Recall: register X, associated CES $\mathcal{X}$.

A quantum state is represented by a density operator.

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

Spectral decomposition: $\rho = \sum_{i=1}^{\dim(\mathcal{X})} p(i)\, u_i u_i^*$, p: prob vector, $\{u_i\} \subseteq \mathcal{X}$

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

Obs:

① $D(\mathcal{X})$ convex

② Extreme points of $D(\mathcal{X})$: $\{uu^* : u \in \mathcal{X},\ \|u\| = 1\}$

③ $D(\mathcal{X})$ compact

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

$$L(\mathcal{X}) \setminus D(\mathcal{X}) = \{A \in L(\mathcal{X}) : A \notin \mathrm{Herm}\} \cup \{A \in L(\mathcal{X}) : A \notin \mathrm{Pos}(\mathcal{X})\} \cup \{A \in L(\mathcal{X}) : \mathrm{tr}\,A \neq 1\}$$

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

Intuitively, $A \notin \mathrm{Herm}$, $A \notin \mathrm{Pos}(\mathcal{X})$, $\mathrm{tr}A \neq 1$ are properties robust against small perturbation.

(See LN for alt proof.)

Def: Let X_i, $i=1,\dots,n$, be registers, $\rho_i \in D(\mathcal{X}_i)$.

Then $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n \in D(\mathcal{X}_1 \otimes \mathcal{X}_2 \cdots \otimes \mathcal{X}_n)$.

It is called a "product state."

<u>Def:</u> X register. A measurement is specified by

① Γ = non-empty finite set (of outcomes)

② function $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$

s.t. $\sum_{a \in \Gamma} \mu(a) = \mathbb{1}_{\mathcal{X}}$.

or POVM element, M_a

Each $\mu(a)$ is a "measurement operator" corr to outcome a.

<u>Axiom:</u> If state is $\rho \in D(X)$, and above meas applied, then

① outcome register is in state $\sigma = E_{a,a}$

with prob $p(a) = \langle \mu(a), \rho \rangle$

② X ceases to exist (demolition meas)

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

<u>Obs:</u> We will derive non-demolition meas from demolition meas later.

<u>Def:</u> If $\mu(a)$ is a projector for each $a \in \Gamma$, μ is called a projective meas

<u>NB:</u> Since $\sum_{a \in \Gamma} \mu(a) = \mathbb{1}_{\mathcal{X}}$, the $\mu(a)$'s project onto mutually orthogonal subspaces.

<u>Def:</u> If $\mu(a) = u_a u_a^*$ for an o.n basis $\{u_a\}$ of $\mathcal{X}$

we say that the measurement is <u>along</u> the basis $\{u_a\}$.

Example : Holevo-Helstrom theorem.

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

If outcome is i, prepares ρ_i in register X.

She gives X to Bob, who replies with $j \in \{0,1\}$.

What meas maximizes $\text{Prob}(i=j)$?

Lemma: $M \in \text{Herm}(X)$, $\|M\|_1 = \max\{\text{Tr}\, MT : T \in \text{Herm}(X), -\mathbb{1}_X \le T \le \mathbb{1}_X\}$

Pf: Let $M = \sum_k \lambda_k x_k x_k^*$ be spec decomp

$$M_{\substack{+\\0\\-}} = \sum_{k:\lambda_k \substack{>\\=\\<} 0} |\lambda_k| x_k x_k^*$$

$$\Pi_{\substack{+\\0\\-}} = \sum_{k:\lambda_k \substack{>\\=\\<} 0} x_k x_k^*$$

Then $M = M_+ - M_-$, $\|M\|_1 = \text{tr}\, M_+ + \text{tr}\, M_-$

(a) Let $-\mathbb{1}_X \le T \le \mathbb{1}_X$.

Define T_+, T_- similarly to $M_\pm$.

