Recall: Register $X$, associated CES $X$.

A quantum state is represented by a density operator.

Set of all density operators $D(X) = \{ \rho \in \text{Pos}(X) : \text{tr} \rho = 1 \}$.

Spectral decomposition: $\rho = \sum_{i=1}^{\dim(X)} p_i \cdot U_i \cdot U_i^* \quad (p_i \in \mathbb{R})$

Def: State is pure if density operator is rank 1.

Obs:

1. $D(X)$ convex
2. Extreme points of $D(X)$: $\{ UU^* : U \in X, \text{null} U = 1 \}$
3. $D(X)$ compact

To see 3, $D(X)$ is clearly bounded, so only need to show $D(X)$ closed, or equivalently, $\text{L}(X)^* \backslash D(X)$ open.

$\text{L}(X)^* \backslash D(X) = \{ A \in \text{L}(X) : A \in \text{Hermitian} \cup \{ A \in \text{L}(X) : A \in \text{Pos}(X) \}$

Each of these 3 sets are open (first principle), and so is their union.

(See LN for alt proof.)

Intuitively, $A \in \text{Hermitian}$, $A \in \text{Pos}(X)$, $\text{tr} A \neq 1$ are properties robust against small perturbations.

Def: Let $X_1, \ldots, X_n$, be registers, $\rho_i \in D(X_i)$.

Then $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n \in D(X_1 \otimes X_2 \cdots \otimes X_n)$.

It is called a "product state."
Def: $X$ register. A measurement is specified by

1. $\Gamma = \text{non-empty finite set }$ (of outcomes)

2. function $M: \Gamma \rightarrow \text{Pos}(X)$

\[ \sum_{a \in \Gamma} m(a) = 1_X \]

Each $m(a)$ is a "measurement operator" corresponding to outcome $a$.

Axiom: If state is $\rho \in D(X)$, and above measurement applied, then

1. outcome register is in state $6 = E_{a \lambda}$
2. $X$ ceases to exist (demolition meas)

Obs: All linear functions from $D(X)$ to prob vectors correspond to measurements.

Obs: We will derive non-demolition meas from demolition meas later.

Def: If $m(a)$ is a projector for each $a \in \Gamma$, $M$ is called a projector meas.

NB: Since $\sum_{a \in \Gamma} m(a) = 1_X$, the meas's project onto mutually orthogonal subspaces.

Def: If $m(a) = u_a u_{\lambda a}^*$ for an orthonormal basis $\{u_a\}$ of $X$

we say that the measurement is along the basis $\{u_a\}$. 

\[ \sum_{a \in \Gamma} m(a) = 1_X \]
Example: Holevo-Helstrom theorem.

Task: Alice picks 0, 1 with prob \( p_0, p_1 \).

If outcome is 1, prepares \( \rho_1 \) in register \( X \).

She gives \( X \) to Bob, who measures with \( j \in \{0, 1\} \).

What means maximizes \( \text{Prob}(\text{ij}) \)?

Lemma: \( M \in \text{Herm}(X), \|M\|_1 = \max \{ \text{Tr} MT : T \in \text{Herm}(X), -I_X \preceq T \leq I_X \} \)

Proof: Let \( M = \sum K \lambda_K x_K x_K^* \) be qec decompt.

\[
M^+_0 = \sum_{K, \lambda_K > 0} \lambda_K x_K x_K^*,
\]

\[
I_M^+_0 = \sum_{K, \lambda_K > 0} x_K x_K^*,
\]

Then \( M = M^+_0 - M^-_0, \|M\|_1 = \text{Tr} M^+_0 + \text{Tr} M^-_0 \).

\( \circ \) Let \( -I_X \preceq T \preceq I_X \).

Define \( T^+ \) similarly to \( H_Z \).

Then: \( T^+ \leq I, T^- \leq I \) \( (\text{omt}\ X) \)

\[
\text{Tr} MT = \text{Tr} (M^+_0 - M^-_0) (T^+_0 - T^-_0) \\
= \text{Tr} M^+_0 T^+_0 + \text{Tr} M^-_0 T^-_0 - \text{Tr} M^+_0 T^-_0 - \text{Tr} M^-_0 T^+_0 \\
\leq \text{Tr} M^+_0 \leq \text{Tr} M^-_0 \\
= \| M \|_1 \).
\]

\( \circ \) \( T = I^+_0 - I^-_0 \), all 4 ineq are equalities.

\( \therefore \text{Tr} MT = \| M \|_1 \).
Pf (HHT) Let Bob's measurement be $M_0, M_1$. ($M_0 = \text{max}$)

Let $T = M_0 - M_1$.

