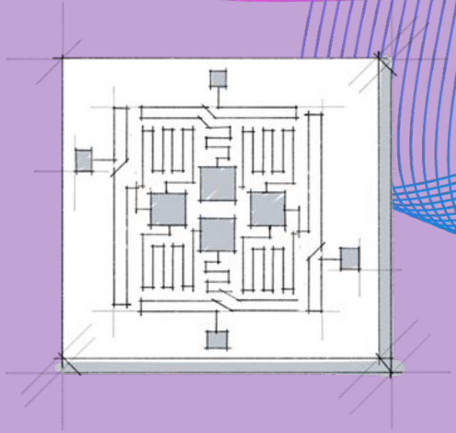
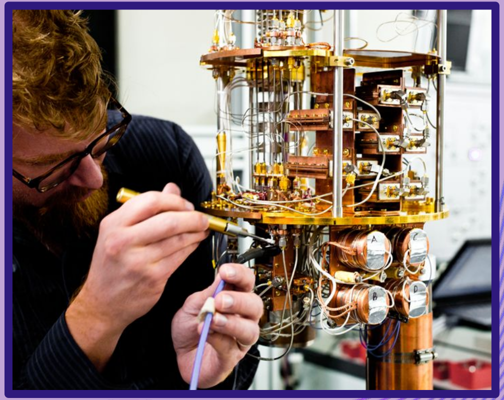
qbits.bitsgoa

Intro to Quantum Computing





Quantum Computers use special bits of data, called qubits, which follow the laws of quantum mechanics.

We these laws to our advantage, enabling us to put qubits into superposition or to create entanglement.

Using these techniques, quantum computers harness nature to compute problems that are too large for classical computers to solve

MIT Technology Review　　　　Topics

Computing

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25

LINEAR ALGEBRA

Today, we aim to cover the following

- Vector Spaces
- Conjugate transpose
- Inner product
- Normalization

Vector Space

Set V on which two operations + and · are defined, called vector addition and scalar multiplication.

Let $u, v, w \in V$, $c, d \in \mathbb{C}$,the set has the following axioms -

1. $u + v \in V$
2. $u + v = v + u$
3. $u + (v + w) = (u + v) + w$
4. The set V contains an additive identity element, denoted by 0, such that $0 + v = v$ and $v + 0 = v$
5. $v + x = 0$ and $x + v = 0$ have a solution x in V, called an additive inverse of v, and denoted by $-v$
6. $c \cdot v \in V$
7. $c \cdot (u + v) = c \cdot u + c \cdot v$
8. $(c + d) \cdot v = c \cdot v + d \cdot v$
9. $c \cdot (d \cdot v) = (cd) \cdot v$
10. $1 \cdot v = v$

Dirac Notation

In QM, we use the bra-ket notation.

Here, you'll see vectors written as: $|v\rangle$
This is called a ket-vector:

It's essentially a column vector consisting of two complex elements.

$$|v\rangle = \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} 2+3i \\ 5i \end{pmatrix}$$

We'll explain bra-vector in the later slides.

Matrix time

The operations we define on matrices are extremely important in quantum mechanics and quantum computing!

Matrices are how we will represent qubits, and build the quantum gates that will manipulate these qubits.

We’ll talk about that in some time

Matrix time

CONJUGATE TRANSPOSE (†)

Conjugate transpose of matrix A = $A^\dagger$ *(pronounced A dagger)*

For an m×n matrix A, $A^\dagger$ is an n×m matrix such that

$$A^\dagger[i][j] = A^*[j][i]$$

$$A = \begin{pmatrix} 2 + i \\ 3 + 4i \end{pmatrix} \qquad A^\dagger = \begin{pmatrix} 2 - i & 3 - 4i \end{pmatrix}$$

Matrix time

CONJUGATE TRANSPOSE BUT QUANTUM (spooky ghost noises)

Dirac notation of a vector: $|v\rangle$

Conjugate transpose of vector: $\langle v|$

$$|v\rangle = \begin{pmatrix} 2 + 3i \\ 5i \end{pmatrix}$$

$$\langle v| = |v\rangle^\dagger = \begin{pmatrix} 2 - 3i & -5i \end{pmatrix}$$

$\langle v|v\rangle$ = inner product = 38

Linear Transformations

Say you have two vector spaces ***U*** and ***V***. A linear transformation is a mapping that “maps” a vector from one vector space to another.

Sort of like a “**function**”.

It has a set of properties though:

1. *L*(**u**) = **v**, where u and v are vectors in U and V respectively.
2. *L*(a**u** + b**w**) = a* *L*(**u**) + b* *L*(**w**), where a and b are scalars.

