Basics of Quantum Information and Open Quantum Systems

j.cho@gnu.ac.kr

9 ~ 13 Jan 2023 @ The 20th KIAS-APCTP Winter School on Statistical Physics.

ref) Wilde, QIT. (arXiv: 1106.1445)

Nielsen & Chuang, QC & QI. (2010)

* Classical Shannon theory ┌ noiseless channel coding theorem — data compression
                            └ noisy " — channel capacity

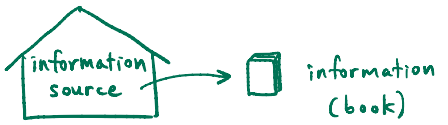
why needed for us? operational meaning of entropies.

Shannon's Noiseless Channel Coding Theorem

~~what is~~ information?

how to describe / quantify.

model



infinite library

(just imagine a file compression
file size of the zip file?)

set of alphabets $\mathcal{X} = \{a, b, c, \cdots\}$.

random variable $X = x$ with probability $p(x)$. $x \in \mathcal{X}$.

information source = random sequence $X^n \equiv X_1 X_2 \cdots X_n$. (n: length).

$X^n = x^n \equiv x_1 x_2 \cdots x_n$ with probability $p(x^n)$

↑ simplified notation

$P_X(x)$, $P_{X^n}(x^n)$, ⋯ → $p(x)$, $p(x^n)$, ⋯

X_i's are i.i.d. (independent and identically distributed)

result as $n \to \infty$, you can encode the message into $nH(X)$ bits.

$$H(X) \equiv -\sum_x p(x) \log p(x)$$ Shannon entropy. ($\log \equiv \log_2$)

ex) $\Pr\{a\} = 1/2$. $\Pr\{b\} = 1/8$. $\Pr\{c\} = 1/4$. $\Pr\{d\} = 1/8$.

method 1 : a → 00, b → 01, c → 10, d → 11. you need 2n bits.

method 2 : a → 0, c → 10, b → 110, d → 111.

01101011 → abcd

# of bits per char $= \frac{1}{2} + \frac{1}{4}\cdot 2 + \frac{1}{8}\cdot 3 \cdot 2 = \frac{7}{4}$. you need $\frac{7}{4}n$ bits.

idea $x^n = x_1 x_2 \cdots x_n$. $n \to \infty$.

$x_i \in \{c_1, c_2, \cdots, c_\alpha, \cdots\}$. $p_\alpha \equiv p(c_\alpha)$.

typical vs atypical sequences.

typical x^n : # of $c_1 \approx np_1$. # of $c_2 \approx np_2$, ⋯

asymptotic equipartition theorem : almose all x^ns are typical .

$$p(\text{typical } x^n) \approx p_1^{np_1} p_2^{np_2} \cdots \quad \text{(all identical)}$$

$$\#\text{ of typical sequences} \approx \frac{1}{p(\text{typical } x^n)}$$

You encode only typical sequences into nR bits . $\boxed{R : \text{compression rate}}$

$p(\text{error}) \to 0$ as $n \to \infty$.

$$nR = \log(|\text{typical set}|) \approx -np_1 \log p_1 - np_2 \log p_2 - \cdots = n\left(-\sum_\alpha p_\alpha \log p_\alpha\right) = nH(X) .$$

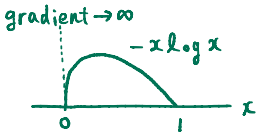
Q) is this optimal? converse theorem.

Shannon Entropy

* random variable $X = x$ with prob. $p(x)$. $\sum_x p(x) = 1$.

$i(x) \equiv \log \frac{1}{p(x)} = -\log p(x)$ information content / surprisal . (by Shannon) .

$H(X) \equiv \langle i(X) \rangle = -\sum_x p(x) \log p(x)$ Shannon entropy . meaning ?



ex) $x \in \{c_1, c_2, \cdots, c_d\}$.

$0 \le H(X) \le \log d$.

$H(X) = 0$ if $p_1 = 1 , p_2 = \cdots = p_d = 0$.

$H(X) = \log d$ if $p_1 = \cdots = p_d = 1/d$. cf) thermodynamic entropy $S = -k \log \Omega$

* two random variables X , Y .

$X = x , Y = y$ with prob $p(x, y)$.

joint entropy

$$H(X,Y) \equiv -\langle \log p(X,Y) \rangle = -\sum_{x,y} p(x,y) \log p(x,y) .$$

if X , Y are independent , $p(x,y) = p(x)p(y)$.

$$H(X,Y) = -\sum p(x)p(y)\left[\log p(x) + \log p(y)\right] = -\sum_x p(x) \log p(x) - \sum_y p(y) \log p(y)$$

$$= H(X) + H(Y)$$ meaning ?

conditional entropy

$$H(X|Y) \equiv -\langle \log p(x|Y) \rangle = -\sum_{x,y} p(x,y) \log p(x|y) = H(X,Y) - H(Y) = \sum_y p(y) H(X|y)$$

conditional probability $p(x|y) \equiv \frac{p(x,y)}{p(y)}$.

