ELEMENTS OF QUANTUM INFORMATION THEORY

Sibasish Ghosh

Optics & Quantum Information Group
The Institute of Mathematical Sciences
C.I.T. Campus, Taramani
Chennai – 600 113

- 'Information' is our knowledge / ignorance about the physical world we are living in.

Examples:

- Under normal atmospheric pressure, ice melts into water at 0°C temperature.
- Plants absorb CO_2 from atmosphere during day time.
- There may be superluminal neutrino particles in our universe.

- In each example, the relevant information is encoded interms of a physical system [e.g., in the constituents of ice] and this information is revealed while processing the physical system by some physical means [e.g., by heating ice].

- Information theory is concerned with storing, processing and transmitting information about physical systems by physical means.

- This leads to the notion:

"Information is physical" and "Physics is all about information"

What is information?

Examples:

(1) Sun will rise tomorrow in the East.

(2) It will rain tonight in Chennai.

- Statement (1) does not contain any useful information as it is a universally valid statement.

- Statement (2) does contain some useful information as it does not rain every night in Chennai.

- Information is all about the probability of occurance of some event [e.g., it will rain tonight in Chennai] — according to Claude Shannon, the inventor of classical information theory.

- Thus the content of information in the following two statements are same:

(3) Three-quarters of Earth's surface is covered by water.

(4) Three-quarters of India's population is below the age of forty years.

- The amount of ignorance we have about the character [land or water] of a chosen portion of Earth's surface is same as the amount of ignorance we have about the age of a person [below forty years or above forty years] from India.

What is information....

- More ignorance we have about an event if the prob. of occurance of the event is less.

Example: • Our ignorance about the event "Sun will rise tomorrow in the East" is nil as this is a certain event.

• We have some amount of ignorance about the event "It will rain tonight in Chennai" as it is neither a certain event nor an impossible event.

- Ignorance gets added for the joint occurance of two independent events.

Example: The ignorance about the event that an Indian woman is below the age of forty years is the sum of the ignorances about the events: (i) a chosen Indian person is a woman and (ii) the person is below the age of forty years.

- Our ignorance about an event should change continuously as we continuously change the probability of occurance of the event.

Example: Ignorance about the event of getting 'head' in tossing a biased coin continuously decreases as the biasedness towards head continuously increases.

- These three considerations led Shannon to define the amount of ignorance $I(p)$ of an event occuring with prob. p as: $I(p) = \log_2\left(\frac{1}{p}\right)$

• Base 2 is related binary expression for information.

What is information ....

- For a situation with N different events $E_1, E_2, \ldots, E_N$ with associated prob. of occurances $p_1, p_2, \ldots, p_N$ respectively, the average amount of ignorance: $\bar{I} = \sum_{i=1}^{N} p_i \log_2\left(\frac{1}{p_i}\right)$

— known as the Shannon entropy $H(p_1, p_2, \ldots, p_N)$ for the prob. distribution $\{p_i\}_{i=1}^{N}$.

Examples:

- In the case of example (1):

E_1 : Sun will rise tomorrow in the East [so $p_1 = 1$]

E_2 : Sun will not rise tomorrow in the East [so $p_2 = 0$]

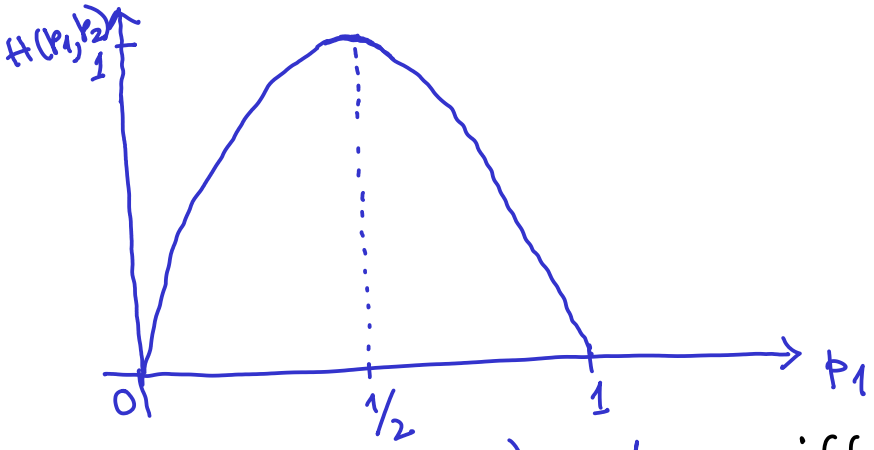
$H(p_1, p_2) = -[1 \times \log_2 1 + \underbrace{0 \times \log_2 0}_{=0}] = 0$

- In the case of example (2):

E_1 : It will rain tonight in Chennai [so p_1 = prob. of occurance of rain tonight in Chennai. Thus $0 < p_1 < 1$]

E_2 : It will not rain tonight in Chennai [so $p_2 = 1 - p_1$]

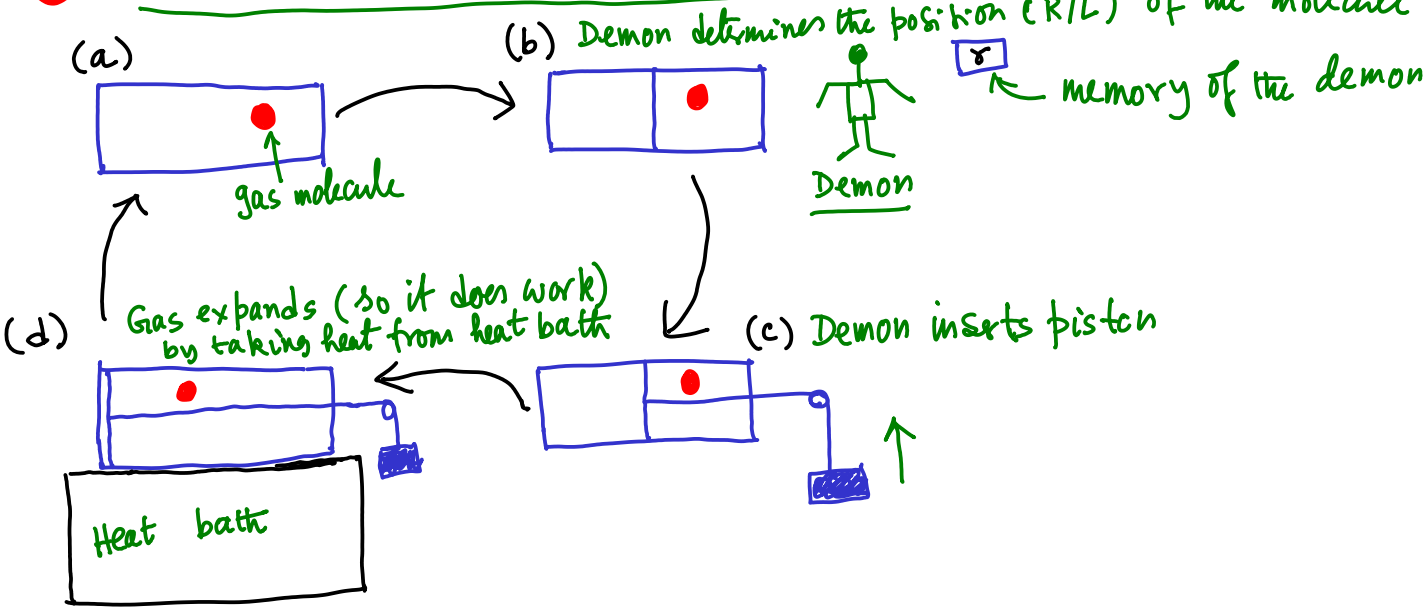
$H(p_1, p_2) = -p_1 \log_2 p_1 - (1-p_1)\log_2(1-p_1)$



- $H_{max}(p_1, p_2, \ldots, p_N) = \log_2 N$ iff $p_j = \frac{1}{N}$ for all j
- $H_{min}(p_1, p_2, \ldots, p_N) = 0$ iff one and only one $p_j = 1$ and all other p_js are zero

Information / Ignorance is physical

- Maxwell's demon [Szilard's engine (1929)]



The device is returned (?) to its initial state and is ready to perform another cycle whose net result is again full conversion of heat into work — a process forbidden by the 2nd law of thermodynamics [as, for isolated system, entropy increases by a thermodynamic process, which is apparently not the case here].

- What happens to the memory of the demon?

- The system will back to its original state only if this memory is erased!

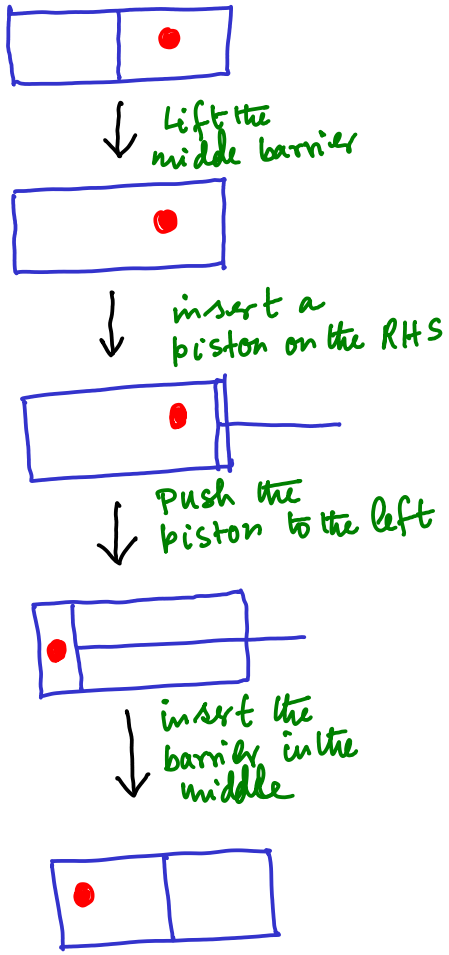
- Landauer's erasure principle:

Erasure of one bit of information costs $kT\ln 2$ amount of energy [k : Boltzman constant, T : temp. of the system]

Information is physical.....

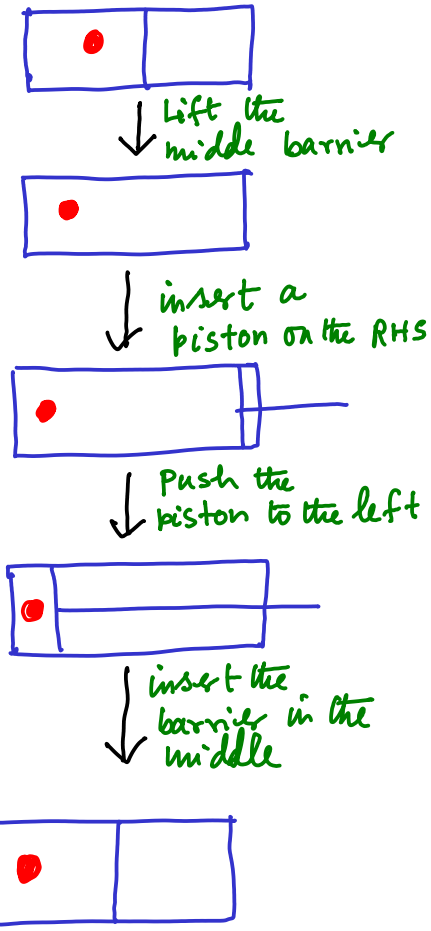
- Erasing one bit of information:

