16/9/19

→ Choose a measurement gate. $\psi \rightarrow$ [↑] $\rightarrow$ which has its own base states.

$\psi = a|0\rangle + b|1\rangle \quad a, b \in \mathbb{C}$

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

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

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

Born Rule

$|\psi\rangle \rightarrow$ [↑] $\rightarrow P(|0\rangle) = |a|^2$, $P(|1\rangle) = |b|^2$

Once a qubit measured in a definite state → its state is no longer probab. its state becomes what is obtained in measurement

Projective Measurement or Von Neumann measurement.

★Global Phase & Relative Phase:

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

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

$= e^{i\theta}|\psi\rangle$

all the rules studied for $|\psi\rangle$ also hold for $|\psi'\rangle$.

- $ae^{i\theta} \xrightarrow[\text{sq}]{\text{mod}} |ae^{i\theta}|^2 = (ae^{i\theta})(a^* e^{-i\theta}) = |a|^2$

also $be^{i\theta} \rightarrow |b|^2$

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

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

if $|\psi\rangle$ normalized $|\psi'\rangle$ also normalized

if $P(|0\rangle) = |a|^2$ for $|\psi\rangle$ then $P(|0\rangle) = |a|^2$ for $|\psi'\rangle$

for all practical purposes ψ & ψ' indistinguishable

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

$|\langle\psi|\psi'\rangle| = 1$

$e^{i\theta}$ → Global phase: overall multiplying factor

→ States differing by a global phase are physically indistinguishable in math ψ & ψ' are 2 diff states. since phase is different. but in QC → physical sig of ψ & ψ' but can't be measured ∴ identical.

Global Phase: physically not imp.

Relative Phase:

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

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

→ Is $|\chi\rangle$ normalized? given $|a|^2 + |b|^2 = 1$

Yes. Phase factor in b component. $(|e^{i\varphi}|^2 = 1)$

→ what abt the measurement statistics?

$P_{|\chi\rangle}(|0\rangle) = |a|^2$, $P_{|\chi\rangle}(|1\rangle) = |b|^2$

also both $|\chi\rangle$ & $|\psi\rangle$ normalized does it imply both states are indistinguishable?

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

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

Since $|0\rangle$ & $|1\rangle$ are orthogonal to e.o. depending on diff vals of a & b, we'll get diff answers.

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

dep. on relative magnitude of a & b & the val of φ, various possibilities

$\varphi = 0\pi$ when $a = b = \frac{1}{\sqrt{2}}$

$\varphi = 0$

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

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

$\langle + | - \rangle = 0$

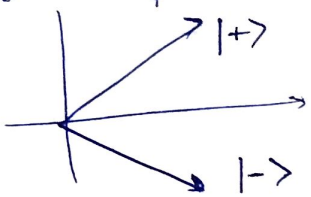
$\langle \psi | \chi \rangle$ maximally distinguishable.

when $\langle \psi | \chi \rangle = 0$

& not distinguishable if

$\langle \psi | \chi \rangle = 1$

given $P_\psi = P_\chi$ for both states.



Topological circle:

every pt x & $x+2\pi$ identical

states which differ by a relative phase are distinguishable physically.

Q Are the states $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ & $\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$ equivalent?

Q For what values of θ are the the states $|1\rangle$ & $\frac{|+\rangle + e^{i\theta}|-\rangle}{\sqrt{2}}$ equivalent?

Q Consider the state $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$ and measurement basis $\{|0\rangle, |1\rangle\}$. What are the possible measurement outcomes & what are their probab?

Q Repeat prev prob for the state $|+\rangle$ & measurement basis?

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

★ Geometric Representation of the States Space of a qubit:

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

↳ represented by a vector in a 2D Complex vector space.

Why we work w normalized vecs? to reduce redundancy.

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

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

but states diff. by a global phase are also identical (measurably)

→ No one-to-one relation bw state & vectors

given phy state does not uniquely give us a unique vector.

Due to ψ & ψ' (global phase) being measurably same we have no redundancy.

We need to identify $|\psi\rangle$ $|\psi'\rangle$ for all such phases (global)

* Complex Projective Space of dim-1

$\boxed{\mathbb{CP}^1}$

not a linear space → we don't know how to add vectors.
non-linear space

∴ difficult to work w $\mathbb{CP}^1$

(*) Extended Complex Plane :

$\boxed{\mathbb{C} \cup \{\infty\}}$ ($\mathbb{C}$ + point at ∞)

identify ψ & ψ' where

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

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

Complex plane : 1D $\mathbb{C}^1$ (not $\mathbb{C}^2$)

⇒ deal w only 1 complex no.

∴ we take $\frac{b}{a} = \alpha$

we keep the relative phase
(phase of $|1\rangle$ / phase of $|0\rangle$)
but getting rid of global phase.