$$H(X|Y) = -\sum p(x,y)\left[\log p(x,y) - \log p(y)\right] = H(X,Y) - H(Y)$$

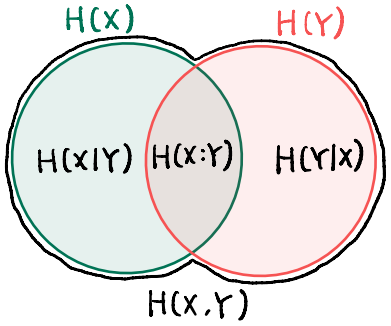
$$= -\sum p(y)\, p(x|y) \log p(x|y) = \sum_y p(y)\, H(X|y)$$

meaning? given information on Y, additional information needed for X .

mutual information

$$I(X:Y) = H(X) + H(Y) - H(X,Y) = I(Y:X)$$.

meaning? information shared by two parties.



subadditivity

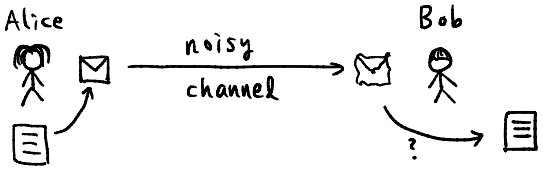
$$H(X,Y) \le H(X) + H(Y) \iff I(X:Y) \ge 0$$.

strong subadditivity

$$H(X|Y,Z) \le H(X|Y) \iff H(X,Y,Z) + H(Y) \le H(X,Y) + H(Y,Z)$$.

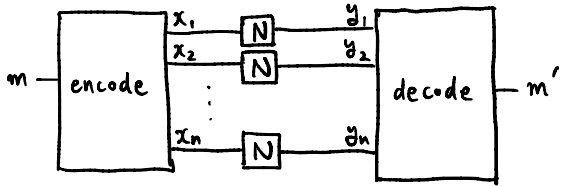
Shannon's Noisy Channel Coding Theorem .

model



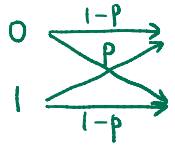
message $m \in \{1, 2, \cdots, M\} \to$ codeword $x^n(m) \equiv x_1(m)\, x_2(m) \cdots x_n(m)$

channel $N : x \to y$ with prob. $p(y|x)$



↑ i.i.d. (discrete memoryless channel)

ex) binary symmetric channel .



$p(0|1) = p(1|0) = p$

$p(0|0) = p(1|1) = 1-p$

rate $R = \frac{\log M}{n}$. $\frac{\#\text{ of message bits}}{\#\text{ of channel uses}}$.

channel capacity $C(N) \equiv$ maximum possible rate . maximum over what? encoding schemes .

result random coding. $p(x_i(m)) = p_X(x_i(m))$ i.i.d.

 uses M typical sequences chosen randomly. (You cannot use all of them!)

$x^n \xrightarrow{\text{noise}} y^n$  finds the most probable x^n. (what about overlap?)

as $n \to \infty$, $\boxed{C(N) = \max_{p_X(x)} I(X:Y)}$

idea $m \to x^n(m) \xrightarrow{p(y|x)} y^n(x^n(m))$

$x, y \in \{a, b, c, d, \cdots\}$

 $x^n(m)$: typical sequence.

$p(x^n(m))$ independent of m.

rearranging $x^n(m)$: $\underbrace{a\,a\cdots a}_{np_X(a)}\ \underbrace{b\,b\cdots b}_{np_X(b)}\ \underbrace{c\,c\cdots c}_{np_X(c)}\cdots$

 rearranging $y^n(x^n)$: $\underbrace{a\cdots a}_{np_X(a)p(a|a)}\ \underbrace{b\cdots b}_{np_X(a)p(b|a)}\ \underbrace{a\cdots a}_{np_X(b)p(a|b)}\ \underbrace{b\cdots b}_{np_X(b)p(b|b)}\cdots$

for given $x^n(m)$, $p(y^n(x^n)) \approx \prod_{x,y} p(y|x)^{np_X(x)p(y|x)}$ same for every m.

"conditionally typical sequence"

$$\# \approx \frac{1}{p(y^n)} \quad \log(\#) \approx -\sum_{x,y} np_X(x)\,p(y|x)\log p(y|x) = n\sum_x p_X(x) H(Y|x)$$

$$= nH(Y|X).$$

$\therefore 2^{nH(Y|X)}$ sequences of y^n correspond to one $x^n(m)$.

on the other hand, # of $y \approx \sum_x np_X(x)\,p(y|x) = np(y)$.

$\Rightarrow y^n$ is also a typical sequence with distribution $p(y)$.

$\# \approx 2^{nH(Y)}$ you are allowed to use all of these.

$$\#\text{ of allowed codewords} = M \approx \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{n[H(Y)-H(Y|X)]} = 2^{nI(X:Y)}$$

what about overlap?

optimality? converse theorem

ex) noiseless channel.

$p(x|y) = \delta_{x,y}$. $H(Y|X) = \sum_x p(x)\,H(Y|x) = 0$. $I(X:Y) = H(Y) - H(Y|X) = H(Y) = H(X)$.

