KITS 2021 Summer School on Quantum and Black Hole Information

Introduction to Quantum Information Theory

Jiaju Zhang jiajuzhang@tju.edu.cn (Tianjin University) 张甲举

Reference: Chapters 1, 2, 8, 9, 10, 11, 12 of Nielsen and Chuang

Outline. 1. Overview
2. Quantum mechanics
3. Quantum operations and quantum noises
4. Distance measures
5. Quantum error-correction
6. Entropy and information
7. Quantum information theory (Holevo bound)

A. quantum teleportation of a mixed state

1. Overview

(1) conventions

Pauli matrices $I=\begin{pmatrix}1&\\&1\end{pmatrix}$ $X=\begin{pmatrix}&1\\1&\end{pmatrix}$ $Y=\begin{pmatrix}&-i\\i&\end{pmatrix}$ $Z=\begin{pmatrix}1&\\&-1\end{pmatrix}$ $\vec{\sigma}=(X,Y,Z)$

states $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$ $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$ $\Rightarrow$ $Z|0\rangle=|0\rangle$ $Z|1\rangle=-|1\rangle$

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

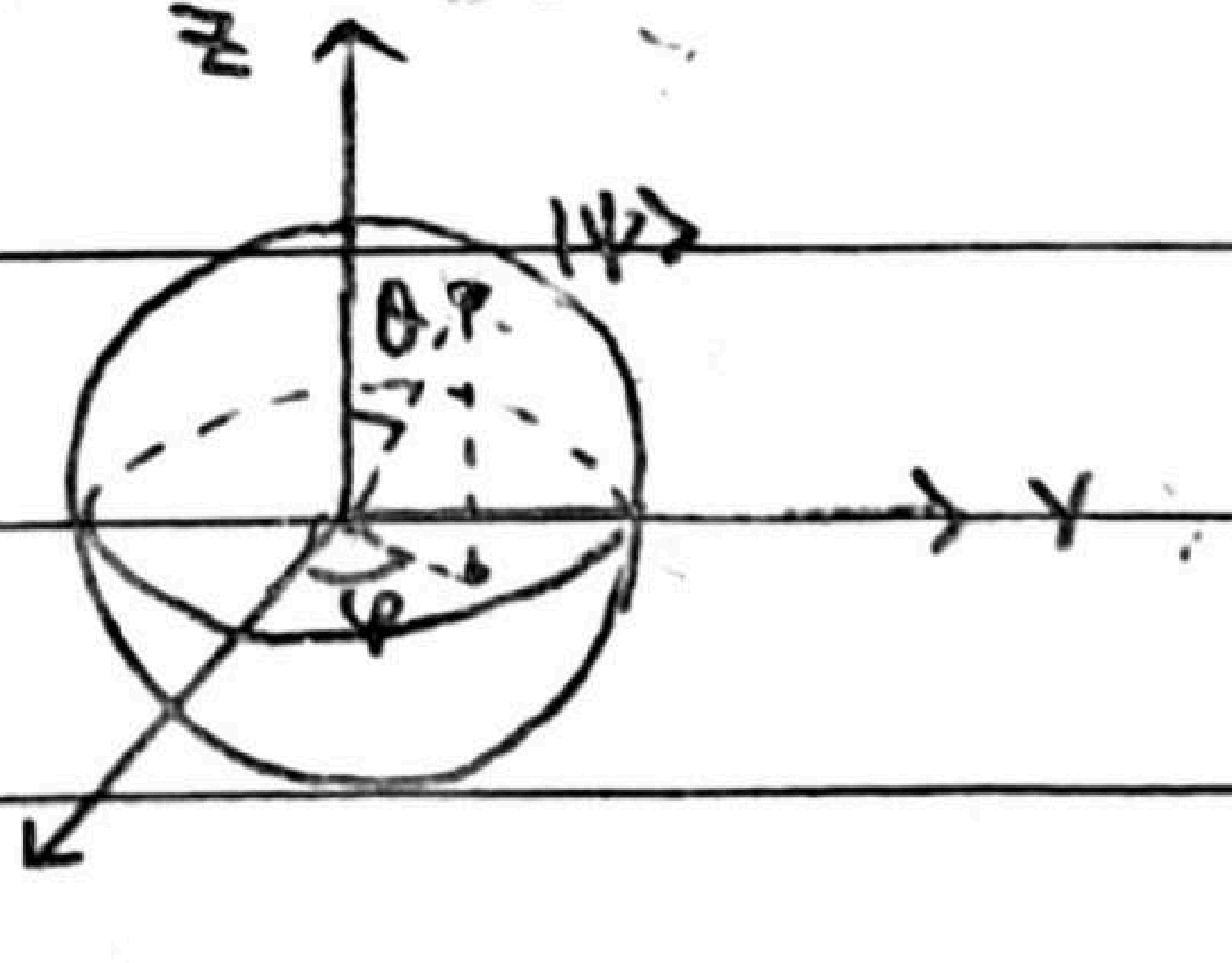
Hadamard matrix $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ $|0\rangle, |1\rangle \overset{H}{\longleftrightarrow} |\pm\rangle$

(2) classical bit 0 or 1 $0\oplus0=0$ $0\oplus1=1$ $1\oplus0=1$ $1\oplus1=0$

quantum bit (qubit) pure state $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ with $|\alpha|^2+|\beta|^2=1$

$$=\underset{\substack{\uparrow\\\text{not important}}}{\cancel{e^{i\gamma}}}\left(\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

surface of Bloch sphere



$\vec{r}=(x,y,z)$

$x=\sin\theta\sin\varphi$

$y=\sin\theta\sin\varphi$

$z=\cos\theta$

density matrix $\rho=|\psi\rangle\langle\psi|=\frac{1}{2}(I+\vec{r}\cdot\vec{\sigma})$

general state $\rho=\frac{1}{2}(I+\vec{r}\cdot\vec{\sigma})$ with $|\vec{r}|\leq1$

mixed state $|\vec{r}|<1$ interior of Bloch sphere especially, maximally mixed state $\vec{r}=0$ $\rho = \frac{I}{2}$

(3) mutiple qubits $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

Bell states (Bell basis, EPR states, EPR pair)

$$\left.\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}\right\rangle \quad |\beta_{xy}\rangle = \frac{1}{\sqrt{2}}(|0y\rangle + (-1)^x|1\bar{y}\rangle)$$

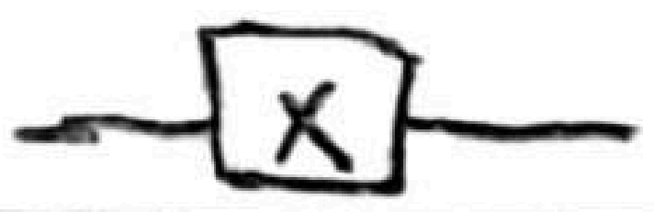
$\bar{y} = y \oplus 1$, $\bar{0} = 1$, $\bar{1} = 0$

(4) quantum gate: linear and unitary transformation of quantum state

single qubit Not gate $|0\rangle \to |1\rangle$

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

$\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$

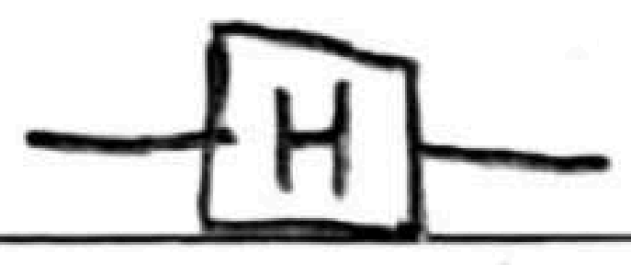


$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Hadamard gate $|0\rangle \to |+\rangle$

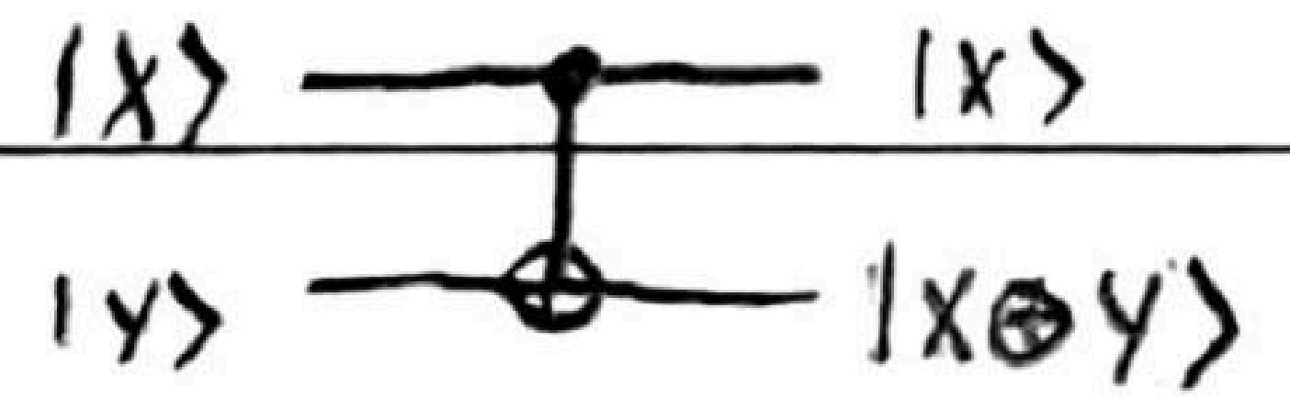
$|1\rangle \to |-\rangle$

$\alpha|0\rangle + \beta|1\rangle \to \alpha|+\rangle + \beta|-\rangle$



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

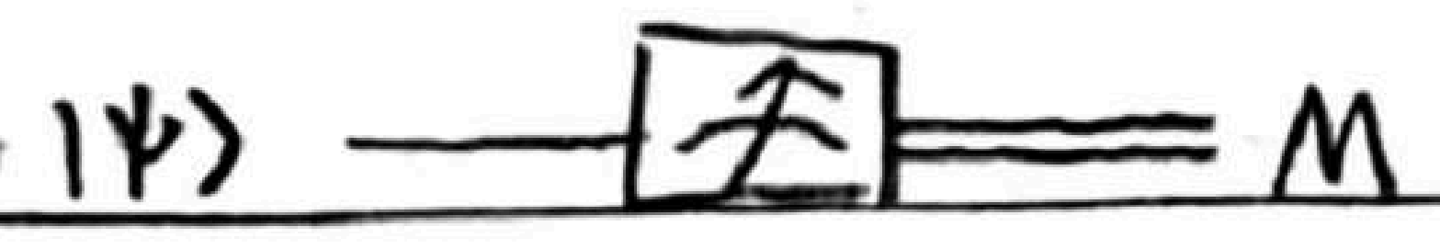
mutiple qubits Controlled not gate (CNOT)



$|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$ $|11\rangle \to |10\rangle$

$|\psi\rangle \to U|\psi\rangle$ $U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

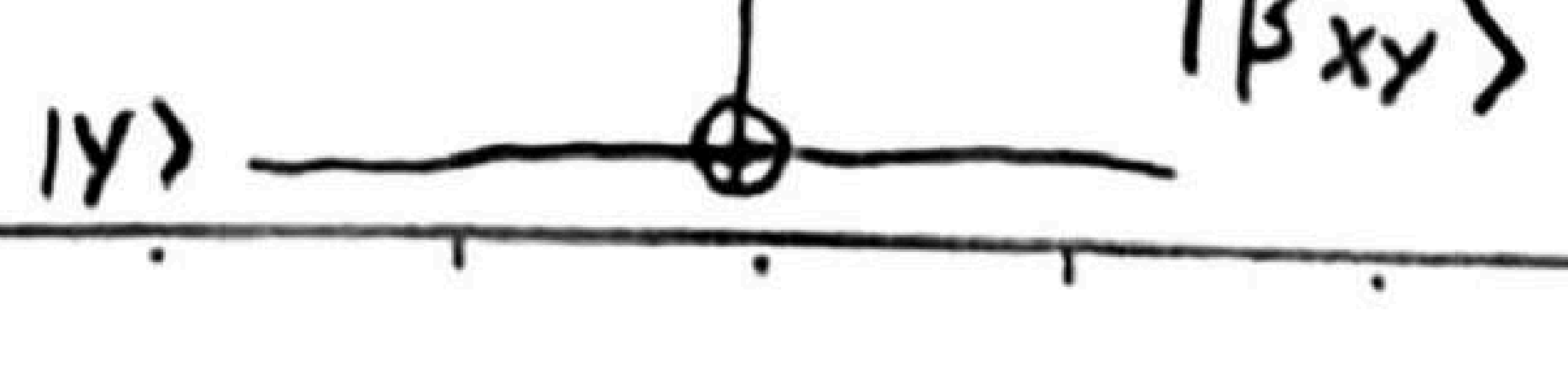
(5) measurement



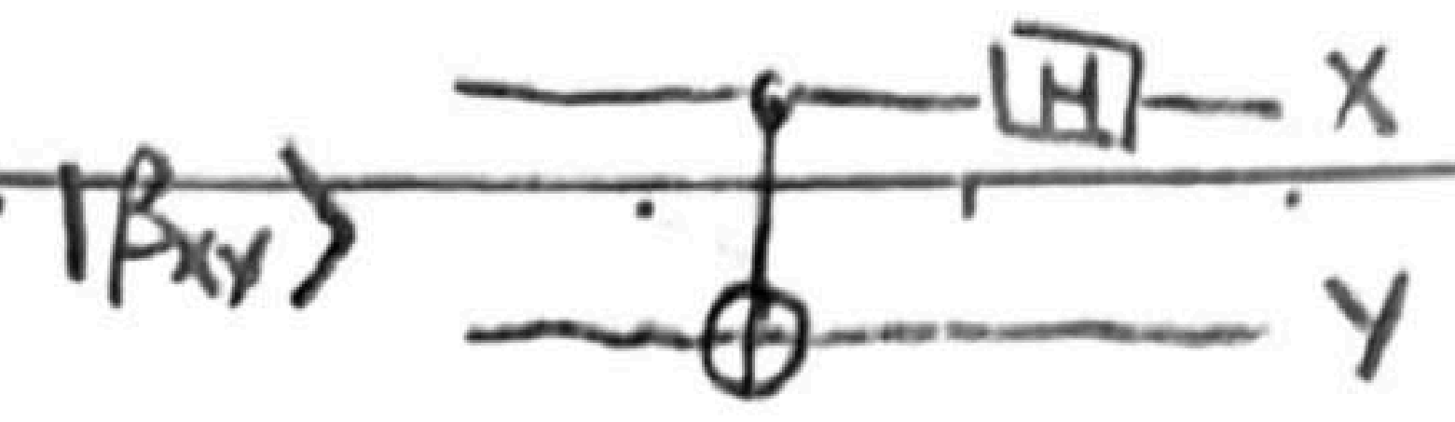
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $M = 0$ or 1 with probabilities $|\alpha|^2$ and $|\beta|^2$

(6) quantum circuits: quantum wires + quantum gates + measurements

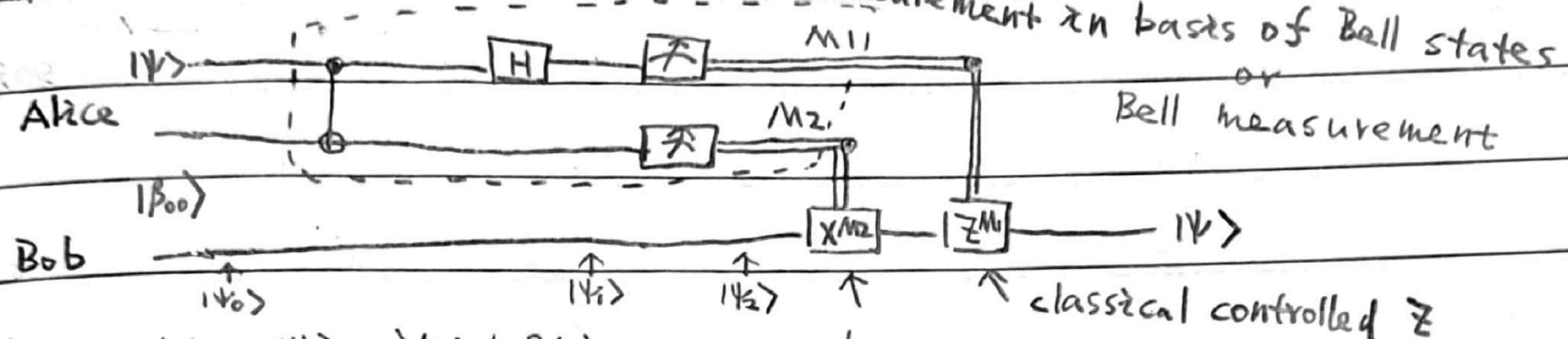
eg: quantum circuit that creates Bell states



the reverse quantum gate



(7) quantum teleportation



general pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

two classical bits M_1, M_2

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\right]$$

$$= \frac{1}{2}\left[|\beta_{00}\rangle(\alpha|0\rangle+\beta|1\rangle) + |\beta_{01}\rangle(\alpha|1\rangle+\beta|0\rangle) + |\beta_{10}\rangle(\alpha|0\rangle-\beta|1\rangle) + |\beta_{11}\rangle(\alpha|1\rangle-\beta|0\rangle)\right]$$

$$|\psi_1\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\right]$$

$M_1M_2 = 00$ $|\psi_2\rangle = \alpha|0\rangle+\beta|1\rangle \longrightarrow |\psi\rangle = |\psi_2\rangle$

01 $|\psi_2\rangle = \alpha|1\rangle+\beta|0\rangle \xrightarrow{X} |\psi\rangle = X|\psi_2\rangle$

10 $|\psi_2\rangle = \alpha|0\rangle-\beta|1\rangle \xrightarrow{Z} |\psi\rangle = Z|\psi_2\rangle$

11 $|\psi_2\rangle = \alpha|1\rangle-\beta|0\rangle \xrightarrow{ZX} |\psi\rangle = ZX|\psi_2\rangle$

$\Big] \rightarrow |\psi\rangle = Z^{M_1}X^{M_2}|\psi_2\rangle$

protocol
1. An EPR pair is generated and sent to Alice and Bob
2. Alice performs Bell measurement for the qubit to be teleported and her EPR qubit
3. Alice sends the result to Bob through two classical bits (limited by speed of light)
4. Bob operates according to Alice's measurement result

2. Quantum mechanics

(1) Hilbert space: complex linear space + inner product

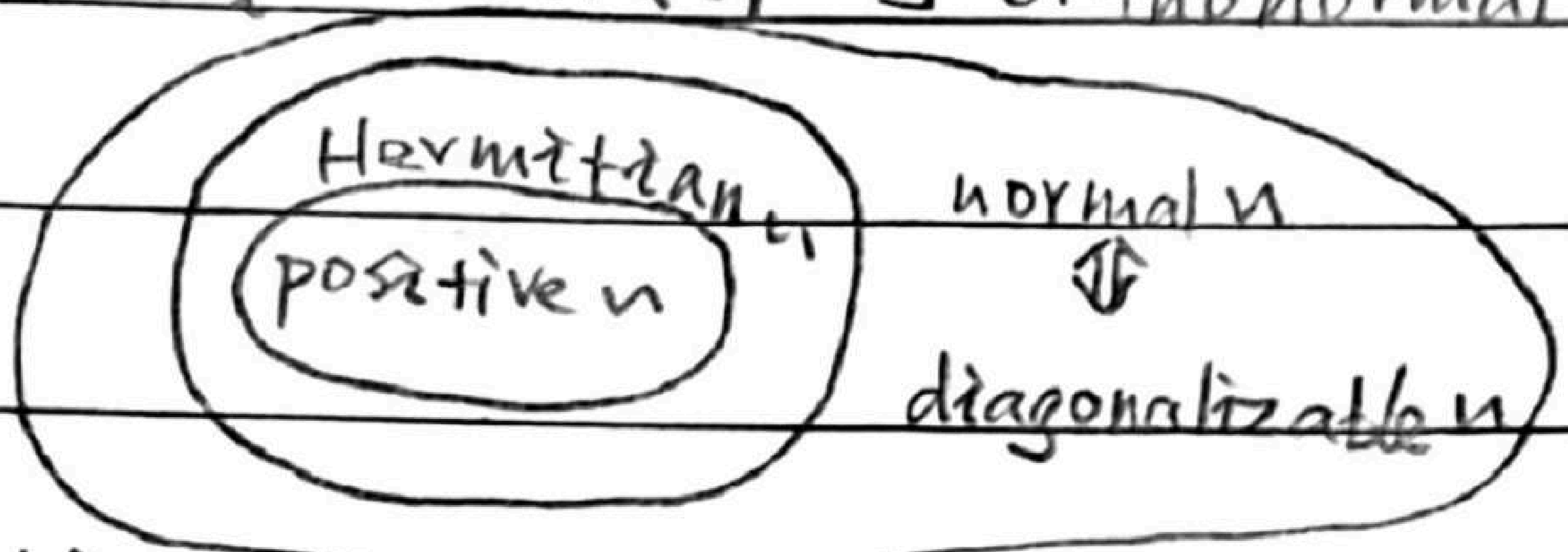
pure state $\Leftrightarrow$ vector ; operator $\Leftrightarrow$ matrix

(2) normal matrix : $AA^{+} = A^{+}A$

Hermitian matrix : $A^{+} = A$

positive matrix : $v^{+}Av \geq 0 \quad \forall$ vector v (nonnegative matrix)

diagonalizable matrix : $A = \sum_i a_i |i\rangle\langle i| \quad \exists$ orthonormal basis



(3) positive 〃 $\Rightarrow$ Hermitian matrix

proof: choose orthonormal basis $v_1, v_2, \cdots$

$v_1^{+}Av_1 = A_{11} \geq 0, \quad v_2^{+}Av_2 = A_{22} \geq 0, \quad \cdots \Rightarrow A_{ii} \geq 0$

$(v_1+v_2)^{+}A(v_1+v_2) = A_{11} + A_{22} + A_{12} + A_{21} \geq 0 \Rightarrow A_{11}+A_{22}+A_{12}+A_{21} = A_{11}+A_{22}+A_{12}^{*}+A_{21}^{*}$

$\Rightarrow A_{12} + A_{21} = A_{12}^{*} + A_{21}^{*}$

$(v_1+iv_2)^{+}A(v_1+iv_2) = A_{11}+A_{22}+i(A_{12}-A_{21}) \geq 0 \Rightarrow A_{11}+A_{22}+i(A_{12}-A_{21}) = A_{11}+A_{22}+i(A_{21}^{*}-A_{12}^{*})$

$\Rightarrow A_{12} - A_{21} = A_{21}^{*} - A_{12}^{*}$

$\Rightarrow A_{12} = A_{21}^{*}, \quad A_{21} = A_{12}^{*}$

$\Rightarrow A_{ij} = A_{ji}^{*}$ Hermitian

(4) spectrum decomposition (eigenvale decomposition) normal 〃 $\Leftrightarrow$ diagonalizable 〃

proof: diagonalizable 〃 $\Rightarrow$ normal 〃 trivial

normal 〃 $\Rightarrow$ diagonalizable

M is a $d \times d$ normal matrix

choose an arbitrary eigen value λ with orthonormal eigenvectors $|v_i\rangle$

$M|v_i\rangle = \lambda|v_i\rangle \quad \langle v_i|v_j\rangle = \delta_{ij} \quad i = 1, 2, \cdots, P$

define λ eigen space $\quad P \equiv \sum_i |v_i\rangle\langle v_i|$

orthogonal complement $Q \equiv I - P$

note $P^{+} = P, \ P^{2} = P, \ Q^{+} = Q, \ Q^{2} = Q, \ PQ = QP = 0$

$QMP = Q\lambda P = 0$

$MM^{+}|v_i\rangle = M^{+}M|v_i\rangle = \lambda M^{+}|v_i\rangle \Rightarrow M^{+}|v_i\rangle \in \lambda$ eigen space

$$\Rightarrow QM^\dagger P = 0 \Rightarrow PMQ = 0$$

$\Rightarrow M = (P+Q)M(P+Q) = PMP + QMQ$

$PMP = \lambda \sum_i |v_i\rangle\langle v_i|$ is diagonal

QMQ is normal $\quad QM = QM(P+Q) = QMQ$

$MQ = (P+Q)MQ = QMQ$

$(QMQ)(QMQ)^\dagger = QMQQM^\dagger Q$

$= QMM^\dagger Q$

$= QM^\dagger MQ$

$= QM^\dagger QQMQ$

$= (QMQ)^\dagger(QMQ)$

(5) polar decomposition: any square matrix $A = UJ = KU$

with $UU^\dagger = I$, $J \equiv \sqrt{A^\dagger A}$, $K \equiv \sqrt{AA^\dagger}$

if A is invertible, U is unique

proof: $J = \sqrt{A^\dagger A}$ is positive $\Rightarrow J = \sum_i \lambda_i |i\rangle\langle i|$ with $\lambda_i \geq 0$, $\langle i|j\rangle = \delta_{ij}$

define $|\psi_i\rangle \equiv A|i\rangle \Rightarrow \langle\psi_i|\psi_j\rangle = \langle i|A^\dagger A|j\rangle = \langle i|J^2|j\rangle = \lambda_i^2 \delta_{ij}$

if $\lambda_i \neq 0$ define $|e_i\rangle \equiv \frac{1}{\lambda_i}|\psi_i\rangle$

if $\lambda_i = 0$ define $|e_i\rangle \equiv |i\rangle$

$|e_i\rangle$ is orthonormal $\quad \langle e_i|e_j\rangle = \delta_{ij}$

define $U \equiv \sum_i |e_i\rangle\langle i|$ $\quad$ check $UU^\dagger = I$

$$\Rightarrow UJ|i\rangle = \lambda_i|e_i\rangle = \begin{cases} |\psi_i\rangle = A|i\rangle & \lambda_i \neq 0 \\ 0 = |\psi_i\rangle = A|i\rangle & \lambda_i = 0 \end{cases}$$

i.e. $UJ|i\rangle = A|i\rangle$ for all $|i\rangle$

$\Rightarrow UJ = A$

$A = UJ = UJU^\dagger U = KU$ with $K \equiv UJU^\dagger$

check $AA^\dagger = KUU^\dagger K = K^2 \Rightarrow K = \sqrt{AA^\dagger}$

(6) singular value decomposition (for any square matrix)

