1 LINEAR ALGEBRA

THEO $V, W \in V$ $\mathbb{R}$ or $\mathbb{C}$-VR $\Rightarrow |\langle v,w\rangle| \le \|v\| \cdot \|w\|$

DEF $P \in \mathbb{C}^{n\times n}$ orth. proj if P Hermitian, $P^2 = P$,
$A \in \mathbb{C}^{n\times n}$ normal if $A^\dagger A = AA^\dagger$

THEO $A \in \mathbb{C}^{n\times n}$ is unit. diag $\Leftrightarrow$ normal
In this case $Av = \sum_{i=1}^{n} \lambda_i u_i u_i^\dagger v$.

DEF spectral radius $\rho(A) = \max\{|\lambda_1|, \dots, |\lambda_n|\}$

THEO $A \in \mathbb{C}^{n\times n} \Rightarrow \exists\, U, V \in \mathcal{U}_n(\mathbb{C}), \sigma_1, \dots, \sigma_n > 0$:
$A = U \begin{pmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_n \end{pmatrix} V^\dagger$

2 BASIC CONCEPTS

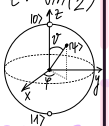
2.1 QUANTUM BITS

DEF quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$

REM α, β can't be measured, instead
$\mathbb{P}(0) = |\alpha|^2$, $\mathbb{P}(1) = |\beta|^2$. $|\psi\rangle$ —[meter]

wavefunction collapse: Measured $0 \rightsquigarrow |\psi\rangle = |0\rangle$

DEF Bloch sphere rep. $\alpha = e^{i\gamma}\cos(\frac{\vartheta}{2})$, $\beta = e^{i(\gamma+\varphi)}\sin(\frac{\vartheta}{2})$
$\Rightarrow |\psi\rangle = e^{i\gamma}(\cos(\frac{\vartheta}{2})|0\rangle + e^{i\varphi}\sin(\frac{\vartheta}{2})|1\rangle)$
$\varphi \in [0, 2\pi)$, $\vartheta \in [0, \pi]$ $\quad \vec{r} = \begin{pmatrix} \cos\varphi\sin\vartheta \\ \sin\varphi\sin\vartheta \\ \cos\vartheta \end{pmatrix}$



2.2 SINGLE QUBIT GATES

DEF Time evolution $\mathcal{U} \in \mathcal{U}_n(\mathbb{C})$:
$|\psi'\rangle = \mathcal{U} \cdot |\psi\rangle$ or $|\psi\rangle$ —[$\mathcal{U}$]— $|\psi'\rangle$ $\quad H^2 = I$

Pauli-X —[X]— $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Hadamard —[H]— $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-Y —[Y]— $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Phase —[S]— $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Pauli-Z —[Z]— $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\pi/8$ —[T]— $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ $\quad T^2 = S$

EX 1) $|\psi\rangle = \cos(\frac{\vartheta}{2})|0\rangle + e^{i\varphi}\sin(\frac{\vartheta}{2})|1\rangle \Rightarrow$
$Z|\psi\rangle = \cos(\frac{\vartheta}{2})|0\rangle + e^{i\pi}e^{i\varphi}\sin(\frac{\vartheta}{2})|1\rangle \Rightarrow \vartheta' = \vartheta$, $\varphi' = \varphi + \pi$,
2) $H(\alpha|0\rangle + \beta|1\rangle) = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

DEF commutator $[A,B] = AB - BA$,
anti-commutator $\{A,B\} = AB + BA$

THEO Pauli matrices satisfy
1) $\sigma_j^2 = I$ 2) $\sigma_j \cdot \sigma_k = -\sigma_k\sigma_j$, $j \neq k$ 3) $[\sigma_1, \sigma_2] = 2i\sigma_3$ (or 231 or 312)

THEO $e^A := \sum_{k=0}^{\infty} \frac{1}{k!}A^k$, $A^2 = I$, $x \in \mathbb{R}$
$\Rightarrow e^{iAx} = \cos(x)I + i\sin(x)A$

DEF rotation operators for $\vartheta \in \mathbb{R}$
$R_x(\vartheta) = e^{iX(-\frac{\vartheta}{2})} = \cos(\frac{\vartheta}{2})I - i\sin(\frac{\vartheta}{2})X = \begin{bmatrix} \cos(\frac{\vartheta}{2}) & -i\sin(\frac{\vartheta}{2}) \\ -i\sin(\frac{\vartheta}{2}) & \cos(\frac{\vartheta}{2}) \end{bmatrix}$
$R_y(\vartheta) = \begin{bmatrix} \cos(\frac{\vartheta}{2}) & -\sin(\frac{\vartheta}{2}) \\ \sin(\frac{\vartheta}{2}) & \cos(\frac{\vartheta}{2}) \end{bmatrix}$, $R_z(\vartheta) = \begin{bmatrix} e^{-i\vartheta/2} & 0 \\ 0 & e^{i\frac{\vartheta}{2}} \end{bmatrix}$

rotation about $\vec{v} \in \mathbb{R}^3$ ($\|\vec{v}\| = 1$) $(\vec{v}\cdot\vec{\sigma})^2 = I$
$R_{\vec{v}}(\vartheta) = e^{i(\vec{v}\cdot\vec{\sigma})(-\frac{\vartheta}{2})} = \cos(\frac{\vartheta}{2})I - i\sin(\frac{\vartheta}{2})(\vec{v}\cdot\vec{\sigma})$

THEO One can show that $R_{\vec{v}}(\vartheta)$ is a conventional rotation by ϑ about $\vec{v}$.