* sending $\begin{pmatrix} \text{classical} \\ \text{quantum} \end{pmatrix}$ information over noisy quantum channel

Quantum State Merging

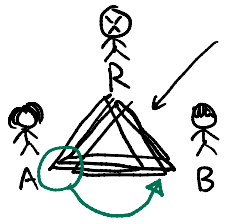
negative conditional entropy?

$S(A|B) = S(AB) - S(B)$ conditional entropy.

$= -\mathrm{Tr}(\rho_{AB} \log \rho_{AB}) + \mathrm{Tr}(\rho_B \log \rho_B)$

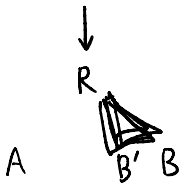
if $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$, $S(A|B) = -1 < 0$. meaning?

objective



n copies of $|\psi\rangle_{ABR}$

$n \to \infty$.



n copies of $|\psi\rangle_{B'BR} \approx |\psi\rangle_{ABR}$.

① if $S(A|B) > 0$, A needs to send $nS(A|B)$ qubits to B

ex) $|\psi\rangle_{ABR} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AR}|0\rangle_B$, $S(AB) = 1$, $S(B) = 0$, $S(A|B) = 1$.

equivalently, A and B need to share $nS(A|B)$ additional Bell pairs $(+ \begin{matrix} \text{quantum} \\ \text{teleportation} \end{matrix})$

② if $S(A|B) = 0$, B can generate $|\psi\rangle_{B'BR}$ locally.

ex) $|\psi\rangle_{ABR} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)_{ABR}$, $S(AB) = S(B) = 1$, $S(A|B) = 0$.

③ if $S(A|B) < 0$, B can generate $|\psi\rangle_{B'BR}$ locally.

furthermore, A and B has already shared $-nS(A|B)$ Bell pairs!

ex) $|\psi\rangle_{ABR} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)_{AB}|0\rangle_R$

* quantum information theory

- quantum information theory (?!)

  : quantum Shannon theory, new things with no classical analogue (distinguishability, entanglement, von Neumann entropy, ···), foundation of QM (nonlocality, contextuality, ···)

- quantum information processing.

  : communication, computation, metrology, ···

- quantum simulation

  : analogue (Hamiltonian egineering, state preparation, ···), digital.

- Applications to physics, chemistry, ···

Axioms of Quantum Mechanics

axiom 1 (state space)

A quantum state $|\psi\rangle$ completely describes a closed quantum system.

$|\psi\rangle$ is a unit vector in a Hilbert space $\mathcal{H}$. $\langle\psi|\psi\rangle = 1$.

NO exchange of any form — energy, particles, etc. — with other systems.

axiom 2 (dynamics)

$|\psi(t=t_1)\rangle \longrightarrow |\psi(t=t_2)\rangle$ is a unitary transformation $|\psi(t_2)\rangle = U(t_2,t_1)|\psi(t_1)\rangle$.

$$UU^\dagger = U^\dagger U = I.$$

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \quad U(t_2,t_1) = e^{-iH(t_2-t_1)}.$$

any unitary U can be written as $U = e^{iK}$ with K being Hermitian.

axiom 3 (projective measurements)

An observable A is Hermitian.

$A = A^\dagger = \sum_m a_m P_m$. $a_m \in \mathbb{R}$ (real number).

$P_m^2 = P_m$. (projection) $P_m P_n = 0$ for $m \neq n$. $\sum_m P_m = I$.

projective measurement of A: $|\psi\rangle \longrightarrow \frac{P_m|\psi\rangle}{\|P_m|\psi\rangle\|}$ with probability $\langle\psi|P_m|\psi\rangle$.

$\||\phi\rangle\| \equiv \sqrt{\langle\phi|\phi\rangle}$ norm.

axiom 4 (composite systems)

system A: $|\psi\rangle_A \in \mathcal{H}_A$.

system B: $|\psi\rangle_B \in \mathcal{H}_B$.

$\Rightarrow$ system A+B: $|\psi\rangle_A \otimes |\psi\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B$.

↑ tensor product. (physists like to omit.)

Hilbert space dimension

$d(\mathcal{H}_A \otimes \mathcal{H}_B) = d(\mathcal{H}_A)\, d(\mathcal{H}_B)$.

* tensor product.

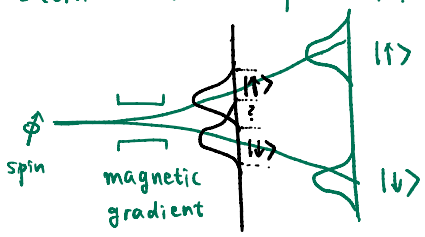
$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$, $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi,\phi\rangle = \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, $A \otimes B = \begin{pmatrix} a\begin{pmatrix} e & f \\ g & h \end{pmatrix} & b\begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ c\begin{pmatrix} e & f \\ g & h \end{pmatrix} & d\begin{pmatrix} e & f \\ g & h \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ae & af & \cdots \\ ag & ah & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$

$(A \otimes B)|\psi\rangle \otimes |\phi\rangle = A|\psi\rangle \otimes B|\phi\rangle$.

