Quantum computation Prabha Mandyal

Lec video by Preskill chp 2 Neilson & Chuang

Classical bits $x \in \{0,1\}$ (Binary fields)

↓

Quantum bits vector space with this set

Qubit space spanned by $\{|0\rangle\ |1\rangle\}$

ket 0 ket 1

vectors in a complex linear vector space!

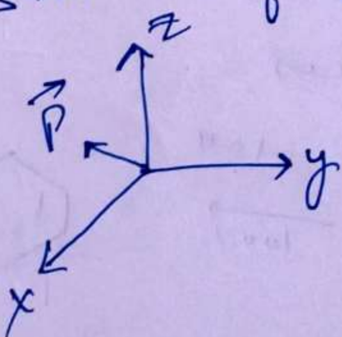
complex linear combinations $\alpha|0\rangle + \beta|1\rangle$

$\alpha, \beta \in \mathbb{C}$

Qubit: span $\{|0\rangle, |1\rangle\} \in \mathbb{C}^2$ (2-dim complex linear vector space)

↓ belong to

Physically eg polarization state of light Transverse em. waves.



X. polarization $= |H\rangle$ Horizontal

Z. polarization = vertical $|V\rangle$

Qubit! $\in \{|H\rangle, |V\rangle\}$ $\perp$ directions ~~direction~~ ↕ orthogonal vectors states in the vector space

↓

$|0\rangle$ $|1\rangle$

* Mathematical, Matrix representation

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

column vector

(2×1 matrix)

General qubit state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

.. ket-psi "superposition"

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

Departure from classical: superposition

Hilbert space is a big place! | $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- Carlton Caves

* Transform qubit states? classically | $\alpha, \beta \in \mathbb{R}$?? R_e-bit | 'Real' qubit

45° $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ | 135: $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

* mathematically, matrix representation.

* Transfer qubit states? classically, logical gates $\longleftrightarrow$ Boolean function $\{0,1\} \rightarrow \{0,1\}$

single-bit gates: Not, ~~identical~~ identity

$$\begin{array}{ccc} 0 & & 0 \\ 1 & & 1 \end{array} \qquad \begin{array}{c} 0 \rightarrow 0 \\ 1 \rightarrow 1 \end{array}$$

- Multibit gates: AND, OR, NOR, NAND, XOR

$\{0,1\}^{\times 2} \longrightarrow \{0,1\}$
2 qubit input → single bit.

Universality: Any Boolean function can be vectorized using a basic set of gates

Universal gates: NAND / NOR

Quantumly, Gates are transformation of 2-d complex vector /

Quantum Not gate?

$|0\rangle \to |1\rangle$

$|1\rangle \to |0\rangle$

$$\begin{pmatrix}1\\0\end{pmatrix}_{2\times1} \longrightarrow \begin{pmatrix}0\\1\end{pmatrix}_{2\times1}$$ column vector

Linear transformation / operator $\Leftrightarrow$ Matrix

$$\begin{pmatrix}a & b\\ 1 & \end{pmatrix}_{2\times2}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$$

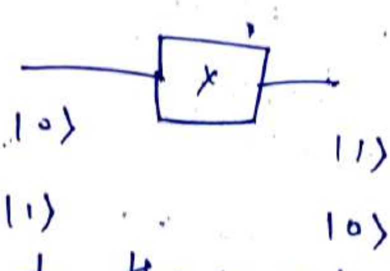
Matrix product

Quantum Not gate "x-gate" = $\cancel{\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}}$ $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$

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

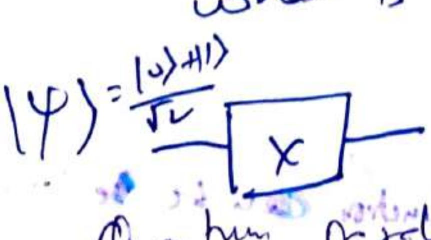
check $X|1\rangle = |0\rangle$

Q: circuit



HW:- Input to the x-gate is $\frac{|0\rangle + |1\rangle}{\sqrt{2}} = |\psi\rangle$

what is the output



Quantum parallelism

Parallism Be carefull

Quantum parralism

Recap : Quantum bit $\{|0\rangle, |1\rangle\} \in \mathbb{C}^2$ Linear vector space

vector

"ket"

(2-d, complex

superposition: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

arbitrary state of a qubit

$\alpha, \beta \in \mathbb{C}$

Quantum Gates : Linear transformations (Matrices)

Quantum Not gate : $|0\rangle \quad |0\rangle$ "Bit flip"

$|1\rangle \quad |1\rangle$

canonical / std. representation

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{2\times 1}, \quad |1\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{2\times 1}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Input $\longrightarrow \boxed{X} \longrightarrow$ output

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

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

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

$$= -|-\rangle$$

$$\left.\begin{aligned} X|+\rangle &= |+\rangle \\ X|-\rangle &= -|-\rangle \end{aligned}\right\} \text{Eigen value equation}$$

single qubit gates :- Infinity ~~set~~ of them!

- 2×2 matrices
- 2×2 unitary matrices

(Classical case
only NOT, Identity)

Identity matrix $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

quantum gate
phase

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

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

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

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

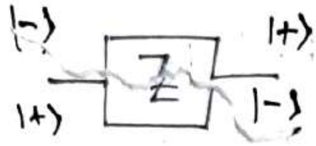
eigenvalue equation

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

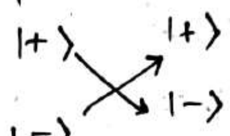
$Z|1\rangle = -|1\rangle$

→ non-trivial phase

→ "overall" phase ??



Z gate flip $|+\rangle$ to $|-\rangle$
$|-\rangle$ to $|+\rangle$



"phase flip"

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

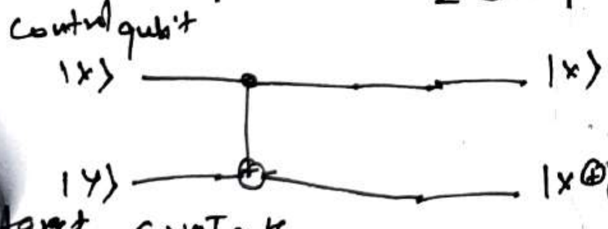
$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

relative phase

* All single qubit gates are reversible
* - Two qubit gates (also reversible)

(classically, OR, AND, NOR, NAND, XOR
↓
quantum XOR

2-bit input → 1-bit output



} unitary matrices (4x4)
||
Reversible

$|x\rangle|y\rangle \longrightarrow$ $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$] 4-dimen. linear vector space

$\begin{pmatrix}-\\ -\end{pmatrix} \otimes \begin{pmatrix}-\\ -\end{pmatrix}$

"tensor product"

$\begin{pmatrix}-\\ -\\ -\\ -\end{pmatrix}_{4\times1}$

2 qubit gets 4x4 matrix

$\begin{pmatrix}-\\ -\\ -\\ -\end{pmatrix}_{4\times1}$

2 qubit gates 4x4 matrices, column vector of length 4

CNOT gate ("Truth table")

$|0\rangle_c |0\rangle_t \longrightarrow |0\rangle_c |0\rangle_t$

$|0\rangle_c |1\rangle_t \longrightarrow |0\rangle_c |1\rangle_t$

$|1\rangle_c |0\rangle_t \longrightarrow |1\rangle_c |1\rangle_t$] flip the target | control Not gate

$|1\rangle_c |1\rangle_t \longrightarrow |1\rangle_c |0\rangle_t$

$|x\rangle |y\rangle \xrightarrow[\text{CNOT}]{} |x\rangle_c |x \oplus y\rangle_t$

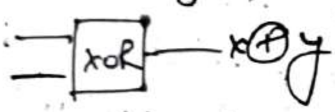
$x, y \in [0,1]$

XOR operation!

$0 \oplus y = y$

$1 \oplus y = \bar{y}$ (flips the bit)

classically



|| irreversible operations

* Universality { CNOT, single qubit gates
2-qubit gate — universal set of q-gates

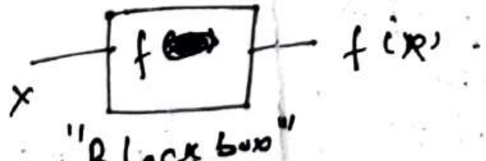
* Deutsch algorithm (David Deutsch 1985)

Toy problem: A binary function $f(x)$, $x \in [0,1]$

$f(0) = f(1)$ ("constant function")

or $f(0) \neq f(1)$ (Balanced function)

~~Identify~~ Task!: Given f, identify whether f is constant or balanced

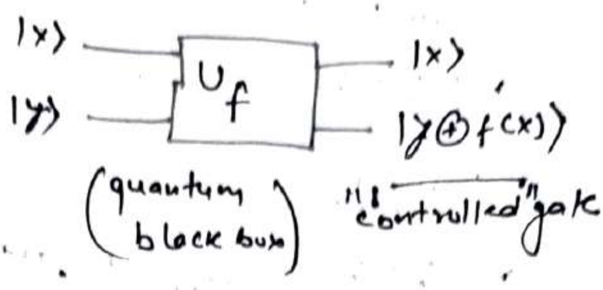


"Black box"

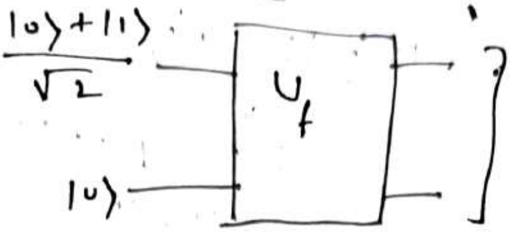
* Classically this task need 2 "queries" to the black box input.

* Quantumly:

Input a superposition state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$



(q-black box)



$$\frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$$

one query evaluate both $f(0)$ and $f(1)$

Step 2 Extract the information about $f(0) \doteq f(1)$ as a relative phase.

Step 3 Measure and identify if f is constant or balanced.

One query to the block box.

L-3

Recall Deutsch problem Given $f(x)$; $x \in [0,1]$

$f(0) = f(1)$ constant,

$f(0) \neq f(1)$ balanced

Task :- Is $f(x)$ constant or balanced?

* Classical "oracle" model of computing:

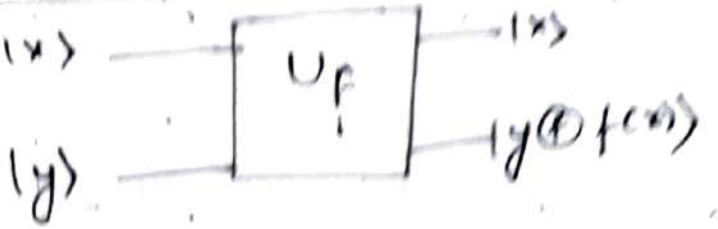
Complexity defined in terms of # of "queries" to the block box

- How many input given before task is complete → queries

* for the Deutsch problem, classically [illegible] of queries?
* Quantum oracle :- need only one query to the [illegible]

[illegible]

$x, y \in \{0,1\}$



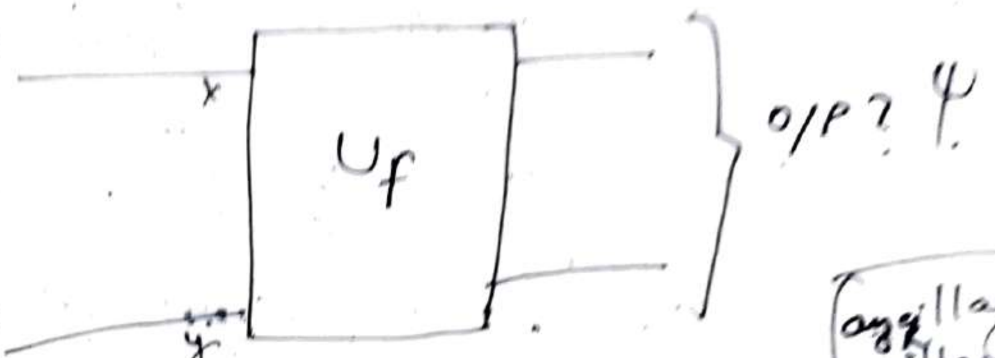
I.B.M.
Deutsch algorithm must go through

Deutsch circuit,

data (x) $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

(ancilla qubit) $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

(ancilla qubit)



[ancilla qubit
ancilla qubit]

$$|x\rangle|y\rangle \xrightarrow[U_f]{} |x\rangle|y \oplus f(x)\rangle$$

Input state $\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)_d \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_a$

$$= \frac{1}{2}\Big[|0\rangle|0\rangle + |1\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|1\rangle\Big]$$

After the action of U_f, state is

$$= \frac{1}{2}\Big[|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle - |0\rangle|1 \oplus f(0)\rangle - |1\rangle|1 \oplus f(1)\rangle\Big]$$

Deul $1 \oplus f(0) = \overline{f(0)}$ (complement)

$1 \oplus f(1) = \overline{f(1)}$

State after $U_f : |\psi\rangle = \frac{1}{2}\Big[|0\rangle\big(|f(0)\rangle + |\overline{f(0)}\rangle\big) + |1\rangle\big(|f(1)\rangle - |\overline{f(1)}\rangle\big)\Big]$

Deut $1 \oplus f(0) = \overline{f(0)}$ (complement)

$1 \oplus f(1) = \overline{f(1)}$

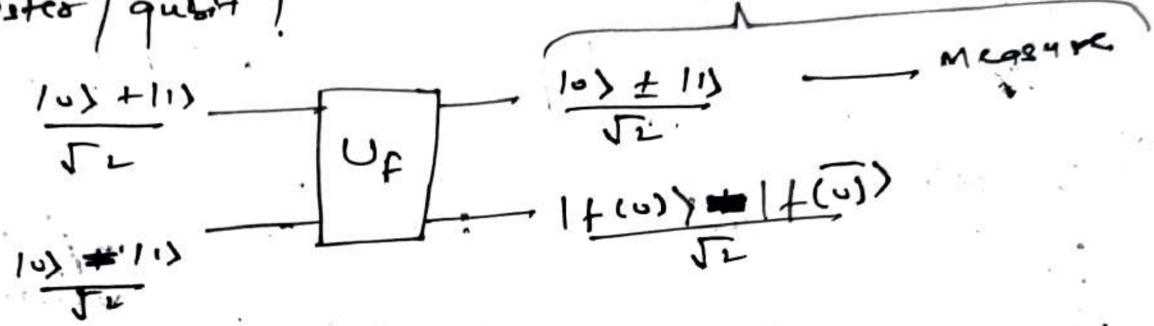
* Two cases (a) If $f(0) = f(1)$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left(\frac{|f(0)\rangle + |\overline{f(0)}\rangle}{\sqrt{2}}\right)$$

(b) $f(0) \neq f(1) \Rightarrow f(0) = \overline{f(1)}$

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

* Information about $f(0) \overset{?}{=} f(1)$ (f is constant or balanced) has been extracted into the relative phase of the data register / qubit !



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

distinct state (orthogonal states)

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

final step is to measure and see whether the o/p is $|+\rangle$ or $|-\rangle$

→ Quantum algorithm which is twice as fast as classical one

$\begin{pmatrix}1\\0\end{pmatrix} \overset{\alpha}{\leftarrow} |0\rangle \longrightarrow \begin{pmatrix}1\\i\end{pmatrix}$

$\begin{pmatrix}0\\1\end{pmatrix} \overset{\beta}{\leftarrow} |1\rangle = \begin{pmatrix}1\\-i\end{pmatrix}$

* <u>Deutsch - Jozsa algorithm</u>

say $f(x)$ is an n-bit binary function

(2^n such string) $x = x_1 x_2 \cdots x_n$ $[x_i \in \{0,1\}]$

$\underbrace{x_1 x_2 \cdots x_n}_{\text{string of } n\text{-bits}}$

If $f(x)$ is constant $\Rightarrow$ $f(x) = 0$ or $f(x) = 1$] for all input string x

* If $f(x)$ is balanced $\Rightarrow$ $f(x) = 0$ for half the input

$f(x) = 1$ for half the input

Task: Given a promise that $f(x)$ is either constant or balanced.

Given f.

queries do you need to decide whether f is constant or balanced

* classically $(2^{n-1}+1)$ queries

Input $\left(\frac{2^n}{2}+1\right)$ string before we know f is constant/balanced.

* quantumly this need only one query

speedup. exponential!

400: 97, 1985
Proceeding of Royal society

L-4

Qubit — Belong to a 2-dimensional Linear vector space

\ state of a 2-level quantum system

Postulate of Quantum Mechanics

① Classically one describe the state of a system using a set of generalized coordinates, gen. moment -um/velocities.

e.g. position coordinate, momentum coordinate

(P1) states of a quantum system are associated with unit vector in a Hilbert space.

Infinite dimension
Issue of convergence, completeness

finite ~~time~~ dimensional linear vector space endowed with a inner product

↓

Inner product space

Recall Say $\mathbb{V}$ is linear vector space

$\mathbb{V}$ is a collection of vectors $[|v\rangle]$ $(|\cdot\rangle$ ket ≡ vector$)$

such that

(i) If $|v\rangle, |w\rangle \in \mathbb{V}$, $|v\rangle + |w\rangle \in \mathbb{V}$

(ii) If $\lambda \in \mathbb{C}$ (scalar)

$$\lambda |v\rangle \in \mathbb{V}$$

(iii) $\alpha, \beta \in \mathbb{C}$, $|v\rangle, |w\rangle \in \mathbb{V}$,

$$\alpha|v\rangle + \beta|w\rangle \in \mathbb{V}$$

(iv) There exist a null vector $|\phi\rangle$ s.t

$$|v\rangle + |\phi\rangle = |v\rangle$$

Example: (1) space of $d \times 1$ complex matrices
d-dimensional complex vector
d-dimensional column vector
(d rows)
$\Big\}\ \mathbb{C}^d$

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ - \\ - \\ - \\ v_d \end{pmatrix}_{d\times 1}$$

d complex no. to describe $|v\rangle$

$(v_1, v_2, \ldots v_d)$

$$= v_1\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix} + v_2\begin{pmatrix}0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix} + v_3\begin{pmatrix}0\\ 0\\ 1\\ \vdots\\ 0\end{pmatrix} + \ldots v_d\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix}$$

Basis for the vector space $\{|e_1\rangle, |e_2\rangle, \ldots |e_d\rangle\}$

Any set of vector that spans the space $\mathbb{V}$ forms a basis for $\mathbb{V}$

$\Rightarrow$ Any $|v\rangle \in \mathbb{V}$ can be written as

$$|v\rangle = \sum_i \underset{\substack{\downarrow\\ \text{complex coefficient}}}{c_i} |e_i\rangle$$

(ii) Space of 2×2 complex matrices : $\mathbb{M}_{2\times2}(\mathbb{C})$ $\rightarrow$ (complex field)

$$M = \begin{pmatrix} a & b\\ c & d\end{pmatrix}_{2\times2} \quad a, b, c, d \in \mathbb{C}$$

* Check that it is a Linear vector space!
* what is a basis for this space?
* what is the "dimension" of this space?

dim = 4!

consider $\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}$

Any $M \in \mathbb{M}_{2\times2}(\mathbb{C}) = a\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + b\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + c\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + d\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$

(iii) $\mathbb{M}_{d\times d}(\mathbb{C}) \equiv$ LVS! (Dimension ??)

(iv) space of square-integral functions $\exists$ Hilbert space

$\psi(x)$ $[0,1] \rightarrow \mathbb{C}$ (wave function for q.m)

(complex-valued function)

$$\int_{x=0}^{1} |\psi^*(x)\,\psi(x)\,dx = \int_0^1 |\psi(x)|^2 dx < \infty$$

finite

* ~~Inner product and norm~~

* Linear independence:- A set of vector $|v_i\rangle \in V$ is linearly independent if

$$\sum_i \alpha_i |v_i\rangle = 0 \iff \alpha_i = 0 \ \forall i!$$

e.g. $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \in \mathbb{C}^2$

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

Question

Test (a) $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \begin{pmatrix}0\\1\end{pmatrix} \in \mathbb{C}^2 \rightarrow$ Are they linearly?

(b) $\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix} \in \mathbb{C}^2 \rightarrow$ Are they linearly independent

* Inner product and norm

– Bra-vector associated with ket-vector

$\langle v|$ $\longleftrightarrow$ $|v\rangle$

dual space ~~dual V space~~ primal V. space eg $|v\rangle \in \mathbb{C}^d$

Action of dual / primal.

$\langle w | v \rangle$ = scalar (number)

inner product

eg $|v\rangle \in \mathbb{C}^d$ $\quad |v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix}$

$\langle v| = \left(\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix}^* \right)^T$ complex conjugate and transpose || Adjoint

bra-"v"

$= \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix}^\dagger$

$= \left(v_1^* \; v_2^* \cdots v_d^* \right)$ row-vector!

$\langle w | v \rangle$ (v_1^* = complex conjugate of v_1)

$\Leftarrow$ Inner product

for $|w\rangle, |v\rangle \in \mathbb{C}^d$

$\langle w | v \rangle = \left(w_1^* w_2^* \cdots w_d^* \right)_{1\times d} \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}_{d\times 1}$

$\langle w|v\rangle = \sum_i^d w_i^* v_i$

* Norm of a vector! $\boxed{\sqrt{\langle v | v \rangle} = \| |v\rangle \|}$

$(|v\rangle \in \mathbb{C}^d)$ $\quad \| |v\rangle \| = \sqrt{\sum |v_i|^2} \geq 0$ $\rightarrow$ real positive

$\| |v\rangle \| = 0$ iff $|v\rangle \equiv$ null vector

Norm $\equiv$ "length" of a vector.

* Any finite-dim LVS with a inner product $\equiv$ Hilbert space

* $|\psi\rangle \in H$ (Hilbert space)

ket-psi

Unit vector = vector with unit norm,

$$\Rightarrow \; \| \, |\psi\rangle \, \| = 1$$

* The Qubit state space (spin-$\frac{1}{2}$ particle)

Qubit $\equiv$ Two level quantum system

$\equiv \mathbb{C}^2$ (2d complex LVS)

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

$$\boxed{\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \text{ form a basis for } \mathbb{C}^2}$$

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

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

* How many real parameters do we need to characterize $|\psi\rangle$?

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \;;\; |\alpha|^2 + |\beta|^2 = 1$$

Ans 2!

$\alpha, \beta \Leftrightarrow$ 4 real parameters

\+ 1 constraint (norm)

3 real parameters
$\Downarrow$ fixed in choosing overall phase
2 real parameters

__Lec 5__ ~~fundamental~~ - I

Postulates of Q. Mech (cont.)

- Qubits the bloch sphere
- Orthonormal Bases
- Operator and the outer product

__Recall__ Complex linear vector space

finite dim $\Leftrightarrow$ Hilbert space (with inner product)

(P1) Q-state are unit vectors in a Hilbert space

eg spin-$\frac{1}{2}$ particle, two level atom (two level quantum systems)

(Polarization state of light)

fundamental particles e^- protons etc have an internal degree of freedom called <u>spin</u> (spin angular momentum)

Planck's constant

In units of "$\hbar$" spin of a spin-$\frac{1}{2}$ takes on one of two values $+\frac{\hbar}{2}$, $-\frac{\hbar}{2}$

spin $\frac{1}{2}$ $\left.\begin{matrix} +\frac{1}{2} \\ -\frac{1}{2} \end{matrix}\right\}$ with reference to an external magnetic field

(. $\parallel$ or anti $\parallel$, $\uparrow$, $\downarrow$).

$\rightarrow$ 2-d. q. system. $\Rightarrow$ $|\uparrow\rangle, |\downarrow\rangle$ or $|+\frac{1}{2}\rangle, |-\frac{1}{2}\rangle$

$\{|0\rangle, |1\rangle\}$ qubit

(b) Two level atom: } not accessed.

model of a superconducting qubit (anharmonic oscillator) ← { excited ——— $|e\rangle \equiv |1\rangle$; ground ——— $|g\rangle \equiv |0\rangle$ } 2-dim. complex LVS.

* State space of 2-level quantum system.

$$\mathbb{C}^2 \equiv 2\text{-dim complex LVS} \equiv \begin{pmatrix} - \\ - \end{pmatrix}_{2\times 1}$$

Basis : $\{|0\rangle, |1\rangle\}$

Any state $|\psi\rangle \in \mathbb{C}^2$ can be expressed as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \left[|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix};\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]$$

"Ket vector"

Unit vectors: Inner product $\langle\psi|\psi\rangle$

Dual state: $\langle\psi| = \alpha^*\langle 0|$
(bra vector)

adjoint ket
↓
(complex conjugate transpose)

$$\langle\psi|\psi\rangle = (\alpha^*\langle 0| + \beta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle)$$

$$= |\alpha|^2\langle 0|0\rangle + \beta^*\alpha\langle 1|0\rangle + \alpha^*\beta\langle 0|1\rangle + |\beta|^2\langle 1|1\rangle$$

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

$$\langle 1|0\rangle = (0\ 1)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 \longrightarrow \text{orthogonal state!}$$

$$\langle 0|1\rangle = (1\ 0)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \nearrow$$

$\{|0\rangle, |1\rangle\}$ are $\perp^r$ to each children

$\langle 1|1\rangle = (0\ 1)\begin{pmatrix}0\\1\end{pmatrix} = 1$ // [$|0\rangle$ $|1\rangle$ are unit vector ! "normalized"]

$\Rightarrow \{|0\rangle, |1\rangle\}$ form an orthonormal basis for $\mathbb{C}^2$

ONB

Homework check $\{|+\rangle, |-\rangle\}$ form an ONB for $\mathbb{C}^2$

* Normalize a vector. If $|\phi\rangle$ is not a unit vector, then,

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

Overall phase freedom $|\phi\rangle, |\tilde{\phi}\rangle$ correspond to the same physical state !

Recall Linear independence $\alpha|v\rangle + \beta|w\rangle = 0 \Leftrightarrow \alpha = \beta = 0$

2-d. LVS $\Rightarrow$ only ~~2 linearly~~ state can A set of lin independent have exactly two elements

$$\boxed{\alpha|0\rangle + \beta|1\rangle = 0} \Rightarrow \alpha = \beta = 0$$

$|0\rangle, |1\rangle$?? a third lin. independent vector to this ~~state~~ set?

Every $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

* A set of vectors which are mutually orthogonal are always lin. independent)

Say $|v\rangle, |w\rangle$ are a pair of orthogonal vector in $\mathbb{C}^2$

suppose $\alpha|v\rangle + \beta|w\rangle = 0$.

$\langle w|(\alpha|v\rangle + \beta|w\rangle) = 0 \Rightarrow \beta = 0$.

but $\langle v|$ " $) = 0$ $\quad \alpha = 0$!

why only 2 orthogonal vector in $\mathbb{C}^2$?

* Geometric description of the Qubit's state space

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

How many real parameters do we need to describe $|\psi\rangle$?

2 complex number $\Rightarrow$ 4 real parameters

$\downarrow$ $|\alpha|^2 + |\beta|^2 = 1$ ~~constant~~ 1 constraint

3 real parameters

$\downarrow$ (Freedom to fix the overall phase)

only 2!

~~we can~~ say $\alpha = |\alpha| e^{i\phi_\alpha}$, $\beta = |\beta| e^{i\phi_\beta}$

$\phi_\alpha, \phi_\beta \in [0, 2\pi]$

$|\alpha|^2 + |\beta|^2 = 1 \Rightarrow |\alpha| = \cos\left(\frac{\theta}{2}\right)$ $\theta = [0, \pi)$

$|\beta| = \sin\left(\frac{\theta}{2}\right)$

$$\Rightarrow |\psi\rangle = \cos\left(\frac{\theta}{2}\right) e^{i\phi_\alpha}|0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi_\beta}|1\rangle$$

$$= e^{i\phi_\alpha}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\phi_\beta - \phi_\alpha)} \sin\left(\frac{\theta}{2}\right)|1\rangle\right]$$

(overall phase)

Define $\phi_\beta - \phi_\alpha = \phi$ (Relative phase)

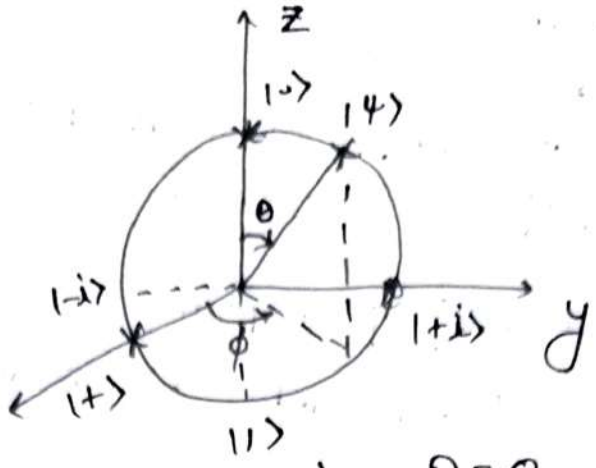
Spherical polar coordinates

$>$ state of a qubit $\Leftrightarrow$ surface of a unit sphere in $\mathbb{R}^3$

one to one mapping (real 3-dim space)

(Bloch Poincare sphere)

$\pi = 180°$



$|0\rangle = \theta = 0, \phi = 0$

on the xy plane

$|1\rangle \Rightarrow \theta = \pi, \phi = 0$

$\theta = \frac{\pi}{2}, \phi = 0 \longrightarrow |+\rangle \left(\cos\frac{\pi}{4}|0\rangle + \sin\frac{\pi}{4}|1\rangle\right)$

$\theta = \frac{\pi}{2}, \phi = \pi \longrightarrow |-\rangle \left(\cos\frac{\pi}{4}|0\rangle + e^{i\pi}\sin\frac{\pi}{4}|1\rangle\right)$

check these two are orthonormal

$\theta = \frac{\pi}{2}, \phi = \frac{\pi}{2} \Rightarrow \cos\frac{\pi}{4}|0\rangle + i\sin\frac{\pi}{4}|1\rangle$

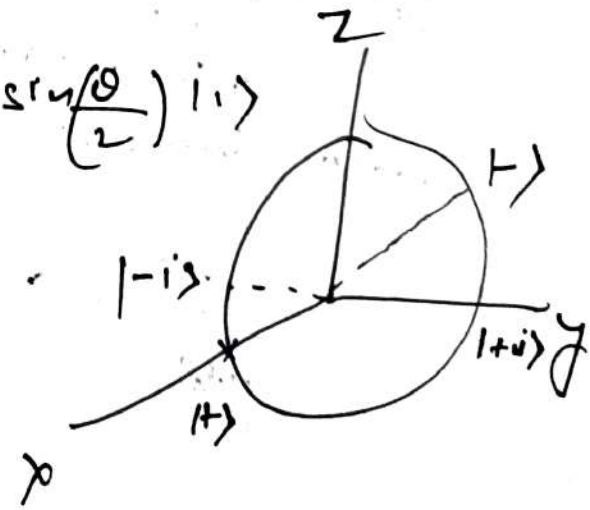
$= \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = |+i\rangle$

$\theta = \frac{\pi}{2}, \phi = \frac{3\pi}{2} \Rightarrow \frac{|0\rangle - i|1\rangle}{\sqrt{2}} = |-i\rangle$

L-6 Operator and outer product

Recap Bloch sphere

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



overall phase

$|\psi\rangle$ and $\lambda|\psi\rangle$

$\lambda \in \mathbb{C}$ are not distinguishable

say $\lambda = e^{i\gamma}$ (γ → gamma)

$\gamma \in [0, 2\pi]$ pure phase

$|\psi\rangle$, $e^{i\gamma}|\psi\rangle$ cannot be distinguished

$$\left\{ \theta = [0, \pi] , \phi = [0, 2\pi] \right\}$$

Half angle in θ, ensures that this is a one to one mapping

$$\left(|\pm i\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}} \right)$$

* Transform $|0\rangle \longrightarrow |1\rangle$: π rotation about the x-axis

$|+\rangle \longrightarrow |-\rangle$ π - rotation about Z-axis

* orthogonal states reside at the end of a diameter

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

orthogonal state $|\psi^{\perp}\rangle = ??$ $|0\rangle + |1\rangle \xrightarrow{??} |1\rangle$

* such a correspondence does not exist in higher dimension $(\mathbb{C}^d)$.

$\mathbb{C}^2 \longrightarrow \mathbb{C}^3$

qubit qutrit

$$\begin{pmatrix} - \\ - \\ - \end{pmatrix}$$

* Points in the interior represent mixed states (mixture of states that live on the surface)
Density operators.

<u>Postulates 2/3</u> observables/operators & Time evolution

classically, state $(\vec{x}, \vec{p})$
position momentum

observables $f(\vec{x}, \vec{p})$ (eg. angular momentum, charge)

* Quantumly, state $\longleftrightarrow$ vector in a Hilbert state

<u>Postulate 2.1</u> observables $\longleftrightarrow$ Hermitian operators on the system Hilbert space

(finite-dim) operators $\longleftrightarrow$ Matrices.

Hermitian matrices! M^{+} = adjoint $\equiv$ complex conjugate transpose
(self-adjoint)

$$M^{+} = (M^{*})^{T}$$

$$\boxed{M \text{ is Hermitian iff } M = M^{+}}$$

eg ① $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

$X^{*} = X$ and $(X^{*})^{T} =$

$X^{+} = X$ Hermitian matrix!

(Pauli spin matrices)

$= \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

h = Plancks constant

$\hbar = \frac{h}{2\pi}$

Physical dimension of angular momentum

② $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_y$

$Y^{*} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$

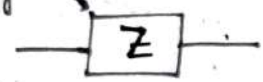
$(Y^{*})^{T} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y$

(c) $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \longrightarrow$ diagonal matrix! real entries.

$Z^{+} = Z$

$\frac{\hbar}{2} Z = \sigma_Z \longrightarrow$ Pauli spin matrix.

Q gate



- $Z|0\rangle = |0\rangle, \; Z|1\rangle = -|1\rangle$

Eigenvalue equations!

$\sigma_Z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\sigma_Z |0\rangle = \frac{\hbar}{2}|0\rangle$, $\sigma_Z|1\rangle = -\frac{\hbar}{2}|0\rangle$

$\{|0\rangle, |1\rangle\}$ are eigenvalue of σ_Z

$+\frac{\hbar}{2}$ $-\frac{\hbar}{2}$

* Hermitian matrices have real eigenvalues values that a physical quantity can take $\equiv$ eigenvalue of the corresponding Hermitian operator

$\sigma_Z \equiv$ operator associated with the spin of a spin-$\frac{1}{2}$ system

$\downarrow$

along the Z-direction.

spin-quantization "value" of spin can be either $+\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$ (Stern-Gerlach experiment)

$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{\sigma_z}$ → $|+\frac{1}{2}\rangle\ (|\uparrow\rangle)$, → $|-\frac{1}{2}\rangle\ (|\downarrow\rangle)$

$\alpha|\downarrow\rangle + \beta|\uparrow\rangle$

Measurement "apparatus"

$\sigma_z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$

* $|0\rangle$ is an eigenstate of σ_z with eigenvalue $+\frac{\hbar}{2}$

$|1\rangle$ " " " " $-\frac{\hbar}{2}$

Eigenstate are state where physical props take on definite value

$|0\rangle \longrightarrow \boxed{\sigma_z}$ → $|0\rangle$, → x <u>Not possible!</u>

Apparatus

$|1\rangle \longrightarrow \boxed{\sigma_z}$ → x Not possible, → $|1\rangle$

$|+\rangle, |-\rangle \longrightarrow$ do these states take on definite value of spin along z-direction?