(a) Gas particle is on RHS of the box



We do not know initially on which side (R/L) the gas particle is

(b) Gas particle is on LHS of the box

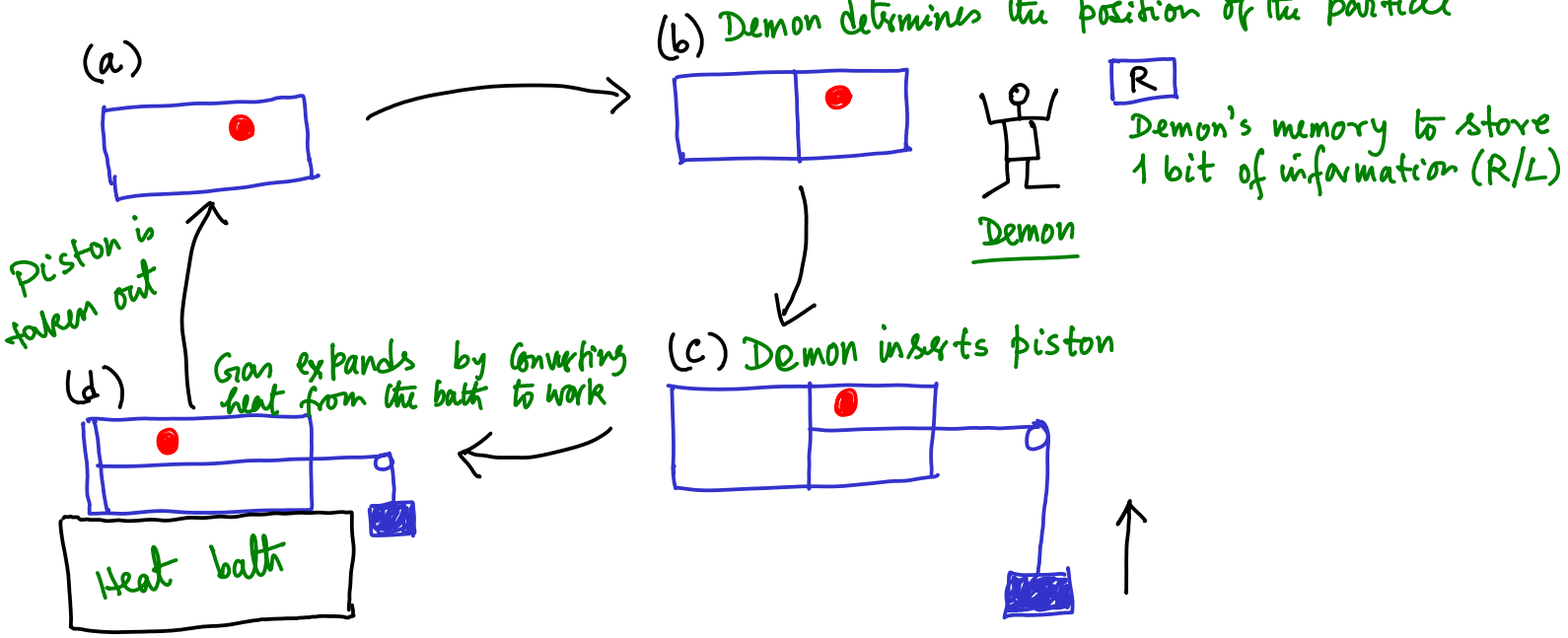


NO information (R/L) about the initial position of the gas particle is there now!

- Compression of the gas particle towards the left by the piston amounts to decrease the thermodynamic entropy of the particle by an amount $k \ln 2$. So the min. work one needs to do on the box (by the piston) is $kT \ln 2$ provided the compression is isothermal and quasi-static. Thus $kT \ln 2$ amount of heat energy is dumped into the environment by the process of compression.
- According to Landauer, the energy cost can not be reduced below this.

Information is physical .....

- Bennett's resolution of the Maxwell's demon (1982):



- The system will convert to its original position only if the memory of the demon is erased. This costs, according to Landauer, an energy of amount $W_{erasure} = -kT\ln 2$.

- Work extracted by the demonic engine in the isothermal expansion of the gas is $W_{extracted} = kT\ln 2$.

- So all the work extracted by the demonic engine needs to be spent to erase one bit of information in the memory of the demon. Thus the net work produced in the cycle is zero!

- Moreover, the erasing process transfers into the environment (i.e., the heat bath) the same amount of heat that was originally extracted from the heat bath to expand the gas. so there is no net flow of heat either!
[2nd law of thermodynamics is saved!]

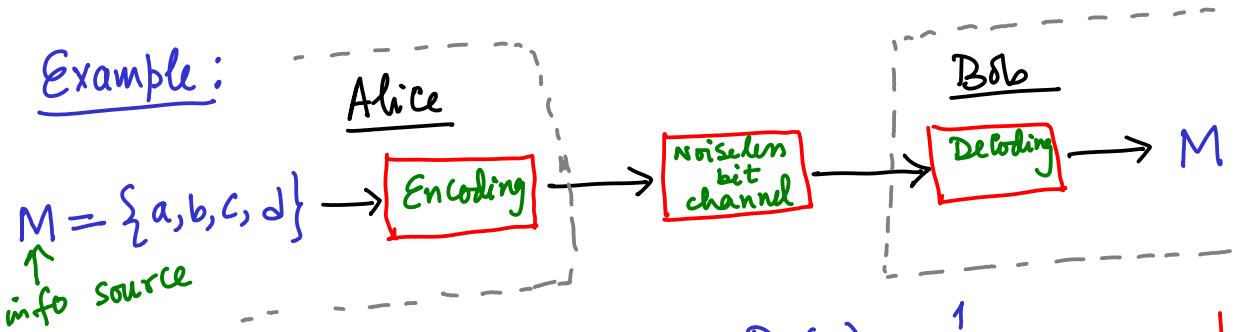
Outline

- Classical information theory
  - Shannon's data compression
  - Shannon's noisy channel coding theorem
- Elements of Quantum Mechanics
  - States
  - Observables
  - Measurements
  - Evolution
- Classical vs quantum information
  - Cbits
  - Qubits
  - Encoding classical info in quantum st.
  - Encoding quantum info in quantum st.
- Extraction of classical information
  - Accesible information
  - Holevo's bound on acc. info
- Quantum noiseless coding theorem
  - Schumacher's data compression
- Theory of entanglement
  - Exact quantum info processing
  - Entanglement concentration
  - Entanglement distillation
- Quantum channels
  - Kraus representation
  - Naimark's dialation
  - Choi – Jamiolkowski isomorphism
- Capacities of quantum channels
  - Classical capacity
  - Entanglement assisted cl. capacity
  - Private capacity
  - Quantum capacity

Classical Information Theory

- Classical information theory deals with storing, processing and sending information about physical systems by means of laws of classical physics.

Example:



Prob. of selecting a from M: $Pr(a) = \frac{1}{2}$, $Pr(b) = Pr(d) = \frac{1}{8}$, $Pr(c) = \frac{1}{4}$

so a is most likely, c is next likely, b, d are least likely

Code words

Encoding 1: $a \equiv 00$, $b \equiv 01$, $c \equiv 10$, $d \equiv 11$ [Blind encoding!]

Expected length of the code word [a measure of performance of the encoding scheme] $= \frac{1}{2} \times 2 + \frac{1}{8} \times 2 + \frac{1}{4} \times 2 + \frac{1}{8} \times 2 = 2$ bits

Encoding 2: $a \equiv 0$, $b \equiv 110$, $c \equiv 10$, $d \equiv 111$ [variable length encoding]

- Any coded sequence of bits [e.g., 00110101111010100010] is uniquely decodable [0 0 110 10 111 0 10 10 0 0 10 $\equiv$ a a b c d a c c a a c]

Expected length of the code word $= \frac{1}{2} \times 1 + \frac{1}{8} \times 3 + \frac{1}{4} \times 2 + \frac{1}{8} \times 3$

$= \frac{7}{4}$ bits

- Incidentally, $H\left(\frac{1}{2}, \frac{1}{8}, \frac{1}{4}, \frac{1}{8}\right) = -\left[\frac{1}{2}\log_2\frac{1}{2} + \frac{2}{8}\log_2\frac{1}{8} + \frac{1}{4}\log_2\frac{1}{4}\right] = \frac{1}{2} + \frac{3}{4} + \frac{1}{2} = \frac{7}{4}$ bits

Classical Information Theory .....

- **Shannon's data compression theorem:** $X_1, X_2, \ldots$ be independent and identically distributed (iid) random variables, distributed according to the r.v. X with value set $M = \{1, 2, \ldots, |M|\}$ and corresponding prob. distribution $Pr(X = m) \equiv p_m$. In order to store reliably values of $(X_1, X_2, \ldots, X_n)$ for large n, in terms of bit strings, $nH(p_1, p_2, \ldots, p_{|M|})$ number of bits is essential.

- The set of all possible values $(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n)$, the sequence $(X_1, X_2, \ldots, X_n)$ can take has cardinality $|M|^n$.

- Out of these sequence of values, a typical sequence will contain np_1 no. of 1, np_2 no. of 2, ..., $np_{|M|}$ no. of $|M|$.

- Total no. of such typical sequences: $\dfrac{n!}{(np_1)! \times (np_2)! \times \cdots \times (np_{|M|})!}$

- Prob. of occurance of any such typical sequence is:
$(p_1)^{np_1} \times (p_2)^{np_2} \times \cdots \times (p_{|M|})^{np_{|M|}}$

- Total no. of bits required to encode all these typical sequences:

$$\log_2 \left[\frac{n!}{(np_1)! \times (np_2)! \times \cdots \times (np_{|M|})!} \right] = \log_2(n!) - \sum_{j=1}^{|M|} \log_2 \{(np_j)!\}$$

(Stirling's approx.)

$$\sim n \log_2 n - n - \sum_{j=1}^{|M|} \left[(np_j) \log_2 (np_j) - np_j \right] = nH(p_1, p_2, \ldots, p_{|M|})$$

- Total prob. of typical sequences: $\dfrac{n!}{(np_1)!\,(np_2)! \cdots (np_{|M|})!} \times (p_1)^{np_1} (p_2)^{np_2} \cdots (p_{|M|})^{np_{|M|}}$

$\longrightarrow 1$ as $n \longrightarrow \infty$

Classical Information Theory .....

- Compression rate $= \frac{\#\text{ of noiseless channel bits}}{\#\text{ of source symbols}} = \frac{nH(p_1, p_2, \ldots, p_{|M|})}{n}$ (for large n)

$= H(p_1, p_2, \ldots, p_{|M|})$

- Thus $H(p_1, p_2, \ldots, p_{|M|})$ may be interpreted as the total no. of bits required to store the compressed data regarding values of large sequence of iid random variables.

- Shannon's source coding theorem tells us that $H(p_1, p_2, \ldots, p_{|M|})$ is the optimal rate!

- Source coding theorem

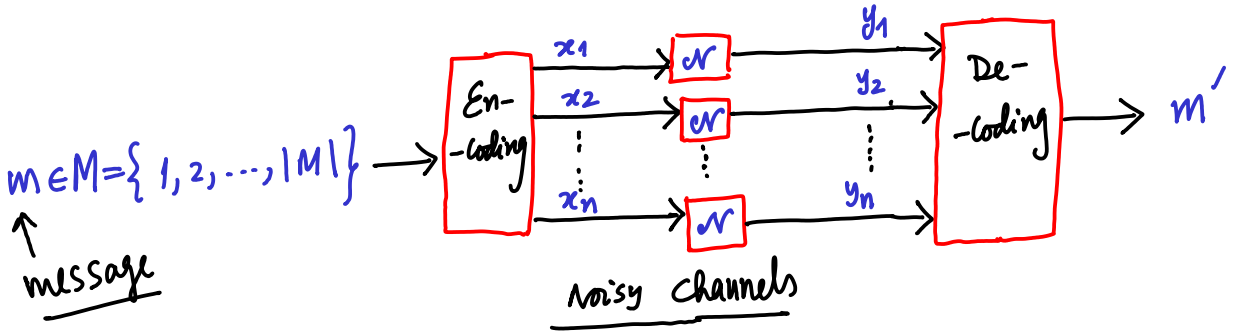
  Direct coding theorem: For a compression rate greater than $H(p_1, p_2, \ldots, p_{|M|})$, there exists a reliable coding scheme with the given compression rate

  Converse theorem: Every reliable compression scheme must have rate greater than $H(p_1, p_2, \ldots, p_{|M|})$

- **Direct coding theorem:** [Using asymptotic equipartition property]

- **Converse theorem:** [Using information theoretic inequalities: To be discussed later]