Then : $T_+ \le \mathbb{1}$, $T_- \le \mathbb{1}$ (omit X)

$$\begin{aligned}\text{Tr}\, MT &= \text{Tr}\,(M_+ - M_-)(T_+ - T_-)\\ &= \underbrace{\text{Tr}\, M_+T_+}_{\le \text{Tr}\, M_+} + \underbrace{\text{Tr}\, M_-T_-}_{\le \text{Tr}\, M_-} - \underbrace{\text{Tr}\, M_+T_-}_{\ge 0} - \underbrace{\text{Tr}\, M_-T_+}_{\ge 0}\\ &= \|M\|_1\end{aligned}$$

(b) $T = \Pi_+ - \Pi_-$, all 4 ineq are equalities

$\therefore \text{Tr}\, MT = \|M\|_1$

Pf (HHT) Let Bob's meas operators be M_0, M_1.   ($M_a = M(a)$)

Let $T = M_0 - M_1$.

$\because \; \mathbb{1} = M_0 + M_1, \; M_{\substack{0\\1}} = \frac{1}{2}(\mathbb{1}_X \pm T)$

As $0 \le M_0 \le \mathbb{1}, \quad -\mathbb{1} \le T \le \mathbb{1}$.

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

$$= (\text{tr}\, M_0 \rho_0)\, p_0 + (\text{tr}\, M_1 \rho_1)\, p_1$$

$$= \frac{1}{2}\left[\text{tr}(\mathbb{1}_X + T)\rho_0 p_0 + \text{tr}(\mathbb{1}_X - T)\rho_1 p_1\right]$$

$$= \frac{1}{2}\left(1 + \text{Tr}(\rho_0 p_0 - \rho_1 p_1) T\right)$$

$$\max_{M} \text{Prob}(i=j) = \max_{-\mathbb{1} \le T \le \mathbb{1}} \frac{1}{2}\left(1 + \text{tr}(\rho_0 p_0 - \rho_1 p_1) T\right)$$

$$= \frac{1}{2}\left(1 + \| \rho_0 p_0 - \rho_1 p_1 \|_1\right)$$

with optimal $T = \Pi_+ - \Pi_-$

proj onto $\underset{-}{+}$ espace of $\rho_0 p_0 - \rho_1 p_1$

$M_{\substack{0\\1}}$ = proj onto $\pm$ espace of $\rho_0 p_0 - \rho_1 p_1$

Sec 3.1.3 Product measurements

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

$$\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}_1 \otimes \dots \otimes \mathcal{X}_n)$$

is a <u>product</u> meas if $\Gamma = \Gamma_1 \times \dots \times \Gamma_n$, and $\exists$ meas

$$\mu_i : \Gamma_i \to \mathrm{Pos}(\mathcal{X}_i)$$

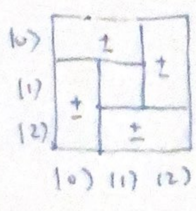
s.t. $\mu(a_1, \dots, a_n) = \mu_1(a_1) \otimes \mu_2(a_2) \otimes \dots \otimes \mu_n(a_n) \quad \forall a_i \in \Gamma_i, \; i = 1, \dots, n$

NB: when we say $\exists$ meas μ_i, we imply $\sum_{j=1}^{|\Gamma_i|} \mu_i(a_j) = \mathbb{1}_{\mathcal{X}_i}$.

Qn: If all $\mu(a_1, \dots, a_n)$ are tensor product operators,

does it give a product meas ?

cf.



More on this last part of course.

Sec 3.1.4 Channels

Q channels transform states of one register into states of another register.

Mathematically: $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$

s.t Φ is linear, $\underbrace{\text{trace-preserving, completely positive}}_{\text{so that } \mathbb{1} \otimes \Phi \text{ maps states to states}}$

- trace preserving: $Tr(\Phi(A)) = Tr(A)$
- completely positive: $\forall$ CES $\mathcal{Z}$, $A \in Pos(\mathcal{X} \otimes \mathcal{Z})$

$$\Phi \otimes \mathbb{1}_{\mathcal{Z}}(A) \in Pos(\mathcal{Y} \otimes \mathcal{Z})$$

Physically, when Φ is applied to X in state ρ

X ceases to exist, replaced by Y

and state $\rho \in D(\mathcal{X})$ is replaced by $\Phi(\rho) \in D(\mathcal{Y})$.

Returning to Sec 2.2, $T(\mathcal{X}, \mathcal{Y}) = L(L(\mathcal{X}), L(\mathcal{Y}))$ (*note linear)

$$T(\mathcal{X}, \mathcal{X}) =: T(\mathcal{X})$$

Nothing new $\boxed{\text{yet}}$: $L(\mathcal{X})$, $L(\mathcal{Y})$'s are CESs.