No!!

$$\left.\begin{aligned}\sigma_x|+\rangle &= \frac{\hbar}{2}|+\rangle \\ \sigma_x|-\rangle &= -\frac{\hbar}{2}|-\rangle\end{aligned}\right\} \longrightarrow$$ along x-direction? yes!

<u>Lect 7.</u> Hermitian & Unitary operators
[outer-Product Notation]

Postulate 2: observables (Physical quantities) $\updownarrow$ Hermitian operators

<u>eg</u> Pauli spin observables (spin of a spin-$\frac{1}{2}$ particle)

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- All Hermitian
- Physically, they correspond to spin along x, z and y directions

* Hermitian operators: $M = M^\dagger$ (self-adjoint matrices)

<u>Properties</u>: (i) Eigenvalues are all real

$$M|e\rangle = \lambda|e\rangle \quad \text{Eigenvalue equation}$$

eigenvalue — λ; eigenvector / eigenstate / eigen-vect — $|e\rangle$

$[|e_i\rangle]$

$$M|e_i\rangle = \lambda_i|e_i\rangle$$

$[\lambda_i]$ are all real for Hermitian matrices

$$(M|e\rangle)^\dagger = \langle e|M^\dagger = \langle e|\lambda^* \quad \text{— (2)}$$

[Aside $(AB)^\dagger = B^\dagger A^\dagger$] Chp 2 Sec 2.1, 2.2

$$(1): \langle e|M|e\rangle = \lambda\langle e|e\rangle$$

$$(2): \langle e|M^\dagger|e\rangle = \lambda^*\langle e|e\rangle$$

$$= \lambda\langle e|e\rangle$$

$$\Rightarrow \lambda = \lambda^*$$

$$|e\rangle \doteq \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} \qquad \langle e| = (a_1^* \; a_2^* \ldots a_d^*)$$

$\langle e|e\rangle = \sum_i |a_i|^2 \geq 0$ |

* Physical $\Leftrightarrow$ Hermitian operator

Value of physical quantities = set of eigenvalue

$\sigma_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \longrightarrow$ E.value are $\pm \frac{\hbar}{2}$

characteristic eqn $|A - \lambda I| = 0$

$\sigma_x = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \longrightarrow$ eigenvalue are $\pm \frac{\hbar}{2}$

$\sigma_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \longrightarrow$ " " $\pm \frac{\hbar}{2}$

Property (ii) Eigenvector of a Hermitian operator ~~form an orthonormal~~ are mutually ortho-gonal

$$M|e_i\rangle = \lambda_i |e_i\rangle$$

$$\langle e_j|e_i\rangle \propto \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

(Kronecker delta function

$$\boxed{\begin{gathered}\langle e_j|e_i\rangle = 0 \\ i \neq j\end{gathered}}$$

Example $\sigma_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \longrightarrow$ eigenvector are $\{|0\rangle, |1\rangle\} \longrightarrow$ ON basis

$\sigma_z|0\rangle = \frac{\hbar}{2}|0\rangle$, $\sigma_z|1\rangle = -\frac{\hbar}{2}|1\rangle$

[$\{|0\rangle, |1\rangle\}$ computational basis / standard basis]

$\sigma_x = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow$ eigenvector are $\{|+\rangle, |-\rangle\}$ $\downarrow$ ON basis

$\sigma_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \longrightarrow$ eigenvectors ? ?

Recall $|\pm i\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}$

on basis

$\sigma_y |\pm i\rangle = \pm\frac{\hbar}{2} |\pm i\rangle$

Given $M|e_i\rangle = \lambda_i |e_i\rangle$, $\{|e_i\rangle\}$ form an ON basis

In the state $|e_i\rangle$; M has a definite value namely λ_i

$\{\sigma_z$ has a definite value in the state $|0\rangle$, $|1\rangle\}$

Outer product representation !

observable $\longleftrightarrow$ Matrices

$M|\psi\rangle = |\phi\rangle$

operator

state vectors

* First note the action of M on some ON basis in the space

say $\{|b_i\rangle\}_{i=1,2,\ldots d}$

$|\psi\rangle = \sum_i c_i |b_i\rangle$, $|\phi\rangle = \sum_i s_i |b_i\rangle$

$M\sum_i c_i |b_i\rangle = \sum_i s_i |b_i\rangle$

$\sum_i c_i \langle b_j | M | b_i\rangle = s_j$

$M|b_i\rangle = |x\rangle = \sum_j c_j$

$\sum_j c_j |b_j\rangle$

(i)

$\langle b_k | M | b_i\rangle = c_k$

$\sigma_x|0\rangle = |1\rangle$

$\sigma_x|1\rangle = |0\rangle$

$\langle 0|\sigma_x|0\rangle \quad \langle 0|\sigma_x|1\rangle$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in $\{|0\rangle, |1\rangle\}$ basis

$\langle 1|\sigma_x|0\rangle \quad \langle 1|\sigma_x|1\rangle$

$$\left.\begin{aligned} \langle 0|\sigma_x|0\rangle &= 0 \\ \langle 0|\sigma_x|1\rangle &= 1 \\ \langle 1|\sigma_x|0\rangle &= 1 \\ \langle 1|\sigma_x|1\rangle &= 0 \end{aligned}\right\}$$

$\frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

σ_x in $\{|+\rangle, |-\rangle\}$ basis ?? $\quad \langle -|\sigma_x|-\rangle$

* Diagnolization M will be diagonal in its eigenbasis (basis made out of its eigenvector)

Hermitian $\Rightarrow$ ON eigenbasis

$\Downarrow$

diagonal representation in its ON basis!

* Hermitian metrices are diagonalizable

$$\begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \lambda_d \end{pmatrix} = M$$

* Representing operators in bra-ket notation

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

$|v\rangle\langle w|$ = outer product

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix}_{d\times 1} (w_1^* \; w_2^* \cdots w_d^*)_{1\times d} = \begin{pmatrix} v_1 w_1^* & \cdots & v_1 w_d^* \\ v_2 w_1^* & & \vdots \\ \vdots & & \\ v_d w_1^* & \cdots & v_d w_d^* \end{pmatrix}_{d\times d}$$

eg $|0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}(1\ 0) = \begin{pmatrix}1&0\\0&0\end{pmatrix}$

$\rightarrow$ Projection operator!

$(|0\rangle\langle 0|)|\psi\rangle$

$\searrow$

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

$|0\rangle\langle 0|$ on any state $|\psi\rangle$ is to project $|\psi\rangle$ onto $|0\rangle$!

True for any vector $|v\rangle \xrightarrow[\text{Projection operator}]{} (|v\rangle\langle v|)$

$|0\rangle\langle 1| = \begin{pmatrix}0&1\\0&0\end{pmatrix}_{2\times 2}$

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

$\downarrow$

Projection operator along $|1\rangle$

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

Notice $|0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix}1&0\\0&1\end{pmatrix} = I_{2\times 2}$!

$|0\rangle\langle 0| - |1\rangle\langle 1| = \sigma_z \rightarrow$ diagnolization

Completeness relation

$|0\rangle\langle 1| + |1\rangle\langle 0| \stackrel{\hbar/2}{=} \begin{pmatrix}0&1\\1&0\end{pmatrix} = \sigma_x$ #

$\rightarrow$ If $\{|b_i\rangle\}$ is an ON basis for lin. vec space

$$\boxed{\sum_{i=1}^{d} |b_i\rangle\langle b_i| = I_{d\times d}}$$

Hermitian M with eigenvalues λ_i, $|e_i\rangle$

$$\begin{bmatrix}\lambda_1 & & 0\\ & \lambda_2 & \\ 0 & \ddots & \lambda_d\end{bmatrix} \quad \boxed{M = \sum_i \lambda_i \underbrace{|e_i\rangle\langle e_i|}_{\text{projection operators!}}}$$

Q :- what is the diagonal ~~otherwise~~ outer product representation for σ_x ?

$$(|0\rangle\langle 1| + |1\rangle\langle 0|)\,|0\rangle = (|0\rangle\langle 1|)|0\rangle + (|1\rangle\langle 0|)|0\rangle$$

$$= |1\rangle$$

$$(|0\rangle\langle 1| + |1\rangle\langle 0|)\,(\alpha|0\rangle + \beta|1\rangle) \xrightarrow[\text{check}]{} \alpha|1\rangle + \beta|0\rangle$$

X-operator

off-diagonal matrix

$$(|0\rangle\langle 1|)\,|0\rangle = 0$$

$(|0\rangle\langle 1|) \rightarrow$ transformation (not a projection)

PH L-8: Outer Product, Unitary Operator

eg. What is the operator that achieves the basis transformation :

$$|0\rangle \longrightarrow |+\rangle \;?$$

$$|1\rangle \longrightarrow |-\rangle$$

(σ_z) (σ_x)

$$\{|0\rangle, |1\rangle\} \longrightarrow \{|+\rangle, |-\rangle\}$$

ON basis ON basis

Recall $(|v\rangle\langle w|)|\psi\rangle = \langle w|\psi\rangle\, |v\rangle$

linear transformation

vectors $\longrightarrow$ vectors

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

In single basis!

$H = |+\rangle\langle 0| + |-\rangle\langle 1|$

$H|0\rangle = (|+\rangle\langle 0|)|0\rangle + (|-\rangle\langle 1|)\cancel{|0\rangle}$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} \qquad H|1\rangle = |-\rangle. \text{ (check!)}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |+\rangle$$

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

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

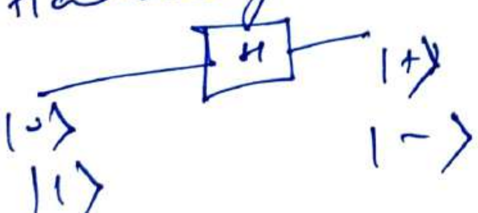
$$H = |+\rangle\langle 0| + |-\rangle\langle 0|$$

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

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

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

Hadmard gate



check $H|+\rangle = ??$

$H|-\rangle = ??$

Props of H: $H^\dagger = H$ (Hermitian!)

$$H^\dagger H = H^2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

$$= I_{2\times 2}$$

$$H H^\dagger = H^2 = I$$

H is a unitary matrix

Postulate 3 (QM): state transform via unitary operations

$$|\psi(t)\rangle = U(t,0)|\psi(t=0)\rangle$$

(Time evolution)

$$|\psi(t_2)\rangle = U(t_2,t_1)|\psi(t_1)\rangle$$

U is unitary iff $U^\dagger U = U U^\dagger = I$

$\boxed{U^\dagger = U^{-1}}$ $\longrightarrow$ reversible dynamics!

* Time evolution is governed by the Schrodinger eqn.

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = \mathcal{H}|\psi(t)\rangle$$

$\rightarrow$ Hamiltonian

Hermitian

then $|\psi(t)\rangle = e^{-\frac{iHt}{\hbar}} |\psi(0)\rangle$

is the solution to schrodinger eqn

$e^{-\frac{iHt}{\hbar}} \rightarrow$ exponentiation of an operator

H (diagonalizable) $= \sum_{i=1}^{d} E_i |E_i\rangle\langle E_i| \longrightarrow$ (projector

E_i = energy ~~eg~~ eigenvalues

$|E_i\rangle \rightarrow$ " eigenstate

$$H = \begin{bmatrix} E_1 & & 0 \\ & E_2 & \\ 0 & & \ddots & E_d \end{bmatrix}$$

$$\underline{H|E_i\rangle = E_i|E_i\rangle}$$

$\downarrow$

ON basis

exp. of any operator $H = \sum_i E_i |E_i\rangle\langle E_i|$ (Eigenvalue decomposition)

$$e^{H} \Longrightarrow I + H + \frac{H^2}{2!} + \frac{H^3}{3!} + \cdots$$

(i) if H is Hermitian e^{H} is also Hermitian

(ii) $[H, e^{H}]$

[commutator : $[A, B] = AB - BA$]

$[A, A] = 0$ / $\rightarrow$ A commutes with itself

$[B, C] = 0 \rightarrow B, C$ commute

Commuting operator can be diagonalized in the same ON basis (simultaneously diagonalized)

$$e^{H} |E_i\rangle = \left(I + H + \frac{H^2}{2!} + \frac{H^3}{3!} + \cdots \right) |E_i\rangle$$

$$e^{H} |E_i\rangle = e^{E_i} |E_i\rangle$$ ($|E_i\rangle$ is also an eigenstate of e^{H})

* Hermitian operator $A|e_i\rangle = \lambda_i |e_i\rangle$

$f(A)|e_i\rangle = f(\lambda_i)|e_i\rangle$ for any polynomial fn. f.

Time evolution $|\psi(t)\rangle = e^{-\frac{iHt}{\hbar}} |\psi(0)\rangle$

$\downarrow$

$$e^{-\frac{iHt}{\hbar}} = \sum_i e^{-i\frac{E_i t}{\hbar}} |E_i\rangle\langle E_i|$$

$$\left(e^{-\frac{iHt}{\hbar}}\right)^{+} =$$

$$e^{iH} = I + iH - \frac{H^2}{2!} - i\frac{H^3}{3!} + \frac{H^4}{4!} - \cdots$$

$$\left(e^{iH}\right)^{+} = I - iH - \frac{H^2}{2!} + i\frac{H^3}{3!} + \cdots$$

$e^{-iH} \rightarrow$ Not Hermitian

* $e^{-iH} e^{iH} = I$!!

$U(t, 0) = e^{-\frac{i H t}{\hbar}}$ is a unitary operator

* **Mathematically**, say $|\phi\rangle = U|\psi\rangle$
unitary

$\langle \phi | \phi \rangle =$

(iii) unitary transformation preserve norm = conserve probability

* quantum computing : Quantum gates are unitary matrix
for d-dim → d×d unitary matrix
for qubit → 2×2 unitary matrix constitute quantum gates.

Spectral theorem (Diagonalization)

If A is Hermitian, then $A = \sum_i \lambda_i |e_i\rangle\langle e_i|$

it admit a diagonal representation

– If A is Hermitian, there exists a unitary matrix U such that

$UAU^{\dagger} = D$ → diagonal matrix

- Basis transformation $\leftrightarrow$ Unitary transformation
$\downarrow$
preserve inner product

let $\langle e_i | e_j \rangle = 0$ if $i \neq j$

$|\tilde{e}_i\rangle = U|e_i\rangle$ and $|\tilde{e}_j\rangle = U|e_j\rangle$

then $\langle \tilde{e}_i | \tilde{e}_j \rangle = \langle e_j | U^{+} U | e_i \rangle = \langle e_j | e_i \rangle$

$= 0$ if $i \neq j$

Lect 9 Quantum Measurement

Spectral theorm

Hermitian $A \rightarrow [\lambda_i, |e_i\rangle]$ ON basis

$\Downarrow$

$|\psi\rangle = \sum_i c_i |e_i\rangle$

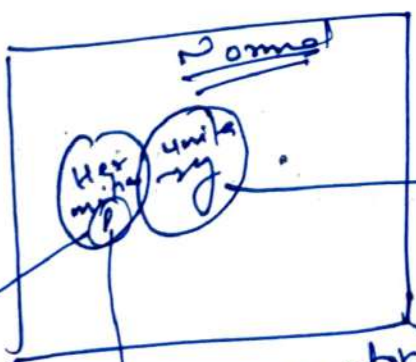
$A|e_i\rangle = \lambda_i |e_i\rangle$

$A|\psi\rangle = A \sum_i c_i |e_i\rangle$

$= \sum_i c_i \lambda_i |e_i\rangle \neq |\psi\rangle$

$\neq \alpha|\psi\rangle$!!

*



$UU^{+} = U^{+}U = I$
$\downarrow$ Norm preserving
time evaluation
Quantum gates

$H = H^{+}$
real λ_i
$\Downarrow$
observables

+ve operator
[eigenvalues are positive $\lambda_i \geq 0$ semidefinite]

* Normal operators: $[N, N^{+}] = 0$

Hermitian / Unitary

$NN^{+} = N^{+}N$

Spectral theorem Box 2.2 Nielsen & Chuang

Given any ~~normal~~ operator N, there exist a set of orthogonal projections $\{P_i\}$ such that

$$\boxed{N = \sum_i \lambda_i P_i} \rightarrow \text{spectral decomposition}$$

where $\{\lambda_i\} \in \mathbb{C}$ (complex scalars) are the eigenvalues of N (spectrum)

if and only if N is normal ($[N, N^\dagger] = 0$)

* Projection operator A Hermitian operator P is a projection iff $P = P^2$

Example: $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\{|0\rangle, |1\rangle\}$

$\downarrow$

(normal)

$|0\rangle\langle 0| = P_0$ projection onto $|0\rangle$

$\cancel{|0\rangle\langle 0| |\psi\rangle}$ $P|\psi\rangle = \alpha|0\rangle = (|0\rangle\langle 0|)|\psi\rangle$

$= (\langle 0|\psi\rangle)|0\rangle = \alpha|0\rangle$

$(|\psi\rangle = \alpha|0\rangle + \beta|1\rangle)$

$P_0^2 = \underbrace{(|0\rangle\langle 0|)(|0\rangle\langle 0|)}_{1} = |0\rangle\langle 0| = P_0!$

$|1\rangle\langle 1| = P_1$; $P_1^2 = P_1$

eigenvalue of P_0 / P_1?

$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $\lambda_i = [0, 1]$

$P_0^{\dagger} = P_0$

Rank of an operator: # of nonzero eigenvalues of an operator

$P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

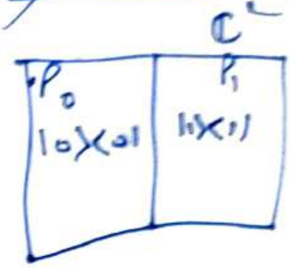
Rank of $\sigma_z = \underline{\underline{2}}$

dim of space $\Rightarrow$ ~~full~~ full rank operator

$\left.\begin{array}{l} \sigma_x = 2 \\ \sigma_y = 2 \\ \sigma_z = 2 \end{array}\right\}$

But $P_0, P_1 \longrightarrow$ have rank-1

<u>rank-1 projectors.</u>



* Projection operator of rank 2 on $\mathbb{C}^2$ $= I$!

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I^2 = I$ (eigenvalue!)

$I = P_0 + P_1$

$\boxed{\sigma_z = P_0 - P_1} \longrightarrow$ spectral decomposition of σ_z operator!

$\underline{\sigma_z = \sum_i \lambda_i P_i}$

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

$P_0 P_1 = (|0\rangle\langle 0|)(|1\rangle\langle 1|)$

$= 0$

$P_1 P_0 = 0$

A set $\{P_i\}$ is said to orthogonal iff $P_i P_j = \delta_{ij} P_i$

$\downarrow$

0 if $i \neq j$

1 if $i = j$

Any ON basis $\{|e_i\rangle\}$, construct projection operator

$$|e_i\rangle\langle e_i| = P_i$$

$$P_i P_j = \delta_{ij} P_j$$

$$\sum_i |e_i\rangle\langle e_i| = M = ??$$

Matrix element $\langle e_k|M|e_j\rangle = m_{kj} =$

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

Different for H; U

$$\sum_i \lambda_i |e_i\rangle\langle e_i| \qquad \sum_i \gamma_i |f_i\rangle\langle f_i|$$

$$\lambda \in \mathbb{R} \qquad \text{eigen} \in \mathbb{C}$$

$$\left[\begin{array}{c} UU^\dagger = U^\dagger U = I \\ \Rightarrow \quad |\gamma_i| = 1 \end{array}\right] \text{ show this}$$

$$= e^{i\phi_i}$$

spectral decomposition

construct a projection operator for state $|\psi\rangle$

rank 1 $\qquad P_{|\psi\rangle} = |\psi\rangle\langle\psi|$

$$P^2_{|\psi\rangle} = (|\psi\rangle\langle\psi|)(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| = P_{|\psi\rangle}$$

Spin system →

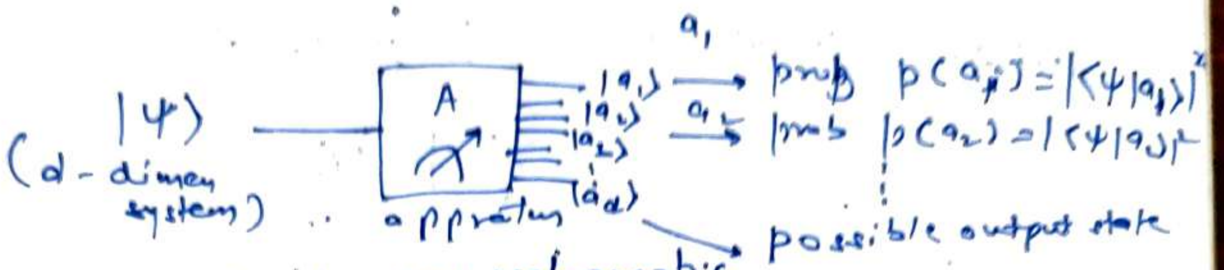
L 10 Quantum measurement when observable

A is measured on state $|\psi\rangle$, the set of outcomes is simply set of eigenvalues of A

(i) The probability of obtaining outcome a_i is given by $p(a_i) = |\langle\psi|a_i\rangle|^2$

$\left[\text{"Born rule" (Max Born)}\right]$: (eigenstate associated with eigen value a_i)

(ii) The state of the system after measurement collapses to one of the eigenstate $\{|a_i\rangle\}$ of A $\left[\text{"collapse postulate" Von Neumann}\right]$



* Measurement device schematic

* collapse : Recall $\{|a_i\rangle\}$ form an orthonormal ON basis for the system

$\Rightarrow$ Expand $|\psi\rangle = \sum_i c_i |a_i\rangle$ as a superposition of the eigenstate of A

o/p of the apparatus is no longer a superposition! It collapses the superposition to one of the $\{|a_i\rangle\}$

* Probabilities : $p(a_i) = |\langle\psi|a_i\rangle|^2 = (\langle\psi|a_i\rangle)(\langle\psi|a_i\rangle)^*$

$= \langle\psi|a_i\rangle\langle a_i|\psi\rangle$

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

$$\cancel{|\psi\rangle = \sum_i c_i|a_i\rangle} \quad \psi = \sum_{j=1}^{d} c_j |a_j\rangle$$

$$\langle a_i|\psi\rangle = \sum_{j=1}^{d} c_j \underbrace{\langle a_i|a_j\rangle}_{\delta_{ij}}$$

$$= c_i$$

$$p(a_i) = |\langle a_i|\psi\rangle|^2 = |\langle \psi|a_i\rangle|^2 = |c_i|^2$$

probability distribution! $0 \leq p(a_i) \leq 1$

$$\underline{\sum_i p(a_i) = 1}$$

$$\langle\psi|\psi\rangle = \left(\sum_j c_j^* \langle a_j|\right)\left(\sum_i c_i|a_i\rangle\right)$$

$$= \sum_{i,j} c_j^* c_i \underbrace{\langle a_j|a_i\rangle}_{\delta_{ij}} = \sum_{i=1}^{d} |c_i|^2 \underbrace{\langle a_i|a_i\rangle}_{1}$$

$$= \sum_{i=1}^{d} |c_i|^2 = 1$$ iff $|\psi\rangle$ is normalized!

ψ is a unit vector

$$\Rightarrow \sum_i p(a_i) = 1$$

Projector operator

Measurement

transformation: $|a_i\rangle\langle a_i| \leftrightarrow P_i$

associate a projector with every eigenstate of the observable A

Input : $|\psi\rangle\langle\psi| \xrightarrow[A]{\text{measurement of}} \frac{P_j(|\psi\rangle\langle\psi|)P_j}{Tr[P_j|\psi\rangle\langle\psi|]}$

Prob. associated with the input state

$$(P_j|\psi\rangle = c_j|a_j\rangle)^\dagger = \langle\psi|P_j = \langle a_j|c_j^*$$

$(P_j^\dagger = P_j)$ $P_j^2 = P_j$

Post measurement state : $\frac{P_j(|\psi\rangle\langle\psi|)P_j = |c_j|^2|a_j\rangle\langle a_j|}{Tr[P_j|\psi\rangle\langle\psi|]}$

Trace of $A = \sum_i A_{ii}$ (sum of diagonal entries)

$= \sum_i \lambda_i$ (sum of eigenvalue for diagonalized operator]

($Tr[M|\psi\rangle\langle\psi|] = \langle\psi|M|\psi\rangle \rightarrow$ show in the assignment)

$M \downarrow$ any operator

$$Tr(P_i|\psi\rangle\langle\psi|) = \langle\psi|P_i|\psi\rangle$$

$$= \langle\psi|(|a_j\rangle\langle a_j|)|\psi\rangle = |\langle\psi|a_j\rangle|^2$$

$$= |c_j|^2$$

$$|\psi\rangle\langle\psi| \rightarrow \frac{P_j|\psi\rangle\langle\psi|P_i}{Tr[P_i|\psi\rangle\langle\psi|]} = (|a_j\rangle\langle a_j|)$$

Measurement of $A \longleftrightarrow \{P_j\}$ orthogonal projectors on to the eigenstate

Probability $= |\langle\psi|a_j\rangle|^2 = \underline{Tr[P_i|\psi\rangle\langle\psi|]}$

(Born rule)

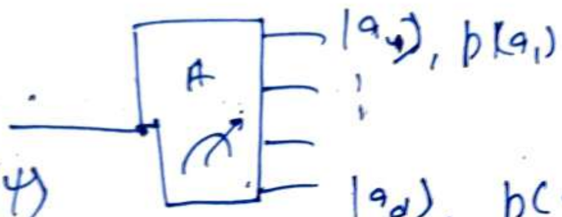
$$\sum_i P_i = \sum_i |a_i\rangle\langle a_i| = I \quad \text{(completeness relation)}$$

A physical example of

$$|\psi\rangle = |a_i\rangle, \text{ with prob. } p_i$$

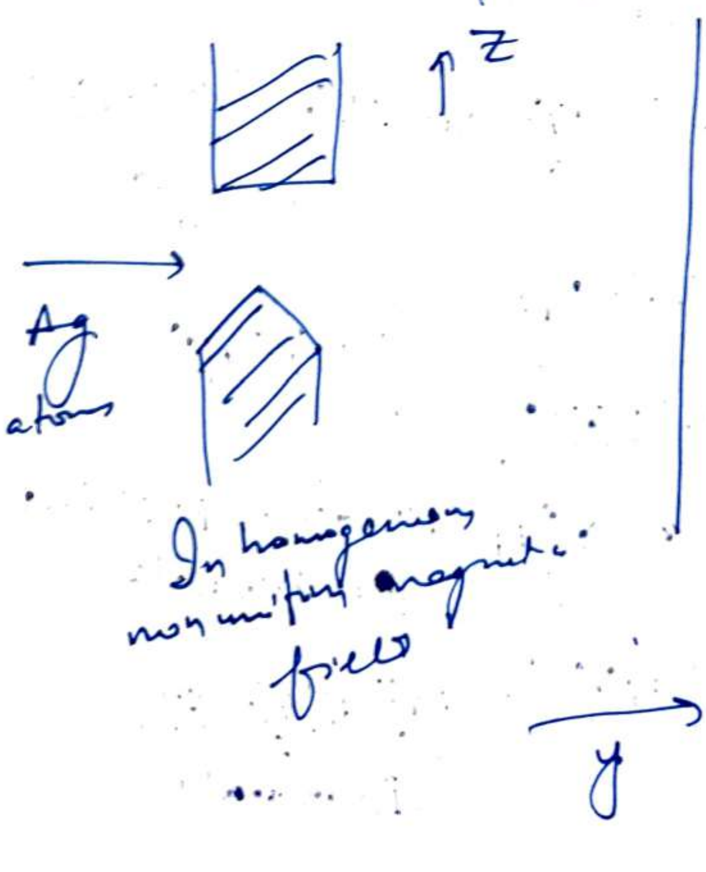
$$|\psi\rangle \xrightarrow{?} \sum_i p_i |a_i\rangle$$

* Measurement transformation does not map vector to vectors! (unlike gates)



→ A physical experiment : spin measurement apparatus

Stern - Gerlach experiment (Sec. 1.5.1 in Nielsen Chuang)



why Ag? Net orbital angular mom zero

* 1 unpaired e^-

probe the spin ang. momentum of e^-

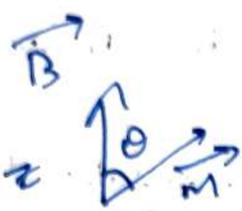
* ~~the~~ Spin → Intrinsic angular momentum

e^- → tiny magnetic dipole

mag dipole passes through a non uniform mag field, it experiences a force and ~~do~~ get deflected

– magnitude of force/deflection and angle made by $\vec{m}$ with the direction of $\vec{B}$

$\cos\theta$



* Outcome of SG experiment

* expected

If $\vec{m}$ is ~~uniformly~~ continuously distributed

* Actual outcome :

L – 11

* Due to spin angular momentum each e^- behaves like a tiny magnetic dipole $\vec{m}$ (mag. moment)

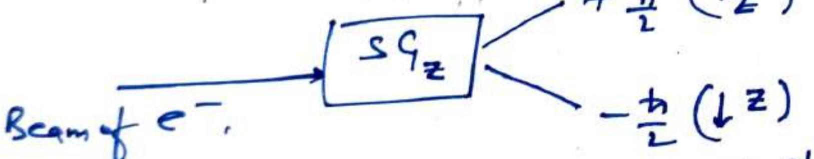
* e^-s (will get defflected) experience a force (F_z) causing them to deflect $\propto$ ($\cos\theta$)

* If $\vec{m}$ is uniformly oriented w.r.t Z axis, we expected a uniform spread of the beam

* But actual outcome was to observe two distinct patches on the screen

$\Rightarrow$ spin is quantized $\longrightarrow$ two possible orientation $\pm\frac{\hbar}{2}$

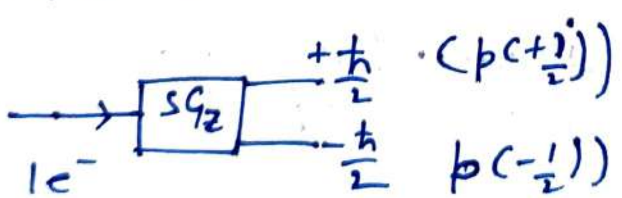
$\uparrow_z, \downarrow_z$



Apparatus that measures the spin along Z direction.

*** $\Rightarrow$ Ensemble of e^-s ($\uparrow_z, \downarrow_z$) $\longrightarrow$ measurement statistics.

* single e^- this the SG setup



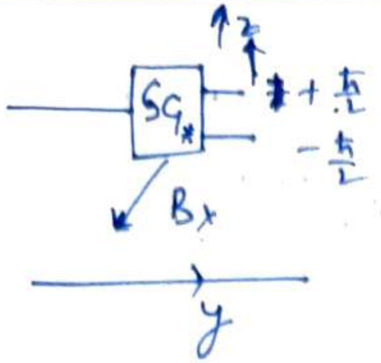
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

probability of $p(+\frac{1}{2}) = \frac{1}{2} = p(-\frac{1}{2})$

$$|\langle 0|\psi\rangle|^2 = \frac{1}{2} = |\langle 1|\psi\rangle|^2$$

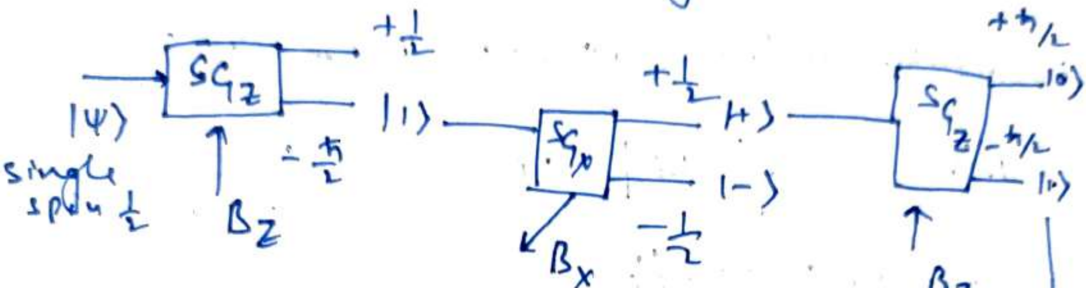
* sequential stern Gerlach set up:



→ SG along x-axis, probes/measure the spin along x-direction.

$\{|0\rangle, |1\rangle\}$ ↓ eigenstate of spin along z

$\{|+\rangle, |-\rangle\}$ eigenstate along x

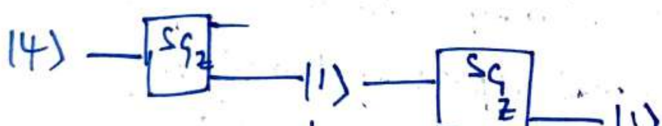


Both outcomes are equally likely

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

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

uniform spin position of $\underbrace{|+\rangle, |-\rangle}_{s_x}$



with probability 1

state with a definite value of spin along z (S_z/σ_z)

$[|0\rangle, |1\rangle] \longrightarrow$ definite value for (S_z/σ_z)

$\{|+\rangle, |-\rangle\} \longrightarrow$ " " " (S_x/σ_x)

⇒ Cannot simultaneously assign definite values of both σ_x and σ_z

⇒ Uncertainty principle !!

σ_x, σ_z are called incompatible observables

eg position and momentum!

$$\Delta\sigma_x \, \Delta\sigma_z \geq \frac{|\langle\psi| \overbrace{[\sigma_x, \sigma_z]}^{\text{Commutator}} |\psi\rangle|}{2}$$

(standard deviation) Variance

* Measurement statistics: $A \to [a_i]$ with prob. $p(a_i)$

(I) Expectation value (average / Mean value).

$$\langle A\rangle = \sum_i a_i \, p(a_i)$$

$$= \sum_i a_i \, |\langle\psi|a_i\rangle|^2$$

$$= \sum_i a_i \langle\psi|a_i\rangle\langle a_i|\psi\rangle$$

$$= \langle\psi| \underbrace{\left(\sum_i a_i |a_i\rangle\langle a_i|\right)}_{\parallel} |\psi\rangle$$

spatial decomposition of operator A!

diagonal representation of A!

$$\langle A\rangle = \langle\psi|A|\psi\rangle$$

(ii) Standard deviation / variance

$$(\Delta^2 A)_{|\psi\rangle} = \langle (A - \langle A\rangle)^2\rangle$$

check! $= \langle A^2\rangle - \langle A\rangle^2$

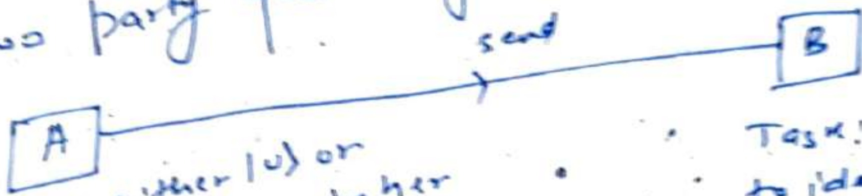
$\Rightarrow$ characterize the spread of a probability distribution

$\Rightarrow$ uncertainty in the value of observable

* $[\sigma_x, \sigma_z] \neq 0 \Rightarrow$ They are incompatible!