<u>axiom 3'</u> (general measurements)

ex) Stern-Gerlach experiment.



$\{M_m\}$: set of measurement operators s.t. $\sum_m E_m = \sum_m M_m^\dagger M_m = I$. $\left(\sum_m M_m M_m^\dagger \neq I\right)$

$E_m \equiv M_m^\dagger M_m$: POVM element.

$\{E_m\}$: POVM (Positive-Operator Valued Measure)

$E_m \geq 0$ (positive-semidefinite), meaning $\langle\psi|E_m|\psi\rangle \geq 0$ for any $|\psi\rangle$.

$\langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\phi|\phi\rangle \geq 0$.

($|\phi\rangle \equiv M_m|\psi\rangle$)

measurement outcome : $|\psi\rangle \longrightarrow \frac{M_m|\psi\rangle}{\|M_m|\psi\rangle\|}$ with probability $p(m) = \|M_m|\psi\rangle\|^2 = \langle\psi|E_m|\psi\rangle$.

ex) $M_1 = \alpha|\uparrow\rangle\langle\uparrow|$. $E_1 = \alpha^2|\uparrow\rangle\langle\uparrow|$

$M_2 = \alpha|\downarrow\rangle\langle\downarrow|$. $E_2 = \alpha^2|\downarrow\rangle\langle\downarrow|$.

$M_3 = \sqrt{1-\alpha^2}\, I$. $E_3 = (1-\alpha^2) I$.

$\sum_m E_m = I$.

* axioms 3 & 4 $\Rightarrow$ axiom 3'.

Apply U_{SA} s.t. $U_{SA}|\psi\rangle_S \otimes |0\rangle_A = \sum_m (M_m|\psi\rangle_S) \otimes |m\rangle_A$ (system, ancilla) this is unitary. why? $\langle\phi,0|U_{SA}^\dagger U_{SA}|\psi,0\rangle = \langle\phi,0|\psi,0\rangle = \langle\phi|\psi\rangle$.

and measure the ancilla in $\{|m\rangle_A\}$. → projective measurement. $P_m = I_S \otimes |m\rangle_A\langle m|$.

$p(m) = \|P_m U_{SA}|\psi,0\rangle\|^2 = \langle\psi,0|U_{SA}^\dagger (I_S \otimes |m\rangle_A\langle m|) U_{SA}|\psi,0\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$

Density Matrices (Density Operators)

ex) ① $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. what would you say about this state?

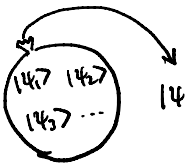
② $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

③ $|0\rangle$ with prob. $\frac{1}{2}$, $|1\rangle$ with prob. $\frac{1}{2}$.

Z measurements : $p(0) = p(1) = \frac{1}{2}$ in all cases .

X " : $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

① $p(+) = 1$, $p(-) = 0$. ② $p(+) = 0$, $p(-) = 1$. ③ $p(+) = \frac{1}{2}$, $p(-) = \frac{1}{2}$.



$|\psi_i\rangle$ with prob. p_i . $\Rightarrow$ $\boxed{\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|}$. $\sum_i p_i = 1$, $p_i \geq 0$.

operator (matrix) .

NOT a vector .

ensemble : collection of events .

when you have ρ, you have only a single event (one of $|\psi_i\rangle$'s), not the ensemble .



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



$\rho = \frac{1}{\sqrt{2}}|+\rangle\langle +| + \frac{1}{\sqrt{2}}|-\rangle\langle -| = \frac{1}{2}I$.

two states are exactly the same! (no way to distinguish)

* pure states vs mixed states .

$|\psi\rangle$: pure state ($\rho = |\psi\rangle\langle\psi|$)

ρ : mixed state (# of non-zero $p_i \geq 2$)

time evolution $|\psi(t_2)\rangle = U|\psi(t_1)\rangle$.

$\rho(t_2) = U\rho(t_1)U^\dagger$. why?

expectation value $\langle A\rangle = \langle\psi|A|\psi\rangle$.

$\langle A\rangle = \mathrm{Tr}(\rho A)$. why?

↑ trace .

* trace

$\mathrm{Tr}(\rho) = \sum_n \langle n|\rho|n\rangle$. $|n\rangle$: basis states .

$\rho = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots \\ 0 & \lambda_2 & 0 & \cdots \\ 0 & 0 & \lambda_3 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$.

$\mathrm{Tr}(\rho) = \sum_i \lambda_i$ (basis independent) .

$\mathrm{Tr}(U\rho U^\dagger) = \mathrm{Tr}(\rho)$.

$\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA) = \mathrm{Tr}(CAB)$. cyclic .

* partial trace .

composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

basis states : $|n\rangle_A \otimes |m\rangle_B = |n, m\rangle$.

notation $\left(|n\rangle_A \otimes |m\rangle_B\right)\left({}_A\langle n'| \otimes {}_B\langle m'|\right) = |n\rangle_A\langle n'| \otimes |m\rangle_B\langle m'| = |n, m\rangle\langle n', m'|$.

