	CLASSICAL COMPUTING	QUANTUM COMPUTING
S/W	BOOLEAN ALGEBRA	LINEAR ALGEBRA
H/W	CLASSICAL MECHANICS SEMICONDUCTORS	QUANTUM MECHANICS * SEMICONDUCTORS * SUPERCONDUCTORS

POSTULATES OF QUANTUM COMPUTING :

→ STATE SPACE RULE

Assume 2 states, $|0\rangle$, $|1\rangle$.

If there are 2 states, there can be linear combinations of the states.

$$\alpha . |0\rangle + \beta . |1\rangle$$

$\alpha, \beta \in$ COMPLEX NUMBERS

α : Probability of being in state $|0\rangle$.

So a new state can be formed through linear combination of other states.

eg: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

→ COMPOSITION RULE

To compose, we use tensor product.

If we have 300 qubits, it is a vector of 2^{300} complex numbers. This is due to tensor product.

n bits → n+1 bits

we add 1 more dimension.

n qubits → n+1 qubits

we double the dimensions

DIRAC NOTATION:

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

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

VECTOR OF 2

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

VECTOR OF 4

$|101\rangle \rightarrow$ VECTOR OF 8

SO EACH TIME, VECTOR SIZE DOUBLES.

→ **STEP RULE**

APPLY MATRIX TO CONVERT FROM ONE STATE TO ANOTHER.

→ **MEASUREMENT** → AMPLITUDES

$$\alpha|0\rangle + \beta|1\rangle$$

We will get 0 or 1 when we measure them with probability $|\alpha|^2$ and $|\beta|^2$ respectively. [BAUM'S RULE]

So $|\alpha|^2 + |\beta|^2 = 1$.

When we measure, the qubit will collapse. So if we see $|0\rangle$ after measuring, then the qubit collapses to $|0\rangle$. So run the same program multiple times and get a sense of the probabilities ($|\alpha|^2$ and $|\beta|^2$). We can never know α, β.

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

$$\alpha|0\rangle + \beta|1\rangle$$

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

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

CLASSICAL :

101 : bit string

$$\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Say state is 101, instead of representing in string, lets use the 1-hot notation in UNIT-VECTOR.

LENGTH : 2^3.

=> This is how state will be represented in Quantum (State-space rules). So lets assume similar in a classical computer.

=> If state become 1011 then we need 2^4 vectors. Doubles → Tensor product.

=> STEP : Apply matrix

=> MEASUREMENT : In classical, its just

measuring bit value.

STEP : MATRIX

$$M = \begin{array}{cc|cccc} & & & \text{FROM} & & \\ & & 00 & 01 & 10 & 11 \\ \hline & 00 & 0 & 0 & 1 & 0 \\ \text{TO} & 01 & 1 & 0 & 0 & 0 \\ & 10 & 0 & 0 & 0 & 1 \\ & 11 & 0 & 1 & 0 & 0 \end{array}$$

$$00 \xrightarrow{M} 01 \xrightarrow{M} 11 \xrightarrow{M} 10$$

$$\downarrow$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

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

This is 01.

PROBABILISTIC:

$$\begin{array}{l} \text{Conf. 0} \\ \text{Conf. 1} \end{array} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$$

$p_0, p_1 \in \mathbb{R}$

$0 \leq p_0, p_1 \leq 1$

$p_0 \rightarrow$ Probability being in state 0.

So this can be represented as

$$p_0 . |0\rangle + p_1 . |1\rangle$$

Consider 2 states

$$\begin{pmatrix} p \\ 1-p \end{pmatrix} \quad \begin{pmatrix} q \\ 1-q \end{pmatrix}$$

$p \rightarrow$ probability of being in state 0

$q \rightarrow$ probability of being in state a.

Lets apply Tensor Product

$$\begin{pmatrix} p \\ 1-p \end{pmatrix} \otimes \begin{pmatrix} q \\ 1-q \end{pmatrix} = \begin{array}{c} 0a \\ 0b \\ 1a \\ 1b \end{array} \begin{pmatrix} pq \\ p(1-q) \\ (1-p)q \\ (1-p)(1-q) \end{pmatrix}$$

What about Matrix?

$$
\begin{array}{cc|cccc}
 & & & \text{FROM} & & \\
 & & 00 & 01 & 10 & 11 \\
\text{TO} & \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \multicolumn{4}{c}{\begin{bmatrix} 0 & 1/3 & 1/2 & 0 \\ 1/2 & 1/3 & 0 & 0 \\ 0 & 1/3 & 1/2 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}}
\end{array}
$$

$\downarrow$

Each column sum up to 1.

Now, from 00, with $p = 1/2$, we can go to 01 and $p = 1/2$ to 11.

From Classical (100% to another state), we have moved to probabilities to other states.