* Projected Measurement: project down to one of a set of orthogonal state projectors.

Two party quantum game :- state discrimination



prepare either $|0\rangle$ or $|+\rangle$ in her lab

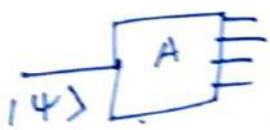
Task: is to identify which state she prepared!

L-12 Beyond projectile Measurement

* 2 party quantum game: quantum state discrimination

$p(a_i) = |\langle\psi|a_i\rangle|^2$

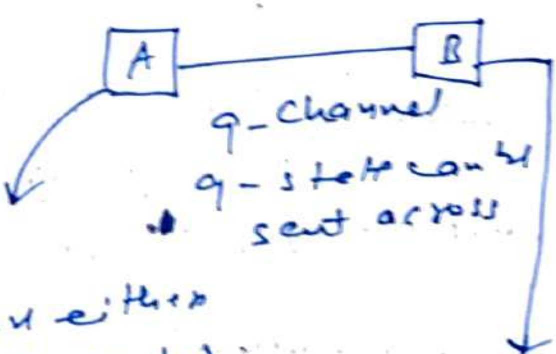
$= Tr[P_i$



$|\psi\rangle$ $\quad |a_1\rangle \longleftrightarrow P_1 = |a_1\rangle\langle a_1|$

$|a_d\rangle \quad P_d = |a_d\rangle\langle a_d|$

$$\text{prob} = p(a_i) = |\langle\psi|a_i\rangle|^2 = Tr[P_i|\psi\rangle\langle\psi|]$$



B's task: identify whether the state is $|0\rangle$ or $|+\rangle$

Prepare either $|0\rangle$ or $|+\rangle$

Measure!

Recall: measurement comprises of a set of orthogonal projectors.

$|0\rangle\langle 0|$

$|0\rangle$ — $\boxed{P_{|0\rangle}}$ — $|0\rangle$.

$|+\rangle$ — $\boxed{P_{|0\rangle}}$ —

Projection onto $|0\rangle$

Same outcome!

(b) Measure in the $\{|0\rangle, |1\rangle\}$ basis (Spin-Z measured)

$|0\rangle$ — $\boxed{S_Z}$ — $|0\rangle$ with ~~probability~~ probability 1!

$|+\rangle$ — $\boxed{S_Z}$ — $|0\rangle$ with ~~pair~~ probability $1/2$ ~~wrong guess~~

— $|1\rangle$ with ~~pair~~ probability $\frac{1}{2}$

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

(c) B-measure in the $\{|+\rangle, |-\rangle\}$ (measuring S_x operator spin x)

$|+\rangle$ — $\boxed{S_x}$ — $|+\rangle$

$|0\rangle$ — $\boxed{S_x}$ — $|+\rangle$ pair $1/2$

— $|-\rangle$ pair $1/2$

$\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right)$

$\Rightarrow$ ~~wrong guess~~

* Non orthogonal quantum states ($|0\rangle, |+\rangle$) $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$

cannot be distinguished ~~project~~ Projectyl!

* Beyond Projective measurement?

$|\psi\rangle$ — $\boxed{M}$] set of outcome $\longleftrightarrow$ Probability distribution consider a set of positive operators : $M = [E_1, E_2, \dots, E_d]$

$(E_i \geq 0) \rightarrow$ eigenvalues are all +ve semidefinite

(a) $0 \leq E_i \leq I$ $\Rightarrow$ [$I - E_i \geq 0$ is a +ve operator]

such that

(b) $\sum_{i=1}^{d} E_i = I$ such a set M can define a general quantum Measurement!

[- Positive - operator valued measures :- POVM]

$$|\psi\rangle \longrightarrow \boxed{M} \begin{cases} 1 \longrightarrow E_1 \\ 2 \longrightarrow E_2 \\ \vdots \\ d \longrightarrow E_d \end{cases}$$

Prob: $p(i) = \mathrm{Tr}(\dots)$

expectation value of E_i

$p(i) = \mathrm{Tr}(E_i |\psi\rangle\langle\psi|) = \langle\psi| E_i |\psi\rangle$

$\cancel{\mathrm{Tr}(E_i |\psi\rangle\langle\psi|)}$ $= 1$

(1) $0 \leq E_i \leq I \Rightarrow 0 \leq \langle\psi| E_i |\psi\rangle \leq 1$

$\Rightarrow \sum_i p(i) = \sum_i \mathrm{Tr}(E_i |\psi\rangle\langle\psi|)$

(2) $= \mathrm{Tr}\left(\underbrace{\left(\sum_i E_i\right)}_{= I} |\psi\rangle\langle\psi|\right)$

$= \mathrm{Tr}(|\psi\rangle\langle\psi|) = \underline{\underline{1}}$

$= \langle\psi|\psi\rangle$

(1) and (2) $\Rightarrow [p(i)]_{i=1}^{d}$ is a valid prob. distribution

~~$\langle\psi| E_i = |\psi$~~

$p(i) = \langle\psi| E_i |\psi\rangle$ $\hookrightarrow E_i = \sum_j \lambda_j^{(i)} \underline{\underline{|e_j^{(i)}\rangle\langle e_j^{(i)}|}}$

$= \underline{\underline{\sum_j \lambda_j^{(i)}}} \, |\langle e_j^{(i)}|\psi\rangle|^2$

Example: Zero error discrimination strategy for distinguishing b/w $|0\rangle$ and $|+\rangle$

Consider: $E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|$

$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} |-\rangle\langle -|$$

$$E_3 = I - (E_1 + E_2)$$

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

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

Suppose:

$M_1 = |1\rangle\langle 1|$, $M_- = |-\rangle\langle -|$ } +ve operators

$$M_1 + M_- = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$$

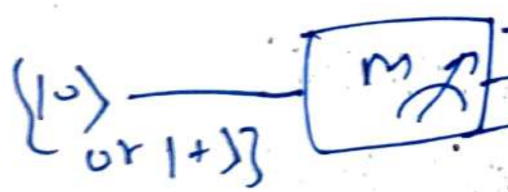
E.value $= 1 \pm \sqrt{2}$

$\Rightarrow M_1 + M_2 > I$

$[M_1, M_-]$ cannot be a valid POVM

$$0 \le E_1, E_2, E_2, E_3 \le I$$

$$E_1 + E_2 + E_3 = I$$



1 $\leftrightarrow E_1 \Rightarrow$ A must reject $|+\rangle$

2 $\leftrightarrow E_2 \Rightarrow$ A must reject $|0\rangle$

3 $\leftrightarrow E_3 \Rightarrow$ Inconclusive

* If we allow for POVMs, can we distinguish perfectly a pair of non orthogonal quantum states? No!

$|\psi_1\rangle$ $|\psi_2\rangle$ such that $\langle \psi_1 | \psi_2 \rangle \neq 0$

L-13 : Distinguishing quantum state and Density operator

Recall: Povm: $M = \{E_1, E_2, \ldots E_N\}$ st
Positive operator valued measure.
$0 \leq E_i \leq I$, $\sum_i E_i = I$

Prob. of outcome 'i' in the state $|\psi\rangle = p(i) = tr(E_i |\psi\rangle\langle\psi|)$
$= \langle\psi|E_i|\psi\rangle$

$$\sum_i p(i) = 1 \Leftrightarrow \underbrace{\sum_i E_i = I}_{\text{completeness}}$$

- Post measurement state ? Recall for projective measurement $\{P_1, P_2, \ldots P_N\}$

$$\{|e_1\rangle\langle e_1|, |e_2\rangle\langle e_2|, \ldots |e_n\rangle\langle e_n|\}$$

corresponding to outcome 'i'

$$|\psi\rangle\langle\psi| \longrightarrow \frac{P_i|\psi\rangle\langle\psi|P_i}{Tr(P_i|\psi\rangle\langle\psi|)}$$

$$(|\psi\rangle \rightarrow |e_i\rangle)$$

- Canonical post measurement state :-

$$|\psi\rangle\langle\psi| \longrightarrow \frac{\sqrt{E_i}(|\psi\rangle\langle\psi|)\sqrt{E_i}}{Tr(\sqrt{E_i}|\psi\rangle\langle\psi|\sqrt{E_i})}$$

$0 \leq E_i \leftrightarrow \sqrt{E_i}$

$\overset{\text{cyclic}}{=}\ Tr(E_i|\psi\rangle\langle\psi|)$

$$\boxed{\sqrt{E_i} = \sum_j \lambda_j^{(i)} |f_j\rangle\langle f_j|}$$

$$\rightarrow \frac{\sqrt{E_i}(|\psi\rangle\langle\psi|)\sqrt{E_i}}{Tr(E_i|\psi\rangle\langle\psi|)}$$

---

* Distinguishing

Theorem Non orthogonal quantum state cannot be distinguished perfectly.

Note that if we have a set of orthogonal q- states.

$$s = \{ |\psi_1\rangle, |\psi_2\rangle \dots |\psi_N\rangle \}$$ in a d-dim space

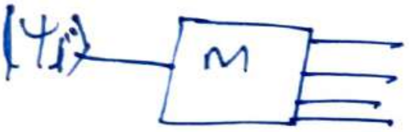
S can always be distinguished perfectly.

orthogonal projection $P_i = |\psi_i\rangle\langle\psi_i|$, $\sum_i P_i = \sum_i |\psi_i\rangle\langle\psi_i| \leq I$

$$P_{N+1} = I - \sum_i |\psi_i\rangle\langle\psi_i|$$

Perform the measurement $M = \{ P_1, P_2, \dots P_N, P_{N+1} \}$

* Perfect distinguishability $\Rightarrow$ If $|\psi_i\rangle$ is "recieved" or input the apparatus



$\Rightarrow$ $p(i) = Tr(P_i |\psi_i\rangle\langle\psi_i|)$
$= 1$

$$\boxed{\text{Hw}: \quad Tr(P_{N+1} |\psi_i\rangle\langle\psi_i|) = 0 \ \forall i = 1, 2, \dots N}$$

- All other outcomes have probability zero.

Prove:- Consider $|\psi_1\rangle, |\psi_2\rangle$ that are non orthogonal

$$\langle\psi_1|\psi_2\rangle \neq 0 .$$

Assume that there exists a measurement (POVM) with two operators E_1, E_2 such that ~~if E~~ ψ_1, ψ_2 are perfectly distinguishable ~~are realized~~

Prob. of outcome ih sate $|\psi_1\rangle = \langle\psi_1| E_1 |\psi_1\rangle = 1$

$$Tr(E_1 |\psi_1\rangle\langle\psi_1|)$$

Prob of outcome 2 in state $|\psi_2\rangle = Tr(E_2|\psi_2\rangle\langle\psi_2|) = \langle\psi_2|E_2|\psi_2\rangle = 1$ —— (*)

$E_1 + E_2 = I$ for it to be a valid measurement

since $\langle\psi_1|E_1|\psi_1\rangle = 1 \Rightarrow \langle\psi_1|E_2|\psi_1\rangle = 0$

$\Rightarrow \langle\psi_1|\sqrt{E_2}\sqrt{E_2}|\psi_1\rangle = 0$

$\Rightarrow (\langle\psi_1|\sqrt{E_2})(\sqrt{E_2}|\psi_1\rangle) = 0$

$\Rightarrow \sqrt{E_2}|\psi_1\rangle = 0$ —— (1)

Note that we can write $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_1^{\perp}\rangle$

$|\psi_1^{\perp}\rangle$ is some state orthogonal to $|\psi_1\rangle$

Normalization $\Rightarrow |\alpha|^2 + |\beta|^2 = 1$ —— (2)

$\sqrt{E_2}|\psi_2\rangle = \alpha\cancel{\sqrt{E_2}|\psi_1\rangle} + \beta\sqrt{E_2}|\psi_1^{\perp}\rangle$

$= \beta\sqrt{E_2}|\psi_1^{\perp}\rangle$ —— (3)

(*) $\Rightarrow \langle\psi_2|E_2|\psi_2\rangle \qquad = |\beta|^2$

$\langle\psi_2|\sqrt{E_2})(\sqrt{E_2}|\psi_2\rangle)$

$\beta^* \langle\psi_1^{\perp}|\sqrt{E_2})(\beta\sqrt{E_2}|\psi_1^{\perp}\rangle) < 1$

prob of outcome 2 in state $|\psi_2\rangle = \langle\psi_2|E_2|\psi_2\rangle < 1$

$\Rightarrow$ not consistent with (*)

$\Rightarrow$ we don't have a measurement that perfectly distinguishes $|\psi_1\rangle$ and $|\psi_2\rangle$

QED!

- Revisit the example of $|0\rangle, |+\rangle$
- Zero error discrimination strategy: $E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|$

$|1\rangle\langle 1| + |+\rangle\langle +| \leq I$

$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} |+\rangle\langle +|$

$|-\rangle\langle -|$

$E_3 = I - E_1 - E_2$

Prob of outcome '1' if input state $|0\rangle = Tr(E_1 |0\rangle\langle 0|)$

$= 0$

L-14 Density operator

* A more general description of the quantum state
* Measurement "proper" description of the post-measurement state? formally describe the measurement transformation unitary $U|\psi\rangle = |\phi\rangle$

Eg Projective measurements:

$$|\psi\rangle \longrightarrow |a_i\rangle, \; p(a_i) = |\langle\psi|a_i\rangle|^2$$

$$P_i = |a_i\rangle\langle a_i| \qquad |\psi\rangle\langle\psi| \longrightarrow \frac{P_i|\psi\rangle\langle\psi| P_i}{Tr(P_i|\psi\rangle\langle\psi|)}$$

* Post measurement state describe an ensemble (collection of possibilities)

Ensemble: $[|a_j\rangle, p(a_j)]$

$$\rho = \sum_j p(a_j) |a_j\rangle\langle a_j|$$

$= p(a_1)|a_1\rangle\langle a_1| + p(a_2)|a_2\rangle\langle a_2| + \dots$

$\dots + p(a_d)|a_d\rangle\langle a_d|$.

- Convex mixture of pure state
- Pure vs mixed state

Pure $\downarrow$ $|\psi\rangle \in \mathbb{C}^d$

Mixed $\rightarrow$ mixture of pure state

$|\phi\rangle = \sum_i c_i |a_i\rangle \longrightarrow$ Superposition of the eigen state $\{|a_i\rangle\}$

$|\phi\rangle \rightarrow$ pure state !

$c_i |a_i\rangle \rightarrow$ (phase information !)

ρ is not a superposition state; its an operator that describe incoherent mixture of pure states an:

- single pure state $|\psi\rangle \longleftrightarrow$ Density operator is $|\psi\rangle\langle\psi|$
- Mixed state $\{p_i, |\psi_i\rangle\}$
- Density operator $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \longrightarrow$ Matrix / operator on the system space
- Properties of ρ: (i) $\rho^\dagger = \rho$ (Hermitian)

(ii) $\langle\phi|\rho|\phi\rangle = \langle\phi|\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right)|\phi\rangle$

expectation value w.r.t $|\phi\rangle$

$= \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle$

≥ 0; for all states $|\phi\rangle$

$\Rightarrow \rho$ is a positive operator

$\rho \geq 0$

(iii) $Tr(\rho) = \sum_j \langle e_j|\rho|e_j\rangle$

(Pick some ON basis $\{|e_j\rangle\}$) $= \sum_{i,j} p_i \langle e_j|\psi_i\rangle\langle\psi_i|e_j\rangle$

$$= \sum_i p_i \Big(\underbrace{\sum_j |\langle e_j|\psi_i\rangle|^2}_{\text{coefficient of } \psi_i} \Big)$$

coefficient of ψ_i
$\parallel$
1 since
$|\psi_i\rangle$ ar normalised!

$= \sum_i p_i = 1$

$\underline{Tr(\rho) = 1}$

Alternatively $Tr(\rho) = Tr(\sum_i p_i |\psi_i\rangle\langle\psi_i|)$

$= \sum_i p_i Tr(|\psi_i\rangle\langle\psi_i|)$

$\parallel$

$\langle\psi_i|\psi_i\rangle$

$= \sum_i p_i = 1$

Modified postulate 1:- Q states are described/associated with density operator on a Hilbert space

$$\rho \geq 0 \text{ with } Tr(\rho) = 1$$

* Lemma ρ is associated with an ensemble of pure states $[p_i, |\psi_i\rangle]$

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|,$$

iff .. $\rho \geq 0$, $Tr(\rho) = 1$

"converse" Given $\rho \geq 0$, $Tr(\rho) = 1$

↓ Hermitian → ↓ Diagonalizable ↓

$\sum \lambda_i = 1$ ↓ form a probability distribution

$\lambda_i \geq 0$ ← $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$

spectral decomposition

"Natural" ensemble for $\rho = [\lambda_i, |e_i\rangle]$

* Measurement transformation: $|\psi\rangle \longrightarrow \boxed{A} \longrightarrow |a_1\rangle, \dots, |a_n\rangle$

Map density operation

$$\rho = |\psi\rangle\langle\psi| \longrightarrow \sum_i \frac{P_i \rho P_i}{Tr(P_i \rho)}$$

↓

$$\sum_i p(a_i)\,|a_i\rangle\langle a_i| \quad \Big| \quad = \sum_i \frac{|a_i\rangle|\langle a_i|\psi\rangle|^2\langle a_i|}{|\langle a}$$

$|\psi\rangle = |a_i\rangle$

$$: \frac{P_i |\psi\rangle\langle\psi| P_i}{\mathrm{Tr}(P_i \rho)}$$

$\mathcal{M}$: density ops. $\longrightarrow$ density ops.

$$\mathcal{M} = \{P_i\} : \rho \longrightarrow \sum_i P_i \rho P_i$$

Eg Q Key Distribution: A prepares $|0\rangle, |+\rangle, |1\rangle, |-\rangle$

$$\text{Ensemble } (\rho) = \frac{1}{4}\left(|0\rangle\langle 0| + |+\rangle\langle +| + |1\rangle\langle 1| + |-\rangle\langle -|\right)$$

$(\mathrm{Tr}(\rho) = 1 \; ; \; \rho \geq 0)$

* Pure vs. mixed state

$$\mathrm{Tr}(\rho) = 1$$

$$\mathrm{Tr}(\rho^2) = ??$$

$$\rho_1 = |\psi\rangle\langle\psi| \qquad \rho_2 = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$\mathrm{Tr}(\rho_1^2) = \mathrm{Tr}(\rho_1) = 1$$

$- \left(\mathrm{Tr}(|\psi\rangle\langle\psi|) = 1\right)$

$$- \mathrm{Tr}(\rho_2^2) = \mathrm{Tr}\Big(\sum_i p_i |\psi_i\rangle\Big)^2 < 1$$

$$= \sum_{i,j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2 < 1$$

$\cdot Tr(\rho^2) \equiv$ Measure of "purity" of a density operator

* $Tr(\rho^2) = 1$ iff ρ is a pure state, then $\rho = |\psi\rangle\langle\psi|$

HW Density operator associated with $|+\rangle\langle+|$? (Matrix form)

– Density operator " " $[\frac{1}{2}, |0\rangle; \frac{1}{2}, |+\rangle]$?

Lect 15 Density operator formalism :-

Postulate 1 :- Q states are represented by density operators. ρ is an operator on the system Hilbert space, such that

$$Tr(\rho) = 1 \quad \text{and} \quad \rho \geq 0$$

$\Longleftrightarrow$ Ensemble of pure states $= \{p_i, |\psi_i\rangle\}$ $\left(\sum_i p_i = 1\right)$

$$\rho = \underbrace{\sum_i p_i |\psi_i\rangle\langle\psi_i|}_{\text{convex sum of}} \text{ projection onto pure states}$$

* Pure vs mixed state :-

$\rho = |+\rangle\langle+| =$

eg (1) $\rho = |0\rangle\langle 0|$
$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

(2) $\rho = |+\rangle\langle+|$
$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

(Qubit density operator will be 2×2 complex matrix)

$\sigma = |-\rangle\langle-|$ (Pure state)
$= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$

(3) $\rho = \left[\frac{1}{2}|0\rangle, \frac{1}{2}|+\rangle\right] = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$

$= \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$ (mixed state)

Pure vs mixed states

$\mathrm{Tr}(\rho^2) = 1$ if and only if ρ is a pure state

Proof: If ρ is $|\psi\rangle\langle\psi|$, then $\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho) = 1$

If $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Then, $\mathrm{Tr}(\rho^2) = \sum_{ij} p_i^2 \langle\psi_i|\psi_j\rangle|^2$

$= \mathrm{Tr}\left(\sum_{ij} p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|\right)$

$= \sum_{ij} p_i p_j \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|)$

$= \sum_{ij} p_i p_j \langle\psi_i|\psi_j\rangle \mathrm{Tr}(|\psi_i\rangle\langle\psi_j|)$

$\mathrm{Tr}(|\psi\rangle\langle\phi|) = \langle\psi|\phi\rangle$ or $\langle\phi|\psi\rangle$

(a) (b)

Imp $\boxed{\mathrm{Tr}(|\psi\rangle\langle\phi|) = \langle\phi|\psi\rangle}$ $= \sum_{ij} p_i p_j |\langle\psi_i|\psi_j\rangle|^2$

when can $\mathrm{Tr}(\rho^2) = \sum_{ij} p_i p_j |\langle\psi_i|\psi_j\rangle|^2 \overset{?}{=} 1$

If and only if $p_i p_j = \delta_{ij}$

$p_i p_j = 1$ for some

$= 0$ other

* $\mathrm{Tr}(\rho^2)$ = Measure of purity of the density matrix

* $1 - \mathrm{Tr}(\rho^2) = S_L(\rho)$ linear entropy of the states ρ

Measure of how mixed the state is!

- $S_L(\rho) = 0 \Leftrightarrow \rho$ is pure

* Is this ensemble description of ρ unique??

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$\boxed{H = \sum_i x_i |e_i\rangle\langle e_i| = \sum_{ij} C_{ij} |f_i\rangle\langle f_j|}$$

eigenbasis representation $\longrightarrow$ any other basis

Example: $\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$

Let $|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$

(check: $\langle a|a\rangle = 1$)

$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$ (check $\langle b|b\rangle = 1$)

$$\langle a|b\rangle = \frac{1}{2}\langle b|a\rangle$$

$|a\rangle, |b\rangle$ are not orthogonal

$$\tilde{\rho} = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b|$$

in term of $\{|0\rangle, |1\rangle\}$ $= \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| = \rho$!!

- Two different ensemble representation for the same density matrix!

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b|$$

$$\Rightarrow \left[\frac{3}{4}, |0\rangle, \frac{1}{4}, |1\rangle\right] = \left[\frac{1}{2}, |a\rangle, \frac{1}{2}, |b\rangle\right]$$

Jozsa

SH JW Theorm: The ensemble representation of a density operator is not unique. Different ensembles associated with ρ, are related to each other as follow.

Schrodinger, Hughston, Wootters

Two ensembles $\{p_i, |\psi_i\rangle\langle\psi_i|\}_{i=1,2,3...m}$ and $\{q_j, |\phi_j\rangle\langle\phi_j|\}_{j=1,2,3...n}$ represent the same density operator ρ if and only if

$$\sqrt{p_i}\,|\psi_i\rangle = \sum_{k=1}^{p} u_{ij}\sqrt{q_k}\,|\phi_k\rangle$$

where $p = \max(m, n)$ and u_{ij} are elements of a $\underline{p \times p}$ unitary matrix.

$$\left[U = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & \cdots & & x_{2p} \\ \vdots & & & \\ x_{p1} & \cdots & & x_{pp} \end{pmatrix} = \text{unitary matrix} \right]$$

append zero vector to the smaller ensemble

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_j q_j\,|\phi_j\rangle\langle\phi_j|$$

$$= \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j|$$

unnormalized state

Proof (i) let $|\tilde{\varphi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$, $|\tilde{\phi}_j\rangle = \sqrt{q_j}\,|\phi_j\rangle$

suppose we are given that

$$|\tilde{\varphi}_i\rangle = \sum_{j=1}^{p} u_{ij}\,|\tilde{\phi}_j\rangle$$ where u_{ij} are of element of a unitary matrix

If U is a unitary matrix;

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

$$[U]_{ij} = u_{ij} \quad [U^{\dagger}]_{ij} = u^{*}_{ji}$$

$$[U^{\dagger}U]_{ij} = \sum_k u^{*}_{jk}u_{ki} =$$

$$\sum_k (U^{\dagger})_{ik}(U)_{kj} = \sum_k u^{*}_{ki}u_{kj} = (I)_{ij} = \delta_{ij}$$

$$\boxed{\sum_k u^{*}_{ki}u_{kj} = \delta_{ij}}$$

$$\boxed{[UU^{\dagger}]_{ij} = \sum_k u_{ik}u^{*}_{jk} = \delta_{ij}}$$

(*)

Given two ensembles $[p_i, |\psi_i\rangle]$ and $[q_j, |\phi_j\rangle]$

such that $\sqrt{p_i}\,|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}\,|\phi_j\rangle$

$$|\tilde{\varphi}_i\rangle = \sum u_{ij}\,|\tilde{\phi}_j\rangle$$

$$\sum_i |\tilde{\varphi}_i\rangle\langle\tilde{\varphi}_i| = \sum_i \left(\sum_{j,k} u_{ij}\,|\tilde{\phi}_j\rangle\langle\tilde{\phi}_k|\,u^{*}_{ik}\right)$$

$=$

$$\sum_{j,k}\left(\sum_i x_{ij} \, U_{ik}^*\right) |\tilde{\phi}_j\rangle\langle\tilde{\phi}_k|$$

$$\Vert$$

δ_{jk} since u is unitary matrix.

$$= \sum_{j,k} \delta_{jk} |\tilde{\phi}_j\rangle\langle\tilde{\phi}_k|$$

$$\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \rho = \sum_j |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j|$$ // QED

Lect 16 Qubit density operator, multipoint of Q. system

SHJW Theorm Two ensembles $\{p_i, |\psi_i\rangle\}_{(n)}$ and $\{q_j, |\phi_j\rangle\}_{(m)}$ represent the same density operator

$$\sqrt{p_i}\,|\psi_i\rangle = \sum_{j=1}^{p} u_{ij} \sqrt{q_j}\,|\phi_j\rangle \quad \forall i = 1,2,3,\dots n \quad \text{①}$$

where $u_{ij} = U$ is $p \times p$ unitary matrix

$$[p = \max(n \times m)]$$

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_{j=1}^{m} q_j |\phi_j\rangle\langle\phi_j| \quad \text{②}$$

* we proved, if ①, then ② !
* converse if ② holds, then there exist a U, such that ① holds.

Proof strategy is to go to the diagonal representation of ρ!

$$\rho = \sum_j \lambda_j |e_j\rangle\langle e_j| \longrightarrow \text{ON states}$$

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad \xleftrightarrow{v} \quad \rho = \sum_j \lambda_j |e_j\rangle\langle e_j| \quad \xleftrightarrow{w} \quad \rho = \sum_j q_j |\phi_j\rangle\langle\phi_j|$$

Note v and w are unitary,

$$u = v w^\dagger$$

$$u^\dagger u = w v^\dagger v w^\dagger = I$$

$$u u^\dagger = v w^\dagger w v^\dagger = I$$

* Qubit density operator:

ρ for a 2-dim q-system $\equiv 2\times2$ complex matrix

$\rho \in M_{2\times2}(\mathbb{C}) \longrightarrow$ linear vector space of 2×2 complex matrices

Basis for $M_{2\times2}(\mathbb{C})$:-

$$\left\{ \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \right.$$

$$\rho = a\begin{pmatrix}1&0\\0&0\end{pmatrix} + b\begin{pmatrix}0&1\\0&0\end{pmatrix} + c\begin{pmatrix}0&0\\1&0\end{pmatrix} + d\begin{pmatrix}0&0\\0&1\end{pmatrix}$$

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

ON basis $\longrightarrow$ Inner product?

$\langle A | B \rangle = \mathrm{Tr}(A^\dagger B) \longrightarrow$ (Assignment Q 2 iv)

Check! B is an ON basis as per this inner product. !

* Pauli Basis $\{I, \sigma_x, \sigma_y, \sigma_z\} \longrightarrow$ mutually orthogonal matrices.

$= \{\sigma_i, i = 0,1,2,3\}$

$(\sigma_0 = I, \sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z)$

$$\underset{I}{Tr(\sigma_i \sigma_j) = 2\delta_{ij}} \Rightarrow \left[\frac{\sigma_i}{\sqrt{2}}\right]_{i=0}^{3} \longrightarrow \text{form an ON basis}$$

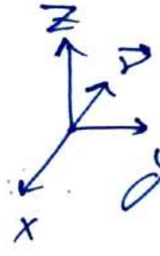
Q what density matrix $\Rightarrow \rho = r_0\sigma_0 + \underbrace{r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3}_{\text{Traceless}})$

(i) $Tr(\rho) = 1 \Rightarrow r_0 = 1$

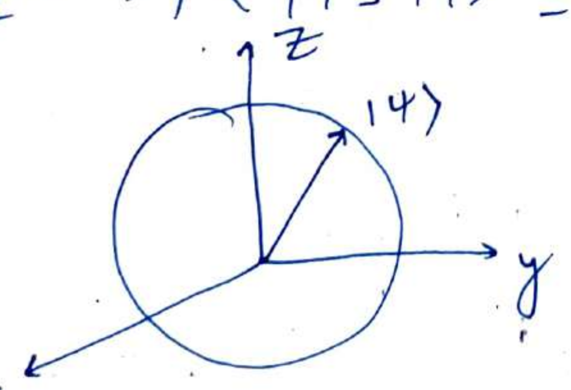
(ii) $\rho^\dagger = \rho \Rightarrow r_1^* \sigma_1 + r_2^* \sigma_2 + r_3^* \sigma_3$

$= r_1, r_2, r_3 \in R$

$\vec{r} = (r_1, r_2, r_3) \in R^3$



(iii) $\rho \geq 0 \Rightarrow \langle\psi|\rho|\psi\rangle \geq 0$



$\Rightarrow$ Bloch - Poincaré sphere

$\Leftrightarrow$ represents all qubits pure states

(iv) $Tr(\rho^2) < 1 \Rightarrow \rho^2 = \frac{1}{4}(I + r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3)^2$

$$Tr(\rho^2) = \frac{1}{4} Tr[(1 + r_1^2 + r_2^2 + r_3^2) I + \cdots]$$

$$= \frac{1}{\cancel{4}_2}(1 + \vec{r}\cdot\vec{r})\cancel{2} = \frac{1}{2}(1 + \vec{r}\cdot\vec{r})$$

$$\therefore = \frac{1}{2}(1 + \vec{r}\cdot\vec{r}) < 1 \Rightarrow \boxed{|\vec{r}|^2 < 1}$$

for mixed state

$$\rho = \frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z)$$

$$(r_1, r_2, r_3) = \vec{r} = (r_x, r_y, r_z)$$

$\Downarrow$

Bloch vector associated with ρ

What is the density matrix associated with origin? (Centre of the Bloch sphere)

$$\rho = \frac{I}{2} \longrightarrow \text{Maximal mixed state}$$

<u>Ensemble description</u> $\rho = \{\frac{1}{2}|0\rangle, \frac{1}{2}|1\rangle\}$

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

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \frac{1}{2} I$$

$$\rho = \{\frac{1}{2}|+\rangle, \frac{1}{2}|-\rangle\}$$

$$= \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{2} I$$

L-17 Multipartite Quantum systems:
(Enter Entanglement)

* Description of multipartite quantum systems?

eg 2 spin - $\frac{1}{2}$ particles

$\downarrow$

(Multiqubit system registers)

* ~~$|\psi\rangle_A \in \mathcal{H}_A$~~

Two d-level quantum systems.

state space = $\mathcal{H}_A \otimes \mathcal{H}_B$

$\mathcal{H}_A \rightarrow$ d-dim. Hilbert space

$\mathcal{H}_B \rightarrow$ d-dimension Hilbert space

$\otimes \rightarrow$ Tensor product or Kronecker product

* In the matrix representation,

U_A on system $\mathcal{H}_A \rightarrow d \times d$ matrix

U_B on system $\mathcal{H}_B \rightarrow d \times d$ matrix

operators on $\mathcal{H}_A \otimes \mathcal{H}_B = U_A \otimes U_B$

~~$U_A \otimes U_B$~~

Let $U_A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & & & \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix}$

$U_B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1d} \\ b_{21} & b_{22} & \cdots & b_{2d} \\ \vdots & & & \\ b_{d1} & b_{d2} & \cdots & b_{dd} \end{pmatrix}$

$$U_A \otimes U_B = \begin{pmatrix} a_{11}U_B & a_{12}U_B & \cdots & a_{1d}U_B \\ \vdots & & & \\ a_{d1}U_B & a_{d2}U_B & \cdots & a_{dd}U_B \end{pmatrix}_{d^2 \times d^2}$$

$(d^2 \times d^2)$

- $\mathcal{H}_A \otimes \mathcal{H}_B$ = composite system / joint system Hilbert space is of dim d^2.

state of joint system $|\varphi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \quad |w\rangle_B = \begin{pmatrix} w_1 \\ \vdots \\ w_d \end{pmatrix}$$

$$\mathcal{H}_A \otimes \mathcal{H}_B = |v_A\rangle \otimes |w_B\rangle = \begin{pmatrix} v_1 |w\rangle_B \\ v_2 |w\rangle_B \\ \vdots \\ v_d |w\rangle_B \end{pmatrix}_{d^2 \times 1}$$

column vector of length d^2 describes state of the joint Hilbert state

$$= \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_d \\ v_2 w_1 \\ \vdots \\ v_2 w_d \\ \vdots \\ v_d w_1 \\ v_d w_2 \\ \vdots \\ v_d w_d \end{pmatrix}_{d^2 \times 1}$$

Example: A pair of qubits : $\mathbb{C}^2 \otimes \mathbb{C}^2$ (dim = 4)

Basis for the two-qubit system:- $[|0\rangle, |1\rangle] \otimes [|0\rangle, |1\rangle]$

$$= [|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle]$$

$$= [|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle]$$

$$\downarrow$$

$$= [|00\rangle, |01\rangle, |10\rangle, |11\rangle]$$

Analogy with classical two bit system

$$= [00, 01, 10, 11] \quad [\text{4 two-bit string}]$$

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

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

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

Easy to check that $\{|00\rangle, |10\rangle, |11\rangle\}$ are a set of 4 ON states ($\Rightarrow$ Basis for a 4-dim space)

* Rules! Inner product b/w $|0\rangle_A|1\rangle_B$ and $|1\rangle_A|0\rangle_B$?

$$(|0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle) = \langle 0|1\rangle_A \langle 1|0\rangle_B$$

$$\boxed{\begin{aligned} &(|v\rangle_A \otimes |w\rangle_B, |e\rangle_A \otimes |f\rangle_B) \\ &= \langle v|e\rangle_A \langle w|f\rangle_B \end{aligned}}$$

(ii) Operators on two qubits $\equiv$ Matrices of dimension $[4 \times 4]$.

$$\boxed{(A \otimes B) . (|v\rangle_A \otimes |w\rangle_B) = A|v\rangle_A \otimes B|w\rangle_B}$$

$(X \otimes Z)\, |0\rangle\, |+\rangle$
$= |1\rangle |-\rangle$

$(Z \otimes X)\, |0\rangle |+\rangle = |0\rangle |+\rangle$

Most general two qubit states $|\psi\rangle_{AB} = ??$

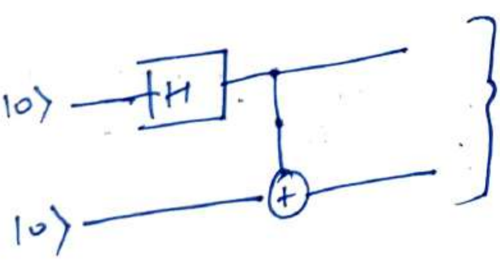
(Basis : $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$)

$|\psi\rangle_{AB} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

with $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$

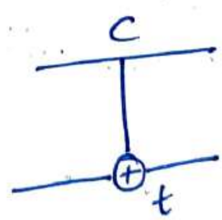
* Two qubit circuit (using a genuine two qubit gates)

CNOT :- Flips the target



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

CNOT



$|0\rangle|0\rangle \to |0\rangle|0\rangle$
$|0\rangle|1\rangle \to |0\rangle|1\rangle$
$|1\rangle|0\rangle \to |1\rangle|1\rangle$
$|1\rangle|1\rangle \to |1\rangle|0\rangle$

Recall, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$;

(in the $\{|0\rangle, |1\rangle\}$ basis)

output $= |+\rangle \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$

$$|0\rangle|0\rangle \xrightarrow{H\otimes I} |+\rangle|0\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|0\rangle$$

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

$\downarrow$ CNOT

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + |1\rangle|1\rangle$$

* Can we write $|\beta_{00}\rangle = |\phi\rangle \otimes |\psi\rangle$??

