5/07/2019

Quantum Computational & Quantum Info:

-> Prof. Rakesh Shrivasal
Room No: 2011

QCQI -> M.A. Neilson & I.L. Chuang
Quantum Computing Explained - Marko

* Grading:
3 Quizzes : -> 25%
Mid Term : 25%
End Term : 50%

* Quantum :
-> Entanglement, Feynman, Manin (Difficult to simulate on traditional computers)
-> Moore's Law reached threshold of size (Avagadro's Number)

* Computation :
-> Turing Machine Model
-> Peter Shor finds Prime Factorisation Algo in 1995.
Q Hilbert : Can Math problem be ~~s~~ solved algorithmically?
ANS. Turing to solve. Mathematically all Turing Machine are mathematical model & all turing machine are algorithms

Strong Version (Incorrect)
-> Any problem that can be effi. solved on any machine can be solved effi. in Turing Machine.
This is the strong Turing Machine (Disproved)
-> Because deterministically Vs Probabilistic Machine
Now Deutsch proposes Quantum Turing Machines due to underlying quantum nature. (Still to be proved)

-> Heisenberg's Principle : $\Delta x \Delta p \geq h$

* Quantum Information:

→ System ~~Im~~ need not be disturbed, so any disturbance is taken to be Noise.

→ That why I Theory is used.

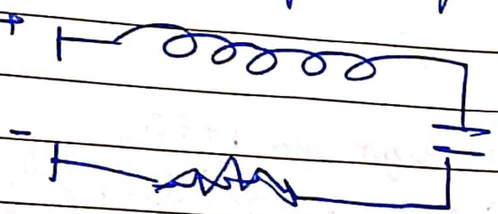
The basic unit of quantum info whose state is unknown cannot be copied.

Analog Computation:

→ By use of Diffraction, use X-Rays diffracted by crystals to compute Fourier Tranform.

→ In some aspects quantum computers are analog.

→



$$V_R = R\frac{dQ}{dt}$$

$$\frac{Q}{C} = V_C$$

$V_R + V_C + V_L =$

$$V_L = L\frac{d^2Q}{dt^2}$$

$$\Rightarrow R\frac{dQ}{dt} + \frac{Q}{C} + L\frac{d^2Q}{dt^2} = 0$$

{Electrical} → Both Inertial

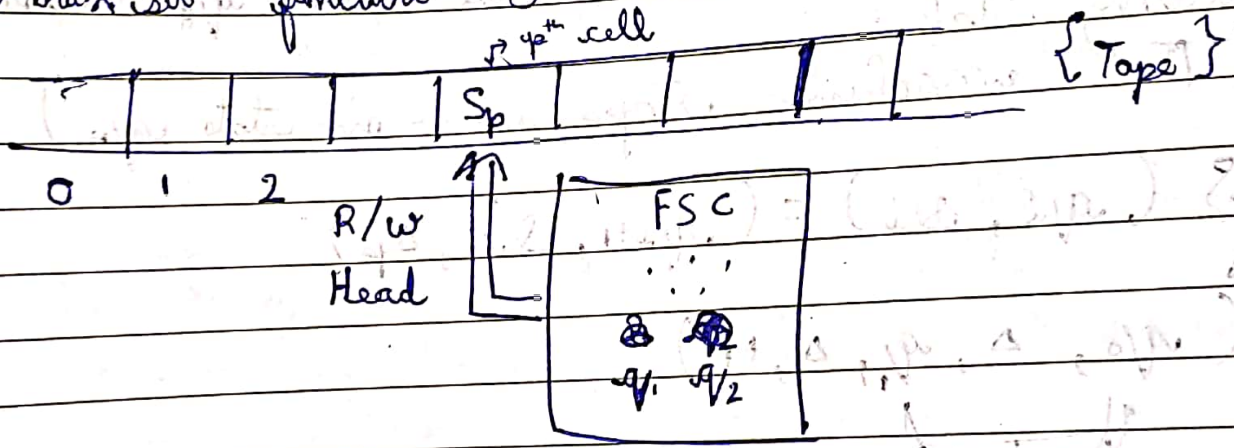
{Mechanical} ∴ Systems are analoguous

Classical Computation:

→ Finite State Machine
→ PDA
→ TM (Turing Machine)

Turing Machine: has the following components:

- a finite set S (alphabet)
- an element $\sqcup \in S$ (blank symbol)
- a set $A \subseteq S$ (ext. alphabet)
  $\sqcup \notin A$
- a finite set Q whose elements are the state of a TM.
- an initial state $q \in Q$
- a Transition function $\delta : Q \times S \to Q \times S \times \{-1, 0, 1\}$



$$\delta(q, s_p) = (q', s_p', \Delta p) \quad \Delta p \in \{-1, 0, 1\}$$

$$\langle \alpha, \sqcup, \sqcup, \sqcup, \ldots, 0, q_0 \rangle$$

↓ Head Position (under 0)
↳ Initial State (under q_0)

$< S_0, S_1, \ldots S_{p-1}, S_p, S_{p+1}, p+\Delta p, q' >$

→ For some inputs the machine will ~~no~~ never stop. In such a case the ~~machine~~ problem cannot be solved.

→ If $p = 0$ & $\Delta p = 1$, Then turing machine will stop.

Eg.: Suppose we are given a string of 0 & 1s and we want to replace this string by $1 \sqcup \sqcup$.

$S = \{ 0, 1, \sqcup, \Delta \}$

↳ Special symbol indicating the beginning of the string.

We will also use a special state q_H called the halting state.

(The machine stops when in state q_H)

$\delta(q_i, s_i) = (q_{i+1}, s_i', \Delta p)$

If Δ

$(q_0, \Delta, q_1, \Delta, +1)$

To diff. b/w 2 states.

If 0

$(q_1, 0, q_1, \sqcup, +1)$ { Replaces 0 by blank & shifts to right }

If 1

$(q_1, 1, q_1, \sqcup, +1)$

If $\sqcup$

$(q_1, \sqcup, q_2, \sqcup, -1)$

PAGE NO.:
DATE: / /

→ If function gives YES & NO {Predicates}

→ If func^n gives no certain YES & NO {Non-Predicate

Non-Computable Predicate}

If $\sqcup$ & q_2

$(q_2, \sqcup, q_2, \sqcup, -1)$

If Δ & q_2

$(q_2, \Delta, q_3, \Delta, +1)$

If Δ & q_3

$(q_3, \sqcup, q_H, 1, 0)$

5 Internal States : q_1, q_2, q_3, q_0, q_H

4 Alphabets : $1, 0, \sqcup, \Delta$

7 Transition States

Diff b/w FSM & Turing

→ Read → Read & Write

→ Forward Only → Move Forward & Backward.

Eg: Design a TM which will compute the parity of a binary string that is i/p to the machine. It writes 0 if the parity is even & writes 1 if the parity is odd.

Computable Functions:

Def: A func^n $f: A^* \rightarrow A^*$ is called computable if $\exists$ a TM M such that the function

ϕ_M that M computes is equal to f for every $x \in A^*$

$$\phi_M(x) = f(x) \quad \forall x \in A^*$$

A^* = set of all strings over A.

PAGE NO.:
DATE: / /

-> Universal TM can mimick the behaviour of other TM. Hence programmable.
-> Not all problems are computable

Church - Turing thesis:
This statement has not be proved & is an empirical statement.
The class of functions computable by a TM corresponds exactly to the class of functions which are regarded as being computable by an algo.

$\boxed{\text{Algorithm} \iff \text{TM}}$

-> TM solved the halting problem, ~~can a TM~~ predict that given an input to a Turing Machine will it stop or not. Turing proved that prediction is not possible.

Computational Complexity:
Classical Physics Vs Quantum Physics
-> Deterministic -> Probabilistic
-> Non-Deterministic Not same as ~~probabilistic~~ probabilistic
Physics is implicit since the READ/WRITE head moves.

-> TM helps to calculate comp. complexity

To Compare -> Time + Energy
-> Space

Complexity Classes
Exact Time is of much significance as in Multiple Tape System, Probabilistic, Deterministic

Asymptotic behaviour (Resources Req. in the limit of large n, $n \to \infty$)

n^3

$2n$

* Asymptotic notation

$O \rightarrow$ worst case scenario (sets the Upper bound)

$\Omega \rightarrow$ the best possible one can do (sets the lower bound on the resource requirement)

If $f(n)$ & $g(n)$ are two functions, one says $f(n)$ is in class $O(g(n))$ if $\exists$ constants c & n_0 such that for all $n > n_0$

$$f(n) \le cg(n)$$

III $f(n)$ is in class $\Omega(g(n))$ if $\exists$ constants c & n_0 such that for all $n > n_0$

$$f(n) \ge cg(n)$$

$\Theta \rightarrow$ $f(n)$ is $\Theta(g(n))$ if $f(n)$ is both $\Omega(g(n))$ & $O(g(n))$

i.e. $f(n) \sim cg(n)$

for $n > n_0$

Eg: Let $f(n) = n^2$

$g(n) = \log n$

$f(n)$ is $\Omega(g(n))$

PAGE NO. :
DATE : / /

Recognisable Problem : Answer is TRUE machine will stop else infinite loop possible

Turing Decidable if ans. T/F the machine will stop.

It is clear that if $f(n)$ is $O(g(n))$ then $g(n)$ is $\Omega(f(n))$

Eg: Suppose $f(n) \sim n^3$
$g(n) \sim 2^n$

$$f(n) \text{ is } O(g(n))$$

The class of functions computable in polynomial time by a TM is called class P.

The space requirement for problems in class P is obviously a polynomial in the size of the i/p.

A function / decision prob. F is said to be computable/ decidable in polynomial space if $\exists$ a TM that computes / decides F & runs in space $S(n) = poly(n)$
The class of all such problems is called PSPACE

It is clear that

$$P \subseteq PSPACE$$

Ex: Prove that $f(n)$ is $O(g(n))$ iff $g(n)$ is $\Omega(f(n))$

Known ~~$g(n) \geq c f(n)$~~

$g(n)$ is $\Omega(f(n))$

$\Leftrightarrow$ $g(n) \geq f(n)$

$\Leftrightarrow$ $f(n) \leq g(n)$

$\Leftrightarrow$ $f(n)$ is $O(g(n))$

* P → Whether a number is composite & Prime.

* NP → Factorisation

PAGE NO.:
DATE: / /

Ex: Show that $\log n$ is $O(n^k)$ for any $k > 0$

ANS

$f(n) = \log n$
$g(n) = n^k \quad k > 0$

$\log n \le n^k$

$f(n) \le g(n)$

$\therefore f(n)$ is $O(g(n))$

Problems for which resource requirement grows faster than any polynomial in n case (wrongly) said to belong to exponential class (EXP).