We've learnt about linear ops in Sec 1.2.

eg Addition and scalar mult: in $T(\mathcal{X}, \mathcal{Y})$

eg. $T(\mathcal{X}, \mathcal{Y})$ is CES with dim ....

eg. $\Phi \in T(\mathcal{X}, \mathcal{Y})$, $\Phi^* \in T(\mathcal{Y}, \mathcal{X}) = L(L(\mathcal{Y}), L(\mathcal{X}))$ defined by

$$\forall A \in L(\mathcal{Y}), B \in L(\mathcal{X}), \ \langle A, \Phi(B) \rangle = \langle \Phi^*(A), B \rangle$$

eg. Tensor product (Sec 2.2.1) of $\Phi_i : L(\mathcal{X}_i) \to L(\mathcal{Y}_i)$, $i=1,\dots,n$

denoted $\Phi_1 \otimes \Phi_2 \otimes \dots \otimes \Phi_n$

takes $L(\mathcal{X}_1 \otimes \mathcal{X}_2 \otimes \dots \otimes \mathcal{X}_n)$ to $L(\mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \dots \otimes \mathcal{Y}_n)$

s.t. $\Phi_1 \otimes \Phi_2 \otimes \dots \otimes \Phi_n (A_1 \otimes \dots \otimes A_n) = \Phi_1(A_1) \otimes \dots \otimes \Phi_n(A_n)$

for all $A_i \in L(\mathcal{X}_i)$, $i=1,\dots,n$.

NB $\Phi \in T(\mathcal{X}, \mathcal{Y})$ are sometimes called <u>super</u>operators

to distinguish them from operators.

Q. What is a super-super operator? (AL maybe...)

<u>Important superoperators and Q channels:</u>

① Identity $I_{\mathcal{X}} : L(\mathcal{X}) \to L(\mathcal{X})$ $\quad (\mathbb{1}_{L(\mathcal{X})} = I_{\mathcal{X}} = I)$

$I_{\mathcal{X}}(A) = A$

linear, trace preserving, completely positive.

Also called the "noiseless channel" on $\mathcal{X}$.

② Transpose $T : L(\mathcal{X}) \to L(\mathcal{X})$

$T(A) = A^T$

linear, trace preserving, <u>NOT</u> completely positive.

$$u = \sum_{i=1}^{\dim(\mathcal{X})} e_i \otimes e_i \qquad \left(\sum_i |i\rangle|i\rangle \right)$$

$$I \otimes T(\underbrace{uu^*}_{\geq 0}) \ngeq 0$$

③ Kraus maps $T: L(X) \to L(Y)$

$$T(A) = \sum_{k=1}^{r} A_k A A_k^*,$$

$$\text{s.t. } A_k \in L(X,Y), \quad \sum_{k=1}^{r} A_k^* A_k = \mathbb{1}_X .$$

linear, trace preserving $\because$ $tr(T(A)) = \sum_{k=1}^{r} tr(A_k A A_k^*)$

$$= \sum_{k=1}^{r} tr(A_k^* A_k A) = tr A$$

complete positive: $\forall Z, \forall B \in Pos(X \otimes Z)$

$$(A_k \otimes \mathbb{1}_Z) B (A_k \otimes \mathbb{1}_Z)^* \in Pos(Y \otimes Z)$$

Same when sum over k.

④ Trace: $Tr: L(X) \to \mathbb{C}$

$$A \mapsto tr A$$

linear, trace-preserving. To see complete positivity, use an o.n basis $\{x_i\}$ and $Tr(A) = \sum_{i=1}^{\dim(X)} x_i^* A x_i$ s.t. $\sum_{i=1}^{\dim} x_i x_i^* = \mathbb{1}_X$ $\therefore$ Tr is a Kraus map.

very Important Cor: Partial trace is also a Q channel $\forall Y$.

$$Tr_X \otimes I_Y =: Tr_X$$

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

Pf 2: if Tr_X CP, $(Tr_X \otimes I_Y) \otimes I_Z$ preserves positivity $\forall Y, Z$.

5 Measurements (Sec 6.1)

a Non-demolition measurements / instruments

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

$$\sum_{a\in\Gamma} \mu(a) = \mathbb{1}_X .$$

Let $M_a \in L(X, Z)$ satisfy $M_a^* M_a = \mu(a)$.