$a|0\rangle + b|1\rangle$ $\quad$ $c|0\rangle + d|1\rangle$

(Try to solve for a, b, c, d
→ inconsistent relations")

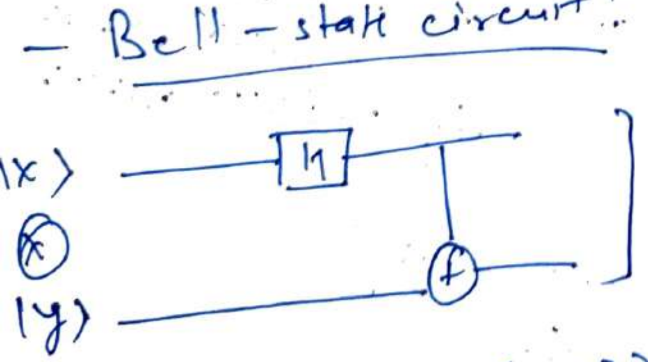
=> No! $|\beta_{00}\rangle$ cannot be factorized as tensor product of two single ($|\phi\rangle\otimes|\psi\rangle$) qubit states.

* Such states ($|\beta_{00}\rangle$) are called entangled states

~~$|\psi\rangle_{AB} \neq |\psi$~~

$$|\psi\rangle_{AB} \left(\in H_A \otimes H_B\right) \neq |\phi\rangle_A \otimes |\chi\rangle_B$$

- Bell-state circuit:



$|\beta_{xy}\rangle$ → ~~4 states~~ 4 entangled states called Bell EPR state

$(x, y \in \{0,1\})$

Bell EPR state

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

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \neq |\phi\rangle \otimes |\chi\rangle$$

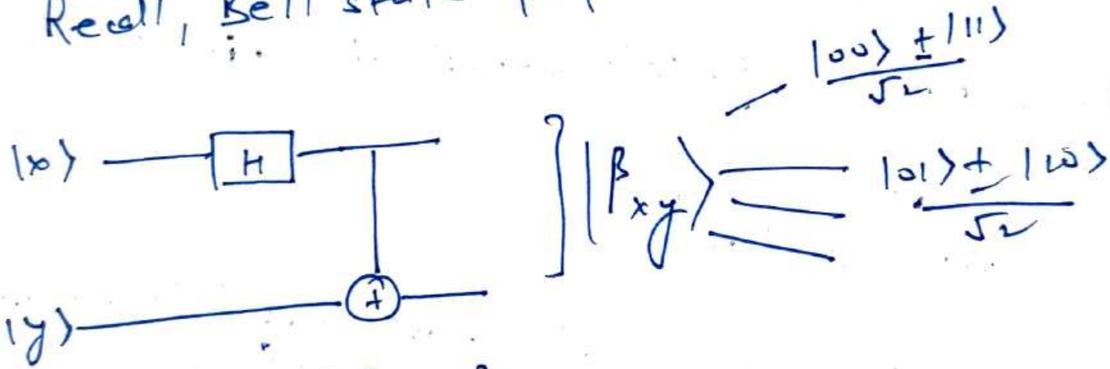
$|0\rangle \otimes |1\rangle$

$$|\beta_{10}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Lec 18 Bell state and Teleportation

Recall, Bell state prep. circuit



$x, y \in [0, 1]$

$\mathbb{C}^2 \otimes \mathbb{C}^2$ Basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

Product state

$|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$

Subsystem

$|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$

$H_A \otimes H_B$

(local states)

subsystem

There do no exist state $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$ such that

$$|\beta_{xy}\rangle = |\psi\rangle_A \otimes |\phi\rangle_B$$

$\Rightarrow$ these are entangled states.

Generally $|\psi\rangle_{A_1 A_2 \cdots A_N} \neq |\psi_1\rangle_{A_1} \otimes |\psi_2\rangle_{A_2} \otimes \cdots |\psi_N\rangle_{A_N}$

(eg N-qubit state) system) N-positive quantum state))

(ii) Bell EPR states: Maximally entangled states

(Einstein Podolsky Rosen)
((1931), Phys. Rev)

John S. Bell (Particle physicist at CERN, 1960)

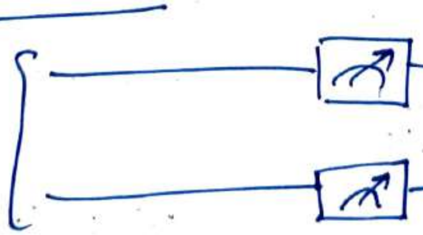
$\downarrow$

(Spin systems)

show that these states have correlation beyond what ~~ate~~ possible in classical physics

(iii) Quantum Correlation

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



classical bit

$b_1 \in [0,1]$

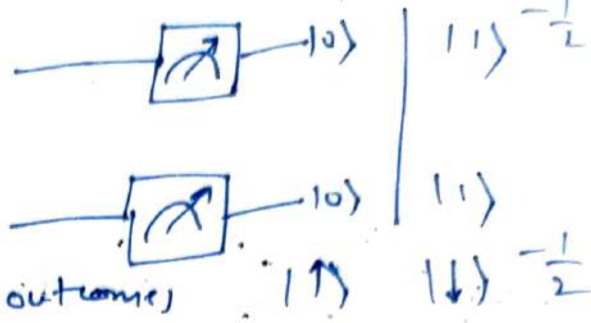
$b_2 \in [0,1]$

$[|0\rangle, |1\rangle]$ basis

All classical outcomes are not allowed!

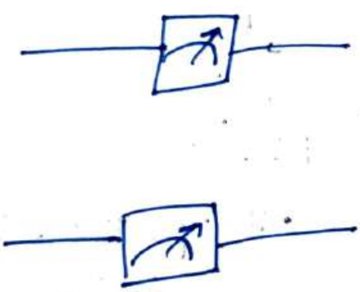
Possible outcomes are $(0,0)$, $(1,1)$

$$\frac{|0_b 0_b\rangle + |11\rangle}{\sqrt{2}}$$



Classical measurement outcomes are completely correlated
fully

Normally



4 possible outcomes $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$

$\text{Prob}(0,0) = \frac{1}{2} = \text{Prob}(1,1)$
↓
Maximally entangled.
(maximally uncertain about the outcomes)

Check :- This is a feature of all 4 Bell EPR states.

$$\frac{|0_{b_1} 1_{b_2}\rangle \pm |10\rangle}{\sqrt{2}} \longrightarrow$$ outcomes are $(0,1)$ and $(1,0)$ perfectly anti correlated.

Consider this state Non maximally entangled state

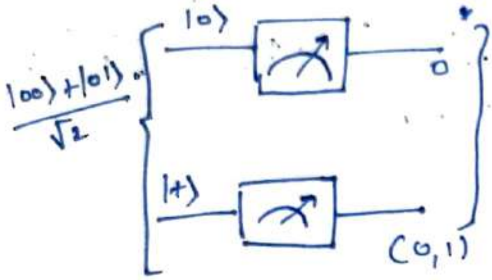
eg. $\frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle \longrightarrow$ possible outcomes $(0,0)$, $(1,1)$

Prob $\left(\frac{3}{4}\right)$ $\left(\frac{1}{4}\right)$

* Consider the state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |\psi\rangle_{AB}$

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

$$= |0\rangle_A \otimes |1\rangle_B \quad \text{Product state}$$



Possible outcomes
(0,0) (0,1)
No correlation b/w the measurement outcome)

(iv) Locality vs causality!

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

- " spooky action at distance"
- Nonlocality (Einstein's Hidden variable theory)

Polarization entangled photon:

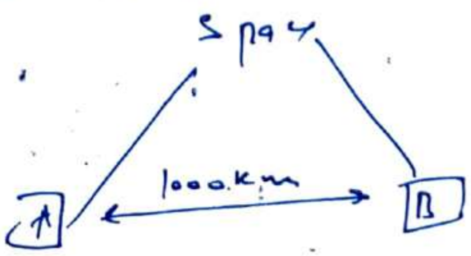
$$\frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$$

(Parametric down conversion)

Post measurement

$|H\rangle|H\rangle \qquad |V\rangle|V\rangle$

Quantum teleportation: (Application of entanglement)



~~Quantum telep~~

$|\psi\rangle|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ (B)

$\boxed{A}$ ——— $\boxed{B}$

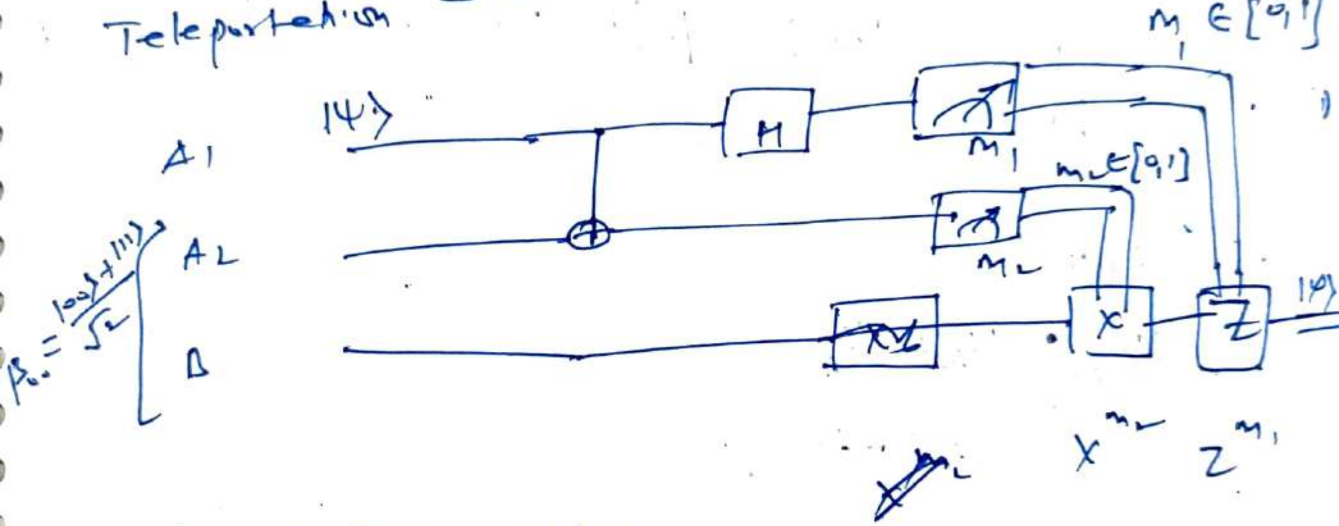
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ "Teleport the state of B

single qubit state

(unknown / arbitrary)

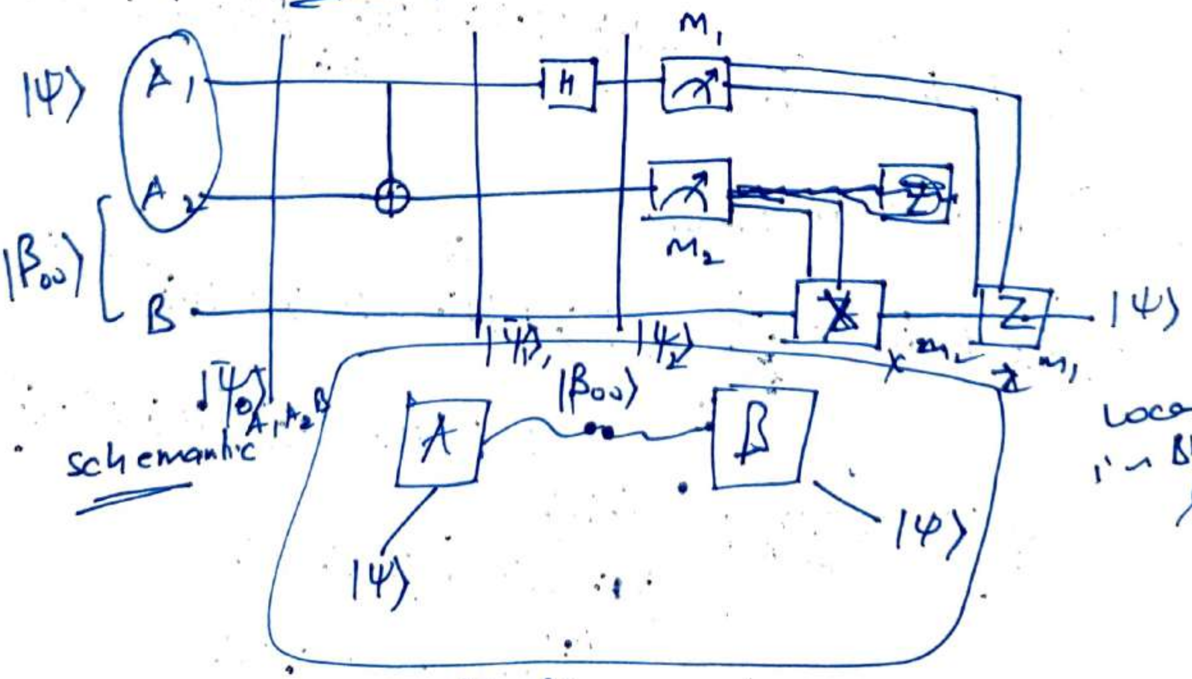
(Disappear form A's lab)

Teleportation Circuit



X^{m_2} Z^{m_1}

L-19 Teleportation



schematic

Local gates in Bhaskar lab.

$\Rightarrow$ classical communication m_1, m_2 are classical outcomes.

$$|\Psi_0\rangle_{A_1A_2B} = |\psi\rangle_{A_1} \otimes \underbrace{|\beta_{00}\rangle_{A_2B}}_{\text{Bell state}}$$

$\swarrow$ arbitrary single qubit state

$$= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)_{A_1A_2B}$$

$$\boxed{\begin{matrix} A_1A_2B \\ H_{A_1} \otimes \underbrace{H_{A_2} \otimes H_B}_{\text{Entangled}} \end{matrix}}$$

(i) After CNOT

$$|\Psi_1\rangle_{A_1A_2B} = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle_{A_1}(|00\rangle + |11\rangle)_{A_2B} + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

(ii) After CNOT & Hadamard

$$|\Psi_2\rangle_{A_1A_2B} = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle + |1\rangle_{A_1}(|00\rangle + |11\rangle)^{A_2B}$$
$$+ \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big]$$

$$= \frac{1}{2}\Big[\alpha|00\rangle_{A_2B}|0\rangle + \beta|00\rangle|1\rangle$$
$$+ \alpha|01\rangle_{A_2A_2}|1\rangle + \beta|01\rangle|0\rangle$$
$$+ \alpha|10\rangle_{A_1A_2}|0\rangle - \beta|10\rangle|1\rangle$$
$$+ \alpha|11\rangle_{A_1A_2}|1\rangle - \beta|11\rangle|0\rangle\Big]$$

$$= \frac{1}{2}\Big[|00\rangle_{A_1A_2} \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle_{A_1A_2} \otimes (\alpha|1\rangle + \beta|0\rangle)_B$$

$$+ (|10\rangle_{A_1A_2} \otimes (\alpha|0\rangle - \beta|1\rangle)_B + |11\rangle_{A_1A_2} \otimes (\alpha|1\rangle - \beta|0\rangle)\Big]_B$$

$\cancel{A_1 \otimes A_2 | B}$

$(A_1 A_2) | B$

(iii) ~~Th~~ final step:- Measurement of $\underbrace{A_1 \text{ and } A_2}_{\text{local measurement}}$ in the $\{|0\rangle, |1\rangle\}$ basis.

M_1 on A_1 given ~~atom~~ outcome m_1

M_2 on A_2 given outcome m_2

m_1	m_2	state of qubit B	
0	0	$\alpha\|0\rangle + \beta\|1\rangle$	Done!
0	1	$\alpha\|1\rangle + \beta\|0\rangle$	B has to do X gate
1	0	$\alpha\|0\rangle - \beta\|1\rangle$	Z gate has to apply
1	1	$\alpha\|1\rangle - \beta\|0\rangle$	Both bit and phase flip gates (X and Z)

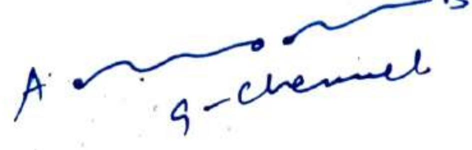
* Resource statement for teleportation protocol

1 e-bit $+ 2$ c-bits $= 1$ qubit

c-bits: classical bit

$|\beta_0\rangle$

1 entangled state



* No faster than light communication! But superimposing transfers instantaneous.

Protocol is incomplete without classical communication.

"speed" $\leq$ speed of classical communication!

History: Bennett, Brassard et al, Rev Lett (1993) vol 70, 1895 (PRL)

Expt (i) squeezed states of light (1998)

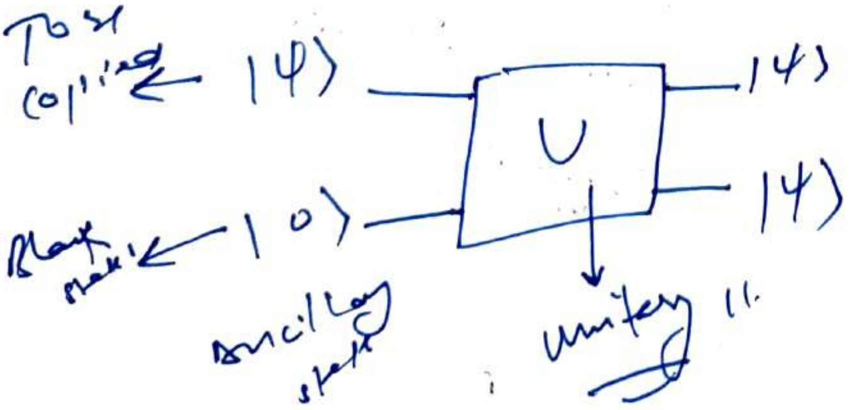
(ii) NMR (nuclear spin) 1998 Nielsen et al

(iii) Polarization entangled state (1997) Bouwmeester

No cloning theorem

* An arbitrary state $|\psi\rangle$ $(=\alpha|0\rangle+\beta|1\rangle)$ cannot be copied.

* There doesn't exist a universal quantum copying machine!



Idealized quantum copying machine

Either

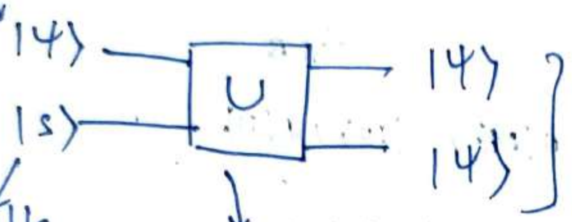
* $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1 \rightarrow$ only pairs of state that can be copied.

$|\psi\rangle = |\phi\rangle$

L20 No cloning theorem & Reduced Density operator

- No cloning theorem :- (Wootters & Zurek, Nature 1982)
- An arbitrary quantum state cannot be copied perfectly
- There does not exist a (Perfect) universal quantum copying machine

Data state



Ideal copying circuit

ancilla state (target state) Blank paper onto which the input is copied

Quantum copying circuit : unitary transformation

* suppose this copying machines for two data state $|\psi\rangle$ and $|\phi\rangle$

$$|\psi\rangle|s\rangle \xrightarrow{U} |\psi\rangle_A|\psi\rangle_B = 1$$

$$|\phi\rangle|s\rangle \xrightarrow{U} |\phi\rangle_A|\phi\rangle_B$$

Consider, $(\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle) = (\langle\psi|\phi\rangle)^2$

$$= \langle\psi|_{AB}\langle s|\underbrace{U^\dagger U}_{I}|\phi\rangle_A|s\rangle_B = (\langle\psi|\langle s|)(|\phi\rangle|s\rangle)$$

$$(|\psi\rangle_A|\psi\rangle_B = U_{AB}|\psi\rangle_A|s\rangle_B) \qquad = \langle\psi|\phi\rangle$$

$\Rightarrow \langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$ Constraint on the data state that copied by U

$\Rightarrow \langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$

$\Rightarrow$ $|\psi\rangle$ and $|\phi\rangle$ must be orthogonal state (or)

$$|\psi\rangle = |\phi\rangle$$

A set of orthogonal state $\rightarrow$ "classical" state $<$ distinguished perfectly / copied perfectly

Reduced Density operator :-

Bipartite quantum state S_{AB}

Pure bipartite state $|\psi\rangle_{AB} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$.

mixed bipartite state $S_{AB} = \underline{\sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB}}$

(2 qubit density operator) $\longrightarrow$ 4x4 matrix

eg: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$

$\left[|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$ —— $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$

$$S_{AB} = |\beta_{00}\rangle\langle\beta_{00}| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$ ~ Relative phase information

(2) S_{AB} = Equal mixture of two Bell states $|00\rangle$ & $|11\rangle$ $\left[= \frac{1}{2}|00\rangle\langle 00|, \frac{1}{2}|11\rangle\langle 11|\right]$

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

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\rho_A = |\psi\rangle\langle\psi|$$

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

$$\tilde{\rho}_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

(2) Equal mixture of two Bell states

$\sigma_{AB} = \frac{1}{2}|\beta_{00}\rangle\langle\beta_{00}| + \frac{1}{2}|\beta_{01}\rangle\langle\beta_{01}|$

$$\left[|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right]$$

$$= \left[\frac{1}{2}|\beta_{00}\rangle + \frac{1}{2}|\beta_{01}\rangle\right]$$

$[\,]\,[\,] = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} +$

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

$\begin{matrix}0\\1\\0\\0\end{matrix} + \begin{matrix}0\\0\\1\\0\end{matrix} = \begin{bmatrix}0\\1\\1\\0\end{bmatrix}$

$$\sigma_{AB} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} & 0 & \\ 0 & \times & 0 \\ & 0 & \end{pmatrix}$$

(X - matrices)

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

General Bipartite state.

$$\rho_{AB} : \in H_A \otimes H_B$$

Global description

- what is the Local description of this state?

A ~~~~ B

- Partial Trace Let $\{|i\rangle_A\}$ is ~~orthonormal~~ ON basis for H_A.

$\{|i\rangle_A \otimes |j\rangle_B\}$

$\{|j\rangle_B\}$ is an ON basis for H_B

Local state on A : $\rho_A = Tr_B(\rho_{AB})$

$$Tr(\rho_{AB}) = \sum_{i,j} \langle i|_A \langle j|_B \, \rho_{AB} |j\rangle_B |i\rangle_A$$

= Number

$$\boxed{\rho_A = \sum_j \langle j|_B \, \rho_{AB} \, |j\rangle_B}$$

→ Reduced density operator
marginal state

$\sum_j p_{ij} = p_i$ Marginal of a joint probability distribution

Local state on subsystem B $= \rho_B = Tr_A(\rho_{AB})$

$= \sum_i \langle i | \rho_{AB} | i \rangle$

- Example (i) Bipartite product state: $|\psi\rangle_A \otimes |\phi\rangle_B$

$\rho = |\psi\rangle_A \, {}_A\langle\psi|$.

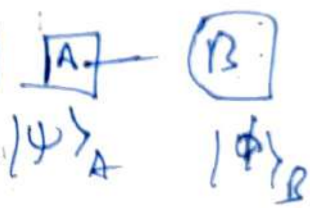
$(p_{ij} = p_i p_j)$

$\rho_A = |\psi\rangle_A \langle\psi|$ and

$\rho_B = |\phi\rangle\langle\phi|$

$$\rho_{AB} = (|\psi\rangle_A \otimes |\phi\rangle_B)(\langle\psi|_A \otimes \langle\phi|_B)$$

$$= |\psi\rangle_A\langle\psi| \otimes |\phi\rangle_B\langle\phi|$$



$p_{ij} = p_i p_j$

$$\boxed{\begin{aligned} &|00\rangle\langle 00| \\ &= |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B \end{aligned}}$$

$$\rho_A = Tr_B(\rho_{AB}) = Tr_B(|\psi\rangle\langle\psi|_A \otimes |\phi\rangle\langle\phi|_B)$$

$= 1!$

$$= |\psi\rangle\langle\psi|_A$$

||ly $\rho_B = Tr_A(\rho_{AB}) = |\phi\rangle\langle\phi|_B$

(ii) Bipartite product mixed state:

$\rho_{AB} = \rho_A \otimes \sigma_B$

Reduced state are simply ρ_A and σ_B!

(ii) Bipartite entangled state : $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Joint density operator $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|$
$+ |00\rangle\langle 11| + |11\rangle\langle 00|)$

$= |\beta_{00}\rangle\langle\beta_{00}|$.

Reduced density operators: $\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

$\rho_B = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

("Maximally mixed state")

Lec 21 Schmidt Decomposition

* Reduced Density operator

eg $|\psi\rangle_{AB} = |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$= \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$

Local state Partial trace $= \rho_A = Tr_B(\rho_{AB}) = Tr_B(|\psi\rangle_{AB}\langle\psi|_{AB})$

Bipart state is pure (entangled state)

$= Tr_B\left(\frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| + \frac{1}{2}|00\rangle\langle 11| + \frac{1}{2}|11\rangle\langle 00|\right)$

$= Tr_B$

$\frac{1}{2}Tr_B[|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B$
$+ |0\rangle\langle 1|_A \otimes |0\rangle\langle 1|_B + |1\rangle\langle 0|_A \otimes |1\rangle\langle 0|_B$

$\boxed{Tr(|0\rangle\langle 1|) = 0}$

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

(maximally mixed state)!

show: $\rho = Tr_A(|\psi\rangle_{AB}\langle\psi|_{AB}) = \frac{I}{2}$

* Bipartite state is pure (external state)] signature of an Entangled state
Reduced states are the most mixed!

"whole has more information than the parts"

* **Entropy**: for any ρ, we can define $H(\{\lambda_i\})$ → shannon entropy of its eigen values

$\rho = \sum_i \lambda_i |i\rangle\langle i|$ (diagonalized)

$\left(\sum_i \lambda_i = 1 \text{ and } 0 \leq \lambda_i \leq 1\right)$

$\{\lambda_i\}$ form a probability distribution!

$H(\{\lambda_i\}) = -\sum_i \lambda_i \log_2 \lambda_i$ → quantifies the spread of the eigen values of density matrix (spectrum)

shannon Entropy

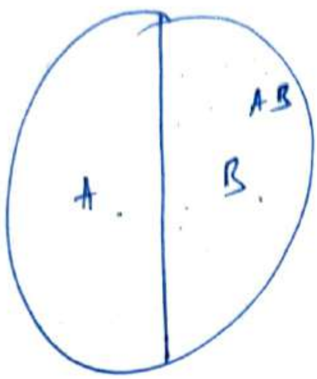
* eg. Bell epr states!

$|\psi\rangle_{AB} \longleftrightarrow \rho_{AB} = |\psi\rangle_{AB}\langle\psi|_{AB}$

$H(\rho_{AB}) = \underline{0}$! (delta distribution)

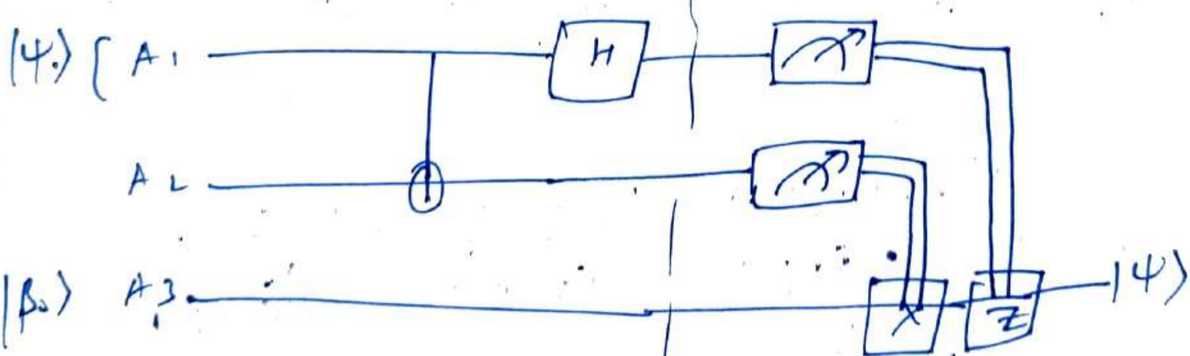
Reduced state $\rho_A = \rho_B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

$H(\rho_A) = \log_2 2 = 1$ Maximum shannon entropy possible for a qubit state!



$\Rightarrow$ Maximally uncertain about reduced state, fully certain about ~~state~~ about joint state
Global vs local description

* Teleportation protocol:-



$$|\Psi\rangle_{A_1A_2B} = \frac{1}{2}\Big[|00\rangle_{A_1A_2}\otimes\overbrace{(\alpha|0\rangle+\beta|1\rangle)}^{|\phi_1\rangle}_B + |01\rangle\otimes\overbrace{(\alpha|1\rangle+\beta|0\rangle)}^{|\phi_2\rangle} + |10\rangle\otimes\underbrace{(\alpha|0\rangle-\beta|1\rangle)}_{|\phi_3\rangle} + |11\rangle\otimes\underbrace{(\alpha|1\rangle-\beta|0\rangle)}_{|\phi_4\rangle}\Big]$$

$|\Psi_{A_1A_2B}\rangle$

Final tripartite state

Tracing out Anita's qubit, local state of B

$$\rho_B = Tr_{A_1 A_2}(\rho_{A_1 A_2 B})$$

$$= Tr_{A_1 A_2}(|\psi\rangle_{A_1 A_2 B} \langle \psi|_{A_1 A_2 B})$$

$$= Tr_{A_1 A_2}(|00\rangle\langle 00|_{A_1 A_2} \otimes |\phi_1\rangle\langle\phi_1|_B + |01\rangle\langle 01|_{A_1 A_2} \otimes |\phi_2\rangle\langle\phi_2| + |10\rangle\langle 10|_{A_1 A_2} \otimes |\phi_3\rangle\langle\phi_3| + |11\rangle\langle 11| \otimes |\phi_4\rangle\langle\phi_4| + \dots |00\rangle\langle 01| \otimes |\rangle\langle| \quad |01\rangle\langle 10| \otimes |\rangle\langle| \dots)$$

$$\boxed{\begin{gathered} Tr(|00\rangle\langle 01|) = 0 = Tr(|00\rangle\langle 11|) \\ Tr(|01\rangle\langle 10|) = 0 = Tr(|11\rangle\langle 01|) \end{gathered}}$$

$$\rho_B = \frac{1}{4}\Big(\underbrace{|\phi_1\rangle}_{\alpha|0\rangle + \beta|1\rangle}\langle\phi_1| + \underbrace{|\phi_2\rangle}_{(\alpha|1\rangle + \beta|0\rangle)}\langle\phi_2| + \underbrace{|\phi_3\rangle}_{(\alpha|0\rangle - \beta|1\rangle)}\langle\phi_3| + \underbrace{|\phi_4\rangle}_{(\alpha|1\rangle - \beta|0\rangle)}\langle\phi_4|$$

$$= \frac{1}{\cancel{4}_2}\,\cancel{2}\big(|\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1| \\ \cancel{+ \alpha\beta^* |0\rangle\langle 1| + \alpha^*\beta |1\rangle\langle 0|}\big)$$

$$\frac{1}{2}\left[\underbrace{(|\alpha|^2+|\beta|^2)}_{\substack{\shortparallel \\ 1}}|0\rangle\langle 0| + \underbrace{(|\alpha|^2+|\beta|^2)}_{\substack{\shortparallel \\ 1}}|1\rangle\langle 1|\right]$$

$$= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{I}{2} \quad \text{maximally mixed state!}$$

no dependence on α or β!

Unless classically bits m_1, m_2 are communicated, B has essentially has no information about $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$!

Quantify entanglement : Bipartite pure state

which of these states is more entangled?

$$|\Psi_1\rangle = \frac{|00\rangle + |01\rangle + |11\rangle}{\sqrt{3}} \quad (2)$$

$$|\Psi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (1) \text{ most entangled!}$$

$$|\Psi_3\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \quad (3)$$

$|\Psi_3\rangle$ is unentangled!! $\Longrightarrow$ $= |+\rangle_A \otimes |+\rangle_B$

$Ent(|\psi_3\rangle) = 0$!

* Basis in which the state is entangled → schmidt decomposition

Schmidt decomposition

Thm Given a pure state $|\psi\rangle_{AB} = H_A \otimes H_B$,

there exist ON states $\{|e_i\rangle_A\}_{i=1}^{K} \in H_A$ and local

$$\{|f_j\rangle_B\}_{j=1}^{K} \in H_B$$

such that, $|\psi\rangle_{AB} = \sum_{i=1}^{K} \lambda_i |e_i\rangle_A |f_i\rangle_B$

$\{\lambda_i\}$ are real, non-negative numbers

satisfying $\sum_i \lambda_i^2 = 1$

$\{\lambda_i\}$ are called schmidt coefficients.

$\{|e_i\rangle_A$ and $\{|f_j\rangle_B$ are called

(local Bases) schmidt Bases.

std. description: ~~the~~ $\{|i\rangle_A\} \in H_A$

$, \{|j\rangle_B\} \in H_B$

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A |j\rangle_B.$$

L-22 Schmidt Decomposition :-

Theorem :

$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ $\{|e_i\rangle_A\} \in \mathcal{H}_A$

↓

Bipartite state $[|f_i\rangle_B] \in \mathcal{H}_B$

$$|\psi_{AB}\rangle = \sum_{i=1}^{R} \lambda_i |e_i\rangle_A |f_i\rangle_B$$

where λ_i are non negative real numbers.