$A = UDV^\dagger$ with $U^\dagger U = V^\dagger V = I$, $D = \sum_i \lambda_i |i\rangle\langle i|$, $\lambda_i \geq 0$, $\langle i|j\rangle = \delta_{ij}$

nonvanishing values of λ_i are singular vales of A

proof: polar decomposition $A = SJ$ with $SS^+ = I$, $J = \sqrt{A^+A}$

eigen value decomposition of positive matrix $J = TDT^+$ with $TT^+ = I$

$\Rightarrow A = STDT^+ = UDV^+$ with $U \equiv ST$, $V \equiv T$, $UU^+ = VV^+ = I$

note: singular vales of A = nonvanishing eigenvales of $J \equiv \sqrt{A^+A}$

= nonvanishing eigenvales of $K \equiv \sqrt{AA^+}$

(7) singular value decomposition (for general m×n matrix M)

$M_{m\times n} = U_{m\times m}\Sigma_{m\times n}V^+_{n\times n}$ $U^+U = I_{m\times m}$ $V^+V = I_{n\times n}$ $\Sigma = \begin{pmatrix}\sigma_1 & & \\ & \sigma_2 & \\ & & \ddots\end{pmatrix}$, $\sigma_i \geq 0$

positive values of σ_i are singular vales of M

proof: positive matrices $(MM^+)_{m\times m}$ and $(M^+M)_{n\times n}$ have the same positive eigen values

$MM^+u_i = \sigma_i^2 u_i$ with $\sigma_i \geq 0$, $u_i^+u_{i'} = \delta_{ii'}$ $i=1,\cdots,m$

$M^+Mv_j = \sigma_j^2 v_j$ with $\sigma_j \geq 0$, $v_j^+v_{j'} = \delta_{jj'}$ $j=1,\cdots,n$

for $\sigma_i \neq 0$ $(M^+M)(M^+u_i) = \sigma_i^2(M^+u_i)$

$\Rightarrow$ we can choose $M^+u_i \propto v_i \Rightarrow M^+u_i = \sigma_i v_i$

$\Rightarrow Mv_i = \sigma_i u_i$

for $\sigma_i = 0$ $\Rightarrow u_i^+MM^+u_i = 0 \Rightarrow M^+u_i = 0$

for $\sigma_j = 0$ $\Rightarrow v_j^+M^+Mv_j = 0 \Rightarrow Mv_j = 0$

define $U \equiv (u_1 \cdots u_m)$, $V \equiv (v_1 \cdots v_n)$, $\Sigma = \begin{pmatrix}\sigma_1 & & \\ & \sigma_2 & \\ & & \ddots\end{pmatrix}$,

check $M^+u_i = (U\Sigma V^+)^+u_i = \sigma_i v_i$ for all i

$Mv_j = U\Sigma V^+v_j = \sigma_j u_j$ for all j

$\Rightarrow M = U\Sigma V^+$

note: singular values of M = nonvanishing eigenvalues of $\sqrt{M^+M}$

= nonvanishing eigenvalues of $\sqrt{MM^+}$

(8) eigenvalue decomposition	vs. singular value decomposition
only for square normal matrix $M_{m\times m}$	for any matrix $M_{m\times n}$
complex eigenvalues	singular values are positive
$M_{m\times m} = U_{m\times m}\Lambda_{m\times m}U^+_{m\times m}$	$M_{m\times n} = U_{m\times m}\Sigma_{m\times n}V^+_{n\times n}$

if M is Hermitian, real eigenvalues

if M is positive, nonnegative eigenvalues, eigen value n ⇔ singular value n

(9) postulates of quantum mechanics (for pure states)

① state space: Hilbert space $|\psi\rangle$

② evolution: $|\psi'\rangle = U|\psi\rangle$, $U^{+}U = I$ ⇔ $i\hbar \frac{d}{dt}|\psi\rangle = H|\psi\rangle$, $H^{+} = H$

③ measurement: measuring operators $\{M_m\}$
(general)

measuring outcomes m

probability $p(m) = \langle\psi| M_m^{+} M_m |\psi\rangle$

after measurement state $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^{+}M_m|\psi\rangle}}$

completeness equation $\sum_m M_m^{+} M_m = I$ ($\Rightarrow \sum_m p(m) = 1$)

eg: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $M_0 = |0\rangle\langle 0|$ $M_1 = |1\rangle\langle 1|$

$p(0) = |\alpha|^2$ $\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle$

$p(1) = |\beta|^2$ $\frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}|1\rangle$

④ composite system $Q_1 \otimes Q_2 \otimes \cdots$ state $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots$

(10) POVM (positive operator valued measurement)

do not care about the after measurement state

positive operators E_m ($E_m = M_m^{+} M_m$)

probability $p(m) = \langle\psi|E_m|\psi\rangle$

completeness equation $\sum_m E_m = I$ ($\Rightarrow \sum_m p(m) = 1$)

(11) projective measurement: observable $M = \sum_m m P_m$
(a special POVM)

projectors $P_m = |m\rangle\langle m|$ $P_m P_n = \delta_{mn} P_m$

probability $p(m) = \langle\psi|P_m|\psi\rangle$

completeness equation $\sum_m P_m = I$ ($\Rightarrow \sum_m p(m) = 1$)

(12) projective measurement $\xrightarrow{\text{Postulate ②, ④}}$ general measurement

proof: system Q, measuring operators M_m with $\sum_m M_m^{+} M_m = I$

ancilla system M with orthonormal basis $|m\rangle$ (measuring equipment)

define $U \equiv \sum_m M_m \otimes |m\rangle\langle 0|$ for fixed $|0\rangle$ in M

for $\forall$ state $|\psi\rangle$ in Q, there is a state $|\psi\rangle\otimes|0\rangle$ in $Q\otimes M$

there is $(\langle\varphi|\otimes\langle 0|)\, U^\dagger U\, (|\psi\rangle\otimes|0\rangle) = (\langle\varphi|\otimes\langle 0|)(|\psi\rangle\otimes|0\rangle)$

$\Leftrightarrow U^\dagger U = I_Q \otimes |0\rangle\langle 0|$

extend U as a unitary operator in $Q\otimes M$, i.e. that $U^\dagger U = I_Q\otimes I_M$

for $|\psi\rangle\otimes|0\rangle$ in $Q\otimes M$, make an evolution U and then a projective measurement with projectors $P_m = I_Q\otimes|m\rangle\langle m|$

probability $p(m) = \langle\psi|\otimes\langle 0|\, U^\dagger P_m U\, |\psi\rangle\otimes|0\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$

after measurement state $\dfrac{P_m U|\psi\rangle\otimes|0\rangle}{\sqrt{\langle\psi|\otimes\langle 0|\, U^\dagger P_m U\, |\psi\rangle\otimes|0\rangle}} = \dfrac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}\otimes|m\rangle$

(13) lemma: Hilbert space $W\subseteq V$

$U: W\to V$ $\quad\forall w_1, w_2\in W$ $\quad\langle w_1|U^\dagger U|w_2\rangle = \langle w_1|w_2\rangle \Leftrightarrow U^\dagger U = I_W$

$\exists U': V\to V$ $\quad\forall v_1, v_2\in V$ $\quad\langle v_1|U'^\dagger U'|v_2\rangle = \langle v_1|v_2\rangle \Leftrightarrow U'^\dagger U' = I_V$

proof: $\dim V = m$ $\quad\dim W = n$ $\quad m > n$

as $U^\dagger U = I_{n\times n} \Rightarrow U_{m\times n} = (\underset{\uparrow \text{m-vector}}{u_1\cdots u_n})$

$\exists$ other m-vectors $u_{n+1}\cdots u_m$

define $U'_{m\times m} \equiv (u_1\cdots u_n\; u_{n+1}\cdots u_m) \Rightarrow U'^\dagger U' = I_{m\times m}$

(14) Nonorthogonal states cannot be reliably distinguished

proof: if states $|\psi_1\rangle$ and $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$ with $|\alpha|^2+|\beta|^2=1$ $\;0<|\beta|<1$

could be reliably distinguished by measurement $\{M_j\}$, $f(j)=1,2$

$E_1 = \sum\limits_{f(j)=1} M_j^\dagger M_j$, $\quad E_2 = \sum\limits_{f(j)=2} M_j^\dagger M_j$ $\quad$ positive

completeness $E_1+E_2 = I$

$\Rightarrow \langle\psi_1|E_1|\psi_1\rangle = 1$ $\quad\langle\psi_1|E_2|\psi_1\rangle = 0$ $\quad\Rightarrow \sqrt{E_2}|\psi_1\rangle = 0$

$\langle\psi_2|E_1|\psi_2\rangle = 0$ $\quad\langle\psi_2|E_2|\psi_2\rangle = 1$ contradiction !

$\Rightarrow \langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\langle\varphi|E_2|\varphi\rangle \leq |\beta|^2 < 1$

(15) no-cloning theorem: it is impossible to make a copy of an unkown quantum state

proof: if $|\psi\rangle\otimes|s\rangle \xrightarrow{U} U(|\psi\rangle\otimes|s\rangle) = |\psi\rangle\otimes|\psi\rangle$

$|\varphi\rangle\otimes|s\rangle \xrightarrow{U} U(|\varphi\rangle\otimes|s\rangle) = |\varphi\rangle\otimes|\varphi\rangle$

$\Rightarrow \langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2 \Rightarrow \langle\varphi|\psi\rangle = 0$ or $1 \rightarrow$ the same state

$0 \downarrow$ orthogonal states (classical

(16) postulates of quantum mechanics (for mixed states)

① density matrix (density operator)

ρ positive and $\mathrm{tr}\rho = 1 \Leftrightarrow \rho = \sum_i p_i |i\rangle\langle i|, \langle i|j\rangle = \delta_{ij}, 0 \leq p_i \leq 1, \sum_i p_i = 1$

pure state $\rho = |\psi\rangle\langle\psi| \Leftrightarrow \mathrm{tr}\rho^2 = 1$

mixed state $\Leftrightarrow \mathrm{tr}\rho^2 < 1$

② evolution $\rho' = U\rho U^+ \Leftrightarrow i\hbar \frac{d}{dt}\rho = [H, \rho]$

③ measurement: measuring operators $\{M_m\}$, outcomes m

completeness equation $\sum_m M_m^+ M_m = I$

probability $p(m) = \mathrm{tr}(M_m \rho M_m^+)$

after measurement state $\dfrac{M_m \rho M_m^+}{\mathrm{tr}(M_m \rho M_m^+)}$

④ composite system $Q_1 \otimes Q_2 \otimes \cdots$, state $\rho_1 \otimes \rho_2 \otimes \cdots$

(17) unitarity freedom in the ensemble for density matrices

$\rho = \sum_i |\hat{\psi}_i\rangle\langle\hat{\psi}_i| = \sum_j |\hat{\varphi}_j\rangle\langle\hat{\varphi}_j| \Leftrightarrow \exists\, U, U^+U = I, |\hat{\psi}_i\rangle = \sum_j U_{ij}|\hat{\varphi}_j\rangle$

note $\{|\hat{\psi}_i\rangle\}, \{|\hat{\varphi}_j\rangle\}$ are not necessarily orthonormal

proof: "$\Leftarrow$" easy

"$\Rightarrow$" singular value decomposition $\rho = \sum_k \lambda_k |k\rangle\langle k| = \sum_k |\hat{k}\rangle\langle\hat{k}|$

$\{|k\rangle\}$ orthonormal, $|\hat{k}\rangle \equiv \sqrt{\lambda_k}\,|k\rangle$

$\forall\, |\psi\rangle$ orthogonal to $\{|k\rangle\}$ is also orthogonal to $\{|\hat{\psi}_i\rangle\}$

$0 = \langle\psi|\rho|\psi\rangle = \sum_i |\langle\psi|\hat{\psi}_i\rangle|^2 = 0 \Rightarrow \langle\psi|\hat{\psi}_i\rangle = 0$

$\Rightarrow |\hat{\psi}_i\rangle = \sum_k c_{ik}|\hat{k}\rangle \Rightarrow \rho = \sum_k |\hat{k}\rangle\langle\hat{k}| = \sum_{k,l} \sum_i (c_{ik}c_{il}^*) |\hat{k}\rangle\langle\hat{l}|$

$\Rightarrow \sum_i c_{ik}c_{il}^* = \delta_{kl} \Rightarrow \exists\, V, V^+V = I$ s.t. $|\hat{\psi}_i\rangle = \sum_k V_{ik}|\hat{k}\rangle$

similarly $\exists\, W, W^+W = I \quad |\hat{\varphi}_j\rangle = \sum_k W_{jk}|\hat{k}\rangle$

$\Rightarrow |\hat{\psi}_i\rangle = \sum_j u_{ij}|\hat{\varphi}_j\rangle, \ u \equiv VW^+$

(18) reduced density matrix (RDM) AB in state ρ_{AB}, A in state $\rho_A = \mathrm{tr}_B\rho_{AB}$

partial trace $\mathrm{tr}_B |a_1 b_1\rangle\langle a_2 b_2| = |a_1\rangle\langle a_2|\, \mathrm{tr}_B(|b_1\rangle\langle b_2|)$

(19) Schmidt decomposition: AB in pure state $|\psi\rangle$, $\exists$ orthonormal states $|i_A\rangle$ in A and $|i_B\rangle$ in B, s.t. $|\psi\rangle = \sum_i \lambda_i |i_A i_B\rangle$

w/ Schmidt coefficients $\lambda_i \geq 0$, $\sum_i \lambda_i^2 = 1$

proof: general pure state $|\psi\rangle = \sum_{jk} a_{jk} |jk\rangle$

w/ orthonormal states $|j\rangle$, $|k\rangle$ in A, B

note dim A, dim B could be different

singular value decomposition $a = \underset{\uparrow}{u}\,\overset{\swarrow \text{diagonal}}{d}\,v$

unitary

$\Rightarrow |\psi\rangle = \sum_{ijk} u_{ji} d_{ii} v^*_{ki} |jk\rangle$

$= \sum_i \lambda_i |i_A i_B\rangle$

w/ definitions $\lambda_i \equiv d_{ii}$, $|i_A\rangle \equiv \sum_j u_{ji} |j\rangle$, $|i_B\rangle \equiv \sum_k v^*_{ki} |k\rangle$

RDM: $\rho_A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$, $\rho_B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$

(20) purification: $\rho_A = \sum_i p_i |i_A\rangle\langle i_B|$ in a mixed state

introduce a reference system R such that AR in pure state $\mathrm{tr}_R |AR\rangle\langle AR| = \rho_A$

eg $|AR\rangle = \sum_i \sqrt{p_i} |i_A i_R\rangle$

(21) Bell inequality (CHSH inequality)

↳ Clauser, Horne, Shimony, Holt

classically satisfied but quantum mechanically broken

Alice	Bob
one particle	another particle
objective properties $Q = \pm 1$, $R = \pm 1$	objective properties $S = \pm 1$, $T = \pm 1$
measure Q or R	measure S or T

at the same time

$$QS + RS + RT - QT = (Q+R)S + (R-Q)T = \pm 2 \leq 2$$

either of them is zero

$$E(QS+RS+RT-QT) = \sum_{q,r,s,t} p(q,r,s,t)(qs+rs+rt-qt)$$

$$\leq \sum_{q,r,s,t} p(q,r,s,t) \times 2 = 2$$

$$E(QS+RS+RT-QT) \leq 2$$

quantum violation $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, $Q = Z_1$, $R = X_1$, $S = \frac{-Z_2 - X_2}{\sqrt{2}}$, $T = \frac{Z_2 - X_2}{\sqrt{2}}$

$$\Rightarrow \langle QS \rangle = \langle RS \rangle = \langle RT \rangle = -\langle QT \rangle = \frac{1}{\sqrt{2}}$$

$$\Rightarrow \langle QS + RS + RT - QT \rangle = 2\sqrt{2} > 2$$

assumptions in derive Bell inequality

local realism / realism: properties Q, R, S, T exist independent of observation
\ locality: Alice's measurement does not influence Bob's measuring result

⇒ either realism or locality or both should be dropped

3. quantum operations and quantum noises

(1) quantum operation $\underset{\uparrow}{\rho} \xrightarrow{\varepsilon} \rho' = \underset{\nwarrow}{\varepsilon(\rho)}$

old density matrix new density matrix

eg: unitary evolution $\varepsilon(\rho) = U \rho U^{\dagger}$

measurement $\varepsilon_m(\rho) = M_m \rho M_m^{\dagger}$ w/ M_m one of the measuring operators $\{M_m\}$

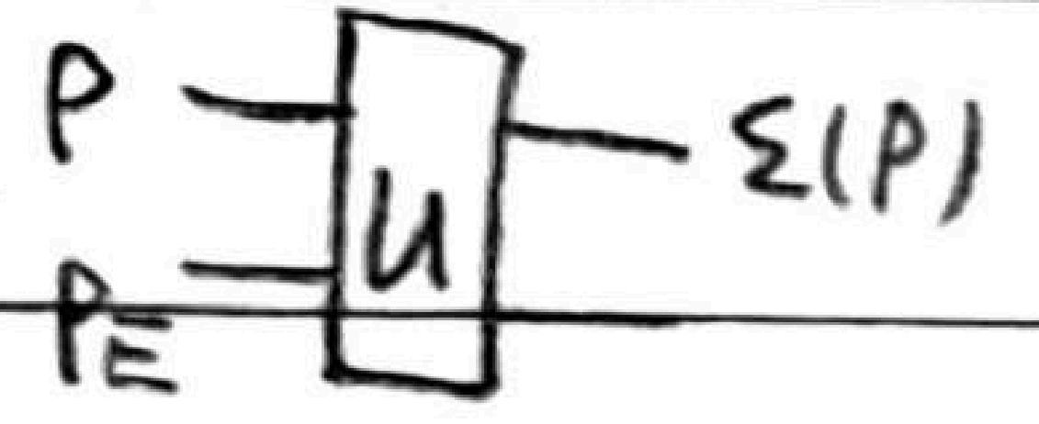
three equivalent approaches ① system coupled to environment (natural)
$\Updownarrow$
② operator-sum approach (convenient)
$\Updownarrow$
③ axiomatic approach (general)

(2) system coupled to environment

trace-preserving quantum operation $\mathrm{tr}\,\varepsilon(\rho) = 1$

$$\varepsilon(\rho) = \mathrm{tr}_E\left[U(\underset{\uparrow}{\rho} \underbrace{\otimes}_{} \underset{\nwarrow}{\rho_E})U^{\dagger}\right]$$

open closed environment



$U^{\dagger}U = 1$

unitary evolution

w/ loss of generality $\rho_{env} = |e_0\rangle\langle e_0|$ (remember purification)

non-trace-preserving quantum operation $\mathrm{tr}\,\varepsilon(\rho) < 1$

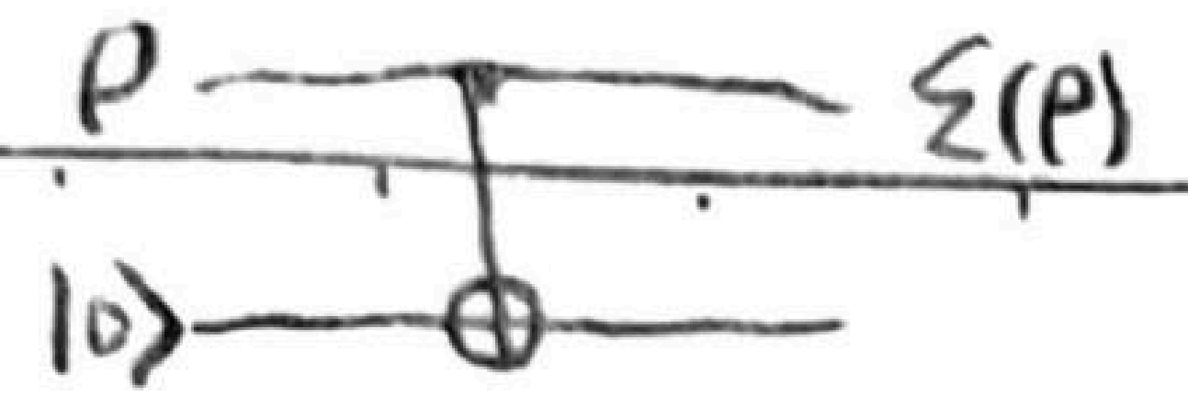
$\varepsilon(\rho) = \mathrm{tr}_E[P U(\rho \otimes \rho_E) U^{\dagger} P]$ projector P w/ $P^{\dagger} = P^2 = P$

(3) operator-sum approach

$\varepsilon(\rho) = \sum_k E_k \rho E_k^{\dagger}$ with operation elements $\{E_k\}$

trace-preserving ": $\sum_k E_k^{\dagger} E_k = I$, probability $p = \varepsilon(\rho) = 1$

non-trace-preserving ": $\sum_k E_k^{\dagger} E_k \leq I$, probability $p = \varepsilon(\rho)$ w/ $0 < p < 1$

$p = 0$ trivial, $p = 1$ trace-preserving eg 

CNOT gate, $U = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$

$\mathcal{E}(\rho) = \mathrm{tr}_E\left[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\right] = P_0 \rho P_0 + P_1 \rho P_1$ w/ $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$

(4) system coupled to environment $\Leftrightarrow$ operator-sum approach

proof: orthonormal basis of E $\{|e_k\rangle\}$

trace-preserving $\mathcal{E}$

"$\Rightarrow$" $\mathcal{E}(\rho) = \sum_k \langle e_k| U(\rho \otimes |e_0\rangle\langle e_0|) U^\dagger |e_k\rangle$

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

$\mathrm{tr}\,\mathcal{E}(\rho) = 1 \Rightarrow \sum_k E_k^\dagger E_k = I_Q$

"$\Leftarrow$" def $U = \sum_k E_k \otimes |e_k\rangle\langle e_0|$

$\Rightarrow U^\dagger U = \left(\sum_k E_k^\dagger E_k\right) \otimes |e_0\rangle\langle e_0| = I_Q \otimes |e_0\rangle\langle e_0|$

extend U s.t. $U^\dagger U = I_Q \otimes I_R$

non-trace-preserving $\mathcal{E}$

"$\Rightarrow$" $\mathcal{E}(\rho) = \sum_k \langle e_k| P U(\rho \otimes |e_0\rangle\langle e_0|) U^\dagger P |e_k\rangle$

$= \sum_k E_k \rho E_k^\dagger$ with $E_k = \langle e_k|PU|e_0\rangle$

$\mathrm{tr}\,\mathcal{E}(\rho) < 1 \Rightarrow \sum_k E_k^\dagger E_k < I$

"$\Leftarrow$" projector $P = I_Q \otimes \sum_k |e_k\rangle\langle e_k|$ (before extension)

add $\sqrt{I - \sum_k E_k^\dagger E_k}$ to operation elements s.t. $\sum_k E_k^\dagger E_k = I_Q$

construct U s.t. $U^\dagger U = I_Q \otimes I_R$

(5) axiomatic approach

A1: $0 \le \mathrm{tr}\,\mathcal{E}(\rho) \le 1$ probability that the operation occurs $p(\mathcal{E}) = \mathrm{tr}\,\mathcal{E}(\rho)$

A2: $\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i)$

$\{p_i, \rho_i\} \xrightarrow{p(\mathcal{E})} \left\{\underset{\uparrow}{p(i|\mathcal{E})}, \frac{\mathcal{E}(\rho_i)}{\mathrm{tr}\,\mathcal{E}(\rho_i)}\right\}$

conditional probability

Bayes' rule $p(i|\mathcal{E}) = \frac{p(\mathcal{E}|i)\, p_i}{p(\mathcal{E})} = \frac{\mathrm{tr}\,\mathcal{E}(\rho_i)\, p_i}{\mathrm{tr}\,\mathcal{E}(\rho)}$

before operation $\rho = \sum_i p_i \rho_i$

after operation $\frac{\mathcal{E}(\rho)}{\mathrm{tr}\,\mathcal{E}(\rho)} = \sum_i p(i|\mathcal{E}) \frac{\mathcal{E}(\rho_i)}{\mathrm{tr}\,\mathcal{E}(\rho_i)} \Rightarrow \mathcal{E}(\rho) = \sum_i p_i \mathcal{E}(\rho_i)$

A3: $P \in Q$, positive $\Rightarrow$ $\mathcal{E}(P)$ positive

$P \in RQ$ positive $\Rightarrow (I_R \otimes \mathcal{E})(P)$ positive R is a reference system

(6) axiomatic approach $\Leftrightarrow$ operator-sum approach

proof: "$\Leftarrow$" $\forall\ P, |\psi\rangle \in RQ$, define $|\varphi_i\rangle \equiv (I_R \otimes E_i^{+})|\psi\rangle$

$$\Rightarrow \langle\psi|(I_R \otimes \mathcal{E})(P)|\psi\rangle = \sum_i \langle\psi|(I_R \otimes E_i)\,P\,(I_R \otimes E_i^{+})|\psi\rangle = \sum_i \langle\varphi_i|P|\varphi_i\rangle \geqslant 0$$

"$\Rightarrow$" orthonormal basis $|i_R\rangle, |i_Q\rangle$

define $|\alpha\rangle \equiv \sum_i |i_R\rangle \otimes |i_Q\rangle$

$$\sigma \equiv (I_R \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|)$$

for $\forall\ |\psi\rangle = \sum_i \psi_i |i_Q\rangle \in Q$, define $|\check{\psi}\rangle = \sum_i \psi_i^{*} |i_R\rangle \in R$