(eg, $Z = X$, $M_a = \mu(a)^{\frac{1}{2}}$ ← function on normal ops).

Consider $\Phi(A) = \sum_{a\in\Gamma} \underbrace{M_a A M_a^*}_{\text{in } L(Z)} \otimes \underbrace{e_a e_a^*}_{\text{in } \mathbb{C}^\Gamma}$ ← $|a\rangle\langle a|$

Ex: show that Φ is linear, trace-preserving, completely-positive.

NB $\Phi(A) = \sum_{a\in\Gamma} \underbrace{(M_a \otimes e_a)}_{\text{in } L(X, Z\otimes\mathbb{C}^\Gamma)} A \, (M_a \otimes e_a)^*$

b

$$\mathrm{Tr}_Z \, \Phi(A) = \sum_{a\in\Gamma} \mathrm{Tr}(M_a A M_a^*) \; e_a e_a^*$$

$$= \sum_{a\in\Gamma} \langle \mu_a, A\rangle \; e_a e_a^* \quad = \text{meas defined by } \mu.$$

Since Φ & Tr_Z are both Q channels, so is meas defined by μ.

(Note linearity, tr-pr, cp all preserved under composition.)

(c) Partial measurements or meas one of many systems (*) Super-important

Consider meas defined in (5)(b), taking X to $Z \otimes G$ (associated w/ X, Z, $\mathbb{C}^{\Gamma}$).

Let Y be collection of all unmeasured registers.

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

Final state after measurement is:

$$\Phi \otimes I_Y(\rho) = \sum_{a \in \Gamma} (M_a \otimes \mathbb{1}_Y)\rho(M_a^* \otimes \mathbb{1}_Y) \otimes e_a e_a^*$$

(Sec 3.3 + Sec 6.1)

(6) (a) Unitary channels : if $U \in U(X)$

then $\Phi(A) = \underbrace{UAU^{\dagger}}_{\text{Kraus map}}$ is a Q channel

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

Sec 6.2.3

then $\Phi(A) = \sum_{k=1}^{r} p_k U_k A U_k^{\dagger}$ is a Q channel

$\{p_k\}$ prob vector.

(c) Dephasing and depolarizing channels (Sec 6.3.2)

X CES, $\{e_a\}_{a=1}^{\dim(X)}$ fixed o.n. basis.

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

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

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

Depolarizing channel $\Omega(A) = (\mathrm{Tr}\, A) \dfrac{\mathbb{1}_X}{\dim X}$

- If $\mathcal{X} = (\mathbb{C}^2)^{\otimes n}$

  $\sigma_0, \sigma_1, \sigma_2, \sigma_3 = \mathbb{1}_{\mathbb{C}^2}$ and Pauli x, y, z operators,

  $(P_j)_i = \sigma_j$ on i-th qubit, tensored with $\mathbb{1}_{\mathbb{C}^2}$ on other qubits

then, $$\Delta(A) = \frac{1}{2^n} \sum_{b_1=0}^{1} \cdots \sum_{b_n=0}^{1} \underbrace{\left(\bigotimes_{i=1}^{n} (P_3)_i^{b_i} \right)} A \left(\sum_{i=1}^{n} (P_3)_i^{b_i} \right)^{\dagger}.$$

all possible tensor product of $\mathbb{1}_{\mathbb{C}^2}$ and σ_z on n qubits as $b_1 \dots b_n$ ranges over all possible n-bit strings

Kraus maps ∴ channels

$$\Omega(A) = \frac{1}{4^n} \sum_{j_1=0}^{3} \cdots \sum_{j_n=0}^{3} \underbrace{\bigotimes_{i=1}^{n} (P_{j_i})_i} A \, (P_{j_i})^{\dagger}$$

ranging over 4^n tensor products of qubit Pauli operators

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

Let $X = \sum_{a \in \mathbb{Z}_n} e_{a+1} e_a^*$ $\quad (X|a\rangle = |a+1\rangle)$,

$Z = \sum_{a \in \mathbb{Z}_n} \omega^a e_a e_a^*$ $\quad (Z|a\rangle = \omega^a |a\rangle)$.