$\sum_i \lambda^2 = 1$ [satisfy]

Let $\mathcal{H}_A \leftrightarrow [|i\rangle_A]$

$\mathcal{H}_B \leftrightarrow [|R\rangle_B]$

$$|\psi_{AB}\rangle = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} C_{jk} |J\rangle_A |R_A\rangle$$

Eigen composition of a matrix

$A \rightarrow$ square matrix size $n \times n$

$q_i \rightarrow$ independent eigenvector

~~$A = Q A Q$~~ $A = Q \Lambda Q^{-1}$ → diagonal matrix ↓ eigenvalue

↓ $n \times n$ matrix diagonali-zation

writing eigen vector column

Only for a square matrix

what happens if it is not a square matrix

Different method → Singular value

Singular values decomposition of a matrix (SVD)

- if we have $m \times n$ matrix we can factorize using a SVD

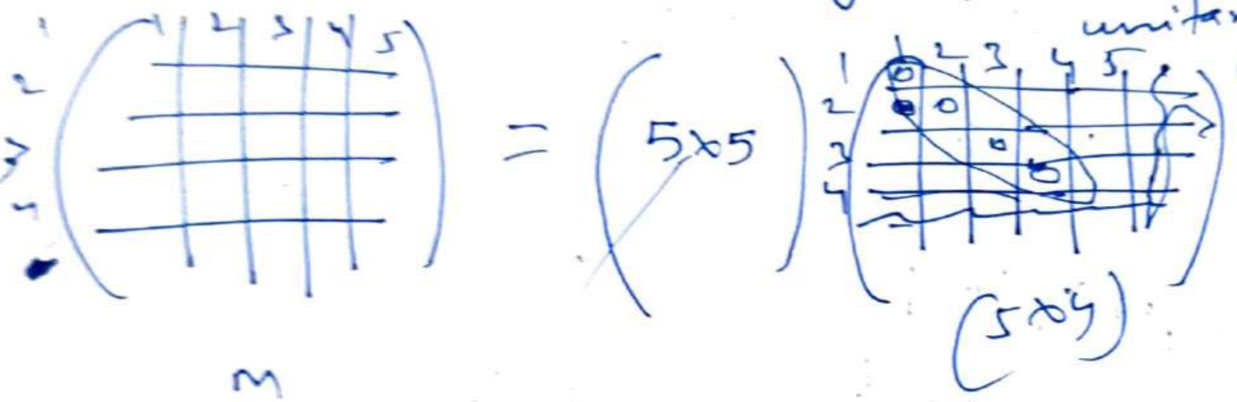
- $M = U \Sigma V$

$M \to$ is a complex $m \times n$ matrix

$U \to$ is a $m \times m$ unitary

$\Sigma \to$ is a $m \times n$ rectangular diagonal matrix

$V \to$ is a $n \times n$ complex unitary



M

$\Sigma = \Sigma_{ii} \to$ diagonal entries singular values of the matrix M

M → Rank of the matrix is the number of the non zero ~~sin~~ singular

SVD ≠ unique

5 4 3 2 1 0 0

Proof

$C \to m \times n$ complex matrix

$C = UDV$

$U = m \times m$ unitary

$V = n \times n$ unitary

$D = m \times n$ rectangular diagonal matrix

$r \leq \min(m,n)$

rank of the matrix — no of nonzero entries on the diagonal

Let us consider $M = \sqrt{C^{+}C}$ $\qquad C^{+}C_{m\times n}$

$n\times n$ square matrix constructed from the C— matrix $\qquad \dfrac{n\times m}{n\times n}$

Let us consider V $(n\times n)$

$$V^{+} M V = V^{+}\sqrt{C^{+}C}\, V = D_{n\times n}$$

Let D have 'r' non zero entries

$$V = \underbrace{\left(\quad\right)}_{r}{}_{n\times n} \qquad V_1 = (\quad)_{n\times r} \qquad V_2 = (\quad)_{n\times(n-r)}$$

$V = (V_1, V_2)$, V_1: $n\times r$, V_2: $n\times(n-r)$. $\qquad C = (C_1, C_2)$, C_1: $n\times r$, C_2: $n\times(n-r)$

$$V_1\sqrt{C_1^{+}C_1}\, V_1 = D_1 \qquad V_2^{+}\sqrt{C_2^{+}C_2}\, V_2 = 0$$

$C = U D V$

$U_1 = C V_1 D_1^{-1}$ $(m\times r)$ matrix

$$U_1^{+}U_1 = D_1^{-1} V_1^{+} C^{+}C\, V_1 D_1^{-1}$$

$$= D_1^{-1} V_1^{+}\sqrt{C^{+}C}\sqrt{C^{+}C}\, V_1 D_1^{-1}$$

$$= D_{+1}^{-1} V_1^{+}\sqrt{C^{+}C}\, V_1 V_1^{+}\sqrt{C^{+}C}\, V_1 D_1^{-1}$$

$$= D_{+1}^{-1} D_1 D_1 D_1^{-1} = \mathbb{1}$$

$U_1 \rightarrow m \times r \qquad m \times m$

$U = (U_1, U_2)$

$UDV^\dagger = (U_1, U_2)\begin{pmatrix} D_1 & \\ & 0 \end{pmatrix}\begin{pmatrix} V_1^\dagger \\ V_2^\dagger \end{pmatrix}$

$= U_1 D_1 V_1^\dagger$

$= C$

$C = U\underset{\text{singular value entries}}{D}V^\dagger$

$V \rightarrow$ columns of the matrix V, are the Right singular vector of $C^\dagger C$

$U \rightarrow$ columns of the matrix U are the left singular vector of $CC^\dagger$

$C^\dagger C = VDU^\dagger UDV^\dagger = VD^2V^\dagger$

$CC^\dagger = UDV^\dagger VDU = UD^2U^\dagger$

$|\psi_{AB}\rangle = \sum_{ik} C_{ik} |i\rangle_A |k\rangle_B$

Using SVD $\qquad d_{pq} = \delta_{pq} d_{pp}$

$C_{ik} = \sum_{p=1}^{d_A} \sum_{q=1}^{d_B} d_{pq} v_{qk}$. for $0 < p, q \leq r$

0 otherwise

$|\psi_A \psi_B\rangle = \sum_{pq} \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} U_{jp} d_{pv} v_{qk} |j\rangle_A |k_B\rangle$

$$= \sum_{l,q}^{d_A, d_B} \alpha_{pq} \left[\left(\sum_{j=1}^{d_A} U_{jp} |j\rangle_A \right) \left(\sum_{k=1}^{d_B} v_{qk} |k\rangle_B \right) \right]$$

$$\therefore \quad = |e_p\rangle_A = \left(\sum_{j=1}^{d_A} U_{jp} |j\rangle_A \right)$$

$$= |f_q\rangle_B = \left(\sum_{j=1}^{d_B} v_{qk} |k\rangle_B \right)$$

$|e\rangle$ and $|f\rangle$

$$\langle e_l | e_j \rangle = \delta_{jl}$$

$$\langle f_l | f_j \rangle = \delta_{jl}$$

$$\therefore |\psi_{AB}\rangle = \sum_{pq} \alpha_{pq} |e_p\rangle_A |f_q\rangle_B$$

$$= \sum_{p=1}^{r} \alpha_{pp} |e_p\rangle_A |f_q\rangle_B$$

$$|\psi_{AB}\rangle = \sum_{i=1}^{k} \lambda_i |e_i\rangle_A |f_i\rangle_B$$

schmidt coefficient

Application of schmidt decomposition

$|\psi_{AB}\rangle \longrightarrow$ schmidt basis

calculate the reduced density matrix

$$\rho_A = \sum_i \lambda_i^2 |i\rangle\langle i|$$

$$\rho_B = \sum_j \lambda_j^2 |i\rangle\langle i|$$

schmidt number / schmidt rank.

$|\psi_{AB}\rangle =$

non zero schmidt coefficients $\downarrow$ schmidt Rank

$1 \leq r \leq \min(d_A, d_B)$

d_A d_B

Ⓐ   Ⓑ

H_A H_B

$1 \leq r \leq 2$

If the schmidt rank is $1 \longrightarrow$ System is not entangled

$d_A = 2$ 2

$d_B = 2$ 3

but if the schmidt rank is $> 1 \longrightarrow$ System is entangled.

$|\psi_{AB}\rangle = |e_i\rangle_A \otimes |f_i\rangle_B \longrightarrow$ Product state

Entanglement entropy

$$|\psi_{AB}\rangle = \sum_i \lambda_i |i\rangle_A |i\rangle_B$$

$$\rho_A = \sum_i \lambda_i^2 |i\rangle_A\langle i|$$

$$\rho_B = \sum_i \lambda_i^2 |i\rangle_B\langle i|$$

$$H(\{\lambda_i^2\}) = -\sum_i \lambda_i \log \lambda_i^2$$

$$0 \leq H(\rho_A) \leq \log_2 r$$

$H(\rho_A) = 0$ (state is not entangled)

$H(\rho_A) = -\frac{1}{2}\log_2 \frac{1}{2}$ $d_a = 2$

$\frac{1}{2}, \frac{1}{2}$

$H(\rho_A) = -\frac{1}{2} \cdot \log_2 \frac{1}{2}$

$= -\frac{1}{2} \log_2 \frac{1}{2}$

$= \log_2 2 \qquad d_n = d \qquad \frac{1}{d}$

$\frac{1}{d} \log_2 \frac{1}{d} + \cdots + \frac{1}{d} \log_2 \frac{1}{d}$

$= -\frac{\cancel{d}}{\cancel{d}} \left[\log_2 \frac{1}{d} \right] = \log_2 d$

$H(\rho_A) = H(\rho_B) = \log_2 d$

L-23 Schmidt Decomposition and Purification

Recall schmidt decomposition

Given a bipartite pure state, then

$\mathcal{H}_A \otimes \mathcal{H}_B$

exist on states $\{|e_i\rangle_A\}$

and $\{|f_i\rangle_B\}$ such that

$|\psi\rangle_{AB} = \sum_i \lambda_i |e_i\rangle_A |f_i\rangle_B \longrightarrow$ Schmidt form

$\{\lambda_i\} \rightarrow$ schmidt coefficient

$\sum \lambda_i^2 = 1$

schmidt rank = # of nonzero schmidt coefficients

- If schmidt rank = 1, state is unentangled

  " " " > 1 state is entangled

schmidt rank $\leq \min(d_A, d_B)$

- Quantify entangled (Ent. Measure) $= H(\{\lambda_i^2\})$

$$= -\sum_i \lambda_i^2 \log \lambda_i^2$$

subsystem entropy

- $\{\lambda_i\}$ are eigenvalues of reduced density matrices ρ_A and ρ_B

(Measure of How mixed the reduced rate state is)

* Purification:

$$|\psi\rangle_{AB} \rightarrow \rho_A, \quad |\psi\rangle_{AB} \rightarrow \rho_B$$

$|\psi\rangle_A \in H_A$ Consider idea!

$\rho_A \in H_A$ ρ_A on system H_A.

* One can always associate a pure state in a larger space with the mixed state.

(Choi-Jamiołkowski isomorphism) Every ρ_A on H_A can be associated with a $|\psi\rangle_{AB}$ on a larger space $H_A \otimes H_B$.

(Isomorphism)

$H_A \otimes H_B$ ← appended or add another system B of appropriate dimension, such that

$$\exists\, |\psi\rangle_{AB} \in H_A \otimes H_B$$

$$\mathrm{Tr}_B\left(|\psi\rangle_{AB}\langle\psi|_{AB}\right) = \rho_A \quad \text{(wired marginal state!)}$$

$$* \ \rho_A = \sum_{i=1}^{d} \lambda_i |i\rangle\langle i|_A \rightarrow \text{spectral decomposition eigenvalue}$$

need H_B to be d-dimensional.

Let $\{|j\rangle_B\}$ is an ON basis for H_B

"Purified" state $|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\, |i\rangle_A \otimes |i\rangle_B$

eg $\mathbb{C}^2$: $\rho_A = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$

$\mathbb{C}^2 \otimes \mathbb{C}^2$: $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$

Alternative
$|\tilde{\psi}\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|+\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$??

$\downarrow$

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

Also a valid purification of the same density matrix

$\Rightarrow$ Purification of a given ρ_A to $|\psi\rangle_{AB}$ is not unique

the two purification $|\psi\rangle_{AB}$ and $|\tilde{\psi}\rangle_{AB}$ are related by a local quantum gate / local unitary

eg: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xleftrightarrow{I_A \otimes H_B} \underline{\frac{1}{\sqrt{2}}\left(|0\rangle|+\rangle + |1\rangle|-\rangle\right)}$

Hadamard

$\downarrow$

maximally entangled state

Schmidt bases are

$[|0\rangle\, |1\rangle]$ and $[|+\rangle\, |-\rangle]$

H_A $\qquad$ H_B

measurement outcomes are now correlated b/w $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$

Note: $|\tilde{\psi}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle|+\rangle + |1\rangle|-\rangle\right)$

$= \frac{1}{2}\underbrace{\left(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\right)}_{\text{all possible states}}$

$\Rightarrow$ No correlation in the $\{|0\rangle\, |1\rangle\}$ bases

(All 4 outcomes are possible!)

* Is the Schmidt decomposition unique??

unique upto local unitary gates

local quantum gates cannot change the entanglement content of a bipartite state

Schmidt bases can be changed

$\{\lambda_i^2\}$ Schmidt coeffs are invariant!

Schmidt rank, ~~entropy~~ entanglement entropy do not change

Bell - CHSH test

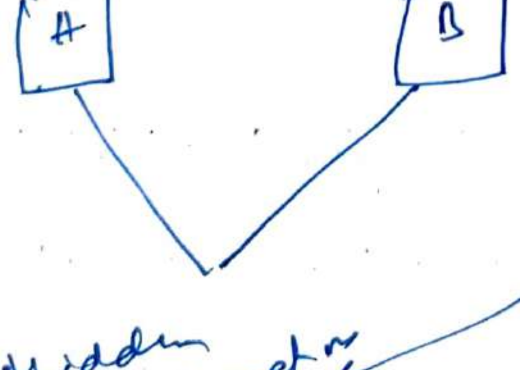
Recall, Bell states: $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ → anticorrelated state

"Beyond classical correlations" $\{|0\rangle, |1\rangle\}$ measurement

[EPR note down these states to justify that q. mech. is <u>incomplete</u>.

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B\right)$$ perfectly anticorrelated =!

in the $\{|+\rangle, |-\rangle\}$ basis



<u>Causally separated</u>

correlation suggests that these outcomes must be predetermined

— violation with q. theory

Hidden information

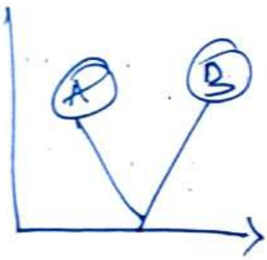
John S. Bell (1964) → quantitative test for quantum theory:

- classical intuition: → values taken by physical properties are inherent to the system

"Realism" measurement merely reveals those value

"objective reality"

→ Locality : Measurement in "A" labs is independent of a measurement B's labs, provided they are causally separated



Classical correlation.

4 physical quantities P, Q, R, S

A	B
$P \in [\pm 1]$	$R \in [\pm 1]$
$Q \in [\pm 1]$	$S \in [\pm 1]$

→ value $[\pm 1]$

P Q R S are binary valued observables

joint probability distribution $Pr(p, q, r, s)$ over the outcomes p, q, r, s of the observables P, Q, R, S

L - 24

An experimental test of q. mechanism

* Consider a general physical theory

$$
\begin{array}{lcl}
P \in [\pm 1] & & R \in [\pm 1] \\
 & \boxed{A} \xleftrightarrow[\text{a joint state}]{\text{share}} \boxed{B} & \\
Q \in [\pm 1] & & S \in [\pm 1]
\end{array}
$$

* binary valued physical observable P, Q, R and S
* Assumption (any "reasonable" physical theory should satisfy")

(i) Realism : P, Q, R, and S are objective properties of the systems.
Act of measurement merely "revels" their value

(ii) Locality : A & B are causally disconnected.
- It is possible to assign joint values to P, Q, R, and S simultaneously (A and B perform their measurement at the same time).

Consider an observable $M = PR + QR - PS + QS$
$$= (P+Q)R + (Q-P)S.$$

~~Since P and Q are binary values~~

Since $P, Q, R, S \in [\pm 1]$, $M \in [\pm 2]$

* Let $P_r(p, q, r, s)$ be a joint probability distribution over the outcome p, q, r, s.

* Let p denote the outcome of measuring observable P

q " " " " " " Q

r " " " " " " R

s " " " " " " S

Expectation value $$\mathbb{E}(M) = \sum_{p,q,r,s \in \{\pm 1\}} Pr(p,q,r,s)\,[pr + qr - ps + qs]$$

$$\leq 2$$

$$\boxed{\mathbb{E}(M) = \mathbb{E}(PR) + \mathbb{E}(QR) - \mathbb{E}(PS) + \mathbb{E}(QS) \leq 2}$$

<u>Bell-CHSH inequality</u>

* Quantum theory allows for states and observable that can violate this inequality!

Let the joint state be $|\Psi\rangle_{AB} = |\beta_{11}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

$$\boxed{A} \xleftrightarrow[|\beta_{11}\rangle]{} \boxed{B}$$

$P = \sigma_Z$ $\qquad R = \frac{-\sigma_Z - \sigma_x}{\sqrt{2}}$

$Q = \sigma_x$ $\qquad S = \frac{\sigma_Z - \sigma_x}{\sqrt{2}}$

$\boxed{PR = (P_A \otimes I_B)(I_A \otimes R_B)}$ $\boxed{P_A \otimes P_B}$

$[P, Q] \neq 0$ $\qquad ([R, S] \neq 0!)$

$$\mathbb{E}(M) = \mathbb{E}(PR) + \mathbb{E}(QR) - \mathbb{E}(PS) + \mathbb{E}(QS)$$

$$= \langle \beta_{11} | \sigma_Z \otimes -\frac{(\sigma_Z + \sigma_x)}{\sqrt{2}} | \beta_{11} \rangle$$

$$+ \langle \beta_{11} | \sigma_x \otimes -\frac{(\sigma_Z + \sigma_x)}{\sqrt{2}} | \beta_{11} \rangle$$

$$- \langle \beta_{11} | \sigma_z \otimes \left(\frac{\sigma_z - \sigma_x}{\sqrt{2}} \right) | \beta_{11} \rangle$$

$$+ \langle \beta_{11} | \sigma_x \otimes \left(\frac{\sigma_z - \sigma_x}{\sqrt{2}} \right) | \beta_{11} \rangle$$

<u>first term</u> $\langle \beta_{11} | \frac{\sigma_z \otimes \sigma_z}{\sqrt{2}} | \beta_{11} \rangle - \frac{\langle \beta_{11} | \sigma_z \otimes \sigma_x | \beta_{11} \rangle}{\sqrt{2}}$

$$= -\frac{1}{\sqrt{2}} \left(\frac{\langle 01| - \langle 10|}{\sqrt{2}} \right) \left(\frac{-|01\rangle + |10\rangle}{\sqrt{2}} \right)$$

$$- \frac{1}{\sqrt{2}} \left(\frac{\langle 01| - \langle 10|}{\sqrt{2}} \right) \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)$$

$$= -\frac{1}{2\sqrt{2}} (-1-1) = \frac{1}{\sqrt{2}}$$

In fact every term evaluate to $\frac{1}{\sqrt{2}}$!

check

$$\langle \beta_{11} | \sigma_x \otimes - \frac{(\sigma_z + \sigma_x)}{\sqrt{2}} | \beta_{11} \rangle = \frac{1}{\sqrt{2}}$$

$$\langle \beta_{11} | \sigma_z \otimes \left(\frac{\sigma_z - \sigma_x}{\sqrt{2}} \right) | \beta_{11} \rangle = \frac{1}{\sqrt{2}}$$

$$\langle \beta_{11} | \sigma_x \otimes \left(\frac{\sigma_z - \sigma_x}{\sqrt{2}} \right) | \beta_{11} \rangle = \frac{1}{\sqrt{2}}$$

$$\therefore \mathbb{E}(M) = \mathbb{E}(P_A \otimes P_B) + \mathbb{E}(Q_A \otimes R_B)$$

$$- \mathbb{E}(P_A \otimes S_B) + \mathbb{E}(Q_A \otimes S_B)$$

$$= \frac{4}{\sqrt{2}} = 2\sqrt{2}$$

A theory allows for states (entangled) and observable (non-commuting) such that

$$\mathbb{E}(M) = 2\sqrt{2}$$

violating the Bell-CHSH inequality ($\mathbb{E}(M) \leq 2$)!

- CHSH Clauser, Holt, Shimony, and Horn (1969)
- Example of a larger class of Bell inequality
  John S. Bell (1964)
- Test for entanglement. (verify entanglement)
- Entaglement measurement!
  - Product state will not violate the Bell CSHS bound!
- $\mathbb{E}(M) \leq 2\sqrt{2} \longrightarrow$ Maximal possible violation of qubits
- Bell states achieve maximum violation in quantum case
- Other entangled state will have

$$\underline{2 \leq \mathbb{E}(M) \leq 2\sqrt{2}}$$

quantify the extents of non-locality

L-25

Chp 4 of Neilson ~~and Chuang~~)

Quantum Gates and circuit I

* Quantum circuit Model [IBM / Google / Honeywell]

Equivalent
- Adiabatic Quantum computing (Quantum Annealing) — D-wave
- Hamiltonian computing

Universal computation models.

* Circuit model / Gate-based model

NISQ — circuits

[Noisy Intermediate-scale Quantum circuits)

50-100 qubits

* Quantum gates are unitary matrices.

Qubit $\in \mathbb{C}^2$

single qubit gate: Pure state is $\mathbb{C}^2 \rightarrow$ pure state in $\mathbb{C}^2$

$|\psi\rangle = a|0\rangle + b|1\rangle$; $|a|^2 + |b|^2 = 1$

[2×2 unitary matrices] → forms a group under multiplication

(norm-preserving operation)

$UU^{+} = U^{+}V = I_{2\times 2}$

?

$SU(2)$

special unitary group

Determinant of $U = 1$

B.T.S

BTS

- Product of two unitary matrices. $UV = W$ is also unitary ($\rightarrow$ check)

* Useful fact about unitary
  - Diagonalizable! $[U, U^\dagger] = 0$
  - Eigenvalues of U: $U = \sum_i \lambda_i |i\rangle\langle i|$

$$\left.\begin{array}{l} U^\dagger U = UU^\dagger = I \\ U^\dagger = \sum_i \lambda_i^* |i\rangle\langle i| \end{array}\right] \rightarrow |\lambda_i| = 1$$

$\downarrow$ unitary unit modulus

$\lambda_i = e^{i\phi_i}$ (pure phase!) $\forall i$

- Determinant = Product of eigenvalues.

  $|\text{Determinant}| = 1$

* Gates on n-qubit : $2^n \times 2^n$ unitary matrix without loss of generality $U \in SU(2^n)$

$\downarrow$ (dimensions)

* Universal set of quantum gates!

(1) Basic set of single-qubit gates!

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

"Phase gate" $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$$—\boxed{S}—$$

(Adds a phase of $\frac{\pi}{2}$ to $|1\rangle$)

$$|0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \longrightarrow i|1\rangle$$

$$\left(\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + i\beta|1\rangle\right)$$

eg $|+\rangle \longrightarrow |+_i\rangle$

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

(eigenstate of Y)

" $\frac{\pi}{8}$ " gates T $(G_{\pi/8})$ $= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

(Add a phase of $\frac{\pi}{4}$ to $|1\rangle$)

$$= e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

(2) Rotation Gates

* Universal set of Quantum gates

G of "elementary" gates in terms of which all quantum gates operations can be decomposed ||

(1) Rotation Gates :- Rotations about the x, y, z axes on the Bloch sphere

$R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$

$$R_x(\theta) = e^{-i\frac{\theta X}{2}} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)X$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)Y$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)Z$$

$$X = R_x(\pi), \quad Y = i R_y(\pi), \quad Z = i R_z(\pi)$$

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

Note $H = \frac{X + Z}{\sqrt{2}}$; $T = R_z\left(\frac{\pi}{4}\right)$

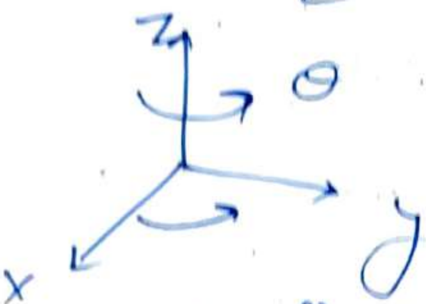
$S = T^2$

* Show that $R_z(\theta)$ rotates an arbitrary state by an angle θ about Z-axis.

$$R_z(\theta)|\psi\rangle = \left(\cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z\right)\left(\cos\frac{\alpha}{2}|0\rangle + e^{i\phi}\sin\frac{\alpha}{2}|1\rangle\right)$$

$$\rightarrow \cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\alpha}{2}\right)|1\rangle$$

$$= e^{-i\theta/2}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{i(\phi+\theta)}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right]$$



||ly, one can show that $R_x(\theta)$ and $R_y(\theta)$ rotate an arbitrary state by θ about x and y axis ~~resp~~ respectively.

L-26

* Single-qubit gates are 2×2 unitary matrices $\in U(2) \cong SU(2)$

group under multiplication

spl. unitary group with $\det U = 1$

$|\det(U)| = 1$

* without loss of generality, single qubit
$U \in SU(2)$

eg $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\det Z = -1 \in U(2)$

$iZ = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ $\det(iZ) = +1 \in SU(2)$

$\alpha|0\rangle + \beta|1\rangle$ — $\boxed{iZ}$ — $i(\alpha|0\rangle - \beta|1\rangle)$

overall phase!

$\alpha|0\rangle + \beta|0\rangle$ — $\boxed{Z}$ — $\alpha|0\rangle - \beta|1\rangle$

Rotation gates (single-qubit)

$R_x|\theta\rangle = e^{-i\frac{\theta}{2}X}$, $R_y|\theta\rangle = e^{-i\frac{\theta}{2}Y}$

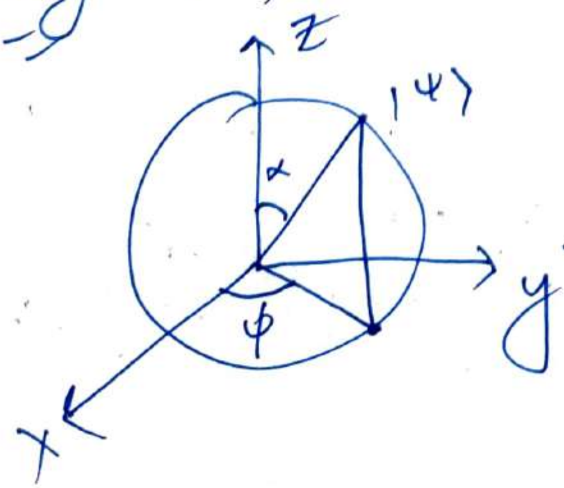
$R_z|\theta\rangle = e^{-i\frac{\theta}{2}Z}$

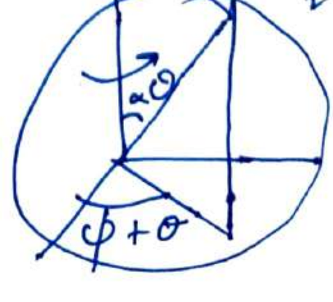
The gate correspond to a rotation by θ, about $X, Y,$ and Z axes in the Bloch sphere

representation

eg $|\psi\rangle = \cos\frac{\alpha}{2}|0\rangle + e^{i\phi}\sin\frac{\alpha}{2}|1\rangle$

$\cos\frac{\alpha}{2}|0\rangle + e^{i(\theta+\phi)}\sin\frac{\alpha}{2}|1\rangle$





* Decomposing single qubit gates as sequen-ces (products) of rotation gates.

Thm: Z-y decomposition of a single-qubit gates

Given $U \in SU(2)$, there exist $\alpha, \beta, \gamma, \delta$ (all reals)

such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$

third. second first

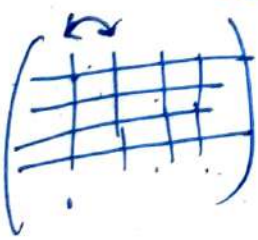
$-\boxed{U}- \; = \; -\boxed{e^{i\alpha} R_z(\delta)}-\boxed{R_y(\gamma)}-\boxed{R_z(\beta)}-$

Proof: ~~In the~~ ~~$\{|0\rangle, |1\rangle\}$ basis,~~

Rows and columns of a unitary are orthonormal.

$$U^{+}U = I = \sum_j (U^{+})_{ij} U_{jk} = \delta_{ik}$$

$$\Rightarrow \sum_j U^{*}_{ji} U_{jk} = \delta_{ik}$$



$$U = \left(\begin{pmatrix} U_1 \\ \\ \end{pmatrix} \begin{pmatrix} U_1^{\perp} \\ \\ \end{pmatrix} \right)$$

In $\{|0\rangle, |1\rangle\}$ basis

$$|U_1\rangle = e^{-i(\lambda_1+\lambda_2)} \cos\frac{\gamma}{2}|0\rangle + e^{i(\lambda_1-\lambda_2)} \sin\frac{\gamma}{2}|1\rangle$$

$$|u_1^{\perp}\rangle = -e^{-i(\lambda_1-\lambda_2)} \sin\frac{\gamma}{2}|0\rangle + e^{i(\lambda_1+\lambda_2)} \cos\frac{\gamma}{2}|1\rangle$$

Check $\left.\begin{array}{l} \langle u_1^{\perp}|u_1\rangle = 0 = \langle u_1|u_1^{\perp}\rangle \\ \langle u_1|u_1\rangle = 1 = \langle u_1^{\perp}|u_1^{\perp}\rangle \end{array}\right]$ orthonormal ~~bases~~ vector

$$U = \begin{pmatrix} e^{-i(\lambda_1+\lambda_2)}\cos\frac{\gamma}{2} & e^{i(\lambda_1-\lambda_2)}\sin\frac{\gamma}{2} \\ e^{i(\lambda_1-\lambda_2)}\sin\frac{\gamma}{2} & e^{i(\lambda_1+\lambda_2)}\cos\frac{\gamma}{2} \end{pmatrix}$$

Recall $R_y(\gamma) = e^{-\frac{i\gamma}{2}Y} = \cos\left(\frac{\gamma}{2}\right)I - i\sin\left(\frac{\gamma}{2}\right)Y$

$$\begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}$$

$$R_z(\delta) = \cos\left(\frac{\delta}{2}\right)I - i\left(\sin\frac{\delta}{2}\right)Z$$

$$= \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{-i\delta/2} \end{pmatrix}$$

set $\lambda_1 = \frac{\beta}{2}$, $\lambda_2 = \frac{\delta}{2}$

Then $U = \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}$

$$\cdot \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

Note, $U = \begin{pmatrix} e^{-i\left(\frac{\beta}{2}+\frac{\delta}{2}\right)} \cos\frac{\gamma}{2} & e^{i\left(-\frac{\beta}{2}+\frac{\delta}{2}\right)} \sin\frac{\gamma}{2} \\ e^{i\left(\frac{\beta}{2}-\frac{\delta}{2}\right)} \sin\frac{\gamma}{2} & e^{-i\left(\beta/2+\delta/2\right)} \sin\frac{\gamma}{2} \end{pmatrix}$

QED !

* Equally, any $U \in SU(2)$ can also be decomposed as a sequence of x-y rotations and a sequence of x-z ~~sequences~~ rotations

$\alpha, \beta, \gamma, \delta, \in$ reals $\rightarrow$ (# of real parameters needed to specify an element of $SU(2)$)

IBM Q use this to implement arbitrary single-qubit gates.

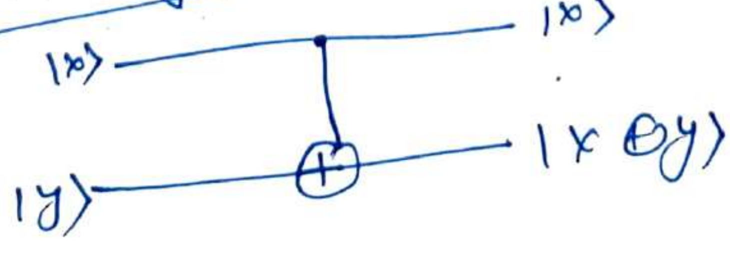
* Universal set of quantum gates $\rightarrow$ finite basic set of gates in terms of which all quantum gates can be decomposed

$\uparrow$

Requires multi qubit gates

* Two qubit gates

CNOT



Standard basis for two qubits

$|00\rangle \longrightarrow |00\rangle$

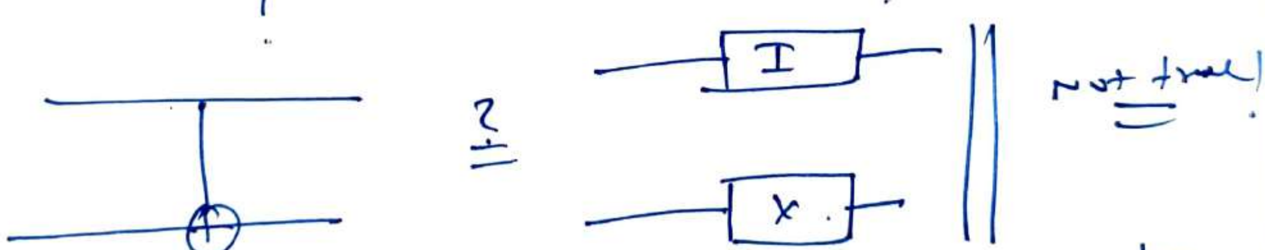
$|0\rangle \otimes |1\rangle \longrightarrow |0\rangle \otimes |1\rangle$

$|1\rangle |0\rangle \longrightarrow |1\rangle |1\rangle$

$|11\rangle \longrightarrow |1\rangle |0\rangle$

$$\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)_{4 \times 4}$$

* CNOT $\overset{?}{\neq}$ $I \otimes X \longrightarrow \left(\begin{array}{cc|cc} \overbrace{0 \quad 1}^{X} & & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & \underbrace{1 \quad 0}_{X} & \end{array}\right)$



* CNOT $= \Lambda(X) \longrightarrow$ controlled-X operation

$\neq I \otimes X$

$\neq X \otimes I$

→ does not have a tensor product decomposition into a product of local gates!