$c^n \qquad c^{\log n}$

NP → decision problems
↓
Non-Deterministic Polynomial (are problems which can be solved in P on non-deterministic Turing Machine but not on a standard Turing Machine)

$P \subseteq NP$

NP Complete (Read)

BPP (Bounded Error Probabilistic)

BQP (Read)

Scanned by CamScanner

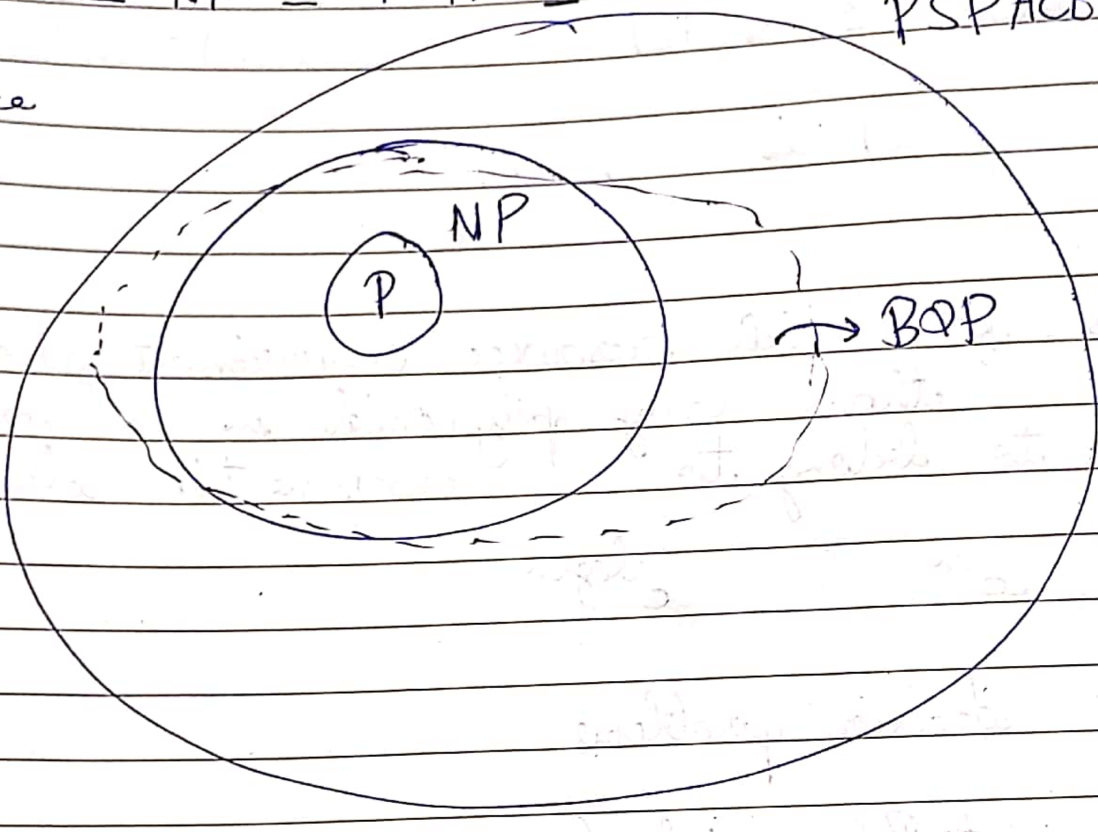
PAGE NO. :
DATE : / /

Heirarchy of Complexity Space:

$L \subseteq P \subseteq NP \subseteq PSPACE \subseteq EXP$

↓

Log Space

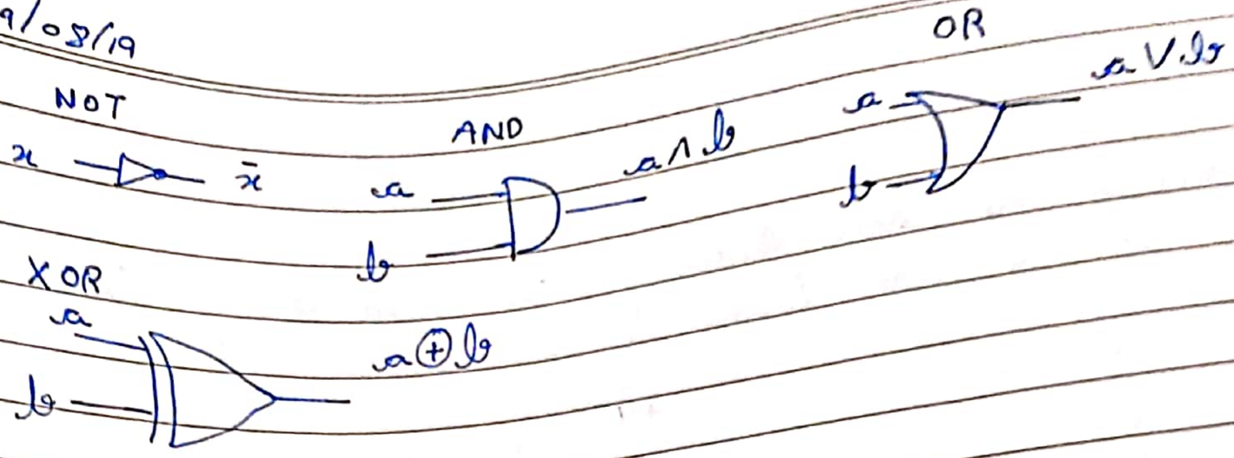


Ramification Vice-Versa

NAND & NOR Gate {Universal}

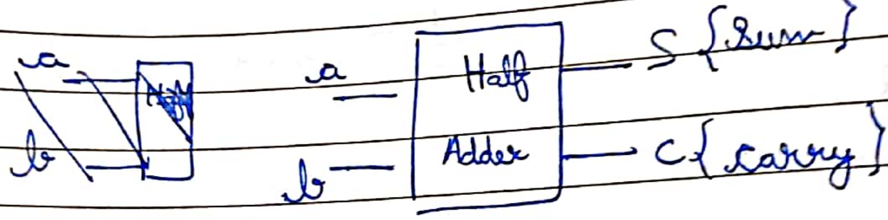
PAGE NO.:
DATE: / /

19/08/19



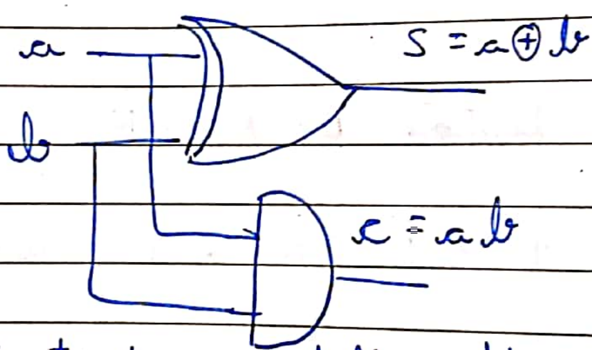
* Circuits: wires & gates.
  binary logic - $\mathbb{B} = \{0, 1\}$
  Acyclic ckt i.e. no feedback

Eg: Half Adder

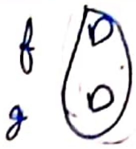


a	b	S	C
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

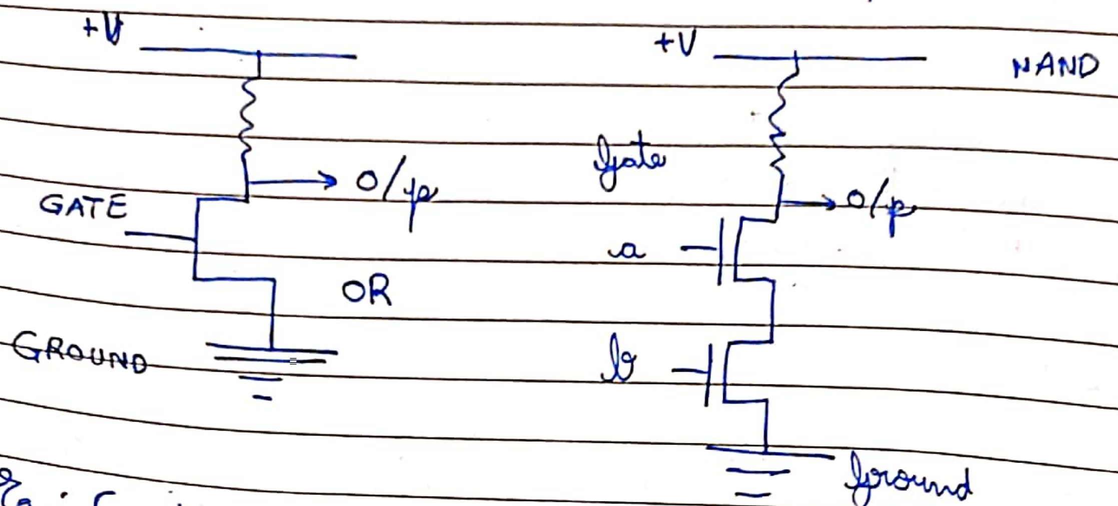
$S = a \oplus b$
$C = ab$



Ex: Construct a full adder
① Directly using XOR, AND & OR
② Using Half Adder



Ex : How many half Adder are reqd to add two n-bit binary nos? Design the corresponding ckt.



Eg : Construct NOR.

A general logic is a function $f : B^n \to B^m$ where $B = \{0,1\}$

If $m = 1$ ie. if $f\ B^n \to B^1$ then f is called a boolean function

→ Minimal set for all logical function then the set is complete (Completeness or the basis)

∴ the function can be expressed in terms of the elements of the minimal set. Eg (i, j, AND, NOT)

$(a+b) = (\bar{a} \cdot \bar{b})$ (De-Morgan's Theorem)

Proof that AND, OR & NOT form a complete set for any boolean function.

Disjunctive Normal Formal & Conjunctive Normal Form :

Any boolean functⁿ can be represented in terms of its TRUTH Table.

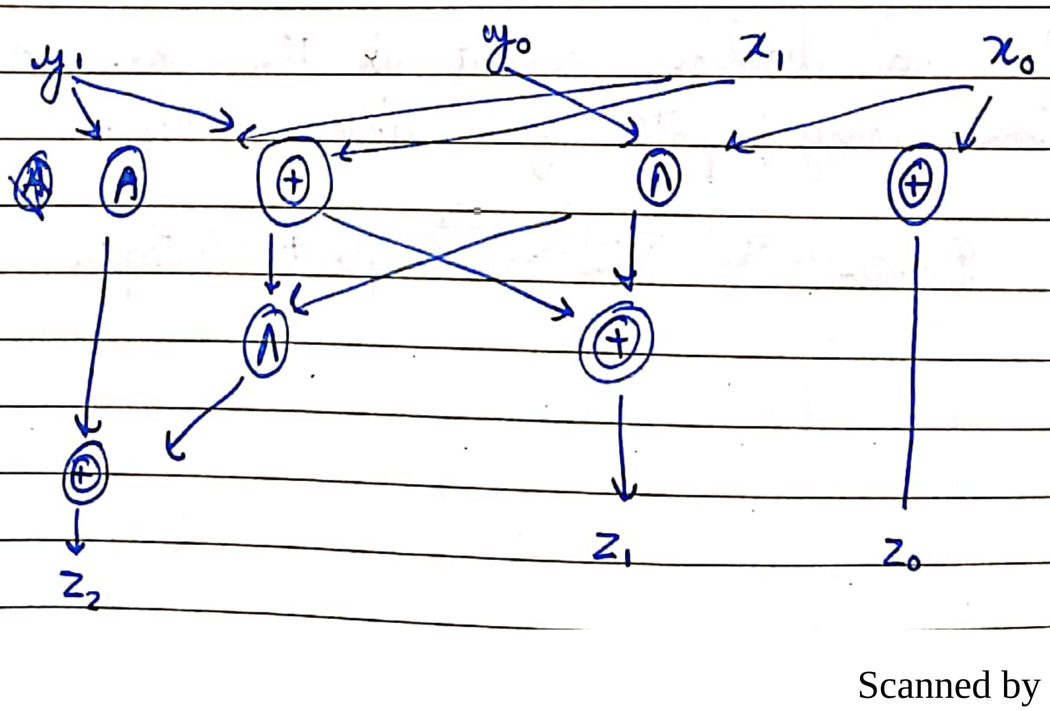
x	y	z	f
0	0	0	0
0	0	1	1
			0
			0
			0
			0
1	1	0	1
1	1	1	0

$x'y'z + xyz'$

Ex : How many distinct n-variable boolean functⁿ are possible?

(ANS) 2^{2^n} { If not boolean : $(m)^{m^n}$ }

Circuits can also be represented in terms of (acyclic) graphs.



Check that the ckt represents the binary addition of two 2-bit binary nos.

Size (a measure of complexity of a circuit)
No. of gates in the circuit.

The minimal size of a circuit over a basis A (($\wedge, \oplus$) in the graph) that computes a given functⁿ f is called the circuit complexity of the funcⁿ (wrt basis A) & is denoted $C_A(f)$.

In going from one basis A_1 to another basis A_2 the circuit complexity changes only a constant multiple i.e.

$$C_{A_1}(f) = O(C_{A_2}(f))$$

and

$$C_{A_2}(f) = O(C_{A_1}(f))$$

$$\Rightarrow \quad C_{A_1}(f) = \Theta(C_{A_2}(f))$$

Basis need not be explicitly mentioned since change by a const.

Depth : of a boolean circuit is the max. no. of gates on any path from i/p to o/p.

Depth $\propto$ Time Complexity $\propto$ Depth

Reversible Computation (Thermodynamics)

Turing Machine versus ckt model:

Circuit Model is non-uniform as opposed to the TM model which is <u>uniform</u>.