$\therefore \quad I = M_0 + M_1, \quad M_0 = \frac{1}{2} \left( I + T \right)$

As $0 \leq M_0 \leq I, \quad -I \leq T \leq I$.

$\text{Prob}(i \rightarrow j) = \text{Prob}(j = 0 \mid i = 0) \times p_0 + \text{Prob}(j = 1 \mid i = 1) \times p_1$

$= (\text{Tr} M_0 \rho_i) p_0 + (\text{Tr} M_1 \rho_i) p_1$

$= \frac{1}{2} \left[ \text{Tr}(I + T) \rho_0 \rho_i + \text{Tr}(I - T) \rho_1 \rho_i \right]$

$= \frac{1}{2} \left( 1 + \text{Tr}(\rho_0 \rho_0 - \rho_1 \rho_i) T \right)$

$\max_{M} \text{Prob}(i \rightarrow j) = \max_{\mathcal{M}} \frac{1}{2} \left( 1 + \text{Tr}(\rho_0 \rho_0 - \rho_1 \rho_i) T \right)$

$\text{with max} T = I_+ - I_-$

$\text{proj onto } + \text{space of } \rho_0 \rho_0 - \rho_1 \rho_1$

$M_0 = \text{proj onto } + \text{space of } \rho_0 \rho_0 - \rho_1 \rho_1$
Sec 3.2 Info complete measurem: reading $\mathfrak{c}_x$.

Sec 3.1.3 Product measurements

For $n$ registers $X_1, X_2, \ldots, X_n$, the meas

$M: \Gamma \to Pos (X_1 \otimes \cdots \otimes X_n)$

is a product meas if $\Gamma = \Gamma_1 \times \cdots \times \Gamma_n$, and $\exists$ meas

$M_i: \Gamma_i \to Pos (X_i)$

s.t.

$M(a_1, \ldots, a_n) = M_1(a_1) \otimes M_2(a_2) \otimes \cdots \otimes M_n(a_n)$ \quad \forall \alpha \in \Gamma_i, \ i = 1, \ldots, n$

NB: when we say $\exists$ meas $M_i$, we imply $\sum_{j=1}^{|\Gamma_i|} M_i(a_j) = 1 X_j$.

Q$n$: if all $M(a_1, \ldots, a_n)$ are tensor product operators, does it give a product meas?

More on this last part of course.
Sec 3.1.4 Channels

Channels transform states of one register into states of another register.

Mathematically: \( A \colon L(X) \to L(Y) \)

\[\text{s.t. } A \text{ is linear, trace-preserving, completely positive} \]

\[ \text{so that } A \otimes A \text{ maps states to states} \]

- **trace preserving**: \( \text{Tr}(A(A)) = \text{Tr}(A) \)
- **completely positive**: \( \forall CES \pi, \ A \in Pos(X \otimes Z) \)

\[ A \otimes A \in Pos(Y \otimes Z) \]

Physically, when \( A \) is applied to \( X \) in state \( \rho \)

\( X \) ceases to exist, replaced by \( Y \)

and state \( \rho \in D(X) \) is replaced by \( A(\rho) \in D(Y) \).

Returning to Sec 2.2:

\[ T(X, Y) = L(L(X), L(Y)) \quad (\star \text{note linear}) \]

\[ T(X, X) = T(X) \]

Nothing new yet: \( L(X), L(Y) \)'s are CES's.

We've learnt about linear ops in Sec 1.2.

- Ex. Addition and scalar mult. in \( T(X, Y) \)
- Ex. \( T(X, Y) \) is CES with dim...
- Ex. \( A \in T(X, Y), \ A^* \in T(Y, X) = L(L(Y), L(X)) \) defined by

\[ \forall A \in L(Y), B \in L(X), \langle A, A(B) \rangle = \langle A^*(A), B \rangle \]
The tensor product (Sec 2.2.1) of \( \varphi_i : L(X_i) \to L(Y_i) \), \( i = 1, \ldots, n \),
denoted \( \varphi_1 \otimes \varphi_2 \otimes \cdots \otimes \varphi_n \),
takes \( L(X_1 \otimes X_2 \otimes \cdots \otimes X_n) \) to \( L(Y_1 \otimes Y_2 \otimes \cdots \otimes Y_n) \),
and for all \( A_i \in L(X_i) \), \( i = 1, \ldots, n \),
\[ \varphi_1 \otimes \varphi_2 \otimes \cdots \otimes \varphi_n (A_1 \otimes A_2 \otimes \cdots \otimes A_n) = \varphi_1(A_1) \otimes \cdots \otimes \varphi_n(A_n) \]

NB \( \varphi \in \mathcal{L}(X,Y) \) are sometimes called superoperators

to distinguish them from operators.