THEO $\sin(\alpha+\beta) = \sin(\alpha)\sin(\beta) + \cos(\alpha)\cos(\beta)$
$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$

THEO Z-Y Decomposition $\mathcal{U} \in \mathcal{U}_2(\mathbb{C})$
$\Rightarrow \exists\, \alpha, \beta, \gamma, \delta \in \mathbb{R}$: $\mathcal{U} = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$

2.3 MULTIPLE QUBITS

DEF general two-qubit state
$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, $\alpha_{ij} \in \mathbb{C}$
$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

REM Measure only one qubit:
0 w.p $|\alpha_{00}|^2 + |\alpha_{01}|^2$, 1 w.p $|\alpha_{10}|^2 + |\alpha_{11}|^2$ (analog for 1)
wavefunction 0: $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

DEF tensor product $\{|i\rangle_V : i = 1, \dots, m\}$ bas. of V
$\{|j\rangle : j = 1, \dots, n\}$ bas. of $W \Rightarrow \{|i\rangle_V \otimes |j\rangle_W\}$ bas. of $V\otimes W$

THEO $\otimes$ is bilinear, $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} v_1w_1 \\ v_1w_2 \\ v_2w_1 \\ v_2w_2 \end{pmatrix}$

DEF inner product on $V \otimes W$
$\langle \sum_j \alpha_j |v_j\rangle \otimes |w_j\rangle | \sum_k \beta_k |\tilde{v}_k\rangle \otimes |\tilde{w}_k\rangle \rangle := \sum_j \sum_k \alpha_j^* \beta_k \langle v_j|\tilde{v}_k\rangle\langle w_j|\tilde{w}_k\rangle$

DEF n-qubit state $|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle$, $\alpha_x \in \mathbb{C}$, $\sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$

2.4 MULTIPLE QUBIT GATES

EX CNOT-gate $|a,b\rangle \mapsto |a, a\oplus b\rangle$, $a, b \in \{0,1\}$
$|a\rangle$ —●— $|a\rangle$; $|b\rangle$ —⊕— $|a\oplus b\rangle$ $\quad \mathcal{U}_{CNOT} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$ (Pauli-X)

EX controlled-$\mathcal{U}$ gate $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$,
$|10\rangle \mapsto |1\rangle \otimes \mathcal{U}|0\rangle$, $|11\rangle \mapsto |1\rangle \otimes \mathcal{U}|1\rangle$ $\quad \hat{=} \begin{pmatrix} 1 & \\ & \mathcal{U} \end{pmatrix}$
← controlled-Z-gate

THEO Single qubit and CNOT gates are universal.

EX Controlled $\mathcal{U}$ for multiple target qubits

EX Single qubit gates acting in parallel
$= A\otimes B\ [|a\,b\rangle \mapsto A|a\rangle \otimes B|b\rangle = A\otimes B|a\rangle\otimes|b\rangle]$

THEO Properties of $\otimes$ 1) $(A\otimes B)^* = A^* \otimes B^*$,
2) $(A\otimes B)^T = A^T \otimes B^T$, 3) $(A\otimes B)^\dagger = A^\dagger \otimes B^\dagger$
4) $(A\otimes B)\otimes C = A\otimes(B\otimes C)$, 5) $(A\otimes B)\cdot(C\otimes D) = (A\cdot C)\otimes(B\cdot D)$
6) A, B Hermit (unitary) $\Rightarrow A\otimes B$ too.

2.5 QUANTUM MEASUREMENT

THEO let $\mathcal{U} \in \mathcal{U}_2(\mathbb{C})$, $\alpha|0\rangle + \beta|1\rangle = a\vec{u}_1 + b\vec{u}_2$ then measurement w.r. to $\{\vec{u}_1, \vec{u}_2\}$
($\vec{u}_1$ w.p $|a|^2$, $\vec{u}_2$ w.p $|b|^2$) is repr. as follows:
—[$\mathcal{U}^\dagger$]—[meter]—[$\mathcal{U}$]— (qubit after collapse; measurement result)

EX $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $|+\rangle := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $|-\rangle := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$
Meas. w.r. to $\{|+\rangle, |-\rangle\} \rightsquigarrow$ "+" w.p $\frac{|\alpha+\beta|^2}{2}$, "−" w.p $\frac{|\alpha-\beta|^2}{2}$.

DEF quantum measurements are descr. by measurement operators $\{M_m\}$. The index m labels possible measur. outcomes.
If $|\psi\rangle$ state before measuring, then
1) m occurs w.p $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \|M_m|\psi\rangle\|^2$
2) state after measur. $M_m|\psi\rangle / \|M_m|\psi\rangle\|$
3) $\sum_m M_m^\dagger M_m \stackrel{!}{=} I$ $(\Rightarrow \sum_m p(m) = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = 1)$

EX $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $M_0 = |0\rangle\langle 0|$, $M_1 := |1\rangle\langle 1|$
$\Rightarrow p(0) = |\alpha|^2$, $p(1) = |\beta|^2$

DEF Recall: A normal $A = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| = \sum_{k=1}^{m} \tilde{\lambda}_k P_k$ (Projection onto eigenspace). Proj. measurement is def. by observable M Hermitian
$M = \sum \lambda_m P_m$ (Proj. onto eigenspace)
1) λ_m occurs w.p. $p(\lambda_m) = \langle\psi|P_m|\psi\rangle$
2) state after measur. $P_m|\psi\rangle / \|P_m|\psi\rangle\|$ $\quad (P_m^\dagger P_m)$

REM Proj. meas. combined w. unitary trafos are equivalent to general meas.

DEF average value of a proj. meas.
$\mathbb{E}[M] = \sum_m \lambda_m p(\lambda_m) = \sum_m \lambda_m \langle\psi|P_m|\psi\rangle$
$= \langle\psi|\sum_m \lambda_m P_m|\psi\rangle = \langle\psi|M|\psi\rangle =: \langle M\rangle$

standard deviation
$\Delta(M) := \sqrt{\langle M^2\rangle - \langle M\rangle^2} = \sqrt{\langle(M - \langle M\rangle)^2\rangle}$

REM 1) Measurement w.r. to orth. basis $\{|u_1\rangle, |u_2\rangle\}$ is a proj. meas.: set $P_m = |u_m\rangle\langle u_m|$
$M = \lambda_1 P_1 + \lambda_2 P_2$, $\lambda_1 \neq \lambda_2 \in \mathbb{R}$
2) $Z = 1\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (-1)\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ agrees with standard measurement w.r. to $\{|0\rangle, |1\rangle\}$
3) P_m's orthogonal projectors, $\sum P_m = I$,
$P_m P_{m'} = \delta_{mm'} P_m$. $M = \sum_m m P_m$ corr. observable