Circuit family (for a particular computational problem)

Notation : $\{C_n\}$
$\hookrightarrow$ i/p size

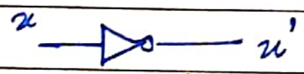
<u>Consistent family</u>

If $m < n$ & if the i/p x is of size is m then the o/p

$$C_m(x) = C_n(x)$$

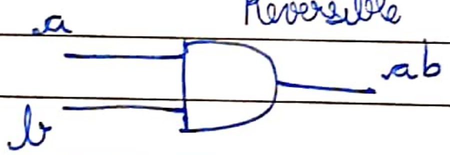
If a TM M O/ps a description of $C_n \forall n \in \mathbb{N}$ in polynomial time then the ckt-family is said to be <u>polynomial time uniform</u>.

★ **Reversible Computation :**



Reversible

x	$\bar{x}$
0	1
1	0



Irreversible

info. Erased

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

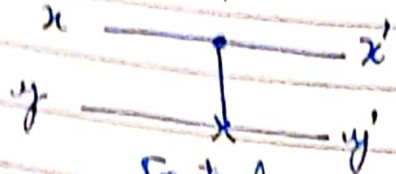
⇒ ~~Landaur~~ → Landauer : the energy dissipated by a computer in erasing a single bit is $k_B T \log 2$.

"Information is Physical"

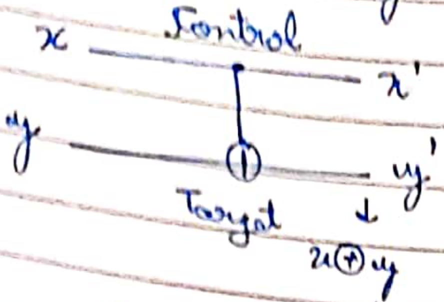
CNOT implements XOR, FANOUT, & NOT

PAGE NO. :
DATE : / /

✡ CNOT :



(there prime doesn't denote the NOT operation)

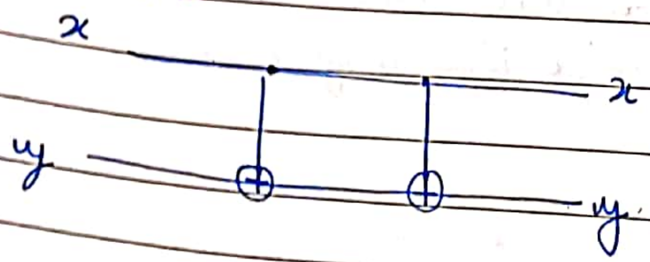


CNOT is a 2 i/p 2 o/p reversible gate.

The dot on the upper wire is the CONTROL bit & the bit on the lower wire is the target bit.

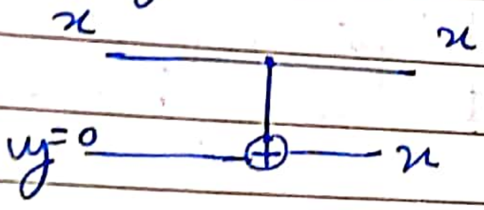
x	y	x'	y'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

EXER : Check

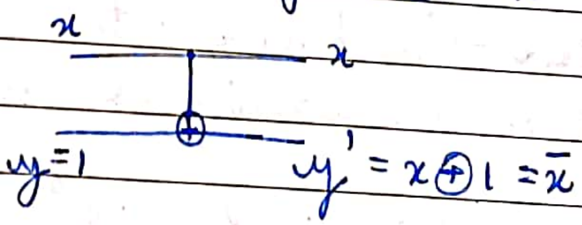


If $y = 0$ then

$y' = x \oplus 0 = x$

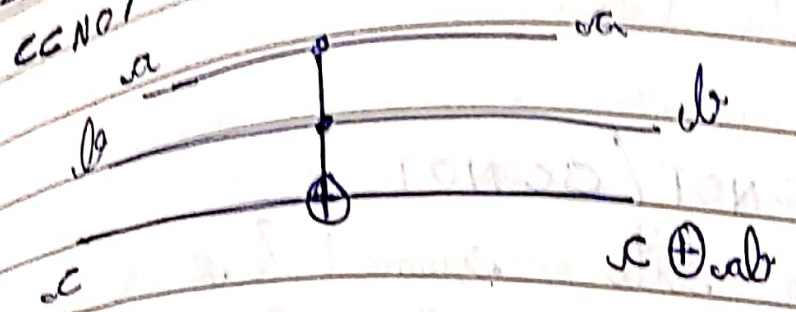


(FANOUT) $y' = x \oplus 1 = \bar{x}$



Scanned by CamScanner

21/8/19 CCNOT (Controlled Controlled NOT) [Toffoli Gate]



a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

★ Reversible Universal:

① If $c = 0$ then the o/p on the target line is ab. i.e. AND operation.

② Suppose we fix $a = 1$ but leave b & c arbitrary then o/p on target line is $c \oplus b$ => XOR gate.

③ If $a = b = 1$ then the Toffol gate function as NOT gate.

Ex: Construct a NAND gate using a ~~one~~ single CCNOT gate.

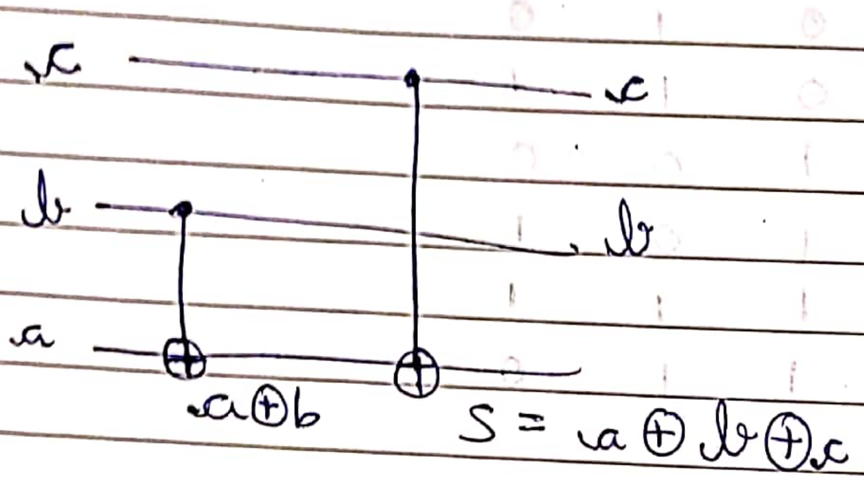
Ex: Construct FANOUT from a single CCNOT.

Bits which are permanently fixed to some definite value are called ancilla bits.

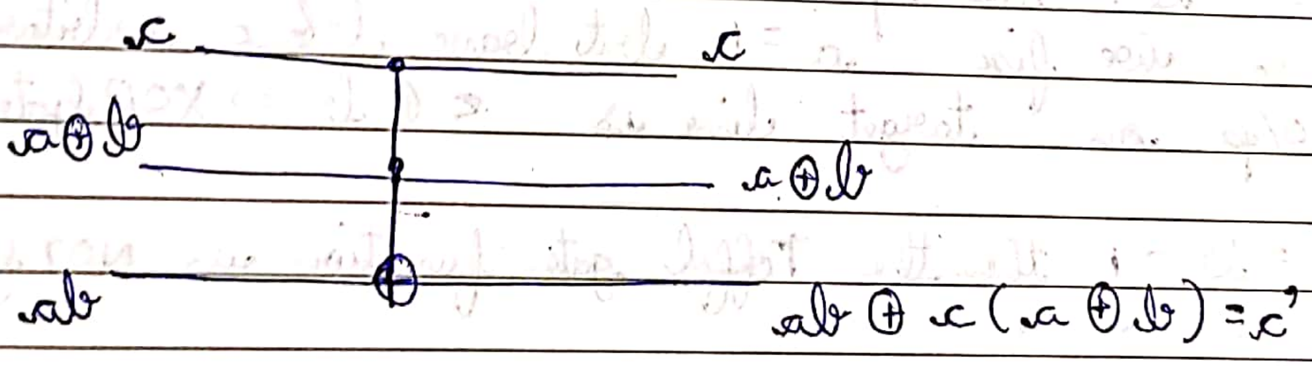
Binary Addition using CNOT / CCNOT

If a, b are the bits sumed & c is a previous carry then sum $S = a \oplus b \oplus c$ & carry

$$c' = ab \vee bc \vee ca$$
$$= ab \oplus bc \oplus ca$$



$$c' = ab \oplus c(a \oplus b)$$



To obtain $a \oplus b$ on the 2^{nd} control line use CNOT & to obtain ab on the i/p of the target above, use another CCNOT.

SWAP:

Physics of Computation:

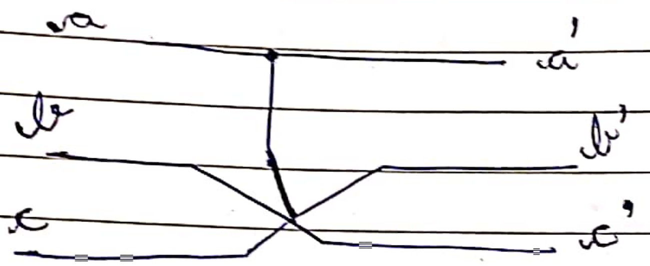
Q How is physics involved in computation?

- → Movement during read & write.
- → I/p & o/p & their manipulation
- → Billard ball Computation (Motion of Ball)
- →

Billiard Ball Computer or the Fredkin Gate:

↓

Controlled SWAP gate.

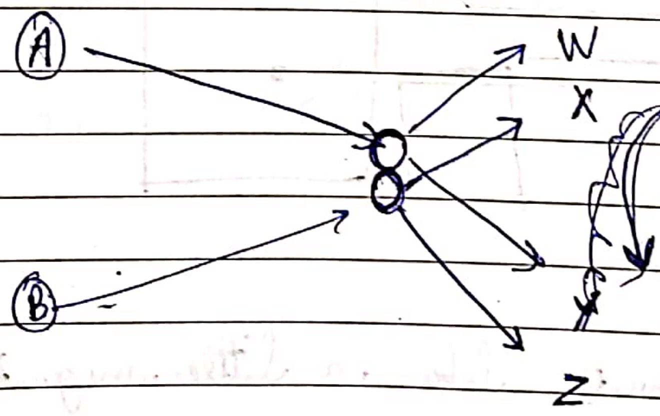


a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Universal Gate **

$a = 0$, ⇒ $b' = b$, $c' = c$

$a = 1$, ⇒ $b' = c$, $c' = b$



If $A = 1$, $B = 0$ ⇒ No Collision

⇒ $Y = 1$, $W = X = Z = 0$

ly, $A = 0$, $B = 1$, $X = 1$ all other are ~~zo~~ zero.