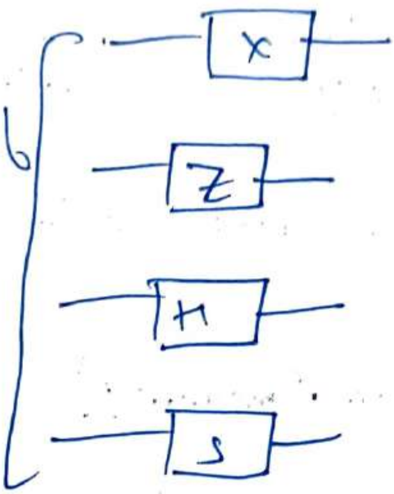
Two qubit gates

- non local gate (entangler)
- local gates (product)

$I \otimes X, \; I \otimes Z$

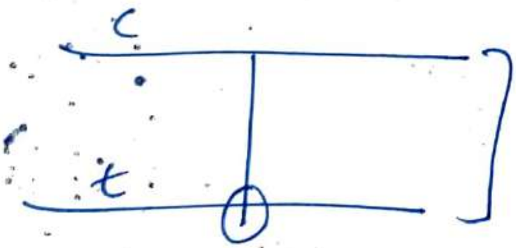
$Z \otimes X, \; H \otimes H$. etc

products of local gates



or

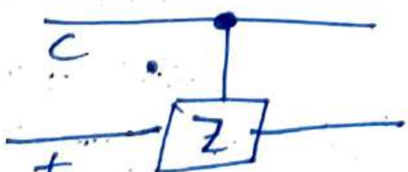
etc



CNOT

$\lambda(X)$

CZ gate (controlled - Z gate)



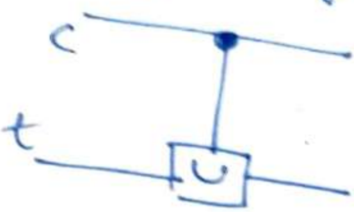
$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$

$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$

$|1\rangle|0\rangle \longrightarrow |1\rangle|0\rangle$

$|1\rangle|1\rangle \longrightarrow -|1\rangle|1\rangle$

* More generally, controlled-U [$\Lambda(U)$]

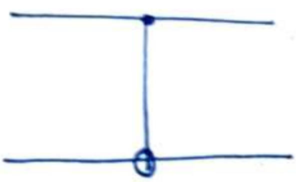


Lec 27 Multi qubit Gates & Universality

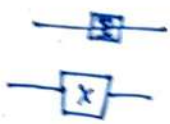
* Controlled-Gates :- (Two qubit gates)

Local — $U \otimes V$

non local — (controlled operations)



$= \text{CNOT} = \Lambda(X) \neq$



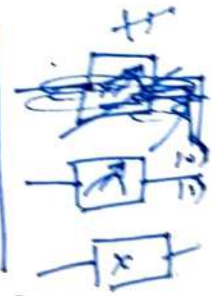
$I \otimes X$

first qubit is being "measured"

$|1\rangle\langle 1|$ — $|0\rangle\langle 0|$

[condition on ~~which~~ whether the first quit is $|0\rangle$ or $|1\rangle$

- Implicit ~~pract~~ projective measurement.



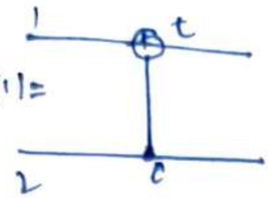
→ Happening in a unitary fashion ⟹ Linear transformation (preserve superposition)

$$\text{CNOT} = \left[(|0\rangle\langle 0|)_c \otimes I_t + (|1\rangle\langle 1|)_c \otimes X_t \right]$$ sum of tensor product

$A_c \otimes B + f_c \otimes g_t$

* Variant of CNOT (i) flipped CNOT: flip c and t

$I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| =$



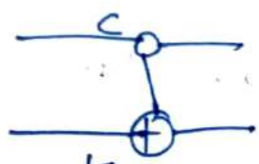
Applied is $|1\rangle|0\rangle$.

$CNOT(|1\rangle \otimes |0\rangle)$

$= \left[|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right]$

$= |1\rangle \otimes X|0\rangle = \underline{|1\rangle|1\rangle}$ ($|1\rangle X|0\rangle$)

(ii) $\overline{CNOT}$ or $\widetilde{CNOT}$



$|0\rangle\langle 0| \otimes + |1\rangle\langle 1| \otimes I$

Recall

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

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

$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes X + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes I$$

$$= \left(\begin{array}{c|c} X & 0 \\ \hline 0 & 0 \end{array}\right) + \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I \end{array}\right)$$

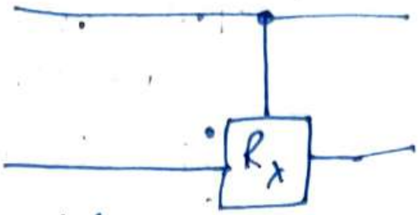
$$= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

eg 2

(check)

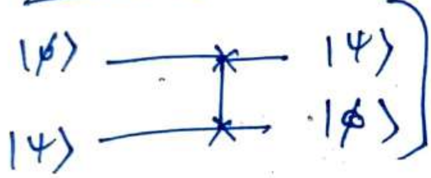
$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

eg 3



$\Lambda(R_x)$ or $\Lambda(R_y)$ or
$\lambda(R_z)$
controlled rotation

eg 4 SWAP gate



nonlocal gate

$|\phi\rangle \otimes |\psi\rangle = |\psi\rangle \otimes |\phi\rangle$

Action on computational basis,

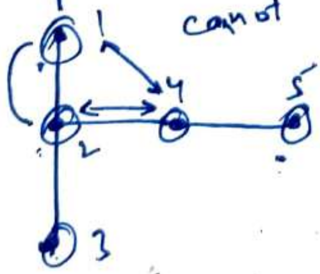
$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$
$|0\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$
$|1\rangle|0\rangle \longrightarrow |0\rangle|1\rangle$
$|1\rangle|1\rangle \longrightarrow |1\rangle|1\rangle$

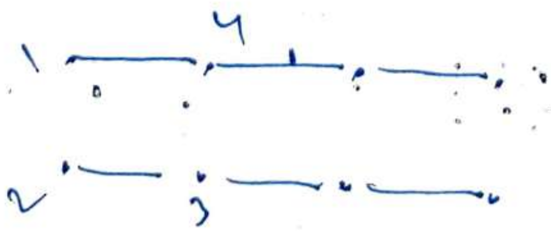
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

* very important Quantum circuit → quantum architecture

cannot do any controlled operation b/w qubits 1 & 4, 3 and 4, 2 and 5

eg 5 qubit Processor on IBM



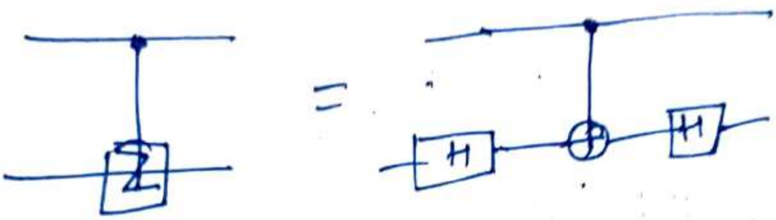


* Circuit Identity

(i)

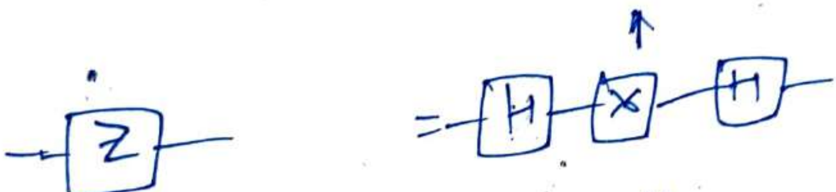
SWAP $\qquad$ sequence of 3 CNOTs !

(ii)



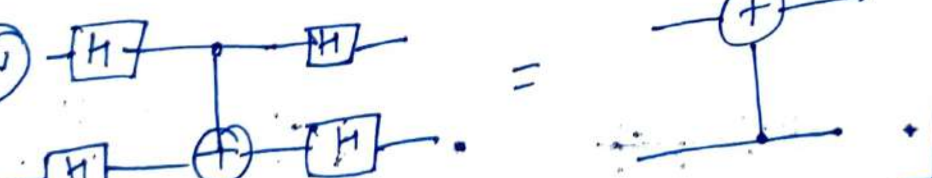
Controlled-Z

(iii)



$$Z = HXH.$$
$$X = HZH$$
$$-Y = HYH$$

(iv)



check!

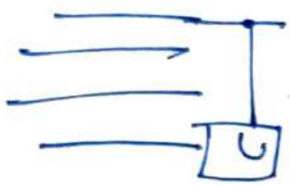
$|\psi\rangle \qquad XS|\psi\rangle \qquad U|\psi\rangle$

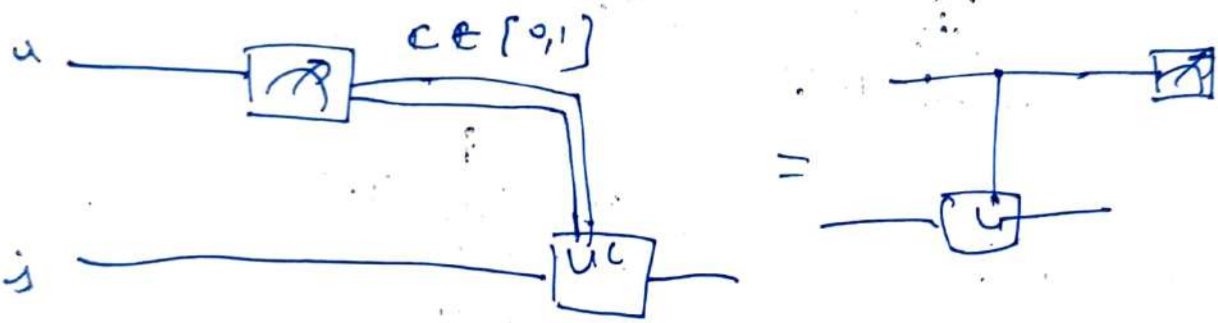
$$\underline{U = XS}$$

Measurement in Quantum circuit

* "Principle of deferred Measurement."

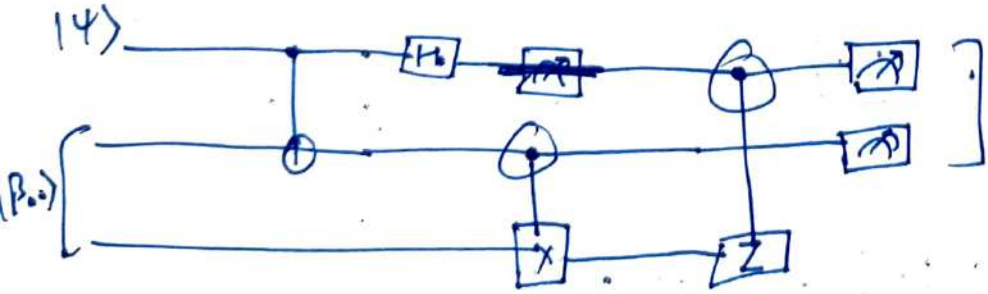
Measurements can always be moved to the end of circuit by making use of controlled operations





I if $c = 0$
U if $c = 1$

eg Teleportation Circuit (within a quantum device)



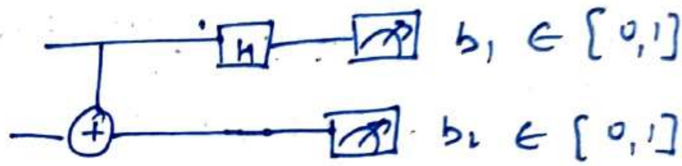
To the very end of the circuit

Modified teleportation circuit uses only $\lambda(X)$, $\lambda(Z)$!

* Bell- basis measurement :- Measure in an entagled basis, simply using CNOT, H, single qubit measurement.

$|\beta_{00}\rangle$
$|\beta_{01}\rangle$
$|\beta_{10}\rangle$
$|\beta_{11}\rangle$

orthonormal & normalized } ON basis

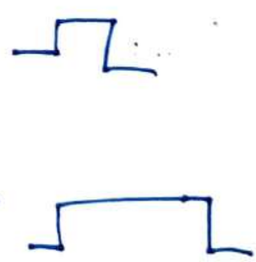


4 - values of (b_1, b_2)
→ distinctly map to
$|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle$
and $|\beta_{11}\rangle$

Lect 28

Qubits

The basic → bits → 0, 1
↓
telegraph



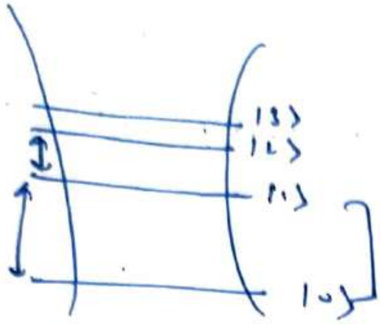
quantum information theory

qubit $|0\rangle$ $\quad a|0\rangle + b|1\rangle$

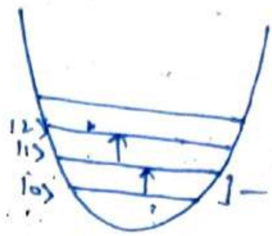
$|1\rangle$ $\quad |a|^2 + |b|^2 = 1$

How to create a qubit out of a physical system
↓ electrical circuit
light waves

Atoms



Quantum Harmonic oscillator



Atoms → natural form of qubit

↳ individual addressing

Macroscopic systems (system: little bigger than atoms)

→ Artificial atoms

NMR qubit

liquid NMR

solid state NMR

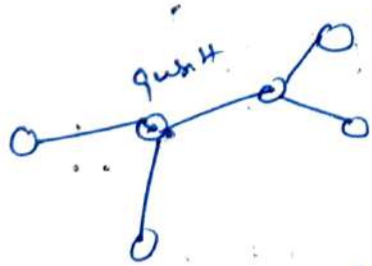
↓

Atomic nuclei - spin-$\frac{1}{2}$ system

↓

we are not using or addressing one single qubit

10^{+15} qubit



ensemble quantum processing

→ disadvantage :-

↓

If you want to scale 2-qubit

4-qubits

$|\psi\rangle \longrightarrow \mathbb{I}$

Solid state NMR]

Diamond → carbon atom,

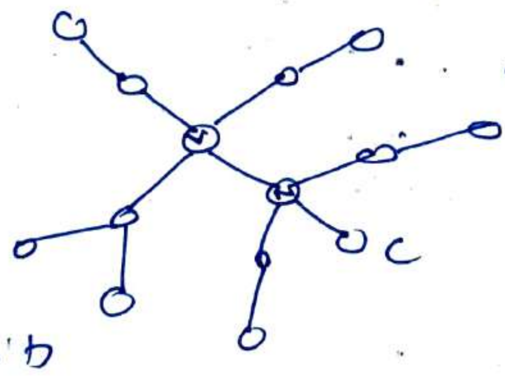
Nitrogen → vacancy

NMR

Solid state NMR

→ ensemble quantum processing

NV center



Diamond

→ defects

→

9- qubits

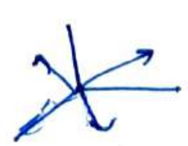
— Photonic qubit

Polarization

linear polarization

$|H\rangle \; |1\rangle$

$|H\rangle \; -|0\rangle$



Circular polarization light

Right circularly polarized

left circularly polarized

Phototonic

↓

generate

laser

visible IR

microwave

wave plate

mirrors

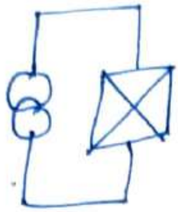
waveguides

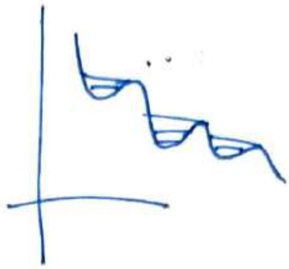
$A \longrightarrow B$

Superconducting qubit

Josephson junction

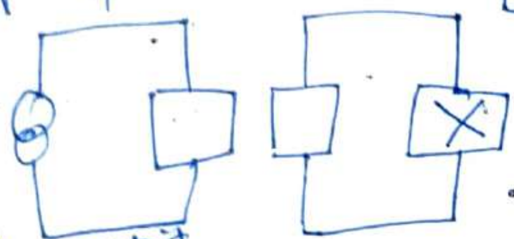
E_J E_C

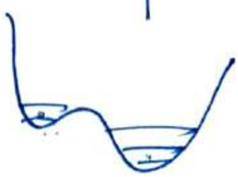




washy board potential

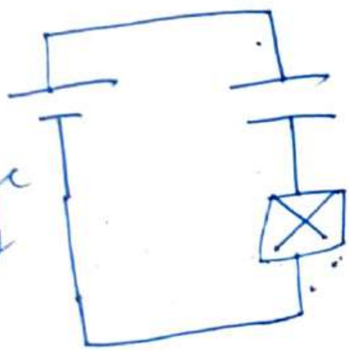
Phase qubit

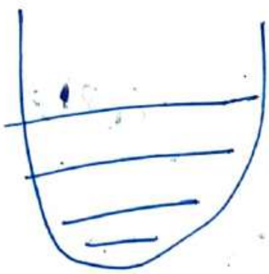


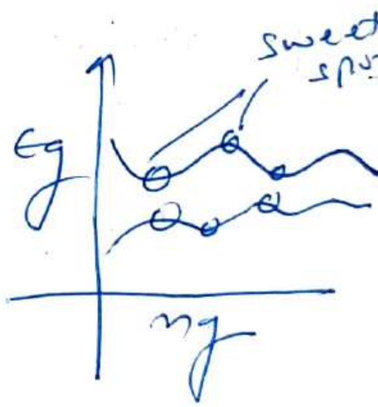


flux qubit

charge qubit

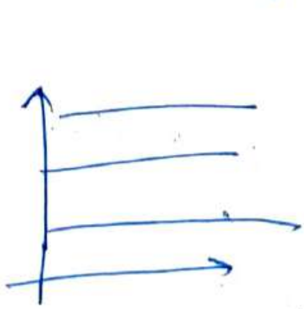






$E_J / E_C \sim 1$

$E_J / E_C \sim 50$



transmon

transmon → IBM Google

Ion trap

electric and magnetic fields

↓

Ion Q → Quantum computer

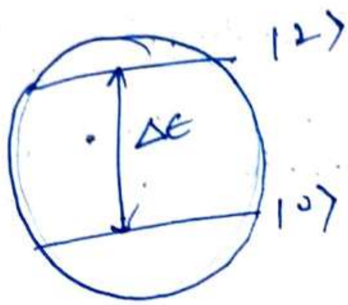
Rydberg atoms

$n \sim 100$

BCC qubit

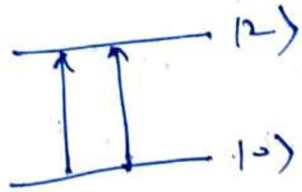
Onix two species of atoms

Qubit frequency



$\Delta E = h\nu$ → qubit frequency

Relaxation time



Coherence time

Quantum → classical

T_2 → decoherence time

Divincenzo criteria

1. Scalability : 2 qubit, 3 qubit →
2. Ability to initialize :- $|01001\rangle$
3. Long decoherence time :—

4. Universal set of quantum gates
5. Measurement capability;

Quantum communication

qubit → stationary, flying

(1) stationary ↔ flying

2: flying qubits

Lec 30 Universal Quantum Gates

* Single-qubit gates (unitary) : $U \in SU(2)$ (group under multiplication)

↓

* Rotation gates $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$

Any $U \in SU(2)$ can be decomposed in terms of $R_x R_y$ or $R_y R_z$ or $R_x R_z$.

* Two qubit gates: controlled unitary gates
  - $U_1 \otimes U_2$
  - Non local gates → SWAP

Universality: is not an exact state, it is approximate state

A set of gates $G = \{g_1, g_2, \ldots g_N\}$ is set to be universal if any arbitrary quantum gate (on any d-dimensional space) can be approximated to arbitrary accuracy by a quantum

Circuit comprises of these gates from G

* One set of universal gate = {H, S, $T(\pi/8)$, CNOT}

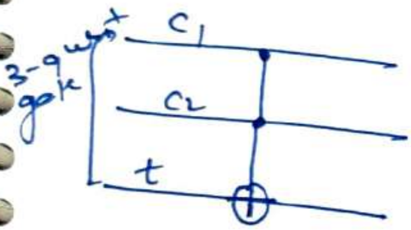
$$\left[\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \quad S = T^2 \right]$$

* <u>Solovay Kitaev theorem</u> → chap 4 of Nielsen and Chuang

* Two step for universality statement

① Arbitrary unitary (U) can be exactly realized as a (product) sequence of single qubit unitary as CNOT

$$G = \{ SU(2), \text{CNOT} \}$$



Controlled-controlled NOT

<u>Toffoli gate</u>

(8x8 unitary matrix)

Harder ② Any single qubit unitary $U \in SU(2)$ can be approximated to arbitrary accuracy using H, S and T

<u>Aside</u> Alternate set of universal gates

$$G = \{H, \text{Toffoli gate}\}$$

① <u>Exact universality</u>: key idea is to reduce arbitrary $d \times d$ unitary → ~~2 level~~ 2 level unitary

* 2 level unitary: acts non trivially only on a 2-qubit subspace of the d-dim space

$$\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}_{d \times d} \xrightarrow{\text{break it down}} \begin{pmatrix} x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & x \end{pmatrix}_{d \times d}$$

eg 2. 8×8 unitary (3-qubit gate)

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & & & & & & 0 \\ 0 & & 1 & & 0 & & & 0 \\ 0 & & & 1 & & & & 0 \\ 0 & & 0 & & 1 & & & 0 \\ 0 & & & & & 1 & & 0 \\ 0 & & & & & & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

3 qubit space ≡ 8 dim space spanned by $\{|000\rangle, |001\rangle, |010\rangle \ldots |110\rangle, |111\rangle\}$

U acts nontrivially only ~~on vector~~ on $|000\rangle$ and $|111\rangle$ (out of this set of 8 ON vectors)

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

* 2-dim subspace $(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$ 3 qubit states

$\{|000\rangle\ |111\rangle\} \longrightarrow \alpha|000\rangle + \beta|111\rangle$ (like a qubit space!)

$|\tilde{0}\rangle \quad |\tilde{1}\rangle$

$\tilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ effectively looks like this in the 2 dim subspace spanned by $|000\rangle$ and $|111\rangle$

* we can show that if U is a d×d unitary then exist 2 level unitaries, $U_1, U_2, U_3 \ldots U_k$ such that

$$U_k U_{k-1} U_{k-2} \cdots U_3 U_2 U_1 U = I$$

$$\Rightarrow \boxed{U = U_1^\dagger U_2^\dagger U_3^\dagger \cdots U_k^\dagger}$$

[In a circuit, this translates to a set of single-qubit gates and CNOTs]

Example consider a 3×3 unitary (qutrit system / 3 dimensional quantum system)

$$U = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}_{3\times 3}$$

Identify $U_1, U_2, U_3 \ldots$ such that (i) hold.

Algorithm (i) If $d = 0$, then $U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

If not, then $U_1 = \begin{pmatrix} \# & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$U_1 = \begin{pmatrix} \dfrac{a^*}{\sqrt{|a|^2+|d|^2}} & \dfrac{d^*}{\sqrt{|a|^2+|d|^2}} & 0 \\[2ex] \dfrac{d}{\sqrt{|a|^2+|d|^2}} & \dfrac{-a}{\sqrt{|a|^2+|d|^2}} & 0 \\[2ex] 0 & 0 & 1 \end{pmatrix}$$

Check $U_1 U = \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ g & h & j \end{pmatrix}$

(ii) Check if $g = 0$, $U_2 = \begin{pmatrix} (a')^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$U_2 = \begin{pmatrix} - & 0 & - \\ 0 & 1 & 0 \\ - & 0 & - \end{pmatrix}$$

$$U_2 = \begin{pmatrix} \frac{a'^*}{\sqrt{|a|^2+|g|^2}} & 0 & \frac{g^*}{\sqrt{|a'|^2+|g|^2}} \\ 0 & 1 & 0 \\ \frac{g'}{\sqrt{|a|^2+|g|^2}} & & \frac{a'}{\sqrt{|a|^2+|g|^2}} \end{pmatrix}$$

check ~~$U_2 U_1 U =$~~

$$U_2 U_1 U = \begin{pmatrix} 1 & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & j'' \end{pmatrix} = V \quad \underline{\underline{\text{unitary}}}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & f'' \\ 0 & h'' & j'' \end{pmatrix} \longrightarrow \text{two level unit}$$

$$= U_2 U_1 U = U_3^\dagger$$

$$\Rightarrow U_3 U_2 U_1 U = I \iff \boxed{U = U_1^\dagger U_2^\dagger U_3^\dagger}$$

$$U_1 = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad U_2 = \begin{pmatrix} * & 0 & * \\ 0 & 1 & 0 \\ * & 0 & * \end{pmatrix}$$

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

* Generally: for a $d \times d$ unitary, U_d

$U_d \rightarrow$ $(d-1)$ two level unitary $\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & & & & \\ 0 & & (U_{d-1}) & & \\ 0 & & & & \\ 0 & & & & \end{pmatrix}_{d-1}$

$(d-1)(d-1)$ unitary

$U_{d-1} \rightarrow (d-2)$ two level unitaries

$\downarrow$

$\vdots$

$$U_3 \quad \begin{pmatrix} 1 & 0 \\ 0 & \boxed{U_{d-2}} \end{pmatrix}$$

$(d-2)(d-2)$ unitary

...

$\downarrow$

$$\begin{pmatrix} 1 & 0 \\ 0 & U_2 \end{pmatrix} \rightarrow \left(\underline{1} \text{. unitary in final step.}\right)$$

2×2

$$U_d = V_1 V_2 \cdots V_k \quad \text{with } k \leq (d-1) + (d-2) + \cdots 1$$

$$= \frac{d(d-1)}{2}$$

two level unitary

L - 3 : Universality and complexity

<u>Recap</u> Universal Quantum Gates.

* Two universal sets
  - H, S, T and CNOT (2-qubit gate)
  - H and C-C NOT (Toffoli) (3-qubit gate)

* Showing universality of {H, S, T, CNOT} is a two step process

(1) Any unitary (d×d) can be realized as a sequence ~~decomposed as a~~ ~~Product of~~ of single qubit unitaries and CNOTs.

<u>Recall!</u> $\underset{d \times d}{U \in SU(d)} \longrightarrow$ Product of 2-level unitary

$U = U_1^{\dagger} U_2^{\dagger} \dots U_m^{\dagger} \longrightarrow$ all the U_i's are of the form

eg 3×3 ~~unitary~~ → 3 two level unitaries.

Two level unitary

$$\begin{pmatrix} a & & 0 & & b \\ & 1 & & & \\ & & 1 & & \\ 0 & & & 1 & 0 \\ & & & & 1 \\ c & & 0 & & d \end{pmatrix}$$

$d \times d \to \frac{d(d-1)}{2}$ unitaries.

acts non trivially only on 2 states of the computational basis

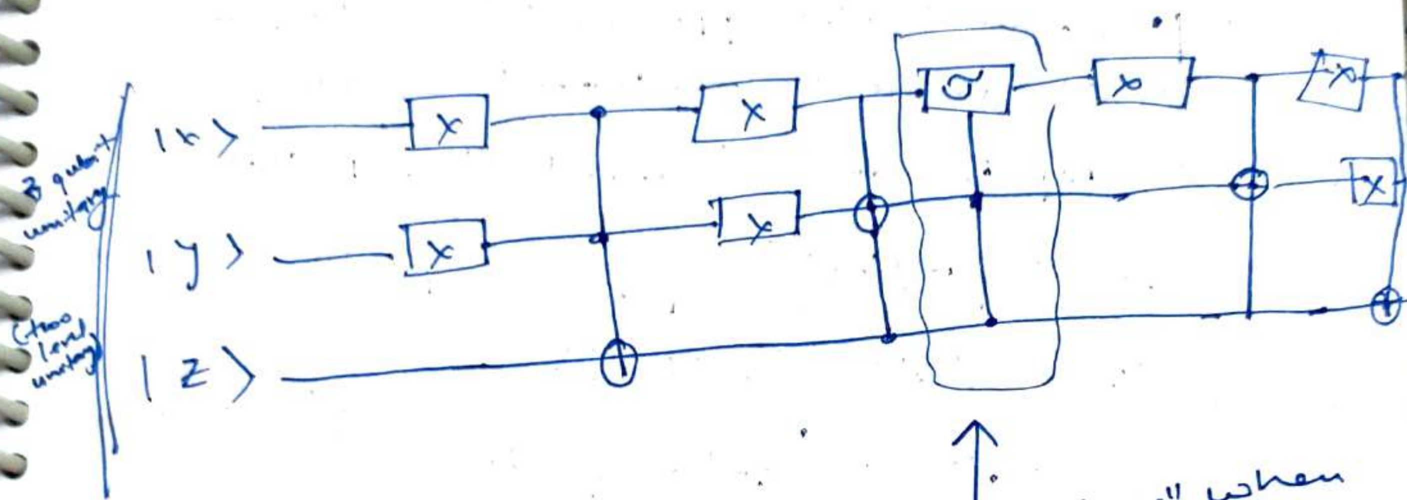
Acts trivially (identity) on the rest of the basis

(1) (b) Any two level unitary can be implemented using CNOT and single ~~qubit~~ qubit ~~unitary~~ matrices

eg 8×8 unitary 3 qubit system $\begin{pmatrix} a & & 0 & b \\ & 1 & & \\ 0 & & \ddots & \\ c & & & d \end{pmatrix}$

If $|000\rangle \equiv |\tilde{0}\rangle$ and $|111\rangle \equiv |\tilde{1}\rangle$ (Logical zero and Logical one)

$\tilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ single qubit gate on $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$



check that the control are "ON" when input are $|000\rangle$ and $|111\rangle$

<u>Exercise</u>

~~check that the control are only~~

(1) Arbitrary $d \times d$ unitaries $\longrightarrow$ single qubits matrices CNOT

<u>Approximate</u> $\downarrow$

$\{H, S$ and $T\}$

(2) <u>Approximate universality</u>: Quantify "approximate"

* we need to implement U but we instead implement V.

Error function: $e(U, V) \stackrel{\max}{=}_{|\psi\rangle} \| U|\psi\rangle - V|\psi\rangle \| = \max_{|\psi\rangle} \| (U - V)|\psi\rangle \|$

Maximum norm of the difference b/w the action of U and V on a particular $|\psi\rangle$

— Maximize this over all $|\psi\rangle \in \mathcal{H}$
(worst-case))

* If $E(U,V)$ is small, any measurement on $V|\psi\rangle$ will give approximately the same statistics as a measurement on $U|\psi\rangle$

* Let M_i be an element of a POVM
($M = \{M_i \geq 0\}$) $p_u(i) \equiv$ prob. of outcome i if the state is $U|\psi\rangle$

$p_v(i) \equiv$ prob. of " " if the state is $V|\psi\rangle$

$$|p_u(i) - p_v(i)| \leq 2E(U,V)$$

* ~~Any~~ single qubit unitary $U_{2\times 2} \in SU(2)$ can be implemented using H, S and T to arbitrary accuracy in $E(U,V)$.

Solovay-Kitaev theorem (chp 4 of Nielsen Chuang)

Quantum algorithms

Oracle based algorithms → Deutsch algorithm

Q. Fourier transform based (exponential faster than a discrete Fourier transform)

— Deutch Jozsa algorithm] | Exponential speedup
— Grover search algorithm] | quadratic speedup

* Computational Hardness | Problem of n-qubits. $(N \simeq 2^n)$

How does circuit size scale with n? (Depth / Breadth)

# of gates scale with n?

Gate complexity

#G ~ poly(n) — circuit of polynomial size BQP — Bounded quantum polynomial.

eg search eu factoring $\in$

G ~ exp(n) quantum hard! QMA (NP)

Lect 32 Deutsch-Jozsa algorithm

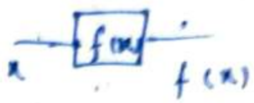
* Recap of Deutsch Algorithm

Problem: Given a single bit Boolean fn. $f(x)$ $(x \in [0,1])$ is $f(x)$ is constant / balanced

constant $\Rightarrow f(0) = f(1)$

Balanced $\Rightarrow f(0) \neq f(1)$

Quan Oracle : classical oracle



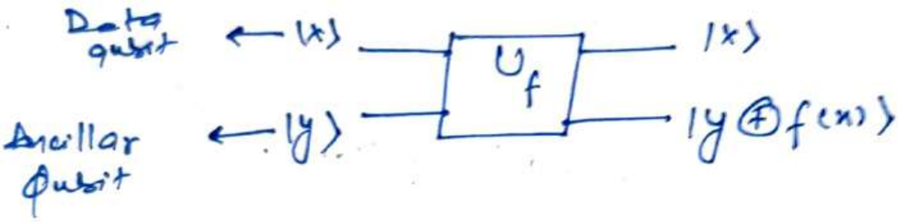
compare output

$f(0) \oplus f(1)$

XOR

Serial fashion $\longrightarrow$ $f(0) \oplus f(1)$ ⟨ 0 constant $f(0)=f(1)$ / 1 balanced. $f(0) \neq f(1)$

* Quantum oracle :



$$U_f |x\rangle|y\rangle = |x\rangle y \oplus f(x)\rangle$$

Let $|x\rangle = 0$, $|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$U_f |0\rangle|-\rangle = \frac{|0\rangle|0 \oplus f(0)\rangle - |0\rangle \oplus f(0)\rangle}{\sqrt{2}}$$

~~If f(0) = 0~~ $|\Psi\rangle$

If $f(0) = 0$, $|\Psi\rangle = \frac{|0\rangle|0\rangle - |0\rangle|1\rangle}{\sqrt{2}}$

$$= |0\rangle|-\rangle = (-1)^0 |0\rangle|-\rangle .$$

If $f(0) = 1$, $|\Psi\rangle = \frac{|0\rangle|1\rangle - |0\rangle|0\rangle}{\sqrt{2}}$

$$= (-)|0\rangle|-\rangle$$

$$= (-1)^1 |0\rangle|-\rangle$$

$\Rightarrow U_f |0\rangle|-\rangle = (-1)^{f(0)}|0\rangle|-\rangle$

Check ~~wt~~ $U_f |1\rangle|-\rangle = (-1)^{f(1)}|1\rangle|-\rangle$]

Implementable

$$\boxed{U_f |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle} \quad \underline{\underline{\text{eqn } 0}}$$

ancillary qubit

Deutch oracle $\underline{|x\rangle \longrightarrow} (-1)^{f(x)}|x\rangle$

∴ This is a desired functionality of oracle

* $\underline{\text{eqn. 0 describes the q. oracle}}$

Query via superposition

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

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

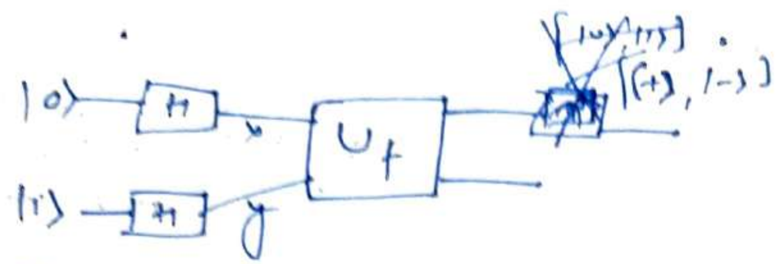
$$= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle\right]$$

$$\cancel{= \frac{1}{\sqrt{2}}(-1)}$$

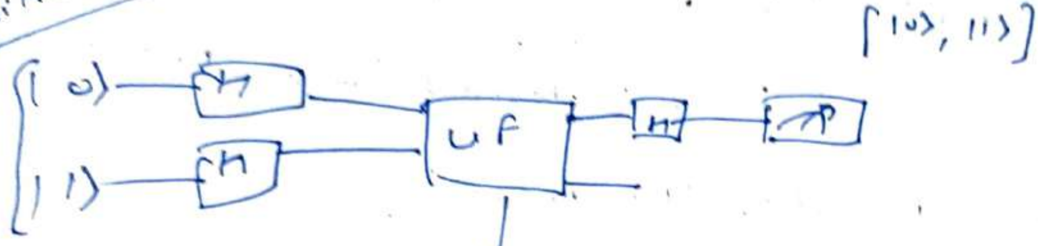
$$(-1)|\pm\rangle|-\rangle$$

$\vert+\rangle$ if $f(0)=f(1)$ (constant)	$\vert-\rangle$ if $f(0) \neq f(1)$ Balanced
$\xrightarrow{H}$ $\vert 0\rangle$	$\xrightarrow{H}$ $\vert 1\rangle$

Circuit for Deutsch Algorithm



Initialization



Circuit for this oracle?