Shannon's noisy channel coding theorem



$$\text{Rate} = \frac{\#\text{ of message bits}}{\#\text{ of channel uses}} = \frac{\log_2 |M|}{n}$$

n = block length

- If there is a correlation between the inputs x and outputs y of the noisy channel $\mathcal{N}$, one can then transmit any message $m \in M$ through n uses of the channel with vanishing prob. of error $[\Pr(m' \neq m)]$ where the rate $R = \frac{\log_2 |M|}{n}$ is less than the capacity $C(\mathcal{N}) = \max_{\{\Pr(X=x_i)\}_i} I(X;Y)$

$$= \max_{\{\Pr(X=x_i)\}_i} [H(Y) - H(Y|X)]$$

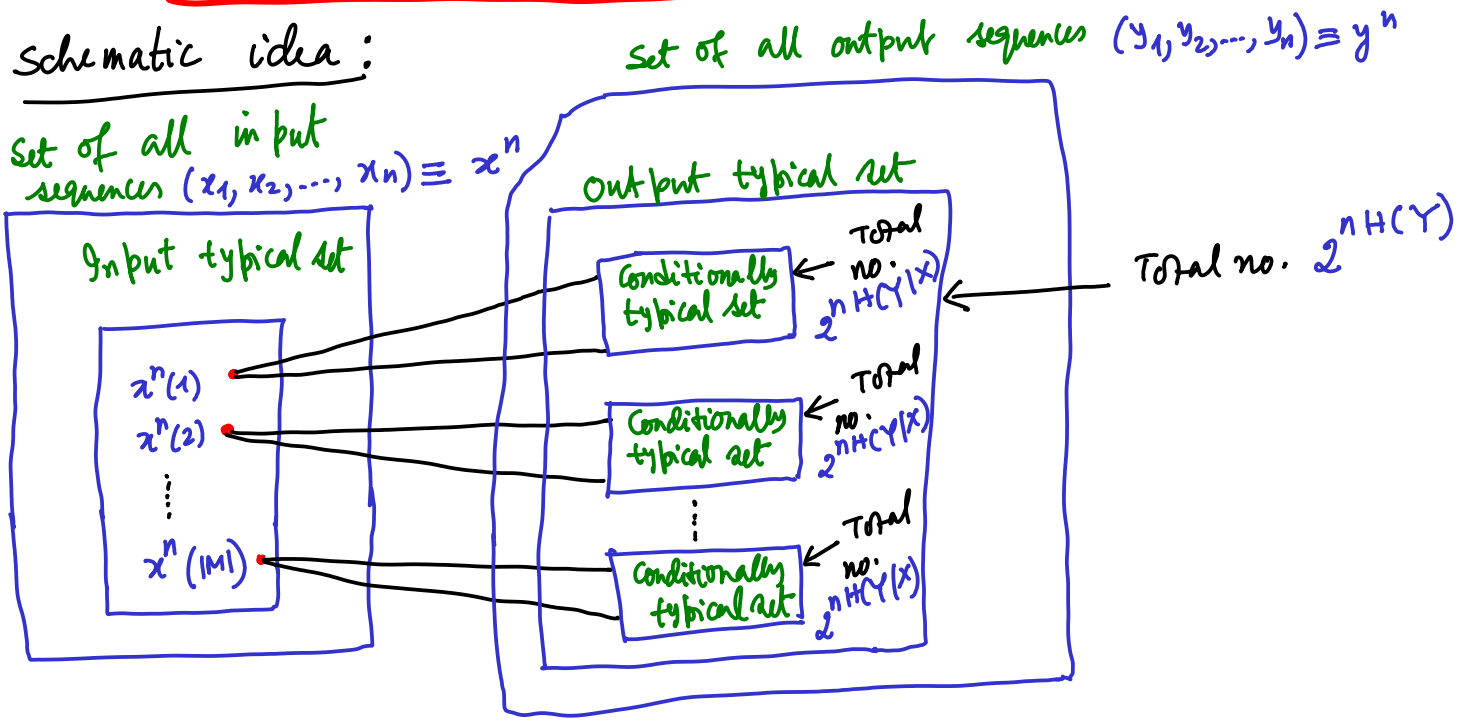
$$= \max_{\{\Pr(X=x_i)\}_i} [H(Y) + H(X) - H(X,Y)]$$

for large block size n.

- Conversely, no transmission of messages $m \in M$ by means of block coding of length n with a rate $R > C(\mathcal{N})$ can be reliable.

Classical Information Theory .....

- Schematic idea:



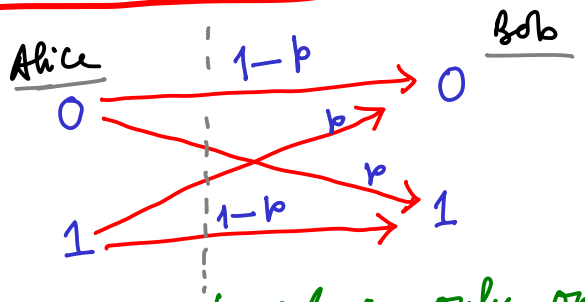
- Conditionally typical sets are disjoint $\Rightarrow$ all the messages can be reliably recovered

So, $$|M| \simeq \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{nI(X;Y)}$$

- Data Compression gets rid of redundancies in the data. Reliable transmission through noisy channel introduces redundancies in the data.

Classical Information Theory.....

- **Binary symmetric channel:**



- **Encoding:** $0 \equiv 000$, $1 \equiv 111$ (000 and 111 are code words)

Majority vote code: only one among the three bits may be corrupted

- Alice sends the code word 000 through three independent uses of the binary symmetric channel

Bob receives		with prob.
000		$(1-p)^3$
001, 010, 100	each	$p(1-p)^2$
011, 101, 110	"	$p^2(1-p)$
111		p^3

If the output is 001, Bob infers the input as 000 by majority vote

- Majority voting performs better than no coding iff the prob. of error in majority voting is less than p, the prob. of error in the case of no coding

prob. of error: $p(e) = p(e|0)\,p(0) + p(e|1)\,p(1)$

same for binary symmetric channel $= 3p^2(1-p) + p^3$

$= [3p^2(1-p) + p^3] \times [\underbrace{p(0) + p(1)}_{=1}]$

$= 3p^2 - 2p^3$

So $3p^2 - 2p^3 < p \iff 0 < p < \frac{1}{2}$ [Rate: $\frac{1}{3}$]

- With encoding: $0 \equiv 000 \equiv 000\ 000\ 000$, $1 \equiv 111 \equiv 111\ 111\ 111$ [Rate: $\frac{1}{9}$]

Prob. of error: $3\{p(e)\}^2 - 2\{p(e)\}^3 = 3(3p^2-2p^3)^2 - 2(3p^2-2p^3)^3$

$= O(p^4)$, much below than p

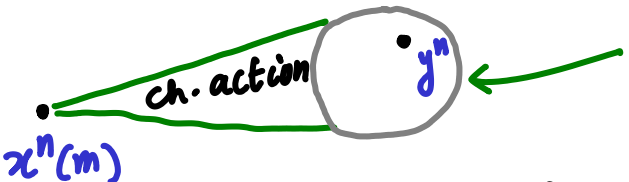
- Lower prob. of error with lower rate (using more bits)!

Classical Information Theory .....

- Can one use a different scheme to transmit classical information through a noisy classical channel with a non-vanishing rate but prob. of error is vanishingly small?

- **Example [Binary symmetric channel]:**

- Message set: $M = \{1, 2, \ldots, |M| = 2^{nR}\}$
- Encoding: 2^{nR} no. of n-bit strings $x_1 x_2 \ldots x_n$ (1)
  $\equiv x^n(1), x^n(2), \ldots, x^n(2^{nR})$
- Apriori prob.: $Pr(x_j = 0) = p_0$, $Pr(x_j = 1) = p_1 = 1 - p_0$ for all j
- So $Pr(x_1(m) = i_1, x_2(m) = i_2, \ldots, x_n(m) = i_n)$
  $= p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_n}$ for $i_1, i_2, \ldots, i_n \in \{0, 1\}$ and $m \in M$
  [For intellegent choice of the input to the channel!]
- $(x_1(m), x_2(m), \ldots, x_n(m)) \xrightarrow[\text{action}]{\text{channel}} (y_1, y_2, \ldots, y_n) \equiv y^n$
  where $y_j \in \{0, 1\}$. [Here $y_j = \mathcal{N}(x_j(m))$ for $j = 1, 2, \ldots, n$]
- Typically, $(y_1, y_2, \ldots, y_n)$ is different from $(x_1(m), x_2(m), \ldots, x_n(m))$ in np places



$\{y^n \in \{0,1\}^n$: Hamming distance of y^n from $x^n(m)$ is $np\}$

y^n is different from $x^n(m)$ in np places

Hamming sphere around $x^n(m)$ of radius np

Classical Information Theory.....

- Total no. of elements in the Hamming sphere: $\frac{n!}{np!\, n(1-p)!}$
  $\simeq$ (Stirling's approximation) $2^{nH(p,1-p)}$ for large n
- Total no. of such Hamming spheres: 2^{nR}
- Total no. of y^n we should concentrate on: total no. of typical y^n sequences $= 2^{nH(Y)}$
  [Y is a random variable with values y]
- The Hamming spheres can be distinguished from each other [to identify & thereby rectify the error] iff

$$2^{nH(Y)} \geq 2^{nR} \times 2^{nH(p,1-p)} \Rightarrow R \leq H(Y) - H(p,1-p)$$

fixed for the channel

- $H(Y) = -\sum_{y=0,1} Pr(Y=y) \times \log_2 Pr(Y=y)$
- $Pr(Y=y) = \sum_{x=0,1} Pr(Y=y \mid X=x)\, Pr(X=x)$, where $Pr(X=x) = p_x$

so $Pr(Y=0) = p_0 \times (1-p) + (1-p_0) \times p$

and $Pr(Y=1) = p_0 \times p + (1-p_0) \times (1-p)$

- $\max_{p_0} H(Y) = 1$, when $p_0 = \frac{1}{2}$
- Thus $\max_{p_0} [\, H(Y) - H(p,1-p)\,] = 1 - H(p,1-p)$
- Capacity of the channel: $1 - H(p,1-p)$ → $H(X,Y) - H(X)$ → $I(X;Y)$

Classical Information Theory (Summary)

- Classical information source is represented by the values $x \in S$ of a random variable X with associated prob. densities $\Pr(X = x) = p_x$.

- The amount of information of a classical information source is given by the Shannon entropy $H(X) = -\sum_{x \in S} p_x \log_2 p_x$ bits.

- The best data compression rate for a classical information source is $H(X)$ bits for storing large sequence of values of X.

- If there is some non-zero correlation, provided by the conditional probabilities $\Pr(Y = y \mid X = x)$, between the input classical information source X and the output classical information source Y under the action of a noisy classical channel $\mathcal{N}$, then the best rate by which large strings of values of X can be sent via the channel with vanishingly small error in decoding, must be bounded above by the capacity $\max_{\{p_x\}_{x \in S}} I(X;Y) \equiv C(\mathcal{N})$ of the channel.

Elements of Quantum Mechanics

QM is a mathematical description of the physical world, based on the following set of axioms:

- **States:** Every quantum mechanical system S is associated with a Hilbert space $\mathcal{H}_S$ and every normalized vector of it is called as a pure state of S, denoted by $|\psi\rangle$.

- **Observables:** Any hermitian operator $A : \mathcal{H}_S \longrightarrow \mathcal{H}_S$ corresponds to an observable for S, denoted by $\hat{A}$.

- **Measurement:** When S is prepared in a state $|\psi\rangle$, measurement of an observable $\hat{A}$ on S gives rise to one of the eigen values a_i of the corresponding hermitian operator A as the measurement outcome with associated probability $|\langle\psi|\psi_i\rangle|^2$, where $A|\psi_i\rangle = a_i|\psi_i\rangle$ (eigenvalue eqn.). The post-measurement state of S: $|\psi_i\rangle$.

- **Dynamics:** If $|\psi(t=0)\rangle$ is the initial state of S, the time-evolved state $|\psi(t=T)\rangle$ is connected to the former by a unitary evolution operator: $|\psi(t=T)\rangle = U(t=0, t=T)\,|\psi(t=0)\rangle$, where $U(t=0, t=T)$ is given by the Hamiltonian of the system, appears in Schrödinger eqn.: $i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$

Elements of QM .....

Example 1: A spin-$\frac{1}{2}$ particle S

- $H_S \equiv \mathbb{C}^2$, two dim. Complex Hilbert space
- State: $|\psi\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = c_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv c_1|0\rangle + c_2|1\rangle$

  with $\langle\psi|\psi\rangle = |c_1|^2 + |c_2|^2 = 1$
- Observable: $A = r_0 \mathbb{1} + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z \equiv r_0\mathbb{1} + \vec{r}.\vec{\sigma}$

  with $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

  and $(r_0, \vec{r}) \in \mathbb{R}^4$.