$\Rightarrow \langle\check{\psi}|\sigma|\check{\psi}\rangle = \mathcal{E}(|\psi\rangle\langle\psi|)$

eigenvalue decomposition $\sigma \overset{A3}{=} \sum_i |s_i\rangle\langle s_i|$ w/ $|s_i\rangle \in RQ$

define E_i in Q s.t. $E_i|\psi\rangle = \langle\check{\psi}|s_i\rangle \in Q$, check E_i is linear

$$\Rightarrow \sum_i E_i|\psi\rangle\langle\psi|E_i^{+} = \langle\check{\psi}|\sum_i |s_i\rangle\langle s_i|\check{\psi}\rangle = \langle\check{\psi}|\sigma|\check{\psi}\rangle = \mathcal{E}(|\psi\rangle\langle\psi|)$$

$$\overset{A2}{\Longrightarrow} \mathcal{E}(\rho) = \sum_i E_i \rho E_i^{+}$$

(7) operation elements are not unique

eg $E_1 = \frac{I}{\sqrt{2}}$, $E_2 = \frac{Z}{\sqrt{2}}$, $F_1 = \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$ $F_2 = \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}$ $\mathcal{E}(\rho) = \mathcal{F}(\rho)$

$\mathcal{E}\ \{E_i\}$, $\mathcal{F}\ \{F_j\}$, $\mathcal{E} = \mathcal{F} \Leftrightarrow E_i = \sum_j u_{ij} F_j$ $u^{+}u = I$

proof: "$\Leftarrow$" easy

"$\Rightarrow$" quantum system Q, reference system R

orthonormal basis $|k_R\rangle, |k_Q\rangle$

define $|e_i\rangle \equiv \sum_k |k_R\rangle \otimes (E_i|k_Q\rangle)$

$$|f_j\rangle \equiv \sum_k |k_R\rangle \otimes (F_j|k_Q\rangle)$$

$$\alpha = \sum_k |k_R\rangle \otimes |k_Q\rangle$$

$$\sigma = (I_R \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|) = (I_R \otimes \mathcal{F})(|\alpha\rangle\langle\alpha|)$$

$$\Rightarrow \sigma = \sum_i |e_i\rangle\langle e_i| = \sum_j |f_j\rangle\langle f_j|$$

$$\Rightarrow |e_i\rangle = \sum_j u_{ij} |f_j\rangle$$

$\forall\ |\psi\rangle = \sum_k \psi_k |k_Q\rangle \in Q$, define $|\check{\psi}\rangle \equiv \sum_k \psi_k^{*} |k_R\rangle \in R$

$$\Rightarrow E_i|\psi\rangle = \langle \tilde{\psi}|e_i\rangle = \sum_j u_{ij} \langle \tilde{\psi}|f_j\rangle = \sum_j u_{ij} F_j|\psi\rangle \Rightarrow E_i = \sum_j u_{ij} F_j$$

(8) trace and partial trace as quantum operations

trace: $E_i \equiv |0\rangle\langle i|$ $\quad \mathcal{E}(\rho) = \sum_i \langle i|\rho|i\rangle\, |0\rangle\langle 0| = \mathrm{tr}\rho\ |0\rangle\langle 0|$

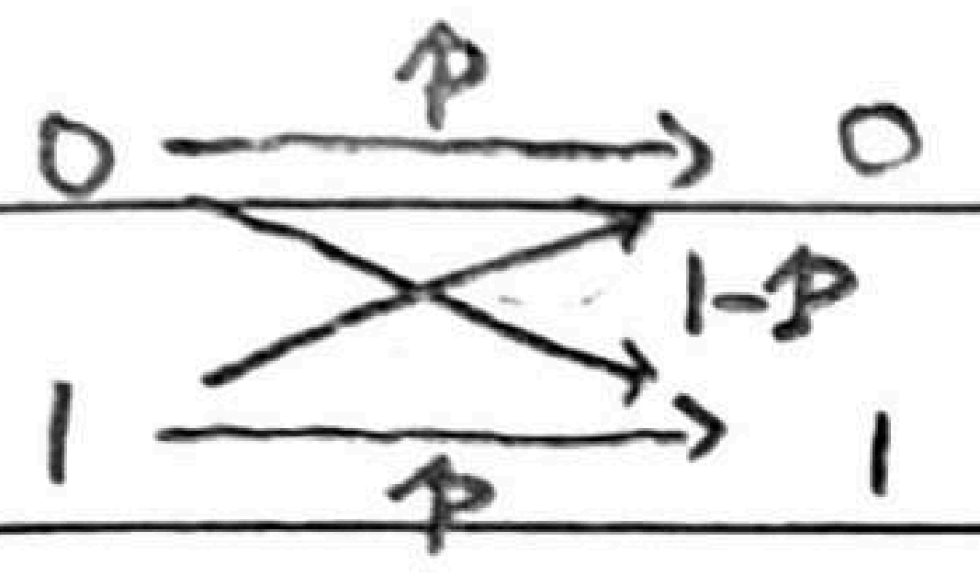
partial trace: quantum system Q, reference system R

$$E_i = I_Q \otimes |0_R\rangle\langle i_R|$$

$$\mathcal{E}(|i_Q j_R\rangle\langle k_Q l_R|) = \delta_{j_R l_R} (|i_Q\rangle\langle k_Q|) \otimes (|0_R\rangle\langle 0_R|)$$

$$\Rightarrow \mathcal{E}(\rho_{QR}) = (\mathrm{tr}_R\, \rho_{QR}) \otimes (|0_R\rangle\langle 0_R|)$$

(9) classical noise bit flip

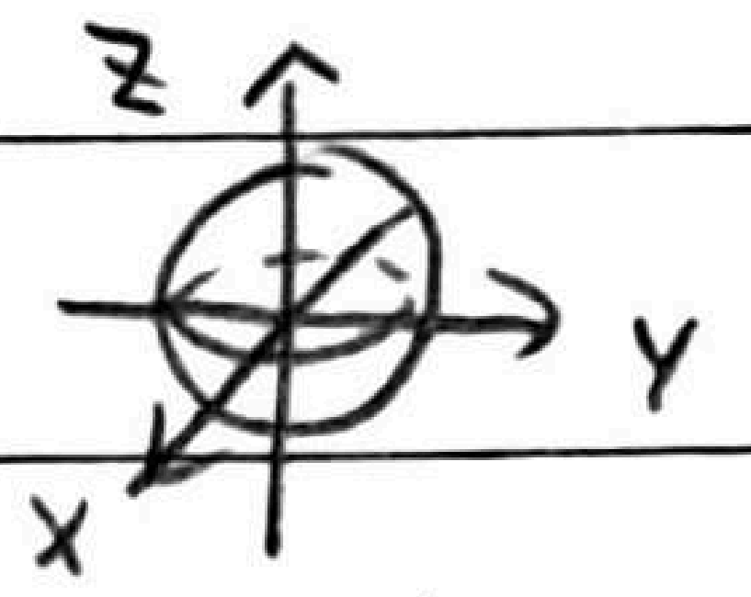


Markow process $\begin{pmatrix} q_0' \\ q_1' \end{pmatrix} = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$

(10) quantum noises as quantum operations

general single qubit state $\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$

$\vec{r} = (x, y, z)$ $\quad \vec{\sigma} = (X, Y, Z)$ $\quad |\vec{r}| \leq 1$



Bloch sphere

① bit flip $\mathcal{E}(\rho) = p\rho + (1-p) X\rho X$ $\quad$ note $\alpha|0\rangle + \beta|1\rangle \xrightarrow{X} \alpha|1\rangle + \beta|0\rangle$

operation elements $E_0 = \sqrt{p}\, I$, $E_1 = \sqrt{1-p}\, X$

② phase flip $\mathcal{E}(\rho) = p\rho + (1-p) Z\rho Z$ $\quad$ note $\alpha|0\rangle + \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle - \beta|1\rangle$

③ bit-phase flip $\mathcal{E}(\rho) = p\rho + (1-p) Y\rho Y$

④ depolarizing $\mathcal{E}(\rho) = p\rho + (1-p)\frac{I}{2}$

⑤ amplitude damping $\quad E_0 = \begin{pmatrix} 1 & \\ & \sqrt{1-\gamma} \end{pmatrix}$ $\quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$ $\quad 0 \leq \gamma \leq 1$

$|0\rangle \xrightarrow{\mathcal{E}} |0\rangle$ $\quad |1\rangle \xrightarrow{\mathcal{E}} \begin{pmatrix} \gamma & \\ & 1-\gamma \end{pmatrix}$

Hamiltonian $H = \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}$ $\quad$ ground state $|0\rangle$
excited state $|1\rangle$

$\mathrm{tr}(H\mathcal{E}(\rho)) = \sqrt{1-\gamma}\ \mathrm{tr}(H\rho)$ energy is lost

⑥ phase damping $\quad E_0 = \begin{pmatrix} 1 & \\ & \sqrt{1-\lambda} \end{pmatrix}$ $\quad E_1 = \begin{pmatrix} 0 & \\ & \sqrt{\lambda} \end{pmatrix}$ $\quad 0 < \lambda < 1$

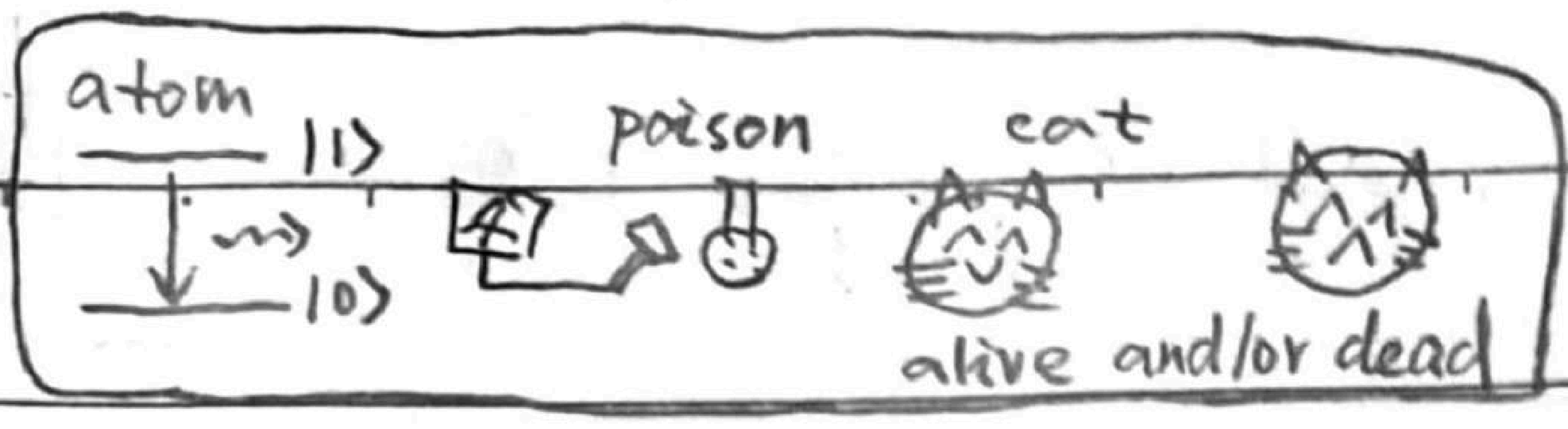
$|0\rangle \xrightarrow{\mathcal{E}} |0\rangle$ $\quad |1\rangle \xrightarrow{\mathcal{E}} |1\rangle$ $\quad \mathrm{tr}(H\mathcal{E}(\rho)) = \mathrm{tr}(H\rho)$ no energy loss

$(x, y, z) \xrightarrow{\mathcal{E}} (\sqrt{1-\lambda}\, x, \sqrt{1-\lambda}\, y, z)$ (equivalent to phase flip)

$\lambda \to 1$ or many phase dampings $\overset{\text{quantum}}{(x, y, z)} \rightsquigarrow \overset{\text{classical}}{(0, 0, z)}$

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \to \rho = \frac{1}{2}\begin{pmatrix} 1+z & \\ & 1-z \end{pmatrix}$$

Schrodinger's cat



$$\overset{\text{cat}}{}\ \overset{\text{atom}}{} \quad |\psi\rangle = |\text{alive}, 1\rangle$$

$$\rightarrow |\text{alive}\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\rightarrow \frac{1}{\sqrt{2}}(|\text{dead}, 0\rangle + |\text{alive}, 1\rangle)$$

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix} \xrightarrow[\text{damping}]{\text{phase}} \frac{1}{2}\begin{pmatrix}1&\\&1\end{pmatrix} \xrightarrow{\text{wave function collapses}} \begin{pmatrix}1&0\\0&0\end{pmatrix} \text{ or } \begin{pmatrix}0&0\\0&1\end{pmatrix}$$

quantum uncertainty — dead and alive

decoherence

classical uncertainty — dead or alive

(11) quantum state tomography: determine an unknown quantum state experimentally

single qubit $\rho = \frac{1}{2}(I + \mathrm{tr}(\rho X)X + \mathrm{tr}(\rho Y)Y + \mathrm{tr}(\rho Z)Z)$

n-qubit $\rho = \frac{1}{2^n}\sum_{\vec{v}} \mathrm{tr}(\rho\, \sigma^{v_1} \otimes \sigma^{v_2} \otimes \cdots \otimes \sigma^{v_n})\, \sigma^{v_1} \otimes \sigma^{v_2} \otimes \cdots \otimes \sigma^{v_n}$

$\vec{v} = (v_1, v_2, \cdots, v_n) \quad v_i = 0, 1, 2, 3$

(12) quantum process tomography: determine an unkown quantum operation experimentally

dimension of Hilbert space d

basis of operators $\hat{E}_m$: $|a\rangle\langle a|$, $|a\rangle\langle b|$ with $a \neq b$, $a, b = 1, 2, \cdots, d$, $m = 1, 2, \cdots, d^2$

$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ w/ operation elements $E_i = \sum_m e_{im} \hat{E}_m$

$= \sum_{m,n} \chi_{mn} \hat{E}_m \rho \hat{E}_n^\dagger$ with $\chi_{mn} \equiv \sum_i e_{im} e_{in}^*$ $d^2 \times d^2$ positive matrix

$\uparrow$ to be determined

constraint $\sum_i E_i^\dagger E_i = I$

independent real parameters $d^4 - d^2$

eg single qubit $d = 2$, $d^4 - d^2 = 12$

basis for ρ: ρ_j $j = 1, 2, \cdots, d^2$

by state tomography $\mathcal{E}(\rho_j) = \sum_k \lambda_{jk} \rho_k$ ⟩ ⇒ $\sum_{m,n} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk}$

calculate $\hat{E}_m \rho_j \hat{E}_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k$

view β_{jk}^{mn} (mn — column, jk — row) $d^2 \times d^2 \times d^2 \times d^2$ tensor → $d^4 \times d^4$ matrix

χ_{mn}, λ_{jk} $d^2 \times d^2$ tensor → d^4-vector

$\Rightarrow \beta\chi = \lambda$ if β invertible $\chi = \beta^{-1}\lambda$

if β non-invertible $\chi = \kappa\lambda$ with κ defined as $\beta = \beta\underset{}{\overset{\substack{\text{generalized inverse, not unique}\\ \downarrow}}{\kappa}}\beta$

check: $\exists\, \chi'$ s.t. $\beta\chi' = \lambda \Rightarrow \beta\chi = \beta\kappa\lambda = \beta\kappa\beta\chi' = \beta\chi' = \lambda$

eigenvalue decomposition $X_{mn} = \sum_i U_{mi} d_i U^*_{ni}$ $d_i \geq 0$

$\Rightarrow e_{im} = \sqrt{d_i}\, U_{mi} \Rightarrow E_i = \sqrt{d_i} \sum_m U_{mi} \check{E}_m$

4. Distance measures

(1) distance (metric)

① $d(X,Y) \geq 0$ nonnegativity

② $d(X,Y) = 0 \Leftrightarrow X = Y$ identity of indiscernible

③ $d(X,Y) = d(Y,X)$ symmetric

④ $d(X,Z) \leq d(X,Y) + d(Y,Z)$ triangle inequality / subadditivity

"divergence"

① $d(X,Y) \geq 0$

② $d(X,Y) = 0 \Leftrightarrow X = Y$

eg: relative entropy (Kullback-Leibler divergence)

(2) Hamming distance for classical bits: number of different places

eg $D(\overset{\downarrow}{0}001\underset{\uparrow}{0}, \overset{\downarrow}{1}001\underset{\uparrow}{1}) = 2$

(3) classical trace distance (L1 distance, Kolmogorov distance)

two probability distributions $\{P_x\}, \{q_x\}$

$D(P_x, q_x) \equiv \frac{1}{2} \sum_x |P_x - q_x| = \max_{S \subseteq \{x\}} (P(S) - q(S))$ $0 \leq D(P_x, q_x) \leq 1$

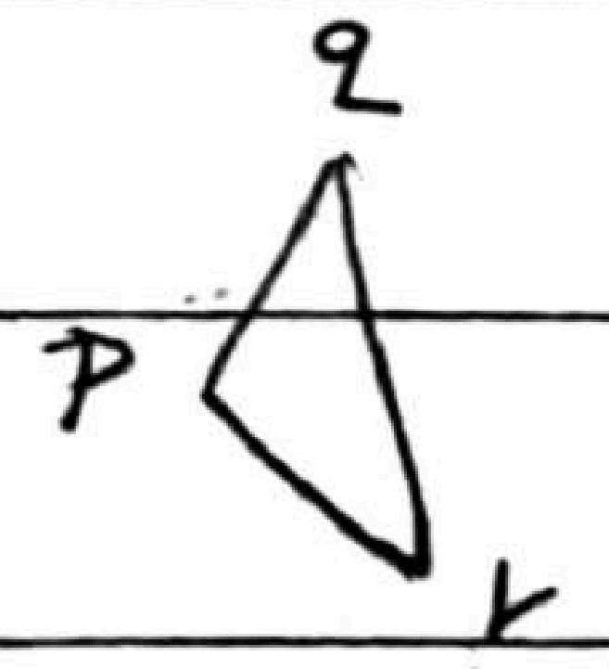
proof: define $S_+ \equiv \{x \mid P_x - q_x > 0\}$ $S_- \equiv \{x \mid P_x - q_x \leq 0\}$

$$D(P_x, q_x) = \frac{1}{2}(P(S_+) - q(S_+)) - \frac{1}{2}(P(S_-) - q(S_-))$$
$$= P(S_+) - q(S_+)$$

note $P(S_+) + P(S_-) = q(S_+) + q(S_-) = 1$

$$= \max_{S \subseteq \{x\}} (P(S) - q(S))$$

triangle inequality: $D(P_x, q_x) = P(S_+) - q(S_+)$



$$= P(S_+) - r(S_+) + r(S_+) - q(S_+)$$
$$\leq D(P_x, r_x) + D(r_x, q_x)$$

static measure: distance of two probability distributions

dynamic measure: distance of one probability before and after a dynamic process

$$\begin{tikzcd} \check{X} \arrow[r, dashed, no head] \arrow[d, no head] & \check{X} \arrow[d, no head] \\ X \arrow[r, "\text{noises}"] & Y \end{tikzcd}$$

← an exact copy of X

two joint distributions $P(\check{X} = x_1, X = x_2) = \delta_{x_1 x_2} P(X = x_2)$

$P(\check{X} = x_1, Y = x_2)$ unknown

$$D((\check{X}, X), (\check{X}, Y)) = \frac{1}{2} \sum_{x_1, x_2} \left| \delta_{x_1 x_2} P(X = x_2) - P(\check{X} = x_1, Y = x_2) \right|$$
$$= \frac{1}{2} \sum_{x_1 \neq x_2} P(\check{X} = x_1, Y = x_2) + \frac{1}{2} \sum_x \left| P(X = x) - P(\check{X} = x, Y = x) \right|$$

$$= \frac{1}{2} \sum_{x_1 \neq x_2} p(X=x_1, Y=x_2) + \frac{1}{2} \sum_x \left(p(X=x) - p(X=x, Y=x) \right)$$

$$= \frac{1}{2} \left(p(X \neq Y) + 1 - p(X=Y) \right)$$

$$= p(X \neq Y)$$

(4) classical fidelity: $F(p_x, q_x) = \sum_x \sqrt{p_x q_x}$ $\quad 0 \leq F \leq \overset{p_x = q_x \swarrow}{1}$

distance: quantitative dissimilarity

fidelity: quantitative similarity

(5) quantum trace distance

for two quantum states ρ and σ $\quad D(\rho, \sigma) \equiv \frac{1}{2} \operatorname{tr}|\rho - \sigma|$

any square matrix $|A| = \sqrt{AA^\dagger}$ $\quad \operatorname{tr}|A| =$ sum of singular values of A

= sum of eigenvalues of $\sqrt{AA^\dagger}$

= sum of eigenvalues of $\sqrt{A^\dagger A}$

if A hermitian $\searrow$ = sum of absolute values of eigenvalues of A

if A positive $\searrow$ = sum of eigenvalues of A

① if ρ and σ commute $\quad \rho = \sum_i r_i |i\rangle\langle i| \quad \sigma = \sum_i s_i |i\rangle\langle i|$

$$D(\rho, \sigma) = D(r_i, s_i)$$

② single qubit $\quad \rho = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}) \quad \sigma = \frac{1}{2}(I + \vec{s} \cdot \vec{\sigma})$

$D(\rho, \sigma) = \frac{1}{4} \operatorname{tr}\left|(\vec{r} - \vec{s}) \cdot \vec{\sigma}\right| = \frac{1}{2}|\vec{r} - \vec{s}|$ ← Euclidean distance

③ $D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma)$

④ $D(\rho, \sigma) = \max\limits_P \operatorname{tr}[P(\rho - \sigma)]$ projector P

proof: eigenvalue decomposition $\rho - \sigma = U \Lambda U^\dagger$

real diagonal matrix Λ with $\operatorname{tr}\Lambda = 0$

$\Lambda = \Lambda_+ + \Lambda_-$, $\Lambda_\pm$ w/ positive/negative eigenvalues of Λ

define orthogonal positive operators $Q \equiv U\Lambda_+U^\dagger$, $S \equiv -U\Lambda_-U^\dagger$

$\operatorname{tr}Q = \operatorname{tr}S$

$\Rightarrow \rho - \sigma = Q - S \Rightarrow |\rho - \sigma| = Q + S \Rightarrow \operatorname{tr}|\rho - \sigma| = \operatorname{tr}Q + \operatorname{tr}S = 2\operatorname{tr}Q$

$\exists P$ projector on Q $\quad \operatorname{tr}[P(\rho - \sigma)] = \operatorname{tr}[P(Q - S)] = \operatorname{tr}PQ = \operatorname{tr}Q = D(\rho, \sigma)$

for general P $\quad \operatorname{tr}[P(\rho - \sigma)] = \operatorname{tr}[P(Q - S)] \leq \operatorname{tr}(PQ) \leq \operatorname{tr}Q = D(\rho, \sigma)$

⑤ $D(\rho,\sigma) = \max_{\{E_m\}} D(p_m, q_m)$ POVM $\{E_m\}$ w/ $\sum_m E_m = I$

probabilities $p_m = tr(\rho E_m)$, $q_m = tr(\sigma E_m)$

proof: choose $E_m = U\begin{pmatrix}0 & & & & \\ & \ddots & & & \\ & & 0\,1\,0 & & \\ & & & \ddots & \\ & & & & 0\end{pmatrix}U^+ \Rightarrow D(\rho,\sigma) = D(p_m, q_m)$

general $\{E_m\}$ $D(p_m, q_m) = \frac{1}{2}\sum_m \left| tr\left[E_m(\rho-\sigma)\right]\right|$

$$= \frac{1}{2}\sum_m \left| tr\left[E_m(Q-S)\right]\right|$$

$$= \frac{1}{2}\sum_m \left| tr(E_m Q) - tr(E_m S)\right|$$

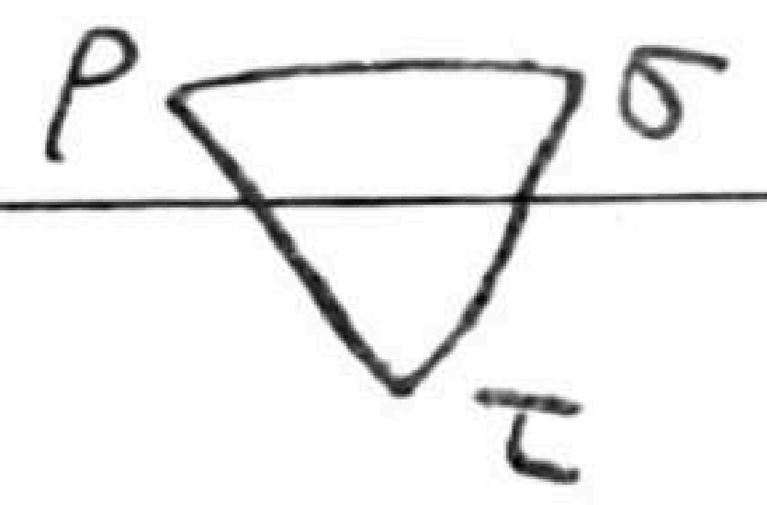
$$\leq \frac{1}{2}\sum_m \left(tr\, E_m Q + tr\, E_m S\right)$$

$$= \frac{1}{2}\sum_m tr\left[E_m(Q+S)\right]$$

$$= \frac{1}{2} tr(Q+S) = D(\rho,\sigma)$$

corollary: $0 \leq D(\rho,\sigma) \leq 1$

⑥ triangle inequality $D(\rho,\sigma) \leq D(\rho,\tau) + D(\tau,\sigma)$



proof: $\exists$ projector P s.t. $D(\rho,\sigma) = tr\left[P(\rho-\sigma)\right]$

$$= tr\left[P(\rho-\tau)\right] + tr\left[P(\tau-\sigma)\right]$$

$$\leq D(\rho,\tau) + D(\tau,\sigma)$$

⑦ trace-preserving quantum operation reduces trace distance

$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho,\sigma)$

proof: $\rho - \sigma \overset{!}{=} Q - S$ $\quad \mathcal{E}(\rho) - \mathcal{E}(\sigma) = \mathcal{E}(Q) - \mathcal{E}(S)$