Query complexity = 1
Classically " = 2

Depend on the fn in quantum

$\boxed{\text{Assignment 3:- } f \rightarrow U_f}$

Deutsch Jozsa

Problem: Given an n-bit Boolean fn.

$$f(x): \{0,1\}^n \rightarrow \{0,1\}$$

Promise $f(x)$ is either constant or balanced.

$f(x) = c$, $\{0,1\}$, $\forall\ 2^n$ bit strings

$f(x) = c_1$ for 2^{n-1} strings, $f(x) = c_2$ for 2^{n-1} string

* Classically oracle

"x"

queries $= \frac{2^n}{2} + 1 = 2^{n-1} + 1$ → scaling exponentially with n

exponential speed up!

* D.J algorithm # queries = 1 !

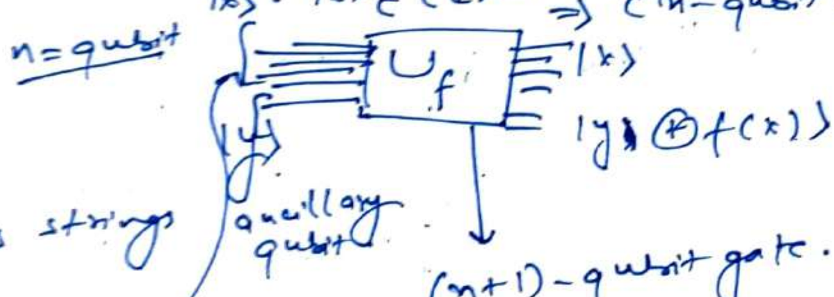
→ fixed constant !

[constant # of queries]

steps of the DJ algorithm

we use the same ~~oracle~~ quantum oracle:

$|x\rangle \cdot |x\rangle \in (\mathbb{C}^2)^{\otimes n} \Rightarrow$ (n-qubit state):



2^n bits strings → 2^n orthogonal states → n-qubit register

[same quantum oracle]

$$\boxed{U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |1\rangle}$$

$|x\rangle$ → n qubit state

* Superposed input → query in superposition

uniform superposition of all 2^n ON states that form the computational basis for the n qubit space!

$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \cdots \otimes \mathbb{C}^2}_{n\text{-times}}$

ON Basis
(computational basis)

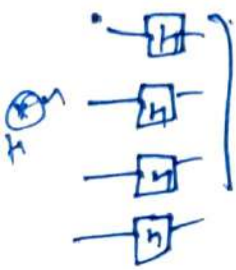
$\{|00\ldots0\rangle, |00\ldots1\rangle, |0\ldots010\rangle, |0\ldots011\rangle, |111\ldots11\rangle\}$

n bit one string

$~~|\Phi\rangle = \sum_{x\in\{0,1\}^{\otimes n}}~~$

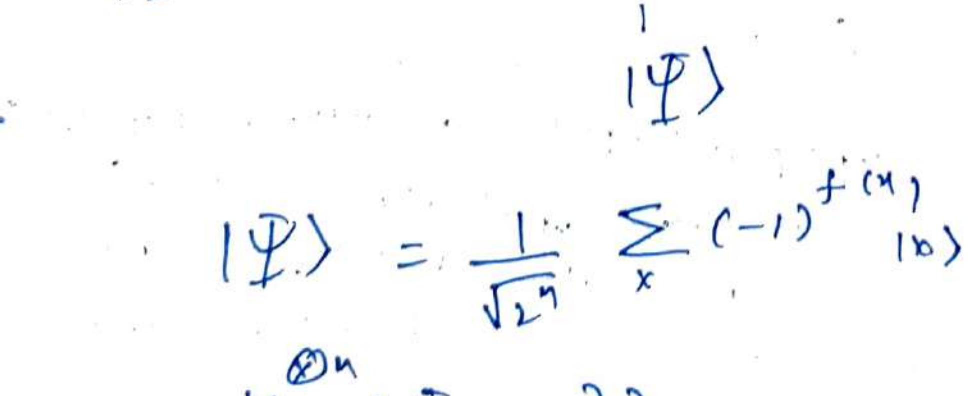
$$|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\substack{x \in n\text{-bit string} \\ x \in \{0,1\}^{\otimes n}}} |x\rangle$$

* start with all zero states $|0\rangle^{\otimes n} = |000\ldots00\rangle$
* Apply $H^{\otimes n}$



$$H^{\otimes n}|00\ldots0\rangle = |\Phi\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^{\otimes n}} |x\rangle$$



2^n possible outcomes.

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle |-\rangle$$

$$H^{\otimes n}|\Psi\rangle = ??$$

→ n-qubit measurements

0 0 ... 0

{00...01, 001...0, 0011...0, 11111}

Chp 33 DJ & Grover search algorithm

$$\begin{matrix} |x\rangle & \to & \boxed{U_f} & \to & |x\rangle \\ |y\rangle & \to & & \to & |y \oplus f(x)\rangle \end{matrix}$$

Steps of DJ algorithm

(1.) start in $|0\rangle^{\otimes n}$ state : $|0\rangle^{\otimes n} = |0 \dots 0\rangle$

(2.) Uniform superposition of all n-bit strings (2^n of them)

→ Use the $\underbrace{H \otimes H \otimes \dots \otimes H}_{n\text{- qubit Hadamard}} \equiv H^{\otimes n}$

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x_1, x_2, x_3 \dots x_n \in [0,1]} |x_1, x_2 \dots x_n\rangle$$

Ancilla qubit $|0\rangle \xrightarrow{X} |1\rangle \xrightarrow{H} |-\rangle$

(3) $$U_f \left[\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes |-\rangle \right] = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle |-\rangle$$

$$= |\psi\rangle$$

(4.) $H^{\otimes n} |\psi\rangle$

(Binary multiplication)

eg single $$H|x\rangle = \sum_{z \in [0,1]} \frac{(-1)^{x \cdot z} |z\rangle}{\sqrt{2}}$$

$$= \frac{(-1)^{x \cdot 0} |0\rangle + (-1)^{x \cdot 1} |1\rangle}{\sqrt{2}}$$

$$H^{\otimes n} |x_1 x_2 \dots x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1, z_2 \dots z_n \in [0,1]} (-1)^{x_1 z_1 \, x_2 z_2 \, x_n z_n}$$

↓

$(H \otimes H \otimes \dots H) |x_1\rangle |x_2\rangle \dots |x_n\rangle$

$$H^{\otimes n} \otimes I \,|\Psi\rangle = \frac{1}{2^n} \sum_x \sum_z (-1)^{f(x)} (-1)^{x_1 z_1 + x_2 z_2 + \cdots + x_n z_n} |z\rangle|-\rangle$$

$\downarrow$
Cancilla)

$$= \frac{1}{2^n} \sum_{x,z} (-1)^{x \cdot z + f(x)} |z\rangle|-\rangle = |\tilde{\Psi}\rangle$$

$$\left[\begin{array}{l} x \cdot z. = \text{bitwise inner product (symplectic products)} \\ = x_1 z_1 + x_2 z_2 + \cdots x_n z_n \end{array}\right]$$

* Two cases

(1.) $f(x) = \text{constant}$ $\begin{cases} \to 0 \;\; \forall x \\ \to 1 \;\; \forall x \end{cases}$

Then, amplitude of $|0 \cdots 0\rangle$

$$= \frac{1}{2^n} \sum_x (-1)^{f(x) + x \cdot \overset{0}{\overset{\shortparallel}{z}}}$$

$$= \frac{1}{2^n} \sum_x (-1)^{f(x)} \begin{cases} +1 \\ -1 \end{cases}$$

$\downarrow$
All phases add constructively

$\Rightarrow$ Probability of getting $|0 \cdots 0\rangle$ in the final measurement $= 1$!

(11.) $f(x)$ is balanced

Amplitudes of $|0 \cdots 0\rangle = \frac{1}{2^n} \sum_x (-1)^{f(x) + \overset{0}{\overset{\shortparallel}{\widehat{x \cdot z}}}}$

$$= \frac{1}{2^n} \sum_x (-1)^{f(x)} = 0!$$

$\longrightarrow$ phase interference destructively

$\left(\begin{array}{l}\text{Half of } f(x) = 0 \\ \text{other half} = 1\end{array}\right)$

Probability of $|0..0\rangle = 0$!

step 5: Measurement in the std. basis

$|0..0\rangle$ with prob $= 1$

$\Downarrow$

$f(x)$ is constant

one of the other 2^{n-1} state $[|0..0\rangle, |1,...1\rangle]$

at least one of the measurement must be 1

$\Downarrow$

$f(x)$ is Balanced

$\Rightarrow$ solved the DJ problem with 1 query of the oracle

* classically, need $2^{n-1}+1$ queries $\Rightarrow$ scaling exponentially with # of bits.

$\Rightarrow$ Q. Algo has an exponential speedup

Quantum search algorithm (Luo Grover, Bells Labs)

* Real world application
* Database with N entries $(N \equiv 2^n)$

Task: Identify one or more "solutions" from the N-entries

eg Travelling salesman problem:

Find the shortest route connecting all cities in a map.

↳ search through all possible routes & compute their length.

find the route with shortest length.

(ii) Prime factorization (shor's factoring algorithm)

search → find a prime factor of $M = pq$ (product of two very large primes)

→ 5893 (RSA crypto system)

search over all numbers from 2 to $\sqrt{m}$

Identify a factor (≡ solution to the search) via simple dimension operations "easy"

↓

Like an oracle operation because it marks the solution states

* for a database with N entries (with one solution)

classically, $O(N)$ operations to identify a solution

→ Grover search shows that this can be done in $O(\sqrt{N})$ operations

quadratic speedup

* Basic idea: Quantum oracle

$$\hat{O}\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle$$

↓

data qubit

marks the solution states

$$\begin{cases} f(x) = 0 & \text{if } x \text{ is not a solution} \\ \quad\;\; = 1 & \text{if } x \text{ is a solution} \end{cases}$$

Lec 34 Grover Search Algorithm

* Oracle-based algorithms

complexity: Query complexity = # of ~~tim~~ times the oracle has to be queried.

# of times the "oracle subroutine" has to be called

* oracle: $\hat{O}$ (unitary operator).

$f(x): [0, N-1]$
↓
search over a database of size $N \cong 2^n$ (n-bit strings to encode N)

$f(x) = 1$ if x is a solution to the search problem

0 if x is not a soln

$\hat{O}: |x\rangle|q\rangle \longrightarrow |x\rangle|q \oplus f(x)\rangle$

$|x\rangle$: n-qubit register

$|q\rangle$: ancilla

follow the same analysis as DJ algorithm.

Let $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, then $\hat{O}|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

$(-1)^{f(x)}$: marks a soln. state

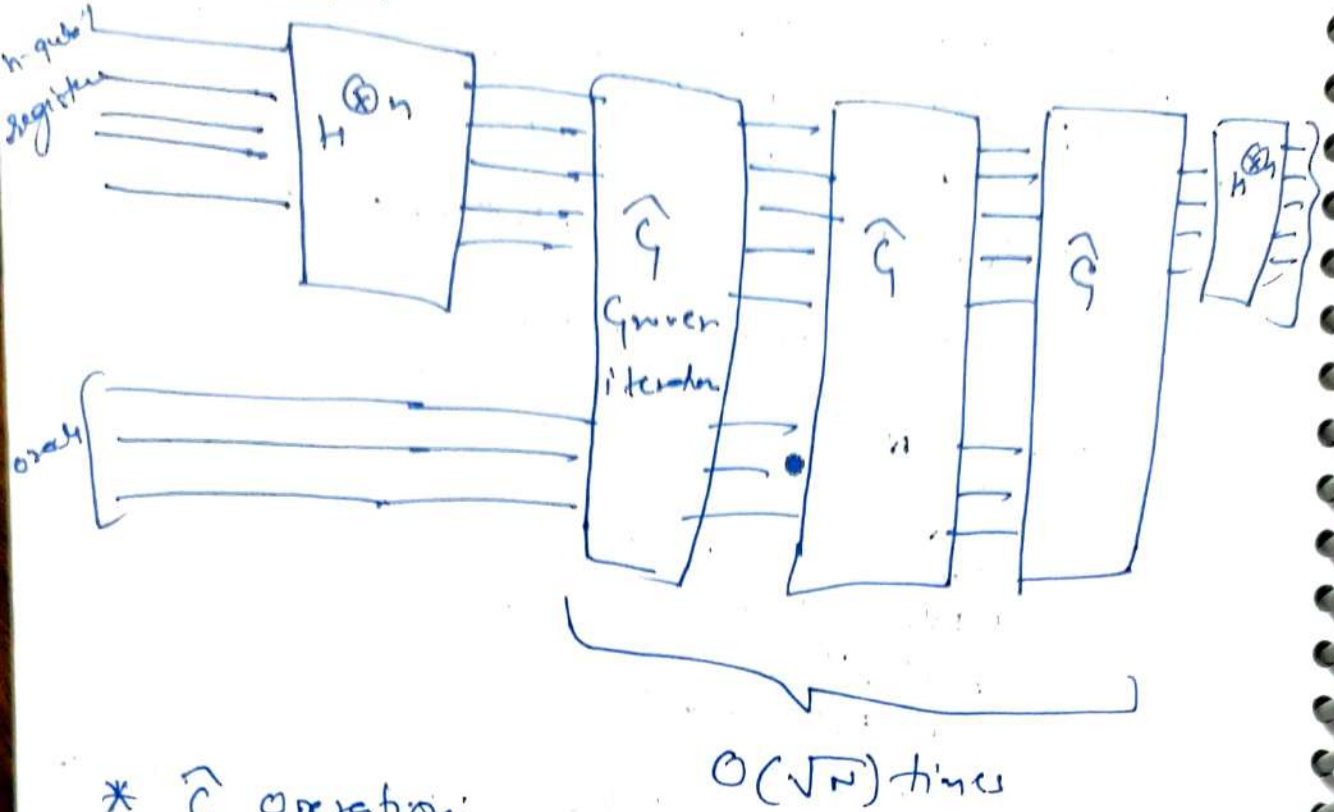
Abstract the oracle action as: $\boxed{\hat{O}|x\rangle = (-1)^{f(x)}|x\rangle}$

* Grovers search algorithm (Lov Grover 1996, Bell Labs)

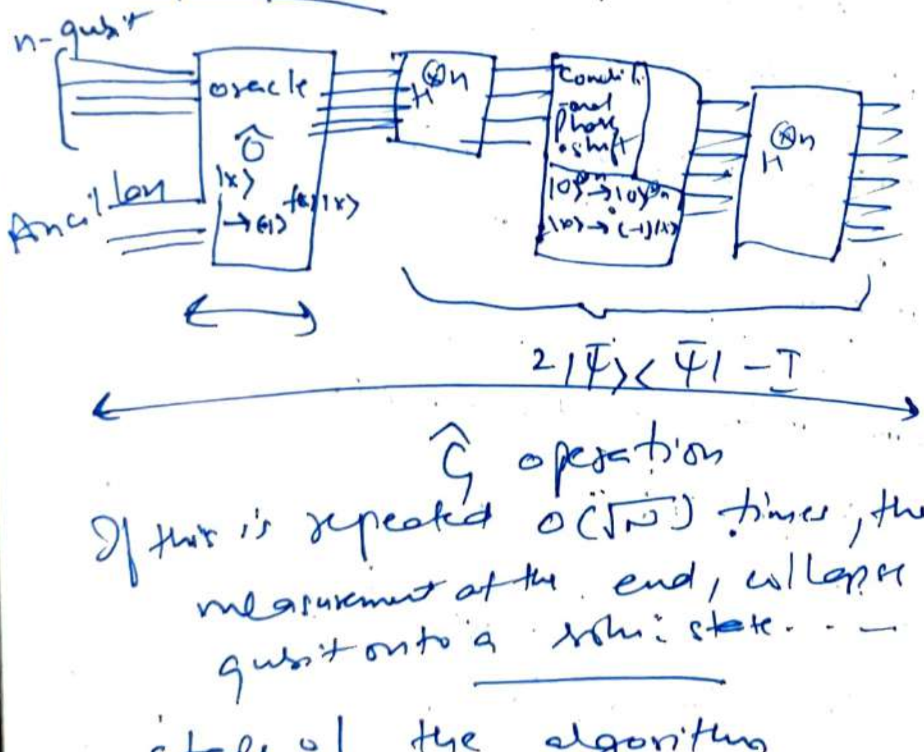
$H^{\otimes n}$ (to query in superposition)

- Grovers iteration: $\hat{G}$ involve $\hat{O}$ and a certain phase shift using $\hat{O}$

- ~~Measurement~~ "$H^{\otimes n}$"
- Measurement



* $\hat{G}$ operation:



If this is repeated $O(\sqrt{N})$ times, then the measurement at the end, collapses the data qubit onto a soln state...

steps of the algorithm

(1) starts with $|0\rangle^{\otimes n}$

(ii) $H^{\otimes n}|0\rangle^{\otimes n} = |\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^{\otimes n}} |x\rangle$

$$= \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

ON basis for $(\mathbb{C}^2)^{\otimes n}$ set of states associated with the entire data base.

(iii) Apply $\hat{G}$ operator multiple times

$$\hat{G} = (H^{\otimes n})\begin{pmatrix}\text{Phase} \\ \text{shift}\end{pmatrix}(H^{\otimes n})\hat{O}$$

$$\hat{P} = 2|0\rangle\langle 0| - I$$

$$\hat{P} = 2|00\ldots0\rangle\langle 0\ldots0| - \underline{I}$$

$$H^{\otimes n}\,\hat{P}\,H^{\otimes n} = H^{\otimes n}\left[2|0\ldots0\rangle\langle 0\ldots| - I\right]H^{\otimes n}$$

$$= 2|\Psi\rangle\langle\Psi| - I$$

$$\hat{G} = (2|\Psi\rangle\langle\Psi| - I)\,\hat{O}$$

"Inversion about the mean"

Exercise: $2(|\Psi\rangle\langle\Psi| - I)\sum_y \alpha_y |y\rangle = \sum_y \left[-\alpha_y + 2\langle\alpha\rangle\right]$

n qubit state

$$\left(\langle\alpha\rangle = \frac{\sum_y \alpha_y}{N}\right)$$

* Visualize $\hat{G}$: Rotation in the two-dimensional space spanned by solns and non solution states

- Set of all n-bit strings
2^n states $|x\rangle$ — set of solution state S
— set of non solution states $\sim S$

- Two superposition states:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \sim S} |x\rangle$$

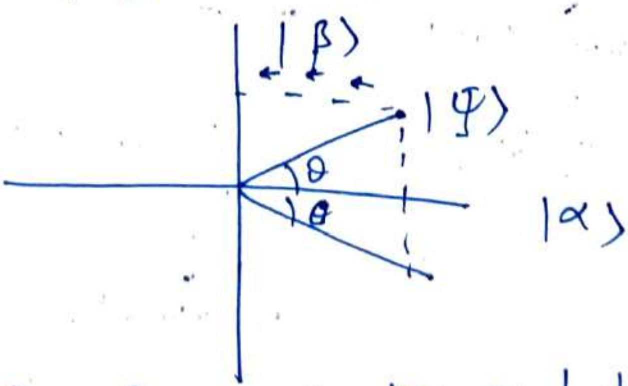
$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$$

Mutually orthogonal
$\langle\alpha|\beta\rangle = 0$
$\langle\alpha|\alpha\rangle = \langle\beta|\beta\rangle = 1$

$\Rightarrow$ $[|\alpha\rangle, |\beta\rangle]$ span a 2-dim subspace of the 2^n-dim space (n-qubit space)

Now, $|\Psi\rangle = |\alpha\rangle + |\beta\rangle$

$$|\Psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$



Visualize the Grover iteration as follows

(i) $\hat{O}|\alpha\rangle = |\alpha\rangle$, $\hat{O}|\beta\rangle = -|\beta\rangle$

$$\hat{O}\left(\sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle\right) = \sqrt{\frac{N-M}{N}} - \sqrt{\frac{M}{N}}|\beta\rangle$$

- Reflecting the state $|\Psi\rangle$ about $|\alpha\rangle$

(ii) $(2|\Psi\rangle\langle\Psi| - I)\ |\Psi\rangle = |\Psi\rangle$

$(2|\Psi\rangle\langle\Psi| - I)(|\Psi^{\perp}\rangle) = -|\Psi\rangle^{\perp}$

$\downarrow$

state $\perp^{n}$ to $|\Psi\rangle$

state orthogonal to $|\Psi\rangle$

$\Rightarrow (2|\Psi\rangle\langle\Psi| - I)$ is a reflection about $|\Psi\rangle$ itself on this plane

$\Rightarrow \hat{G}$ = Product of 2 reflection on this plane

= Rotation

- Rotation by an angle θ on the $|\alpha\rangle - |\beta\rangle$ plane

- Rotation by an angle θ on the $|\alpha\rangle - |\beta\rangle$ plane

where $\frac{\theta}{2} = \cos^{-1}\left[\sqrt{\frac{N-M}{N}}\right]$

Lec 35 Grover search Algorithm 2

Recall :- Grover search algorithm

$\lceil N \rceil \rightarrow$ ceiling function

smallest integer that is $\geq N$

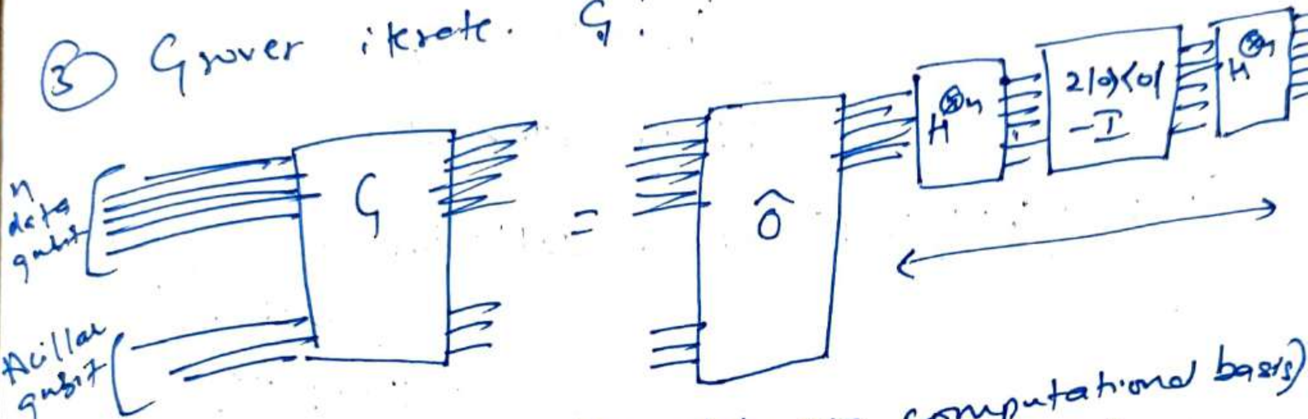
$\lfloor 2^{n} \rfloor \rightarrow$ floor function
Largest integer smaller than 2^{n}

$N \leq 2^n$

(1) Prepare data qubit in $|0\rangle^{\otimes n}$.

(2) $H^{\otimes n}$ $\quad \Psi = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$

(3) Grover iterate. $\hat{G}$:



(4) Measurement (in the std. or computational basis)

* 2d space spanned by $|\alpha\rangle$, $|\beta\rangle$

$|\alpha\rangle$ → nonsolution state

$|\beta\rangle$ → solution state

Let M be the # of solutions to the search problem

S = set of all solutions / $\sim S$ = set of all non-solution states.

$|x\rangle \in S \Leftrightarrow |x\rangle$ is a soln.

$|x\rangle \in \sim S \Leftrightarrow |x\rangle$ is not solution

2-d subspace

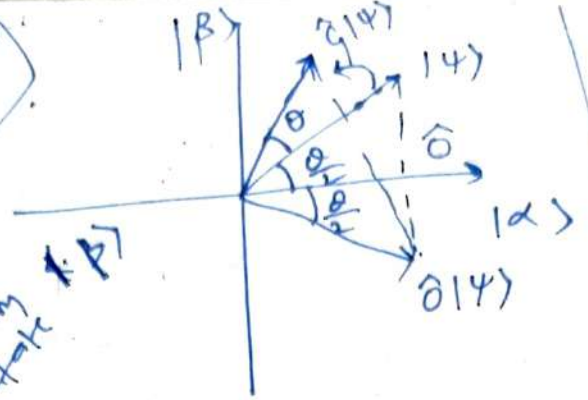
$$\begin{cases} |\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \sim S} |x\rangle \\ \beta = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle \end{cases}$$

$\langle \alpha | \beta \rangle = 0$

$\langle \alpha | \alpha \rangle = \langle \beta | \beta \rangle = 1$

$\hat{G} = (2|\psi\rangle\langle\psi| - I)\hat{O}$

solution state $|\beta\rangle$



$\hat{G}|\psi\rangle$ is a rotation of $|\psi\rangle$ by an angle θ!

Initial state $|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$

$= \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{2}}$$

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

- $\hat{O}|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle - \sin\left(\frac{\theta}{2}\right)|\beta\rangle$

Reflection about $|\alpha\rangle$ axis on the 2-d plane spanned by $\{|\alpha\rangle, |\beta\rangle\}$

Recall oracle (computationally easy) marks all the solution states verifies whether $|x\rangle$ is a solution or not

$f(x) \rightarrow \hat{O}|x\rangle = (-1)^{f(x)}|x\rangle$

$f(x) = 1$ iff $|x\rangle \in S$

- $H^{\otimes n}(2|0\ldots0\rangle\langle0\ldots0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$

generally, this is a reflection about $|\psi\rangle$ on the $|\alpha\rangle$-$|\beta\rangle$ plane

$\Rightarrow \hat{G}|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{3\theta}{2}\right)|\beta\rangle$

- Apply $\hat{G}$ k times $\Rightarrow (\hat{G})^k$:

$$\hat{G}^k |\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|\beta\rangle$$

Exercise In the $\{|\alpha\rangle, |\beta\rangle\}$ basis, show that $\hat{G}$ is a rotation matrix, which states any vector in $\{|\alpha\rangle, |\beta\rangle\}$ plane by angle θ.

- final state: $\cos\left(\frac{(2k+1)\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|\beta\rangle$

measured in $\{|x\rangle\}$ basis

$|\text{coeff of } |\beta\rangle|^2 \equiv$ Probability of finding a soln.

* Performance of the algorithms:

starting with $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$

- rotating by $\cos^{-1}\left(\sqrt{\frac{M}{N}}\right)$ radians takes $|\psi\rangle$ to $|\beta\rangle$
- Each step of Grover search algorithm rotates by θ
- # of times we need to run Grover $= \left\lceil\left(\frac{\cos^{-1}\sqrt{\frac{M}{N}}}{\theta}\right)\right\rceil$

Get to within $\frac{\pi}{4}$ of $|\beta\rangle$

$\cos\left(\frac{\pi}{4}\right)|\alpha\rangle + \sin\left(\frac{\pi}{4}\right)|\beta\rangle \Rightarrow$ with prob-ty $\frac{1}{2}$ the algo. vector a soln.

$- M << N \qquad \sin\theta = \sqrt{\frac{M}{N}} << 1$

$$\cancel{\theta <<} \; \frac{\theta}{2} \approx \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

$$\therefore \boxed{\theta \approx 2\sqrt{\frac{M}{N}}} \quad — (1)$$

* Bound on R: $\cos\sqrt{\frac{M}{N}} \leq \frac{\pi}{2}$

$$R \leq \left\lceil \frac{\pi}{2\theta} \right\rceil \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil \approx O\left(\sqrt{\frac{N}{M}}\right)$$

equivalent, say, $M < \frac{N}{2}$. Then $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$.

then $\frac{\theta}{2} > \sqrt{\frac{M}{N}}$

\# of queries to the oracle $\leq O\left(\sqrt{\frac{N}{M}}\right)$

compare with classical case \# of queries $= O\left(\frac{N}{M}\right)$

$\Rightarrow$ Quadratic speedup!

* what if $M > \frac{N}{2}$?

→ Add more dummy indices to your database!

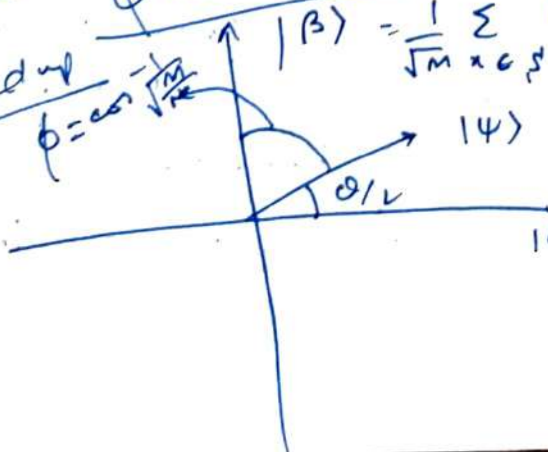
→ M solutions in 2N entries.

→ $M \leq \frac{\tilde{N}}{2}$ → all previous argument go through!

Lec 36: Quantum fourier transforms

Grover speedup

$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$ → uniform superposition of the soln state



$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x} |x\rangle$

$x \in \sim S$

(not a soln.)

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \sqrt{\frac{N-M}{N}}\, |\alpha\rangle + \sqrt{\frac{M}{N}}\, |\beta\rangle$$

Starting overlapping with the "soln. axis $\frac{1}{2}\cos^{-1}\sqrt{\frac{M}{N}}$

- Each query to the oracle / each run of the Grover iteration

$$\underbrace{\hat{G} = (2|\Psi\rangle\langle\Psi| - I)\,\hat{O}}$$

rotate the state $|\Psi\rangle$ by angle θ

- How many times should we query the oracle to have a success probability $\geq \frac{1}{2}$?

$$R = \text{closest Integer}\left(\frac{\cos^{-1}\sqrt{\frac{M}{N}}}{\theta}\right) \text{ times}$$

$$= k + \delta \; , \quad 0 \leq \delta \leq 0.5$$

within an angle $\frac{\pi}{4}$ of $|\beta\rangle$ axis

$\Rightarrow$ Angular error $\varepsilon \leq \frac{\pi}{4}$

$$\varepsilon = \underbrace{\cos^{-1}\sqrt{\frac{M}{N}} + \frac{\theta}{2}}_{\left(\frac{I}{2}\right)} - \frac{(2k+1)\,\theta}{2}$$

$$= \cos^{-1}\sqrt{\frac{M}{N}} - k\theta = \delta\theta \leq \frac{\theta}{2} \leq \frac{\pi}{4}$$

(provided, $M \leq \frac{N}{2}$!)

$\therefore \boxed{\varepsilon \leq \frac{\pi}{4}} \Rightarrow$ success probability of finding a soln state $\geq \frac{1}{2}$

* Bound in query complexity?

$$R = \left[\frac{\cos^{-1}\sqrt{\frac{M}{N}}}{\theta} \right] \le \left[\frac{\pi}{2\theta} \right].$$

But, $\frac{\theta}{2} \ge \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$

$$\therefore\ R \le \left[\frac{\pi}{4}\sqrt{\frac{N}{M}} \right] = O\left(\sqrt{\frac{N}{M}}\right)$$

Quantum Query complexity $= O\left(\sqrt{\frac{N}{M}}\right)$

classically $\approx O(N)$

* Is Grover search optimal?? <u>Yes!!</u>

No quantum algorithm that can search with fewer than $\sqrt{N}$ queries

* Gate complexity of algorithm? Hadamard (n-qubit) = $\log(N)$ operation

conditional phase shift $= O(n)$

$$\boxed{\text{Poly}(\log N)}.$$

* <u>Quantum factoring algorithm</u>

(1) Quantum fourier transform
↓
(2) Quantum phase estimation algorithm (eigenvalue of unitary operator)
↓
(3) Quantum order finding algorithm
↓
(4) Quantum factoring algorithm

Recall, Discrete fourier Transformer:

$\vec{x} = x_0, x_1, x_2 \ldots x_{N-1}$ (N complex no.)

$$(I/P) \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} \xrightarrow[DFT]{} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} \rightarrow \text{(fourier space)} \; (O/P)$$

$$\int e^{2\pi xy} f(x)\,dx$$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{jk}{N}} x_j$$

* Quantum fourier transform:-

on basis of an N-dimensional space

$$\left[\,|0\rangle, |1\rangle, \ldots |N-1\rangle\,\right] \; |j\rangle$$

$\downarrow$ QFT

$$|\tilde{k}\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N-1} e^{\frac{2\pi i jk}{N}} |j\rangle$$

Arbitrary vector in the N-dimensional space!

$$|\Psi\rangle = \sum_{j=1}^{N-1} x_j |j\rangle \xrightarrow[QFT]{} \sum_{k=0}^{N-1} y_k |\tilde{k}\rangle$$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}$$

(DFT!)

$$\vec{y} = DFT(\vec{x})$$

* Properties of the QFT:

(i) $\langle \tilde{j} | \tilde{l} \rangle = \delta_{jl} \quad \forall j, l \in [0, N-1]$

$\Rightarrow [\, |\tilde{0}\rangle, |\tilde{1}\rangle, \ldots |\widetilde{N-1}\rangle]$ is also an ON basis!

(ii) QFT is a unitary transformation

$\Rightarrow$ Q. circuit! which need to only $O(n^2)$ gates!

$\left(\begin{array}{l} n = \log N \\ 2^n = N \end{array} \right)$

Check $\langle \tilde{j} | \tilde{l} \rangle = \frac{1}{N} \sum_k e^{2\pi i \frac{lk}{N}} e^{-2\pi i \frac{jk}{N}}$

$= \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i \frac{(l-j)k}{N}} = \underline{\delta_{jl}}$

(sum of roots of unity)

* $[\, |j\rangle] \xrightarrow{QFT} [\, |\tilde{k}\rangle]$

$|\tilde{k}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{jk}{N}} |j\rangle$

$|\tilde{0}\rangle = \frac{1}{N} \sum_{j=0}^{N-1} |j\rangle \longrightarrow$ uniform superposition of the computational basis states!