X_{AB} : acting on $\mathcal{H}_A \otimes \mathcal{H}_B$.

$\mathrm{Tr}(X_{AB}) = \sum_{n,m} \langle n, m| X_{AB} |n, m\rangle$.

partial trace $\mathrm{Tr}_A(X_{AB}) = \sum_n {}_A\langle n| X_{AB} |n\rangle_A$: operator acting on $\mathcal{H}_B$.

$\mathrm{Tr}_B(X_{AB}) = \sum_m {}_B\langle m| X_{AB} |m\rangle_B$: " $\mathcal{H}_A$.

$\mathrm{Tr}(X_{AB}) = \mathrm{Tr}_A(\mathrm{Tr}_B(X_{AB})) = \mathrm{Tr}_B(\mathrm{Tr}_A(X_{AB}))$.

* reduced density matrix .

state ρ_{AB} of composite system A+B .

state of system A (ignoring B) $\rho_A = \mathrm{Tr}_B(\rho_{AB})$.

" B (" A) $\rho_B = \mathrm{Tr}_A(\rho_{AB})$.

why? for any operator X_A on A, you can show

$$\langle X_A \rangle = \langle X_A \otimes I_B \rangle = \mathrm{Tr}\left[\rho_{AB}(X_A \otimes I_B)\right] = \mathrm{Tr}_A\left[\mathrm{Tr}_B(\rho_{AB})\, X_A\right] = \mathrm{Tr}_A(\rho_A X_A) .$$

any local operation on A (unitary, measurement, whatever) cannot alter ρ_B !

ex) $|\psi\rangle_{AB} = \alpha|00\rangle_{AB} + \beta|11\rangle_{AB}$.

$\rho_A = |\alpha|^2 |0\rangle_A\langle 0| + |\beta|^2 |1\rangle_B\langle 1|$.

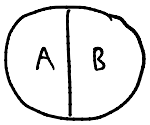
$\rho_B = |\alpha|^2 |0\rangle_B\langle 0| + |\beta|^2 |1\rangle_B\langle 1|$.

A+B : pure $\longrightarrow$ A or B alone : mixed ! (when A, B are entangled) .

* ρ is a valid quantum state iff ① $\rho \geq 0$ $(\Rightarrow \rho = \rho^\dagger)$.

② $\mathrm{Tr}(\rho) = 1$.

Schmidt Decomposition and Purification .



A : dimension d_A . basis : $|0\rangle_A, |1\rangle_A, \cdots, |d_A-1\rangle_A$.

B : " d_B . basis : $|0\rangle_B, |1\rangle_B, \cdots, |d_B-1\rangle_B$.

AB : dimension $d_A d_B$.

$$|\psi\rangle_{AB} = \sum_{n=0}^{d_A-1} \sum_{m=0}^{d_B-1} C_{nm} \underbrace{|n\rangle_A |m\rangle_B}_{\#\text{ of basis states} = d_A d_B} .$$

Schmidt decomposition (for pure states).

You can always write

$$|\psi\rangle_{AB} = \sum_{i=0}^{d_A-1} \lambda_i |\phi_i\rangle_A |\phi_i'\rangle_B$$

$|\phi_i\rangle_A$, $|\phi_i'\rangle_B$: orthonormal basis states.

# of basis states $= \min(d_A, d_B)$.

λ_i : Schmidt coefficient.

# of non-zero λ_i's : Schmidt rank / Schmidt number $\leq \min(d_A, d_B)$.

ex) two-qubit state $|\psi\rangle = a|0\rangle|0\rangle + b|0\rangle|1\rangle + c|1\rangle|0\rangle + d|1\rangle|1\rangle$

can be written as $|\psi\rangle = \lambda_1 |\phi_1\rangle|\phi_1'\rangle + \lambda_2 |\phi_2\rangle|\phi_2'\rangle$.

(proof) $|\psi\rangle = \sum_{n,m} C_{nm} |n\rangle|m\rangle$. ← singular value decomposition

C_{nm} is a matrix $\xrightarrow{\text{SVD}}$ $C_{nm} = (U d V^\dagger)_{nm} = \sum_\ell U_{n\ell} d_{\ell\ell} V^\dagger_{\ell m}$

(U: unitary, d: diagonal)

$$|\psi\rangle = \sum_{\ell,n,m} U_{n\ell} d_{\ell\ell} V^\dagger_{\ell m} |n\rangle|m\rangle$$

Let $|\phi_\ell\rangle = \sum_n U_{n\ell} |n\rangle = \sum_n U^\dagger_{\ell n} |n\rangle$ (basis transformation).

