Lec 12, June 15, 2010

Note Title 13/06/2010

Last time :

Stinespring dilations

Complementary channels

Degradable & anti-degradable channels

Additivity (weak) of coherent info for degradable channels

Calculation of the 1-shot coherent info & quantum capacity for the erasure channel & dephasing channel.

This time :

- Quantum capacity of the depolarizing channel + some general results.

The depolarizing channel (on a qubit):

$$\mathcal{N}(\rho) = (1-p)\rho + p\frac{I}{2}$$

$$= (1-q)\rho + \frac{q}{3}(X\rho X + Y\rho Y + Z\rho Z) = \mathcal{N}_q(\rho)$$

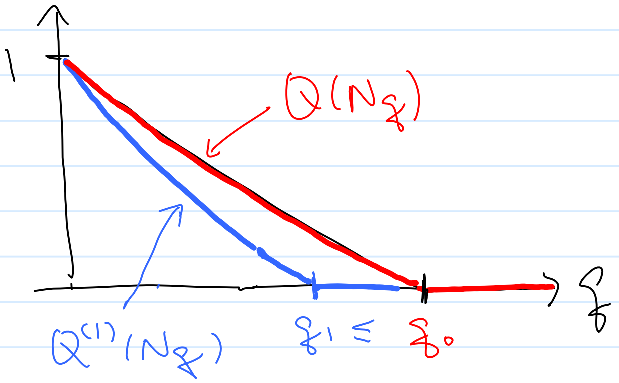
where $q = \frac{3}{4}p$ is called "the error prob".

When $q \approx 0$, $Q(\mathcal{N}_q) \approx 1$

$q = 3/4$, $Q(\mathcal{N}_q) = 0$ (proved last time)

Given $\mathcal{N}_q$, Bob can simulate the output for $\mathcal{N}_{q'}$ for $q' > q$

$\therefore$ $Q(\mathcal{N}_q)$ is monotonically decreasing with q.



q_0: value of q when $Q(\mathcal{N}_q)$ first turns 0.

called the "threshold error rate".

still unknown after 14 years of research.

This & the next class:

① find $Q^{(1)}(\mathcal{N}_p)$ which lower bounds $Q(\mathcal{N}_p)$.
obtain p_1 (where $Q^{(1)}(\mathcal{N}_p)$ first turns 0) to lower bdd p_0.

② Given an explicit nondegenerate code to achieve $Q^{(1)}(\mathcal{N}_p)$.

③ Given a degenerate code making $Q^{(m)}(\mathcal{N}_p) > 0$
for finite m & $p_1 < p$

∴ Showing ⓐ degenerate code strictly outperforms nondeg codes
ⓑ $Q^{(1)}(N) \lneq Q^{(m)}(N)$ in general.

thus the regularized expression is necessary

Will do ①-③ for random Pauli channels.

④ Upper bounds on $Q(N_\zeta)$ & thus ζ_0 by studying

(a) Additive extension of a quantum channel

(b) Symmetric assisted quantum capacity of a quantum channel

Will do ④ for general channels.

Def (Random Pauli Channel):

$$N_{\vec{q}}(\rho) = (1-q_x-q_y-q_z)\rho + q_x X\rho X + q_y Y\rho Y + q_z Z\rho Z$$

$0 \leq q_x, q_y, q_z, 1-q_x-q_y-q_z \leq 1$

eg $N_q = N(\frac{q}{3}, \frac{q}{3}, \frac{q}{3})$

Let $H_{\vec{q}} = H(\{q_x, q_y, q_z, 1-q_x-q_y-q_z\})$

① What is $Q^{(1)}(N_{\vec{q}}) = \max_{|\psi\rangle_{RA}} I_c(R\rangle B)_{I \otimes N_{\vec{q}}(|\psi\rangle\langle\psi|)}$?

Claim: optimal $|\psi\rangle_{RA} = \begin{cases} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & \text{if } 1 - H_{\vec{q}} \geq 0 \\ |0\rangle_R |0\rangle_A & \text{otherwise} \end{cases}$

To prove this, we need a general result concerning coherent information & a teleportation trick.

Bad news: there is a small problem with the proof given in the class. I have no quick fix to the proof, but will come back to the proof later in the course. For now, I will leave the mistake proof in the notes (and label where the mistake is) and pasted in earlier numerical arguments for the depolarizing

Properties of $I_c(R>B)$:

Properties concerning Ic(R>B) appear correct still.