Matrix time: Eigen-stuff

EIGENVALUES

For a vector **v**, eigen values λ are defined such that

$$Av = \lambda v \text{ for some } v\text{, where } A \text{ is a matrix}$$

$$\Rightarrow \; (\lambda I - A)v = 0 \text{ (Characteristic equation)}$$

$$A = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$$

Matrix time

EIGENVALUES

$$\lambda I - A = \begin{pmatrix} \lambda - 3 & 4 \\ 1 & \lambda - 2 \end{pmatrix} = 0$$

$$(\lambda - 3)(\lambda - 2) - 4 = 0$$

$$\lambda^2 - 5\lambda + 2 = 0$$

$$= 5/2 \pm \sqrt{17}/2$$

Matrix time

TENSOR PRODUCT/ KRONECKER PRODUCT

$$A = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_0 B \\ a_1 B \end{pmatrix} = \begin{pmatrix} a_0 b_{00} & a_0 b_{01} \\ a_0 b_{10} & a_0 b_{11} \\ a_1 b_{00} & a_1 b_{01} \\ a_1 b_{10} & a_1 b_{11} \end{pmatrix}$$

Matrix time

NORMALISATION

The normalized vector if x is a vector in the same direction but with a norm(length) = 1. It is denoted by x and given by

This is also known as unit vector. We'll deal with this when we talk about probabilities of quantum systems.

$$\hat{x} = \frac{x}{|x|}$$

$$\langle a | a \rangle = 1$$

UNITARY MATRIX

A square matrix whose

Conjugate transpose = Inverse

Square matrix U such that

$$U^{\dagger} = U^{-1}$$

Or in other words

$$UU^{\dagger} = U^{\dagger}U = I$$

QUANTUM GATES

What is a state of a quantum mechanical particle?

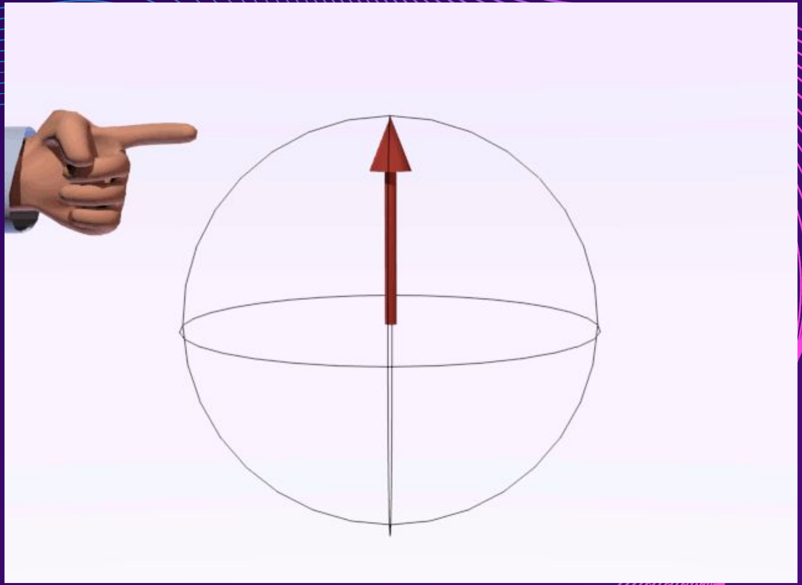
They are just vectors form a specific vector space called as a Hilbert space!

BASIS STATES

While working in any space we define some reference states to work in them. For example in the argand plane we use 1, i or on real space we use x y z coordinates. Similarly for Quantum States depending upon the size of the space we basis for these. For any n-D space we need n linearly independent vectors. For sake of simplicity we chose orthogonal vectors

Qubits!

- Qubits are two level quantum systems.They are quantum analogue of a classical bit is a qubit.
- It can have the values $|0\rangle$, $|1\rangle$, or a linear combination of both.
- $|0\rangle$ and $|1\rangle$ are the orthogonal **z-basis states**

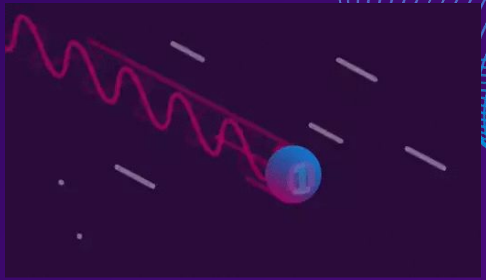


Measurement?

- It is the act of taking information out of a quantum mechanical system
- What kind of information we take out of the system is the “basis of measurement”
- For example if I am trying to know position of a particle, then I am measuring it in position basis, if I am trying to know the momentum of a particle, then I am measuring it in momentum basis
- Measuring a particle changes it’s state!

SUPERPOSITION

- Fundamental property of a quantum mechanics
- Any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state
- Conversely, every quantum state can be represented as a sum of two or more other distinct states (This is very important for us!!).
- Any qubit state can be represented as the linear combination or “superposition” of the two basis vectors, $|0\rangle$ and $|1\rangle$.
- We’ll see an example to see how the superposition works.



