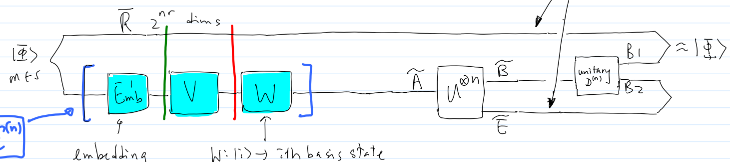
Lec 11, Jun 10, 2010

Note Title 09/06/2010

Last time: proved LSD theorem

Direct coding for sharing MES between $\bar{R}$ & B_1:

decoupled if $r < I_c(R\rangle B)_\alpha$



embedding 2^{nr} dim in $2^{n(S(R)_\alpha+\epsilon)}$

$W: |i\rangle \to$ ith basis state of ϵ-typical space of $\alpha_R^{\otimes n}$.
ie W^{-1} compresses $\alpha_R^{\otimes n}$.
Embeds $2^{nS(R)}$ dims in d_A^n.

Note correction

$\tilde{X} = X^{\otimes n}$ for $X = R, A, B, E$

Encodes the 2^{nr} logical space in a subspace (defined by V) of typical space of $\alpha_R^{\otimes n}$.

We can obtain a code for transmitting arbitrary quantum state with small worse case error:

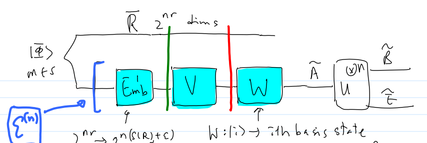
* { Find the vector $|v\rangle$ in the logical space with worse fidelity.
  Restrict to space orthogonal to $|v\rangle$.

Repeat *, and remove half of the dims.

Remaining space has large worse-case-fidelity.

(See 0311037 Prop 4.5)

Other codes & proofs:



$2^{nr} \to 2^{n(S(R)_\alpha+\epsilon)}$

$W: |i\rangle \to$ ith basis state of ϵ-typical space of $\alpha_R^{\otimes n}$.

Code specification (V)	Sufficient condition	Who
① V randomly unitary / Clifford group gate	$\bar{R}\,\tilde{E} \simeq$ product state in trace distance	0702005 Hayden Horodecki Yard Winter
② V takes $\lvert k\rangle$ to $\sum_{m=1}^{M} e^{i\theta_{km}} \lvert s_{km}\rangle$ (special; random $nS(R)_\alpha$-bit string), $M = 2^{n\chi(\{p_x, \rho_{xE}\})}$ (channel output to Eve)	Coherent version of private classical message code. Bob can decode $\lvert km\rangle$ from $\tilde{B}$. Eve's state (labeled by k) approx const (in trace distance)	0304127 Devetak; ① ② ③: transmit MES
③ V takes $\lvert k\rangle$ to $\sum_{i=1}^{2^{nS(R)}} \sqrt{q_i}\, e^{i\phi_i} \lvert i\rangle$ (q_i: prob of ith basis state in ϵ-typical space of $\alpha_R^{\otimes n}$; ϕ_i uniform)	Show Bob can decode $\lvert k\rangle$ & Eve's state close to const on average	0702006 Horodecki Lloyd, Winter; if $\lvert k\rangle$ not orthogonal ~~take~~ their span as code space .....
④ V takes $\lvert k\rangle$ to $\sum_{i=1}^{2^{nS(R)}} g_i e^{i\phi_i} \lvert i\rangle$ (g_i gaussian var)	Show for typical set of Kraus ops of N, QECC criterion holds	Shor

eg 1 N: binary erasure channel: $N(\rho) = (1-p)\rho + p\,|2\rangle\langle 2|$

Consider any $|\psi\rangle_{RA}$.

$$I_R \otimes N_{A\to B}(|\psi\rangle\langle\psi|) = (1-p)|\psi\rangle\langle\psi|_{RB} + p\, \mathrm{tr}_A(|\psi\rangle\langle\psi|) \otimes |2\rangle\langle 2|_B$$