Q, S orthogonal positive

$\mathcal{E}(Q), \mathcal{E}(S)$ positive, not necessarily orthogonal

$\exists$ projector P, $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = tr\left(P\left[\mathcal{E}(\rho) - \mathcal{E}(\sigma)\right]\right)$

$$= tr\left(P\left[\mathcal{E}(Q) - \mathcal{E}(S)\right]\right)$$

$$\leq tr\, P\mathcal{E}(Q)$$

$$\leq tr\, \mathcal{E}(Q)$$

$$= tr\, Q$$

$$= D(\rho,\sigma)$$

eg: partial trace $D(\rho_A, \sigma_A) \leq D(\rho_{AB}, \sigma_{AB})$

 vs  distinguishability lost for partial trace

⑧ strong convexity 凸 $\cancel{\cup}$

$D(\sum_i p_i \rho_i, \sum_i q_i \sigma_i) \leq D(p_i, q_i) + \sum_i p_i D(\rho_i, \sigma_i)$

proof: $\exists P$ $D(\sum_i p_i \rho_i, \sum_i q_i \sigma_i) = \sum_i p_i \, tr(P\rho_i) - \sum_i q_i \, tr(P\sigma_i)$

$= \sum_i p_i \, tr[P(\rho_i - \sigma_i)] + \sum_i (p_i - q_i) \, tr(P\sigma_i)$

$\leq \sum_i p_i D(\rho_i, \sigma_i) + D(p_i \, q_i)$

⑨ joint convexity $D(\sum_i p_i \rho_i, \sum_i p_i \sigma_i) \leq \sum_i p_i D(\rho_i, \sigma_i)$

⑩ convexity $D(\sum_i p_i \rho_i, \sigma) \leq \sum_i p_i D(\rho_i, \sigma)$

(6) quantum fidelity $F(\rho, \sigma) \equiv tr\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$

① $F(\rho,\sigma) = F(\sigma,\rho)$ proof: $|X| = \sqrt{XX^\dagger} \Rightarrow |\sqrt{\rho}\sqrt{\sigma}| = \sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$

$|\sqrt{\sigma}\sqrt{\rho}| = \sqrt{\sqrt{\sigma}\,\rho\sqrt{\sigma}}$

$\sqrt{\rho}\sqrt{\sigma} = (\sqrt{\sigma}\sqrt{\rho})^\dagger$

note $M, M^\dagger$ have the same singular values

$M = U\Sigma V^\dagger \quad M^\dagger = V\Sigma^\dagger U^\dagger$

$\Rightarrow tr|\sqrt{\rho}\sqrt{\sigma}| = tr|\sqrt{\sigma}\sqrt{\rho}| \Rightarrow F(\rho,\sigma) = F(\sigma,\rho)$

② $F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$

③ Uhlmann's theorem $F(\rho,\sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|$ w/ $|\psi\rangle, |\phi\rangle$ purify ρ, σ

proof: quantum system Q, reference system R

orthogonal basis $|i_Q\rangle$ $|i_R\rangle$

define $|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle \in RQ$

general $|\psi\rangle = (U_R \otimes \sqrt{\rho}\, U_Q)|m\rangle = \sum_i U_R|i_R\rangle \otimes \sqrt{\rho}\, U_Q|i_Q\rangle$

$|\phi\rangle = (V_R \otimes \sqrt{\rho}\, V_Q)|m\rangle = \sum_i V_R|i_R\rangle \otimes \sqrt{\sigma}\, V_Q|i_Q\rangle$

check $tr_R|\psi\rangle\langle\psi| = \rho$, $tr_R|\phi\rangle\langle\phi| = \sigma$

$|\langle\psi|\phi\rangle| = |\langle m| U_R^\dagger V_R \otimes U_Q^\dagger \sqrt{\rho}\sqrt{\sigma}\, V_Q|m\rangle|$

$= |tr(V_R^T U_R^* U_Q^\dagger \sqrt{\rho}\sqrt{\sigma}\, V_Q)|$ (use $tr(A^T B) = \langle m|A\otimes B|m\rangle$)

$= |tr(\sqrt{\rho}\sqrt{\sigma}\, U)|$ $(U \equiv V_Q V_R^T U_R^* U_Q^\dagger)$

equality with choice $U=I$ $\rightarrow$ $\leq tr|\sqrt{\rho}\sqrt{\sigma}|$ (use…)

$= F(\rho, \sigma)$

(use $|\mathrm{tr}(AU)| \underset{\substack{\uparrow \\ \text{polar decomposition}}}{=} |\mathrm{tr}(|A|VU)| = |\mathrm{tr}(|A|^{\frac{1}{2}} |A|^{\frac{1}{2}} VU)| \underset{\substack{\uparrow \\ \text{Cauchy-Schwarz inequality}}}{\leq} \mathrm{tr}|A|$)

Cauchy-Schwarz inequality $|\mathrm{tr}(AB)| \leq \sqrt{\mathrm{tr}(A^{+}A)\,\mathrm{tr}(B^{+}B)}$

corollary: $F(\rho,\sigma) = F(\sigma,\rho)$

④ fix $|\psi\rangle$ $F(\rho,\sigma) = \max_{|\varphi\rangle} |\langle\psi|\varphi\rangle|$ fix U_R, U_Q, choose V_R, V_Q s.t. $U = I$

⑤ $F(\rho,\sigma) = \min_{\{E_m\}} F(p_m, q_m)$ POVM $\{E_m\}$ $\sum_m E_m = I$

probabilities $p_m = \mathrm{tr}(\rho E_m)$, $q_m = \mathrm{tr}(\sigma E_m)$

proof: polar decomposition $\sqrt{\rho}\sqrt{\sigma} = \sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\; U$

$$\Rightarrow F(\rho,\sigma) = \mathrm{tr}(\sqrt{\rho}\sqrt{\sigma}\, U^{+})$$

$$= \sum_m \mathrm{tr}(\sqrt{\rho}\sqrt{E_m}\sqrt{E_m}\sqrt{\sigma}\, U^{+}) \quad (\text{use } \sum_m E_m = I)$$

$$\leq \sum_m \sqrt{\mathrm{tr}(\rho E_m)\,\mathrm{tr}(\sigma E_m)} \quad (\text{Cauchy-Schwarz inequality})$$

$$= F(p_m, q_m)$$

for "=" we need $\sqrt{\rho}\sqrt{E_m} = 0$ or $\sqrt{E_m}\sqrt{\sigma}\,U^{+} = 0$ or $\sqrt{E_m}\sqrt{\rho} = \lambda_m \sqrt{E_m}\sqrt{\sigma}\,U^{+}$ for all m

if ρ invertible $\sqrt{\sigma}\,U^{+} = \rho^{-\frac{1}{2}}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}$

$$\Rightarrow \sqrt{E_m} = \lambda_m \sqrt{E_m}\, \underbrace{\rho^{-\frac{1}{2}}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\,\rho^{-\frac{1}{2}}}_{\equiv M \text{ Hermitian}}$$

$$\Rightarrow \sqrt{E_m}(I - \lambda_m M) = 0$$

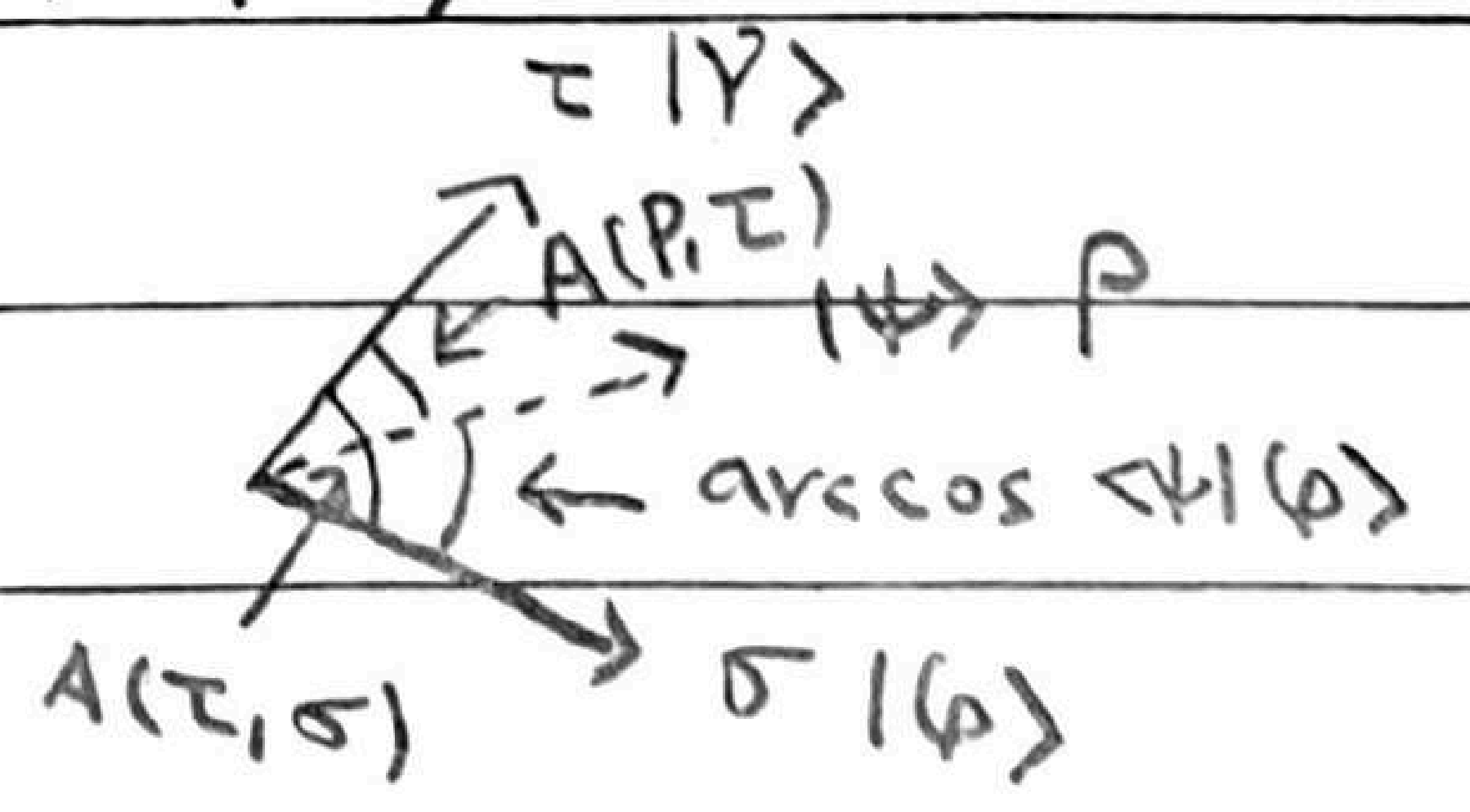
eigenvalue decomposition $M = \sum_m \beta_m |m\rangle\langle m|$

if $\beta_m \neq 0$ for all m choose $E_m = |m\rangle\langle m|$, $\lambda_m = \frac{1}{\beta_m}$

more general cases from limit

⑥ distance $A(\rho,\sigma) \equiv \arccos F(\rho,\sigma)$ (A for angle, $A \in [0,\pi]$)

proof: triangle inequality $A(\rho,\sigma) \leq A(\rho,\tau) + A(\tau,\sigma)$



fix purification of τ, $|\gamma\rangle$

$\exists$ purification of ρ, $|\psi\rangle$

purification of σ, φ

s.t. $F(\rho,\tau) = \langle\psi|\gamma\rangle$, $F(\tau,\sigma) = \langle\gamma|\varphi\rangle$

$$\Rightarrow \arccos\langle\psi|\varphi\rangle \leq A(\rho,\tau) + A(\tau,\sigma)$$

$$F(\rho,\sigma) \geq \langle\psi|\varphi\rangle$$

$$\Rightarrow A(\rho,\sigma) \leq \arccos\langle\psi|\varphi\rangle \leq A(\rho,\tau) + A(\tau,\sigma)$$

⑦ trace-preserving quantum correction increases fidelity

$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma)$

proof: $\exists$ purification $|\psi\rangle, |\varphi\rangle$ s.t. $F(\rho,\sigma) = |\langle\psi|\varphi\rangle|$

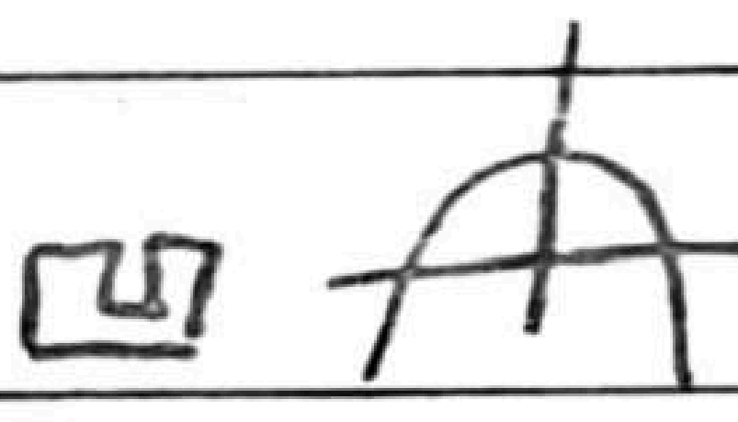
$$\begin{array}{ll} Q & \rho_Q \\ R & \\ E & \\ E' & \end{array} \left.\begin{array}{l} \rho_Q \rangle |\psi_{QR}\rangle \\ |0_E\rangle \end{array}\right\} |\psi_{QR}\rangle|0_E\rangle \xrightarrow{\mathcal{E}} \left.\begin{array}{l} U_{QE}|\psi_{QR}\rangle|0_E\rangle \\ |0_{E'}\rangle \end{array}\right\} U_{QE}|\psi_{QR}\rangle|0_E\rangle|0_{E'}\rangle$$

$\Rightarrow U_{QE}|\psi_{QR}\rangle|0_E\rangle|0_{E'}\rangle$ is a purification of $\mathcal{E}(\rho_Q) \otimes |0_{E'}\rangle\langle 0_{E'}|$

similarly $U_{QE}|\varphi_{QR}\rangle|0_E\rangle|0_{E'}\rangle$ is a purification of $\mathcal{E}(\sigma_Q) \otimes |0_{E'}\rangle\langle 0_{E'}|$

$$\begin{aligned} \Rightarrow F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &= F(\mathcal{E}(\rho_Q) \otimes |0_{E'}\rangle\langle 0_{E'}|, \mathcal{E}(\sigma_Q) \otimes |0_{E'}\rangle\langle 0_{E'}|) \\ &\geq |\langle\psi_{QR}|\langle 0_E|\langle 0_{E'}| U_{QE}^{+} U_{QE}|\varphi_{QR}\rangle|0_E\rangle|0_{E'}\rangle| \\ &= |\langle\psi_{QR}|\varphi_{QR}\rangle| \\ &= |\langle\psi|\varphi\rangle| = F(\rho,\sigma) \end{aligned}$$

corollary: $A(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq A(\rho, \sigma)$

⑧ strong concavity $F(\sum_i p_i \rho_i, \sum_i q_i \sigma_i) \geq \sum_i \sqrt{p_i q_i}\, F(\rho_i, \sigma_i)$ 

proof: $\exists$ purifications $|\psi_i\rangle, |\varphi_i\rangle$ s.t. $F(\rho_i, \sigma_i) = \langle\psi_i|\varphi_i\rangle$

$$\begin{array}{ll} Q & \rho_i^Q \\ R & \end{array} \Big\} |\psi_i^{QR}\rangle \qquad \begin{array}{ll} Q & \rho_Q \\ R & \\ R' & \\ Q' & \end{array} \left.\begin{array}{l} \Big\} |\psi_{QRR'}\rangle \equiv \sum_i \sqrt{p_i}\, |\psi_i^{QR}\rangle |i_{R'}\rangle \\ |0_{Q'}\rangle \end{array}\right\} |\psi_{QRR'}\rangle|0_{Q'}\rangle$$

$\rho = \sum_i p_i \rho_i$ $\qquad |\psi_{QRR'}\rangle|0_{Q'}\rangle$ purifies $\rho_Q \otimes |0_{Q'}\rangle\langle 0_{Q'}|$

similarly $\sigma = \sum_i q_i \sigma_i$, $|\varphi_{QRR'}\rangle \equiv \sum_i \sqrt{q_i}\, |\varphi_i^{QR}\rangle |i_{R'}\rangle$

$|\varphi_{QRR'}\rangle|0_{Q'}\rangle$ purifies $\sigma_Q \otimes |0_{Q'}\rangle\langle 0_{Q'}|$

$$\begin{aligned} F(\rho,\sigma) &= F(\rho_Q \otimes |0_{Q'}\rangle\langle 0_{Q'}|, \sigma_Q \otimes |0_{Q'}\rangle\langle 0_{Q'}|) \\ &\geq |\langle\psi_{QRR'}|\langle 0_{Q'}| \varphi_{QRR'}\rangle|0_{Q'}\rangle| \\ &= \sum_i \sqrt{p_i q_i}\, \langle\psi_i|\varphi_i\rangle \\ &= \sum_i \sqrt{p_i q_i}\, F(\rho_i, \sigma_i) \end{aligned}$$

⑨ joint concavity $F(\sum_i p_i \rho_i, \sum_i p_i \sigma_i) \geq \sum_i p_i F(\rho_i, \sigma_i)$

⑩ concavity $F(\sum_i p_i \rho_i, \sigma) \geq \sum_i p_i F(\rho_i, \sigma)$

(7) relation pure states $D(|\psi\rangle, |\varphi\rangle) = \sqrt{1 - |\langle\psi|\varphi\rangle|^2}$, $F(|\psi\rangle, |\varphi\rangle) = |\langle\psi|\varphi\rangle|$, $D = \sqrt{1 - F^2}$

general states $1-F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1-F(\rho,\sigma)^2}$

proof: ① $\exists$ purifications $|\psi\rangle, |\varphi\rangle$ s.t. $F(\rho,\sigma) = |\langle\psi|\varphi\rangle|$

$$D(\rho,\sigma) \leq D(|\psi\rangle, |\varphi\rangle) = \sqrt{1-|\langle\psi|\varphi\rangle|^2} = \sqrt{1-F(\rho,\sigma)^2}$$

② $\exists$ POVM $\{E_m\}$ s.t. $F(\rho,\sigma) = \sum_m \sqrt{p_m q_m}$ w/ $p_m = tr(\rho E_m)$, $q_m = tr(\sigma E_m)$

$$\sum_m |\sqrt{p_m} - \sqrt{q_m}|^2 = 2(1-F(\rho,\sigma))$$
$$\leq \sum_m |\sqrt{p_m} - \sqrt{q_m}| \cdot |\sqrt{p_m} + \sqrt{q_m}|$$
$$= \sum_m |p_m - q_m|$$
$$= 2D(p_m, q_m)$$
$$\leq 2D(\rho,\sigma)$$

(8) dynamic measure $F(\rho, \mathcal{E}(\rho))$

eg depolarizing channel $\mathcal{E}(\rho) = p\rho + (1-p)\frac{I}{2} \Rightarrow F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\frac{1+p}{2}}$

phase damping channel $\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z \Rightarrow F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{p + (1-p)\langle\psi|Z|\psi\rangle^2}$

↑ state-dependent

(9) minimal fidelity (the worst case)

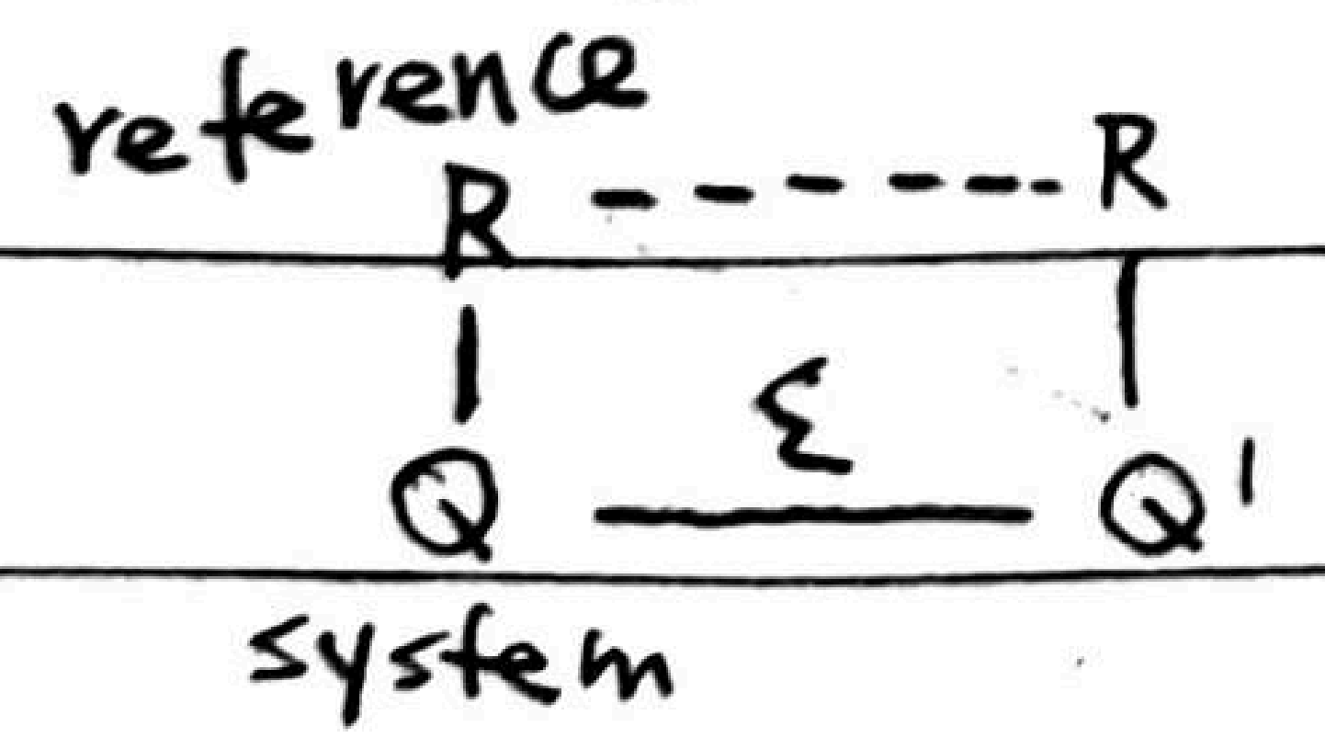
$$F_{min}(\mathcal{E}) \equiv \min_{|\psi\rangle} F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \min_{\rho} F(\rho, \mathcal{E}(\rho))$$

proof: any $\rho = \sum_i \lambda_i |i\rangle\langle i|$

$$F(\rho, \mathcal{E}(\rho)) = F(\sum_i \lambda_i |i\rangle\langle i|, \sum_i \lambda_i \mathcal{E}(|i\rangle\langle i|))$$
$$\geq \sum_i \lambda_i F(|i\rangle\langle i|, \mathcal{E}(|i\rangle\langle i|))$$
$$\geq F_{min}(\mathcal{E})$$

(10) ensemble average fidelity $\{p_j, \rho_j\}$ $\bar{F}(\mathcal{E}) = \sum_j p_j F(\rho_j, \mathcal{E}(\rho_j))^2$

(11) entanglement fidelity: quantifies how entanglement is preserved



Q in state ρ, RQ in state $|\psi\rangle = |RQ\rangle$

$$F(\rho, \mathcal{E}) \equiv F(RQ, RQ')^2$$
$$= \langle RQ|(I_R \otimes \mathcal{E})(|RQ\rangle\langle RQ|)|RQ\rangle$$
$$= \langle RQ| \sum_i (E_i |RQ\rangle\langle RQ| E_i^\dagger) |RQ\rangle$$
$$= \sum_i |\langle RQ|E_i|RQ\rangle|^2$$
$$= \sum_i |tr(\rho E_i)|^2 \quad (E_i \text{ act only on } Q)$$

independent of explicit purification

convexity: $F(\rho, \mathcal{E})$ is a conver function of ρ 凸 

$$F(\sum_j p_j \rho_j, \mathcal{E}) \leq \sum_j p_j F(\rho_j, \mathcal{E})$$

proof: define $f(x) = F(x\rho_1 + (1-x)\rho_2, \mathcal{E})$

$$= \sum_i \left| tr\left([x\rho_1 + (1-x)\rho_2] E_i\right)\right|^2$$

$$f''(x) = 2\sum_i \left|tr[(\rho_1-\rho_2)E_i]\right|^2 \geq 0$$

up bound: $F(\sum_j p_j\rho_j, \mathcal{E}) \leq \sum_j p_j F(\rho_j, \mathcal{E})$ (convexity)

$$= \sum_j p_j F(|\psi_j\rangle, (I_R \otimes \mathcal{E})(|\psi_j\rangle\langle\psi_j|))^2$$

$$\leq \sum_j p_j F(\rho_j, \mathcal{E}(\rho_j))^2$$ (partical trace increases fidelity)