Q. What is a super-superoperator? (As maybe...)

Important superoperators and channels:

1. Identity \( I_X : L(X) \to L(X) \) \( (I_{L(X)} = I_X) \)

\[ I_X(A) = A \]

Linear, trace preserving, completely positive.

Also called the "noiseless channel" on \( X \).

2. Transpose \( T : L(X) \to L(X) \)

\[ T(A) = A^\top \]

Linear, trace preserving, \textbf{not} completely positive.

\[ U = \sum_{i=1}^{\dim(X)} e_i \otimes e_i \quad \left( \sum_{i=1}^{\dim(X)} e_i \right) \]

\[ I \otimes T(uu^\top) \neq 0 \]

\( \triangleright \)
3. Kraus maps \( T: L(X) \to L(Y) \)

\[
T(A) = \sum_{k=1}^{\infty} \kappa_k A \kappa_k^*,
\]

st. \( \kappa_k \in L(X, Y), \sum_{k=1}^{\infty} \kappa_k^* \kappa_k = I_X \)

linear, trace preserving: \( \text{tr}(T(A)) = \sum_{k=1}^{\infty} \text{tr}(\kappa_k A \kappa_k^*) = \sum_{k=1}^{\infty} \text{tr}(\kappa_k^* \kappa_k A) = \text{tr}A \)

Complete positive: \( \forall \Xi, \forall \Phi \in \text{Pos} (X \otimes \Xi) \)

\[
(\kappa_k \otimes 1_{\Xi}) \Phi (\kappa_k \otimes 1_{\Xi})^* \in \text{Pos} (Y \otimes \Xi)
\]

Same when sum over \( k \).

4. Trace: \( \text{Tr} : L(X) \to \mathbb{C} \)

\[
A \mapsto \text{tr}A
\]

linear, trace-preserving. To see complete positivity, use an o.n basis \( \{ x_i \} \)

and \( \text{tr}(A) = \sum_{i=1}^{\dim(X)} x_i^* A x_i \) st. \( \sum_{i=1}^{\dim(X)} x_i x_i^* = I_X \) \( \text{i.e.} \) \( \text{Tr} \) is a Kraus map.

\( \text{or: Partial trace} \) is also a CP channel \( \forall Y \).

\[
\text{Tr}_X \otimes I_Y =: \text{Tr}_X
\]

Pf 1: has Kraus form \( \sum_{i=1}^{\dim(X)} (x_i^* \otimes I_Y) A (x_i \otimes I_Y) \)

Pf 2: if \( \text{Tr}_X \) CP, \( (\text{Tr}_X \otimes I_Y) \otimes I_\Xi \) preserves positivity \( \forall Y, \Xi \).
5. Measurements (Sec 6.1)

(a) Non-demolition measurements / instruments

Consider a measurement on $X$ defined by $\mu: \Gamma \rightarrow \text{Pos}(X)$

$$\sum_{a \in \Gamma} \mu(a) = I_X.$$ 

Let $M_a \in L(X, \mathbb{C})$ satisfy $M_a^* M_a = \mu(a).$

(eg, $\mathbb{E} = X$, $M_a = \mu(a)^{1/2}$: *function on normal obs*).

Consider $\Xi(A) = \sum_{a \in \Gamma} M_a A M_a^*\otimes E_a E_a^*$

in $L(\mathbb{C})$ in $C^*.$

Ex: show that $\Xi$ is linear, trace-preserving, completely-positive.

$\operatorname{Tr}_\mathbb{Z} \Xi(A) = \sum_{a \in \Gamma} (M_a \otimes E_a) A (M_a \otimes E_a)^*$

in $L(X, \mathbb{Z}\otimes C^*).$

(b) $\operatorname{Tr}_\mathbb{Z} \Xi(A) = \sum_{a \in \Gamma} \operatorname{Tr} (M_a A M_a^*) E_a E_a^*$

$$= \sum_{a \in \Gamma} \langle m_a, A \rangle E_a E_a^* = \text{meas defined by } \mu.$$

Since $\Xi$ & $\operatorname{Tr}_\mathbb{Z}$ are both $\mathbb{Q}$-channels, so is meas defined by $\mu.$

(Note linearity, $\operatorname{Tr}$-pr, cp all preserved under composition.)
(c) Partial measurements or meas one of many systems

Consider meas defined in (50), taking $X$ to $ZG$ (associated w/ $X$, $Z$, $C$).