(orthogonal)

$$\begin{aligned} I_c(R\rangle B) &= S(B) - S(RB) \\ &= H(p) + (1-p)\, S(\mathrm{tr}_R|\psi\rangle\langle\psi|) \\ &\quad - [H(p) + p\, S(\mathrm{tr}_A|\psi\rangle\langle\psi|)] \\ &= (1-2p)\, S(\mathrm{tr}_A|\psi\rangle\langle\psi|). \end{aligned}$$

$$I_c(R\rangle B) = (1-2p)\, S(\mathrm{tr}_A|\psi\rangle\langle\psi|)$$

If $p < \frac{1}{2}$, we maximize $S(\mathrm{tr}_A|\psi\rangle\langle\psi|) = 1$ with max ent $|\psi\rangle$.

$\therefore Q^{(1)}(N) = (1-2p)$

How does the achieving quantum code look like?

$\alpha_R = \frac{I}{2}$, so typical space is entire input space.

① • Take a random subspace of $2^{n(1-2p)}$ dims OR
• take the span $2^{n(1-2p)}$ vectors, each is an equal superposition of basis vectors with random phases

② Remove states with low fidelity.

$$I_c(R\rangle B) = (1-2p)\, S(\mathrm{tr}_A|\psi\rangle\langle\psi|)$$

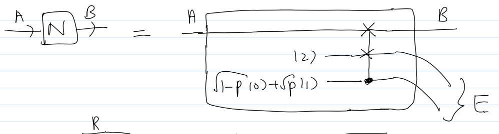
If $p \geq \frac{1}{2}$, we minimize $S(\mathrm{tr}_A|\psi\rangle\langle\psi|) = 0$ with $|\psi\rangle_{RA} = |\psi_1\rangle_R |\psi_2\rangle_A$

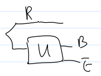
$\therefore Q^{(1)}(N) = 0$. Shouldn't bother sending anything.

Together, $Q^{(1)}(N) = \max(1-2p, 0)$.

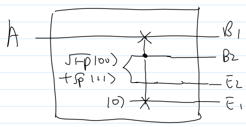
Note the discontinuity in the optimal $|\psi\rangle_{RA}$.

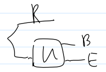
Useful to think about the Stinespring dilation of the erasure channel.



$|\alpha\rangle =$  $= |\psi\rangle_{RB}|2\rangle_E \sqrt{1-p}|0\rangle + |\psi\rangle_{RE}|2\rangle_B \sqrt{p}|1\rangle$

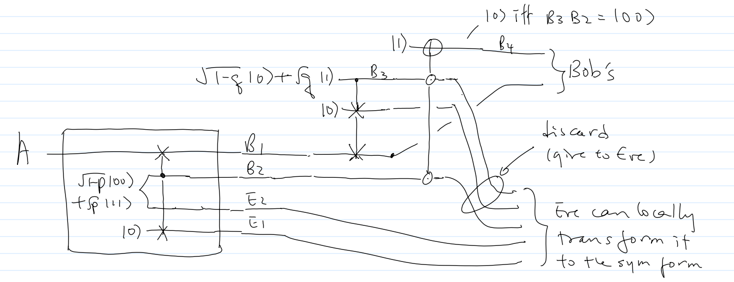
or equivalently:



$|\alpha\rangle =$  $= \sqrt{1-p}\,|00\rangle_{B_2E_2}|\psi\rangle_{RB_1}|0\rangle_{E_1} + \sqrt{p}\,|11\rangle_{B_2E_2}|\psi\rangle_{RE_1}|0\rangle_{B_1}$

- Erasure channel "splits" the input between B & E.

- By "discarding" B, with some probability, Bob can obtain the output of an erasure channel with higher probability of erasure.