2.6 THE HEISENBERG UNCERTAINTY PRINCIPLE

A, B Hermitian, $\langle\psi|AB|\psi\rangle = x + iy$, $x, y \in \mathbb{R}$

$\langle\psi|AB|\psi\rangle^* = \langle\psi|(AB)^\dagger|\psi\rangle = \langle\psi|BA|\psi\rangle$
$\Rightarrow \langle\psi|[A,B]|\psi\rangle = 2iy$, $\langle\psi|\{A,B\}|\psi\rangle = 2x$
$\Rightarrow |\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2$ (∗)

Cauchy-Schwarz $|\langle v|w\rangle|^2 \le \|v\|^2\|w\|^2$ $\quad (|v\rangle = A|\psi\rangle$, $|w\rangle = B|\psi\rangle)$
$\Rightarrow |\langle\psi|AB|\psi\rangle|^2 \le \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$
$\stackrel{(*)}{\Rightarrow} |\langle\psi|[A,B]|\psi\rangle|^2 \le 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$

C & D two observables $\rightsquigarrow A = C - \langle C\rangle$, $B := D - \langle D\rangle$
$\Rightarrow \Delta(C)\Delta(D) \ge \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}$ (Prepare large # of $|\psi\rangle$, meas. C and D)

3. ENTANGLEMENT & ITS APPLIC.

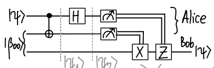
DEF A n-qubit state $|\psi\rangle$ ($n \ge 2$) is entangled if
$|\psi\rangle \neq |\varphi_{n-1}\rangle \otimes \dots \otimes |\varphi_0\rangle$, $|\varphi_i\rangle \in \mathbb{C}^2$

EX Bell states (EPR) $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,
$|x\rangle$ —[H]—●—; $|y\rangle$ ——⊕— $\}|\beta_{xy}\rangle$, $x, y \in \{0,1\}$
$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$,
$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$,
$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

3.1 QUANTUM TELEPORTATION

1) Alice & Bob generated $|\beta_{00}\rangle$. They keep one qubit of the pair.
2) Alice wants to send $|\psi\rangle$ to Bob

Quantum circuit for teleporting $|\psi\rangle$:



Input: $|\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}[|\psi\rangle \otimes (|00\rangle + |11\rangle)] = \frac{1}{\sqrt{2}}[(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)]$
$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$
$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$
$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$
$= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$

3) Alice meas. her qubits w.r.to computat. basis
(Proj. meas. $P_1 = |00\rangle\langle 00| \otimes I$, $P_2 = |01\rangle\langle 01| \otimes I$, $P_3 = |10\rangle\langle 10| \otimes I$, $P_4 = |11\rangle\langle 11| \otimes I$)
Meas 00, then $|\psi_2\rangle$ collapses to $|00\rangle|\psi\rangle$ ...
4) Alice transmits (class. info) to Bob, he applies X or Z.
5) No faster-than-light comm. due to class. comm.

3.2 EPR AND THE BELL INEQUALITY

1) Alice & Bob share $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
2) They measure the observable $\vec{v}\cdot\vec{\sigma} = v_1X + v_2Y + v_3Z$, $\|\vec{v}\| = 1$
($\vec{v}\cdot\vec{\sigma}$ Hermitian, unitary, eigenvalues ± 1)
3) Alice measures before Bob
• $\vec{v} = (0,0,1) \Rightarrow \vec{v}\cdot\vec{\sigma} = Z = 1|0\rangle\langle 0| + (-1)|1\rangle\langle 1|$ (stand. measurem.)
Alice meas. $1 \rightsquigarrow |01\rangle$, $-1 \rightsquigarrow |10\rangle$ $\Rightarrow$ Bob gets the opposite
• $\vec{v} = (1,0,0) \Rightarrow \vec{v}\cdot\vec{\sigma} = X = 1|+\rangle\langle +| + (-1)|-\rangle\langle -|$ (meas. w.r.to $\{|+\rangle, |-\rangle\}$)
$|\beta_{11}\rangle = -\frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \Rightarrow$ Bob gets the opposite
• $\vec{v}$ general. Let $\{|a\rangle, |b\rangle\}$ orth. eigenstates of $\vec{v}\cdot\vec{\sigma}$,
$|0\rangle = \alpha|a\rangle + \beta|b\rangle$, $|1\rangle = \gamma|a\rangle + \delta|b\rangle$ $\quad$ base change $\mathcal{U} := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$
$\Rightarrow |\beta_{11}\rangle = (\alpha\delta - \beta\gamma)\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$, $\mathcal{U}$ unitary $\Rightarrow |\alpha\delta - \beta\gamma| = 1$
$= e^{i\vartheta}\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$
$\Rightarrow$ Bob gets the opposite
4) Alice can predict Bob's result. (bc of measurem. works)

Bell's inequality: Many repetitions of the setup:
1) A (decide rand. whether to meas. Q or R (S or T)) Q or R ● — C prepares two particles — ● S or T B
2) $Q, R, S, T \in \{\pm 1\}$
3) Alice and Bob perform meas. simultaneously
4) Alice and Bob analyze data
• $QS + RS + RT - QT = \underbrace{(Q+R)}_{=\pm 2 \vee 0}S + \underbrace{(R-Q)}_{=0 \vee \pm 2}T = \pm 2$
• $p(q,r,s,t)$ prob. that the system before meas.: $Q = q, R = r$, $S = s, T = t$
$\Rightarrow \mathbb{E}[QS + RS + RT - QT] = \sum p(q,r,s,t)\underbrace{(qs + rs + rt - qt)}_{\pm 2} \le 2$
$\Rightarrow \mathbb{E}[QS] + \mathbb{E}[RS] + \mathbb{E}[RT] - \mathbb{E}[QT] \le 2$ ← Bell's inequality

1) Charly prepares $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and sends the first qubit to Alice and the second to Bob.
2) $Q = Z_1$, $S = \frac{-Z_2 - X_2}{\sqrt{2}}$, $R = X_1$, $T = \frac{Z_2 - X_2}{\sqrt{2}}$ $\Rightarrow \langle QS\rangle = \langle RS\rangle = \langle RT\rangle = \frac{1}{\sqrt{2}}$, $\langle QT\rangle = -\frac{1}{\sqrt{2}}$
$\Rightarrow \langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \not\le 2$

∘ "realism": Q, R, S, T have definite values indep. of observation.
∘ "locality": Alice performing her meas. cannot influence Bob's meas and vice versa.
$\rightsquigarrow$ Nature is not "locally realistic."