Recall it is
- inv under local unitary, attaching/removing pure state local ancillas
- non increasing when discarding subsys of B (thus non increasing under TCP maps on B)
- increasing / decreasing when discarding subsys of R

Furthermore, it is
- non increasing under classical comm from B to R
- increasing / decreasing under classical comm from R to B

Modeling classical communication:

$$|\Psi\rangle_{RBE} \xrightarrow[\substack{\text{local}\\ \text{unitary}\\ \text{by sender}}]{} \sum_c \sqrt{p_c}\, \underset{\substack{4\ C\\ \text{comp basis state on}\\ \text{sender's sub sys } C}}{|c\rangle} |\Psi_c\rangle_{RBE} \xrightarrow[CC]{} \sum_c \sqrt{p_c}\, \underbrace{|ccc\rangle}_{\substack{R'B'E'\\ \text{sender, receiver \& } E\\ \text{all have a copy}}} |\Psi_c\rangle_{RBE}$$

Given classical comm from R to B :

eq 1 $$|\psi\rangle_{RBE} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{RE} |0\rangle_B$$

$$\Big\downarrow \text{ R attaches } |0\rangle \text{ \& performs a CNOT}$$

$$|\psi'\rangle_{RCBE} = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{RCE} |0\rangle_B$$

$$\Big\downarrow \text{ CC}$$

$$|\psi''\rangle_{\substack{RBE \\ R'B'E'}} = \frac{1}{\sqrt{2}}\left(|00000\rangle + |11111\rangle\right)_{RR'EE'B'} |0\rangle_B$$

$$I_c(R>B)_{|\psi\rangle} = S_B - S_E = -1, \quad I_c(R>B)_{|\psi''\rangle} = S_{BB'} - S_{EE'} = 0$$

increases

eq2 $|\psi\rangle_{RBE} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{R\cancel{E}B} |0\rangle_{\cancel{B}E}$

$\downarrow$ R attaches $|0\rangle$ & performs a CNOT

$|\psi'\rangle_{RCBE} = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{RC\cancel{E}B} |0\rangle_{\cancel{B}E}$

$\downarrow$ CC

$|\psi''\rangle_{RBER'B'E'} = \frac{1}{\sqrt{2}}\left(|00000\rangle + |11111\rangle\right)_{RR'\cancel{E}BE'B'} |0\rangle_{\cancel{B}E}$

$I_c(R\rangle B)_{|\psi\rangle} = S_B - S_E = +1, \quad I_c(R\rangle B)_{|\psi''\rangle} = S_{BB'} - S_{EE'} = 0$

$\longrightarrow$

de~~in~~creases

eq3. $$|\psi\rangle_{RBE} \xrightarrow[\text{on } R]{\text{local unitary}} \sum_c \sqrt{p_c}\, |c\rangle_{R'} |\psi_c\rangle_{RBE} \xrightarrow{CC} \sum_c \sqrt{p_c}\, \underbrace{|ccc\rangle_{R'B'E'}}_{\text{sender, receiver \& E all have a copy}} |\psi_c\rangle_{RBE}$$

☆ If $E'E$ in product state

then $$\left(S_B - S_E\right)_{|\psi\rangle_{RBE}} - \left(S_{BB'} - S_{EE'}\right)_{\sum_c \sqrt{p_c}\, |ccc\rangle_{R'B'E'} |\psi_c\rangle_{RBE}}$$

$$= S_B - S_{BB'} + S_{E'}$$

$$= S_B - S_{BB'} + S_{B'} \geq 0$$

In this special case, $I_c(R\rangle B)$ nonincreasing.

- Given classical comm from B to R:

$$\begin{tikzcd}
|\psi\rangle_{RBE} \arrow[r, "\text{local}"', "\text{unitary}"] & \sum_c \sqrt{p_c}\,|c\rangle_C\,|\psi_c\rangle_{RBE} \arrow[r, "\cancel{CC}"'] \arrow[d, "ⓐ"] & \sum_c \sqrt{p_c}\,\underbrace{|ccc\rangle_{R'B'E'}}_{\text{sender receiver \& E all have a copy}}\,|\psi_c\rangle_{RBE} \\
 & \sum_c \sqrt{p_c}\,|c\rangle_{B'}\,|c\rangle_{E'}\,|\psi_c\rangle_{RBE} \arrow[ur, "ⓑ"'] &
\end{tikzcd}$$

local unitary ~~by sender~~

from B → BC

$I_c(R>B)$ inv

comp basis state on sender's sub sys C

In Step ⓐ, Bob changes $|c\rangle_C$ to $|c\rangle_{B'}|c\rangle_{B''}$ (I_c inv)