Let $Y$ be collection of all unmeasured regis.

Let $\rho \in D(XY)$ be initial state.

Final state after measurement is:

$$\Xi \otimes I_Y (\rho) = \sum_{a \in F} (M_a \otimes I_Y) \rho (M^*_a \otimes I_Y) \otimes e_a e_a^*$$

(Sec 3.3 + Sec 6.1)

(b) Unitary channels: if $U \in U(X)$

then $\Xi(A) = UAU^+$ is a $\hat{Q}$ channel

Kraus map

(b) Mixed unitary channels if $U_k \in U(X)$, $k = 1, \ldots, r$

Sec 6.2.3 then $\Xi(A) = \sum_{k \in K} \rho_k U_k A U_k^+$ is a $\hat{Q}$ channel

$f\rho k$ prob vector.

(c) Dephasing and depolarizing channels (Sec 6.3.2)

$X \subseteq S$, $\{e_a\}_{a \in A}$ fixed o.n. basis.

Dephasing channel $\Delta(A) = \text{diag}(A)$

$$\text{ie} \ (\Delta(A))_{a,a} = A_{a,a}$$

$$\Delta(A)_{a,b} = 0 \quad \text{if } a \neq b.$$  

Depolarizing channel $\Omega(A) = \text{tr}(A) \frac{1}{\dim X}$
If $X = (C^2)^{\otimes n}$

$6_0, 6_1, 6_2, 6_3 = 1_{C^2}$ and Pauli $X,Y,Z$ operators,
$(P_3)_i = 6_3$ on $i$-th qubit, tensored with $1_{C^2}$ on other qubits

then, \( \Delta(A) = \frac{1}{2^n} \sum_{i=0}^{3} \sum_{b_i=0}^{3} \left( \bigotimes_{i=1}^{n} (P_3)_i^{b_i} \right) A \left( \bigotimes_{i=1}^{n} (P_3)_i^{b_i} \right)^* \)

Kraus maps of channels as $b_0...b_n$ ranges over all possible $n$-bit strings

\( \Omega(A) = \frac{1}{4^n} \sum_{j=0}^{3} \sum_{j=0}^{3} \left( \bigotimes_{i=1}^{n} (P_3)_i^{b_i} \right) A \left( \bigotimes_{i=1}^{n} (P_3)_i^{b_i} \right)^* \)

ranging over $4^n$ tensor products of qubit Pauli operators

If $X = C^d$, let $Z_d = \{0, 1, ..., d-1\}$, $\omega = e^{2\pi i/d}$ (principal $d$-th root of unity)

Let $X = \sum_{a \in Z_d} \omega^a e_a^* \ (X1_a) = 1_{a+1}$

$Z = \sum_{a \in Z_d} \omega^a e_a e_a^* \ (Z1_a) = \omega^a (1_a)$

Let $W_{b,c} = X^b Z^c$. The set $\{W_{b,c}\}$ for $b,c \in Z_d$
are known as discrete Weyl operators or generalized Pauli operators,
orNice error basis.
Useful facts (proof as exercise):

- $\text{Tr}(W_{b,c}) = \begin{cases} 1 & \text{if } b = c = 0 \\ 0 & \text{otherwise} \end{cases}$

- $\langle W_g, b, W_{c,f} \rangle = \text{Tr}(z^{-b} x^{-g} x^c z^f) = \text{Tr}(W_c z^{-g} z^f) = \begin{cases} 1 & \text{if } c = g \text{ and } f = b \\ 0 & \text{otherwise} \end{cases}$

- $z x = w x z$

- $\mathfrak{g}_1 \oplus \mathfrak{g}_2$ generate the group $\{ W_a W_b \}_{a,b \in \mathbb{Z}_d}$ multiplicatively.

- $\{ \frac{1}{d} W_{b,c} \}_{b,c \in \mathbb{Z}_d}$ is an orthonormal basis for $L(X)$.

Ex: Check that $\Delta(A) = \frac{1}{d} \sum_{c \in \mathbb{Z}_d} W_{0,c} A W_{0,c}^*$ (not Hermitian but unitary).