For spin-$\frac{1}{2}$ observable: $r_0 = 0$ and $|\vec{r}| = 1$. In that case the eigen values of A are ± 1. Here

$$A = \hat{r}.\vec{\sigma} = \underbrace{\sin\theta\cos\phi}_{r_x}\sigma_x + \underbrace{\sin\theta\sin\phi}_{r_y}\sigma_y + \underbrace{\cos\theta}_{r_z}\sigma_z$$

$$= \begin{pmatrix} \cos\theta & \sin\theta e^{-i\phi} \\ \sin\theta e^{i\phi} & -\cos\theta \end{pmatrix} = \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\phi} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{i\phi} & \sin^2\frac{\theta}{2} \end{pmatrix}$$

$$- \begin{pmatrix} \sin^2\frac{\theta}{2} & -\cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\phi} \\ -\cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{i\phi} & \cos^2\frac{\theta}{2} \end{pmatrix} = (+1) \times \underbrace{\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}}_{\to |\psi(\theta,\phi)\rangle} \times \left(\cos\tfrac{\theta}{2}, e^{-i\phi}\sin\tfrac{\theta}{2}\right)$$

$$+ (-1) \times \underbrace{\begin{pmatrix} \sin\frac{\theta}{2} \\ -e^{i\phi}\cos\frac{\theta}{2} \end{pmatrix}}_{\to |\psi(\pi-\theta, \pi+\phi)\rangle} \times \left(\sin\tfrac{\theta}{2}, -e^{-i\phi}\cos\tfrac{\theta}{2}\right)$$

spectral decomposition

$$\equiv (+1) \times |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)| + (-1) \times |\psi(\pi-\theta,\pi+\phi)\rangle\langle\psi(\pi-\theta,\pi+\phi)|$$

orthogonal

- For a general observable: $A = r_0\mathbb{1} + \vec{r}.\vec{\sigma} = r_0\mathbb{1} + |\vec{r}|\,\hat{r}.\vec{\sigma}$

  with $\hat{r} = \vec{r}/|\vec{r}|$

so $A \overset{\text{sp. dec.}}{=\!=} (r_0 + |\vec{r}|)|\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)| + (r_0 - |\vec{r}|)|\psi(\pi-\theta,\pi+\phi)\rangle \times \langle\psi(\pi-\theta,\pi+\phi)|$

Elements of QM.....

- **Measurement:** Initial state of the system: $|\eta\rangle$

  Measurement of the observable A gives:

(i) value $(r_0 + |\vec{r}|)$ with prob. $|\langle\eta|\psi(\theta,\phi)\rangle|^2$ and the post-measurement state is $|\psi(\theta,\phi)\rangle$

(ii) value $(r_0 - |\vec{r}|)$ with prob. $|\langle\eta|\psi(\pi-\theta,\pi+\phi)\rangle|^2$ and the post-measurement state is $|\psi(\pi-\theta,\pi+\phi)\rangle$

- **Dynamics:** Any Hamiltonian of s:

$H = s_0 \mathbb{1} + \vec{s}\cdot\vec{\sigma}$ with $(s_0, \vec{s}) \in \mathbb{R}^4$

Let $H \overset{\text{sp. dec.}}{=\!=} (s_0 + |\vec{s}|)|\psi(\theta',\phi')\rangle\langle\psi(\theta',\phi')| + (s_0 - |\vec{s}|)|\psi(\pi-\theta',\pi+\phi')\rangle\langle\psi(\pi-\theta',\pi+\phi')|$

where $\hat{s} = \vec{s}/|\vec{s}| = (\sin\theta'\cos\phi', \sin\theta'\sin\phi', \cos\theta')$

Unitary evolution operator: $U(t,0) = e^{-itH/\hbar}$ [Assuming H to be time-independent]

$$= \exp\left[-\frac{it}{\hbar}\{s_0\mathbb{1} + |\vec{s}|(\hat{s}\cdot\vec{\sigma})\}\right]$$

$$= \exp\left[-\frac{it s_0}{\hbar}\right] \times \left\{\cos\left(\frac{t|\vec{s}|}{\hbar}\right)\mathbb{1} - i\sin\left(\frac{t|\vec{s}|}{\hbar}\right)(\hat{s}\cdot\vec{\sigma})\right\}$$

$$= \exp\left[-\frac{it s_0}{\hbar}\right] \times \left\{\exp\left[-\frac{it|\vec{s}|}{\hbar}\right]|\psi(\theta',\phi')\rangle\langle\psi(\theta',\phi')| + \exp\left[\frac{it|\vec{s}|}{\hbar}\right]|\psi(\pi-\theta',\pi+\phi')\rangle\langle\psi(\pi-\theta',\pi+\phi')|\right\}$$

Thus $|\eta(t)\rangle = U(t,0)|\eta(0)\rangle$

$$= \exp\left[-\frac{it}{\hbar}(s_0 + |\vec{s}|)\right]\langle\psi(\theta',\phi')|\eta(0)\rangle|\psi(\theta',\phi')\rangle + \exp\left[-\frac{it}{\hbar}(s_0 - |\vec{s}|)\right]\langle\psi(\pi-\theta',\pi+\phi')|\eta(0)\rangle|\psi(\pi-\theta',\pi+\phi')\rangle$$

$(s_0 + |\vec{s}|)$ → eigenvalue of H; $|\psi(\theta',\phi')\rangle$ → post-measurement st.

$(s_0 - |\vec{s}|)$ → eigenvalue of H; $|\psi(\pi-\theta',\pi+\phi')\rangle$ → post-measurement st.

Elements of QM .....

Example 2: One dim. quantum harmonic oscillator S

- **States:** $\mathcal{H}_S \equiv L^2(-\infty, +\infty)$, the space of all square-integrable complex-valued fns on $\mathbb{R}$

$\mathcal{H}_S$ being a separable Hilbert space, there exists a countable complete orthonormal basis $\{|f_n\rangle : n = 0, 1, 2, \ldots\}$ of $\mathcal{H}_S$.

Any state $|\psi\rangle$ of S can be written as: $|\psi\rangle = \sum_{n=0}^{\infty} a_n |f_n\rangle$ with $a_n = \langle f_n|\psi\rangle$

- **Observables:** Any hermitian operator $A : \mathcal{H}_S \longrightarrow \mathcal{H}_S$ [e.g., $A = x_{op}$, the position operator; $A = p_{op}$, the momentum operator; $A = \frac{p_{op}^2}{2m} + \frac{1}{2}m\omega^2 x_{op}^2$, the harmonic Hamiltonian]

- **Measurement:** Measurement of any observable [e.g., the energy observable H, the Hamiltonian], given the initial state of S being $|\psi\rangle$, gives rise to one of the eigenvalues [e.g., one of the energy eigenvalues E] with the collapsed state of S being the corresponding eigenstate [e.g., the energy eigenstate $|E\rangle$] with the associated probability [e.g. $|\langle E|\psi\rangle|^2$]

- **Dynamics:** $H \overset{\text{sp. dec.}}{=\!=} \sum_{n=0}^{\infty} \hbar\omega(n+\frac{1}{2}) |E_n\rangle\langle E_n|$

$\hbar\omega(n+\frac{1}{2}) = E_n$

so $U(t,0)|\psi(0)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle$

$= \sum_{n=0}^{\infty} e^{-iE_nt/\hbar}\langle E_n|\psi(0)\rangle |E_n\rangle$

Elements of QM.....

- **Composite quantum systems:** For any two quantum mechanical systems A and B with associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the composite quantum system $S = A + B$ is associated with the tensor product Hilbert space $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B$.

- **Basis for $\mathcal{H}_S$:** If $\{|\psi_i\rangle\}_{i=1}^{\dim \mathcal{H}_A}$ and $\{|\phi_j\rangle\}_{j=1}^{\dim \mathcal{H}_B}$ be complete ONBs for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, the tensor product basis $\{|\chi_{ij}\rangle \equiv |\psi_i\rangle \otimes |\phi_j\rangle : i = 1, 2, \ldots, \dim \mathcal{H}_A, j = 1, 2, \ldots, \dim \mathcal{H}_B\}$ is a complete ONB for $\mathcal{H}_S$.

- $\langle \chi_{ij} | \chi_{i'j'} \rangle \equiv \langle \psi_i | \psi_{i'} \rangle \times \langle \phi_j | \phi_{j'} \rangle = \delta_{ii'} \times \delta_{jj'}$

- A general state $|\Psi\rangle$ of $\mathcal{H}_S$ can be taken as: $|\Psi\rangle = \sum_{i=1}^{\dim \mathcal{H}_A} \sum_{j=1}^{\dim \mathcal{H}_B} \lambda_{ij} |\chi_{ij}\rangle$ with $\sum_i \sum_j |\lambda_{ij}|^2 = 1$.

- **Inner product:** For any two states $|\Psi\rangle = \sum_i \sum_j \lambda_{ij} |\chi_{ij}\rangle$ and $|\Phi\rangle = \sum_i \sum_j \mu_{ij} |\chi_{ij}\rangle$, we have:

$$\langle \Psi | \Phi \rangle = \sum_i \sum_j \lambda_{ij}^* \mu_{ij}$$

- **Operator action:** Any linear operator T on $\mathcal{H}_S$ can be written as: $T = \sum_l \sum_m t_{lm} A_l \otimes B_m$, where A_l : linear op. on $\mathcal{H}_A$ and B_m : linear op. on $\mathcal{H}_B$ and $t_{lm} \in \mathbb{C}$.

Then $T|\Psi\rangle = \sum_l \sum_m t_{lm} (A_l \otimes B_m) |\Psi\rangle = \sum_l \sum_m \sum_i \sum_j t_{lm} \times \lambda_{ij} (A_l |\psi_i\rangle) \otimes (B_m |\phi_j\rangle)$.

Elements of QM .....

Example 1: Electron of Hydrogen atom:

system A : spatial degree of freedom with $\mathcal{H}_A = L^2(\mathbb{R}^3)$

system B : spin degree of freedom with $\mathcal{H}_B = \mathbb{C}^2$

Thus the Hilbert space of the entire system S is :

$\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B = L^2(\mathbb{R}^3) \otimes \mathbb{C}^2$

- Any state of $L^2(\mathbb{R}^3)$ is a normalized infinite dim. vector of the form $(\ldots, \psi(\vec{r}_\alpha), \ldots, \psi(\vec{r}_\beta), \ldots\ldots, \psi(\vec{r}_\eta), \ldots)^T$ where $\psi(\vec{r}) \in \mathbb{C}$ for any $\vec{r} \in \mathbb{R}^3$
- Any state of $\mathbb{C}^2$ is a normalized two dim. vector of the form $(c_1, c_2)^T$ where $c_1, c_2 \in \mathbb{C}$.
- Thus any product state of $\mathcal{H}_S$ is of the form:

$(\ldots, c_1\psi(\vec{r}_\alpha), c_2\psi(\vec{r}_\alpha), \ldots, c_1\psi(\vec{r}_\beta), c_2\psi(\vec{r}_\beta), \ldots\ldots,$
$c_1\psi(\vec{r}_\eta), c_2\psi(\vec{r}_\eta), \ldots\ldots)^T$, which, in short, is denoted by:

$$\begin{pmatrix} c_1\psi(\vec{r}) \\ c_2\psi(\vec{r}) \end{pmatrix}_{\vec{r}\in\mathbb{R}^3} \leftarrow [\text{a spinor}]$$

- ONB for $\mathcal{H}_S$:

$$\left\{ \begin{pmatrix} \psi_{nlm}(\vec{r}) \\ 0 \end{pmatrix}_{\vec{r}\in\mathbb{R}^3}, \begin{pmatrix} 0 \\ \psi_{nlm}(\vec{r}) \end{pmatrix}_{\vec{r}\in\mathbb{R}^3} : \right.$$

n: principle quantum no., l : azimuthal quantum no.,
m: magnetic quantum no. $\Big\}$

Elements of QM .....