Let $W_{b,c} = X^b Z^c$. The set $\{W_{b,c}\}$ for $b, c \in \mathbb{Z}_d$ are known as discrete Weyl operators or generalized Pauli operators, or nice error basis.

Useful facts (proof as exercise):

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

- $\langle W_{g,b}, W_{c,f}\rangle = \mathrm{Tr}(Z^{-b}X^{-g}X^{c}Z^{f}) = \mathrm{Tr}(W_{c-g,f-b}) = \begin{cases} d & \text{if } c=g \text{ and } f=b \\ 0 & \text{otherwise} \end{cases}$

- $ZX = \omega XZ$

- X, Z generate the group $\{\omega^c W_{a,b}\}_{a,b,c \in \mathbb{Z}_d}$ multiplicatively

- $\therefore$ $\left\{\frac{1}{\sqrt{d}} W_{b,c}\right\}_{b,c \in \mathbb{Z}_d}$ is an o.n basis for $L(X)$.

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

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

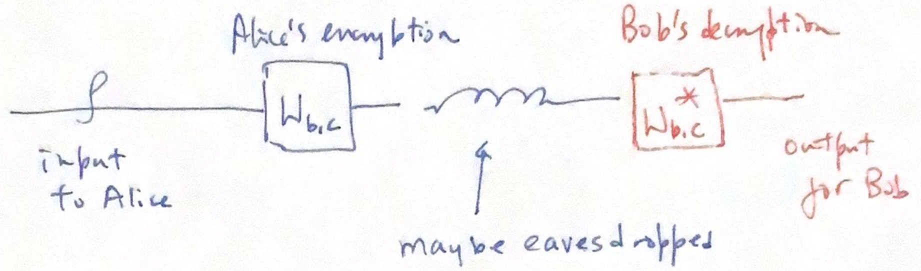
Depolarizing channel, encryption, and teleportation

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

$\because$ $\forall A \in L(X)$, $\Omega(A) = \frac{1}{d^2} \sum_{b,c} W_{b,c} A W_{b,c}^{*} = \frac{\mathbb{1}_X}{d}$

if sender Alice and receiver Bob share secret keys c, d,

then: $\forall \rho \in D(X)$



without eavesdropping $\forall b,c$, the encryption & decryption ops cancel one another so Bob receives the input.

Without the key, an eavesdropper sees $\frac{1}{d^2} \sum_{b,c} W_{b,c} \rho W_{b,c}^{*} = \frac{\mathbb{1}_X}{d}$ as the transmitted q state which is independent of the input ρ.

- This is <u>one</u> q. generalization of the one-time-pad to the quantum setting. It requires $2 \log d$ key-bits of secret.

<u>Teleportation revisited:</u>

*** Lemma:** for the meas $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$ applied to $\mathcal{X}_1$, with $\mathcal{X}_1 \mathcal{X}_2$ in the maximally entangled state in $\mathcal{X} \otimes \mathcal{X}$, the post measurement state is:

MES

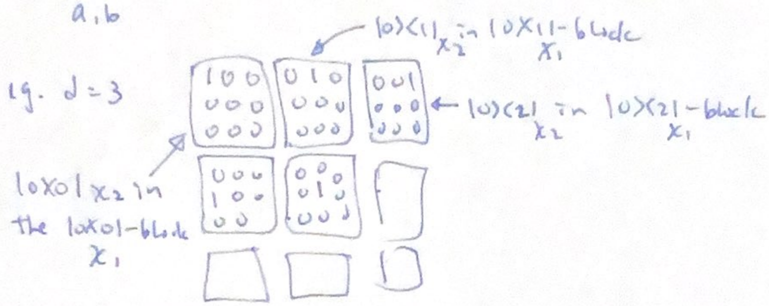
$$\frac{1}{d} \sum_a |a\rangle\langle a| \otimes \mu(a)^T$$

Proof: assignment 1.