4. QUANTUM SEARCH ALGOR.

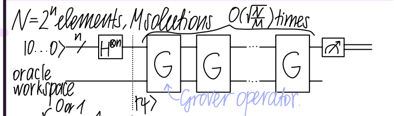
Classical search $-\mathcal{O}(N)$ (# of elements) $\quad$ Quant. Grover's Alg $-\mathcal{O}(\sqrt{N})$ (given precond.)

4.1 QUANTUM ORACLES

1) Given $N = 2^n$ elem., labeled $0, 1, \dots, N-1$ & $1 \le M \le N$ solut.
2) Define $f = \mathbb{1}_{\{solutions\}}: \{0, \dots, N-1\} \to \{0,1\}$. Assume we have an "oracle"
$x = x_{n-1} \cdots x_1 x_0$, $|x\rangle = |x_{n-1}\rangle \dots |x_1\rangle|x_0\rangle$ binary repres.
$|x\rangle$ —/n— [$\mathcal{U}_f$] — $|x\rangle$ (maps basis states to bas. states, $\mathcal{U}_f^2 = I$)
$|q\rangle$ —— [$\mathcal{U}_f$] — $|q \oplus f(x)\rangle$ ("oracle qubit" $q \in \{0,1\}$)
3) $|q\rangle := |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \Rightarrow |x\rangle \otimes |-\rangle \mapsto (-1)^{f(x)}|x\rangle \otimes |-\rangle$ (unchanged)
$\rightsquigarrow$ effective action of oracle: $|x\rangle$ —[$\mathcal{U}_f$]— $(-1)^{f(x)}|x\rangle$

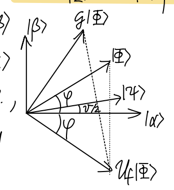
4.2 GROVER'S ALGORITHM

$N = 2^n$ elements, M solutions



1) $H|x\rangle = \frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{zx}|z\rangle \Rightarrow$ (0 or 1)
$H^{\otimes n}|x_1 \dots x_n\rangle = H|x_1\rangle \otimes \dots \otimes H|x_n\rangle = \frac{1}{\sqrt{2^n}}\sum_{z_1, \dots, z_n = 0}^{1}(-1)^{x_1z_1 + \dots + x_nz_n}|z_1 \dots z_n\rangle$
$= \frac{1}{\sqrt{2^n}}\sum_{z=0}^{2^n-1}(-1)^{x\cdot z}|z\rangle$ (bit string)
$\Rightarrow |\psi\rangle = H^{\otimes n}|0\dots0\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}|z\rangle$
2) $|x\rangle$ —/n—[G]— $=$ —[$\mathcal{U}_f$]—[$H^{\otimes n}$]—[phase gate]—[$H^{\otimes n}$]— (oracle: $|x\rangle \mapsto (-1)^{f(x)}|x\rangle$)
phase gate $= \begin{matrix} |0\rangle \mapsto |0\rangle \\ |x\rangle \mapsto -|x\rangle \end{matrix}$ $x \neq 0$ (binary) $= 2|0\rangle\langle 0| - I$
$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\psi\rangle\langle\psi| - I$
$\Rightarrow G = [(2|\psi\rangle\langle\psi| - I) \otimes I^{\otimes \ell}] \cdot \mathcal{U}_f$

Geometric interpretation
1) $|\alpha\rangle := \frac{1}{\sqrt{N-M}}\sum_{x=0,\, f(x)=0}^{N-1}|x\rangle$, $|\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x=0,\, f(x)=1}^{N-1}|x\rangle$
ϑ: $\sin(\frac{\vartheta}{2}) = \sqrt{M/N} \Rightarrow |\psi\rangle = \cos(\frac{\vartheta}{2})|\alpha\rangle + \sin(\frac{\vartheta}{2})|\beta\rangle$
2) $\mathcal{U}_f|\alpha\rangle = |\alpha\rangle$, $\mathcal{U}_f|\beta\rangle = -|\beta\rangle$
$\Rightarrow \mathcal{U}_f$ is a refl. about $|\alpha\rangle$ within subspace $\langle|\alpha\rangle, |\beta\rangle\rangle$,
$2|\psi\rangle\langle\psi| - I$ reflection about $|\psi\rangle$.



3) $\Rightarrow G$ is a rotation by ϑ in $\langle|\alpha\rangle, |\beta\rangle\rangle$
$\Rightarrow G^k|\Phi\rangle = \cos(\varphi + k\vartheta)|\alpha\rangle + \sin(\varphi + k\vartheta)|\beta\rangle$
$\stackrel{\varphi = \vartheta/2}{\Rightarrow} G^k|\psi\rangle = \cos((k+\frac{1}{2})\vartheta)|\alpha\rangle + \sin((k+\frac{1}{2})\vartheta)|\beta\rangle$.
$(k+\frac{1}{2})\vartheta \stackrel{!}{=} \frac{\pi}{2}$, $\sin(\frac{\vartheta}{2}) = \sqrt{\frac{M}{N}} \stackrel{M \ll N}{\rightsquigarrow} \vartheta \approx 2\sqrt{\frac{M}{N}}$
$\Rightarrow$ thus need $\mathcal{O}(\sqrt{N/M})$ rotations.
4) Standard meas. will coll. se to a solut.