$= \bar{F}(\mathcal{E})$ ensemble average fidelity

5. quantum error correction

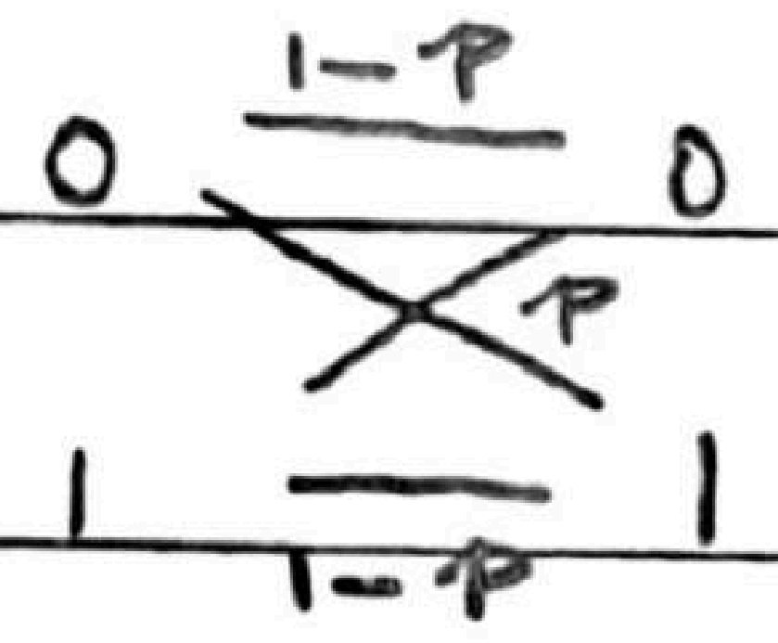
(1) classical error-corretion

key: redundant information

repetition code $0 \rightarrow 0_L = 000$ L for logical

$1 \rightarrow 1_L = 111$ 1 logical bit, 3 physical bits

error probability p



correct single-bit errors by majority voting 100, 010, 001 → 000

011, 101, 110 → 111

new error probability $\underset{\substack{\uparrow \\ 2 \text{ errors}}}{3p^2(1-p)} + \underset{\substack{\uparrow \\ 3 \text{ errors}}}{p^3} = 3p^2 - 2p^3 < p$ if $p < \frac{1}{2}$

(2) bit flip code

error $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$

$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle$

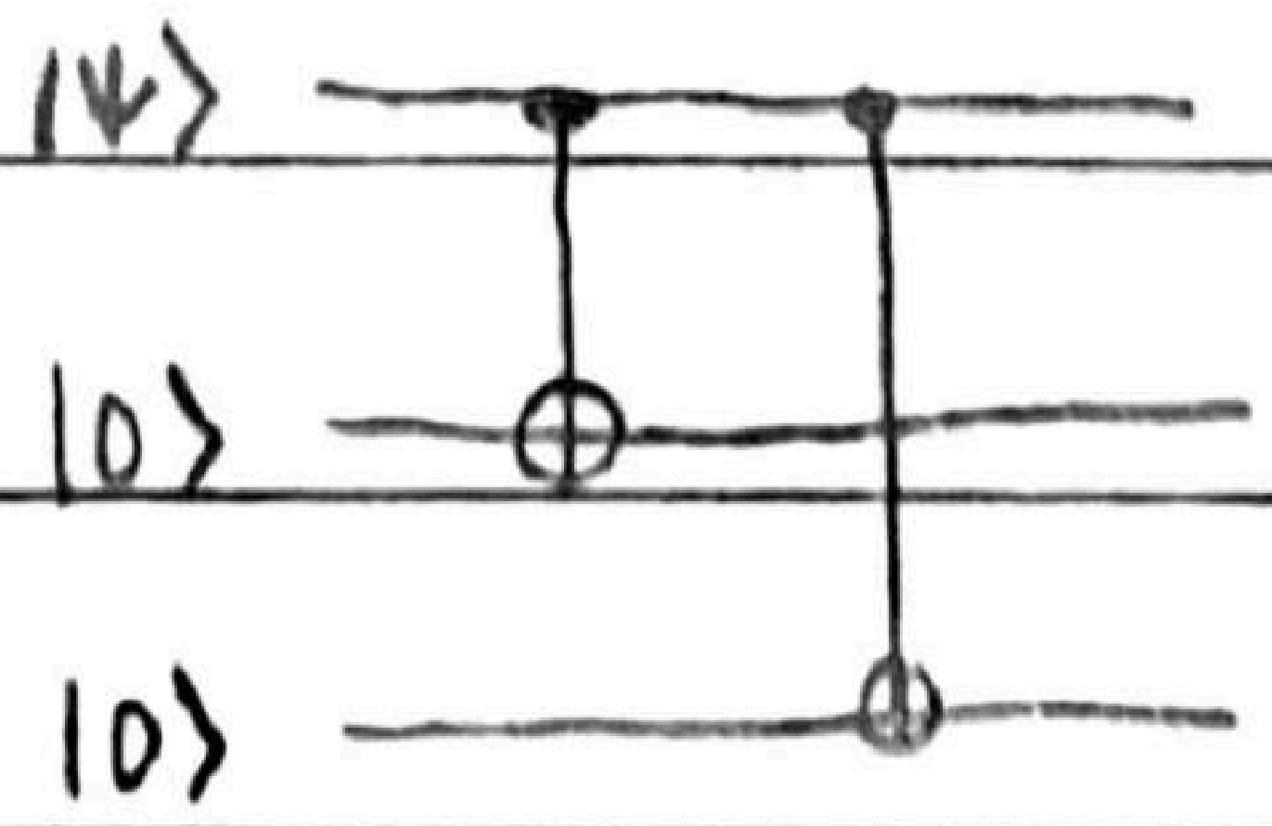
$|1\rangle \rightarrow \underset{\uparrow}{|1_L\rangle} \equiv |111\rangle$

1 logical qubit, 3 physical qubits } [3,1] code

$\underset{\substack{\uparrow \\ \text{physical}}}{[n,}\underset{\substack{\nwarrow \\ \text{logical}}}{k]}$ code

encoding circuit

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



$a|000\rangle + b|111\rangle$

correct single-qubit errors: ① syndrome diagnosis (error detection) ② recovery

state	error position	measure Z_1Z_2	Z_2Z_3	act
$a\|000\rangle + b\|111\rangle$	no error	1	1	I
$a\|100\rangle + b\|011\rangle$	1	-1	1	X_1
$a\|010\rangle + b\|101\rangle$	2	-1	-1	X_2
$a\|001\rangle + b\|110\rangle$	3	1	-1	X_3

(3) phase-flip code [3, 1] code

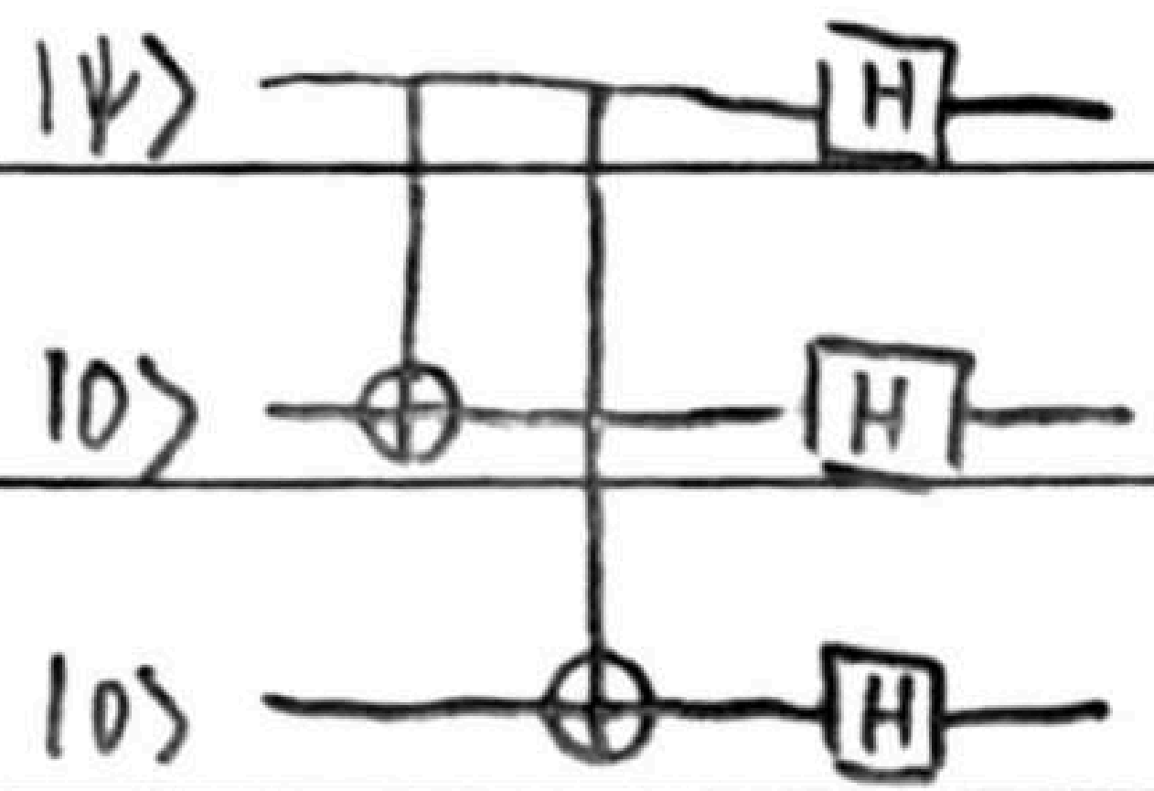
error $\mathcal{E}(\rho) = (1-p)\rho + p Z\rho Z$

$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ $X|\pm\rangle = \pm|\pm\rangle$ $|+\rangle \overset{Z}{\longleftrightarrow} |-\rangle$

Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $|+\rangle \overset{H}{\longleftrightarrow} |0\rangle$ $|-\rangle \overset{H}{\longleftrightarrow} |1\rangle$

$|0_L\rangle = |+++\rangle$ ecoding circuit

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



$a|+++\rangle + b|---\rangle$

state	error position	measure X_1X_2	X_2X_3	act
$a\|+++\rangle + b\|---\rangle$	no error	1	1	I
$a\|-++\rangle + b\|+--\rangle$	1	-1	1	Z_1
$a\|+-+\rangle + b\|-+-\rangle$	2	-1	-1	Z_2
$a\|++-\rangle + b\|--+\rangle$	3	1	-1	Z_3

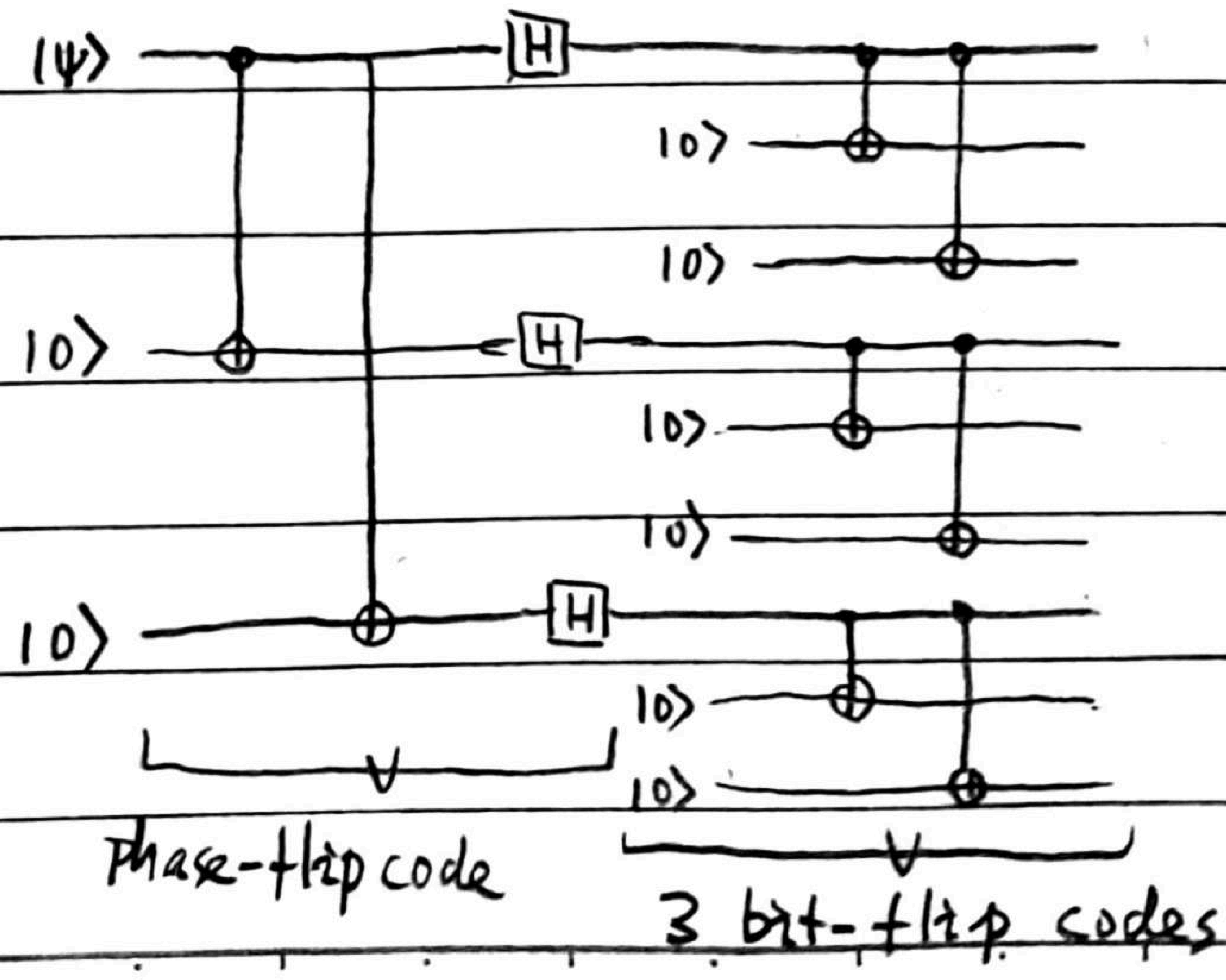
(4) Shor code [9, 1] code   it corrects any single-qubit error

logical qubit $|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) = |PPP\rangle$ $P \equiv \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

$|1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) = |MMM\rangle$ $M \equiv \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$

encoding circuit

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



$a|0_L\rangle + b|1_L\rangle$

① bit-flip error

state	error position	Z_1Z_2	Z_2Z_3	Z_4Z_5	Z_5Z_6	Z_7Z_8	Z_8Z_9	act
$a\|0_L\rangle+b\|1_L\rangle$ ···	no error	1	1	1	1	1	1	I
$a(\|100\rangle+\|011\rangle)\cdots+b(\|100\rangle-\|011\rangle)\cdots$	1	-1	1	1	1	1	1	X_1
$a(\|010\rangle+\|101\rangle)\cdots+b(\|010\rangle-\|101\rangle)\cdots$	2	-1	-1	1	1	1	1	X_2
$a(\|001\rangle+\|110\rangle)\cdots+b(\|001\rangle-\|110\rangle)\cdots$	3	1	-1	1	1	1	1	X_3
$a\cdots(\|100\rangle+\|011\rangle)\cdots+b\cdots(\|100\rangle-\|011\rangle)\cdots$	4	1	1	-1	1	1	1	X_4
$a\cdots(\|010\rangle+\|101\rangle)\cdots+b\cdots(\|010\rangle-\|101\rangle)\cdots$	5	1	1	-1	-1	1	1	X_5
$a\cdots(\|001\rangle+\|110\rangle)\cdots+b\cdots(\|001\rangle-\|110\rangle)\cdots$	6	1	1	1	-1	1	1	X_6
$a\cdots(\|100\rangle+\|011\rangle)+b\cdots(\|100\rangle-\|011\rangle)$	7	1	1	1	1	-1	1	X_7
$a\cdots(\|010\rangle+\|101\rangle)+b\cdots(\|010\rangle-\|101\rangle)$	8	1	1	1	1	-1	-1	X_8
$a\cdots(\|001\rangle+\|110\rangle)+b\cdots(\|001\rangle-\|110\rangle)$	9	1	1	1	1	1	-1	X_9

② phase-flip error

$|P\rangle\equiv\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$ $|M\rangle=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)$

state	error position	$X_1X_2X_3X_4X_5X_6$	$X_4X_5X_6X_7X_8X_9$	act
$a\|PPP\rangle+b\|MMM\rangle$	no error	1	1	I
$a\|MPP\rangle+b\|PMM\rangle$	1 or 2 or 3	-1	1	$Z_1Z_2Z_3$
$a\|PMP\rangle+b\|MPM\rangle$	4 or 5 or 6	-1	-1	$Z_4Z_5Z_6$
$a\|PPM\rangle+b\|MMP\rangle$	7 or 8 or 9	1	-1	$Z_7Z_8Z_9$

③ bit-phase flip at the 1st qubit

$$a(|000\rangle+|111\rangle)\cdots+b(|000\rangle-|111\rangle)\cdots\xrightarrow{Z_1X_1}a(-|100\rangle+|011\rangle)\cdots+b(-|100\rangle-|011\rangle)\cdots$$

$$\xrightarrow{\text{bit-flip correction}}a(-|000\rangle+|111\rangle)\cdots+b(-|000\rangle-|111\rangle)\cdots$$

$$\xrightarrow{\text{phase-flip correction}}a(-|000\rangle-|111\rangle)\cdots+b(-|000\rangle+|111\rangle)\cdots$$

④ any error at the 1st qubit

quantum errors $\mathcal{E}(|\psi\rangle\langle\psi|)=\sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger=\sum_{i,j=1,2,3,4}P_{ij}|\psi_i\rangle\langle\psi_j|$

$$E_i=e_{i0}I+e_{i1}X_1+e_{i2}Z_1+e_{i3}X_1Z_1$$

define states $|\psi_1\rangle\equiv|\psi\rangle=a(|000\rangle+|111\rangle)\cdots+b(|000\rangle-|111\rangle)\cdots$

$|\psi_2\rangle\equiv X_1|\psi\rangle=a(|100\rangle+|011\rangle)\cdots+b(|100\rangle-|011\rangle)\cdots$

$$|\psi_3\rangle \equiv Z_1|\psi\rangle = a\left(|000\rangle - |111\rangle\right)\cdots + b\left(|000\rangle + |111\rangle\right)\cdots$$

$$|\psi_4\rangle \equiv Z_1X_1|\psi\rangle = a\left(|100\rangle - |011\rangle\right)\cdots + b\left(|100\rangle + |011\rangle\right)\cdots$$

key: measurement collapses quantum states

$$\begin{tikzcd}
\rho = \sum_{i,j=1,2,3,4} p_{ij}|\psi_i\rangle\langle\psi_j| \arrow[r, "Z_1Z_2"] \arrow[dr] & -1 \quad \rho \propto \sum_{i,j=2,4} p_{ij}|\psi_i\rangle\langle\psi_j| \arrow[d, bend left, "\text{bit-flip correction act } X_1"] & \\
& 1 \quad \rho \propto \sum_{i,j=1,3} p_{ij}|\psi_i\rangle\langle\psi_j| \arrow[dl] \arrow[dr, "X_1X_2X_3X_4X_5X_6"] & \\
-1 \quad \rho \propto |\psi_3\rangle\langle\psi_3| \arrow[rr, bend right, "\text{phase flip correction act } Z_1Z_2Z_3"'] & & 1 \quad \rho \propto |\psi_1\rangle\langle\psi_1|
\end{tikzcd}$$

(5) quantum error-correction conditions

code space C, projector P onto C, error $\mathcal{E}$ w/ operation elements $\{E_i\}$

$$\exists\, \mathcal{R} \text{ s.t. } \underset{\substack{\uparrow \\ \text{detection+recovery, trace-preserving}}}{(\mathcal{R}\circ\mathcal{E})}(\rho) \propto \rho \iff PE_i^\dagger E_j P = \underset{\substack{\uparrow \\ \text{Hermitian matrix}}}{\alpha_{ij}} P$$

proof: "$\Rightarrow$" $\forall \rho$, not necessarily $\in C$, $P\rho P \in C$

$$(\mathcal{R}\circ\mathcal{E})(P\rho P) = cP\rho P \iff \sum_{ij} R_j E_i P\rho P E_i^\dagger R_j^\dagger = cP\rho P$$

$$\Rightarrow \{R_j E_i P\} \Leftrightarrow \{\sqrt{c}P\} \Rightarrow R_j E_i P = c_{ji} P$$

$$\Rightarrow PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$$

use $\sum_k R_k^\dagger R_k = I \Rightarrow PE_i^\dagger E_j P = \alpha_{ij} P$ w/ $\alpha_{ij} \equiv \sum_k c_{ki}^* c_{kj}$

"$\Leftarrow$" eigenvalue decomposition $\alpha = u d u^\dagger$

define $F_k \equiv \sum_i u_{ik} E_i$, $\{E_i\} \Leftrightarrow \{F_i\}$

$\Rightarrow PF_k^\dagger F_L P = \delta_{kL} d_{kk} P$ w/ $d_{kk} \neq 0$ (as $d_{kk} = 0$ annihilates a code)

polar decomposition $F_k P = U_k\sqrt{PF_k^\dagger F_k P} = \sqrt{d_{kk}}\, U_k P$

$$\text{define } \underset{\substack{\uparrow \\ \text{projector, check } P_kP_L = \frac{1}{\sqrt{d_{kk}d_{LL}}} U_k P F_k^\dagger F_L P U_L^\dagger = \delta_{kL} P_k \\ \uparrow \\ \text{error detection measurement}}}{P_k} \equiv U_k P U_k^\dagger = \frac{1}{\sqrt{d_{kk}}} F_k P U_k^\dagger = \frac{1}{\sqrt{d_{kk}}} U_k P F_k^\dagger$$

$$\mathcal{R}: \{U_k^\dagger P_k\} \quad \text{for } \rho \in C \quad (\mathcal{R}\circ\mathcal{E})(\rho) = \sum_{kL} \overset{\substack{\text{recovery} \\ \nwarrow}}{U_k^\dagger} \overset{\substack{\text{detection} \\ \uparrow}}{P_k} \overset{\substack{\text{error} \\ \uparrow}}{F_L} \overset{\substack{\text{code} \\ \uparrow}}{\rho} F_L^\dagger P_k U_k$$

$$\left(\begin{aligned} U_k^\dagger P_k F_L\sqrt{\rho} &= U_k^\dagger \frac{1}{\sqrt{d_{kk}}} U_k \underset{\sim}{PF_k^\dagger F_L P}\sqrt{\rho} \\ &= \delta_{kL}\sqrt{d_{kk}}\sqrt{\rho} \end{aligned}\right) \overset{\curvearrowright}{=} \sum_{kL} \delta_{kL}\, d_{kk}\, \rho \propto \rho$$

(6) discretization of errors

if $\mathcal{R}$ could correct error $\mathcal{E}$ w/ $\{E_i\}$, then it also corrects $\mathcal{F}$ w/ $\{F_j = \sum_i m_{ji} E_i\}$

proof: $P E_i^\dagger E_j P = \alpha_{ij} P \Rightarrow P F_k^\dagger F_l P = \beta_{kl} P$ w/ $\beta_{kl} \equiv \sum_{ij} m_{ki}^* m_{lj} \alpha_{ij}$

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \Rightarrow U_k^\dagger P_k F_j \sqrt{\rho} = m_{ji} \sqrt{d_{kk}} \sqrt{\rho}$$

$$\Rightarrow \mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k$$

$$= \sum_{kj} |m_{jk}|^2 d_{kk} \rho$$

$$\propto \rho$$

(7) quantum error correction improves fidelity

	single qubit	(n,1) code
probabily of no error	$1-p$	$(1-p)^n + np(1-p)^{n-1} \approx 1 - \frac{n(n-1)}{2}p^2 + O(p^3)$
errors	p	$\frac{n(n-1)}{2}p^2 + O(p^3)$

(8) degenerate code: different errors may have the same syndrome eg Shor code

non-degenerate code: different errors have different syndromes

(9) quantum Hamming bound for non-degenerate code

[n, k] code: n physical qubits encoding k logical qubits

corrects any errors of t or fewer qubits

$$\underset{\substack{\uparrow \\ \text{code spae dimension}}}{2^k} \underset{\substack{\uparrow \\ \text{\# of correctable errors for each code}}}{\sum_{j=0}^{t} C_n^j 3^j} \leq \underset{\substack{\uparrow \\ \text{tocal dimention}}}{2^n}$$

eg $k=1$, $t=1$, $n \geq 5$

(10) classical linear codes

use n bits to encode k bits [n, k] code

① $n \times k$ generator matrix G maps a message (M) to its code (C)

$G = (y_1, y_2, \cdots, y_k)$ $\quad x = (x_1, x_2, \cdots, x_k) \in M$ $\quad G(x) = x_1 y_1 + x_2 y_2 + \cdots + x_k y_k \in C$

y_i w/ $i = 1, 2, \cdots, k$, linealy independent vectors of dimension n, s.t. different meassages are mapped to different codes

y_i are k of the codes

eg [3,1] code $G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $\quad G(0) = 000$ $\quad G(1) = 111$

[6,2] code $G=\begin{bmatrix}1&0\\1&0\\1&0\\0&1\\0&1\\0&1\end{bmatrix}$ $G(00)=000000$ $G(01)=000111$

$G(10)=111000$ $G(11)=111111$

② equivalent way to define the code : $Y \in C$

$(n-k)\times n$ parity check matrix $H=\begin{pmatrix}\check{y}_1^T\\ \check{y}_2^T\\ \vdots\\ \check{y}_{n-k}\end{pmatrix}$ $HY=\begin{pmatrix}\check{y}_1\cdot Y\\ \check{y}_2\cdot Y\\ \vdots\\ \check{y}_{n-k}\cdot Y\end{pmatrix}=0$

$\check{y}_j$ w/ $j=1,2,\cdots,n-k$ linearly independent vectors of dimension n, s.t.

there are 2^k code words

$\Rightarrow \check{y}_j\cdot Y_i = 0$ for all $i=1,2,\cdots,k$, $j=1,2,\cdots,n-k$ $\Leftrightarrow \overset{(n-k)\times n}{H}\overset{n\times k}{G}=0$

parity check matrix generator matrix

eg [3,1] code $G=\begin{pmatrix}1\\1\\1\end{pmatrix}$ $H=\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix}$