Example 2: Addition of two spin-1/2 angular momenta:

- Spin-1/2 angular momentum operators: $\hat{S}_x, \hat{S}_y, \hat{S}_z$ such that

$$\hat{S}_z \left| j=\tfrac{1}{2}, m=\pm\tfrac{1}{2} \right\rangle = \pm\tfrac{1}{2}\hbar \left| j=\tfrac{1}{2}, m=\pm\tfrac{1}{2} \right\rangle \text{ and}$$

$$\hat{\vec{S}}^2 \left| j=\tfrac{1}{2}, m=\pm\tfrac{1}{2} \right\rangle = (\hat{S}_x^2 + \hat{S}_y^2 + \hat{S}_z^2) \left| j=\tfrac{1}{2}, m=\pm\tfrac{1}{2} \right\rangle$$

$$= \underbrace{j}_{=1/2}(j+1)\hbar^2 \left| j=\tfrac{1}{2}, m=\pm\tfrac{1}{2} \right\rangle$$

- Addition of $\hat{\vec{S}}_1 = (\hat{S}_{1x}, \hat{S}_{1y}, \hat{S}_{1z})$ and $\hat{\vec{S}}_2 = (\hat{S}_{2x}, \hat{S}_{2y}, \hat{S}_{2z})$

$$\hat{\vec{S}} = \hat{\vec{S}}_1 + \hat{\vec{S}}_2 = (\hat{S}_{1x} + \hat{S}_{2x}, \hat{S}_{1y} + \hat{S}_{2y}, \hat{S}_{1z} + \hat{S}_{2z})$$

- J-values for $\hat{\vec{S}}$: 0 and 1 [so $M=0$ for $J=0$ and $M \in \{+1, 0, -1\}$ for $J=1$]

- $\hat{\vec{S}}^2 \left| J, M \right\rangle = J(J+1)\hbar^2 \left| J, M \right\rangle$ and $\hat{S}_z \left| J, M \right\rangle = M\hbar \left| J, M \right\rangle$

- CG coefficients:

$$\left| J=0, M=0 \right\rangle = \underbrace{\frac{1}{\sqrt{2}}}_{\text{CG coeff.}} \times \left| j_1=\tfrac{1}{2}, m_1=+\tfrac{1}{2} \right\rangle \otimes \left| j_2=\tfrac{1}{2}, m_2=-\tfrac{1}{2} \right\rangle - \underbrace{\frac{1}{\sqrt{2}}}_{\text{CG coeff.}} \times \left| j_1=\tfrac{1}{2}, m_1=-\tfrac{1}{2} \right\rangle \otimes \left| j_2=\tfrac{1}{2}, m_2=+\tfrac{1}{2} \right\rangle$$

- Note that $\hat{S}_{1x} + \hat{S}_{2x} \equiv \hat{S}_{1x} \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes \hat{S}_{2x}$, etc.

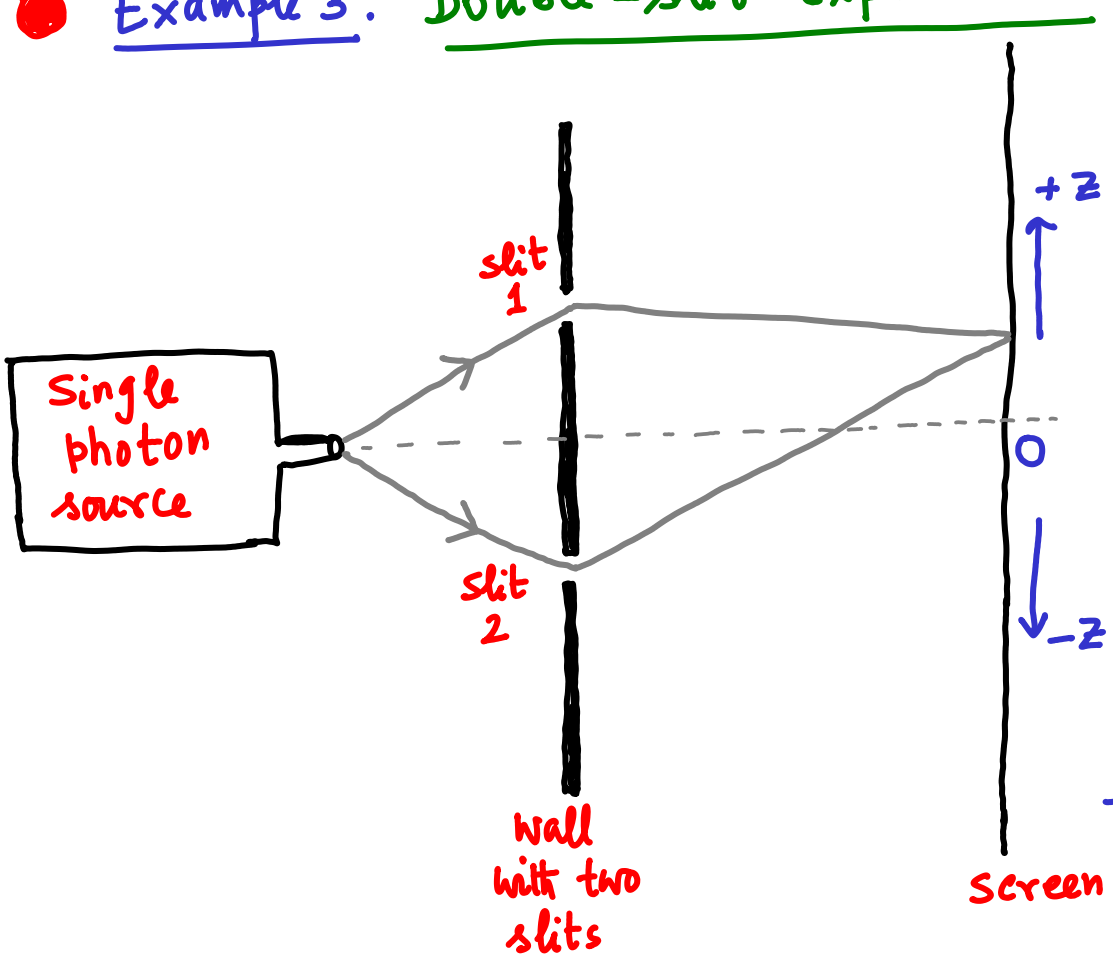
- Thus the Hilbert space $\mathcal{H}_S$ of addition of two spin-1/2 angular momenta is given by:

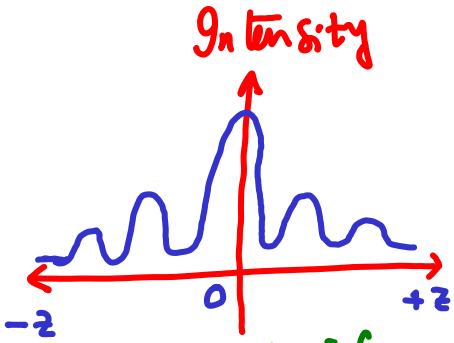
$$\mathcal{H}_S = \mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$$

- $\left| J=0, M=0 \right\rangle$ is called as the <u>singlet state</u>

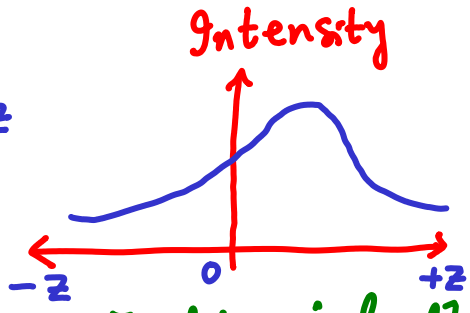
Elements of QM.....

Example 3: Double-slit experiment:





[No slit info. is there]



[slit 2 is closed]

- Proper description of the experiment is possible only when both polarization degree of freedom as well as path degree of freedom [that is whether the particle passes through slit 1 or slit 2]

Thus the Hilbert space of the entire system:

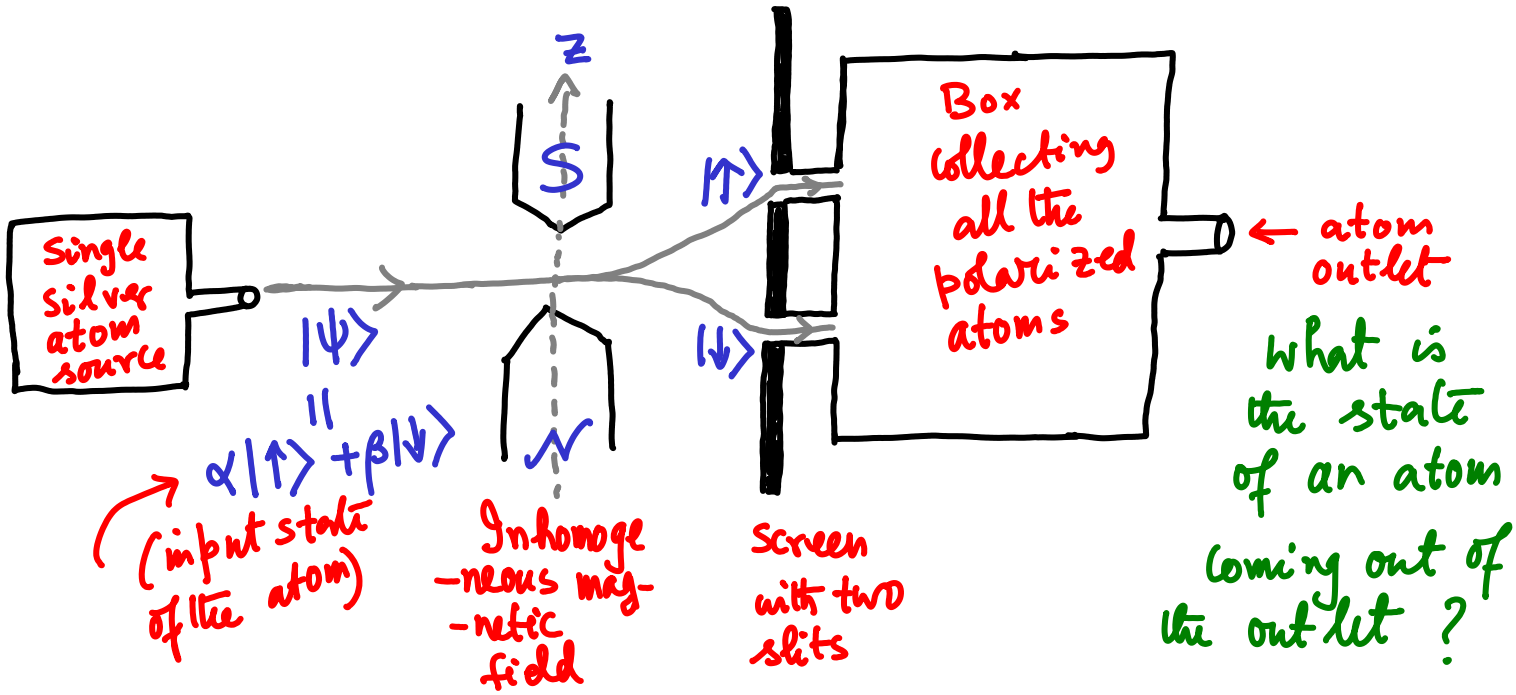
$$\mathcal{H}_S = \mathcal{H}_{polarization} \otimes \mathcal{H}_{path} = \mathbb{C}^2 \otimes \mathbb{C}^2$$

- So, if for example, we want to check whether the photon detected at the screen is polarized vertically and at the same time it passed through slit 1, we need to measure an observable whose one eigenstate is:

$|V\rangle \otimes |slit\,1\rangle$

Elements of QM .....

Noisy quantum systems:



- The state of a single atom coming out of the outlet of the box is: mixture of the state $|\uparrow\rangle$ with weight $|\alpha|^2$ and the state $|\downarrow\rangle$ with weight $|\beta|^2$:

$$|\alpha|^2 |\uparrow\rangle\langle\uparrow| + |\beta|^2 |\downarrow\rangle\langle\downarrow|$$

$|\downarrow\rangle\langle\downarrow|$ → projector on $|\downarrow\rangle$

$|\uparrow\rangle\langle\uparrow|$ → projector on $|\uparrow\rangle$

↳ mixed state

- **Mixed states:** Any linear operator $\rho : \mathcal{H}_S \to \mathcal{H}_S$ with: (i) ρ is hermitian, i.e., $\langle\psi|\rho|\phi\rangle = \overline{\langle\phi|\rho|\psi\rangle}$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}_S$ [we then write: $\rho = \rho^\dagger$];
(ii) ρ is positive operator, i.e., $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}_S$ [we then write: $\rho \geq 0$];
(iii) ρ is normalized, i.e., $\mathrm{Tr}\,\rho \equiv \sum_{i=1}^{\dim \mathcal{H}_S} \langle\psi_i|\rho|\psi_i\rangle = 1$ for any complete ONB $\{|\psi_i\rangle\}_{i=1}^{\dim \mathcal{H}_S}$ of $\mathcal{H}_S$.
- ρ is also called as a density matrix

Elements of QM.....

- **Pure vs. mixed states:** A density matrix ρ of a system S is a pure state if and only if $\rho^2 = \rho$. If a density matrix ρ is not pure, it must be a mixed state, i.e., $\rho^2 < \rho$.

- Any normalized state vector $|\psi\rangle \in \mathcal{H}_S$ corresponds to the pure state $\rho = |\psi\rangle\langle\psi|$, the projector on $|\psi\rangle$.