$|\phi_\ell'\rangle = \sum_m V^\dagger_{\ell m} |m\rangle$

Then, $|\psi\rangle = \sum_\ell d_\ell |\phi_\ell\rangle|\phi_\ell'\rangle$

$$\rho_{AB} = \sum_i \sum_j \lambda_i \lambda_j^* |\phi_i\rangle_A\langle\phi_j| \otimes |\phi_i'\rangle_B\langle\phi_j'|.$$

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \sum_i |\lambda_i|^2 |\phi_i\rangle_A\langle\phi_i|$$

$$\rho_B = \mathrm{Tr}_A(\rho_{AB}) = \sum_i |\lambda_i|^2 |\phi_i'\rangle_B\langle\phi_i'|.$$

Schmidt rank $= 1$: pure state

> 1 : entangled state. (much more complicated for mixed ρ_{AB}!)

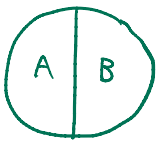
von Neumann entropy

cf) $H(X) = -\sum_x p(x) \log p(x)$

$S(\rho) = -\mathrm{Tr}(\rho \log \rho)$.

function of a matrix

$$f(M) = \begin{pmatrix} f(\lambda_1) & 0 & \cdots \\ 0 & f(\lambda_2) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$ in the diagonalizing basis.



suppose $|\psi\rangle_{AB} = \sum_i \sqrt{p_i} |\phi_i\rangle_A |\phi_i'\rangle_B$.

$S(AB) \equiv S(\rho_{AB}) = 0$ ∵ pure state.

$S(A) \equiv S(\rho_A) = S\left(\sum_i p_i |\phi_i\rangle_A\langle\phi_i|\right) = -\sum_i p_i \log p_i$.

$= S(B)$.

* if composite system A+B is in a pure state,

$S(AB) = 0$.

$S(A) = S(B)$ is called the "entanglement entropy", which is an "entanglement measure".

$$S(A) = \begin{cases} 0 & \text{if } \rho_A = |\phi\rangle_A\langle\phi| \quad (|\psi\rangle_{AB} = |\phi\rangle_A|\phi'\rangle_B) \\ \log d & \text{if } \rho_A = \frac{1}{d}\sum_{i=1}^{d}|\phi_i\rangle_A\langle\phi_i| \quad (|\psi\rangle_{AB} = \sum_{i=1}^{d}\sqrt{\frac{1}{d}}|\phi_i\rangle_A|\phi_i'\rangle_B \text{ maximally entangled}) \end{cases}$$

entanglement for bipartite mixed states

ρ_{AB} is <u>separable</u> if you can write $\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$. $p_i \geq 0$, $\sum_i p_i = 1$. why?

<u>entangled</u> otherwise .

entanglement measure? 😐

even discriminating between the two is very hard! why?

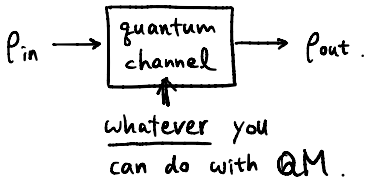
purification

mixed state $\rho_A \longrightarrow |\psi\rangle_{AR}$ s.t. $\rho_A = \mathrm{Tr}_R(|\psi\rangle_{AR}\langle\psi|)$. R : reference system.

ρ_A is Hermitian → diagonalizable.

$$\rho_A = \sum_i p_i|\phi_i\rangle_A\langle\phi_i| \longrightarrow |\psi\rangle_{AR} = \sum_i \sqrt{p_i}\,|\phi_i\rangle_A|i\rangle_R .$$

Quantum Operations (Quantum Channels)



$\rho_{out} = \mathcal{E}(\rho_{in})$

ex) unitary transformation

$$\mathcal{E}(\rho) = U\rho U^\dagger .$$

ex) projective measurement.

$$\mathcal{E}(\rho) = \sum_m |m\rangle\underbrace{\langle m|\rho|m\rangle}_{p(m)}\langle m| = \sum_m p(m)\,|m\rangle\langle m| .$$

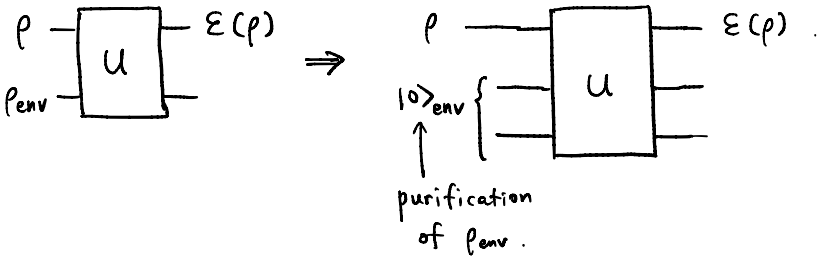
$$\rho = (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|)$$

$$\mathcal{E}(\rho) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| .$$

* operator-sum representation (physically-motivated approach)

system only : ρ — [U] — $U\rho U^\dagger$

system + environment :



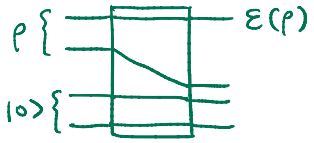
$$\mathcal{E}(\rho) = Tr_{env}\left[U(\rho \otimes |0\rangle_{env}\langle 0|)U^\dagger\right]$$

initially uncorrelated!

this is an assumption. See our motivation.