<u>Def</u>: let $|\beta_d\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle|a\rangle$ be the MES in $\mathbb{C}^d \otimes \mathbb{C}^d$,

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

eg. $d=3$



Recall also the <u>Transpose trick</u>: $\forall A \in L(\mathcal{X})$

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

<u>Teleportation in d-dim:</u>

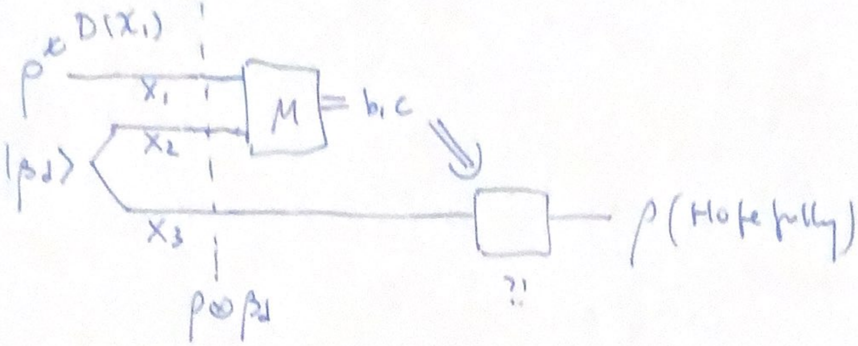
Define a measurement $\mu : \mathbb{Z}_d \times \mathbb{Z}_d \to \mathrm{Pos}(\mathbb{C}^d \otimes \mathbb{C}^d)$, $\mathbb{1}_{\mathbb{C}^d} = \mathbb{1}$.

$$\mu(b,c) = \left(W_{b,c} \otimes \mathbb{1}\right) \beta_d \left(W_{b,c}^* \otimes \mathbb{1}\right)$$

$\in \mathrm{Pos}(\mathbb{C}^d \otimes \mathbb{C}^d)$

Too see that $\sum_{b,c} \mu(b,c) = \mathbb{1} \otimes \mathbb{1}$,

- either note that $\{W_{b,c} \otimes \mathbb{1} |\beta_d\rangle\}_{b,c}$ is an on basis
- or note that $\Omega \otimes I(\rho) = \frac{\mathbb{1}_{\mathcal{X}_1}}{d} \otimes \mathrm{tr}_{\mathcal{X}_1} \rho$ for $\rho \in D(\mathcal{X}_1 \otimes \mathcal{X}_2)$.



• State on $X_1 X_2 X_3$ after meas:

$$\sum_{b,c} |b,c\rangle\langle b,c| \otimes \underbrace{\mathrm{tr}_{X_1 X_2} \big(M(b,c) \otimes \mathbb{1}\big)(\rho \otimes \beta_d)} = \mathrm{tr}_{X_1 X_2} \big(\sqrt{M(b,c)} \otimes \mathbb{1}\big)(\rho\otimes\beta_d)\big(\sqrt{M(b,c)}\otimes\mathbb{1}\big)$$

$$\|$$

$$\mathrm{tr}_{X_1X_2}\Big(\big[(W_{b,c}\otimes \mathbb{1})\beta_d(W_{b,c}^*\otimes\mathbb{1})\big]\otimes\mathbb{1}\Big)(\rho\otimes\beta_d)$$

$$\|$$

$$\mathrm{tr}_{X_1X_2}\Big(\beta_d(W_{b,c}^*\,\rho\, W_{b,c})\otimes\mathbb{1}\otimes\mathbb{1}\Big)(\mathbb{1}\otimes\beta_d)$$

$\|$ Lemma, $\mathrm{tr}_{X_1}\big(\beta_d(M\otimes\mathbb{1})\big) = M^T_{X_2}$

$$\mathrm{tr}_{X_2}\Big[\big(W_{b,c}^*\,\rho\, W_{b,c}\big)^T\otimes\mathbb{1}\Big]\cdot(\beta_d)$$

$$\|$$

$$\big(W_{b,c}^*\,\rho\, W_{b,c}\big)^{TT} = W_{b,c}^*\,\rho\, W_{b,c}.$$

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

$$\mathrm{tr}_X (\underset{L(X)}{\underset{\Uparrow}{M}} \otimes \underset{L(Y)}{\underset{\Uparrow}{\mathbb{1}}})\underset{L(X\otimes Y)}{\underset{\Uparrow}{K}} = \mathrm{tr}_X K(\mathbb{1}\otimes M)$$

Qn: is it true that

$\mathrm{tr}_X K_1 K_2 = \mathrm{tr}_X K_2 K_1$?

∴ Bob can perform $W_{b,c}$ if outcome (b,c) sent to him to recover ρ.