- **Reduced density matrix:** Joint state of A+B:

$$|\Psi\rangle = \sum_{i=1}^{\dim \mathcal{H}_A} \sum_{j=1}^{\dim \mathcal{H}_B} \lambda_{ij} |\psi_i\rangle \otimes |\phi_j\rangle$$

- Measurement of the observable $\hat{T}_A \overset{\text{sp. decom}}{=\!=} \sum_{k=1}^{\dim \mathcal{H}_A} \mu_k |f_k\rangle\langle f_k|$ on subsystem A: Prob. of occurance of the outcome μ_k:

$$\langle\Psi| \left(|f_k\rangle\langle f_k| \otimes \mathbb{1}_B \right) |\Psi\rangle = \sum_{i,i'=1}^{\dim \mathcal{H}_A} \sum_{j,j'=1}^{\dim \mathcal{H}_B} \lambda_{ij}^* \lambda_{i'j'} \times \langle\psi_i|f_k\rangle \times \langle f_k|\psi_{i'}\rangle \times \langle\phi_j|\mathbb{1}_B|\phi_{j'}\rangle$$

$$= \langle f_k| \left\{ \sum_{j=1}^{\dim \mathcal{H}_B} \left(\sum_{i'=1}^{\dim \mathcal{H}_A} \lambda_{i'j} |\psi_{i'}\rangle \right) \left(\sum_{i=1}^{\dim \mathcal{H}_A} \lambda_{ij'} |\psi_i\rangle \right)^\dagger \right\} |f_k\rangle = \rho_A^{(\Psi)}$$

$$\equiv \langle f_k| \rho_A^{(\Psi)} |f_k\rangle$$

- $$\rho_A^{(\Psi)} = \mathrm{Tr}_B \left[|\Psi\rangle\langle\Psi| \right] = \sum_{j=1}^{\dim \mathcal{H}_B} \langle\phi_j| \Psi\rangle\langle\Psi| \phi_j\rangle$$

$$\rho_B^{(\Psi)} = \mathrm{Tr}_A \left[|\Psi\rangle\langle\Psi| \right] = \sum_{i=1}^{\dim \mathcal{H}_A} \langle\psi_i| \Psi\rangle\langle\Psi| \psi_i\rangle$$

are the reduced density matrices of A and B respectively

Elements of QM.....

POVM vs. PVM: The measurement so far described is a projection-valued measurement:

$\hat{A} \overset{\text{sp. decom.}}{=\!=} \sum_{i=1}^{\dim \mathcal{H}_S} a_i |\psi_i\rangle\langle\psi_i|$

a_i: eigenvalue of $\hat{A}$; $|\psi_i\rangle\langle\psi_i|$: projection on the eigenstate $|\psi_i\rangle$ of $\hat{A}$

- Here $|\psi_i\rangle\langle\psi_i|$s are orthogonal to each other [that is: $\mathrm{Tr}[\,|\psi_i\rangle\langle\psi_i| \times |\psi_j\rangle\langle\psi_j|\,] = \delta_{ij}$]
- Also $\sum_{i=1}^{\dim \mathcal{H}_S} |\psi_i\rangle\langle\psi_i| = \mathbb{1}_{\mathcal{H}_S}$ and the post-measurement state [if a_i is the measurement outcome and the initial state of S being ρ] is $(|\psi_i\rangle\langle\psi_i|\rho|\psi_i\rangle\langle\psi_i|)/\langle\psi_i|\rho|\psi_i\rangle$ $= |\psi_i\rangle\langle\psi_i|$, which occurs with prob. $\langle\psi_i|\rho|\psi_i\rangle$
- A set $M = \{E_j\}_{j=1}^{N}$ of linear operators $E_j : \mathcal{H}_S \to \mathcal{H}_S$ with the properties: (i) $E_j \geq 0$ for all j, (ii) $\sum_{j=1}^{N} E_j = \mathbb{1}_{\mathcal{H}_S}$ is said to be a positive-operator-valued measure (POVM)

  E_js are called POVM elements or effects
- Prob. of occurance of E_j [given the initial state of S being ρ] is $\mathrm{Tr}[\rho E_j]$
- The post-measurement state may be either $(E_j^{1/2}\,\rho\,E_j^{1/2})/\mathrm{Tr}[\rho E_j]$ or something else, depending upon the physical realization of the POVM

Elements of QM.....

Distinguishing two non-orthogonal states in $\mathbb{C}^2$:

$$|\psi_1\rangle = \cos\tfrac{\theta}{2}|0\rangle + \sin\tfrac{\theta}{2}|1\rangle$$
$$|\psi_2\rangle = \cos\tfrac{\theta}{2}|0\rangle - \sin\tfrac{\theta}{2}|1\rangle$$
$$0 < \theta < \tfrac{\pi}{2}, \quad \langle 0|1\rangle = 0, \quad \langle\psi_1|\psi_2\rangle = \cos\theta$$

- Measure the spin-½ observable $\sigma_z \overset{\text{Sp. decom.}}{=\!=} |0\rangle\langle 0| - |1\rangle\langle 1|$:

+1 eigenvalue clicks { for $|\psi_1\rangle$ with prob. $|\langle 0|\psi_1\rangle|^2 = \cos^2\frac{\theta}{2}$; for $|\psi_2\rangle$ with prob. $|\langle 0|\psi_2\rangle|^2 = \cos^2\frac{\theta}{2}$ },

−1 eigenvalue clicks { for $|\psi_1\rangle$ with prob. $|\langle 1|\psi_1\rangle|^2 = \sin^2\frac{\theta}{2}$; for $|\psi_2\rangle$ with prob. $|\langle 1|\psi_2\rangle|^2 = \sin^2\frac{\theta}{2}$ }.

$\Longrightarrow$ Inconclusive decision about the input state

- Measure the spin-½ observable $\sigma_{\hat{n}} \overset{\text{Sp. decom.}}{=\!=} |\psi_1\rangle\langle\psi_1| - |\psi_1^{\perp}\rangle\langle\psi_1^{\perp}|$

where $|\psi_1^{\perp}\rangle = \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle$

+1 eigenvalue clicks { for $|\psi_1\rangle$ with prob. $|\langle\psi_1|\psi_1\rangle|^2 = 1$; for $|\psi_2\rangle$ with prob. $|\langle\psi_1|\psi_2\rangle|^2 = \cos^2\theta$ },

−1 eigenvalue clicks { for $|\psi_1\rangle$ with prob. $|\langle\psi_1^{\perp}|\psi_1\rangle|^2 = 0$; for $|\psi_2\rangle$ with prob. $|\langle\psi_1^{\perp}|\psi_2\rangle|^2 = \sin^2\theta$ }

So the input state must be $|\psi_2\rangle$

$\Longrightarrow$ Partially conclusive decision can be made about the input state

- POVM can make the error prob. of making such partially conclusive decision minimum!

Elements of QM.....

Distinguishing $|\psi_1\rangle$ and $|\psi_2\rangle$ with POVM:

- Choice of POVM: $M = \{E_1, E_2, E_3\}$ with

$E_1 = x|\psi_1^\perp\rangle\langle\psi_1^\perp|$ $\quad E_2 = x|\psi_2^\perp\rangle\langle\psi_2^\perp|$ $\quad E_3 = \mathbb{1} - E_1 - E_2$

where $0 < x < 1$ and $E_3 \geq 0$

- Here $E_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - x\begin{pmatrix} \sin^2\frac{\theta}{2} & -\frac{1}{2}\sin\theta \\ -\frac{1}{2}\sin\theta & \cos^2\frac{\theta}{2} \end{pmatrix} - x\begin{pmatrix} \sin^2\frac{\theta}{2} & \frac{1}{2}\sin\theta \\ \frac{1}{2}\sin\theta & \cos^2\frac{\theta}{2} \end{pmatrix}$

$= \begin{pmatrix} 1-2x\sin^2\frac{\theta}{2} & 0 \\ 0 & 1-2x\cos^2\frac{\theta}{2} \end{pmatrix} \geq 0$ iff $x \leq \frac{1}{2\sin^2\frac{\theta}{2}}$ (< 1)

- If E_1 clicks : the input state must be $|\psi_2\rangle$
  If E_2 clicks : the input state must be $|\psi_1\rangle$
  If E_3 clicks : the input state may be either $|\psi_1\rangle$ or $|\psi_2\rangle$

- Prob. of success: $\frac{1}{2}\mathrm{Tr}[E_1|\psi_2\rangle\langle\psi_2|] + \frac{1}{2}[E_2|\psi_1\rangle\langle\psi_1|]$

$= \frac{1}{2}x\{|\langle\psi_2|\psi_1^\perp\rangle|^2 + |\langle\psi_1|\psi_2^\perp\rangle|^2\}$

$= x\sin^2\theta$, which is 1 when $\theta = \frac{\pi}{2}$ and $x = 1$

$\Rightarrow$ Unambiguous discrimination [in the best possible way] of two non-orthogal states

- Can be extended for more than two linearly independent states

Elements of QM.....

• Physical realization of POVM : [Naimark's dilation Th.]

Given any POVM $M = \{E_i\}_{i=1}^{N}$, acting on the initial state ρ of S, there always exists PVM $\{|\psi_i\rangle\}_{i=1}^{N+N'}$, acting on the state $\rho \otimes |0\rangle_A\langle 0|$ of the extended system $S+A$ [$|0\rangle_A$ being a fixed state of the ancilla system A], such that:

$$\mathrm{Tr}[E_i \rho] = \langle \psi_i | (\rho \otimes |0\rangle_A\langle 0|) |\psi_i\rangle \quad \text{for all } i = 1, 2, \ldots, N$$

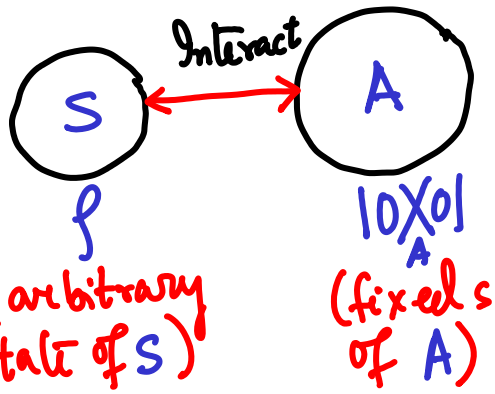
- We say that 'E_i clicks' iff $|\psi_i\rangle$ clicks
- Post-measurement state: $\mathrm{Tr}_A\left[\dfrac{|\psi_i\rangle\langle\psi_i| (\rho \otimes |0\rangle_A\langle 0|) |\psi_i\rangle\langle\psi_i|}{\langle \psi_i | (\rho \otimes |0\rangle_A\langle 0|) |\psi_i\rangle}\right]$
- So, it is not always true that the post-measurement state will be of Lüders-type:

$$\frac{E_i^{1/2} \rho E_i^{1/2}}{\mathrm{Tr}[E_i \rho]}$$

- The most general measurement we encounter in QM is a POVM

Elements of QM.....

• Most general dynamics in QM:



- Interaction Hamiltonian: H_{SA}, acting on states of $\mathcal{H}_S \otimes \mathcal{H}_A$

- Unitary evolution of S+A:

$$\exp\left[-\frac{i}{\hbar} H_{SA} t\right] (\rho \otimes |0\rangle\langle 0|_A) \exp\left[\frac{i}{\hbar} H_{SA} t\right]$$

$$= U(t,0)^\dagger$$

- Ignoring system A:

$$\rho_S^{out}(t) = \mathrm{Tr}_A\left[\exp\left[-\frac{i}{\hbar} H_{SA} t\right] (\rho \otimes |0\rangle\langle 0|_A) \exp\left[\frac{i}{\hbar} H_{SA} t\right]\right]$$

- Time evolution of A:

$$\rho \longmapsto \rho_S^{out}(t) = \sum_{j=1}^{\dim \mathcal{H}_A} A_j(t)\, \rho\, A_j(t)^\dagger$$

with $\sum_{j=1}^{\dim \mathcal{H}_A} A_j(t)^\dagger A_j(t) = \mathbb{1}_{\mathcal{H}_S}$

and $A_j(t) = {}_A\langle j|\, U(t,0)\, |0\rangle_A$ → Kraus operators

$\{|j\rangle_A\}_{j=1}^{\dim \mathcal{H}_A}$: ONB for $\mathcal{H}_A$

Elements of QM.....

Realization a general quantum evolution in terms of unitary evolution:

- Evolution interms of Kraus representation:

$$\rho_S \longmapsto \sum_{i=1}^{N} A_i \rho_S A_i^\dagger \quad \text{with} \quad \sum_{i=1}^{N} A_i^\dagger A_i = \mathbb{1}_{\mathcal{H}_S},$$

the identity operator acting on the system Hilbert space $\mathcal{H}_S$.