The above is an erasure channel with erasure prob

$= 1-(1-p)(1-q) = p+q-pq \geq p.$

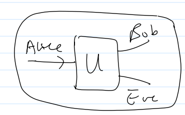
- If $p < \frac{1}{2}$, Bob can choose $p+q-pq = 1-p$ ($q = \frac{1-2p}{1-p}$) then he will end up having Eve's output from the origin erasure channel.
- Likewise if $p \geq \frac{1}{2}$, Eve can locally process her state and get what Bob has.
- If $p \geq \frac{1}{2}$, not only $Q(N)=0$, one cannot even send a qubit with arbitrarily many uses of the channel. If so, Bob decodes the input qubit but so does Eve, thus cloning it!

Complementary Channel:

Let N be a channel, U be its Stinespring dilation

The complementary channel N^c is given by

$N^c(\rho) = \mathrm{Tr}_B(U\rho U^\dagger)$



ie N^c: channel from Alice to Eve.

Given N, N^c determined up to a unitary.

eg1. If N erasure channel w/ prob erasure p

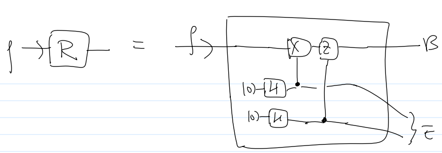
N^c … … 1−p

eg2. If N = completely randomization map

N^c = identity channel.

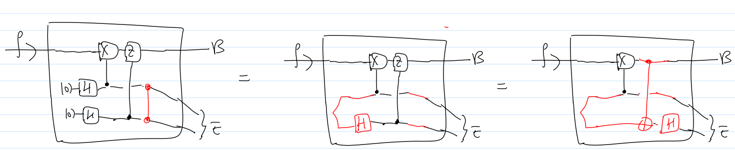
NB. $(N^c)^c = N$.

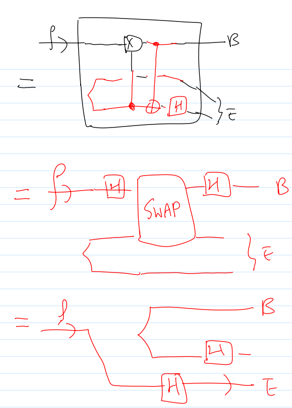
Checking:



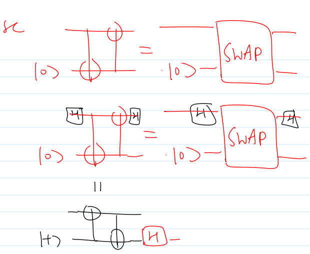
If Eve measures (ie perform a CNOT from her states to Frank's |0> states), she knows "what Pauli" has occured to \rho. That corresponds to having the classical communication share of teleportation, while Bob has the encrypted state. They each hold a share of the secret, neither has any info but together they recover the secret -- it is a (2,2) threshold scheme.

But she can do much better!

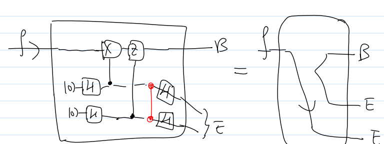




Because



So



a stinespring dilation for R!

A useful digression: 0605009 (Kretschmann, Schlingemann, Werner)

① Continuity of stinespring's dilations (U_i = dilation of N_i):

(Thm 1)

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

② Approx complementarity relation between I & R ← completely randomizing map
(Thm 3) $\quad$ ↑ identity channel

$$\frac{1}{4}\inf_{\mathcal{D}} \|\mathcal{D}\circ N - I\|_\diamond^2 \le \|N^c - R\|_\diamond \le 2\inf_{\mathcal{D}}\|\mathcal{D}\circ N - I\|_\diamond^{\frac{1}{2}}$$

Degradable & antidegradable channels:

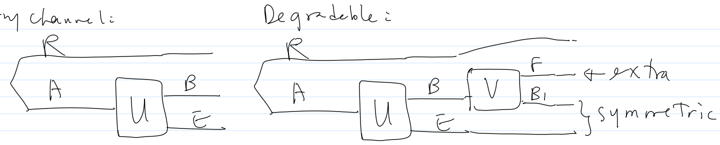
- N is degradable if $\exists\, \mathcal{D}$ (a TCP map) s.t. $\mathcal{D}\circ N = N^c$.
  ie Bob can apply $\mathcal{D}$ (the degrading map) to his output and obtain Eve's output. Since E & B purify one another Eve now gets what Bob originally has ie $(\mathcal{D}\circ N)^c = (N^c)^c = N$.