Algebraic derivation (see above) $|\psi\rangle = \cos(\frac{\vartheta}{2})|\alpha\rangle + \sin(\frac{\vartheta}{2})|\beta\rangle$
$|\Phi\rangle = \cos\varphi|\alpha\rangle + \sin\varphi|\beta\rangle$ arbitrary
$\Rightarrow \langle\psi|\mathcal{U}_f|\Phi\rangle = \cos(\frac{\vartheta}{2} + \varphi)$ $\quad$ use $2\cos(\frac{\vartheta}{2})\cos(\frac{\vartheta}{2} + \varphi) - \cos(\varphi) = \cos(\varphi + \vartheta)$
$\Rightarrow G|\Phi\rangle = \cos(\varphi + \vartheta)|\alpha\rangle + \sin(\varphi + \vartheta)|\beta\rangle$

4.3 OPTIMALITY

Show that any quantum search alg needs $\Omega(\sqrt{N})$ oracle calles.
1) For simplicity: single solution $x \rightsquigarrow O_x = I - 2|x\rangle\langle x|$ $(= \mathcal{U}_f)$
2) State after k steps: $|\psi_k^x\rangle := \mathcal{U}_k O_x \dots \mathcal{U}_1 O_x|\psi_0\rangle$,
$|\psi_k\rangle := \mathcal{U}_k \dots \mathcal{U}_1|\psi_0\rangle$, $D_k := \sum_{x=0}^{N-1}\||\psi_k^x\rangle - |\psi_k\rangle\|^2$
3) One can show $c \cdot N \le D_k \le 4 \cdot k^2 \Rightarrow k \ge \sqrt{\frac{cN}{4}}$
If $\mathcal{O}(\log(N))$ would be possible, a QC could solve NP problems efficiently

5. THE DENSITY OPERATOR

DEF Given a quantum sys. in one of states $|\psi_i\rangle$ w.p. p_i ⇝ ensemble of states $\{p_i,|\psi_i\rangle\}$. The density operator ρ of $\{p_i,|\psi_i\rangle\}$:

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

∘ unitary operations Given $U\in\mathcal{U}(\mathbb{C})$
$|\psi_i\rangle\mapsto U|\psi_i\rangle$; $\{p_i,|\psi_i\rangle\}\mapsto\{p_i,U|\psi_i\rangle\}$
$\Rightarrow \rho \overset{U}{\mapsto}\sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger$

∘ measurements Given $\{M_m\}$ meas. operations
$p(m|i)=\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = tr[M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|]$
$\Rightarrow p(m)=\sum_i p(m|i)p_i=\sum_i p_i\, tr[M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|]$
$= tr[M_m^\dagger M_m\sum_i p_i|\psi_i\rangle\langle\psi_i|] = tr[M_m^\dagger M_m\rho]$

∘ density operator ρ_m after obtaining m:
$|\psi_i\rangle\mapsto\frac{M_m|\psi_i\rangle}{\|M_m|\psi_i\rangle\|}=:|\psi_i^m\rangle \Rightarrow$
$\rho_m=\sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\|M_m|\psi_i\rangle\|^2}$
$=\sum_i p_i\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{p(m)} = \frac{M_m\rho M_m^\dagger}{tr[M_m^\dagger M_m\rho]}$ ($=p(m|i)$)

5.2 GENERAL PROPERTIES OF ρ

THEO ρ is the density matrix assoc. to $\{p_i,|\psi_i\rangle\}$ ⟺ 1. $tr[\rho]=1$ (trace condition) 2. ρ is a pos. operator (positivity condition)
(2. ⟺ ρ is Hermitian and eigenvalues ≥0 ⟺ $\langle\varphi|\rho|\varphi\rangle\geq0\ \forall|\varphi\rangle$)

proof. "⇒": $\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i| \Rightarrow tr[\rho]=\sum_i p_i\, tr[|\psi_i\rangle\langle\psi_i|]=1$
$\rho^\dagger=\rho$ ✓, $\langle\varphi|\rho|\varphi\rangle=\sum_i p_i\langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle=\sum_i p_i|\langle\varphi|\psi_i\rangle|^2\geq0$
"⇐": ρ Hermitian, eigenvalues $\lambda_j\geq0 \Rightarrow \rho=\sum_j\lambda_j|\varphi_j\rangle\langle\varphi_j|$
$1=tr[\rho]=\sum_j\lambda_j\, tr[|\varphi_j\rangle\langle\varphi_j|]=\sum_j\lambda_j\langle\varphi_j|\varphi_j\rangle=\sum_j\lambda_j$ (ortho-norm.)
$\Rightarrow \{\lambda_j,|\varphi_j\rangle\}$ an ensemble giving rise to ρ. ■

Define a density operator as positive ρ, $tr[\rho]=1$.

"pure state" $\{1,|\psi\rangle\}$ ⇝ $\rho=|\psi\rangle\langle\psi|$ $\Rightarrow tr[\rho^2]=tr[|\psi\rangle\langle\psi|\psi\rangle\langle\psi|]=1$
"mixed state" $\{p_i,|\psi_i\rangle\}, p_i<1$; $\rho=|\psi\rangle\langle\psi|$ not possible $\Rightarrow tr[\rho^2]=\sum_i p_i^2<1$

THEO $tr[\rho^2]\leq1$ and $tr[\rho^2]=1$ ⟺ ρ pure
proof. $\{\lambda_i\}$ eigenvalues of ρ $\Rightarrow 0\leq\lambda_i\leq1$ (ρ positive, $tr\,\rho=\sum\lambda_i=1$)
$\Rightarrow tr[\rho^2]=\sum_i\lambda_i^2\leq1$. "⇐" see above, "⇒": "=1" $\Rightarrow \lambda_i=1$, $\lambda_i=0$ else ■

REM Ensemble repr. is not unique!
$\{\frac34,|0\rangle;\frac14,|1\rangle\}$, $\{\frac12,|a\rangle=\sqrt{\frac34}|0\rangle+\sqrt{\frac14}|1\rangle;\frac12,|b\rangle=\sqrt{\frac34}|0\rangle-\sqrt{\frac14}|1\rangle\}$
$\rightsquigarrow\rho=\frac34|0\rangle\langle0|+\frac14|1\rangle\langle1|=\frac12|a\rangle\langle a|+\frac12|b\rangle\langle b|$. ($\langle a|b\rangle\neq0$)

