Basics of Quantum Computing

Tianyi Zhou

PRIMES CS Circle

December 2024

Quantum Bits (Qubits)

Classical computing: a bit has 2 states: $|0\rangle$ and $|1\rangle$. Bits are observable.
Quantum computing: qubits can be in a *superposition* of the states $|0\rangle$ and $|1\rangle$. Not directly observable.

Definition

A *qubit* $|\phi\rangle$ is written as

$$|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$. $\alpha_0, \alpha_1 \in \mathbb{C}$ are *amplitudes*.

Qubits

One thing you can do to a qubit is *measure* it.
Measuring a qubit collapses it into an observable state of either $|0\rangle$ or $|1\rangle$ and destroys information of its amplitudes.

- Probability $|\alpha_0|^2$ of $|\phi\rangle$ ending up in $|0\rangle$ when measured
- Probability $|\alpha_1|^2$ of $|\phi\rangle$ ending up in $|1\rangle$ when measured

Example

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Dirac ("bra-ket") Notation

$|\phi\rangle$ equals the 2x1 vector $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$|\phi\rangle$ is a "ket" vector. Its conjugate transpose is the 1x2 "bra" vector

$$\langle\phi| = (\alpha_0^*, \alpha_1^*).$$

Bra-ket comes from the inner product of bra and ket vectors:

$$\langle\phi|\psi\rangle = \langle\phi| \cdot |\psi\rangle$$

(inner product) (bra $\cdot$ ket)

Unitary transformations

We can apply some operation U to a quantum state $|\phi\rangle$ to get $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$.

Since $|\phi\rangle$ is a 2x1 vector, this operation U is a 2x2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Since our new state $|\psi\rangle$ must obey $|\beta_0|^2 + |\beta_1|^2 = 1$, U must preserve the norm of the vector, and so must be a *unitary* transformation.

Definition

Matrix U is *unitary* if

$$U^\dagger U = I$$

where $U^\dagger$ is the adjoint, or conjugate transpose, of U

Why Do Unitary Matrices Preserve the Norm?

Because $|\psi\rangle = U|\phi\rangle$, we have

$$\langle\psi| = (U|\phi\rangle)^\dagger = \langle\phi| U^\dagger$$

Suggesting

$$\langle\psi|\psi\rangle = \langle\phi| U^\dagger U |\phi\rangle = 1$$

Since $\langle\phi|\phi\rangle = 1$, we thus must have $U^\dagger U = I$.

Thus, any valid operator U we can apply to a quantum state $|\phi\rangle$ must be a unitary transformation.

2-Qubit Quantum States

A *2-qubit quantum system* is mathemtically defined as the tensor product of 2 qubits

$$\begin{aligned}|\phi\rangle \otimes |\psi\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle\end{aligned}$$

It has the 4 basis states

$$\begin{aligned}|0\rangle \otimes |0\rangle &= |00\rangle \\ |0\rangle \otimes |1\rangle &= |01\rangle \\ |1\rangle \otimes |0\rangle &= |10\rangle \\ |1\rangle \otimes |1\rangle &= |11\rangle\end{aligned}$$

Entanglement

A unique feature in quantum is that you can have *entangled* states, where the states are somehow intrinsically linked.

Example

EPR pair:

$$|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

If you measure the first 1 qubit in this system, you get information on the state of the second qubit.

- These 2 qubits are maximally entangled.

Entangled quantum states cannot be written as tensor products over single qubits.

No Cloning Theorem

Important theorem in quantum computing that states that you can't arbitrarily replicate ("clone") quantum states.

Proof

- Suppose a universal cloning machine exists.
- Given 2 arbitrary states $|\phi\rangle, |\psi\rangle$, we would be able to get

$$|\phi\rangle \otimes |0\rangle \rightarrow |\phi\rangle \otimes |\phi\rangle$$
$$|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$$

- However, this would mean the cloning process gives both $(\alpha |\phi\rangle + \beta |\psi\rangle) \otimes |0\rangle \rightarrow (\alpha |\phi\rangle + \beta |\psi\rangle) \otimes (\alpha |\phi\rangle + \beta |\psi\rangle)$ and $(\alpha |\phi\rangle + \beta |\psi\rangle) \otimes |0\rangle \rightarrow \alpha |\phi\rangle \otimes |\phi\rangle + \beta |\psi\rangle \otimes |\psi\rangle$ for all $\alpha, \beta \in \mathbb{C}$ and arbitrary states $|\phi\rangle, |\psi\rangle$.
- Contradiction!

Acknowledgments

A huge thank you to Lalita, Yael, and Justin, our amazing mentors.

And a big thank you to the MIT PRIMES program for this wonderful opportunity!