  Intuitively, for a degradable channel, "Bob is better than Eve."

  eg. We've seen that erasure channel with $p \le \frac{1}{2}$ is degradable
- N is antidegradable if N^c is degradable.
  ie $\exists\, \mathcal{E}$ s.t. $\mathcal{E}\circ N^c = N$.
  Here Eve is better than Bob. $\quad$ eg. Erasure channel w/ $p \ge \frac{1}{2}$.

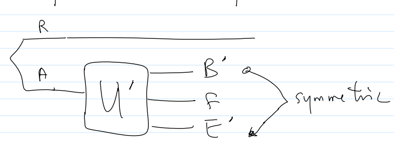
Yet another interpretation:

Any channel: $\quad$ Degradable:



Antidegradable: F is with Eve.

∴ Degradable / antidegradable:



Thm: If N antidegradable, $Q(N) = 0$.

In fact, not a single qubit can be sent with arbitrarily large number of uses of N.

Pf: If so, both Bob & Eve have a copy of the input implying cloning.

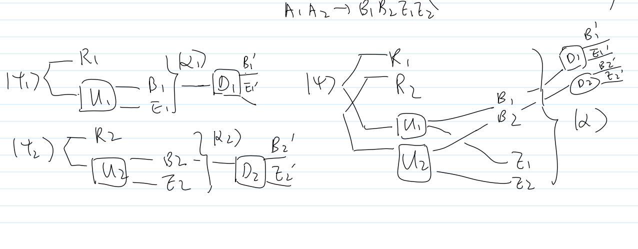
(Devetak & Shor)

Thm: If N degradable, then $Q^{(n)}(N) = Q^{(1)}(N)$.

Pf: Let N_1, N_2 be degradable channels, $\quad Q^{(1)}(N_1\otimes N_2) = Q^{(1)}(N_1) + Q^{(1)}(N_2)$
U_1, U_2 be their Stinespring dilations.

let $|\alpha_i\rangle = I_{R_i} \otimes U_{i\, A_i\to B_iE_i}(|\psi_i\rangle_{R_iA_i})$

$|\alpha\rangle = I_{R_1R_2} \otimes \underset{A_1A_2\to B_1B_2E_1E_2}{U_1\otimes U_2}\left(|\psi\rangle_{R_1R_2A_1A_2}\right)$



Note that tensor product of Stinespring dilations is a Stinespring dilation of the tensor product of the channels.

Also tensor product of degradable channels is degradable.
& - - - - - - degrading maps degrades the tensor product of channels.

$$I_c(R_i \rangle B_i)_{|\alpha_i\rangle} = S(B_i) - S(E_i)$$

unitarity of degrading map

$$= S(B_i' E_i') - S(E_i')$$
$$= S(B_i' | E_i')$$

Claim $S(B_1'B_2' | E_1'E_2') \le S(B_1'|E_1') + S(B_2'|E_2')$

Pf (Claim):

LHS $= S(B_1' B_2' E_1' E_2') - S(E_1' E_2')$

RHS $= S(B_1' E_1') - S(E_1') + S(B_2' E_2') - S(E_2')$

$$\text{RHS} - \text{LHS} = S(B_1'E_1') + S(B_2'E_2') - S(B_1'B_2'E_1'E_2') + S(E_1'E_2') - S(E_1') - S(E_2')$$

$$= S(B_1'E_1' : B_2'E_2') - S(E_1' : E_2')$$

≥ 0 by monotonicity of QMI
(tracing of B_1', B_2' are local)

