not measure?
- Trick question. But it is hypothesized that when nature evolves *closed quantum systems* it maintains all continuous variable. *Key to quantum computation*.
- *qubit* states can be manipulated and transformed in interesting ways that can lead to meaningful measurement outcomes.

Multiple *qubits*

- For two classical bits we can have four states 00, 01, 10 and 11.
- Correspondingly, for a 2 *qubit* system we have four computational basis states: $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.
- The 2 *qubit* state is $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \sum_{x\in\{0,1\}^2} \alpha_x|x\rangle$
- We could measure only the first *qubit*. If we get $|0\rangle$ *wp* $|\alpha_{00}|^2 + |\alpha_{01}|^2$, the post measurement state is

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Hilbert space is a very large space

- Tensor product of two vector spaces V (dimension k) and W (dimension l) is $V \otimes W$ (dimension kl). If $\left|v_1\right\rangle \left|v_2\right\rangle \ldots \left|v_k\right\rangle$ and $\left|w_1\right\rangle \left|w_2\right\rangle \ldots \left|w_l\right\rangle$ are the bases for V and W, then a basis for $V \otimes W$ is $\{\left|v_i\right\rangle \otimes \left|w_j\right\rangle : 1 \leq i \leq k, 1 \leq j \leq l\}$.
- *Hilbert space is a very large space*. Nature seems to find extra storage when we combine two subsystems.

Entangled states: a key component of quantum computing

- A fantastic 2 *qubit* state is the *Bell state* or *EPR pair*

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

- There are no single *qubit* states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |ab\rangle$.
- On measuring the first *qubit* we get $|0\rangle$ or $|1\rangle$ with equal probability.
- Post measurement state is $|\psi'\rangle = |00\rangle$ or $|\psi'\rangle = |11\rangle$. Measurement of the second *qubit* gives *exactly* the same result as the first.
- The two *qubits* are *correlated* or *entangled*.
- *The measurement correlations in the* Bell state *is stronger than could exist in two components of any classical system*.
- 'Spooky action at a distance"

Quantum computation

- In the *classical circuit model* computational algorithms are described by wires and logic gates (*NAND*).
- Only one non-trivial 1 bit gate - *NOT*.
- Quantum analogue: $\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$ (the quantum *NOT* acts linearly).
- Can be represented by a matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

- All quantum gates U must be *unitary operators*: $U^\dagger U = I$.
- Quantum operations are reversible.

Important single *qubit* gates

- Pauli matrices:

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

- Hadamard:

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

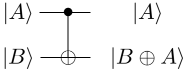
$$\alpha|0\rangle + \beta|1\rangle \;—\boxed{H}—\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- Rotation:

$$U = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Multiple *qubit* gates

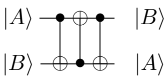
Controlled NOT $(CNOT)$



$$\left|00\right\rangle \to \left|00\right\rangle; \quad \left|01\right\rangle \to \left|01\right\rangle;$$
$$\left|10\right\rangle \to \left|11\right\rangle; \quad \left|11\right\rangle \to \left|10\right\rangle$$

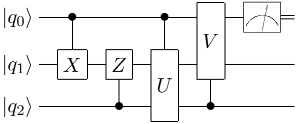
Derive that $U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Swap



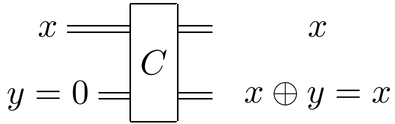
$$\begin{aligned} \left|A, B\right\rangle &\to \left|A, A \oplus B\right\rangle \\ &\to \left|A \oplus (A \oplus B), A \oplus B\right\rangle = \left|B, A \oplus B\right\rangle \\ &\to \left|B, (A \oplus B) \oplus B\right\rangle = \left|B, A\right\rangle \end{aligned}$$

A typical quantum circuit

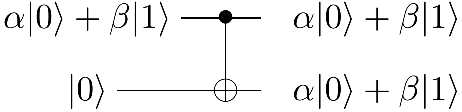


Quantum copying?

Classical cloning



Quantum cloning?



$$\left[\alpha|0\rangle + \beta|1\rangle\right]|0\rangle = \alpha|00\rangle + \beta|10\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle$$

Have we cloned? For a general state $\psi = \alpha|0\rangle + \beta|1\rangle$,

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

$\boxed{\textbf{Actually quantum cloning is not possible}}$

The no-cloning theorem

- Suppose source slot A and the target slot B start out with $|\psi\rangle$ and $|s\rangle$ respectively. Initial state is

$$|\psi\rangle \otimes |s\rangle$$

- Suppose some unitary U effects the copying procedure

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

- Suppose this works for two states $|\psi\rangle$ and $|\phi\rangle$. Then

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

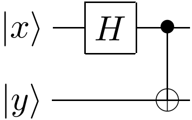
- The inner product of the two equations gives us

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$$

- $x = x^2$ implies $x = 0$ or $x = 1$. So, either $|\phi\rangle = |\psi\rangle$, or $|\phi\rangle$ and $|\psi\rangle$ are orthogonal. Therefore, a general cloning device is not possible.

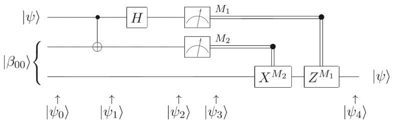
Primitives for quantum computations: Hadamard transformation

- $$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$
- Use *Hadamard* and *CNOT* to produce the *Bell states*



$$\begin{array}{ccl} |00\rangle & \rightarrow & \left(|00\rangle + |11\rangle\right)/\sqrt{2} = \beta_{00} \\ |01\rangle & \rightarrow & \left(|01\rangle + |10\rangle\right)/\sqrt{2} = \beta_{01} \\ |10\rangle & \rightarrow & \left(|00\rangle - |11\rangle\right)/\sqrt{2} = \beta_{10} \\ |11\rangle & \rightarrow & \left(|01\rangle - |10\rangle\right)/\sqrt{2} = \beta_{11} \end{array}$$

Quantum teleportation



- Alice and Bob separated after generating an EPR pair. Alice now wants to transfer $|\psi\rangle$ to Bob. Top two qubits are Alice's, the last one is Bob's.
- $$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle\big(|00\rangle + |11\rangle\big) + \beta|1\rangle\big(|00\rangle + |11\rangle\big)\Big]$$
- $$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle\big(|00\rangle + |11\rangle\big) + \beta|1\rangle\big(|10\rangle + |01\rangle\big)\Big]$$
- $$\begin{aligned} |\psi_2\rangle &= \tfrac{1}{2}\Big[\alpha\big(|0\rangle + |1\rangle\big)\big(|00\rangle + |11\rangle\big) + \beta\big(|0\rangle - |1\rangle\big)\big(|10\rangle + |01\rangle\big)\Big] \\ &= \tfrac{1}{2}\Big[|00\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |01\rangle\big(\alpha|1\rangle + \beta|0\rangle\big) \\ &\quad +|10\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |11\rangle\big(\alpha|1\rangle - \beta|0\rangle\big)\Big] \end{aligned}$$

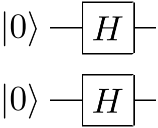
Quantum teleportation

Depending on Alice's measurements

$$\begin{array}{lllr}
00 & \longrightarrow |\psi_3(00)\rangle = \left[\alpha|0\rangle + \beta|1\rangle\right] & & \text{Bob has } \left|\psi\right\rangle \\
01 & \longrightarrow |\psi_3(01)\rangle = \left[\alpha|1\rangle + \beta|0\rangle\right] & & \text{Bob applies } X \\
10 & \longrightarrow |\psi_3(10)\rangle = \left[\alpha|0\rangle - \beta|1\rangle\right] & & \text{Bob applies } Z \\
11 & \longrightarrow |\psi_3(11)\rangle = \left[\alpha|1\rangle - \beta|0\rangle\right] & & \text{Bob applies } X \text{ and } Z
\end{array}$$

Primitives for quantum computations: Hadamard transformation

- Parallel action of two *Hadamard* gates: $H^{\otimes 2}$



$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

- $H_{2^n} = H^{\otimes n}$ is the *Fourier transform* over the abelian group Z_{2^n}.
- H_{2^n} is the $2^n \times 2^n$ matrix in which the (x, y) entry is $2^{-n/2}(-1)^{x.y}$

Primitives for quantum computations: Hadamard transformation

- Applying H_{2^n} to the state of all zeroes give an equal superposition

$$H_{2^n}\left|0\ldots0\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}\left|x\right\rangle$$

- Applying H_{2^n} to a state $\left|u\right\rangle$ modifies the above superposition by a phase

$$H_{2^n}\left|u\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{u.x}\left|x\right\rangle$$

- *Extremely efficient*: n gates produce equal superposition of 2^n states.
- In general, if we start with $\left|\phi\right\rangle = \sum_x \alpha_x\left|x\right\rangle$, after *Fourier transform* over Z_{2^n} we get $\left|\hat{\phi}\right\rangle = \sum_x \hat{\alpha}_x\left|x\right\rangle$
- To read the answer we must make a measurement. We obtain x with probability $|\hat{\alpha}_x|^2$ (**Fourier sampling**).