In Quantum each element can be a complex number. So each column has complex numbers summing to 1.

$$\begin{array}{c} \begin{pmatrix} p \\ q \end{pmatrix} \end{array} \begin{array}{l} \text{tails} \\ \text{heads} \end{array}$$

$$\begin{pmatrix} P(\text{tails} \mid \text{tails}) & P(\text{tails} \mid \text{heads}) \\ P(\text{heads} \mid \text{tails}) & P(\text{heads} \mid \text{heads}) \end{pmatrix}$$

FAIR COIN :

$$\begin{array}{cc} & \text{FROM} \\ & \begin{array}{cc} T & \quad H \end{array} \\ \text{TO} \begin{array}{c} T \\ H \end{array} & \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \end{array}$$

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} 1/2\,p + 1/2\,q \\ 1/2\,p + 1/2\,q \end{pmatrix}$$

$$= 1/2 \underbrace{(p+q)}_{\downarrow \atop 1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

FROM ANY STATE

$P(H) = P(T) = 1/2.$

IS VECTOR $\begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix}$ POSSIBLE ?

NO!

$$\begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix} \begin{matrix} \rightarrow 0a \\ \rightarrow 0b \\ \rightarrow 1a \\ \rightarrow 1b \end{matrix}$$

$$(0a)(1b) = (0b)(1a) = 0 \cdot 0 = 0$$

$$\downarrow$$

$$\tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4}$$

NOT SAME

So, probabilistic model doesn't explain all states.

	Probabilistic	Quantum
1.	Real numbers	Complex numbers
2.	Vector of probabilities	Vector of amplitudes
3.	$\sum p_i = 1$	$\sum \lvert \alpha_i \rvert^2 = 1$ UNIT VECTOR
4.	Stochastic Matrices (Column sums = 1) (Preserve $\sum p_i = 1$)	Unitary matrices (Unit vector columns) [Converts unit vector to unit vector] (Preserve $\sum \lvert \alpha_i \rvert^2 = 1$).
5.	$\begin{pmatrix} p \\ 1-p \end{pmatrix}$. Coin is either in state H or T. We just don't know	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. STATE IS BASICALLY A SUPERPOSITION OF STATES $\lvert 0 \rangle, \lvert 1 \rangle$. IN OTHER WORDS, it is in a linear combination of the 2 states.

QUANTUM MATRICES:

$$U = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & \\ 01 & \\ 10 & \\ 11 & \end{array} \quad \text{TO} \downarrow \; \text{FROM} \rightarrow \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \\ 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}$$

$$UU^{+} = I = U^{+}U$$ U has to be invertible.

→ Conjugate transpose

$$\text{STATE} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \\ 0 \end{pmatrix}$$

PROBABILISTIC:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rightarrow \text{NOT UNITARY}$$

$$|1/2|^2 + |1/2|^2 = 1/2$$

QUANTUM EQUIVALENT OF FAIR COIN:

HADAMARD:

$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\left|1/\sqrt{2}\right|^2 + \left|1/\sqrt{2}\right|^2 = 1$$

$$\left|1/\sqrt{2}\right|^2 + \left|-1/\sqrt{2}\right|^2 = 1 .$$

Why Fair Coin?

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

$$H|0\rangle = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1/\sqrt{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H|1\rangle = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1/\sqrt{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\alpha = 1/\sqrt{2} \qquad \beta = -1/\sqrt{2}$$

$$|\alpha|^2 = |\beta|^2 = 1/2$$

PROBABILITY OF $1/2$ FOR BOTH STATES.

CLASSICAL NAND:

$$\begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & & & & \\ 01 & & & & \\ 10 & & & & \\ 11 & & & & \end{array} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

RANK = 3

NOT INVERTIBLE

$\Downarrow$

CANNOT IMPLEMENT IN QUANTUM.

NAND ↓

00 → 10

01 → 11

10 → 10

11 → 01

↑ 2ND QUBIT UNTOUCHED

QUANTUM:

$$f : \{0,1\} \to \{0,1\}$$

↳ May not be invertible

$$x \to f(x)$$

$$f(f(x)) \neq x$$

So, we introduce,

$$U_f : \{0,1\}^2 \to \{0,1\}^2$$

$$U_f(x, b) = (x, b \oplus f(x))$$

↳ some bit

$$U_f \cdot U_f(x, b) = U_f(x, b \oplus f(x))$$

$$= (x, b \oplus f(x) \oplus f(x))$$

$$= (x, b)$$

HENCE IT IS INVERTIBLE NOW.

$$(x, b) \longrightarrow (x, b \oplus f(x))$$

to get back x, we need to XOR with $f(x)$ [we need x for that]

$$f(x, b \oplus f(x)) = (x, b).$$

QUANTUM PROGRAM:

QUBIT REGISTERS, x_1, x_2, x_3 IN AN INITIAL STATE.

If we want to do H on x_2 but keep x_1, x_3 as such.

$$H(x_2)$$

$$||$$

$\Downarrow$

TENSOR FOR THIS IS

$$I_1 \otimes H_2 \otimes I_3$$

$\hookrightarrow$ IDENTITY.

$$CNOT(x_1, x_2) \Rightarrow CNOT_{1,2} \otimes I_3$$

PROGRAM	SEMANTICS (MEANING)
$H(x_2)$	$I_1 \otimes H_2 \otimes I_3$
$CNOT(x_1, x_2)$	$CNOT_{1,2} \otimes I_3$

CIRCUIT: