Last time. lec 15.

LSD thm:

$$Q(N) = \sup_n Q^n(N)$$

$$= \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA_1\ldots A_n}} I(R\rangle B_1 \ldots B_n)_{I\otimes N^{\otimes n}(|\psi\rangle\langle\psi|)}$$

- Converse ✓
- Decoupling lemma ✓

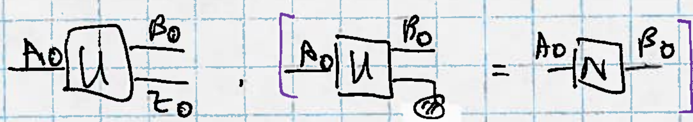
Direct coding:

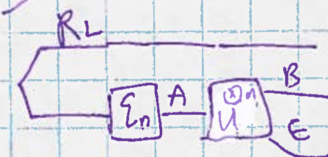
- Suffices to show $Q^{(1)}(N)$ achievable $\forall N$

$$\left[\because\ Q^{(m)}(N) = \frac{1}{m} Q^{(1)}(N^{\otimes m})\right]$$

- for any $|\psi\rangle_{R_0 A_0}$ isometric extension, unitary rep, Stinespring's dilation — need symbols for the 1-shot concepts.

let $|\alpha\rangle = I_{R_0} \otimes U(|\psi\rangle)$





Take $A = A_1 \dots A_n$, $B = B_1 \dots B_n$, $E = E_1 \dots E_n$

- Consider random set of (M, n) codes
- Show average over these codes gives

$$\mathbb{E}_{\text{codes}} \left\| \rho_{R_L E} - \frac{I}{M_{R_L}} \otimes \rho_E \right\|_1 \longrightarrow 0$$

if $\frac{1}{n} \log M < I_c(R_0 \rangle B_0)_{|\alpha\rangle\langle\alpha|}$

- $\therefore$ $\exists$ code achieving decoupling at the desired rate.

$r = I_c(R_0 \rangle B)_\alpha$.

- By approx decoupling, $\exists$ code achieving def (2a). $\therefore$ $\exists$ code achieving same rate for all defs.

[Analogous to ave $\Rightarrow$ worst case error]

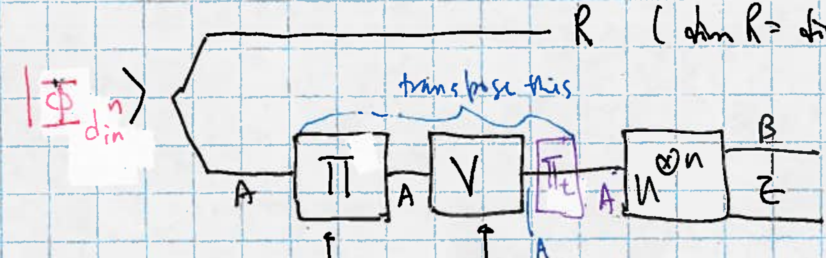
- $\because$ true $\forall\, |\psi\rangle$ we can max over $|\psi\rangle$

☆: Want to show decoupling condition on:

Actual code ↗ ↳ random isometry from M to $2^{nS(R)}$ dim subspace in d_{in}^n dims

^ a special — with projector Π_t

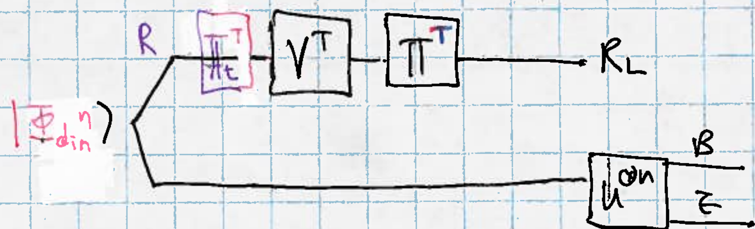
||



× normalization

↑ on M dims ↑ random unitary ∴ $-\boxed{\Pi}-\boxed{V}- = -\boxed{\Pi_S}-$ projection on random subspace

|| transpose trick.



× normalization

Claim: $\left[\int dV \; \| \rho_{R_L E} - \frac{I}{M} \otimes \rho_E \|_1 \right]^2 \leq (\dim R_L E)\, \mathrm{Tr}(\rho_B)^2$

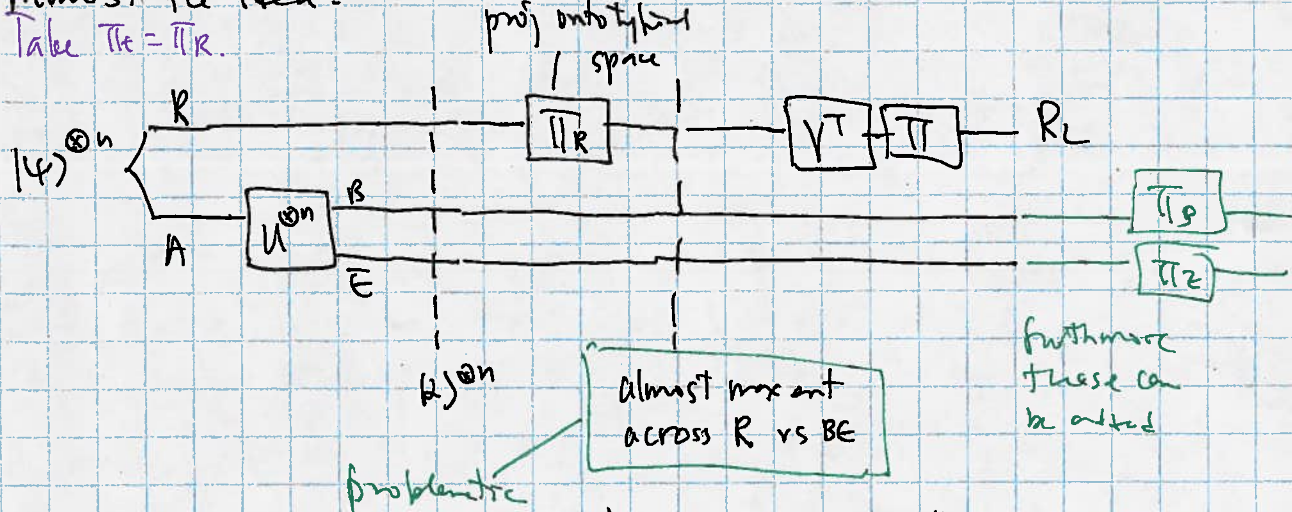
Haar meas

Pf: See preskill notes Ph/CS 219 Mar 7, 2011 Appendix A.

To bound RHS of "claim"

Almost the idea:

Take $\Pi_E = \Pi_R$.



∴ back to previous diagram

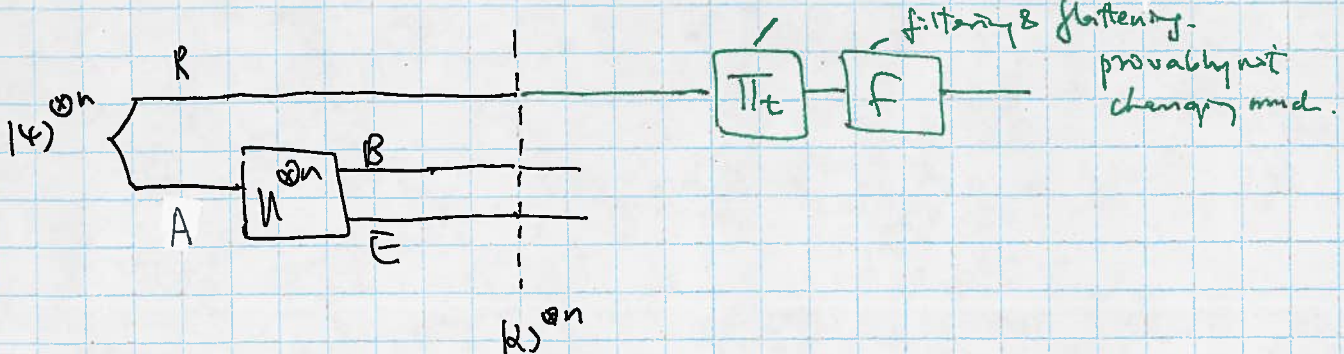
Then $\dim R_L E \leq M \cdot 2^{n S(E_0)_\sigma}$

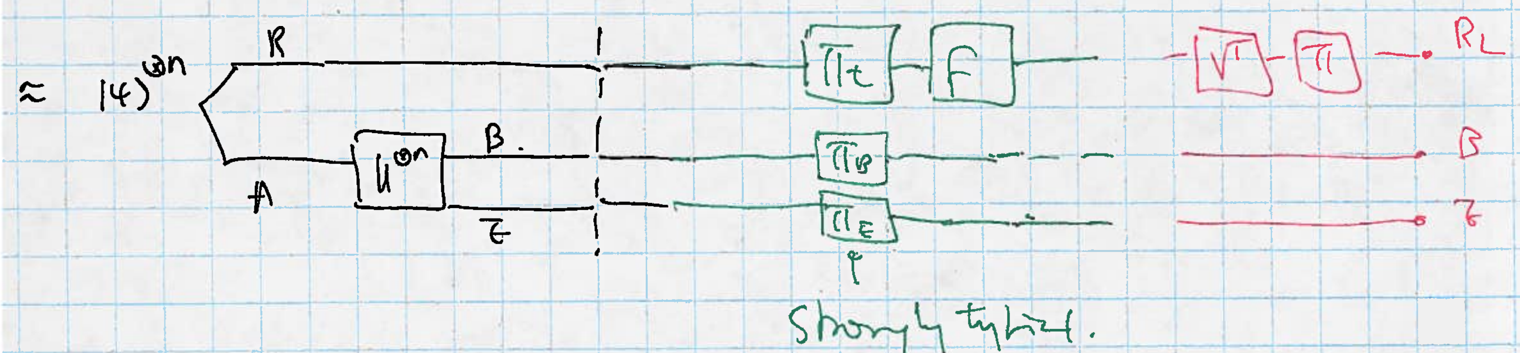
$\mathrm{Tr}(\rho_B)^2 \approx 2^{-n S(B_0)_\sigma}$ $\quad\left(\mathrm{tr}\left(\frac{I}{d}\right)^2 = \frac{1}{d}\right)$

∴ If $M \approx 2^{n\left[I_c(R_0 \rangle B_0)_\sigma - \delta\right]}$

then $M \cdot \dim E \cdot \mathrm{Tr}(\rho_B)^2 \to 0$

Bound of "RHS of claim" in 0702005 :





So we can add $-\boxed{\sqrt{T}}-\boxed{\Pi}-$ to R above and bound RHS of claim using the above state instead.

Result similar to "almost" argument.

NB: There are $\binom{n+\dim R_0 -1}{\dim R_0 -1} \leq (n+1)^{[\dim R_0]}$ type classes here.

Each of the high prob ones has size $\approx 2^{n[S(R) - \text{small term}]}$.

NB If $\rho_{R_0} = \sum_i \lambda_i |e_i\rangle\langle e_i|$, each type class is spanned by

$|e_{i_1}\rangle|e_{i_2}\rangle \cdots |e_{i_n}\rangle$

where $|e_1\rangle$ appears a specific n_1 times,
$|e_2\rangle$ " " " n_2 - - -, etc.

Method of types: [0606225]

$x^n = x_1 x_2 \ldots x_n \in \mathcal{X}^n$

t^{x^n} = empirical dist^n in $\mathcal{X}^n$

$T_t^n = \{x^n \in \mathcal{X}^n : t^{x^n} = t\}$ = sequences of the same type.

defined w/o dist^n.

Given dist^n p on $\mathcal{X}$, $\epsilon > 0$

- let $\tau_\epsilon = \{t : \|t - p\|_\infty \le \epsilon\}$

- $T_{p,\epsilon}^n = \bigcup_{t \in \tau_\epsilon} T_t^n = \{x^n : \|t^{x^n} - p\|_\infty \le \epsilon\}$

strongly typical set

- $p^n = p$ iid n times

- AEP: ① $p^n(T_{p,\epsilon}^n) \geq 1-\delta$

② $\forall x^n \in T_{p,\epsilon}^n$, $p^n(x^n) \in [2^{-n[H(p)+c\epsilon]}, 2^{-n[H(p)-c\epsilon]}]$

③ $(1-\delta)^{-1} 2^{n[H(p)-c\epsilon]} \le |T_{p,\epsilon}^n| \le 2^{n[H(p)+c\epsilon]}$ (c = const)

④ $\forall t \in \tau_\epsilon$, $|T_t^n| \geq 2^{n[H(p) - \tilde{c}(\epsilon)]}$ where $\tilde{c}(\epsilon) \to 0$ as $\epsilon \to 0$.

NB ①–③ only require weak typicality.

Quantum setting:

- $\rho = \sum_{x \in \mathcal{X}} p_x \, |x\rangle\langle x|$.

- $\Pi_t^n = \sum_{x^n \in T_t^n} |x^n\rangle\langle x^n|$

Given ρ:

- $\Pi_{\rho,\epsilon}^n = \sum_{t \in T_\epsilon} \Pi_t^n = \sum_{x^n \in T_{\rho,\epsilon}^n} |x^n\rangle\langle x^n|$. typical subspace

- QAEP: ① $\operatorname{Tr} \rho^{\otimes n} \Pi_{\rho,\epsilon}^n \geq 1-\delta$

  ② $\Pi_{\rho,\epsilon}^n \rho^{\otimes n} \Pi_{\rho,\epsilon}^n \in \left[2^{-n[S(\rho)+c\epsilon]}, 2^{-n[S(\rho)-c\epsilon]} \right] \cdot \Pi_{\rho,\epsilon}^n$

  ③ $(1-\delta)^{-1} 2^{n[S(\rho)-c\epsilon]} \leq \operatorname{Tr} \Pi_{\rho,\epsilon}^n \leq 2^{n[S(\rho)+c\epsilon]}$

  ④ $\operatorname{Tr} \Pi_t^n \geq 2^{n[S(\rho)-\tilde{c}(\epsilon)]}$

- Again ①-③ require only weak typicality.

Reminder:

From this random code for producing approx $E(M)$,

we can ① get code with small worse case fidelity

- by removing $|\psi\rangle$ in logical space with worst fidelity
- repeat on the orthogonal complement of $|\psi\rangle$ in logical space until half of the original M dims are left.

② the same code transmits arbitrary entangled state well via the Barnum-Knill-Nielsen argument.

Variations of codes & proofs:

Let $\rho = \sum_x p_x |\phi_x\rangle\langle\phi_x| = \mathrm{tr}_R |\psi\rangle\langle\psi|$

Let $x^n = x_1 \ldots x_n$ be a strongly typical sequence, $|\phi_{x^n}\rangle = |\phi_{x_1}\rangle |\phi_{x_2}\rangle \ldots |\phi_{x_n}\rangle$.

Code:	Who.	How
① Random $2^{n I_c(R\rangle B)_{I\otimes N(|\psi\rangle\langle\psi|)}}$-dim subspace of typical space of $\rho^{\otimes n}$ in $A = A_1 \ldots A_n$.	Hayden Horodecki Yard Winter 0702005.	R & E in $\approx$ product state
* Can take random stabilizer space		
② Generalized CSS code $\|k\rangle \to \sum_{m=1}^{M} e^{i\theta_{km}} \|\phi_{x^n}\rangle$ ($km \to x^n$ random code). θ_{km}: special; $M = 2^{n\chi(\{p_x, \rho_x\})}$	Devetak 0304127.	① $\|k\rangle$ can be decoded by Bob ② Env knows little about $\|k\rangle$.
③ $\|k\rangle \to \sum_{i=1}^{2^{nS(R)}} \sqrt{p_{x^n}}\, e^{i\phi_i} \|\phi_{x^n}\rangle$, ϕ_i: random, $x^n \leftarrow i$ random code	Horodecki, Lloyd, Winter 0702006	
④ $\|k\rangle \to \sum_{i=1}^{2^{nS(R)}} g_i\, e^{i\phi_i} \|\phi_{x^n}\rangle$. g_i: gaussians.	Shor 02	Direct proof for QECC criterion for typical Kraus Terms.

$I_c(R>B)$ if part of B is classical:

If $\rho_{RB} = \sum_i p_i \, \rho^{(i)}_{RB_1} \otimes |i\rangle\langle i|_{B_2}$ $\quad (B = B_1 B_2)$

then $I_c(R>B)_\rho = \sum_i p_i \, I_c(R>B_1)_{\rho^{(i)}_{RB_1}}$

Pf: $\rho_B = \sum_i p_i \, \mathrm{tr}_R \, \rho^{(i)}_{RB_1} \otimes |i\rangle\langle i|_{B_2}$

$$S(RB)_\rho = H(p) + \sum_i p_i \, S(RB_1)_{\rho^{(i)}_{RB_1}}$$

$$S(B)_{\rho_B} = H(p) + \sum_i p_i \, S(B_1)_{\mathrm{tr}_R \rho^{(i)}_{RB_1}}$$

$$\therefore I_c(R>B)_\rho = -S(RB)_\rho + S(B)_{\rho_B}$$

$$= \sum_i p_i \left[-S(RB_1)_{\rho^{(i)}_{RB_1}} + S(B_1)_{\mathrm{tr}_R \rho^{(i)}_{RB_1}} \right]$$

$$= \sum_i p_i \, I_c(R>B)_{\rho^{(i)}_{RB_1}}$$

eg Binary erasure channel

$N_p(\rho) = (1-p)\,\rho + p\,|2\rangle\langle 2|$ where $|2\rangle$ ortho to the input space

$\underset{\uparrow}{=} (1-p)\,\rho \otimes |0\rangle\langle 0| + p\,|2\rangle\langle 2| \otimes |1\rangle\langle 1|$. (on $B_1 B_2$)

locally equivalent to

whether there is an error or not.

For any $|\psi\rangle_{RA}$: (let $\psi_R = \mathrm{tr}_A |\psi\rangle\langle\psi|$)

$\underset{R}{I} \otimes N(\,|\psi\rangle\langle\psi|_{RA})$

$= (1-p)\ \underset{RB_1}{|\psi\rangle\langle\psi|} \otimes \underset{B_2}{|0\rangle\langle 0|} + p\ \psi_R \otimes \underset{B_1}{|2\rangle\langle 2|} \otimes \underset{B_2}{|1\rangle\langle 1|}$

$I_c(R\rangle B) = (1-p)\ I_c(R\rangle B_1)_{|\psi\rangle_{RB_1}} + p\ I_c(R\rangle B_1)_{\psi_R \otimes |2\rangle\langle 2|_{B_1}}$

$= (1-p)\ S\left(\mathrm{tr}_{B_1} |\psi\rangle\langle\psi|_{RB_1}\right) + p \cdot (-S(\psi_R))$

$= (1-2p)\ S(\psi_R)$

If $p \le \frac{1}{2}$, optimal $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{RA}$

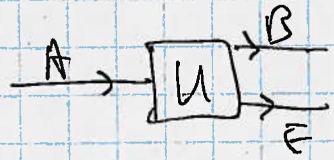
If $p > \frac{1}{2}$, optimal $|\psi\rangle = |0\rangle|0\rangle_{RA}$

$\therefore\ Q^{(1)}(N_p) = \max\limits_{|\psi\rangle_{RA}} \ I_c(R\rangle B)_{I\otimes N(|\psi\rangle\langle\psi|)} = \max(1-2p,\ 0)$.

Note $Q^{(1)}(N_p)$ cts in p, but not optimal $|\psi\rangle$. What about $Q^n(N_p)$?

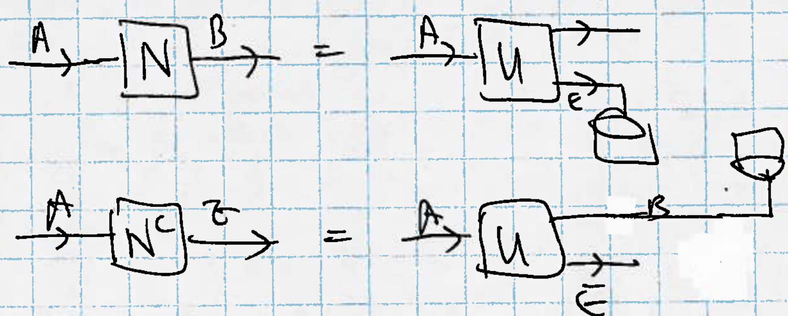
Complementary Channel:

Let N be a channel, and U its isometric extension.



The complementary channel N^c is given by:

$$N^c(\rho) = \mathrm{tr}_B\,(U \rho U^{+})$$

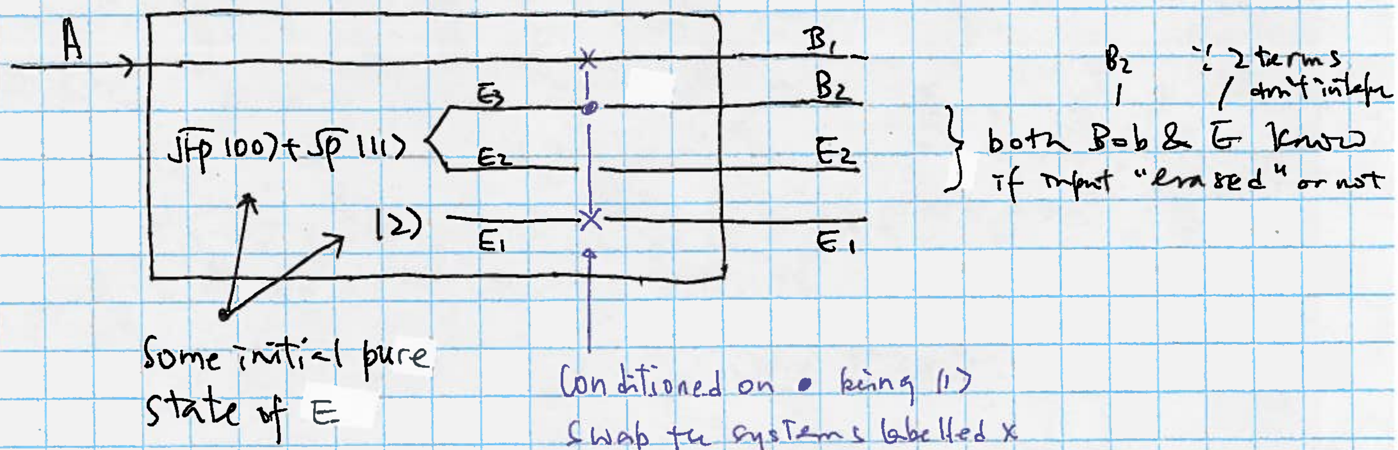


Both U & N_c determined up to a unitary on E.

$(N^c)^c = N$ up to a unitary on B.

eg. $\mathcal{N}_p(\rho) = (1-p)\, \underset{B_1}{\rho} \otimes \underset{B_2}{|0\rangle\langle 0|} + p\, \underset{B_1}{|2\rangle\langle 2|} \otimes \underset{B_2}{|1\rangle\langle 1|}$

Consider this isometric extension:



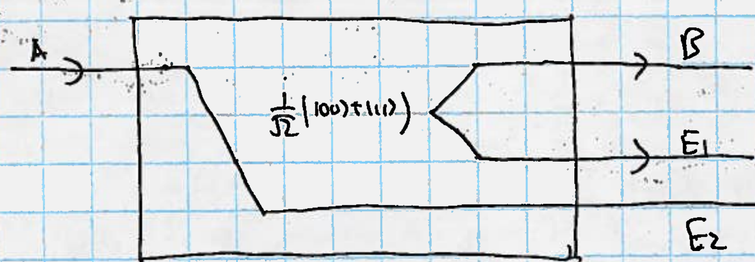
∴ Erasure channel splits the input between B & E

$\mathcal{N}_p^c = \mathcal{N}_{1-p}$!

eg 2: If $N(\rho) = \frac{I}{2}$ (complete randomization map)

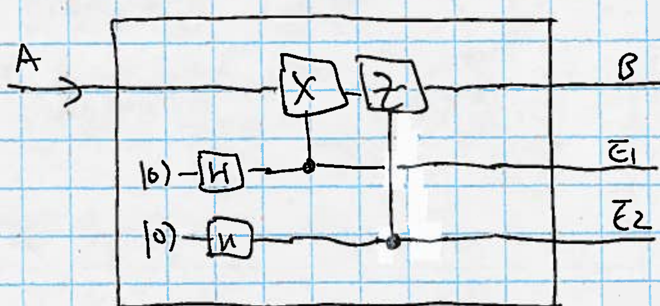
then $N^c(\rho) = \rho$ (identity channel)

Pf: A particularly useful isometric extension for N:

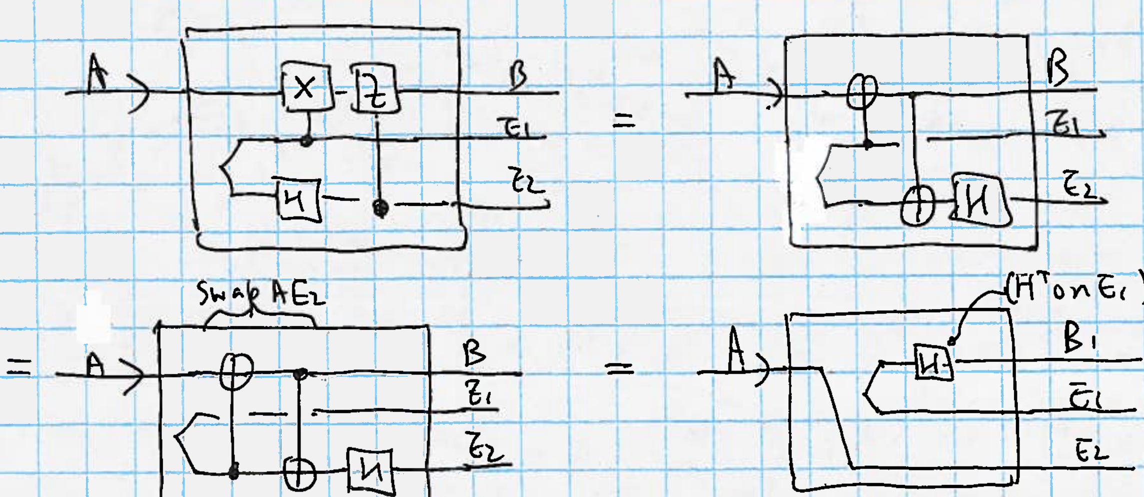


Aside: $N(\rho) = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z)$

Another isometric extension is



You can derive the 1st extension using the 2nd:



A useful digression

0605009 Kretschmann, Schlingemann, (RI Werner

(1) Continuity of Stinespring's dilations (Thm 1).

For any 2 channels N_1, N_2:

$$\inf_{U_1, U_2} \| U_1 - U_2 \|_\infty^2 \le \| N_1 - N_2 \|_\diamond \le 2 \inf_{U_1, U_2} \| U_1 - U_2 \|_\infty$$

Where the inf is taken over the dilations U_1, U_2 of N_1, N_2.

? or min

identity completely randomizing channel.

(2) Approx complementary relation between I & R (Thm 3)

$$\forall N. \quad \frac{1}{4} \inf_D \| D \circ N - I \|_\diamond^2 \le \| N^c - R \|_\diamond \le 2 \inf_D \| D \circ N - I \|_\diamond^{\frac{1}{2}}$$

where the inf is taken over decoding maps from dout to din dims.