Then discards B'' (relabeled as E') (I_c nonincreasing)

In Step ⓑ, Bob changes $|c\rangle_{B'}$ to $|c\rangle_{B'}|c\rangle_{B'''}$ (I_c inv)

gives B''' to R (relabeled as R')

$S_{BB'}$ & $S_{BB'RR'}$ both unchanged (I_c inv)

Side notes on the proof:

Reduced state on BB' before & after ⓑ both equal to

$$\sum_c p_c |c\rangle\langle c|_{B'} \operatorname{tr}_{RE}(|\psi_c\rangle\langle\psi_c|)$$

Reduced state on BB'RR' before ⓑ:

$$\left.\begin{aligned} &\sum_c p_c |c\rangle\langle c|_{B'} \operatorname{tr}_E(|\psi_c\rangle\langle\psi_c|) \\ \text{after ⓑ: } &\sum_c p_c |cc\rangle\langle cc|_{B'R'} \operatorname{tr}_E(|\psi_c\rangle\langle\psi_c|) \end{aligned}\right\} \text{same entropy}$$

Important to have step ⓐ first (monotonicity already proved) then $|c\rangle$ "decohered" already on B' (so giving a copy to R' is then entropy preserving).

Back to $Q^{(1)}(N_{\vec{f}}) = \max_{|\psi\rangle_{RA}} I_c(R\rangle B)_{I\otimes N_{\vec{f}}(|\psi\rangle\langle\psi|)}$?

Claim: optimal $|\psi\rangle_{RA} = \begin{cases} |\Phi\rangle_{RA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & \text{if } 1 - H_{\vec{f}} \geq 0 \\ |0\rangle_R |0\rangle_A & \text{otherwise.} \end{cases}$

Teleportation trick:

Let $|\psi\rangle_{RA}$ be optimal.

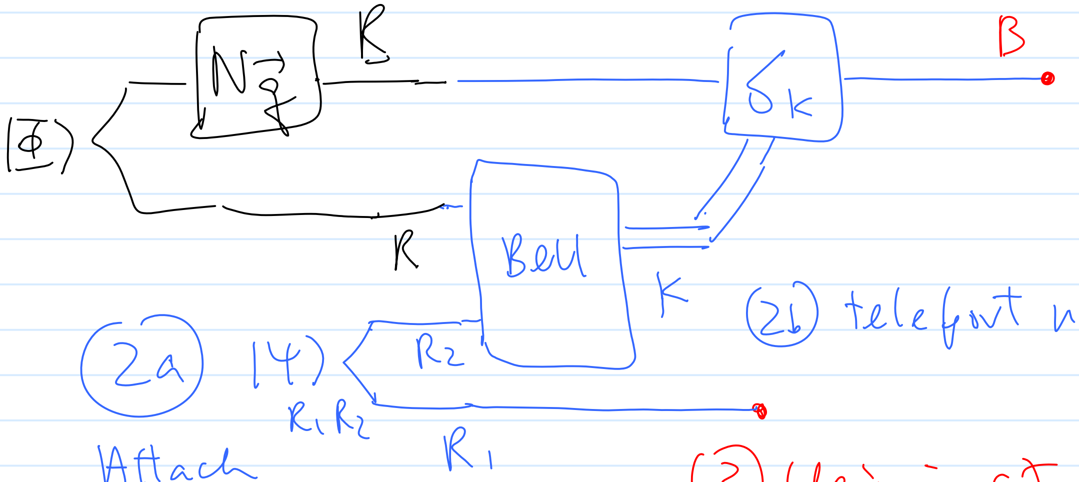
Will show how to create $I\otimes N_{\vec{f}}(|\psi\rangle\langle\psi|)$ using $I\otimes N_{\vec{f}}(|\Phi\rangle\langle\Phi|)$ & classical comm from R to B, with the comm in product state with E's initial state.

The problem turns out that the communication may be NOT independent of Eve's state.