- $A_i = \sum_{j,k=1}^{\dim \mathcal{H}_S} a_{ijk} |k\rangle_S\langle j|$: $\{|j\rangle_S\}_{j=1}^{\dim \mathcal{H}_S}$ is an ONB for $\mathcal{H}_S$.

- $\sum_{i=1}^{N} A_i^\dagger A_i = \mathbb{1}_{\mathcal{H}_S} \iff \sum_{i=1}^{N}\sum_{k=1}^{\dim \mathcal{H}_S} a^*_{ijk} a_{ij'k} = \delta_{jj'}$
  (for $j, j' = 1, 2, \ldots, \dim \mathcal{H}_S$)

- $\mathcal{H}_A$: ancilla Hilbert space of dim. N with an ONB $\{|e_\ell\rangle_A\}_{\ell=1}^{N}$

- choose column vectors $\vec{u}_1, \vec{u}_{N+1}, \vec{u}_{2N+1}, \ldots, \vec{u}_{(d-1)N+1}$ in $\mathbb{C}^{dN}$: $\vec{u}_{mN+1} =$

$$\big(a_{1(m+1)1}, a_{2(m+1)1}, \ldots, a_{N(m+1)1}, a_{1(m+1)2}, a_{2(m+1)2}, \ldots, a_{N(m+1)2}, \ldots\ldots, a_{1(m+1)d}, a_{2(m+1)d}, \ldots, a_{N(m+1)d}\big)^T$$

[$m = 0, 1, 2, \ldots, d-1$]

- Orthonormality of $\vec{u}$'s:

$$\vec{u}^{\,\dagger}_{mN+1}\, \vec{u}_{m'N+1} = \sum_{i=1}^{N}\sum_{\ell=1}^{d} a^*_{i(m+1)\ell}\, a_{i(m'+1)\ell} = \delta_{(m+1)(m'+1)}$$

Elements of QM .....

- So we can extend the incomplete ONB $\{\vec{u}_1, \vec{u}_{N+1}, \vec{u}_{2N+1}, \cdots, \vec{u}_{(d-1)N+1}\}$ of $\mathbb{C}^{dN}$ to a complete ONB $\{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_{dN}\}$ of $\mathbb{C}^{dN}$

- Construct the $dN \times dN$ unitary matrix U_{S+A}:

$$U_{S+A} = \left[\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_{dN}\right]$$

($\vec{u}_1$: 1st col., $\vec{u}_2$: 2nd col., $\vec{u}_{dN}$: dN-th col.)

- $\vec{u}_j$ s are column vectors with respect to the product basis: $\{|1\rangle_S \otimes |e_1\rangle_A, |1\rangle_S \otimes |e_2\rangle_A, \cdots, |1\rangle_S \otimes |e_N\rangle_A, |2\rangle_S \otimes |e_1\rangle_A, |2\rangle_S \otimes |e_2\rangle_A, \cdots, |2\rangle_S \otimes |e_N\rangle_A, \cdots, |d\rangle_S \otimes |e_1\rangle_A, |d\rangle_S \otimes |e_2\rangle_A, \cdots, |d\rangle_S \otimes |e_N\rangle_A\}$ ← [Construction has been made so]

- So here: $\underset{A}{\langle} e_i | U_{S+A} | e_1 \rangle_A = A_i$

for $i = 1, 2, \cdots, N$

- Thus for any density matrix ρ_S of S:

$$Tr_A\left[U_{S+A}\left(\rho_S \otimes |e_1\rangle\underset{A}{\langle} e_1|\right) U_{S+A}^{\dagger}\right] = \sum_{i=1}^{N} A_i \rho_S A_i^{\dagger}$$

- Construction of U_{S+A} is not unique!

[As the completion of the ONB $\{\vec{u}_1, \vec{u}_{N+1}, \cdots, \vec{u}_{(d-1)N+1}\}$ to $\{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_{dN}\}$ is not unique]

Elements of QM.....

Non-uniquenes of Kraus operators:

- $\rho_s \longmapsto \sum_{i=1}^{N} A_i \rho_s A_i^\dagger$ with $\sum_{i=1}^{N} A_i^\dagger A_i = \mathbb{1}_{\mathcal{H}_s}$

  ↓ Kraus operators

let $A_i = \sum_{j=1}^{M} u_{ij} B_j$ with $\sum_{j=1}^{M} B_j^\dagger B_j = \mathbb{1}_{\mathcal{H}_s}$ and

$$\sum_{i=1}^{N} u_{ij} u_{ij'}^* \equiv \sum_{i=1}^{N} (U^\dagger)_{j'i} (U)_{ij} = \delta_{j'j}$$

[Thus the $N \times M$ matrix $U = (u_{ij})$ is such that $U^\dagger U$ is equal to the $M \times M$ identity matrix $\mathbb{1}_M$]

- So U is an isometry.
- Here $\rho_s \longmapsto \sum_{i=1}^{N} A_i \rho_s A_i^\dagger = \sum_{i=1}^{N} \sum_{j,j'=1}^{M} u_{ij} u_{ij'}^* B_j \rho_s B_{j'}$

$$= \sum_{j,j'=1}^{M} \delta_{jj'} B_j \rho_s B_{j'}^\dagger = \sum_{j=1}^{M} B_j \rho_s B_j^\dagger$$ with

$$\mathbb{1}_{\mathcal{H}_s} = \sum_{i=1}^{N} A_i^\dagger A_i = \sum_{i=1}^{N} \sum_{j,j'=1}^{M} u_{ij}^* u_{ij'} B_j^\dagger B_{j'}$$

$$= \sum_{j,j'=1}^{M} \delta_{jj'} B_j^\dagger B_{j'} = \sum_{j=1}^{M} B_j^\dagger B_j$$

- So $\{B_1, B_2, \ldots, B_M\}$ is a new set of Kraus operators reproducing the same evolution as done by the set of Kraus operators $\{A_1, A_2, \ldots, A_N\}$
- Thus Kraus operators are not unique!
- $N \leq (\dim \mathcal{H}_s)^2$

Elements of QM.....

- **Character of any physical map allowed by QM:**

- $\mathcal{B}(\mathcal{H}_S)$: Collection of all bounded linear operators on $\mathcal{H}_S$ [$\mathcal{B}(\mathcal{H}_S)$ is a linear space]

- Any linear map $\mathcal{N} : \mathcal{B}(\mathcal{H}_S) \longrightarrow \mathcal{B}(\mathcal{H}_S)$ satisfying:

(i) $\mathcal{N}$ is hermiticity-preserving : $(\mathcal{N}(A))^\dagger = \mathcal{N}(A)$
for all hermitian operators A in $\mathcal{B}(\mathcal{H}_S)$

(ii) $\mathcal{N}$ is trace-preserving : $\mathrm{Tr}[\mathcal{N}(A)] = \mathrm{Tr}\, A$
for all A in $\mathcal{B}(\mathcal{H}_S)$

(iii) $\mathcal{N}$ is positivity-preserving : $\mathcal{N}(A) \geq 0$
for all positive operators A in $\mathcal{B}(\mathcal{H}_S)$

(iv) $\mathcal{N}$ is completely-positive : $(\mathcal{N} \otimes \mathbb{1}_A)(B) \geq 0$
for all positive operators B in $\mathcal{B}(\mathcal{H}_S \otimes \mathcal{H}_A)$
irrespective of the dimension of $\mathcal{H}_A$
[(iv) includes (iii) !]

- Kraus representation satisfies all these properties

- Every physical map, allowed in QM, has a Kraus representation

Elements of QM.....

Motivation behind the properties of quantum map $\mathcal{N}$:

- Linearity of $\mathcal{N}$: Every evolution allowed in QM should be linear [compatible with superposition principle]
- $\mathcal{N}$ is hermiticity-preserving:
- $\mathcal{N}$ is trace-preserving:
- $\mathcal{N}$ is positivity-preserving:

} Every density matrix in $\mathcal{B}(\mathcal{H}_S)$ must be mapped to a density matrix in $\mathcal{B}(\mathcal{H}_S)$

- $\mathcal{N}$ is completely positive: Required to map every bipartite density matrix [when the map acts on one party] to a bonafide density matrix

Example [Transpose map] [$\dim \mathcal{H}_S = 2$]:

- $\rho_S = \sum_{i,j=0}^{1} \rho_{ij} |i\rangle\langle j| \xmapsto{\mathcal{N}} \rho_S^T = \sum_{i,j=0}^{1} \rho_{ji} |i\rangle\langle j|$ [Defn of transpose map]
- so $(\rho_S^T)_{ij} \equiv \sum_{k,l=0}^{1} \mathcal{N}_{ij,kl} (\rho_S)_{kl} = \rho_{ji} = (\rho_S)_{ji}$

$$\Rightarrow \boxed{\mathcal{N}_{ij,kl} = \delta_{il}\delta_{jk}}$$

- $\left((\mathcal{N}(A))^\dagger\right)_{ij} = \left((\mathcal{N}(A))^*\right)_{ji} = A^*_{ji} = A_{ij}$ [if $A^\dagger = A$]

$\Rightarrow$ $\mathcal{N}$ is hermiticity-preserving

Elements of QM .....

- $\mathrm{Tr}\left[\mathcal{N}(A)\right] = \sum_{i=0}^{1} \left(\mathcal{N}(A)\right)_{ii} = \sum_{i=0}^{1} A_{ii} = \mathrm{Tr}(A)$

$\Rightarrow$ $\mathcal{N}$ is trace-preserving

- $\sum_{i,j=0}^{1} x_i^* \left(\mathcal{N}(A)\right)_{ij} x_j = \sum_{i,j=0}^{1} x_i^* A_{ji} x_j \geq 0$ if $A \geq 0$

$\Rightarrow$ $\mathcal{N}$ is positivity-preserving

- Two-qubit state $\rho_{AB} = |\phi^+\rangle\langle\phi^+| = \frac{1}{2}\left[|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |0\rangle\langle 1|_A \otimes |0\rangle\langle 1|_B + |1\rangle\langle 0|_A \otimes |1\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \right]$

with $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$

- $(\mathcal{N}\otimes\mathbb{1})(\rho_{AB}) = \frac{1}{2}\left[\mathcal{N}(|0\rangle\langle 0|_A) \otimes |0\rangle\langle 0|_B + \mathcal{N}(|0\rangle\langle 1|_A) \otimes |0\rangle\langle 1|_B + \mathcal{N}(|1\rangle\langle 0|_A) \otimes |1\rangle\langle 0|_B + \mathcal{N}(|1\rangle\langle 1|_A) \otimes |1\rangle\langle 1|_B \right]$

$= \frac{1}{2}\left[|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 0|_A \otimes |0\rangle\langle 1|_B + |0\rangle\langle 1|_A \otimes |1\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \right]$

$= \frac{1}{2}\left[|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB} + |\psi^+\rangle\langle\psi^+|_{AB} - |\psi^-\rangle\langle\psi^-|_{AB} \right]$

with $|\psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} \pm |10\rangle_{AB}\right)$

$\Rightarrow$ $(\mathcal{N}\otimes\mathbb{1})(\rho_{AB})$ has a negative eigenvalue!

$\Rightarrow$ $(\mathcal{N}\otimes\mathbb{1})(\rho_{AB})$ is not a positive operator

$\Rightarrow$ $\mathcal{N}\otimes\mathbb{1}$ is not a physical map!

- Thus the transpose map is not a completely positive map
- so it is not a physical map!

Elements of QM.....

- **Hughston – Jozsa – Wootters Theorem:** Every mixed state ρ of S has infinitely many pure state ensemble representation.