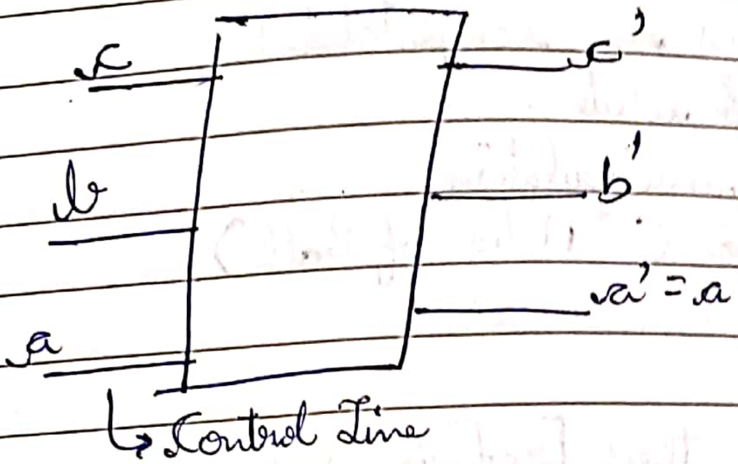
$Y = A \wedge \bar{B}$

$X = \bar{A} \wedge B$

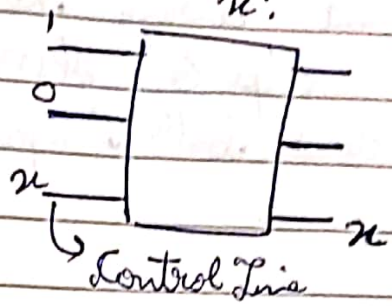
If $A = 1 = B$

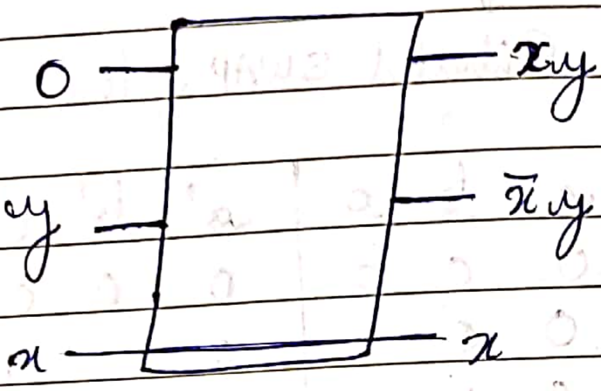
⇒ $W = Z = 1 = A \wedge B$

$X = Y = 0$



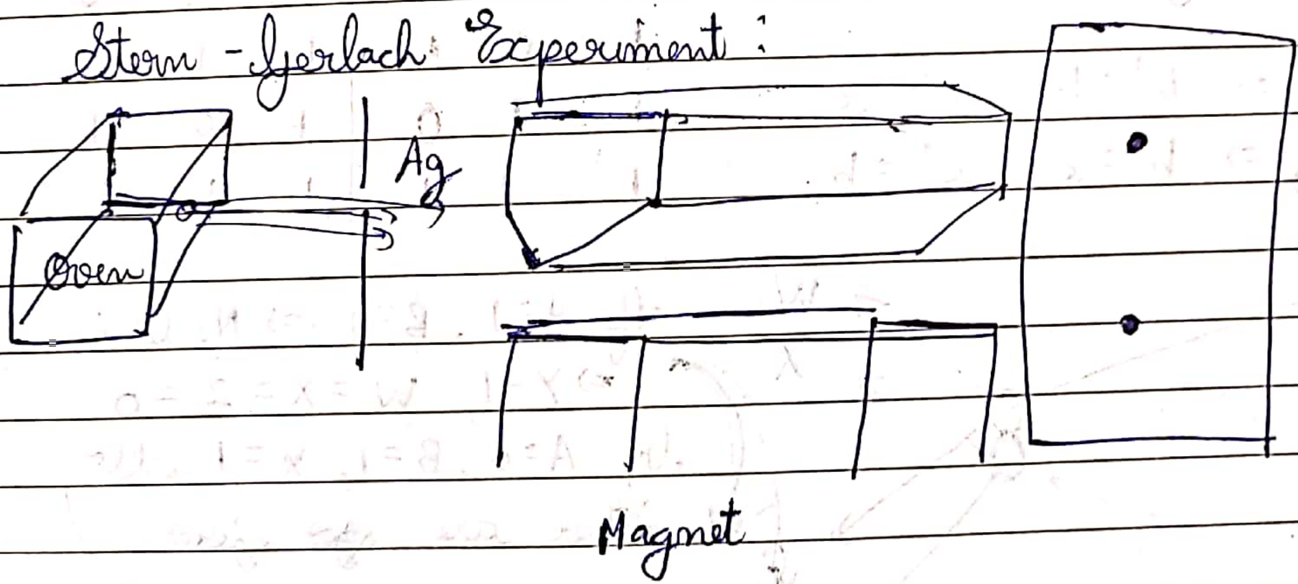
Ex. Find in terms of x?





Quantum Mechanics:

Stern-Gerlach Experiment:



Every silver atom behaves like a little magnets

If it has magnetic moment μ & the Mag. field is $\vec{B}$ then $\Delta U = -\vec{\mu}\cdot\vec{B}$ is the change in energy $= -\mu B\cos\theta$

DATE : / /

θ is the $\angle$ between the direction of $\vec{\mu}$ & $\vec{B}$.
We take $\vec{B}$ to point in z-direction $\Rightarrow$ θ is the $\angle$ between the direction of $\vec{\mu}$ & the z-axis

Force $= -\vec{\nabla} V$ {Potential}

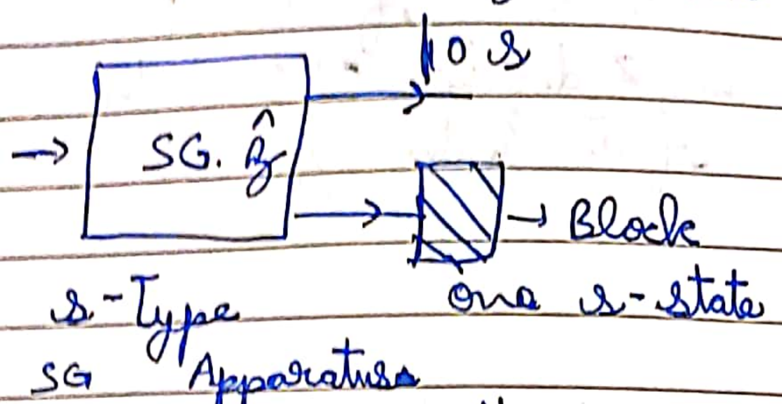
B'cos of the sharp magnetic pole the $\vec{B}$ field is not uniform & there will be a force of the Ag atoms

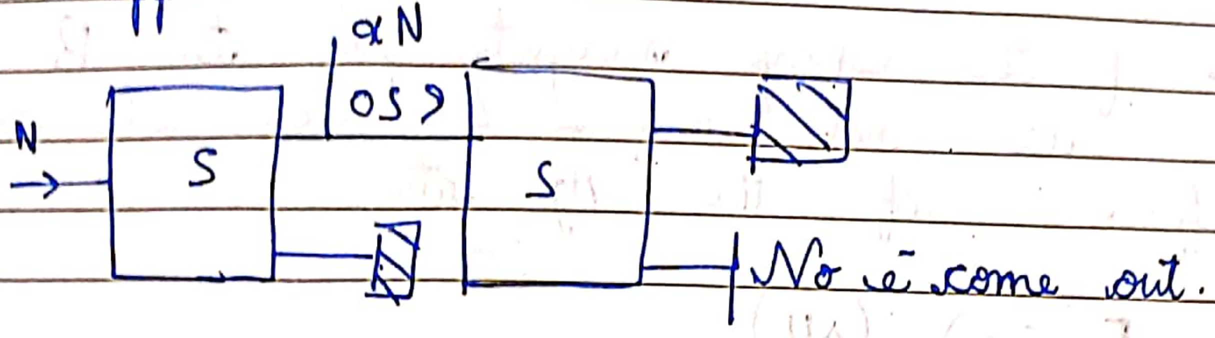
$$F_z = -\frac{\partial}{\partial z}(\Delta U)$$

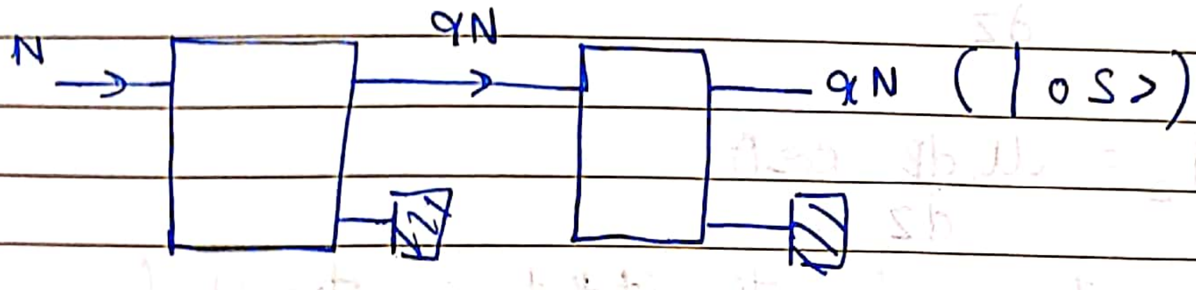
$$F_z = \mu \frac{dB}{dz} \cos\theta$$

Now it can be thought that a straight line is to be expected but it is found that there are only 2 spots found for any orientation of the magnet.

→ We say that the mag. moment & hence the spin of the unpaired $\bar{e}$ are quantised & can have 2 possible spin states ~~not~~







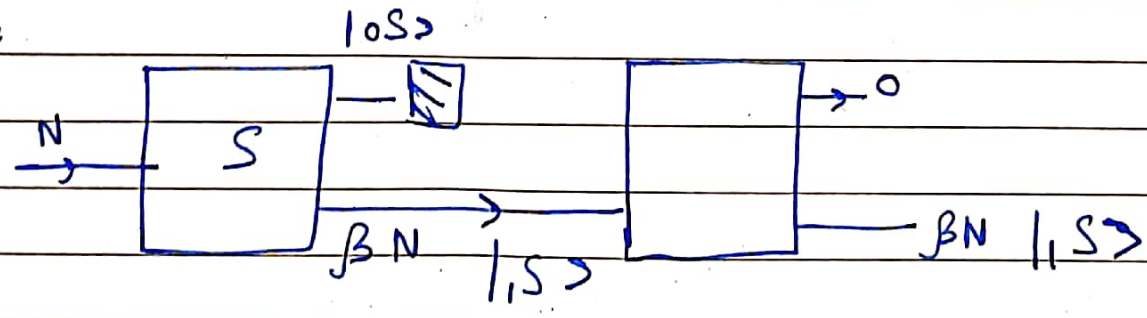
$\langle {}_1S \,|\, {}_0S \rangle = 0$ Prob. Amp. for e in $|{}_0S\rangle$ state to go in the $|{}_1S\rangle$ state

Final State ↵ ↳ Initial State

$\langle {}_0S \,|\, {}_0S \rangle = 1$

final initial

For



we ||| find: $\langle {}_0S \,|\, {}_1S \rangle = 0$

$\langle {}_1S \,|\, {}_1S \rangle = 1$

End \ Initial	$\|{}_0S\rangle$	$\|{}_1S\rangle$
$\|{}_0S\rangle$	1	0
$\|{}_1S\rangle$	0	1

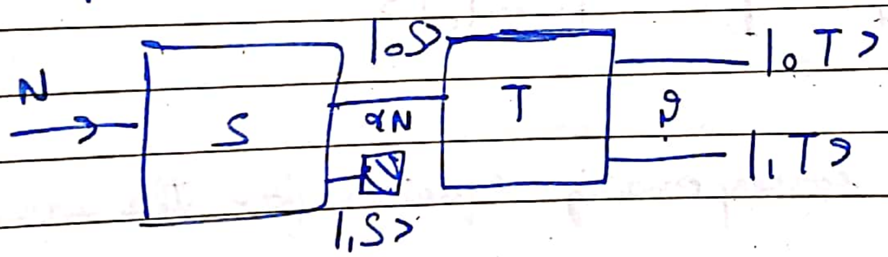
→ In general, the notation $\langle b|a\rangle$ gives the prob. amp. for starting starts $|a\rangle$ to be found in state $|b\rangle$

→ The prob. for the process is given by the absolute sq. of the prob. amplitude

ie. $P(|a\rangle \to |b\rangle) = |\langle b|a\rangle|^2$
$= \langle b|a\rangle \langle b|a\rangle^*$

* denotes complex conjugate.