$I_c(R\rangle B)$ monotonic so $I_c(R\rangle B)_{I\otimes N_{\vec{f}}(|\Phi\rangle\langle\Phi|)} \geq I_c(R\rangle B)_{I\otimes N_{\vec{f}}(|\psi\rangle\langle\psi|)}$

① Given:

② Bob teleports half of $|\psi\rangle$ to R:

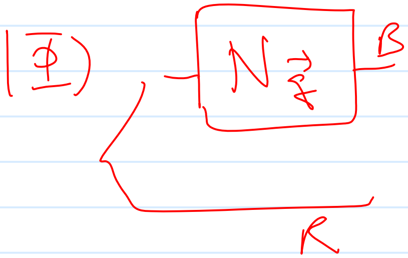


(2a) Attach $|\psi\rangle$ locally.

(2b) teleport using $I\otimes N_{\vec{q}}|\Phi\rangle$ instead of $|\Phi\rangle$

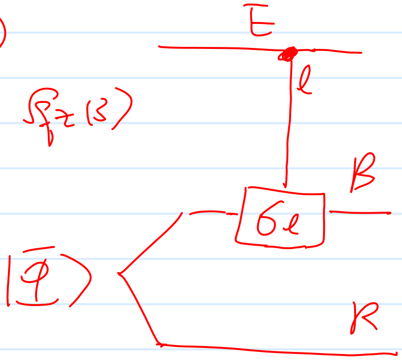
③ Claim: State on R_1B is $I\otimes N_{\vec{q}}|\psi\rangle$

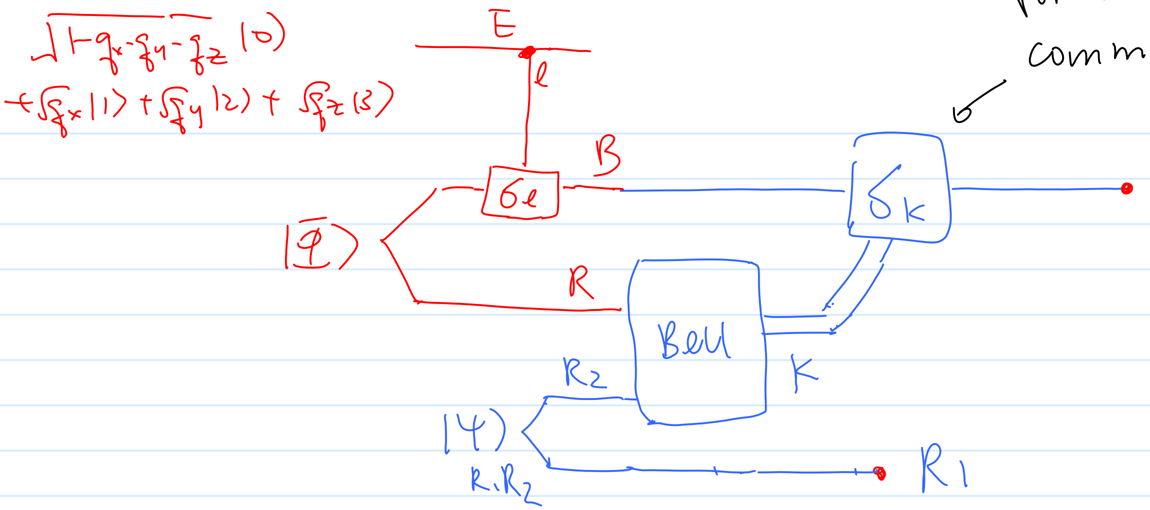
Pf of ③: Rewrite



as

$$\sqrt{1-q_x-q_y-q_z}\,|0\rangle + \sqrt{q_x}\,|1\rangle + \sqrt{q_y}\,|2\rangle + \sqrt{q_z}\,|3\rangle$$