- $\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|$ with $0 \le p_i \le 1$, $\sum_{i=1}^{N} p_i = 1$ and $|\psi_i\rangle \in \mathcal{H}_S$

- Let $|\psi_i\rangle = \sum_{j=1}^{M} u_{ij} |\phi_j\rangle$ with $|\phi_j\rangle \in \mathcal{H}_S$ and $u_{ij} \in \mathbb{C}$

$$\Rightarrow \rho = \sum_{i=1}^{N} \sum_{j,k=1}^{M} p_i u_{ij}^* u_{ik} |\phi_j\rangle\langle\phi_k|$$

$$= \sum_{j,k=1}^{M} \left(\sum_{i=1}^{N} \left(\sqrt{p_i} u_{ij}\right)^* \left(\sqrt{p_i} u_{ik}\right) \right) |\phi_j\rangle\langle\phi_k|$$

$$= \sum_{j,k=1}^{M} \left(\sum_{i=1}^{N} (U^\dagger)_{ji} (U)_{ik} \right) |\phi_j\rangle\langle\phi_k|$$

with $U_{ik} = \sqrt{p_i} u_{ik}$ for $i = 1, 2, \ldots, N$ and $k = 1, 2, \ldots, M$

- Choose u_{ik}s in such a way that the $N \times M$ matrix $U = \left(\sqrt{p_i} u_{ik}\right)_{\substack{i=1,2,\ldots,N \\ k=1,2,\ldots,M}}$ satisfies:

$$(U^\dagger U)_{jk} = \sqrt{q_j q_k}\, \delta_{jk} \quad \text{with} \quad 0 \le q_j \le 1$$

and $\sum_{j=1}^{M} q_j = 1$

$$\Rightarrow \sum_{i=1}^{N} p_i u_{ij}^* u_{ik} = \sqrt{q_j q_k}\, \delta_{jk} \quad \text{for} \quad j, k = 1, 2, \ldots, M$$

$$\Rightarrow \sum_{i=1}^{N} \left(\frac{\sqrt{p_i} u_{ij}}{\sqrt{q_j}}\right)^* \left(\frac{\sqrt{p_i} u_{ik}}{\sqrt{q_k}}\right) \equiv v_{ik} \text{ (say)} = \delta_{jk}$$

$$\Rightarrow \rho = \sum_{j,k=1}^{M} \sqrt{q_j q_k}\, \delta_{jk}\, |\phi_j\rangle\langle\phi_k| = \sum_{j=1}^{M} q_j |\phi_j\rangle\langle\phi_j|$$

- Thus, considering the unnormalized states $|\tilde{\psi}_i\rangle \equiv \sqrt{p_i}\,|\psi_i\rangle$ [so $\rho = \sum_{i=1}^{N} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$], and thereby considering the transformation:

$$|\tilde{\psi}_i\rangle = \sum_{j=1}^{M} v_{ij}\,|\tilde{\phi}_j\rangle,$$

where $V = (v_{ij})_{\substack{i=1,2,\ldots,N \\ j=1,2,\ldots,M}}$ is an $N \times M$ isometry,

[that is: $V^\dagger V = \mathbb{1}_{M\times M}$]

we get: $\rho = \sum_{j=1}^{M} |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j| \equiv \sum_{j=1}^{M} q_j |\phi_j\rangle\langle\phi_j|$

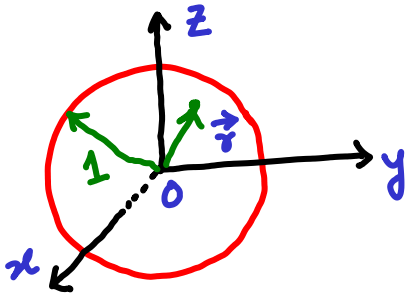
where the normalized states $|\phi_j\rangle$s are related to the unnormalized states $|\tilde{\phi}_j\rangle$s as: $|\tilde{\phi}_j\rangle = \sqrt{q_j}\,|\phi_j\rangle$.

$\Rightarrow$ So there are infinitely many pure state ensemble representations of any given mixed state.

- Example: $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$

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

- Bloch sphere representation of single-qubit system:



$$\rho = \frac{1}{2}(\mathbb{1}_{2\times 2} + \vec{r}\cdot\vec{\sigma})$$

with $|\vec{r}| \leq 1$

Classical vs. Quantum Information

Encoding classical information:

- Classical information [e.g., information about N different objects/events] can always be encoded in terms of distinct states of a physical system described by classical physics.
- It can also be encoded in terms of N pairwise orthogonal states of an N dim. quantum system.
- But, in some cases, it may be more useful to encode classical information in terms of non-orthogonal states of a quantum system [schumacher data compression]
- In order to encode N classical messages, $\log_2 N$ bits are required

Encoding quantum information:

- Quantum information can be encoded in terms of quantum mechanical states
- In order to encode the information about the state ρ of a d dim. quantum system [that is quantum info.], $S(\rho)$ [the von Neumann entropy of ρ] no. of qubits are required — Schumacher data compression limit.

Classical vs. Quantum Information .....

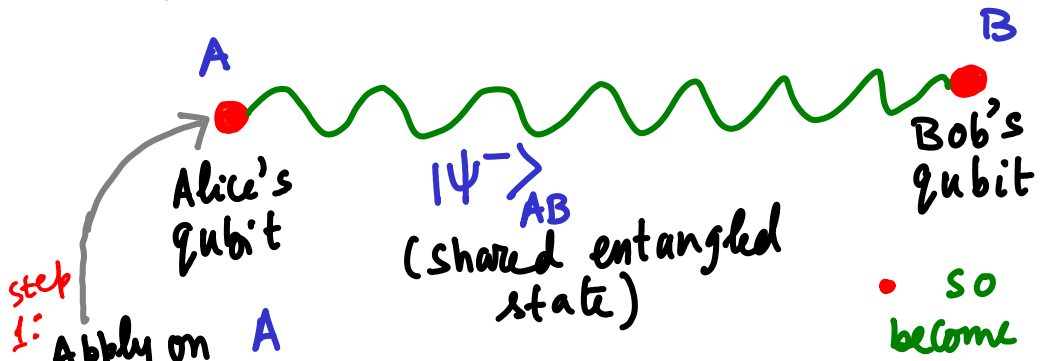
- Encoding classical information in terms of quantum states helps in enhancing efficiency [super dense coding]

- One among four different informations to be sent in a noiseless manner from Alice to Bob

$\Rightarrow$ One of the four two-bits strings 00, 01, 10, 11 needs to be sent

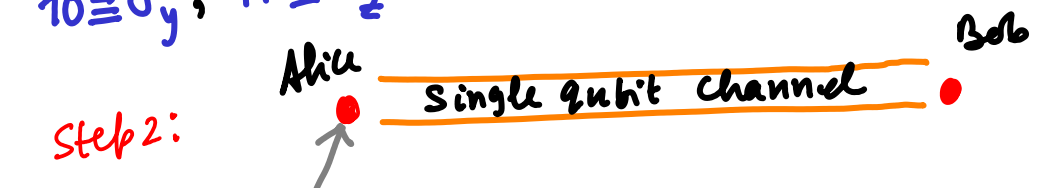
$\Rightarrow$ Requirement of <u>two single bit</u> noiseless channels

- <u>shared entanglement</u> and <u>a single qubit</u> noiseless channel are sufficient



step 1: Apply on A one of the four transformations:
$00 \equiv \mathbb{1}_2$, $01 \equiv \sigma_x$, $10 \equiv \sigma_y$, $11 \equiv \sigma_z$

- so the shared state would become one of $|\psi^-\rangle$, $|\phi^-\rangle$, $|\phi^+\rangle$ and $|\psi^+\rangle$



step 2: Send A to Bob via the single qubit noiseless channel shared between Alice and Bob

- So Bob will now have one of the four states $|\psi^-\rangle$, $|\phi^-\rangle$, $|\phi^+\rangle$ and $|\psi^+\rangle$ in his lab.

Step 3: Bob now performs a two-qubit projective measurement to distinguish the states $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

- So Bob will now get to know which unitary operation [$\mathbb{1}_2$ or σ_x or σ_y or σ_z] was applied by Alice, and hence the communication of the message is done.
- Note that the shared entangled state $|\psi^-\rangle$ alone can not help in communicating the classical message.

1 ebit of shared entanglement + 1 single qubit channel

$\Rightarrow$ communication of 2 classical bits

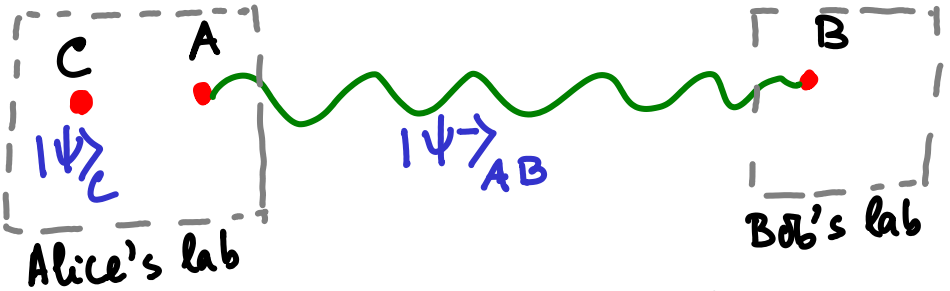
- **Variants of superdense coding:**
  - Shared entangled state is noisy [e.g., it is a mixed st.]
  - Single qubit channel is noisy [e.g., depolarizing channel]

Different capacities of quantum channels take into account these possibilities.

Classical vs. Quantum Information ....

Sending quantum information using shared entanglement and two single-bit communication [Quantum teleportation]:

- Alice wants to send a two-level quantum system C [i.e., qubit], prepared in an arbitrary state $|\psi\rangle_C$ to Bob.



Step 1: Alice performs a projective measurement on C+A in the basis $\{|\psi^-\rangle_{CA}, |\phi^-\rangle_{CA}, |\phi^+\rangle_{CA}, |\psi^+\rangle_{CA}\}$

$$|\psi\rangle_C \otimes |\psi^-\rangle_{AB} = (\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$$

$$= \frac{1}{\sqrt{2}}[|00\rangle_{CA} \otimes \alpha|1\rangle_B - |01\rangle_{CA} \otimes \alpha|0\rangle_B + |10\rangle_{CA} \otimes \beta|1\rangle_B - |11\rangle_{CA} \otimes \beta|0\rangle_B]$$

$$= \frac{1}{2}[|\psi^-\rangle_{CA} \otimes (-\alpha|0\rangle_B - \beta|1\rangle_B) + |\phi^-\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B)$$
$$+ |\phi^+\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) + |\psi^+\rangle_{CA} \otimes (-\alpha|0\rangle_B + \beta|1\rangle_B)]$$

$$= \frac{1}{2}[|\psi^-\rangle_{CA} \otimes \mathbb{1}_2^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B) + |\phi^-\rangle_{CA} \otimes \sigma_x^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)$$
$$- i|\phi^+\rangle_{CA} \otimes \sigma_y^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B) - |\psi^+\rangle_{CA} \otimes \sigma_z^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)]$$

- So the state of B will become: $\mathbb{1}_2^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)$ or $\sigma_x^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)$ or $\sigma_y^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)$ or $\sigma_z^{-1}(\alpha|0\rangle_B + \beta|1\rangle_B)$

Step 2: Alice sends the measurement result $|\psi^-\rangle_{CA} \equiv 00$, $|\phi^-\rangle_{CA} \equiv 01$, $|\phi^+\rangle_{CA} \equiv 10$ or $|\psi^+\rangle_{CA} \equiv 11$ to Bob by using the two-bits noiseless channel. [e.g., using telephone calls]

step3: After receiving the measurement result, Bob applies on B one of the four operations [depending upon the info. about the measurement result of Alice]

$\mathbb{1}_2$, σ_x, σ_y or σ_z.

- so the state of B will now become $\alpha|0\rangle_B + \beta|1\rangle_B \equiv |\psi\rangle_B$, the state Alice wanted to send to Bob!
- Shared entangled state is essential
- Two bits of communication is essential
- The state $|\psi\rangle_C$ of C is completely destroyed
  [so, no violation of no-cloning theorem!]
- C is not sent physically
- NO violation of causality as the average density matrix of B, before applying the unitaries, remains same as initial

1 ebit of shared entanglement + 2 bits of classical communication $\Longrightarrow$ communication of 1 qubit information

- Sharing noisy entanglement and/or noisy bit channels $\Longrightarrow$ noisy qubit channel
  [A topic for Capacities of quantum channels]

Extraction of Classical Information

Encoding classical information in terms of quantum states:

- The states $|\psi\rangle_S = \sum_{j=1}^{d} \alpha_j |j\rangle_S$ of a d dim. quantum system require values of the infinitely many d-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{C}^d$
- So, in principle, information about infinitely many classical messages may be encoded in terms of $|\psi\rangle_S$ s!
- Can we reliably extract all these messages?
- NO! According to Holevo, only $\log_2 d$ bits of different messages may be extracted!
- Example: $0 \equiv |\psi_1\rangle = |0\rangle$, $1 \equiv |\psi_2\rangle = |1\rangle$
  By performing a projective measurement in the basis $\{|0\rangle, |1\rangle\}$ it is possible to reliably know the classical message 0 or 1
- Example: $0 \equiv |\psi_1\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$
  $1 \equiv |\psi_2\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$ [with $0 < \theta < \frac{\pi}{2}$]
  NO measurement can reliably distinguish $|\psi_1\rangle$ and $|\psi_2\rangle$
  So the classical messages can not be reliably extracted!