Consider another SG arrangement say, T-type (where the ~~mg~~ magnetic field is oriented differently compared to the s-Type)



$\langle {}_1T|{}_0S\rangle \neq 0$

$\langle {}_0T|{}_0S\rangle \neq 0$

& likewise, if we select the $|{}_1S\rangle$ state from the 1st SG arrangement, we find

Scanned by CamScanner

$\langle {}_0T | {}_1S \rangle \neq 0$

$\langle {}_1T | {}_1S \rangle \neq 0$

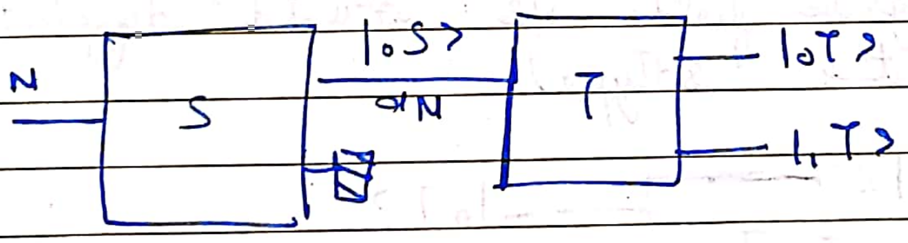
	Initial	
	$\vert {}_0S \rangle$	$\vert {}_1S \rangle$
$\vert {}_0T \rangle$	$\langle {}_0T \vert {}_0S \rangle$	$\langle {}_0T \vert {}_1S \rangle$
$\vert {}_1T \rangle$	$\langle {}_1T \vert {}_0S \rangle$	$\langle {}_1T \vert {}_1S \rangle$

If no e^- are created or absorbed then the no. of e^- coming out of the T-type arrangement with both $|{}_0T\rangle$ & $|{}_1T\rangle$ channels open is the same as the no. e^- entering the T-type apparatus in the $|{}_0S\rangle$ state. (statement of conservation of e^- no. or of prob. conservation)

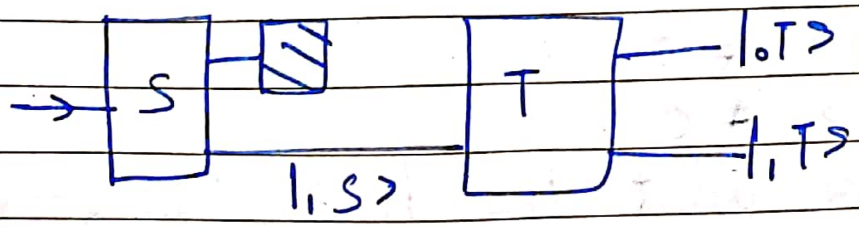
$$|\langle {}_0T | {}_0S \rangle|^2 + |\langle {}_1T | {}_0S \rangle|^2 = 1$$

or

$$\langle {}_0T | {}_0S \rangle \langle {}_0T | {}_0S \rangle^* + \langle {}_1T | {}_0S \rangle \langle {}_1T | {}_0S \rangle^* = 1$$



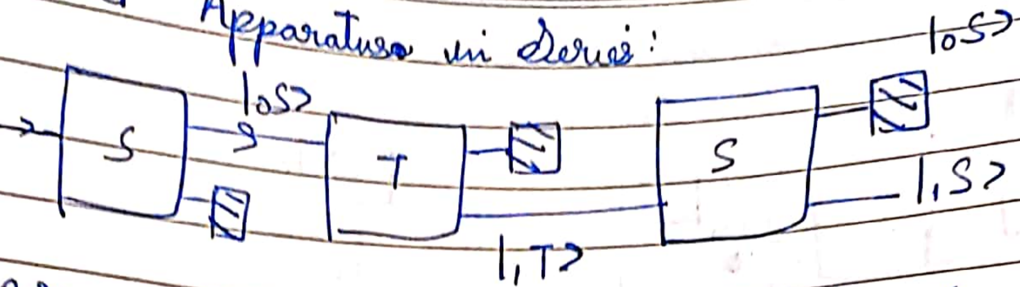
Ex: What is the corresponding equation for the arrangement



$|\langle {}_0T | {}_1S \rangle|^2 + |\langle {}_1T | {}_1S|^2 = 1$

DATE : / /

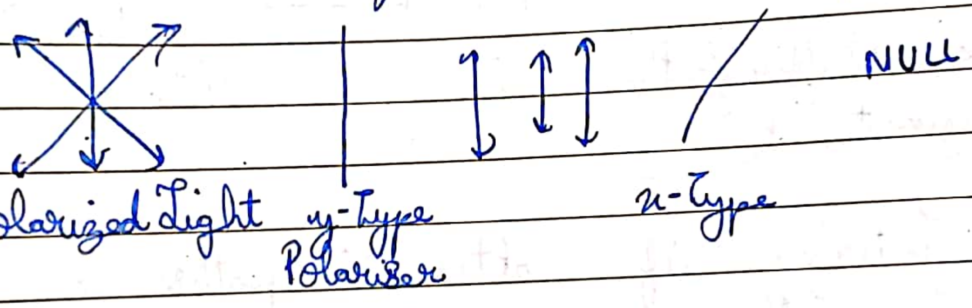
S-G Apparatus in Series:



We find the o/p from $|1S>$ channel of the 3^{rd} apparatus is not zero.

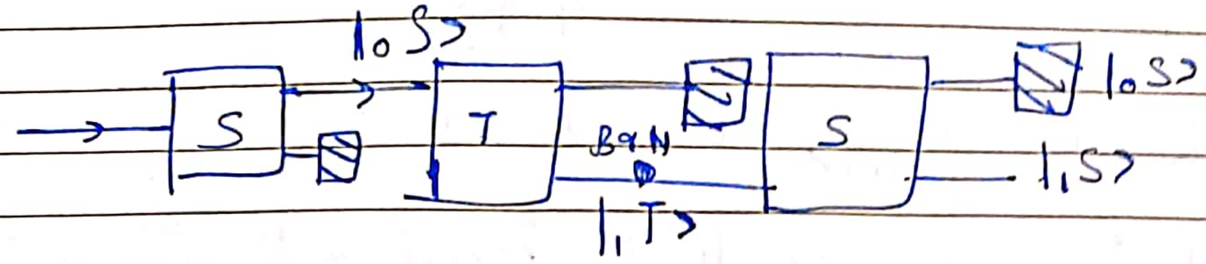
Likewise, the o/p from the $|0S>$ arm is in general non-zero.

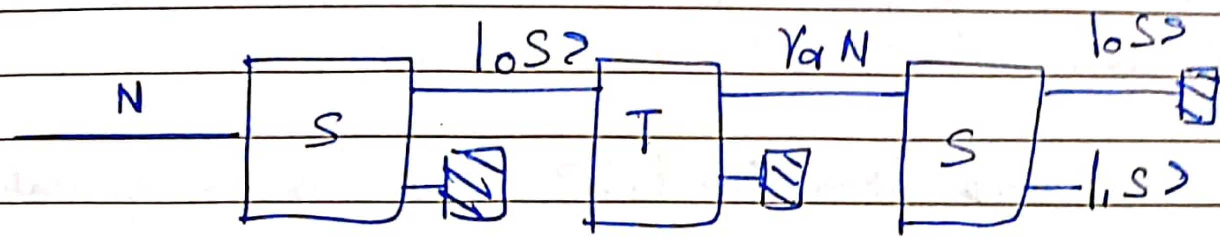
Selection of $|1,T>$ state by the 2^{nd} apparatus completely destroys any information about the previous state of the e^- (namely $|0S>$ in the present case)

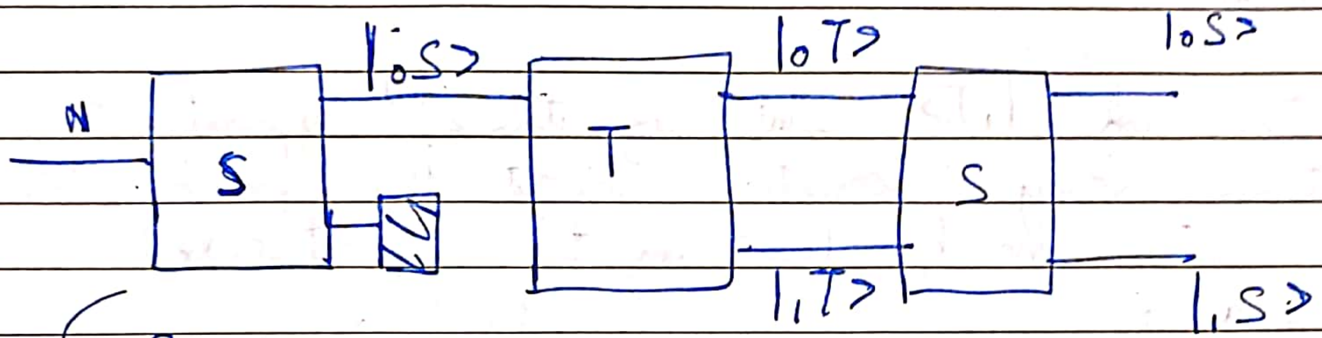


Base States: We say that filtering process separates the system in base states (wrt that particular apparatus) & the future behaviour of the system in a particular base state depends only on that state.

☆ S-G Apparatus in Series:







{Analogous to Young's Double Slit Arrangement}

Nothing comes out

Prob. Amp. Interfere if alternative paths are available for the same starting condition & same final condition.

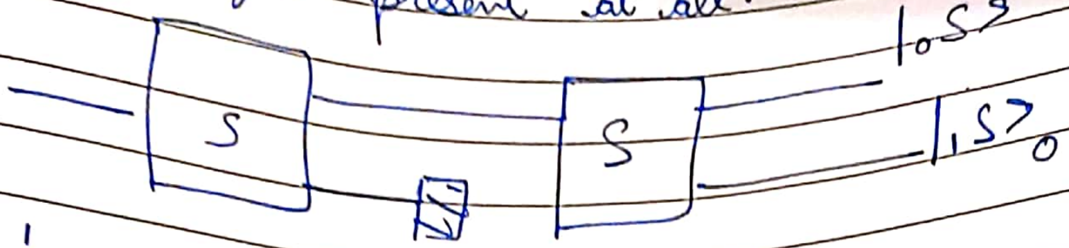
$$\langle {}_1S | {}_0T\rangle \langle {}_0T | {}_0S\rangle + \langle {}_1S | {}_1T\rangle \langle {}_1T | {}_0S\rangle = 0 \quad \text{—(1)}$$

Ex: All the e^- come out in the $|_0S\rangle$ state of the 3rd apparatus. Write the Expression III to (1) to describe this

$$\langle {}_0S | {}_0T\rangle \langle {}_0T | {}_0S\rangle + \langle {}_0S | {}_1T\rangle \langle {}_1T | {}_0S\rangle = 1$$

DATE :

A wide open T apparatus is equivalent to the apparatus not being present at all.



$$\sum_{i=0}^{1} \langle {}_0S | i \rangle \langle i | {}_0S \rangle = 1 = \langle {}_0S | {}_0S \rangle$$

$$\sum_{i=0}^{1} \langle {}_1S | i \rangle \langle i | {}_0S \rangle = 0 = \langle {}_1S | {}_0S \rangle$$

Nothing special about $|{}_0S\rangle$ & $|{}_1S\rangle$ states

$$\langle x | \varphi \rangle = \sum_{i=0}^{1} \langle x | i \rangle \langle i | \varphi \rangle$$

$$\left(\Rightarrow \sum_{i=0}^{1} | i \rangle \langle i | = 1 \right)$$

$$\langle j | i \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

(here $|i\rangle$ & $|j\rangle$ are the states wrt. the same kind of SG apparatus)

$$\langle j | i \rangle = \delta_{ji} \text{ (Kronecker Delta Symbol)}$$

$$\delta_{ji} = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

$$\delta_{00} = 1 = \delta_{11} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\delta_{01} = 0 = \delta_{10}$$

2/9/19

Linear Algebra: (Vector Space)

Def: A vector space is a set S whose elements are called vectors (denoted by $|\rangle$) with following 2 operation defined:

① Vector Addition: If $|a\rangle, |b\rangle \in S$ then $|a\rangle + |b\rangle \in S$

② ~~Multiplica~~ Multiplication of a vector by a scalar (complex no. for us) if $\alpha \in \mathbb{C}$ & $|a\rangle \in S$, then $\alpha|a\rangle \in S$

~~Bcos~~ (Because the scalar for us belong to $\mathbb{C}$, the vector space is a complex vector space; if scalars $\in \mathbb{R}$ then ~~we~~ we have a real vector space)

③ In addition, S consists of a special vector, the zero ~~vector~~ vector (0_v) such that

$$|a\rangle + 0_v = |a\rangle \quad \forall \ |a\rangle \in S$$

④ For every $|a\rangle \in S$ there is a $|a'\rangle \in S$ such that

$$|a\rangle + |a'\rangle = 0_v$$

Vector addition is commutative

$$|a\rangle + |b\rangle = |b\rangle + |a\rangle \quad \forall \ |a\rangle, |b\rangle \in S$$

& and also associative:

$$|a\rangle + (|b\rangle + |c\rangle) = (|a\rangle + |b\rangle) + |c\rangle$$

PAGE NO.:
DATE: / /

* Scalar Multiplication:
follows the usual commutative, associative & distributive laws. $\alpha, \beta \in \mathbb{C}$

$$\alpha(\beta|a\rangle) = (\alpha.\beta)|a\rangle$$
$$(\alpha+\beta)|a\rangle = \alpha|a\rangle + \beta|a\rangle$$
$$\alpha(|a\rangle + |b\rangle) = \alpha|a\rangle + \alpha|b\rangle$$

Ex: Is the set of all quadratic polynomials over real nos. a vector space? ax^2+bx+c

* Linear Independence of Vectors:
A set of vectors $|v_1\rangle, |v_2\rangle, \_\_, |v_N\rangle$ is said to be linearly independent if a relation $\sum_{i=1}^{N} \lambda_i |v_i\rangle = 0$ —(1)

necessarily $\Rightarrow$ $\lambda_i = 0 \ \forall i$

On the other hand if (1) holds with atleast two λ_i's non-zero then the set of vectors is linearly dependent.