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

Take a to be real & +ve.:

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

Constructing inverse map.
given α, find a & b.

if $a = 0$
$\alpha = \infty$
$b = \frac{\infty}{\infty} = 1$

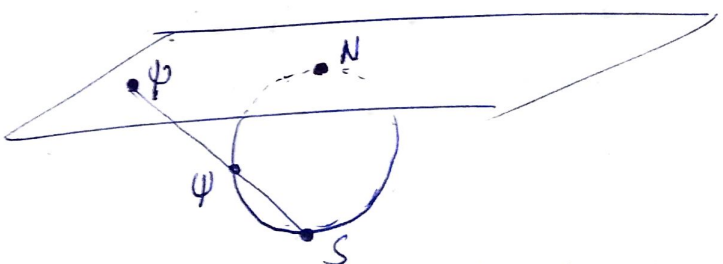
why? because $\{\infty\}$ included in ~~domain~~ range

state $|1\rangle$ maps to ∞.

Pf $|\psi\rangle = |1\rangle$
ie $a=0$, $b=1$
includes pt at ∞

Block Sphere

Stereographic Projec^n.
unit sphere
∞'ly big $\mathbb{C}^1$ plane



plane tangential to unit block sphere at North Pole.

any pt on $\mathbb{C}$ (ψ) joined to South Pole cuts sphere at 1 pt.
that is also ψ.

Polar form of $|\psi\rangle$

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

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

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

$e^{i\theta}$ → global phase can be discarded

$$\Downarrow$$

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

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

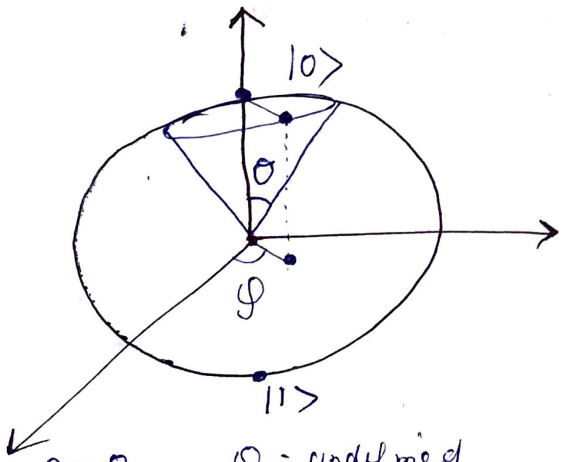
∴ we can take a to be real & +ve.

$|a| = \cos\theta/2 \qquad |b| = \sin\theta/2$

$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + \sin\frac{\theta}{2} e^{i\varphi} |1\rangle$$

where θ & φ are the usual polar

Is on the unit sphere (block sphere)



$\theta = 0$, φ : undefined

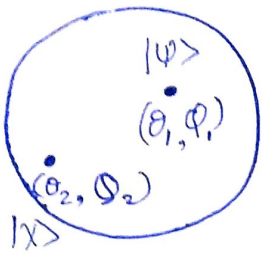
$|\psi\rangle = |0\rangle$

$\theta = \pi \qquad \varphi = 0$

$|\chi\rangle = |1\rangle$

ex $|+\rangle$ & $|-\rangle$, identify on block sphere.

$U|\psi\rangle = |x\rangle$



→ Some rotation in 3D.
→ mimicking 3×3 real matrix.
→ every transforma^n is a 3D rotat.

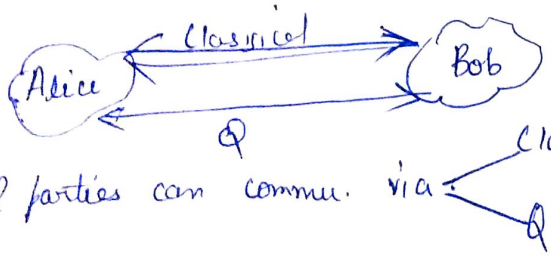
$|\psi\rangle \xrightarrow{U} U|\psi\rangle = |x\rangle$
- changed state
- a different set of θ & φ.

Quantum Key Distribu^n: Applica^n of extended plane.

→ Cryptography
Tx of msg in encrypted form
lock the msg. → need a key.
unlocking also reqs a key.

Forms of key:
Public – Private Key:
Symmetric key:
Public key:
Symmetric key:
2 parties universally called Alice & Bob.
A & B both reqd to maintain secrecy of key. → They generate their own key.
How to ensure secrecy of key?

Q encrypt^n works not on math formula^n but, on properties & Δ's of qubits.