[6,2] code $G=\begin{bmatrix}1&0\\1&0\\1&0\\0&1\\0&1\\0&1\end{bmatrix}$. $H=\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix}$

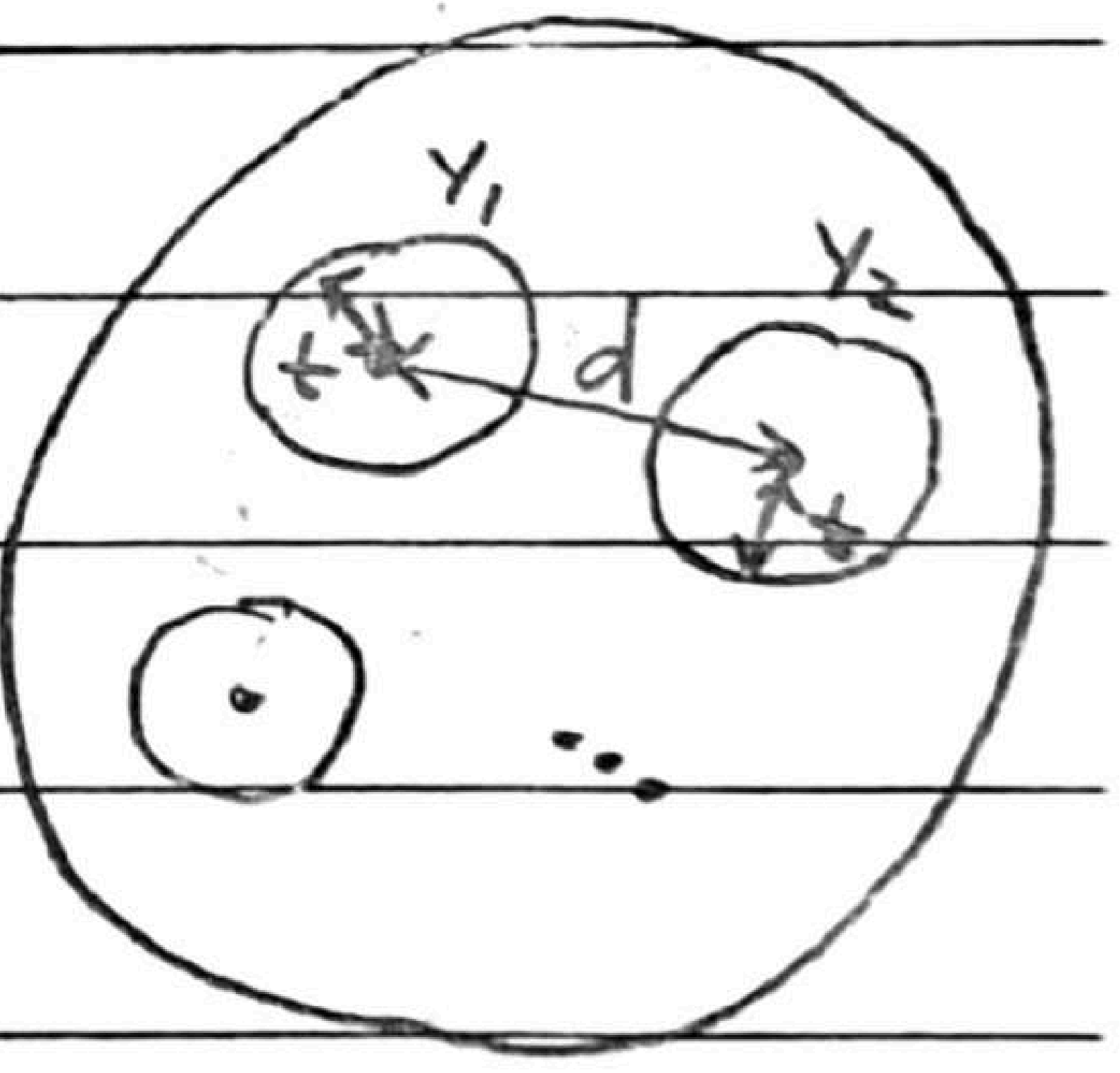
③ code $Y\in C \rightarrow Y'=Y+\overset{\text{error}}{e}$, as $HY=0 \Rightarrow HY'=He$ error syndrome

if $HY'\neq 0$, change Y' to Y that minimizes the Hamming distane $d(Y,Y')$

Hamming distance $d(Y,Y')=$ (# of different letters for the words Y,Y')

weight $w(Y)=d(Y,0)$

distance of a code $d(C)=\min_{Y_1,Y_2\in C,\,Y_1\neq Y_2} d(Y_1,Y_2)=\min_{Y\in C} w(Y)$



[n,k,d] code

the code can correct t and less errors $\Rightarrow d\geq 2t+1$

Singleton bound $k\leq n-d+1$ (remover d-1 letters, it still works)

④ dual construction

code $C=[n,k]$ $HG=0$ $\Rightarrow$ $G^T H^T=0$

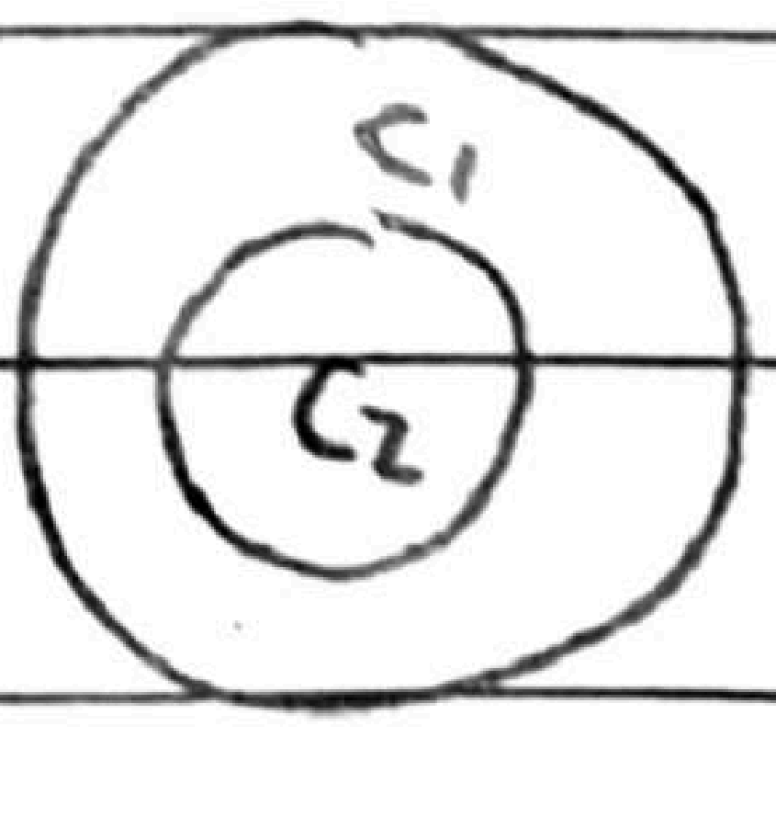
$\Rightarrow$ dual code $C^\perp=[n,k]^\perp=[n,n-k]$ $G^\perp=H^T$, $H^\perp=G^T$

(11) CSS codes (Calderbank-Shor-Stean codes)

two classical linear codes $C_1=[n,k_1]$, $C_2=[n,k_2]$

$C_2\subset C_1$ $(k_2<k_1)$

both C_1 and $C_2^\perp$ can correct t errors.



$CSS(C_1, C_2)$ CSS code of C_1 over C_2

code space $x \in C_1$ $\quad |x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$

equivalent class, # of code's $\frac{|C_1|}{|C_2|} = 2^{k_1 - k_2} \Rightarrow [n, k_1 - k_2]$ quantum code

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle \xrightarrow{\text{error}} \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} \underset{\text{phase flip error}}{(-)^{(x+y)\cdot e_2}} \underset{\nwarrow \text{bit flip error in } C_1}{|x+y+e_1\rangle}$$

note $x \in C_1, y \in C_2 \subset C_1$
$x + y \in C_1$

$\downarrow$ add ancilla

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-)^{(x+y)\cdot e_2} |x+y+e_1\rangle |x+y+e_1\rangle$$

$\downarrow$ impose H_1 on ancilla, $H_1(x+y+e_1) = H_1 e_1$, error syndrome

$$\left[\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-)^{(x+y)\cdot e_2} |x+y+e_1\rangle\right] |H_1 e_1\rangle$$

$\downarrow$ correct e_1 using C_1 and discard ancilla

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-)^{(x+y)\cdot e_2} |x+y\rangle$$

$*\downarrow$ apply Hadamard gates $H^{\otimes n}$ $\quad \left(\begin{array}{l} \text{note } H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ H|x\rangle = \frac{1}{\sqrt{2}} \sum_z (-)^{x\cdot z} |z\rangle \end{array} \right)$

$$\frac{1}{\sqrt{|C_2| 2^n}} \sum_z \sum_{y \in C_2} (-)^{(x+y)\cdot(e_2 + z)} |z\rangle$$

$\downarrow$ $z \equiv z' + e_2$

$$\frac{1}{\sqrt{|C_2| 2^n}} \sum_{z'} \sum_{y \in C_2} (-)^{(x+y)\cdot z'} |z' + e_2\rangle$$

$\downarrow$ if $z' \in C_2^\perp$ $\quad \sum_{y \in C_2} (-)^{y \cdot z'} \overset{\swarrow y\cdot z' = 0}{=} |C_2|$

if $z' \notin C_2^\perp$ $\quad \sum_{y \in C_2} (-)^{y\cdot z'} = \sum_x (-)^{z' \cdot G_2 \cdot x} \overset{\swarrow G_2^T \cdot z' = H_2^\perp \cdot z' \neq 0}{=} 0$

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-)^{x\cdot z'} \underset{\nwarrow \text{bit flip error in } C_2^\perp}{|z' + e_2\rangle}$$

$\downarrow$ correct e_2 using $C_2^\perp$

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-)^{x\cdot z'} |z'\rangle$$

$*^{-1}\downarrow$ impose $H^{\otimes n}$

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$$

eg: Steane code $\quad$ classical linear code $[7,4,3]$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \qquad H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$C_1 = C = [7,4,3]$ $\quad t = 1$ $\quad \Rightarrow$ $CSS[C_1, C_2] = [7,1]$ quantum code $t = 1$

$C_2 = C^\perp = [7,4,4]$ $\quad t = 1$

code $|0_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + \cdots)$, $\quad |1_L\rangle = \frac{1}{\sqrt{8}}(|1111111\rangle + \cdots)$

(12) stabilizer codes

① stabilizer formulism (+ is understood as $\oplus$).

(a) state $|\psi\rangle$ is stabilized by operators $O_1, O_2, \cdots \Leftrightarrow |\psi\rangle = O_1|\psi\rangle = O_2|\psi\rangle = \cdots$

each operator is a stabilizer of the state

eg: EPR state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is stabilized by X_1X_2 and Z_1Z_2.

(b) Pauli group G_n on n qubits: {direct product of Pauli matrices with multiplicative factors $\pm 1, \pm i$}

\# of elements $4 \times 4^n = 4^{n+1}$

(c) for a subgroup $S \subseteq G_n$, V_S is the vector space stabilized by S

$\Leftrightarrow$ group S is the stabilizer of V_S

$S = \langle g_1, g_2, \cdots, g_l \rangle$ generators of S g_j w/ $j = 1, 2, \cdots, l$

independent, the number l cannot be smaller

a state is stabilized by $S \Leftrightarrow$ it is stablized by all generators of S

eg: $n=2$ $S = \{I, Z_1\} = \langle Z_1 \rangle \Leftrightarrow V_S$ is spanned by $\{|00\rangle, |01\rangle\}$

$S = \{I, Z_1, Z_2, Z_1Z_2\} = \langle Z_1, Z_2 \rangle \Leftrightarrow V_S$ is spanned by $\{|00\rangle\}$

$n=3$ $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\} \Leftrightarrow V_S$ is spanned by $\{|000\rangle, |111\rangle\}$

$\Leftrightarrow \langle Z_1Z_2, Z_2Z_3 \rangle$

(d) $V_S \neq \phi \Rightarrow$

- $-I \notin S$ (if $-I \in S \Rightarrow |\psi\rangle = -I|\psi\rangle = -|\psi\rangle \Rightarrow |\psi\rangle = 0$)
- $\pm i$(Pauli) $\notin S$ ($[\pm i(\text{Pauli})]^2 = -I$)
- if $g \in S$, $-g \notin S$ (if $g, -g \in S$, $|\psi\rangle = -g|\psi\rangle = -|\psi\rangle \Rightarrow |\psi\rangle = 0$)
- elements of S commute (if $M, N \in S$ and anticommute $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle \Rightarrow |\psi\rangle = 0$)

(e) $l \times 2n$ check matrix H: l rows, each row for a generator

(2n)- vector

rule $g \to r(g)$

00	10	01	11
I	X	Z	Y

note: H has no information about the multiplative factors

eg $n=3$ $S = \langle Z_1Z_2, Z_2Z_3 \rangle$

$= \langle Z_1Z_2I_3, I_1Z_2Z_3 \rangle$

$$H = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

(f) g and g' commute ⟺ $\underset{\substack{\uparrow \\ \text{row-vector}}}{r(g)} \Lambda \underset{\substack{\uparrow \\ \text{column-vector}}}{r(g')^T} = 0$ $\Lambda_{2n\times 2n} = \begin{pmatrix} 0 & I_{n\times n} \\ I_{n\times n} & 0 \end{pmatrix}$

proof: from 1 qubit to n-qubit

(g) $g_1, \cdots, g_l$ independent ⟺ rows of the check matrix are linearly independent

proof: note $r(g) + r(g') = r(gg')$

$$\sum_{i=1}^{l} a_i r(g_i) = 0 \text{ with } a_j \neq 0 \text{ for some } j$$

$$\Leftrightarrow \prod_{i=1}^{l} g_i^{a_i} = I \quad (\text{note } -I \notin S,\ \pm i(\text{Pauli}) \notin S)$$

$$\Leftrightarrow g_j = g_j^{-1} = \prod_{i\neq j} g_i^{a_i}$$

(h) fix $j \in [1, l]$, $\exists h_j \in G_n$ s.t. $h_j g_j h_j^\dagger = -g_j$, $h_j g_i h_j^\dagger = g_i$, $i \neq j$

proof: we want a column vector a_j with $2n$ components

$$\text{s.t. } \begin{cases} r(g_j)\cdot a_j = 1 \\ r(g_i)\cdot a_j = 0 & i\neq j \end{cases}$$

$r(g_i)$ $i = 1, 2, \cdots, l$ are linearly independent
(# of equations) = l
(# of unknown parameters) = $2n$
⇒ solution exists

choose h_j s.t. $r(h_j) = (\Lambda a_j)^T$

$$\Rightarrow \begin{cases} r(g_j) \Lambda r(h_j)^T = 1 \\ r(g_i) \Lambda r(h_j)^T = 0 & i\neq j \end{cases} \Leftrightarrow \begin{cases} h_j g_j h_j^\dagger = -g_j \\ h_j g_i h_j^\dagger = g_i & i \neq j \end{cases}$$

(i) for $S = \langle g_1, \cdots, g_{n-k} \rangle$ $(l = n-k)$, V_S is a 2^k-dimensional vector space

note: each generator halves the dimension $\frac{2^n}{2^{n-k}} = 2^k$

proof: define $x \equiv (x_1, \cdots, x_{n-k}) \in \mathbb{Z}_2^{n-k}$

$$P_S^x = \frac{1}{2^{n-k}} \prod_{j=1}^{n-k} \left[I + (-1)^{x_j} g_j \right]$$

orthogonal projectors, # = 2^{n-k}

define $h_x \equiv \prod_{j=1}^{n-k} h_j^{x_j}$ ⇒ $h_x P_S^{(0,\cdots,0)} h_x^\dagger = P_S^x$

⇒ ($P_S^{(0,\cdots,0)}$ space) and (P_S^x space) have the same dimension

note $I = \sum_x P_S^x$

$$\Rightarrow \text{dimension of } V_S = \frac{\overset{\text{total dimension}}{2^n}}{\underbrace{2^{n-k}}_{\# \text{ of } P_S^x}} = 2^k$$

(i) cenralizer of S in G_n: $Z(S) = \{E \in G_n \mid Eg = gE \text{ for all } g \in S\}$,

normalizer of S in G_n: $N(S) = \{E \in G_n \mid EgE^\dagger \in S \text{ for all } g \in S\}$

$Z(S) = N(S)$

proof: if $E \in Z(S)$, $Eg = gE \Rightarrow EgE^\dagger = g \in S \Rightarrow E \in N(S)$

if $E \in N(S)$, $EgE^\dagger \in S$, as $EgE^\dagger = g$ or $-g$ and $-g \notin S$

$\Rightarrow EgE^\dagger = g \Rightarrow Eg = gE \Rightarrow Z(S)$

② $[n, k]$ stabilizer code

(a) subgroup $S \subset$ Pauli group G_n, $-I \notin S$,

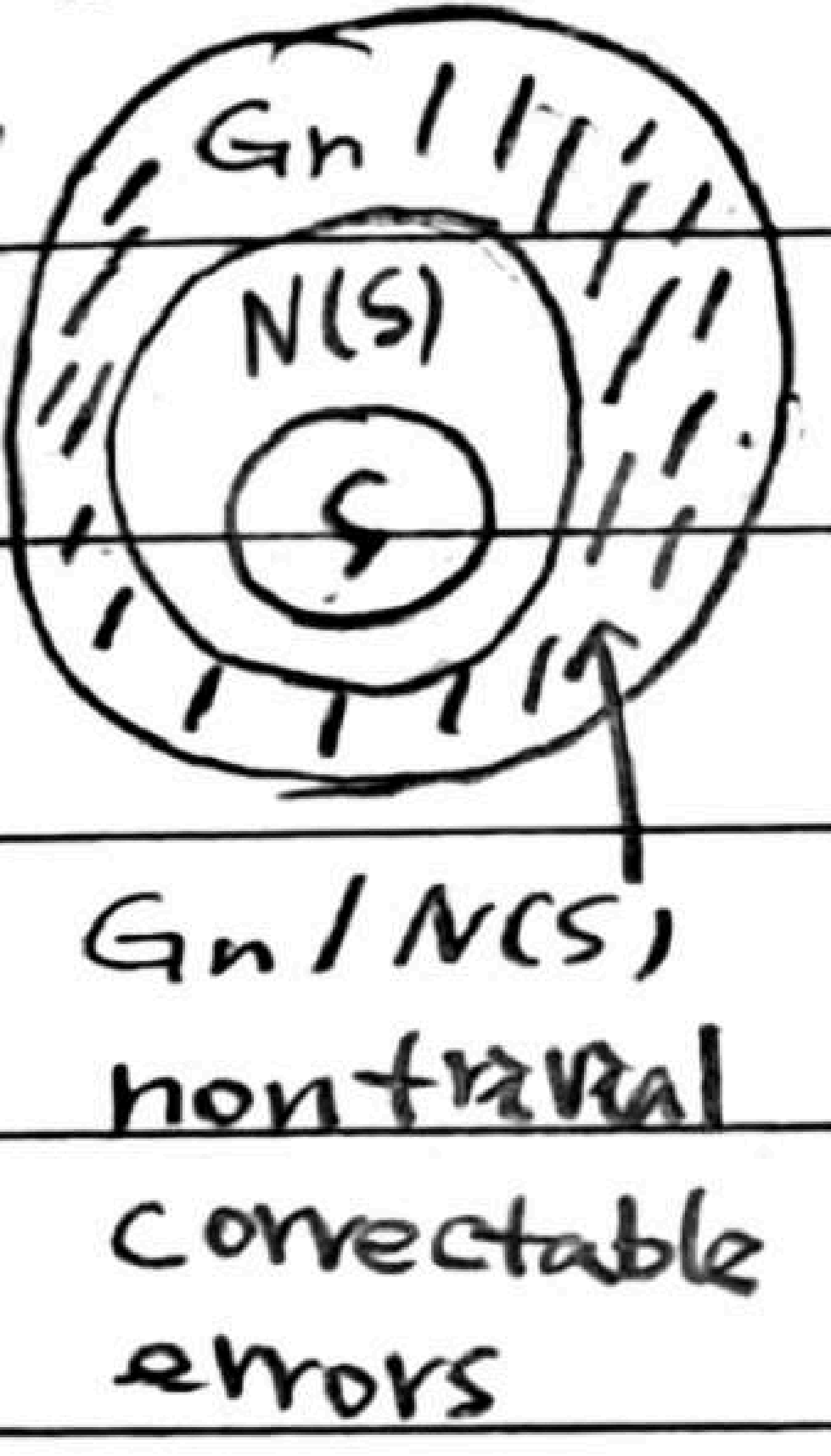
$S = \langle g_1, \cdots, g_{n-k} \rangle$ $n-k$ independent and commuting generators

code space $C(S) = V_S$

$\exists$ n independent and commuting generators $g_1, \cdots, g_{n-k}, \overbrace{\bar{Z}_1, \cdots, \bar{Z}_k}^{\text{logical } Z\text{s}}$

logical state $|x_1 \cdots x_k\rangle_L =$ (the state stablized by $g_1, \cdots, g_{n-k}, (-)^{x_1}\bar{Z}_1, \cdots, (-)^{x_k}\bar{Z}_k$)

(b)



for code $|\psi\rangle$ and error E

if $E \in S$, $E|\psi\rangle = |\psi\rangle$, no need to correct, trivial

if $E \in G_n \backslash N(S)$ $\langle\psi|E|\psi\rangle = \langle\psi|Eg|\psi\rangle$ $(\forall g \in S)$

$= -\langle\psi|gE|\psi\rangle$

$= -\langle\psi|E|\psi\rangle$

$\Rightarrow \langle\psi|E|\psi\rangle = 0$, detectable and correctable

if $E \in N(S) \backslash S$ not correctable

(c) correctable errors: $\{E_j\}$ $E_j^\dagger E_k \notin N(S)/S$ for all j, k

proof: projector onto code space $P = \frac{1}{2^{n-k}} \prod_{j=1}^{n-k} (I + g_j) = \sum_{x_1 \cdots x_k} |x_1 \cdots x_k\rangle_L {}_L\langle x_1 \cdots x_k|$

if $E_j^\dagger E_k \in S \Rightarrow P E_j^\dagger E_k P = P$

if $E_j^\dagger E_k \in G_n \in G_n - N(S)$ $E_j^\dagger E_k$ anticommute with at least one of the generators, say g

$\Rightarrow P E_j^\dagger E_k P = P E_j^\dagger E_k g P = -P g E_j^\dagger E_k P$

$= -P E_j^\dagger E_k P$

$\Rightarrow P E_j^\dagger E_k P = 0$

(d) error detection and recovery

$$\text{code } |\psi\rangle \xrightarrow[E_j]{\text{error}} E_j|\psi\rangle \xrightarrow[g_i,\, i=1,\cdots,n-k]{\text{measure}} g_i E_j|\psi\rangle = \beta_i E_j|\psi\rangle \xrightarrow[E_j]{\text{apply}} |\psi\rangle$$

↗ error syndrome $\{\beta_i = \pm 1\}$ note $E_j g_i E_j^\dagger = \beta_i g_i$

degenerate code: different errors $E_j, E_{j'}$ have the same error syndrome $\{\beta_i\}$

$$E_j P E_j^\dagger = E_{j'} P E_{j'}^\dagger \Rightarrow E_j E_{j'} P E_{j'}^\dagger E_j^\dagger = P$$

(e) number of errors the stabilizer code $C(S)$ could correct

(weight of an operator $E \in G_n$) ≡ (# of non-identity terms)

(distance of the stabilizer code $C(S)$) = (minimum weight of elements of $N(S)\setminus S$)

$[n, k, d]$ stabilizer code correts t and less errors w/ $d \geq 2t+1$

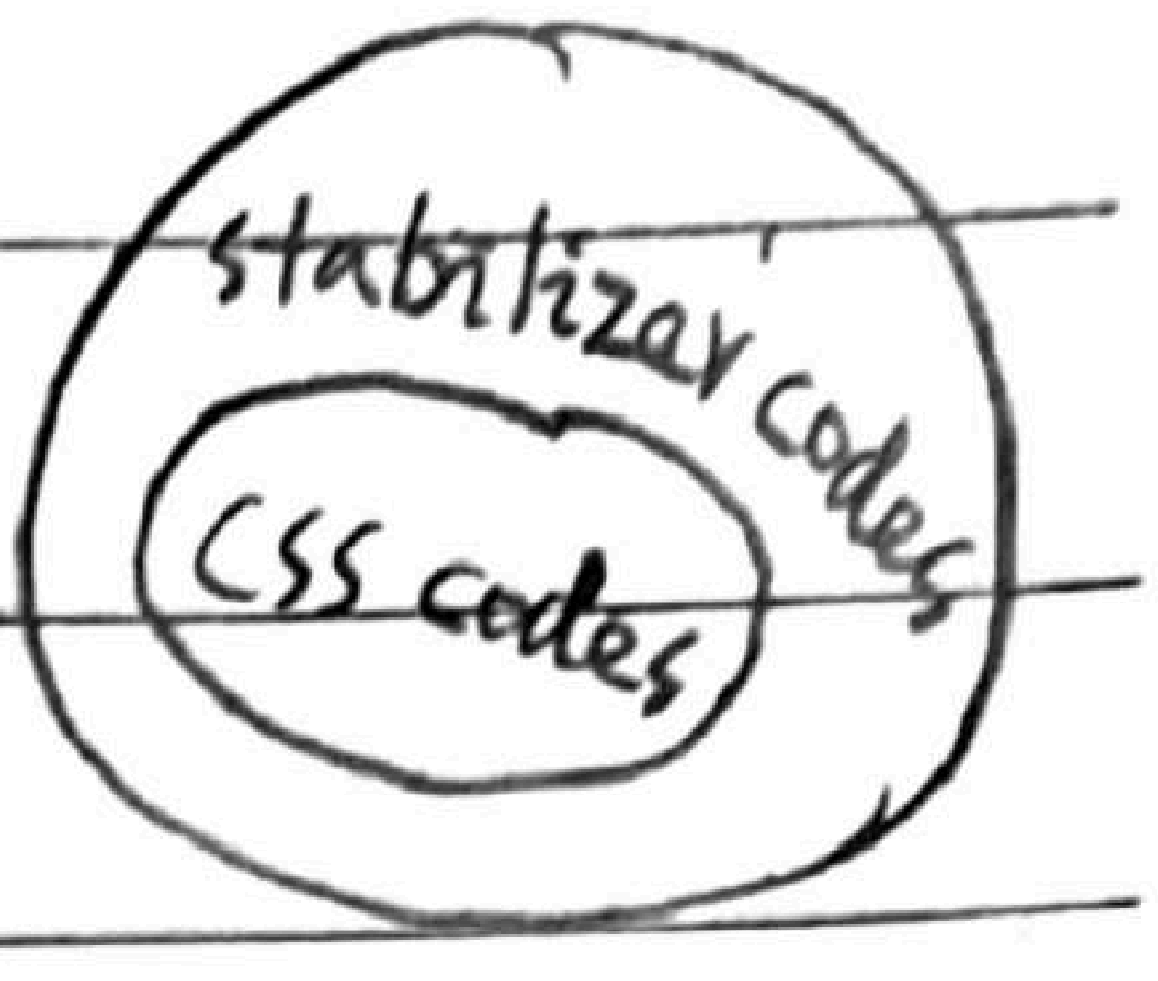
(f) three qubit bit flip code	$g_1 = Z_1 Z_2$	logical state	correctable errors
$[3,1]$ $t=1$	$g_2 = Z_2 Z_3$		$E_1 = X_1$
	$\bar{Z} = Z_1 Z_2 Z_3$	$|0_L\rangle = |000\rangle$	$E_2 = X_2$
	$\bar{X} = X_1 X_2 X_3$	$|1_L\rangle = |111\rangle$	$E_3 = X_3$