We also assume $\mathcal{H}_{in} = \mathcal{H}_{out}$

$\mathcal{H}_{in} \neq \mathcal{H}_{out}$ in general ex)



bases for env. : $|e_0\rangle, |e_1\rangle, |e_2\rangle, \cdots$

$$\mathcal{E}(\rho) = Tr_{env}\left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right]$$

$$= \sum_k \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle$$

$$= \sum_k \langle e_k|U|e_0\rangle \rho \langle e_0|U^\dagger|e_k\rangle$$

$$\boxed{\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger} \qquad E_k \equiv \langle e_k|U|e_0\rangle \quad \text{Kraus operator}$$

$$\boxed{\sum_k E_k^\dagger E_k = I} \quad \text{trace preserving.}$$

$$\sum_k \langle e_0|U^\dagger|e_k\rangle\langle e_k|U|e_0\rangle = \langle e_0|U^\dagger I U|e_0\rangle = 1.$$

* axiomatic approach.

ρ_A — [ℰ] — ρ_B. $\mathcal{H}_A \neq \mathcal{H}_B$ in general.

axiom 1 (linear map)

$$\mathcal{E}(p_1\rho_1 + p_2\rho_2) = p_1\mathcal{E}(\rho_1) + p_2\mathcal{E}(\rho_2). \quad \text{why?}$$

axiom 2 (completely-positive map)

$\rho \geq 0$ positive(-semidefinite) operator.

$\mathcal{E}(\rho) \geq 0$ positive map.

additional system R of any size.

$(I_R \otimes \mathcal{E})(\rho_{RA}) \geq 0$ completely-positive map. cf) transposition is positive, but not completely-positive

$|i\rangle\langle j| \to |j\rangle\langle i|$

axiom 3 (trace-preserving map)

$$\mathrm{Tr}[\mathcal{E}(\rho)] = 1 .$$

physical operations are CPTP maps. completely-positive trace-preserving.

$\mathcal{E}(\rho)$ is CPTP iff $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, $\sum_k E_k^\dagger E_k = I$.

Choi-Jamiołkowski (CJ) isomorphism

cf) $M = \sum_{ij} M_{ij} |i\rangle\langle j| \iff \Phi_M = \sum_{ij} M_{ij} |i\rangle|j\rangle$. operator-state duality.

note $\left[\left(\sum_{ij} M_{ij} |i\rangle_A\langle j|\right) \otimes I_B\right] \sum_k |k\rangle_A |k\rangle_B = \sum_k \sum_i M_{ik} |i\rangle_A |k\rangle_B$

$\mathcal{E}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$, $\mathcal{L}(\mathcal{H})$: space of linear operators (square matrices) on $\mathcal{H}$.

$|\alpha\rangle_{RA} \equiv \sum_i |i\rangle_R |i\rangle_A$. (unnormalized maximally-entangled state)

$\mathcal{E}_{A\to B} \iff \sigma_{RB} \equiv (I_R \otimes \mathcal{E}_{A\to B})(|\alpha\rangle_{RA}\langle\alpha|) = \sum_{ij} |i\rangle_R\langle j| \otimes \mathcal{E}_{A\to B}(|i\rangle_A\langle j|)$. channel-operator duality.

why needed? $\mathcal{E}_{A\to B}$ is CP iff $\sigma_{RB} \geq 0$.

Hermitian-preserving iff $\sigma_{RB}^\dagger = \sigma_{RB}$

...

idea proving $\leftarrow$ is simple.

proving $\rightarrow$?

$\mathcal{E}_{A\to B}$ is CPTP $\Rightarrow \sigma_{RB} \geq 0 \Rightarrow \sigma_{RB} = \sum_k |\phi_k\rangle_{RB}\langle\phi_k|$ (unnormalized).

$$|\phi_k\rangle_{RB} = \sum_{ij} \phi_{ij}^k |i\rangle_R |j\rangle_B$$

We will recover $\sigma_{RB} \to \mathcal{E}_{A\to B}$.

define $E_k \equiv \sum_{ij} \phi_{ij}^k |j\rangle_B\langle i|_A$

Then, $(I_R \otimes E_k)|\alpha\rangle_{RA} = |\phi_k\rangle_{RB}$.

$\Rightarrow \sum_k E_k |\alpha\rangle_{RA}\langle\alpha| E_k^\dagger = \sum_k |\phi_k\rangle_{RB}\langle\phi_k| = \sigma_{RB}$.

${}_R\langle i|$ ↙ $|j\rangle_R = \sum_k E_k |i\rangle_A\langle j| E_k^\dagger = \mathcal{E}_{A\to B}(|i\rangle_A\langle j|)$ for $\forall i, j$.

axiom 3 $\Rightarrow \sum_k E_k^\dagger E_k = I$.