$$\therefore \forall |\alpha\rangle,\ I_c(R_1R_2\rangle B_1B_2)_{|\alpha\rangle} \leq I_c(R_1\rangle B_1)_{\mathrm{tr}_{R_2B_2}|\alpha\rangle} + I_c(R_2\rangle B_2)_{\mathrm{tr}_{R_1B_1}|\alpha\rangle}$$
$$\leq \max_{|\alpha_1\rangle} I_c(R_1\rangle B_1)_{|\alpha_1\rangle} + \max_{|\alpha_2\rangle} I_c(R_2\rangle B_2)_{|\alpha_2\rangle}$$

$$\therefore Q^{(1)}(N_1 \otimes N_2) \leq Q^{(1)}(N_1) + Q^{(1)}(N_2)$$

($\geq$) obvious.

Finally, if N degradable:

$$Q^{(m)}(N) = Q^{(1)}(N \otimes \underbrace{N^{\otimes(m-1)}}_{\text{still degradable}})$$
$$= Q^{(1)}(N) + Q^{(1)}(N^{\otimes(m-1)})$$
$$= \vdots$$
$$= m\, Q^{(1)}(N)$$

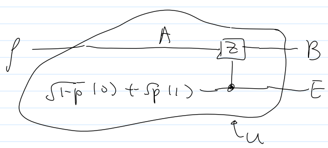
$\therefore Q(N) = Q^{(1)}(N)$.

Cor: $Q(N) = \max(1-2p, 0)$ for erasure channel w/ error prob p.
note factor of 2.

eg Phase damping channel:

$$N_p(\rho) = (1-p)\rho + p Z\rho Z^\dagger$$

Stinespring's dilation:

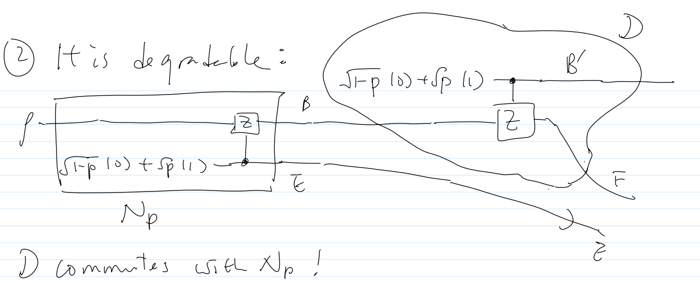


Like the erasure channel

① Bob can append another phase damping channel to the output and "damp" it further:

$$N_q \circ N_p(\rho) = [(1-p)(1-q) + pq]\,\rho + (p+q)\, Z\rho Z^\dagger$$

② It is degradable:

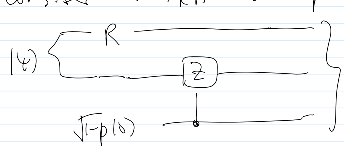


D commutes with N_p!

So B' and E symmetric.

Note that this is true $\forall p \in [0,1]$ ($p = \frac{1}{2}$ is worst).

Consider $|\psi\rangle_{RA}$ as input.



$$|\alpha\rangle = \sqrt{1-p}\,|0\rangle_E\, |\psi\rangle_{RB} + \sqrt{1-p}\,|1\rangle_E\, (I\otimes Z)|\psi\rangle_{RB}$$

$$I(R\rangle B) = \underset{\leq 1}{S(B)} - \underset{= H(p)}{S(E)}$$

achievable for $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$$Q(N) = Q^{(1)}(N) = 1 - H(p)$$

eg. Amplitude damping channel.

There's a nice Stinespring dilation leaving $|0\rangle_A$ as $|0\rangle_B$ but sending $|1\rangle_A$ to a state sym on B & E.

It is also degradable up to $\gamma \leq \gamma_0$

So $Q(N) = Q^{(1)}(N)$ can be found.

Detail left in Assignment 3.

(NB Before degradability was understood, we had no idea what's the capacity of the AD channel, esp due to the possibility of approx QEC.)