$\downarrow$

$H^{\otimes n}$!

Lect 37

Lec 37 Quantum Fourier Transformations

* Quantum analysis of the DFT

* Unitary transformation on an n-qubit system space ON basis $[|0\rangle, |1\rangle \ldots |N-1\rangle]$, $N = 2^n$

(computational basis)

$$|j\rangle \longrightarrow |\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle$$

(ON basis)

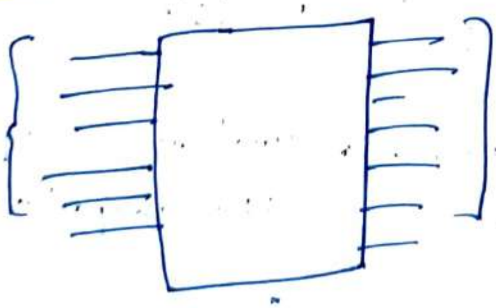
$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

QFT

$$\vec{x} = (x_0, x_2, \ldots x_{N-1}) \xrightarrow[(DFT!)]{QFT} \vec{y} = (y_0, y_1 \ldots y_{N-1})$$

* Circuit for QFT : n-qubit transfer

n-qubit input register



n-qubit output register

* Product form for QFT :

$N = 2^n$

Represent $j = j_1 j_2 \ldots j_n$ $\quad j_i \in [0, 1]$

n-bit binary string that represent $j \in [0, N-1]$

Note : $0.j_l j_{l+1} \cdots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$

(fractional powers of 2)

we will show that $|j\rangle = |j_1 j_2 j_3 \cdots j_n\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$

$$\xrightarrow{QFT} \left(|0\rangle + e^{2\pi i (0.j_n)}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i (0.j_{n-1} j_n)}|1\rangle\right)$$

$$\otimes \cdots \left(|0\rangle + e^{2\pi i (0.j_1 j_2 \cdots j_n)}|1\rangle\right)$$

single qubit state

$$\frac{2^{n/n}}{(\sqrt{n})}$$

"Proof"

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2}} |k_1 \cdots k_n\rangle$$

$$= \frac{1}{2^{n/2}}$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k_1\rangle |k_2\rangle |k_3\rangle \cdots |k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} e^{\frac{2\pi i j k}{2^n}} |k_1\rangle |k_2\rangle \cdots |k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1\rangle |k_2\rangle \cdots |k_n\rangle$$

$$= k = \sum_{l=1}^{n} k_l 2^{n-l} \longrightarrow \frac{k}{2^n} = \sum_{l=1}^{n} k_l 2^{-l}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j \frac{k_l}{2^l}} |k_l\rangle$$

$$= \underline{\frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i \frac{j}{2^l}} |1\rangle \right)}$$ Product form

Last step! $j = \sum_{m=1}^{n} j_m 2^{n-m}$

$$|j\rangle \xrightarrow{QFT} |\tilde{j}\rangle$$

$$= \frac{\bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i \frac{j}{2^l}} |1\rangle \right)}{2^{n/2}}$$

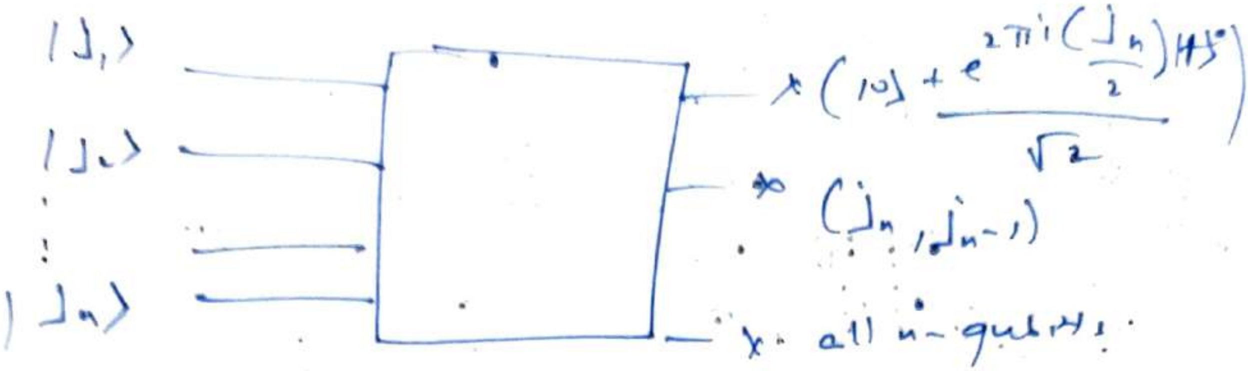
$$= \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i \frac{j}{2}} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i j/2^2} |1\rangle \right)$$

$$= \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i\, 0.j_n} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i (0.j_{n-1} j_n)} |1\rangle \right)$$

$$e^{2\pi i \frac{j}{2}} = e^{2\pi i \frac{\sum_{m=1}^{n} j_m 2^{n-m}}{2}}$$

$$= \underbrace{e^{2\pi i \left(j_1 2^{n-2} + j_2 2^{n-3} + \cdots + \frac{j_n}{2} \right)}}$$

$$= e^{2\pi i \frac{j_n}{2}} = e^{2\pi i (0.j_n)}$$



Lec 37 B

QFT Circuit & Phase-Estimation Circuit

Recall

QFT: $|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle = |\tilde{j}\rangle$

on Basis

(n qubit system
2^n dim space)

$$|\tilde{j}\rangle = (|0\rangle + e^{2\pi i (0.j_n)}|1\rangle) \otimes (|0\rangle + e^{2\pi i (0.j_{n-1} j_n)}|1\rangle) \otimes \cdots$$

$$\otimes \cdots \otimes (|0\rangle + e^{2\pi i (0.j_1 j_2 \cdots j_n)}|1\rangle)$$

$2^{n/2}$

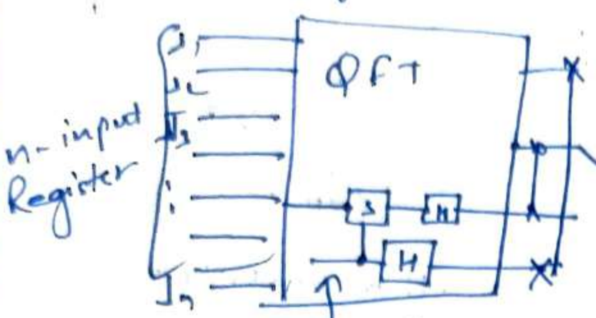
Notation

$$j = j_1 j_2 \cdots j_n = \sum_{l=1}^{n} j_l 2^{n-l}$$

$$0.j_1 j_2 \cdots j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \cdots \frac{j_n}{2^n}$$

$$= \sum_{l=1}^{n} j_l 2^{-l}$$

Circuit for QFT



$$\frac{|0\rangle + e^{2\pi i \frac{j_n}{2}}|1\rangle}{\sqrt{2}}$$

$$|0\rangle + e^{2\pi i \left(\frac{j_{n-1}}{2} + \frac{j_n}{4}\right)}|1\rangle$$

$\downarrow$ H. $\quad \dfrac{|0\rangle \pm |1\rangle}{\sqrt{2}}$

S controlled phase gate

$2\pi i \frac{j_n}{8}$ require a T gate

Define Phase gate

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

$R_0 = I$

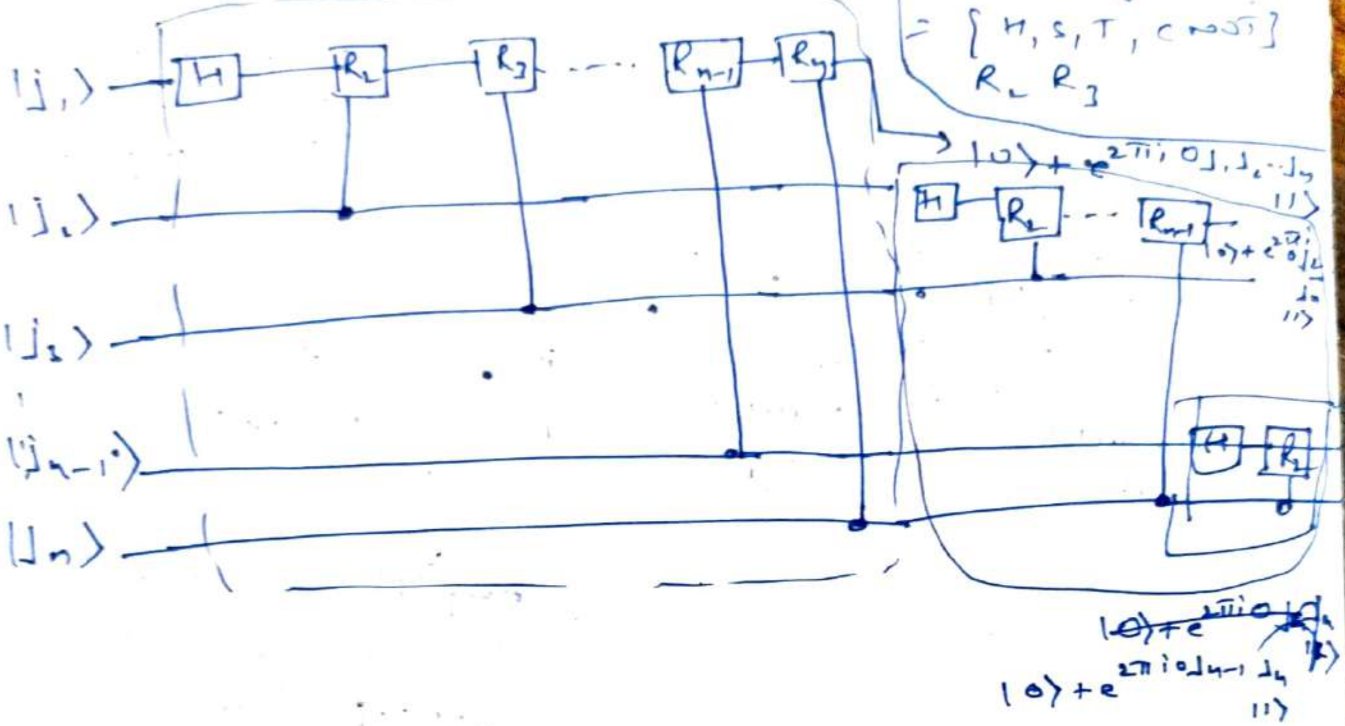
$R_1 = Z \xrightarrow{\text{realized via a}} H$

$R_2 = S$

$R_3 = T$ etc etc

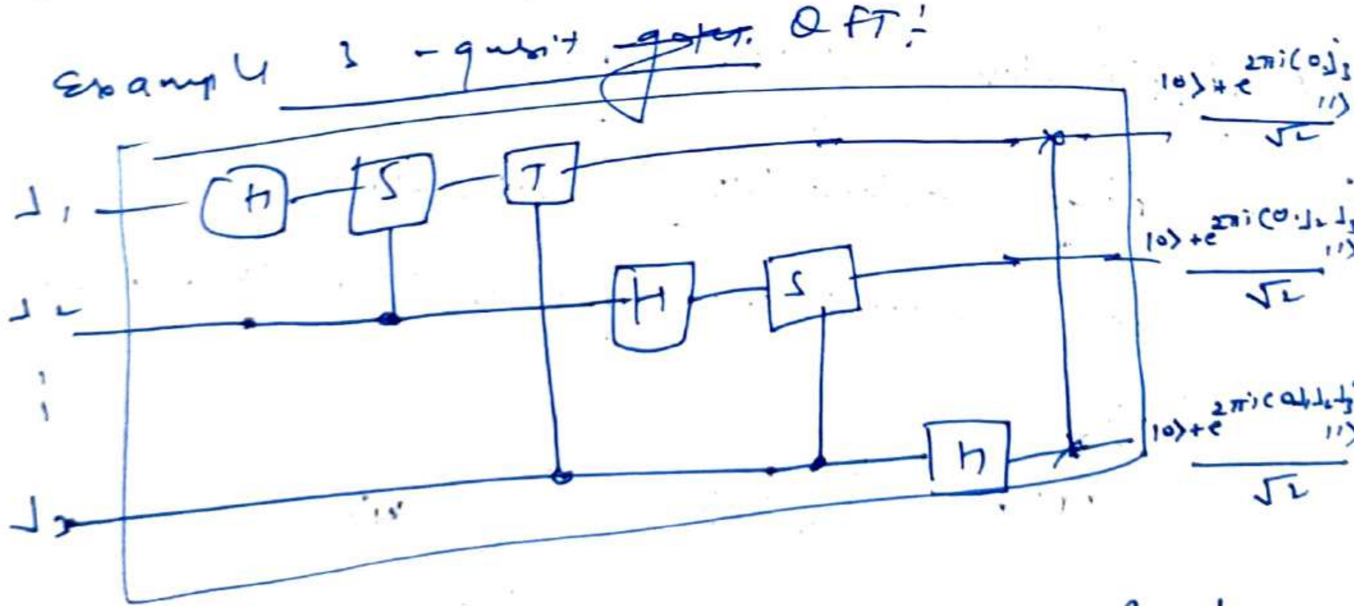
QFT circuit:

Universal gate set = $\{H, S, T, CNOT\}$
R_2 R_3



follow by a set of SWAP gates:

Example 3-qubit ~~gates~~ QFT:



Total # of gate required (gate complexity) $= \frac{n}{2}$ SWAP gates $+ (1 + 2 + \cdots n)$

$= \frac{n(n+1)}{2} + \frac{n}{2}$ gates

$\simeq O(n^2)$ gates!

Classically FFT requires $O(n2^n)$ gate

(exponential speed up in term of gates complexity)

$|j\rangle \;-\!/\!-\; \boxed{QFT} \;-\!/\!-\; |\tilde{J}\rangle \rightarrow R \sum e^{\frac{2\pi i jk}{N}} |k\rangle$

n-qubit state $\quad O(n^2) \quad$ n qubit o/p.

amplitudes are strictly hidden in the superposition

→ need measurement and interferometry

* Application of the QFT

① Phase estimation (subroutine)

Given a unitary operator U with eigenvectors $|u\rangle$

$$U|u\rangle = \lambda_x |x\rangle = e^{2\pi i \phi} |u\rangle$$

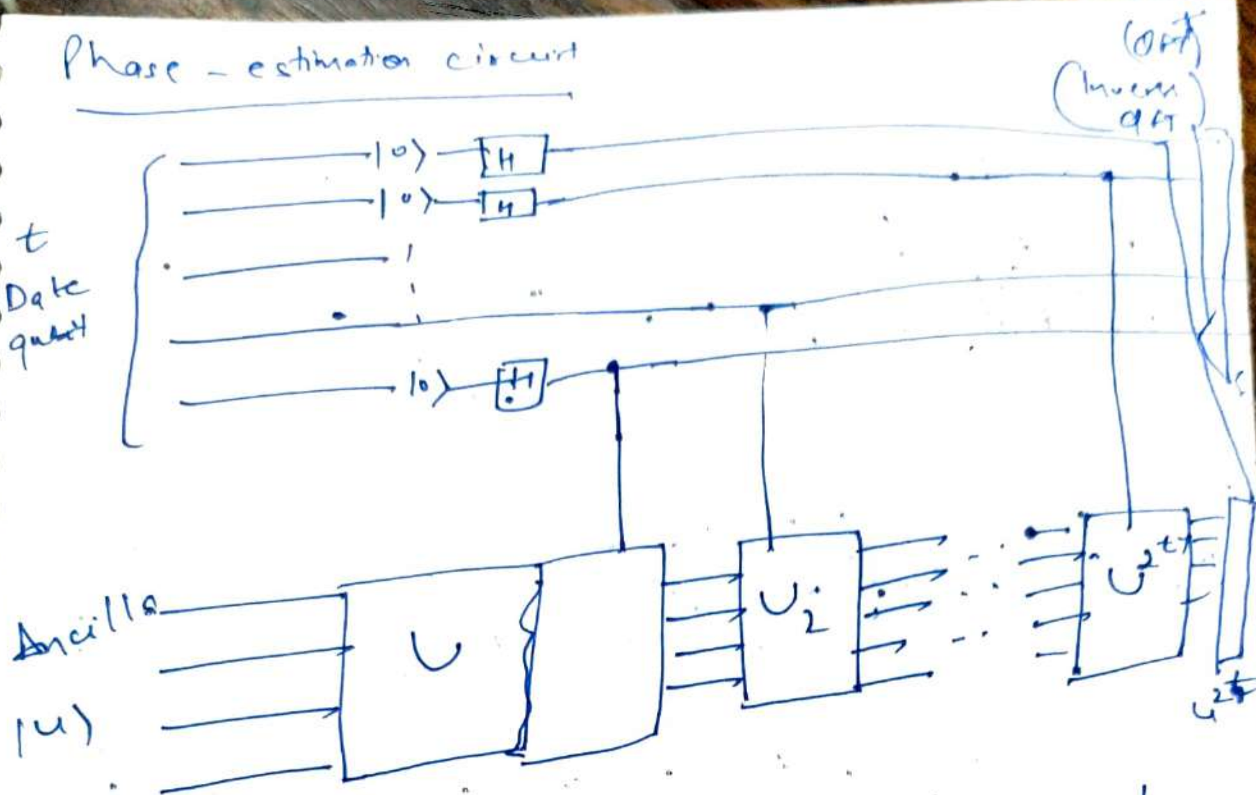
$$(0 \leq \phi \leq 1)$$

ϕ → phase associated with eigenvector $|u\rangle$

Task is to determine / estimate ϕ

- we are given the state $|u\rangle$, U and U^k (power of U)

Phase - estimation circuit



L-39 Phase estimation and order finding

* Problem of phase estimation

$$U|u\rangle = e^{2\pi i \phi}|u\rangle$$

Estimate ϕ, given U and $|u\rangle$

$0 \leq \phi$

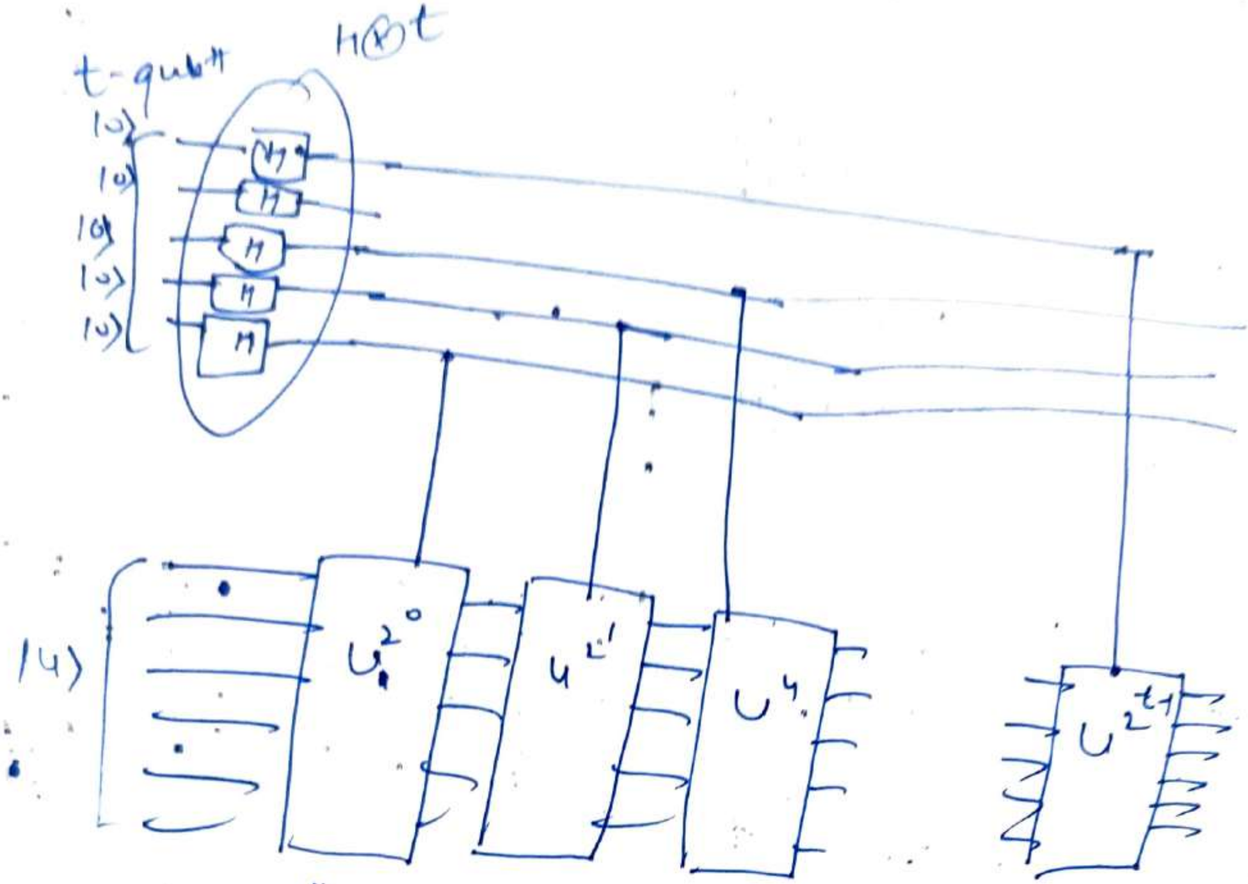
* Circuit for phase estimation :

Say we want estimate ϕ upto 't' bits of accuracy

$$\phi = 0.\phi_1 \phi_2 \phi_3 \ldots \phi_t = \frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \ldots \frac{\phi_t}{2^t}$$

$$\phi_i \in [0,1]$$

- Then we start with "t" data qubits and the ancilla qubits in state $|u\rangle$



On the t^{th} data qubit: $\Lambda(U)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|u\rangle$

Controlled U

$$= \frac{|0\rangle|u\rangle + e^{2\pi i\phi}|1\rangle|u\rangle}{\sqrt{2}}$$

$$= \frac{\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right)}{\sqrt{2}} \otimes |u\rangle$$

On the $(t-1)^{th}$ data qubit $\Lambda(U^2)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|u\rangle$

$$= \frac{|0\rangle|u\rangle + |1\rangle\otimes(U^2|u\rangle)}{\sqrt{2}}$$

$$= \frac{|0\rangle|u\rangle + e^{2\pi i(2\phi)}|1\rangle|u\rangle}{\sqrt{2}}$$

$$= \left(\frac{|0\rangle + e^{2\pi i(2\phi)}|1\rangle}{\sqrt{2}}\right) \otimes |u\rangle$$

* $\Rightarrow$ On the first data qubit, $\lambda(U^{2^{t-1}})\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |u\rangle$

$$= \left(\frac{|0\rangle + e^{2\pi i(2^{t-1}\phi)}|1\rangle}{\sqrt{2}}\right) \otimes |u\rangle$$

$\therefore$ The complete state of the 't' data qubit after $\lambda(U^{2^i})$

$$|0\rangle + e^{2\pi i \cdot 2^{t-1}\phi}$$

$$|0\rangle + e^{2\pi i(0.\phi_t)}|1\rangle$$

[Recall $2^{t-1}\phi = 2^{t-1}\left(\frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \dots + \frac{\phi_t}{2^t}\right)$]

$$\frac{\left(|0\rangle + e^{2\pi i(0.\phi_t)}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i(0.\phi_{t-1}\phi_t)}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i(0.\phi_1\phi_2 \dots \phi_t)}|1\rangle\right)}{2^{t/2}}$$

$\Rightarrow$ Final state of the data qubits

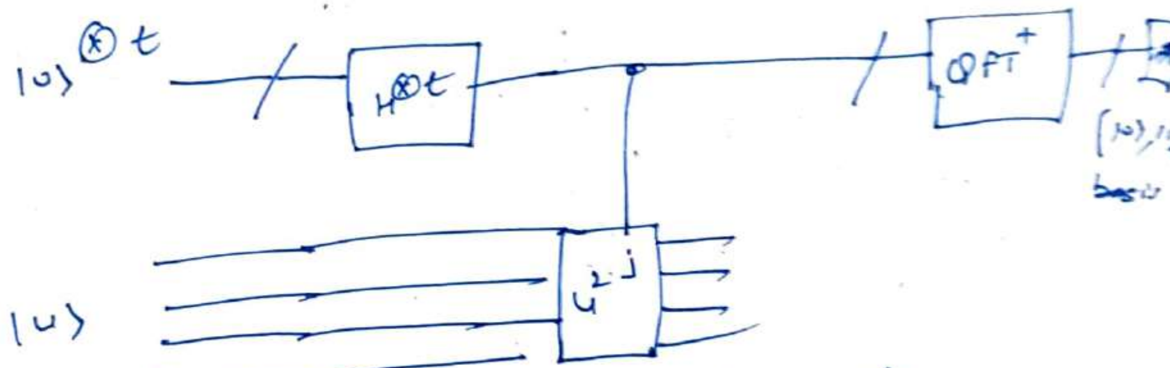
$= QFT\,|\phi_1 \phi_2 \phi_3 \dots \phi_{t-1} \phi_t\rangle$

$= QFT\,|\phi\rangle$

⇒ The last step of phase estimation circuit is to perform an inverse QFT on data qubit and measure

$$(QFT)^{-1} = (QFT)^{\dagger}$$

full schematic of phase-estimation:



(for $0 \le j \le t-1$)

$\wedge (U^{2^j}) \longrightarrow$ modular exponentiation

Box 5.2 (Neilsen / Chuang)

* Performance analysis

$\phi_1, \phi_2, \phi_3 - - \phi_t \longrightarrow \tilde{\phi}$

Suppose we want to estimate ϕ ~~to within~~ ~~an error~~ accurate to n bits, with a probability of success at $(1-\varepsilon)$ then we need

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil \text{ qubits}$$

* final state before QFT:

$\sum_{j=0}^{2^t-1} e^{2\pi i \varphi_j} |j\rangle|u\rangle \xrightarrow[QFT^\dagger]{} |\tilde{\varphi}\rangle|u\rangle$.

(Ideal case)

Phase estimation for Order finding:

order = ?? Given a pair of co-prime integers (no-common factor other than 1)

x and N with $x < N$

* Modular arithmetic with N

$a = c \bmod N$, $a = bN + c$ (residue)

$2 = 5 \bmod 3 = 11 \bmod 3 = 8 \bmod 3$.

$8 = 2 \bmod 3$

(Powers of x) mod N

order of x modulo N is defined to be the smallest the integer 'r' such that $x^r = 1 \bmod N$. (x and N donot have any common factor)

$\Rightarrow (x^r - 1) = 0 \bmod N$

$\Rightarrow x^r - 1$ divide N; $x^r - 1$ is a factor of N!

$(x^{r/2}+1)(x^{r/2}-1)$

crucial step in factoring algorithm.

eg $x = 4$ and $N = 7$ order of $4 \bmod 7 = 3$

$4^0 = 4 \bmod 7$

$4^2 = 2 \bmod 7$

$4^3 = 1 \bmod 7$

show that $1 \le r < N$

[totient function: $\phi(N)$]

$x^1, x^2, \dots, x^{N+1} \rightarrow N$ such numbers.

$0, 1, 2, \dots N-1 \rightarrow$ set of numbers in the group defined by modulo N

$x^s = x^t \bmod N$, $s, t \le N$

$x^{s-t} = 1 \bmod N$, $s-t < N = r < N$

* Problem is to find (smallest) r (order) such that

$x^r = 1 \bmod N$

Given x, N (need L bits to specify N)

say $L \sim \lceil \log N \rceil$

* Classically there is no poly(L) algorithm for order finding!

* Quantum algorithm for order finding

Define U on L-qubits

computation basis $\{|0\rangle, |1\rangle \dots |2^L-1\rangle\}$

$|y\rangle$, $y \in$ L-bit strings $\in [0,1]^{\otimes L}$

$$U_{x,N}|y\rangle = |(xy) \bmod N\rangle$$

L :- 40 Order finding & factoring

Recall :- Order finding :- Given two coprime +ve integer x, N ($x<N$) find the smallest +ve integer r such that $x^r = 1 \bmod N$ ($r<N$)

- Say $L = \lceil \log N \rceil \Rightarrow$ # of bits need to specify N

- consider an L-qubit unitary

$$U_{x,N}|y\rangle = |xy \bmod N\rangle$$

$\downarrow$

computational bases states

$y \in [0, 2^L-1]$

$[0, N-1]$

- U

- $U_{x,N}|y'\rangle = |xy' \bmod N\rangle$

Suppose $xy' \bmod N = xy \bmod N$

$\Rightarrow x(y'-y) \bmod N = 0$

$\Rightarrow y' = y \bmod N$

Action of $U_{x,N}$ is to map each basis state to a distinct state

(ii) output $|xy \bmod N\rangle \in [|0\rangle, |1\rangle, \ldots |N-1\rangle]$

$= [|0\rangle, |1\rangle, \ldots |2^L-1\rangle]$

$U_{x,N} = [|0\rangle, |1\rangle, \ldots |2^L-1\rangle] \to [|0\rangle, |1\rangle \ldots |2^L-1\rangle]$

$\Rightarrow U_{x,N}$ is a permutation matrix!!

$\Rightarrow U_{x,N}$ is a Unitary transformation//

(iii) $U^2_{xy}|y \bmod N\rangle = |x^2 y \bmod N\rangle$

$U^r_{x,N}|y\rangle = |x^r y \bmod N\rangle = |y\rangle \quad \forall y \in [0, 2^L-1]$

$\Rightarrow \boxed{U^r = I}$

eigenvalue of $U_{x,N}$ must be the r^{th} roots of unity!

(N) Note that the eigenstate of $U_{x,N}$ are form.

$|x_1\rangle, |x_2\rangle, \ldots |u_{r-1}\rangle] \to r$ distinct eigenstate

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s \frac{k}{r}} |x^k \bmod N\rangle$$

check $$u|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} |x^{k+1} \bmod N\rangle$$

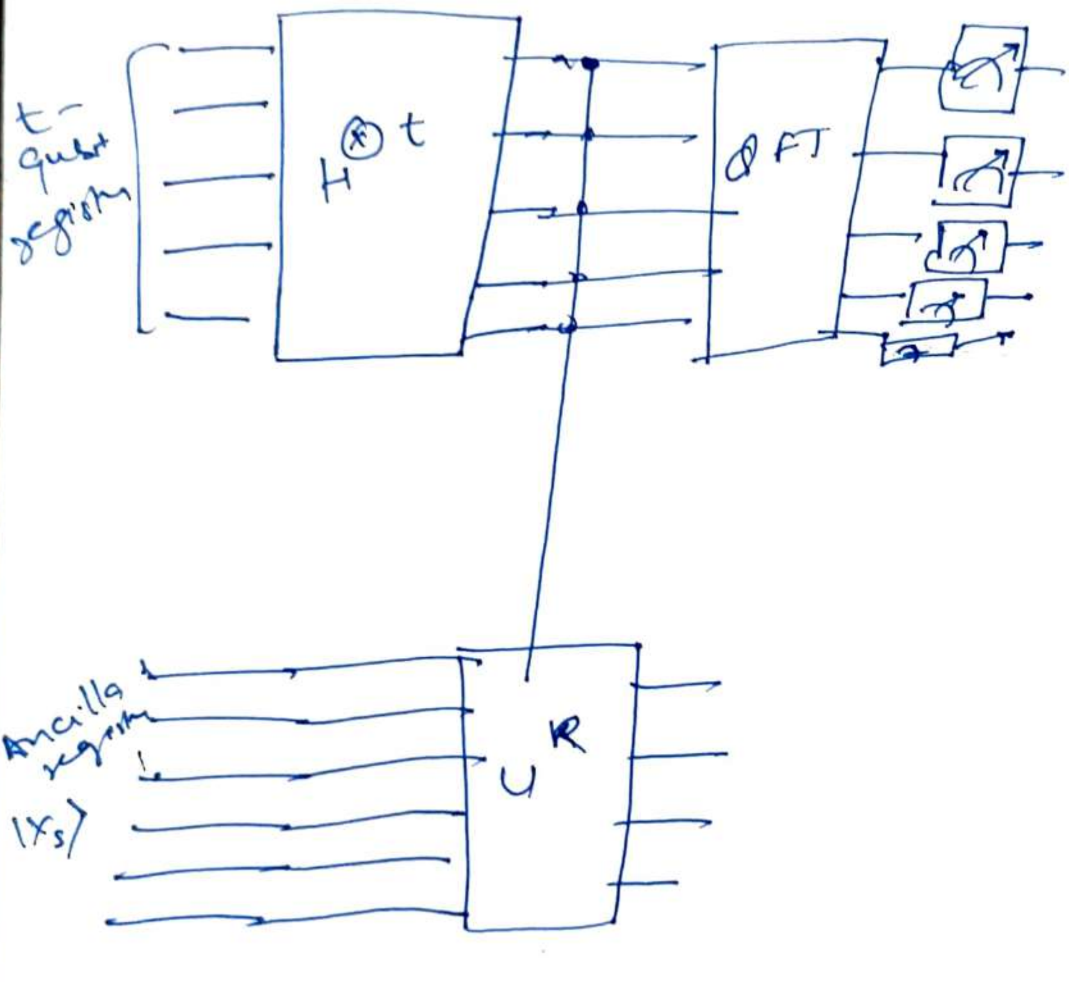
$$= e^{2\pi i s/r} \left[\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i \frac{s(k+1)}{r}} |x^{k+1} \bmod N\rangle \right]$$

$$U|u_s\rangle = e^{2\pi i s/r} |u_s\rangle$$

Phase of the eigenvalues are $\left(\frac{s}{r}\right)$

Route to order finding: Run the phase estimation circuit to obtain the value $\left(\frac{s}{r}\right)$ and hence obtain r. [(involve continued fraction exponential)
sec. 5.3]

* The order finding algorithm :-



* Prepare the ancilla register in a superposition of the eigenstate

consider the uniform superposition:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle$$

$$\text{(check!)} = |1\rangle$$

$$= |0\ldots01\rangle$$

using ⊛ L-bit string

⟹ Resources required:- $L \approx \log N$

$O(L^3)$ algorithm)

- $O(L^3)$ gates to do the $N(L^k)$ operations (modular exponentiation) [Box 5.2 of N & C]

$O(L^3)$ for the continued fraction algorithm classical algo. to estimate r given $(\frac{s}{r})$

poly($\log N$) scaling!! $0 \leq s \leq r-1$

* The factoring algorithm:

Problem: Given the integer N, find its prime factor $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ {m prime factors $p_1, p_2, \ldots p_m$ - $\alpha_1, \alpha_2 \ldots \alpha_m$

(I) classify N is even → return 2 as a factor

(II) If $N = a^b$, return a as a factor (Classical $O(L^3)$ algorithm)

(III) Choose $1 \leq x \leq N-1$
If $GCD(x, N) > 1$, return $GCD(x, N)$ as a factor

(IV) Use order finding to find r such that
$x^r = 1 \bmod N$

Quantum step

If r is even (with high probability) compute the $GCD(x^{\frac{r}{2}} \pm 1, N)$
→ One of these must be a non trivial factor!

→ Resources: $O(L^3)$ gates/operation
$= O((\log N)^3)$