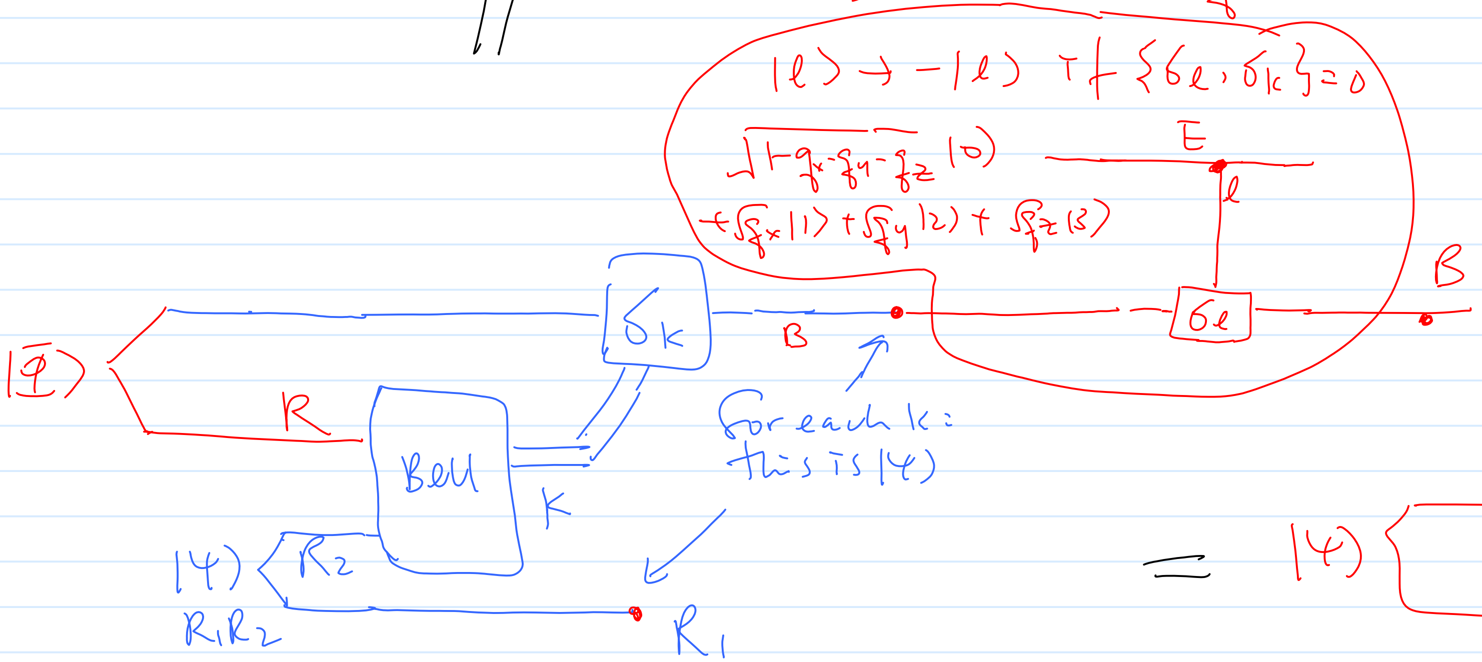




for each k
commutes / anti-commutes
with σ_l

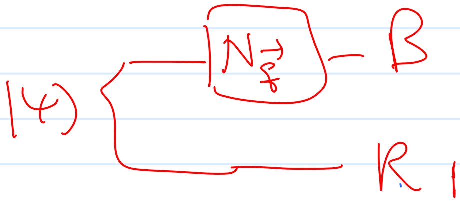
||

Still does $N_{\vec{f}}$



for each k:
this is $|\psi\rangle$

=

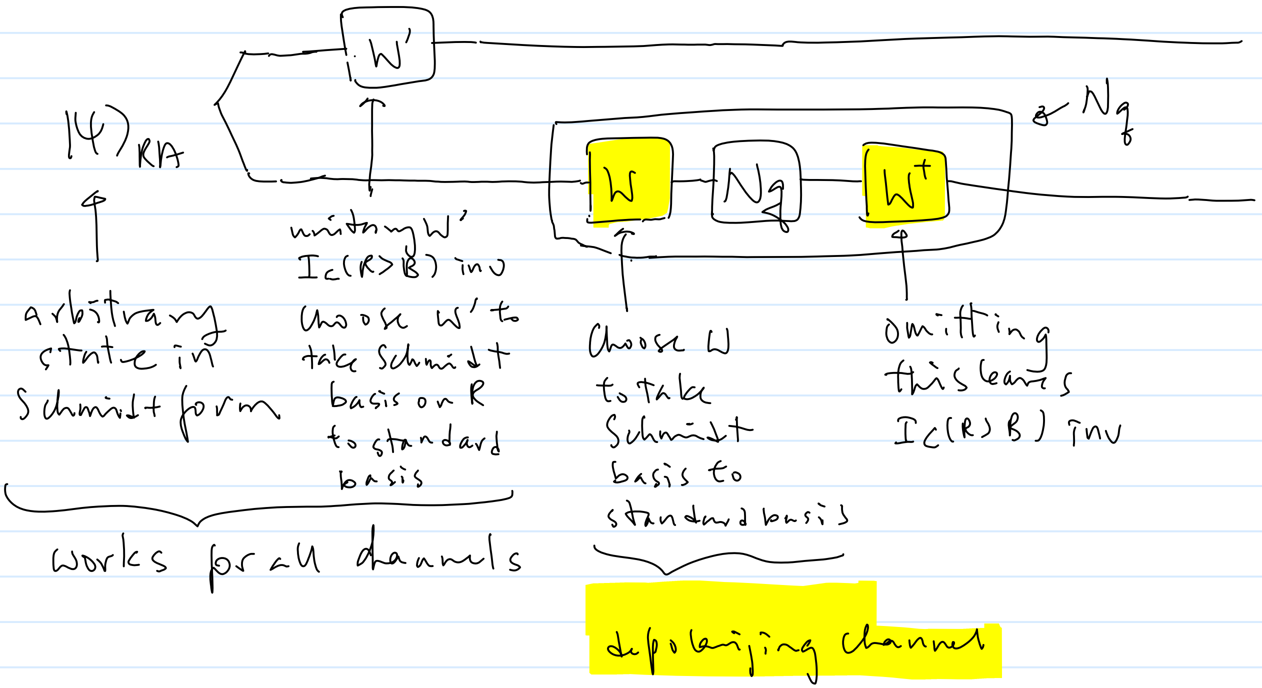


For now, use this alternative argument (that only works for N_q not in general for $N_{\vec{q}}$) to max $I_c(R\rangle B)_{I\otimes N_q(|\psi\rangle\langle\psi|)}$

Note that $\forall W$ unitary qubit operation, $\forall \rho$

$$W^\dagger \circ N_q \circ W(\rho) = N_q(\rho)$$

This also implies $I \otimes W^\dagger \circ N_q \circ W = I \otimes N_q$.



WLOG $|\psi\rangle_{RA} = \alpha|00\rangle + \beta|11\rangle$.