THEO $\{p_i,|\psi_i\rangle\}$, $\{q_j,|\varphi_j\rangle\}$ ensembles. Set $|\tilde\psi_i\rangle=\sqrt{p_i}|\psi_i\rangle$, $|\tilde\varphi_j\rangle=\sqrt{q_j}|\varphi_j\rangle$. If
$\rho=\sum|\tilde\psi_i\rangle\langle\tilde\psi_i|=\sum_j|\tilde\varphi_j\rangle\langle\tilde\varphi_j|$
i.e. $\{|\tilde\psi_i\rangle\}$, $\{|\tilde\varphi_j\rangle\}$ generate the same density ρ.
⟺ $|\tilde\psi_i\rangle=\sum_j u_{ij}|\tilde\varphi_j\rangle$ for (u_{ij}) unitary.

proof. "⇐": $\sum_i|\tilde\psi_i\rangle\langle\tilde\psi_i|=\sum_{ijk}u_{ij}u_{ik}^*|\tilde\varphi_j\rangle\langle\tilde\varphi_k|$
$=\sum_{jk}(\sum_i u_{ki}^\dagger u_{ij})|\tilde\varphi_j\rangle\langle\tilde\varphi_k|=\sum_{jk}\delta_{kj}|\tilde\varphi_j\rangle\langle\tilde\varphi_k|$
"⇒": Spectral decomp. $\rho=\sum_k\lambda_k|\chi_k\rangle\langle\chi_k|$.
Set $|\tilde\chi_k\rangle:=\sqrt{\lambda_k}|\chi_k\rangle$, express $|\tilde\psi_i\rangle=\sum_k v_{ik}|\tilde\chi_k\rangle$
Then $\sum_k|\tilde\chi_k\rangle\langle\tilde\chi_k|=\rho=\sum_i|\tilde\psi_i\rangle\langle\tilde\psi_i|=\sum_{k,\ell}(\sum_i v_{ik}v_{i\ell}^*)|\tilde\chi_k\rangle\langle\tilde\chi_\ell|$
$\overset{!}{=}\sum_{k\ell}\delta_{k\ell}|\tilde\chi_k\rangle\langle\tilde\chi_\ell| \Rightarrow (v_{ik})$ unitary.
Analog. $|\tilde\varphi_j\rangle=\sum_k w_{jk}|\tilde\chi_k\rangle$ for (w_{jk}) unitary
$\Rightarrow|\tilde\psi_i\rangle=\sum_k v_{ik}|\tilde\chi_k\rangle=\sum_{k,j}v_{ik}w_{jk}^*|\tilde\varphi_j\rangle=\sum_j(vw^\dagger)_{ij}|\tilde\varphi_j\rangle$ ■

5.3 THE REDUCED DENSITY OP.

DEF partial trace $M_1\in\mathbb{C}^{n_1\times n_1}$, $M_2\in\mathbb{C}^{n_2\times n_2}$
$tr_1:\mathbb{C}^{n_1n_2\times n_1n_2}\to\mathbb{C}^{n_2\times n_2}$, $M_1\otimes M_2\mapsto tr[M_1]M_2$ (tr_2 analog.)
$tr_1[\alpha M_1\otimes M_2+\beta N_1\otimes N_2]=\alpha\, tr_1[M_1\otimes M_2]+\beta\, tr_1[N_1\otimes N_2]$.

DEF reduced density operator A{ B{
Let the quantum system be described by ρ^{AB}
$\Rightarrow\rho^A:=tr_B[\rho^{AB}]$, $\rho^B:=tr_A[\rho^{AB}]$

EX 1) $|a_1\rangle,|a_2\rangle\in A$ and $|b_1\rangle,|b_2\rangle\in B$ $\Rightarrow \langle b_1|b_2\rangle\in\mathbb{C}$
$tr_B[|a_1\rangle\langle a_2|\otimes|b_1\rangle\langle b_2|]=|a_1\rangle\langle a_2|\cdot tr(|b_1\rangle\langle b_2|)$
2) ρ density for A, σ for B and suppose $\rho^{AB}=\rho\otimes\sigma$
$\Rightarrow tr_B[\rho\otimes\sigma]=\rho\, tr[\sigma]=\rho$, $tr_A[\rho\otimes\sigma]=tr[\rho]\cdot\sigma=\sigma$.
3) $|\psi\rangle=\frac{1}{\sqrt2}(|00\rangle+|11\rangle)$ ⇒
$\rho^{AB}=|\psi\rangle\langle\psi|=\frac12(|00\rangle+|11\rangle)(\langle00|+\langle11|)=\frac12(|00\rangle\langle00|+|00\rangle\langle11|$
$+|11\rangle\langle00|+|11\rangle\langle11|)=\frac12(|0\rangle\langle0|\otimes|0\rangle\langle0|+|0\rangle\langle1|\otimes|0\rangle\langle1|+|1\rangle\langle0|\otimes|1\rangle\langle0|$
$+|1\rangle\langle1|\otimes|1\rangle\langle1|)\Rightarrow\rho^A=\frac12(|0\rangle\langle0|+|1\rangle\langle1|)=\frac{I}{2}$.
Note: $|\psi\rangle$ pure, but $tr[(\rho^A)^2]=\frac14 tr[I]=\frac12<1$ ⇝ mixed

THEO (Justification for partial trace)
M observable on A $\Rightarrow M\otimes I_B$ corr. observ. on AB
$\langle M\rangle=tr[M\cdot\rho^A]\overset{!}{=}tr[(M\otimes I)\rho^{AB}]=\langle M\otimes I\rangle$
⇒ partial trace op. for computing ρ^A from ρ^{AB} is the unique op. with this property.