Matrix Representation of a qubit

A complex vector of size 2-

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Bloch Sphere

$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$

$0 \leq \theta \leq \pi$

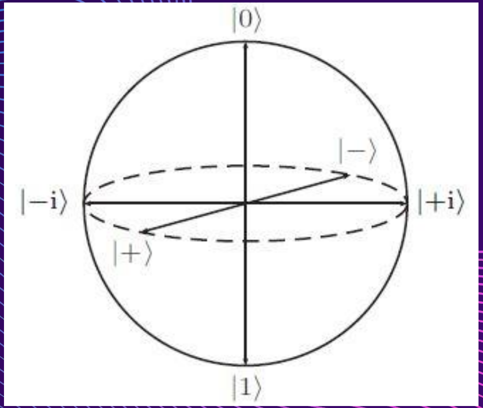
$0 \leq \phi < 2\pi$

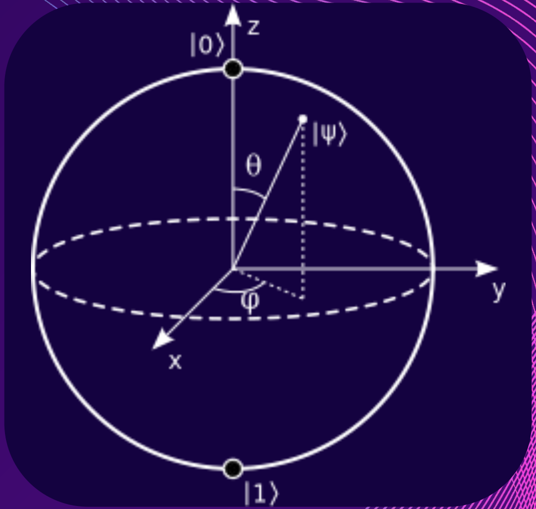
Global phase does not matter.

$x = \sin\theta \cos\phi$

$y = \sin\theta \sin\phi$

$z = \cos\theta$





Basis vectors of 2 qubits systems

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

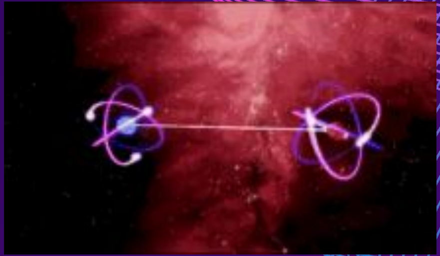
$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

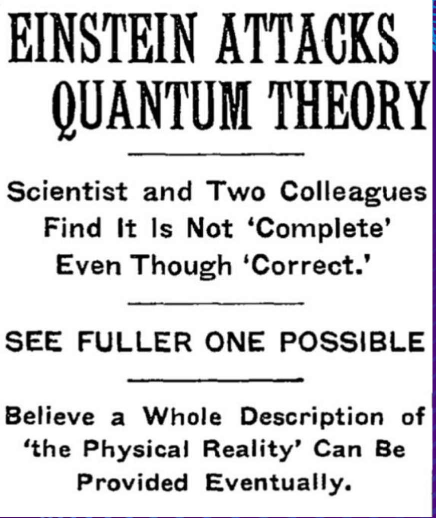
$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

ENTANGLEMENT

- Quantum entanglement is a close connection between a pair or groups of quantum systems.
- When 2 such quantum systems come close together and interact with one another, they become entangled.
- When 2 systems are entangled, a change in state of one causes an immediate change of state in the other system as well no matter how far the two systems are.
- So, if you happen to observe and determine the state of one of these system, you immediately know the state of the other without having to observe it.





EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

QUANTUM GATES

A gate that operates on N qubits is represented as a $2^N \times 2^N$ unitary matrix.

For example, a gate that operates on 1 qubit is represented by a 2×2 unitary matrix.

Tensor product is used to combine quantum states.

PAULI GATES

X gate : $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

X gate is similar to the classical NOT gate.

Y gate : $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

$Y|0\rangle = i|1\rangle$

$Y|1\rangle = -i|0\rangle$

Z gate : $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$Z|0\rangle = |0\rangle$

$Z|1\rangle = -|1\rangle$

OTHER IMPORTANT GATES

H gate : $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H|0\rangle = |+\rangle$

$H|1\rangle = |-\rangle$

CNOT gate : $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

$CNOT|00\rangle = |00\rangle$

$CNOT|01\rangle = |01\rangle$

$CNOT|10\rangle = |11\rangle$

$CNOT|11\rangle = |10\rangle$

CNOT gate is similar to the classical XOR gate.

OTHER IMPORTANT GATES

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		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

QISKIT

Qiskit is a library written in python used to programming IBM's quantum computers.

You can use any quantum system and library. But we recommend qiskit & IBM QE so that you can follow along

THANK YOU
&
QnA