Lindblad Equation (Master Equation) ???

in the absence of environment,

$$\frac{d\rho}{dt} = -i[H,\rho] .$$

$$\rho(t+dt) = \rho(t) + \frac{d\rho}{dt}dt = \rho - iH\rho\,dt + i\rho H\,dt$$

$$= (I - iH\,dt)\,\rho\,(I + iH\,dt) + O(dt^2) .$$

$$= E_0 \rho E_0^\dagger \qquad E_0 \equiv I - iH\,dt .$$

in the presence of environment,

$$E_0 \to I - iH\,dt + K\,dt + O(dt^2)$$

$$E_k \equiv L_k\sqrt{dt} + O(dt) .$$

$$\rho(t+dt) = \sum_k E_k \rho E_k^\dagger = (I - iH\,dt + K\,dt)\,\rho(t)\,(I + iH\,dt + K^\dagger dt) + \sum_{k\neq 0} L_k \rho L_k^\dagger\,dt + O(dt^2)$$

$$= \rho - i[H,\rho]\,dt + K\rho\,dt + \rho K^\dagger dt + \sum_{k\neq 0} L_k \rho L_k^\dagger\,dt + O(dt^2)$$

$$\sum_k E_k^\dagger E_k = I + (K+K^\dagger)\,dt + \sum_{k\neq 0} L_k^\dagger L_k\,dt + O(dt^2) = I .$$

$$\Rightarrow K = K^\dagger \quad \text{Hermitian}$$

$$K = -\frac{1}{2}\sum_k L_k^\dagger L_k .$$

$$\boxed{\frac{d\rho}{dt} = -i[H,\rho] + \sum_k \left(L_k \rho L_k^\dagger - \frac{1}{2}L_k^\dagger L_k \rho - \frac{1}{2}\rho L_k^\dagger L_k\right)}$$

Lindblad equation

L_k: Lindblad operator.

ex) suppose $H = 0$. $L = \sqrt{\Gamma}\,|0\rangle\langle 1|$. $L^\dagger L = \Gamma\,|1\rangle\langle 1|$.



$$\rho(t) = \begin{pmatrix} 1-p(t) & f(t) \\ f^*(t) & p(t) \end{pmatrix} = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1| + f|0\rangle\langle 1| + f^*|1\rangle\langle 0| .$$

$$\dot\rho = -\dot p\,|0\rangle\langle 0| + \dot p\,|1\rangle\langle 1| + \dot f\,|0\rangle\langle 1| + \dot f^*|1\rangle\langle 0|$$

$$= \Gamma p\,|0\rangle\langle 0| - \Gamma p\,|1\rangle\langle 1| - \frac{\Gamma}{2} f\,|0\rangle\langle 1| - \frac{\Gamma}{2} f^*|1\rangle\langle 0|$$

$$p(t) = p(0)\,e^{-\Gamma t} , \quad f(t) = f(0)\,e^{-\Gamma t/2} .$$

$$\rho(t) = \begin{pmatrix} 1-p(0)e^{-\Gamma t} & f(0)e^{-\Gamma t/2} \\ f^*(0)e^{-\Gamma t/2} & p(0)e^{-\Gamma t} \end{pmatrix}$$

steady state : $\dot\rho = 0 \Rightarrow \rho(\infty) = |0\rangle\langle 0|$.

Examples of Quantum Channels.

(general) measurement

$\{M_m\}$ measurement operators.

$\sum_m M_m^\dagger M_m = I$.

$$\mathcal{E}(\rho) = \sum_m M_m \rho M_m^\dagger = \sum_m \underbrace{\mathrm{Tr}(M_m \rho M_m^\dagger)}_{\mathrm{Tr}(E_m \rho) \,=\, p(m)} \underbrace{\frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m \rho M_m^\dagger)}}_{\text{state after having a measurement outcome } m}.$$

Pauli operators $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

bit flip. phase flip.

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

$X|1\rangle = |0\rangle$ $Z|1\rangle = -|1\rangle$.

$X^2 = Y^2 = Z^2 = I$, $XY = Z$, $YZ = X$, $ZX = Y$.

$YX = -Z$, $ZY = -X$, $XZ = -Y$.

dephasing channels

$\mathcal{E}(\rho) = (1-p)\rho + p Z\rho Z$.

$E_1 = \sqrt{1-p}\, I$, $E_2 = \sqrt{p}\, Z$.

$\mathcal{E}\left[\begin{pmatrix} \rho_0 & f \\ f^* & \rho_1 \end{pmatrix}\right] = ?$

depolarizing channels

$\mathcal{E}(\rho) = (1-p)\rho + p\frac{I}{2}$.

$\rho = \begin{pmatrix} \rho_0 & f \\ f^* & \rho_1 \end{pmatrix} = \square I + \square X + \square Y + \square Z$.

$I\rho I + X\rho X + Y\rho Y + Z\rho Z = 2I$.

$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$.

amplitude damping

$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-r} \end{pmatrix} = |0\rangle\langle 0| + \sqrt{1-r}\,|1\rangle\langle 1|$

$E_1 = \begin{pmatrix} 0 & \sqrt{r} \\ 0 & 0 \end{pmatrix} = \sqrt{r}\,|0\rangle\langle 1|$. $E_1 \rho E_1^\dagger = r\,|0\rangle\langle 1|\rho|1\rangle\langle 0|$.