(g) three qubit phase flip code	$g_1 = X_1 X_2$	logical state	correctable errors
$[3,1]$ $t=1$	$g_2 = X_2 X_3$	$|0_L\rangle = |+++\rangle$	$E_1 = Z_1$
	$\bar{Z} = X_1 X_2 X_3$	$|1_L\rangle = |---\rangle$	$E_2 = Z_2$
	$\bar{X} = Z_1 Z_2 Z_3$		$E_3 = Z_3$

(h) nine qubit shor code	$g_1 = Z_1 Z_2$	logical state	correctable errors
$[9,1]$ $t=1$	$g_2 = Z_2 Z_3$	$|0_L\rangle = |PPP\rangle$	X_i $i=1,\cdots,8$
	$g_3 = Z_4 Z_5$	$|1_L\rangle = |MMM\rangle$	Z_i $i=1,\cdots,8$
	$g_4 = Z_5 Z_6$		
	$g_5 = Z_7 Z_8$	$|P\rangle \equiv \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$	$X_i Z_i$ $i=1,\cdots,8$
	$g_6 = Z_8 Z_9$	$|M\rangle \equiv \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$	
	$g_7 = X_1 X_2 X_3 X_4 X_5 X_6$		
	$g_8 = X_4 X_5 X_6 X_7 X_8 X_9$		
	$\bar{Z} = X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9$		
	$\bar{X} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7 Z_8 Z_9$		

(i) five qubit shor code	$g_1 = X_1 Z_2 Z_3 X_4$	logical state	correctable errors
$[5,1]$ $t=1$	$g_2 = X_2 Z_3 Z_4 X_5$	$|0_L\rangle = \frac{1}{4}(|00000\rangle + \cdots)$	X_i $i=1,\cdots,5$
saturates the quantum	$g_3 = X_1 X_3 Z_4 Z_5$		
Hamming bound	$g_4 = Z_1 X_2 X_4 Z_5$	$|1_L\rangle = \frac{1}{4}(|11111\rangle + \cdots)$	Z_i $i=1,\cdots,5$
the minimal number of	$\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5$		$X_i Z_i$ $i=1,\cdots,5$
physical qubits that could	$\bar{X} = X_1 X_2 X_3 X_4 X_5$		
correct any single qubit error			

(13) CSS codes are an excellent example of a class of stabilizer codes



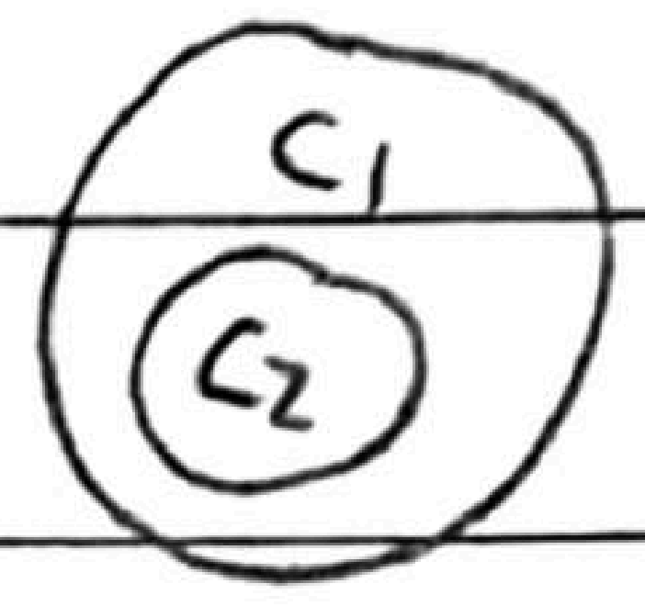
$CSS(C_1; C_2)$ $\quad C_2 \subset C_1$ $\quad k_2 < k_1$ $\quad k = k_1 - k_2$

$[n, k]$ $\quad [n, k_2]$ $\quad [n, k_1]$

check matrix $\underset{(n-k_1+k_2)\times n}{H} = \begin{pmatrix} \overset{k_2\times n}{H(C_2^\perp)} & 0 \\ 0 & \underset{(n-k_1)\times n}{H(C_1)} \end{pmatrix}$

proof: ① rows of check matrix H are independent ⇔ generators are independent

② $H(C_1)\, H(C_2^\perp)^T = H(C_1)\, G(C_2) = 0$ (as $C_2 \subset C_1$)



$\Rightarrow r(g_i) \Lambda r(g_j)^T$ for all $i, j = 1, 2, \cdots, n-k_1+k_2$

⇔ generators commute

$H(C_2^\perp)^T = G(C_2)$

③ $g_j |\psi\rangle = |\psi\rangle$ for code $|\psi\rangle$

$x \in C_1$ $\quad |x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$

for $j = 1, \cdots, k_2$ $\quad g_j$ are products of X's (note $10 \Leftrightarrow X$)

$g_j |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y+y_j\rangle$ $\qquad y_j$ = one of rows of $H(C_2^\perp)$

$= \frac{1}{\sqrt{|C_2|}} \sum_{y' \in C_2} |x+y'\rangle$ $\quad y' \equiv y + y_j \in C_2$ $\qquad$ = one of columns of $G(C_2)$ $\in C_2$

$= |x + C_2\rangle$

for $j = k_2+1, \cdots, n-k_1+k_2$ $\quad g_j$ are products of Z's (note $01 \Leftrightarrow Z$)

$g_j |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-)^{z_j \cdot (x+y)} |x+y\rangle$ $\qquad z_j$ = one of rows of $H(C_1)$

$x \in C_1,\ y \in C_2 \subset C_1$

$= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$ $\qquad \Rightarrow x + y \in C_1$

$\Rightarrow z_j \cdot (x+y) = 0$

$= |x + C_2\rangle$

6. Entropy and information

(1) Shannon entropy

a probability distribution $X = \{p_1, \cdots, p_n\}$, $0 \leq p_x \leq 1$, $x = 1, \cdots, n$, $\sum_x p_x = 1$

entroy = uncertainty = information $\quad H(X) \equiv -\sum_x p_x \log p_x$

w/ $0 \log 0 = \lim_{p \to 0} p \log p = 0$

eg: a fair coin $X = \{\frac{1}{2}, \frac{1}{2}\}$ $\quad H(X) = \log 2$

a fair dice $X = \{\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\}$ $\quad H(X) = \log 6$

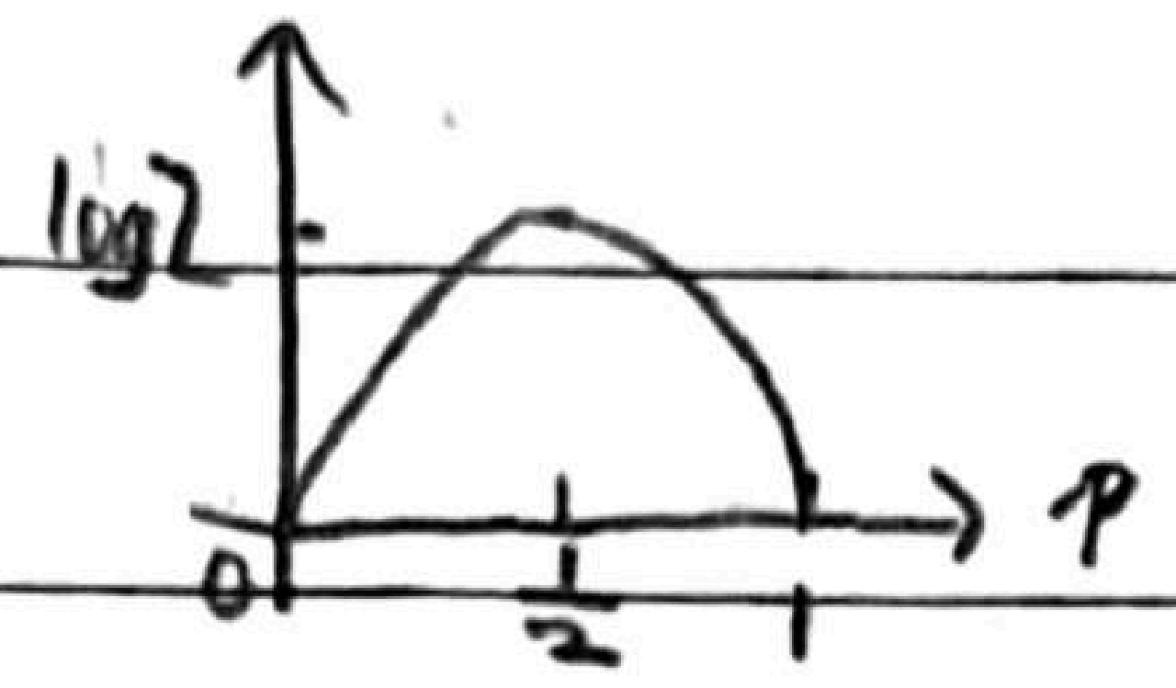
intuitive justification: $H(X) = \sum_x p_x I(p_x)$ · with information function $I(p)$, $p \in [0,1]$

satisfying $I(pq) = I(p) + I(q)$

$$\Rightarrow I'(pq)\,q = I'(p) \Rightarrow I'(pq) + I''(pq)\,pq = 0$$

$$\Rightarrow I(p) = k \log p \Rightarrow H(p_x) = k \sum_x p_x \log p_x$$

(2) binary entropy $X = \{p, 1-p\}$



$H_{max} = \log 2$ at $p = \frac{1}{2}$

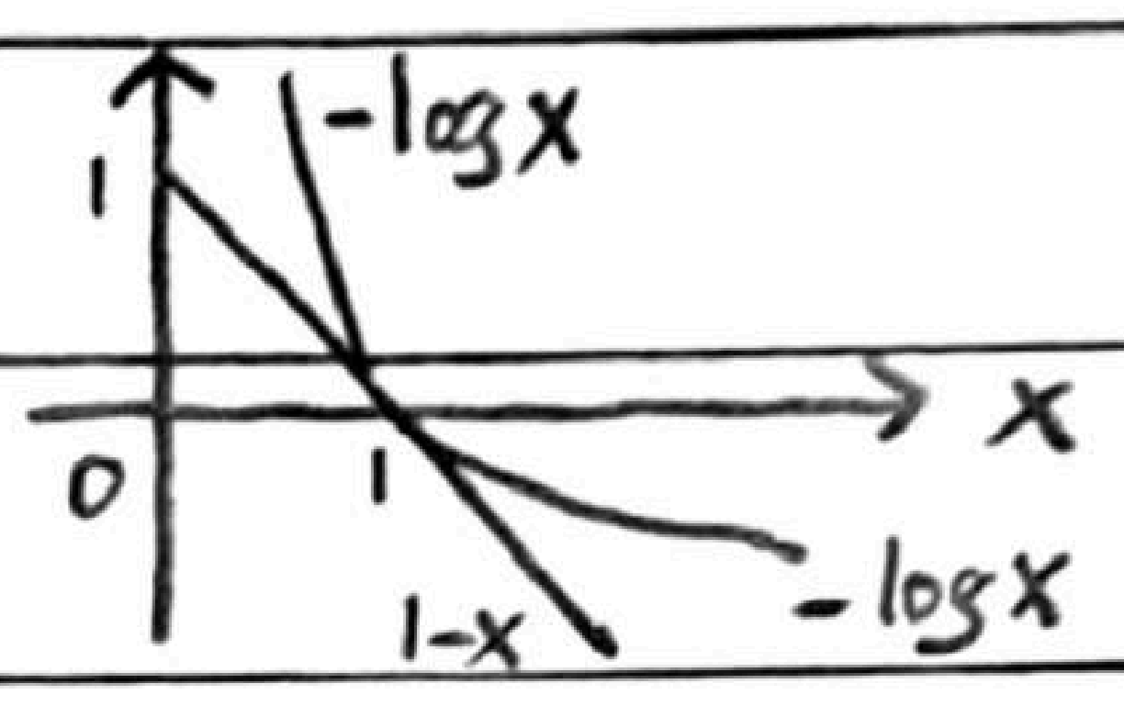
$$H(p) = -p\log p - (1-p)\log(1-p)$$

(3) relative entropy (Kullback-Leibler divergence)

$$H(p_x \| q_x) \equiv \sum_x p_x \log \frac{p_x}{q_x}$$ w/ $0 \log 0 = 0$, $-p \log 0 = +\infty$ if $p > 0$

theorem: $H(p_x \| q_x) \geq 0$ w/ equality iff $p_x = q_x$ for all x

proof: note $-\log x \geq 1 - x$ for $x > 0$ w/ equality iff $x = 1$



$$H(p_x \| q_x) = \sum_x p_x \left(-\log \frac{q_x}{p_x}\right)$$

$$\geq \sum_x p_x \left(1 - \frac{q_x}{p_x}\right)$$ w/ equality iff $p_x = q_x$ for all x

$$= \sum_x (p_x - q_x) = 0$$

(4) joint entropy $H(X,Y) \equiv -\sum_{x,y} p(x,y) \log p(x,y)$ joint probability $p(x,y)$

(5) conditional entropy: the entropy of X conditional on knowing Y

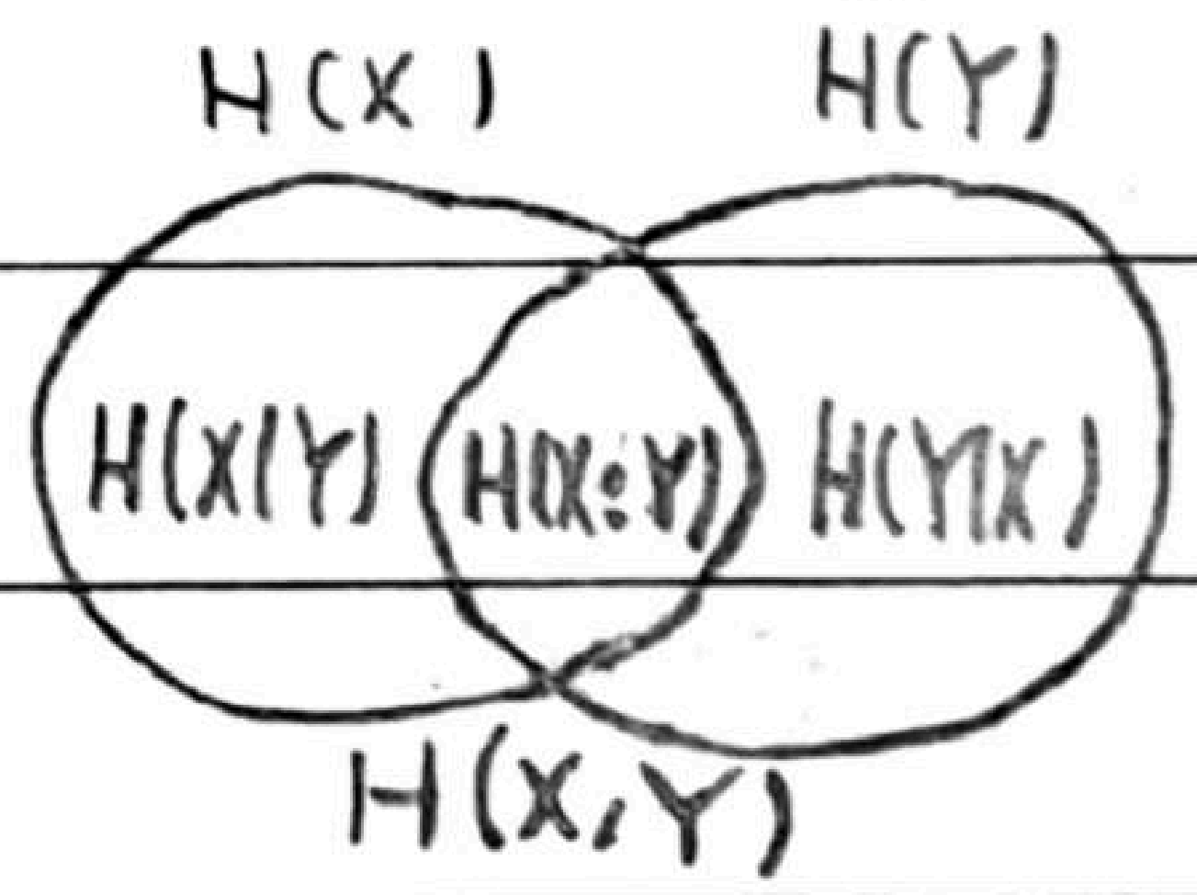
$$H(X|Y) \equiv H(X,Y) - H(Y)$$

(6) mutual information $H(X:Y) = H(X) + H(Y) - H(X,Y)$

$= H(X) - H(X|Y)$

$= H(Y) - H(Y|X)$

Venn diagram



(7) properties

① $H(X,Y) = H(Y,X)$, $H(X:Y) = H(Y:X)$ obvious

② $H(X|Y) \geq 0$ with equality iff $X = f(Y)$

proof: $p(x,y) = p(x|y)\,p(y)$ w/ conditional entropy $p(x|y)$

$$\Rightarrow H(X,Y) = -\sum_{x,y} p(x,y) \log [p(x|y)\,p(y)]$$

$$= -\sum_{x,y} p(x,y) \log p(x|y) - \sum_y p(y) \log p(y)$$

$$= H(Y) - \sum_{x,y} p(x,y) \log p(x|y)$$

$$\Rightarrow H(X|Y) = H(X,Y) - H(Y) = -\sum_{x,y} p(x,y) \log p(x|y) \geq 0$$

w/ equality $p(x|y) = 0$ or 1 for all x, y, i.e. $X = f(Y)$

③ $H(X) \leq H(X,Y)$ w/ equality iff $Y = f(X)$ (equivalent to ②)

④ subadditivity $H(X,Y) \leq H(X)+H(Y)$ with equality iff X, Y are independent

proof: note $\log x \leq x-1$ for $x>0$ w/ enequality iff $x=1$

$$H(X,Y)-H(X)-H(Y) = \sum_{x,y} p(x,y) \log \frac{p(x)p(y)}{p(x,y)} \leq \sum_{x,y} p(x,y)\left(\frac{p(x)p(y)}{p(x,y)}-1\right) = 0$$

w/ equality iff $p(x,y) = p(x)p(y)$ for all x, y, i.e. X, Y are independent

⑤ $H(X:Y) \geq 0$ w/ equality iff X, Y are independent (equivalent to ④)

(8) von Neumann entropy $S(\rho) \equiv -\mathrm{tr}(\rho \log \rho)$

(9) relative entropy $S(\rho\|\sigma) \equiv \mathrm{tr}(\rho\log\rho) - \mathrm{tr}(\rho\log\sigma) = -S(\rho) - \mathrm{tr}(\rho\log\sigma)$

Klein's inequality: $S(\rho\|\sigma) \geq 0$ w/ equality iff $\rho = \sigma$

proof: $\rho = \sum_i p_i |i\rangle\langle i|$ in orthonormal basis $|i\rangle$

$\sigma = \sum_j q_j |j\rangle\langle j|$ in orthonormal basis $|j\rangle$

$$\mathrm{tr}(\rho\log\sigma) = \sum_i \langle i|\rho\log\sigma|i\rangle = \sum_{ij} p_i P_{ij} \log q_j$$

w/ $P_{ij} \equiv \langle i|j\rangle\langle j|i\rangle$ $\quad 0 \leq P_{ij} \leq 1 \quad \sum_i P_{ij} = \sum_j P_{ij} = 1$

note $\log x$ is strictly concave

$$\sum_j P_{ij}\log q_j \leq \log\Big(\overset{r_i\,\equiv}{\sum_j P_{ij} q_j}\Big)$$

w/ equality iff $P_{ij} = 0$ or 1

w/o loss of generality $P_{ij} = \delta_{ij}$

$$\Rightarrow S(\rho\|\sigma) = \sum_i p_i\Big(\log p_i - \sum_j P_{ij}\log q_j\Big)$$

$$\geq \sum_i p_i \log\frac{p_i}{r_i} \quad \text{w/ equality iff } P_{ij} = 0 \text{ or } 1$$

$$\geq 0 \quad \text{w/ equality iff } p_i = r_i \text{ for all } i$$

$\Rightarrow S(\rho\|\sigma) \geq 0$ w/ equality iff $\rho = \sigma$

(10) properties

① $S(\rho) \geq 0$ obvious

② for d-dimentional Hilbert space $S_{max} = \log d$ only for $\rho = \frac{I}{d}$

proof: $S(\rho\|\frac{I}{d}) = -S(\rho) + \log d \geq 0 \Rightarrow S(\rho) \leq \log d$ w/ equality iff $\rho = \frac{I}{d}$

③ composite system AB in pure state $S(\rho_A) = S(\rho_B)$

proof: Schmidt decomposition $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$

$\Rightarrow \rho_A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$, $\rho_B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$

$\Rightarrow S(\rho_A) = S(\rho_B) = -\sum_i \lambda_i^2 \log \lambda_i^2$

④ probability p_i, orthogonal states ρ_i $S(\sum_i p_i \rho_i) = H(p_i) + \sum_i p_i S(\rho_i)$

proof: $\rho_i = \sum_j \lambda_{ij} |ij\rangle\langle ij| \Rightarrow \sum_i p_i \rho_i = \sum_{ij} p_i \lambda_{ij} |ij\rangle\langle ij|$

$$\Rightarrow S(\sum_i p_i \rho_i) = -\sum_{ij} p_i \lambda_{ij} \log(p_i \lambda_{ij})$$

$$= -\sum_i p_i \log p_i - \sum_i p_i \sum_j \lambda_{ij} \log \lambda_{ij}$$

$$= H(p_i) + \sum_i p_i S(\rho_i)$$

⑤ $S(\sum_i p_i \rho_i \otimes |i\rangle\langle i|) = H(p_i) + \sum_i p_i S(\rho_i)$ (obvious from ④)

(11) conditional entropy $S(A|B) = S(A,B) - S(B)$ not necessarily positive

(12) mutual information $S(A:B) = S(A) + S(B) - S(A,B)$

(13) projective measurement increases entropy

proof: $\rho \to \rho' = \sum_i P_i \rho P_i$ $\sum_i P_i = I$ $P_i P_j = \delta_{ij} P_i$

$$tr(\rho \log \rho') = tr(\sum_i P_i \rho \log \rho') = tr(\sum_i P_i \rho \log \rho' P_i) = tr(\sum_i P_i \rho P_i \log \rho') = tr(\rho' \log \rho')$$

$$\Rightarrow 0 \le S(\rho\|\sigma) = -S(\rho) - tr(\rho \log \rho') = -S(\rho) - tr(\rho' \log \rho') = -S(\rho) + S(\rho')$$

$\Rightarrow S(\rho') \geq S(\rho)$ w/ equality iff $\rho' = \rho$

(14) subadditivity $S(A,B) \le S(A) + S(B)$ w/ enequality $\rho_{A,B} = \rho_A \otimes \rho_B$

proof: $\rho = \rho_{AB}$ $\sigma = \rho_A \otimes \rho_B$

$$-tr(\rho \log \sigma) = -tr[\rho_{AB} \log(\rho_A \otimes \rho_B)]$$

$$= -tr[\rho_{AB}(\log \rho_A \otimes I_B + I_A \otimes \log \rho_B)]$$

$$= -tr(\rho_A \log \rho_A) - tr(\rho_B \log \rho_B)$$

$$= S(\rho_A) + S(\rho_B)$$

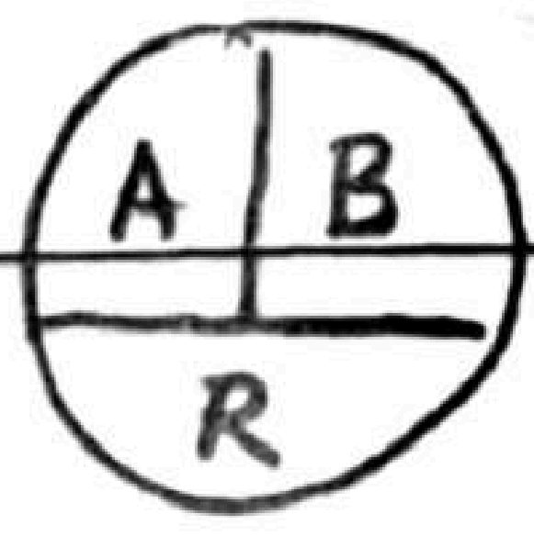
$$0 \le S(\rho\|\sigma) = -S(\rho) - tr(\rho \log \sigma) = -S(A,B) + S(A) + S(B)$$