Eg: in R^2, $a_x \hat{i} + a_y \hat{j} = 0$
$\Rightarrow a_x = 0 = a_y$

$\Rightarrow \hat{i}$ & $\hat{j}$ are linearly independent.

Dimension of a Vector Space: is the ~~no~~ max. no. of linearly independent vectors in that space.

Scanned by CamScanner

In practical Q. Mechanics, the dimensions are ~~not~~ indefinitely infinite due to infinite states possible.

PAGE NO. :
DATE : / /

* Span : A subset of vectors in S with the property that any vectors in S can be expressed in terms of the vectors in the subset is said to span S.

If $|V_1\rangle, |V_2\rangle, \ldots, |V_N\rangle \in S$ & satisfy the propo. that any $|a\rangle \in S$ can be written as
$$|a\rangle = \sum_{i=1}^{N} a_i |V\rangle$$ then

the set $|V_i\rangle$ span S.

Basis: A set of linearly independent vectors in S which span S is said to form a basis for S.

* Postulates of Quantum Mechanics :

① Any isolated (or closed) physical system has an associated (complex) vector space also called the state space of the system. The state of the system is described by a vector (the state vector) in the state space.

Dim of state space depends on the system under consideration

$|a\rangle \rightarrow$ ket vectors &

state space also called ket space

&

state space also called ket space

$|0\,S\rangle, |1,T\rangle$

If $|a\rangle$ & $|b\rangle$ are any two ~~ket~~ ket vectors then their sum is another ket vector.

$$|a\rangle + |b\rangle = |c\rangle$$

$\alpha |a\rangle$ $(\alpha \in \mathbb{C})$ is another ket ~~vec~~ vector

* In Q. Mechanics $|a\rangle$ & $\alpha|a\rangle$ describe the same state.

If ~~we~~ we multiply $|a\rangle$ by the number zero we get the zero vector $0.|a\rangle = 0_v$

A more general linear combination of state vectors will be

$$\alpha|a\rangle + \beta|b\rangle, \quad \alpha, \beta \in \mathbb{C}$$

& ~~we~~ we say that this represents a linear superposition of $|a\rangle$ & $|b\rangle$.

2 Observables (for eg: position, momentum, spin etc) are represented by linear operators on the vector space (we denote operators as $\hat{O}$, $\hat{A}$ etc)

Op' act on ket vectors from the left:

$\hat{A}(|c\rangle) \equiv \hat{A}|c\rangle$ & the result is another ket.

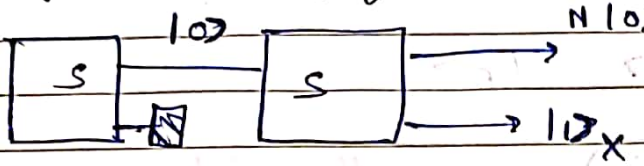
$$|\beta\rangle = \hat{A}|c\rangle$$

Sometimes the action of an operation on a vector gives the same vector multiplied by a number

$$\hat{A}|a\rangle = a|a\rangle$$

Scanned by CamScanner

In such cases we say that $|a\rangle$ is an eigenvector of $\hat{A}$ belonging to eigenvalue a.



$$S_z |0\rangle = \frac{\hbar}{2} |0\rangle$$

$$S_z |1\rangle = -\frac{\hbar}{2} |1\rangle$$

Eigenvalue of Z Axis.

→ Comes Before

* Operator Algebra:

If $\hat{X}$ & $\hat{Y}$ are any 2 operator then $\hat{X} + \hat{Y} = \hat{Y} + \hat{X}$ is also an operator

$$(\hat{X} + \hat{Y}) |a\rangle = \hat{X} |a\rangle + \hat{Y} |a\rangle$$

2 operators $\hat{A}$ & $\hat{B}$ are said to be equal $(\hat{A} = \hat{B})$ iff $\hat{A} |a\rangle = \hat{B} |a\rangle \quad \forall \ |a\rangle \in S$.

If $\hat{X} |a\rangle = 0_V \quad \forall \ |a\rangle \in S$
then $\hat{X}$ is ~~called~~ called the NULL operator

$$\hat{X} (\alpha |a\rangle + \beta |b\rangle) = \alpha \hat{X} |a\rangle + \beta \hat{X} |b\rangle$$

{Linearity of Operations}

Commute ($\hat{X}\hat{Y} = \hat{Y}\hat{X}$)

$\hat{X}(\hat{Y}\hat{Z}) = (\hat{X}\hat{Y})\hat{Z}$ (associative law)

Inner Product: Additional str. on the vector space.

$S \times S \to \mathbb{C}$

Notation: If $|\alpha\rangle$ & $|\beta\rangle$ are 2 vectors then the inner product of $|\alpha\rangle$ & $|\beta\rangle$ is denoted $\langle\alpha|\beta\rangle$

inner product of $|\beta\rangle$ & $|\alpha\rangle$ is $\langle\beta|\alpha\rangle$.

① Inner Product has to be linear in the 2nd argument. That is, if $|\beta\rangle = a|\gamma\rangle + b|\delta\rangle$ then inner product $|\alpha\rangle, |\beta\rangle$ is

$$\langle\alpha|\beta\rangle = \langle\alpha|\left(a|\gamma\rangle + b|\delta\rangle\right)$$
$$= a\langle\alpha|\gamma\rangle + b\langle\alpha|\delta\rangle$$

② $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$ { $-$ & $*$ $\Rightarrow$ Complex Conjugate }

$\Updownarrow$

$\overline{\langle\beta|\alpha\rangle}$

③ $\langle\alpha|\alpha\rangle \geq 0$ with equality sign holding iff $|\alpha\rangle = 0_v$

Orthogonal Vectors ~~$|a\rangle$~~ $|a\rangle$ & $|b\rangle$ are orthogonal if

$$\langle a|b\rangle = \langle b|a\rangle = 0$$

For any vector $|\alpha\rangle$, $\sqrt{\langle\alpha|\alpha\rangle}$ is called the norm (or the length) of $|\alpha\rangle$ (notation $\||\alpha\rangle\|$)

$\Rightarrow$ given any $|\alpha\rangle$ we can construct a unit vector

$$|\tilde{\alpha}\rangle = \frac{|\alpha\rangle}{\||\alpha\rangle\|} = \frac{|\alpha\rangle}{\sqrt{|\langle\alpha|\alpha\rangle|}}$$

$\downarrow$

Normalized Vector

Dual Vector (or bra vector)

Given any $|\alpha\rangle$ in S we can defined a vector dual to $|\alpha\rangle$ denoted by $\langle\alpha|$ Dual Vectors can "act" on ket vectors to give scalars. In particular if $|\beta\rangle$ is a ket vector & $\langle\alpha|$ is dual to $|\alpha\rangle$ then

$$\langle\alpha|(|\beta\rangle) = \langle\alpha|\beta\rangle$$

$$\langle\alpha|.|\beta\rangle = \langle\alpha|\beta\rangle$$

bracket

Ex: Check that the space of dual vectors is also a vector space?

ANS. Use Postulates of Vector Space.

$\rightarrow \quad |\alpha\rangle \xleftrightarrow{\text{dual}} \langle\alpha|$

$\rightarrow \quad |\alpha\rangle + |\beta\rangle \xleftrightarrow{\text{dual}} \langle\alpha| + \langle\beta|$

To Prove:

$$\underbrace{a|\alpha\rangle + b|\beta\rangle}_{|\gamma\rangle} \xleftrightarrow{\text{dual}} a^*\langle\alpha| + b^*\langle\beta|$$

$$|\gamma\rangle \longleftrightarrow \langle\gamma|$$

L.H.S. $\Rightarrow \langle\gamma|\delta\rangle = \overline{\langle\delta|\gamma\rangle} = \overline{\langle\delta|(a|\alpha\rangle + b|\beta\rangle)}$

$\Rightarrow \overline{a\langle\delta|\alpha\rangle + b\langle\delta|\beta\rangle}$

$\Rightarrow \langle\gamma|\delta\rangle \Leftrightarrow a^*\langle\alpha|\delta\rangle + b^*\langle\beta|\delta\rangle$

$\Rightarrow \boxed{\langle\gamma| \Leftrightarrow a^*\langle\alpha| + b^*\langle\beta|}$

Proved.

(2) $(3+i)|1\rangle + 4i|2\rangle = |v\rangle$

Find Dual:

~~x tas~~ $a|\alpha\rangle + b|\beta\rangle \Leftrightarrow a^*\langle\alpha| + b^*\langle\beta|$

$\Rightarrow (3-i)\langle 1| - 4i\langle 2|$

Length of $|v\rangle$ if $|1\rangle$ & $|2\rangle$ are unit vectors

$\langle 1|1\rangle = \langle 2|2\rangle = 1$

& $\langle 1|2\rangle = \langle 2|1\rangle = 0$

Square of Length is $\langle v|v\rangle = \big((3-i)\langle 1| - 4i\langle 2|\big)\big((3+i)|1\rangle + 4i|2\rangle\big)$

$= (3^2 - i^2)\cancel{\langle 1|1\rangle} + (3-i)(4i)\langle 1|2\rangle$
$+ (-4i)(3+i)\langle 2|1\rangle + (-4i)(+4i)\langle 2|2\rangle$

$= 10 + 16$

$= 26$

Length $= \sqrt{26}$

Scanned by CamScanner

PAGE NO. :
DATE : / /

To Prove :

$\underbrace{\hat{A}\,|\gamma\rangle}_{|\delta\rangle} \xrightarrow{\text{dual}} \langle\gamma|\hat{A}^{\dagger}$

$\langle\delta|$ ↳ $\hat{A}$ dagger (adjoint of operator $\hat{A}$)

Let $\hat{A}\,|\gamma\rangle = |\delta\rangle$ — (1)

If $|\alpha\rangle$ is any other vector then

$\langle\alpha|\delta\rangle = \langle\alpha|\hat{A}|\gamma\rangle$ — (2)

But $\langle\alpha|\delta\rangle = \overline{\langle\delta|\alpha\rangle} = \overline{\langle\gamma|\hat{A}^{\dagger}|\alpha\rangle}$ — (3)

(2) = (3)

$\Rightarrow \overline{\langle\gamma|\hat{A}^{\dagger}|\alpha\rangle} = \langle\alpha|\hat{A}|\gamma\rangle$

or $\langle\gamma|\hat{A}^{\dagger}|\alpha\rangle = \overline{\langle\alpha|\hat{A}|\gamma\rangle}$

$\Rightarrow \langle\gamma|\hat{A}^{\dagger}| = |\hat{A}|\gamma\rangle$

If $\hat{A}^{\dagger} = \hat{A}$ ie.

$\langle\gamma|\hat{A}^{\dagger}|\alpha\rangle = \langle\gamma|\hat{A}|\alpha\rangle = \overline{\langle\alpha|\hat{A}|\gamma\rangle}$

then $\hat{A}$ is called Hermitian Op. or Self-Adjoint Op.