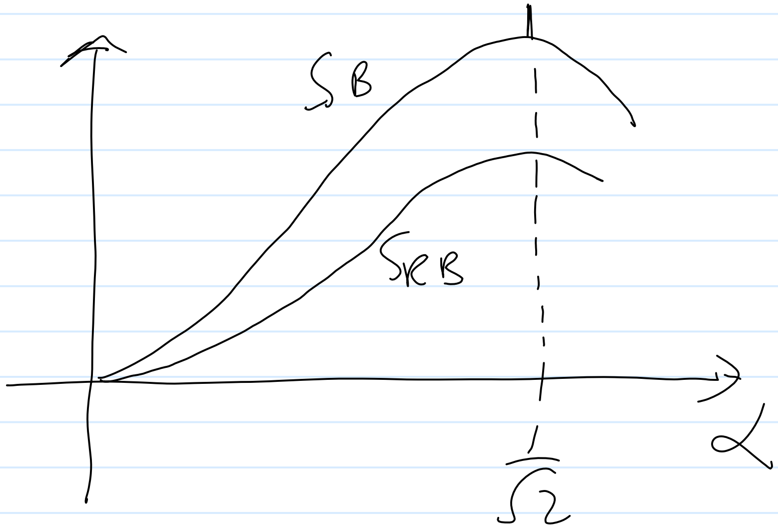
Unfortunately, I don't have an analytic proof that

$I_c(R\rangle B)_{I\otimes N_q(|\psi\rangle\langle\psi|)}$ is maximized by

$$\begin{cases} \alpha = \beta = \frac{1}{\sqrt{2}} & \text{if } 1 - H_{\vec{q}} \geq 0 \\ \alpha = 1, \beta = 0 & \text{otherwise.} \end{cases}$$

For each z, it is easy to plot S_B & S_{RB} as a fcn of α.

When $1 - H_{\vec{z}} \geq 0$:



When $1 - H_{\vec{z}} < 0$:

S_{RB}, S_B have similar shape but S_{RB} is above S_B so optimal point is $\alpha = 0$

This proves the claim at least for the depolarizing channel.
For now, we will assume the claim, and we will come back to fix it for the general random Pauli channel.