2 parties can commu. via: Classical channel, Q

- Alice generates a random seq of N bits.
Eg 10100011 10100011
(bit seq)
- A encodes this seq using qubits.
encode bit 1
bit 0
makes use of 2 qubits on 2 basis
computa^{n}l & Hadamard basis

$(|0\rangle, |1\rangle)$
$(|+\rangle, |-\rangle)$

used to encode bit '1' . used to encode bit '0'.

'1' → $|0\rangle$ or $|+\rangle$
which out of these 2: RANDOM.
'0' → $|1\rangle$ or $|-\rangle$

bit	1	0	1	0	0	0	1	1	1	0	1	0	0	0	1	1
qbits	0	1	+	−	1	1	+	0	0	−	+	1	−	−	+	0

Now (1) transmitted to Bob via the Q channel.
(Bit string converted to qbits)

- Bob recieves qubit seq.
Has to make measurement
Randomly choose b/w computa^{n}l & hadamard basis
-to make measurement (C) (H)
Choose random seq of basis:
say: CHCH | HCCH | HCHH | HHCC

(if Bob choose same measu. basis that A used to encode: Bob will definitely know which qubit).

(None of A & B know ~~the~~ 0's choice of basis)

In the meanwhile :

Over the classical channel :

→ A & B ensure that B got all bits

→ share which basis used for w. bit

→ for those bits whose basis of encoding & measurmt did not match, simply discarded those ~~basis~~ bits.

Sharing only basis info, not which exact bits sent.

On an avg 50% bits dropped.

No of bits → Yes / NO

Say eve tries to intercept.

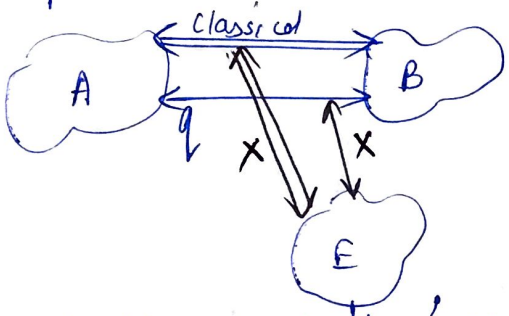
Classical channel :

- A & B share no of bits.
  → doesn't help
- A & B share

To get access to key has to tap Q channel :

* 3rd party Eavesdropper

— Eve should not be able to tap on classical or Q channel.



Eve should not get 'key'. What is key?

'key' not generated yet.

in the process of generating "key".

(*) M NN M | N M N N | NN M N | M M N M

M: matched, N: unmatched

retain only those bits that correspond to 'M'

$|0\rangle$ $|-\rangle$ $|1\rangle$ H H H $|0\rangle$

Now we know which qubit is representing which bit. so we get

1	0	0	1	0	0	1

Our key.

★ Gates:

- X, Y, Z, H.
- $X^2 = Y^2 = Z^2 = H^2 = \mathbb{1}$
- $XX^\dagger = \mathbb{1} = YY^\dagger = \dots$

★ Phase Shift- gate:

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

$$P|\psi\rangle = P(a|0\rangle + b|1\rangle)$$

w.k.t: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ & $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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

$$\therefore P|\psi\rangle = a|0\rangle + e^{i\theta} b|1\rangle \rightarrow \text{relative Phase}$$

- $(U\ V\ W \dots)^\dagger = \dots W^\dagger V^\dagger U^\dagger$

can't do significant computation task. need multiple qubits.

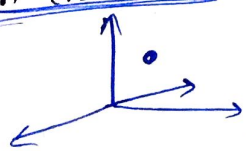
★ Multiple Qubits:

A qubit: 2D complex vec space or a pt on Block sphere.

Entanglement?

Need to know: How size of state space changes when 'N' particles in classical v/s Q.

In classical:



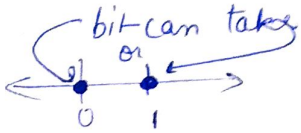
To represent a particle in 3D: need 3 number to specify position

Lets say state < posi'n ✓ / momentum ✗

To represent 'N' particles need 3N numbers → Linear increase in state space.

In classical:

To represent 2 bits: need 2 regs.



size of state space grows linearly w no. of bits / particles.

★ Say: N particles

$U, V, W \dots$

$U \oplus V \oplus W \oplus \dots$ direct sum

$\dim(U \oplus V \oplus \dots)$

① first particle has state space U say $\mathbb{R}^2$

② second " " " V say $\mathbb{R}^3$

for ① need to give 2 nos

② " " 3 nos.

Quantum:

2 qubits ↑ ↑

if I make measurement:

↑ → $|0\rangle$ / $|1\rangle$

↑ → $|0\rangle$ / $|1\rangle$

$|0\rangle|0\rangle$

$|0\rangle|1\rangle$

$|1\rangle|0\rangle$

$|1\rangle|1\rangle$

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

where $|\alpha_{00}|^2 + \dots + |\alpha_{11}|^2 = 1$