Ex: Show that $(\hat{X}\hat{Y})^{\dagger} = \hat{Y}^{\dagger}\hat{X}^{\dagger}$

Nakahara

PAGE NO. :
DATE : / /

☆ Outer Product:

$$|\alpha\rangle\langle\beta| \longrightarrow \text{An Operator}$$

$|\alpha\rangle\langle\beta|\gamma\rangle$

$\langle\delta|\alpha\rangle\langle\beta|$

→ Acting from left on ket vector it gives a ket vector, acting from right on dual vector it gives a dual vector

Eg: Show that

$$\underbrace{|\alpha\rangle\langle\beta|}_{\hat{X}} \xleftrightarrow{\text{dual}} \underbrace{|\beta\rangle\langle\alpha|}_{\hat{X}^\dagger}$$

$$\hat{A}|a\rangle = a|a\rangle$$

For Hermitian Op. i.e. for op. $\hat{H}$ satisfying $\hat{H}^\dagger = \hat{H}$, the eigenvalues are all real

$$\hat{H}|h_i\rangle = h_i|h_i\rangle \quad h_i \in \mathbb{R}$$

& if $|h_i\rangle$ & $|h_j\rangle$ are eigenvectors belonging to diff. eigen values

$h_i \neq h_j$ then $|h_i\rangle$ & $|h_j\rangle$ are orthogonal, $\langle h_i|h_j\rangle = \langle h_j|h_i\rangle = 0$.

16/9/18

~~✱~~ Single Qubit Systems:

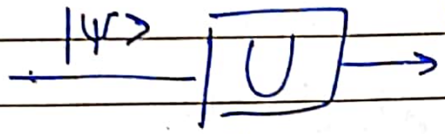
→ qubits → 2 static quantum system

$|0\rangle, |1\rangle$ → Computational Basis

→ Unitary Operation → quantum gate

X, Z, H^{**}, Y

→ Quantum Circuit:

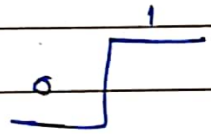


$|\chi\rangle = U|\psi\rangle$

U
Gate

→ Single Qubit Measurement

Classical



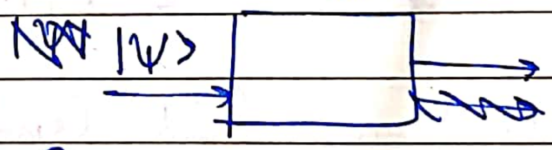
Quantum:

$|\psi\rangle = a|0\rangle + b|1\rangle$

$a, b \in \mathbb{C}$

$|a|^2 + |b|^2 = 1$ Born

Measurement



$P(|0\rangle) = |a|^2$

$P(|1\rangle) = |b|^2$

Projective Measurement or Von Neumann measurement:

— × —— Recap Done —— × ——

☆ Global Phase & Relative Phase:

$$|\psi'\rangle = e^{i\theta}\left(a|0\rangle + b|1\rangle\right)$$
$$= e^{i\theta}|\psi\rangle$$

$$a e^{i\theta} \xrightarrow{\text{Mod Sq.}} |a e^{i\theta}|^2 = (a e^{i\theta})(a e^{-i\theta})$$
$$= |a|^2$$

Similarly,

$$b e^{i\theta} \xrightarrow{\text{Mod Sq.}} |b|^2$$

$$|\psi'\rangle \xrightarrow{P(|0\rangle)} |a|^2$$
$$\xrightarrow{P(|1\rangle)} |b|^2 \rightarrow e^{i\theta} \cdot e^{-i\theta} = 1$$

$$|\langle\psi|\psi'\rangle|^2 = |e^{i\theta}|^2 = 1$$

* * States differing by a global phase are physically indistinguishable

☆ Relative Phase:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$|\chi\rangle = a|0\rangle + e^{i\phi} b|1\rangle$$

Q) IS $|\chi\rangle$ normalised (given that $|\psi\rangle$ is normalized)

ANS) Yes $\left(|a|^2 + |e^{i\phi} b|^2\right)$

Q) What about the measurement statistics?

$$P_{|\chi\rangle}(|0\rangle) = |a|^2$$

$$P_{|\chi\rangle}(|1\rangle) = |b|^2$$

$$\langle \psi | \chi \rangle = \left(a^* \langle 0| + b^* \langle 1| \right)\left(a|0\rangle + e^{i\phi} b|1\rangle \right)$$

$$= |a|^2 + e^{i\phi} |b|^2$$

(Many Possibilities)

& depending on the relative mag. of a & b and the value of ϕ there are various possibilities

$$0 \leq |\langle \psi | \chi \rangle| \leq 1$$

Eg: $|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$\langle + | - \rangle = 0$$

We see that states $|\psi\rangle$ & $|\chi\rangle$ which differ by a relative phase are physically distinguishable

$a = \alpha + i\beta$ $\quad \{\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1\}$

$b = \gamma + i\delta$

Ex: Are the state $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ & $\left(\dfrac{-|0\rangle + i|1\rangle}{\sqrt{2}}\right)$ equivalent?

Exe: For what value of θ are the states $|1\rangle$ & $\dfrac{|+\rangle + e^{i\theta}|-\rangle}{\sqrt{2}}$ equivalent?

Ex: Consider the state

$\dfrac{\sqrt{3}}{2}|0\rangle - \dfrac{1}{2}|1\rangle$ & measurement basis $\{|0\rangle, |1\rangle\}$

What are the possible measurement outcomes & what are their prob?

DATE: / /

Ex: Repeat the prev. problem for the state $|+\rangle$ & the measurement basis

$$\left\{ \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \, , \, \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \right\}$$

* Infinitely Vectors correspond to one physical state. (Global Phase)
→ Therefore to identify one - to - one Relation.
Use of CP_1 Space. (Non-Linear Vector Space)

PAGE NO.:
DATE: / /

☆ Geometrical Representation of the state space of a qubit:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

↳ Represented by a vector in a 2-dim complex vector Space

$$|\langle\psi|\psi\rangle|^2 = 1 \qquad \{|a|^2+|b|^2=1\}$$

Infinitely many states with same Geometrical Representation.

∴ To Identify all vectors which differ by a global phase.

$$|\psi\rangle, \quad |\psi'\rangle = e^{i\theta}|\psi\rangle$$
$$|\psi\rangle \sim |\psi'\rangle$$

∴ To get one-to-one relation b/w Geometrical Rep. & physical state use of Complex Projective Space of dim 1.

① Extended Complex plane:

$$(\mathbb{C} + \text{Point at infinity})$$
$$\mathbb{C} \cup \{\infty\}$$

Complex Number

$$\left\{\frac{b}{a} = \alpha\right\}$$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$|\psi'\rangle = e^{i\theta}a|0\rangle + e^{i\theta}b|1\rangle$$

$$\left\{|a|^2 + |b^2| = 1\right\}$$

Now take a to be real & +ve so that

$$\Leftrightarrow |a|^2 = \frac{1}{1+|\alpha|^2}$$

$$a = \frac{1}{\sqrt{1+|\alpha|^2}} \qquad b = \frac{\alpha}{\sqrt{1+|\alpha|^2}}$$

$$\Leftrightarrow |b|^2 = \frac{|\alpha|^2}{1+|\alpha|^2}$$

~~$a \to 0$ because if $a = 0$~~
~~$\Leftrightarrow \alpha = \infty \Leftrightarrow b = \frac{\infty}{\infty}$ {Undefined}~~

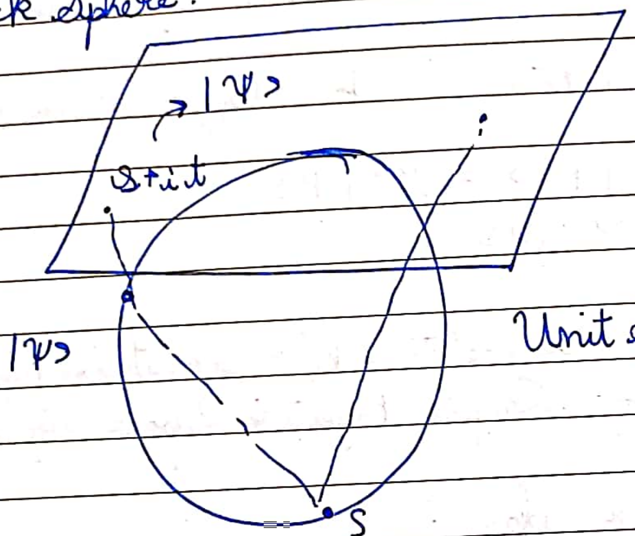
If $|\psi\rangle = |1\rangle$

i.e. $a = 0$, $b = 1$

~~One~~ --- One includes the pt. at infinity in the complex plane to have

$\mathbb{C} \cup \{\infty\}$ & $|1\rangle \to \infty$

☆ Block Sphere:



Any Pt in Extended CP, can be mapped to a Pt on a unit sphere with $\alpha^2+\beta^2+\gamma^2=1$

Unit Sphere

Stereographical Projection

$$|\psi\rangle = |a| e^{i\theta} |0\rangle + |b| e^{i\theta'} |1\rangle$$

$$= e^{i\theta} \left[|a| |0\rangle + |b| e^{i\theta} |1\rangle \right]$$

$$\theta' - \theta = \phi$$

$$|\psi\rangle = |a| |0\rangle + |b| e^{i\phi} |1\rangle$$

$$|a|^2 + |b|^2 = 1$$

Let $|a| = \cos\theta/2$

$|b| = \sin\theta/2$

(Diametrically Opposite Pts)

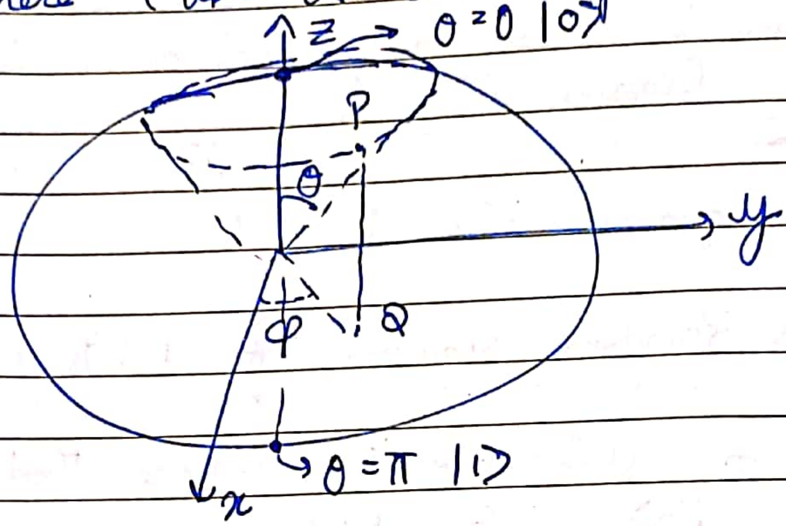
PAGE NO. :

DATE : / / - $|0\rangle$ & $|0\rangle$

$\theta/2$ is used to Maintain Uniqueness

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

where θ & ϕ are the usual polar ∠s on the unit sphere (the ~~...~~ bloch sphere)



$\theta = 0 \qquad \phi =$ ~~...~~ Undefined

$|\psi\rangle = |0\rangle$

$\theta = \pi \qquad \phi = 0$

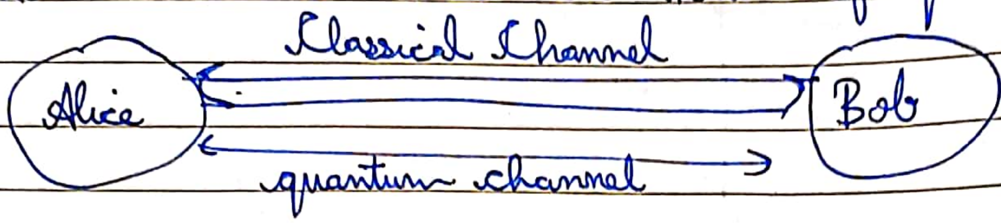
Ex : $|+\rangle, |-\rangle$ on Bloch Sphere ?

☆ Quantum Key Distribution : {Encryption}

-> Using Symmetric Key encryption concept.

-> Classical is based on high computational complexity.

-> ~~Q~~ Quantum is based on nature of qubits.



Alice generates Random sequence of N bits

1 0 0 1 1 0 0 ① Generate bits ② Encode Method

1 → $|0\rangle$ or $|+\rangle$

0 → $|0\rangle$ or ~~N~~ $|-\rangle$

Suppose : 1 0 1 0 | 0 0 1 1 | 1 0 1 0 | 0 0 1 1

$|0\rangle$ $|1\rangle$ $|+\rangle$ $|-\rangle$ | $|-\rangle$ $|+\rangle$ $|0\rangle$ $|0\rangle$ – – – – – –

Transmit qubits to Bob over quantum channel.