$\Omega(A) = \frac{1}{d^2} \sum_{b,c \in \mathbb{Z}_d} W_{b,c} A W_{b,c}^*$
Depolarizing channel, encryption, and teleportation

We can obtain a method to encrypt quantum states using the Kraus form for the depolarizing channel.

\[ \forall A \in L(H), \quad SL(A) = \frac{1}{d^2} \sum_{b,c} W_{b,c} A W_{b,c}^* = \frac{\mathbb{I}}{d} \]

If sender Alice and receiver Bob share secret keys \( c, d \), then: \( \forall \rho \in D(H) \)

\[ \text{Alice's encryption} \quad W_{b,c} \quad \text{output for Bob} \]

\[ \text{Bob's decryption} \quad W_{b,c}^* \]

Input to Alice

\[ \text{maybe eavesdropped} \]

Without eavesdropping \( A_{b,c} \), the encryption & decryption ops cancel one another so Bob receives the input.

Without the key, an eavesdropper sees \( \frac{1}{d^2} \sum_{b,c} W_{b,c} \rho W_{b,c}^* = \frac{\mathbb{I}}{d} \)

as the transmitted q state which is independent of the input \( \rho \).

* This is one q. generalization of the one-time-pad to the quantum setting.

It requires \( 2 \log d \) key-bits of secret.
Teleportation revisited:

*Lemma*: for the map $M: \Gamma \to \text{Pos}(X)$ applied to $X_i$, with $X_iX_j$ in the maximally entangled state in $X \otimes X$, the post-measurement state is:

$$\frac{1}{d} \sum_a |a_X a_X \rangle \otimes M(a)^T$$

Proof: assignment 1.

Def: let $|\beta_d\rangle = \frac{1}{\sqrt{d}} \sum_{a,b} |a\rangle |a\rangle$ be the MES in $C^d \otimes C^d$,

$$|\beta_d\rangle = |\beta_d\rangle \langle \beta_d| = \frac{1}{d} \sum_{a,b} |a\rangle \langle b| \otimes |a\rangle \langle b|$$

Recall also the Transpose trick: $\forall A \in L(X)$

$$A \otimes I |\beta_d\rangle = I \otimes A^T |\beta_d\rangle$$

Teleportation in detail:

Define a measurement $M: \mathbb{Z}_d \times \mathbb{Z}_d \to \text{Pos}(C^d \otimes C^d)$, $1_{\mathbb{Z}_d^2} = I$.

$$M(b,c) = (W_{b,c} \otimes I) |\beta_d\rangle \langle \beta_d| (W_{b,c}^* \otimes I)$$

To see that $\sum b,c M(b,c) = 1 \otimes I$, either note that $\{ W_{b,c} \otimes I |\beta_d\rangle \} b,c$ is an orthonormal basis.

or note that $\mathbb{E} \otimes I (\rho) = \frac{1}{d} \sum_{x, y} \text{tr}_X \rho$ for $\rho \in \mathcal{D}(X \otimes X)$.
State on $x_1 x_2 x_3$ after meas:

$$
\sum_{b, c} \langle b, c | x_1 x_2 x_3 \rangle \langle x_1 x_2 x_3 | (M(b, c) \otimes \mathbb{1}) \otimes \mathbb{1} (\rho \otimes \beta_d) = \text{tr}_{x_1 x_2} \left( \left[ (W_{b, c} \otimes \mathbb{1}) \beta_d (W_{b, c}^* \otimes \mathbb{1}) \right] \otimes \mathbb{1} \right) (\rho \otimes \beta_d).
$$

$$
\text{tr}_{x_1 x_2} \left( \beta_d (W_{b, c}^* \otimes \mathbb{1}) \otimes \mathbb{1} \right) (\mathbb{1} \otimes \beta_d)
$$

// Lemma, \text{tr}_{x_1} (\beta_d (\mathbb{1} \otimes 1)) = M_{x_2}^T

$$
\text{tr}_{x_2} \left[ (W_{b, c}^* \otimes \mathbb{1}) \otimes \mathbb{1} \right]. (\beta_d)
$$

//

$$
(W_{b, c}^* \otimes \mathbb{1})^T = W_{b, c}^*. (W_{b, c}^* \otimes \mathbb{1})
$$

Ex: prove that $\forall M, K$:

$$
\text{tr}_x (M(M \otimes \mathbb{1}) K \mathbb{1}) = \text{tr}_x K (\mathbb{1} \otimes \text{tr}_x (M(M \otimes \mathbb{1}) K \mathbb{1})).
$$

Qn: is it true that

$$
\text{tr}_x K_1 K_2 = \text{tr}_x K_2 K_1 ?
$$

1. Bob can perform $W_{b, c}$ if outcome $(b, c)$ sent do him to recover $\rho$. 