Finish off the calculation of $Q^{(1)}(N_{\vec{q}})$:

Let $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi\rangle$

$|\Phi_{01}\rangle = 1 \otimes Z \, |\Phi\rangle$

$|\Phi_{10}\rangle = 1 \otimes X \, |\Phi\rangle$

$|\Phi_{11}\rangle = 1 \otimes Y \, |\Phi\rangle$

$$I \otimes N_{\vec{q}}(|\Phi\rangle\langle\Phi|) = (1 - q_x - q_y - q_z)\, |\Phi_{00}\rangle\langle\Phi_{00}| + q_x \, |\Phi_{10}\rangle\langle\Phi_{10}| + q_y \, |\Phi_{11}\rangle\langle\Phi_{11}| + q_z \, |\Phi_{01}\rangle\langle\Phi_{01}|$$

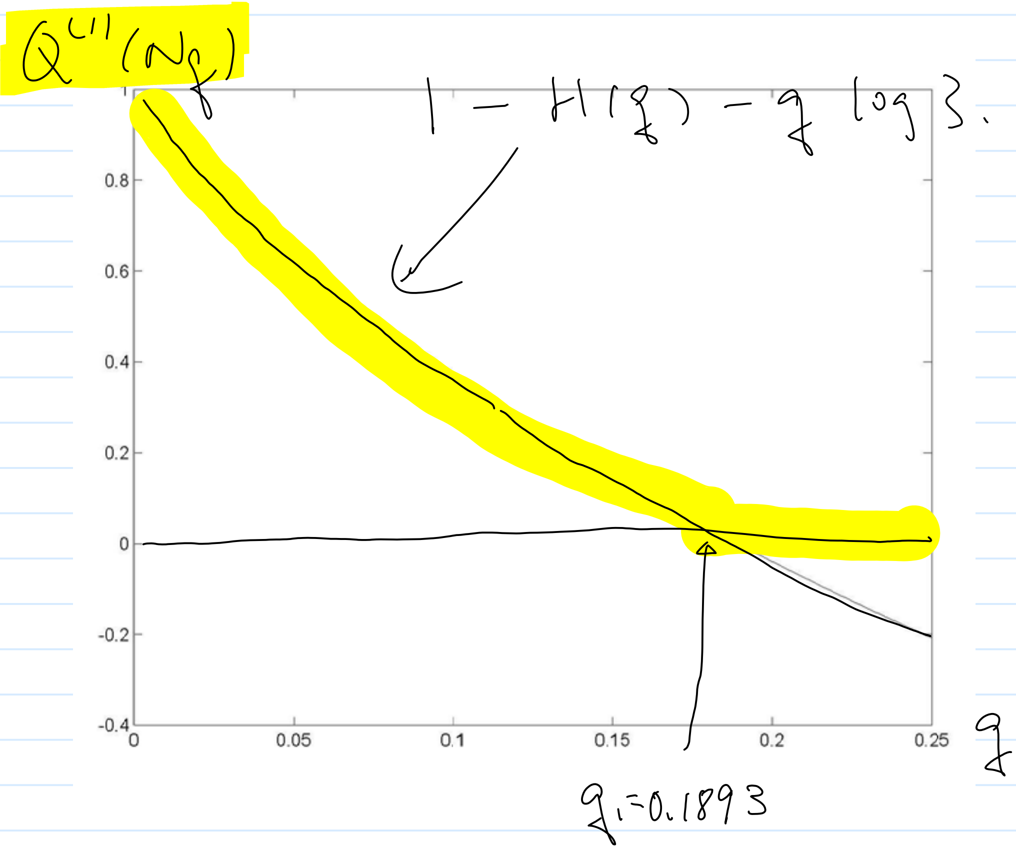
$$I_c(R\rangle B)_{I \otimes N_{\vec{q}}(|\Phi\rangle\langle\Phi|)} = S_B - S_{RB} = 1 - H_{\vec{q}}$$

$$I_c(R\rangle B)_{I \otimes N_{\vec{q}}(|00\rangle\langle 00|)} = 0$$

for N_q, w/ $q_x = q_y = q_z = \frac{q}{3}$

$$H_q = -(1-q)\log(1-q) - 3 \times \frac{q}{3}\log\frac{q}{3} = \overbrace{H(q)}^{\text{binary entropy fcn}} + q\log 3$$

$$Q^{(1)}(N_q) = \max\{1 - H(q) + q\log 3, 0\}$$



② Nondegenerate code achieving $Q^{(1)}(N_{\vec{q}})$ <u>when it is positive</u> :