Bob makes measurements on those choosing randomly ~~bett~~ bet^n the Hadamard basis (H) & Computational basis

~~CHHCH~~ H C C H H | H H C C |

-> Over classical channel A & B ensure that B has read all the qubits & they also check the basis that was used by them, rejecting those that do not match.

M N N M |

Match Not Match – – – |

PAGE NO. :
DATE : / /

If N large $\Rightarrow$ on avg 50% of qubits will be retained

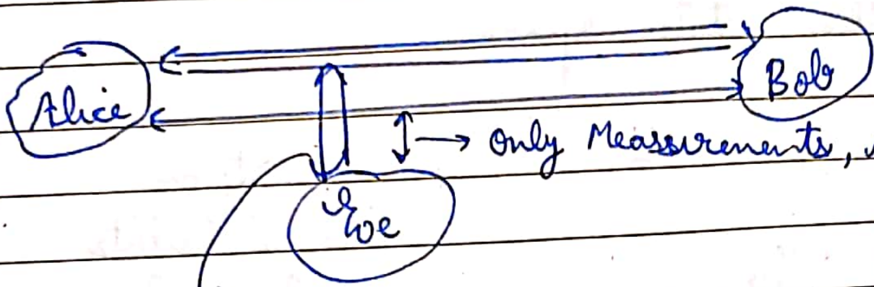
$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \Rightarrow |0\rangle = |+\rangle + |-\rangle / \sqrt{2}$

$|-\rangle = |0\rangle - |1\rangle / \sqrt{2} \Rightarrow |1\rangle = |+\rangle - |-\rangle / \sqrt{2}$

Matched Seq. $\Rightarrow$ $|0\rangle$ $|-\rangle$ $|1\rangle$ $|+\rangle$ $|-\rangle$ $|-\rangle$ $|0\rangle$

$\Rightarrow$ 1 0 0 1 0 0 1

Now Eve is the hacker



$\updownarrow \rightarrow$ Only Measurements, no cloning Theorem :

Only classical won't help in decoding

	Eve chooses Hadamard	Bob Comp.
Alice $|0\rangle$ $\longrightarrow$	$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\longrightarrow$	$|0\rangle - 1$, $|1\rangle$ 0

Gate:

① X, Y, Z, H : $X^2 = Y^2 = Z^2 = H^2 = I$

$XX^\dagger = I$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$ Phase Shift Gate

② $P|\psi\rangle = P(a|0\rangle + b|1\rangle)$
$= aP|0\rangle + bP|1\rangle = a|0\rangle + e^{i\theta}|1\rangle$

③ $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$

④ $(UVW \ldots)^\dagger = \ldots W^\dagger V^\dagger U^\dagger$

DATE: / /

Multiple Qubits :

Additional Features in multiple qubits :

① State Space (Infinite)

② Entanglement

→ Size of the state space

Classical	Vs	Quantum
↓		For 2 Qubits :
in 3-d for n Particles size of the state space is 3n		$|0\rangle \quad |0\rangle$ $|0\rangle \quad |1\rangle$ $|1\rangle \quad |0\rangle$ $|1\rangle \quad |1\rangle$

n Bits ⇒ we need to give n bit values

U, V, W

$U \oplus V \oplus W \oplus \ldots$

direct sum

$\dim (U \oplus V \oplus W \ldots)$

$\Rightarrow \dim U + \dim V + \dim W$

$\Rightarrow 3 + 3 + 3 + \ldots$

Generalised :

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ (For 2 Qubits)

Basis is 4. $= 2^2$

∴ For n qubits.

State Space is 2^n.

Exponential Increase. Therefore very complex.

* Multiple qubit system:

* Tensor Product Spaces:

If V & W are 2 linear spaces (real or complex) of dim m & n resp with the corresponding basis

$$A = \{ |\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_m\rangle \} \ \&$$

$$B = \{ |\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_n\rangle \}$$

Then their tensor product, denoted $V \otimes W$, is a mn-dimensional vector space with a basis consisting of m·n elements

$$C = \{ |\alpha_1\rangle \otimes |\beta_1\rangle, |\alpha_1\rangle \otimes |\beta_2\rangle, \ldots, |\alpha_1\rangle \otimes |\beta_n\rangle,$$
$$|\alpha_2\rangle \otimes |\beta_1\rangle, |\alpha_2\rangle \otimes |\beta_2\rangle, \ldots, |\alpha_2\rangle \otimes |\beta_n\rangle,$$
$$\vdots$$
$$|\alpha_m\rangle \otimes |\beta_1\rangle, |\alpha_m\rangle \otimes |\beta_2\rangle, \ldots, |\alpha_m\rangle \otimes |\beta_n\rangle, \}$$

(here $\otimes$ denotes the tensor product)

Properties of $V \otimes W$: {Tensor Product Space}

If $|v_i\rangle \in V$, $|w_j\rangle \in W$ then

① $(|v_1\rangle + |v_2\rangle) \otimes |w_j\rangle = |v_1\rangle \otimes |w_j\rangle + |v_2\rangle \otimes |w_j\rangle$

② $|v_i\rangle \otimes (|w_1\rangle + |w_2\rangle)$
$= |v_i\rangle \otimes |w_1\rangle + |v_i\rangle \otimes |w_2\rangle$

$\frac{1}{\sqrt{2}}$ $\frac{i}{\sqrt{2}}$ $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$

PAGE NO.:
DATE: / /

③ $(a\,|v_i\rangle) \otimes |w_j\rangle = |v_i\rangle \otimes (a\,|w_j\rangle)$
$= a\,(|v_i\rangle \otimes |w_j\rangle)$

$a \in \mathbb{C}$

Eg: Let $|v\rangle = a_1|\alpha_1\rangle + a_2|\alpha_2\rangle$

$|w\rangle = b_1|\beta_1\rangle + b_2|\beta_2\rangle$

$$|v\rangle \otimes |w\rangle = (a|\alpha_1\rangle + a_2|\alpha_2\rangle) \otimes (b_1|\beta_1\rangle + b_2|\beta_2\rangle)$$
$$= a_1b_1|\alpha_1\rangle \otimes |\beta_1\rangle + a_1b_2|\alpha_1\rangle \otimes |\beta_2\rangle$$
$$+ a_2b_1|\alpha_2\rangle \otimes |\beta_1\rangle + a_2b_2|\alpha_2\rangle \otimes |\beta_2\rangle$$

Eg: Suppose $|\alpha_1\rangle, |\beta_1\rangle = |0\rangle$ {Basis must be known}
$|\alpha_2\rangle, |\beta_2\rangle = |1\rangle$

$a_1 = \frac{1}{\sqrt{2}}$ $a_2 = \frac{i}{\sqrt{2}}$ $b_1 = \frac{-1}{\sqrt{10}}$ $b_2 = \frac{3}{\sqrt{10}}$

$$|v\rangle \equiv \begin{array}{c} \begin{pmatrix} 1/\sqrt{2} \\ i/\sqrt{2} \end{pmatrix} \end{array} \begin{array}{c} 0 \\ 1 \end{array} \qquad |w\rangle \equiv \begin{pmatrix} -1/\sqrt{10} \\ 3/\sqrt{10} \end{pmatrix} \begin{array}{c} 0 \\ 1 \end{array}$$

$$|v\rangle \otimes |w\rangle \equiv \begin{pmatrix} -1/\sqrt{20} \\ 3/\sqrt{20} \\ -i/\sqrt{20} \\ 3i/\sqrt{20} \end{pmatrix} \begin{array}{c} |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |0\rangle \\ |1\rangle \otimes |1\rangle \end{array}$$

DATE: / /

→ If V & W are both inner product spaces then $V \otimes W$ can also be made into an inner product space.

Let $|\psi_1\rangle = |v_1\rangle \otimes |w_1\rangle$

$|\psi_2\rangle = |v_2\rangle \otimes |w_2\rangle$

Then $\langle \psi_2 | \psi_1 \rangle$

$= (\langle v_2| \otimes \langle w_2|)(|v_1\rangle \otimes |w_1\rangle)$

$= \langle v_2|v_1\rangle \langle w_2|w_1\rangle$

⇒ tensor prod. of 2 unit vectors is a unit vector & given an orthonormal basis $\{|\alpha_i\rangle\}$ of V & an orthonormal basis $\{|\beta_i\rangle\}$ of W, the basis

$\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ of $V \otimes W$ is orthonormal.

Exe: Confirm this:

* State-Space of n-Qbit System:

Let V be the vector space of a single Qubit ($\mathbb{C}^2$ in vector space representation)

If the system consists of n-Qbits then the resulting state space is

$V \otimes V \otimes \cdots \otimes V \equiv V^{\otimes n} = (\mathbb{C}^2)^{\otimes n}$

& ~~...~~ will have the dim $= \underbrace{2 \times 2 \times 2 \times \ldots \times 2}_{n\text{-Factors}}$

$= 2^n$.

Computational basis for this space –

$|0\rangle \otimes |0\rangle$ ——— $|0\rangle$ {n-Factors} $= |00\ldots0\rangle \equiv |0\rangle$

$|0\rangle \otimes |0\rangle \otimes$ ——— $|1\rangle \equiv |000\ldots1\rangle \equiv |1\rangle$ ↳ Decimal Rep.

Notation : $|i\rangle \otimes |j\rangle \otimes |k\rangle$

$|i\rangle |j\rangle |k\rangle$

$|ijk\rangle$

2 Qbits $|0\rangle \otimes |0\rangle \equiv |0\rangle |0\rangle \equiv |00\rangle = |0\rangle_2$

$|0\rangle \otimes |1\rangle \equiv |0\rangle |1\rangle \equiv |01\rangle = |1\rangle_2$

$|1\rangle \otimes |0\rangle \equiv |1\rangle |0\rangle \equiv |10\rangle = |2\rangle_2$

$|1\rangle \otimes |1\rangle \equiv |1\rangle |1\rangle \equiv |11\rangle = |3\rangle_3$

Consider a 2 Qubit System.

A general state of a 2-Qubit System

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad (1)$$

Now consider the case where the normalized state of the 1st qubit is

$|\hat{\phi}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ & the normalized state of the 2^{nd} qubits is

$$|\chi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$$

$\Rightarrow$ the combined state of the 2 Qbit system is

$$|\phi\rangle \otimes |\chi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \quad (2)$$

Notice that the product of coeff. of $|00\rangle$ & $|11\rangle$ is the same as the product of the coeff. of $|01\rangle$ & $|10\rangle$

$$\alpha_0\beta_0\alpha_1\beta_1 = \alpha_0\beta_1\alpha_1\beta_0 \quad - (2\text{-}a)$$

Contrast (2) with (1)

In (1) there is no restriction on the coeff α_{ij} except for (1-a). In particular

$$(1) \not\Rightarrow \alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$$

$\Rightarrow$ a general state in $V \otimes V$ cannot be written as the tensor product of the state of the 1^{st} Qbit with the state of the 2^{nd} Qbit.

→ States of the kind in (2) are called <u>Product States</u>. & we have find that most states

$\Rightarrow$ in $V \otimes V$ are <u>not product states</u>. These states are called ~~ental~~ <u>entanglement states</u>.

DATE: / /

Ex: Expand the tensor product:

$$\left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle \otimes \frac{i}{\sqrt{2}}|1\rangle \right)$$

& write the result using diff. notation.

Ex 2: Is the state

$$|\psi\rangle = \frac{1}{2}\left(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle \right)$$

a product state?

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle) \right]$$

$$= \frac{1}{2}\left(|0\rangle + |1\rangle \right) \otimes \left(|0\rangle - |1\rangle \right)$$

= $|\psi\rangle$ is a product state

No. of Coeff Required $= 2n = n$ (High)

But if consider a state

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle \right)$$

If we know 1 qbit to be zero the other will definitely be zero.

No of Coeff. Required $= 2^n$.

$$\alpha_0 |0\rangle_3 + \alpha_1 |1\rangle_3 + \alpha_2 |2\rangle_3 + \ldots + \alpha_7 |7\rangle_3$$

DATE: / /

Eg: Is the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle - i|01\rangle + |10\rangle + i|11\rangle\right]$$

a product state or an entangled state?

Basis for $V \otimes V$ $\quad |00\rangle, |01\rangle, |10\rangle, |11\rangle$

* Bell States: (~~Initial~~ Entangled)

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right]$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right]$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle - |10\rangle\right]$$