$\Rightarrow S(A,B) \le S(A) + S(B)$

corollary: $S(A:B) \geq 0$

(15) Arakai-Lieb inequality $S(A,B) \geq |S(A) - S(B)|$

proof: purification



subadditivity $S(R) + S(A) \geq S(R,A)$

$\Rightarrow S(A,B) + S(A) \geq S(B)$

$\Rightarrow S(A,B) \geq S(B) - S(A)$ w/ equality iff $\rho_{RA} = \rho_R \otimes \rho_A$

similarly $S(A,B) \geq S(A) - S(B)$ w/ equality iff $\rho_{RB} = \rho_R \otimes \rho_B$

(16) concavity of entropy $S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$ 凹

proof: define $\rho_{A,B} \equiv \sum_i p_i \rho_i \otimes |i\rangle\langle i|$ $\quad S(A,B) = H(p_i) + \sum_i p_i S(\rho_i)$

$\Rightarrow \rho_A = \sum_i p_i \rho_i$ $\quad \Rightarrow \quad S(A) = S(\sum_i p_i \rho_i)$

$\rho_B = \sum_i p_i |i\rangle\langle i|$ $\quad S(B) = H(p_i)$

subadditivity $S(A) + S(B) \geq S(A,B) \Rightarrow S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$

(17) $S(\sum_i p_i \rho_i) \leq H(p_i) + \sum_i p_i S(\rho_i)$

proof: ① the special case $\rho_i = |\psi_i\rangle\langle\psi_i|$ note $|\psi_i\rangle$ are not necessarilly orthogonal

define $|AB\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle$ ($|i\rangle$ orthonormal)

$\Rightarrow \rho_A = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$\rho_B = \sum_{i,i'} \sqrt{p_i p_{i'}} \langle\psi_{i'}|\psi_i\rangle |i\rangle\langle i'|$

$\Rightarrow S_A = S(\sum_i p_i |\psi_i\rangle\langle\psi_i|) = S_B$

projective measurement $\rho'_B = \sum_i P_i \rho_B P_i$ (w/ $P_i \equiv |i\rangle\langle i|$)

$= \sum_i p_i |i\rangle\langle i|$

entropy increases

$S_{B'} = S(\rho'_B) = H(p_i)$

$S_B \leq S_{B'} \Rightarrow S(\sum_i p_i |\psi_i\rangle\langle\psi_i|) \leq H(p_i)$ w/ equality iff $|\psi_i\rangle$ orthogonal

② general case $\rho_i = \sum_j \lambda_{ij} |ij\rangle\langle ij|$

$\Rightarrow \sum_i p_i \rho_i = \sum_{ij} p_i \lambda_{ij} |ij\rangle\langle ij|$

$\Rightarrow S(\sum_i p_i \rho_i) \leq -\sum_{ij} p_i \lambda_{ij} \log(p_i \lambda_{ij})$

$= -\sum_i p_i \log p_i - \sum_i p_i \sum_j \lambda_{ij} \log \lambda_{ij}$

$= H(p_i) + \sum_i p_i S(\rho_i)$

w/ equality iff $|e_{ij}\rangle$ orthogonal, i.e. ρ_i orthogonal

(18) strong subadditivity $S_A + S_B \leq S_{A,C} + S_{B,C}$

$S_{A,B,C} + S_B \leq S_{A,B} + S_{B,C}$

(equivalent forms
$S_{A|B} + S_{B|A} \leq S_A + S_B$
$S_{A\cup B} + S_{A\cap B} \leq S_A + S_B$)

proof: no transparent proof is known, see details in the book

applications: ① conditioning reduces entropy $S(A|B,C) \leq S(A|B)$

proof: $\Leftrightarrow S(A,B,C) - S(B,C) \leq S(A,B) - S(B)$

$\Leftrightarrow S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$

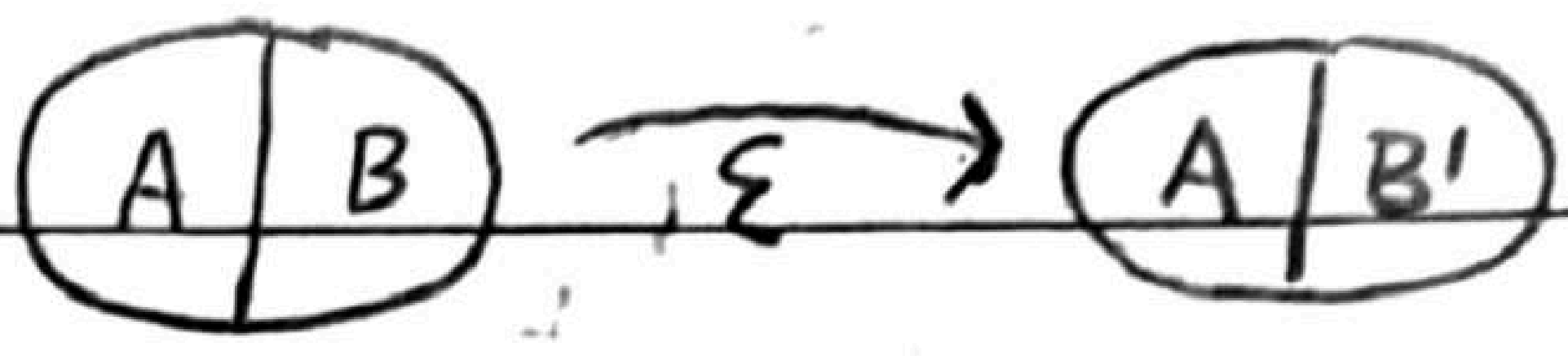
② discarding reduces mutual information $S(A:B) \le S(A:B,C)$

proof: $\Leftrightarrow S(A)+S(B)-S(A,B) \le S(A)+S(B,C)-S(A,B,C)$

$\Leftrightarrow S(A,B,C) + S(B) \le S(A,B) + S(B,C)$

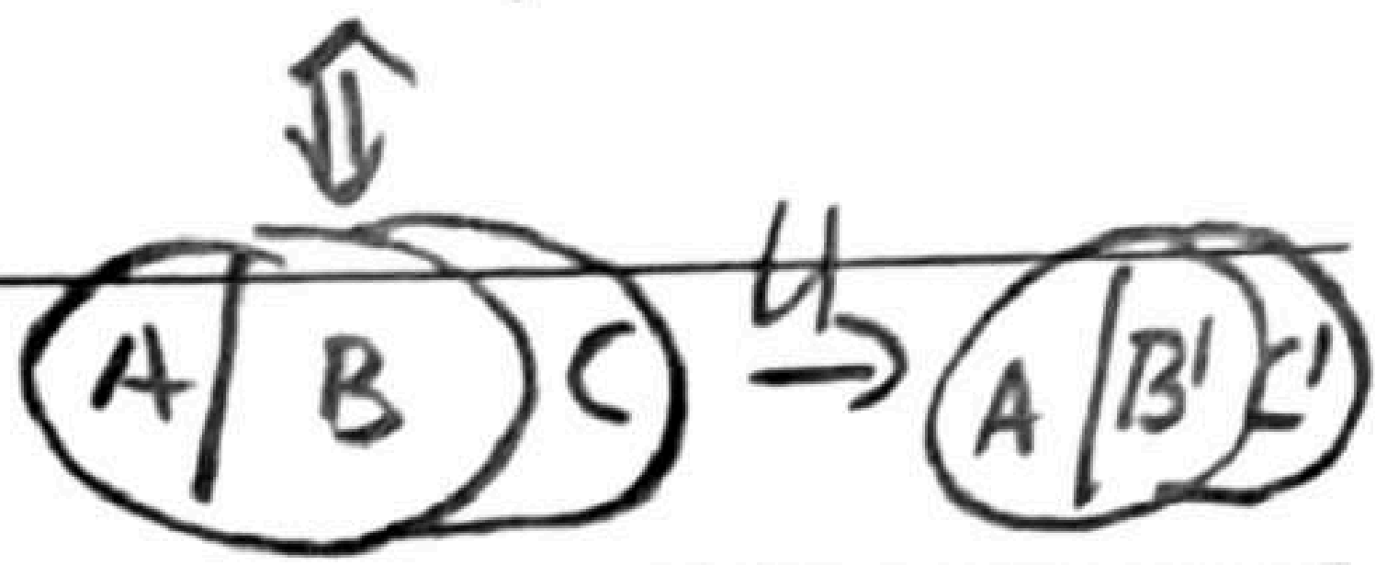
③ quantum operation reduces mutual information

$S(A:B') \le S(A:B)$



trace-preserving quantum operation on B

proof: $\mathcal{E}$ on B $\Leftrightarrow$ unitary operation on B, C



$\rho_{ABC} = \rho_{AB} \otimes |0\rangle\langle 0|$

$$\underset{\underset{S(A:B)}{\overset{\text{product}}{\parallel}}}{S(A:B,C)} \overset{\text{unitarity}}{=} \underset{\underset{S(A:B')}{\overset{\text{discarding}}{\vee\!|}}}{S(A:B',C')}$$

7. Quantum information theory (Holevo bound)

(1) Holevo bound (Holevo information, Holevo χ quantity)

Alice prepares quantum states $\rho_0, \cdots, \rho_n$ w/ probabilities $X = \{p_0, \cdots p_n\}$ and sends it to Bob. Bob performs measurement $\{E_y\} = \{E_0, \cdots, E_m\}$ with out come Y. mutual information $H(X:Y) \le S(\underset{\underset{\rho}{|||}}{\sum_x p_x \rho_x}) - \sum_x p_x S(\rho_x) \equiv \chi$

proof: Alice ⟶ Bob

P preparation system, Q quantum system, M measuring device

$$\underset{\underset{\rho_x = \rho}{\uparrow}}{0} \le \chi \le \underset{\overset{\nwarrow}{\rho_x \text{ orthogonal}}}{H(p_x)}$$

initial state $\rho_{PQM} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|$

$\rho_P = \sum_x p_x |x\rangle\langle x|$ $\quad \rho_Q = \sum_x p_x \rho_x$ $\quad \rho_M = |0\rangle\langle 0|$

$\rho_{PQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$

measurement of Bob $PQM \xrightarrow{\mathcal{E}} PQ'M'$ $\quad$ POVM elements $\{E_y\}$ on $\sigma \in Q$

$\mathcal{E}(\sigma \otimes |0\rangle\langle 0|) = \sum_y \sqrt{E_y}\, \sigma \sqrt{E_y} \otimes |y\rangle\langle y|$

measurement on QM w/ $\{\sqrt{E_y} \otimes U_y\}$ $\quad U_y|y'\rangle = |y+y' \bmod m+1\rangle$

$\Rightarrow S(P:Q) = S(P:Q,M)$ as $\rho_{PQM} = \rho_{PQ} \otimes \rho_M$

$S(P:QM) \geq S(P:Q'M')$ as quantum operation reduces mutual information

$S(P:Q'M') \geq S(P:M')$ as discarding reduces mutual information

$\Rightarrow S(P:M') \le S(P:Q)$

LHS: $\rho_{PM'Q'} = \sum_{x,y} p_x |x\rangle\langle x| \otimes \sqrt{E_y}\rho_x\sqrt{E_y} \otimes |y\rangle\langle y|$

$\Rightarrow \rho_{PM'} = \sum_{x,y} p_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y|$ w/ $p_{x,y} \equiv p_x \mathrm{tr}(\sqrt{E_y}\rho_x\sqrt{E_y}) = p_x \mathrm{tr}(\rho_x E_y)$

$= p_x\, p_{y|x}$ conditional probability

$\Rightarrow \rho_P = \sum_x p_x |x\rangle\langle x| \quad \rho_{M'} = \sum_y p_y |y\rangle\langle y|$

$\Rightarrow S(P:M') = H(X:Y)$

RHS $S(P) = H(p_x) \quad S(Q) = S(\sum_x p_x \rho_x) \quad S(P,Q) = H(p_x) + \sum_x p_x S(\rho_x)$

$\Rightarrow S(P:Q) = S(\sum_x p_x\rho_x) - \sum_x p_x \rho_x = \chi$

$\Rightarrow H(X:Y) \leq \chi$

A. quantum teleportation of a mixed state

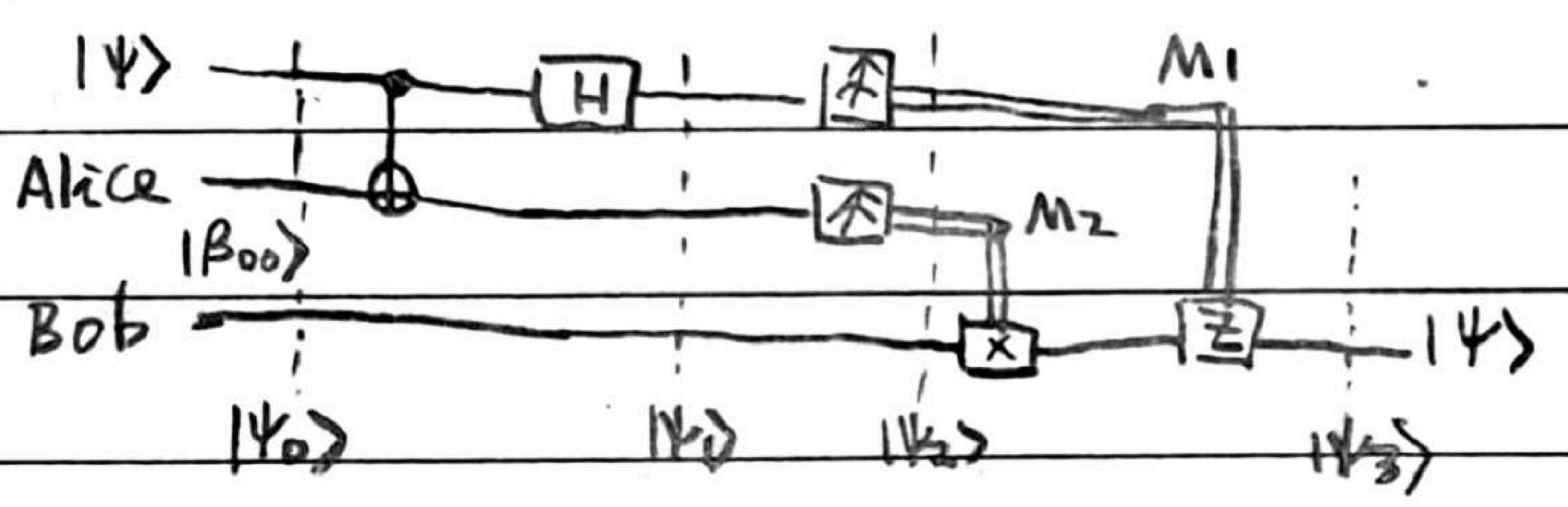
(1) Is a mixed state quantum or classical? Quantum.

How does a quantum state become classical? Wave function collapses.

Why and how does a wave function collapse? Unkown.

How should I do calculate? Follow the measurement protocol.

(2) general pure state



CNOT gate $U = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$

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

general pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

initial state $|\psi_0\rangle = |\psi\rangle \otimes |\psi_{00}\rangle$

$\Rightarrow |\psi_1\rangle = (H\otimes I\otimes I)(U\otimes I)|\psi_0\rangle$

~~Bob acts~~

Alice measures $P_{00} = |00\rangle\langle 00| \otimes I \quad p_{00} = \langle\psi_1|P_{00}|\psi_1\rangle \quad |\psi_2\rangle = \frac{P_{00}|\psi_1\rangle}{\sqrt{p_{00}}} \quad \Rightarrow |\psi_3\rangle = |\psi_2\rangle = |00\rangle\otimes|\psi\rangle$

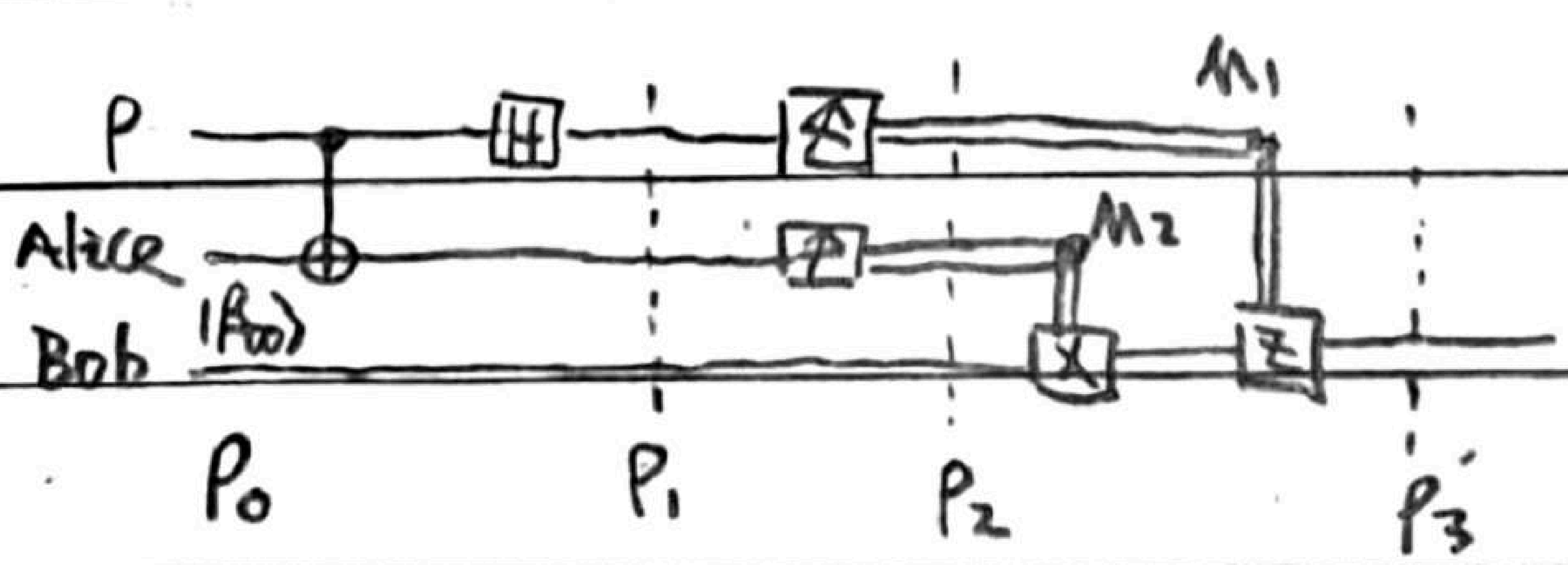
$P_{01} = |01\rangle\langle 01| \otimes I \quad p_{01} = \langle\psi_1|P_{01}|\psi_1\rangle \quad |\psi_2\rangle = \frac{P_{01}|\psi_1\rangle}{\sqrt{p_{01}}} \quad \Rightarrow |\psi_3\rangle = X|\psi_2\rangle = |01\rangle\otimes|\psi\rangle$

$P_{10} = |10\rangle\langle 10| \otimes I \quad p_{10} = \langle\psi_1|P_{10}|\psi_1\rangle \quad |\psi_2\rangle = \frac{P_{10}|\psi_1\rangle}{\sqrt{p_{10}}} \quad \Rightarrow |\psi_3\rangle = Z|\psi_2\rangle = |10\rangle\otimes|\psi\rangle$

$P_{11} = |11\rangle\langle 11| \otimes I \quad p_{11} = \langle\psi_1|P_{11}|\psi_1\rangle \quad |\psi_2\rangle = \frac{P_{11}|\psi_1\rangle}{\sqrt{p_{11}}} \quad \Rightarrow |\psi_3\rangle = ZX|\psi_2\rangle = |11\rangle\otimes|\psi\rangle$

(3) general mixed state

$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$



initial state $\rho_0 = \rho \otimes |\beta_{00}\rangle\langle\beta_{00}|$

$\Rightarrow \rho_1 = (H\otimes I\otimes I)(U\otimes I)\rho_0(U\otimes I)(H\otimes I\otimes I)$

Bob acts

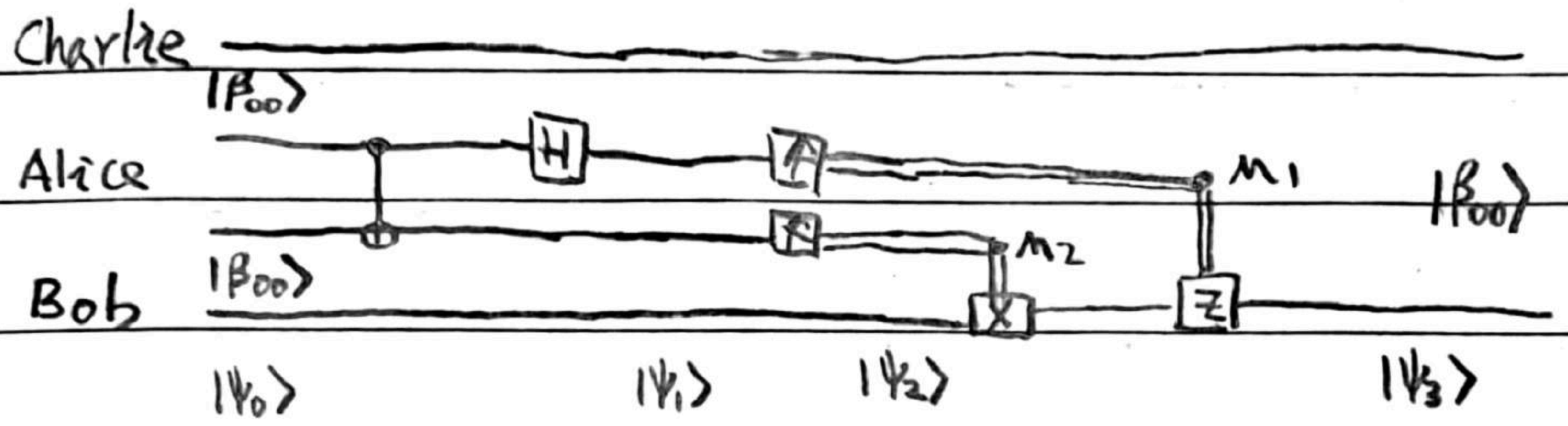
Alice measures $P_{00} = |00\rangle\langle 00| \otimes I$ $\quad p_{00} = tr(\rho_1 P_{00})$ $\quad \rho_2 = \frac{P_{00}\rho_1 P_{00}}{p_{00}}$ $\quad \Rightarrow \rho_3 = \rho_2 = |00\rangle\langle 00| \otimes \rho$

$P_{01} = |01\rangle\langle 01| \otimes I$ $\quad p_{01} = tr(\rho_1 P_{01})$ $\quad \rho_2 = \frac{P_{01}\rho_1 P_{01}}{p_{01}}$ $\quad \Rightarrow \rho_3 = X\rho_2 X = |01\rangle\langle 01| \otimes \rho$

$P_{10} = |10\rangle\langle 10| \otimes I$ $\quad p_{10} = tr(\rho_1 P_{10})$ $\quad \rho_2 = \frac{P_{10}\rho_1 P_{10}}{p_{10}}$ $\quad \Rightarrow \rho_3 = Z\rho_2 Z = |10\rangle\langle 10| \otimes \rho$

$P_{11} = |11\rangle\langle 11| \otimes I$ $\quad p_{11} = tr(\rho_1 P_{11})$ $\quad \rho_2 = \frac{P_{11}\rho_1 P_{11}}{p_{11}}$ $\quad \Rightarrow \rho_3 = ZX\rho_2 XZ = |11\rangle\langle 11| \otimes \rho$

(4) entanglement transfer



initial state $|\psi_0\rangle = |\beta_{00}\rangle \otimes |\beta_{00}\rangle$

$\Rightarrow |\psi_1\rangle = (I\otimes H\otimes I\otimes I)(I\otimes U\otimes I)|\psi_0\rangle$

Bob acts

Alice measures $P_{00} = I\otimes|00\rangle\langle 00|\otimes I$ $\quad p_{00} = \langle\psi_1|P_{00}|\psi_1\rangle$ $\quad |\psi_2\rangle = \frac{P_{00}|\psi_1\rangle}{\sqrt{p_{00}}}$ $\quad \Rightarrow |\psi_3\rangle = |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1001\rangle)$

$P_{01} = I\otimes|01\rangle\langle 01|\otimes I$ $\quad p_{01} = \langle\psi_1|P_{01}|\psi_1\rangle$ $\quad |\psi_2\rangle = \frac{P_{01}|\psi_1\rangle}{\sqrt{p_{01}}}$ $\quad \Rightarrow |\psi_3\rangle = X|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0010\rangle + |1011\rangle)$

$P_{10} = I\otimes|10\rangle\langle 10|\otimes I$ $\quad p_{10} = \langle\psi_1|P_{10}|\psi_1\rangle$ $\quad |\psi_2\rangle = \frac{P_{10}|\psi_1\rangle}{\sqrt{p_{10}}}$ $\quad \Rightarrow |\psi_3\rangle = Z|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0100\rangle + |1101\rangle)$

$P_{11} = I\otimes|11\rangle\langle 11|\otimes I$ $\quad p_{11} = \langle\psi_1|P_{11}|\psi_1\rangle$ $\quad |\psi_2\rangle = \frac{P_{11}|\psi_1\rangle}{\sqrt{p_{11}}}$ $\quad \Rightarrow |\psi_3\rangle = ZX|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1111\rangle)$

<over>