EX (quantum telep. application) After Alice's meas.:
$|\psi_1\rangle=|00\rangle(\alpha|0\rangle+\beta|1\rangle)$ w.p. $\frac14$, $|\psi_2\rangle=|01\rangle(\alpha|1\rangle+\beta|0\rangle)$ w.p. $\frac14$
$|\psi_3\rangle=|10\rangle(\alpha|0\rangle-\beta|1\rangle)$ w.p. $\frac14$, $|\psi_4\rangle=|11\rangle(\alpha|1\rangle-\beta|0\rangle)$ w.p. $\frac14$
⇝ ensemble $\{\frac14,|\psi_j\rangle\}_{j=1,\dots,4}\Rightarrow\rho^{AB}=\frac14\sum_{j=1}^4|\psi_j\rangle\langle\psi_j|$
$=\frac14[|00\rangle\langle00|\otimes(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle0|+\beta^*\langle1|)+|01\rangle\langle01|\otimes(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle1|+\beta^*\langle0|)+$
$|10\rangle\langle10|\otimes(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle0|-\beta^*\langle1|)+|11\rangle\langle11|\otimes(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle1|-\beta^*\langle0|)]$
$\Rightarrow\rho^B=\dots=\frac12(|0\rangle\langle0|+|1\rangle\langle1|)=\frac{I}{2}$ ← indep. of $|\psi\rangle$
Meas. by Bob cannot reveal info about $|\psi\rangle$ (encoded in α,β)

6. QUANTUM OPERATIONS

6.1 MOTIVATION & OVERVIEW

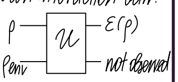
DEF quantum operations (or channels) are a (math.) generalization and unification of time evolution and measurement:
$\rho'=\mathcal{E}(\rho)$ (density matrix; quantum op.)

EX special cases 1) Unit. time evol. $\mathcal{E}(\rho)=U\rho U^\dagger$
2) Measurement with $\{M_m\}$: $p(m)=tr[M_m^\dagger M_m\rho]$,
$\rho_m=\frac{M_m\rho M_m^\dagger}{p(m)}$ ⇝ $\mathcal{E}_m(\rho)=M_m\rho M_m^\dagger$, $p(m)=tr[\mathcal{E}_m(\rho)]$
⇝ $\mathcal{E}(\rho)=\sum_m p(m)\rho_m=\sum_m\mathcal{E}_m(\rho)=\sum_m M_m\rho M_m^\dagger$ (op.-sum rep. of $\mathcal{E}$)

REM (equivalent) perspectives on quant. operations ∘ system coupled to environment (Stinespring dilation) ∘ operator-sum (Kraus) repr. ∘ physically motiv. axioms ∘ choi matrix repr.

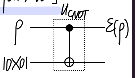
6.2 ENVIRONMENTS & Q.O.

DEF open quantum sys. is an interaction betw.
∘ principal quant. sys (ρ)
∘ environment (ρ_{env})



$U(\rho\otimes\rho_{env})U^\dagger$ ⇝ $\mathcal{E}(\rho)=tr_{env}[U(\rho\otimes\rho_{env})U^\dagger]$

EX $\rho=\begin{pmatrix}\rho_{00}&\rho_{01}\\\rho_{10}&\rho_{11}\end{pmatrix}=\rho_{00}|0\rangle\langle0|+\rho_{01}|0\rangle\langle1|+\rho_{10}|1\rangle\langle0|+\rho_{11}|1\rangle\langle1|$ ⇒



$U_{CNOT}(\rho\otimes|0\rangle\langle0|)U_{CNOT}^\dagger=\rho_{00}|00\rangle\langle00|+\rho_{01}|00\rangle\langle11|+\rho_{10}|11\rangle\langle00|+\rho_{11}|11\rangle\langle11|$
$\Rightarrow tr_{env}[\dots]=\rho_{00}|0\rangle\langle0|+\rho_{11}|1\rangle\langle1|=\begin{pmatrix}\rho_{00}&0\\0&\rho_{11}\end{pmatrix}=P_0\rho P_0+P_1\rho P_1$
with $P_0=|0\rangle\langle0|$, $P_1=|1\rangle\langle1|$.

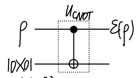
6.3 OPERATOR-SUM REPRES.

Assume w.l.o.g. $\rho_{env}=|e_0\rangle\langle e_0|$, $\{|e_k\rangle\}$ is an orthonormal basis of the env.

THEO Every env. $\mathcal{E}(\rho)$ has an oper.-sum repr.
proof. $\mathcal{E}(\rho)=tr_{env}[U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger]$
$=tr_{env}[\sum M_i\otimes N_i]=\sum M_i\, tr(N_i)$
$=\sum_i M_i\sum_k\langle e_k|N_i|e_k\rangle=\sum_k\sum_i M_i\langle e_k|N_i|e_k\rangle$
$=:\sum_k\langle e_k|\sum_i M_i\otimes N_i|e_k\rangle=\sum_k\langle e_k|U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger|e_k\rangle$
$=\sum_k E_k\rho E_k^\dagger$ with $E_k=\langle e_k|U|e_0\rangle$, $(E_k)_{\ell m}=\langle e_\ell, k|U|m,e_0\rangle$ ■

DEF The E_k's are operation elements (Kraus operators) of $\mathcal{E}$.

EX $(E_0)_{\ell m}=\langle\ell,0|U_{CNOT}|m,0\rangle$



$=\langle\ell,0|\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}|m,0\rangle=\begin{pmatrix}1&0\\0&0\end{pmatrix}=P_0$
$(E_1)_{\ell m}=\langle\ell,1|U_{CNOT}|m,0\rangle=\begin{pmatrix}0&0\\0&1\end{pmatrix}=P_1$

REM (completeness relation of Kraus op)
$\sum_k E_k^\dagger E_k=I$. Otherwise, if $\mathcal{E}$ is trace preserving $\Rightarrow 1=tr[\mathcal{E}(\rho)]=tr[(\sum_k E_k^\dagger E_k)\rho]\Rightarrow\sum_k E_k^\dagger E_k=I$
We allow $\sum_k E_k^\dagger E_k\leq I$ (⟺ $tr[\mathcal{E}(\rho)]\leq1$ e.g. meas.)
"$A\leq B$" $\Rightarrow B-A$ (Hermitian) p.s.d.

REM (phys. interpret.) as meas. performed on environment w.r.t. to $\{|e_k\rangle\}$; i.e. meas. operators $|e_k\rangle\langle e_k| \Rightarrow \rho_k\propto tr_{env}[|e_k\rangle\langle e_k|U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|]=E_k\rho E_k^\dagger$

THEO (Sys.-env. model of Kraus rep.)
$\mathcal{E}(\rho)=\sum_{k=0}^{n-1}E_k\rho E_k^\dagger$ trace-preserving ⇒
$\mathcal{E}(\rho)=tr_{env}[U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger]$ for $U|\psi\rangle|e_0\rangle=\sum_k(E_k|\psi\rangle)|e_k\rangle$
proof. Define env. as VS of dim n with orth. basis $\{|e_k\rangle\}_{k=0,\dots,n-1}$
Env. in $|e_0\rangle$ state. $U^\dagger U=I$ since
$\langle\varphi|\langle e_0|U^\dagger U|\psi\rangle|e_0\rangle=\sum_{kk'}\langle\varphi|E_k^\dagger E_{k'}|\psi\rangle\langle e_k|e_{k'}\rangle=\langle\varphi|\underbrace{\sum_k E_k^\dagger E_k}_{=I}|\varphi\rangle$
$tr_{env}[U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger]=\sum_{kk'}tr_{env}[E_k\rho E_{k'}^\dagger\otimes|e_k\rangle\langle e_{k'}|]$ ■

6.4 AXIOMATIC APPR. TO Q.O.

AXIOMS A1: $tr[\mathcal{E}(\rho)]$ is prob. that $\mathcal{E}$ occurs, thus $0\leq tr[\mathcal{E}(\rho)]\leq1$ ∀ density matr. ρ.
A2: $\mathcal{E}$ is convex-linear: $\mathcal{E}(\sum_i p_i\rho_i)=\sum_i p_i\mathcal{E}(\rho_i)$ ∀ prob. vect. p, dens. matr. ρ
A3: $\mathcal{E}$ is completely positive: $\mathcal{E}(A)$ p.s.d. ∀ p.s.d. A
Moreover, enlarging the principal sys. Q by R: $(I\otimes\mathcal{E})(A)$ must be p.s.d. ∀ p.s.d. A on RQ. (on R, on Q)

THEO $\mathcal{E}$ satisfies A1,A2,A3 ⟺ $\mathcal{E}(\rho)=\sum_k E_k\rho E_k^\dagger$ for complex $\{E_k\}$ with $\sum E_k^\dagger E_k\leq I$
proof. "⇐": A1: follows from ρ is pos, $\sum E_k^\dagger E_k\leq I$.
A2: is clear. A3: $\langle\psi|(I\otimes\mathcal{E})(A)|\psi\rangle$
$=\sum_k\langle\psi|(I\otimes E_k)A(I\otimes E_k^\dagger)|\psi\rangle\geq0$ ∀ A p.s.d.
"⇒": Denote system, which $\mathcal{E}$ acts on as Q. Let R be a system with the same dim, R{ Q{
$\{|j_Q\rangle: j=1,\dots,n\}$ orth. basis of Q
$\{|j_R\rangle: j=1,\dots,n\}$ " R; let $|\alpha\rangle:=\sum_{j=1}^n|j_R\rangle|j_Q\rangle\in RQ$
choi matrix
$\sigma:=(I\otimes\mathcal{E})(|\alpha\rangle\langle\alpha|)$ p.s.d. by A3.
For any $|\psi\rangle=\sum\psi_j|j_Q\rangle$ on Q set $|\tilde\psi\rangle:=\sum_j\psi_j^*|j_R\rangle$ on R
⇝ $\langle\tilde\psi|\sigma|\tilde\psi\rangle=\langle\tilde\psi|\sum_{ij}|i_R\rangle\langle j_R|\otimes\mathcal{E}(|i_Q\rangle\langle j_Q|)|\tilde\psi\rangle$ (on R)
$=\sum_{ij}\psi_i\psi_j^*\mathcal{E}(|i_Q\rangle\langle j_Q|)=\mathcal{E}(|\psi\rangle\langle\psi|)$
Let $\sigma=\sum|s_i\rangle\langle s_i|$. Define $E_i(|\psi\rangle)\equiv\langle\tilde\psi|s_i\rangle$ (linear)
$\Rightarrow\sum_k E_k|\psi\rangle\langle\psi|E_k^\dagger=\sum_k\langle\tilde\psi|s_k\rangle\langle s_k|\tilde\psi\rangle=\langle\tilde\psi|\sum_k|s_k\rangle\langle s_k|\tilde\psi\rangle=\mathcal{E}(|\psi\rangle\langle\psi|)$
$\overset{A2}{\rightsquigarrow}\mathcal{E}(\rho)=\sum_k E_k\rho E_k^\dagger$ ∀ density ρ
$\sum E_k E_k^\dagger\leq I$ follows from A1. ■

6.5 EXAMPLES OF Q.O.

EX 1) Bit flip channel: flips $|0\rangle\leftrightarrow|1\rangle$ w.p. $1-p\in[0,1]$
$E_0=\sqrt p\, I$, $E_1=\sqrt{1-p}\,X$ ⇝ $\mathcal{E}(\rho)=p\rho+(1-p)X\rho X$
2) Phase flip. $E_0=\sqrt p\, I$, $E_1=\sqrt{1-p}\,Z$
3) Depolarizing channel: replace ρ by completely mixed state $I/2$ w.p. p:
$\mathcal{E}(\rho)=p\cdot\frac I2+(1-p)\rho$. (uniform contraction on Bloch sphere)
4) Amplitude damping
$E_0=\begin{pmatrix}1&0\\0&\sqrt{1-\gamma}\end{pmatrix}$, $E_1=\begin{pmatrix}0&\sqrt\gamma\\0&0\end{pmatrix}$, $E_1|1\rangle=\sqrt\gamma|0\rangle$
($|1\rangle\to|0\rangle$ w. prob. γ)