For this part, use the Kraus rep of $N_{\vec{q}}$:

for each channel use,

$$\begin{array}{r}\text{treat these}\\ \text{symbols as}\\ \text{random vars}\end{array}\left\{\begin{array}{llll} I & \text{occurs} & \text{wp} & 1-q_x-q_y-q_z \\ X & \text{- - -} & & q_x \\ Y & & & q_y \\ Z & & & q_z \end{array}\right.$$

For n uses, wp $1-\delta_n$, "the error" is a tensor product of n Pauli matrices given by a typical sequence of IXYZ.

Call each of such "typical error" E_i (occurring wp p_i).

$$N_{\vec{q}}^{\otimes n}(\rho) = \sum_{i=1}^{2^{n(H_{\vec{q}}+\varepsilon_n)}} p_i E_i \rho E_i^{\dagger} + \delta_n \underset{\text{TCP map.}}{A}(\rho) \quad \text{———} \circledast$$

e.g. $q_x = 0.01$, $q_y = 0.03$, $q_z = 0.06$, $n = 1000$

$H\vec{q} = 0.4617$.

$$\text{Typical errors} = \underbrace{1\,1\,1\,X\,Y\,1\,1\,1\,Z\,Z\,1 \qquad 1}_{\approx\ 10\ X\text{'s},\ 30\ Y\text{'s}\ \&\ 60\ Z\text{'s}.}$$

Say, call this E_1

Out of 4^{1000} Pauli errors, only include $2^{461.7+n\epsilon_n}$ errors in 1st term of ⊛

Since E_i's are unitary, if Bob determines "i" whp he can revert E_i and recovers the input whp.

Claim:

if we pick a random stabilizer code (encoding k qubits in n then

$$\operatorname*{Prob}_{C}\left[\operatorname*{Prob}_{i}\left(\exists E_j \text{ s.t. } E_i, E_j \text{ have same syndrome}\right)\right]$$

$$\leq 2^{n(H(\vec{p})+\epsilon_n)}\; 2^{-(n-k)}$$

If the claim holds, there exists a code C_0 s.t.

$$\operatorname*{Prob}_{i}\Big(\underbrace{\exists E_j \text{ s.t. } E_i, E_j \text{ have same syndrome}}_{E_i \text{ does not have unique syndrome \& may not be correctable}}\Big) \leq 2^{n(H(\vec{p})+\epsilon_n)}\; 2^{-(n-k)}$$

$1 - \text{Prob}_i \left(\exists E_j \text{ s.t. } E_i, E_j \text{ have same syndrome} \right)$ represents

the prob to have an E_i with unique syndrome

If above $\simeq 1$, then most E_i's can be identified

& corrected.

In particular: use this Co

choose $n\alpha_n$ with $\alpha_n \to 0$ & $n\alpha_n \to \infty$

choose $K = n(1 - H_{\vec{\xi}} - \epsilon_n - \alpha_n)$

Then above prob $\leq 2^{-n\alpha_n} \to 0$

$\frac{K}{n} \to 1 - H_{\vec{\xi}} = Q^{(1)}(\mathcal{N}_{\vec{\xi}})$

Let Bob's decoder be $\mathcal{D}$: it finds "i" & applies $E_i^\dagger$.

$$N_{\vec{q}}^{\otimes n}(\rho) = \sum_{i=1}^{2^{n(H_{\vec{q}}+\varepsilon_n)}} p_i E_i \rho E_i^\dagger + \delta_n A(\rho)$$

$$\Big\downarrow \mathcal{D}$$

$$\mathcal{D}\circ N_{\vec{q}}^{\otimes n}(\rho) = \sum_{\substack{i \text{ with}\\ \text{unique}\\ \text{syndrome}}} p_i \rho + \sum_{\substack{i \text{ without}\\ \text{unique}\\ \text{syndrome}}} \mathcal{D}(E_i \rho E_i^\dagger) + \delta_n \mathcal{D}\circ A(\rho)$$

$$= \left(1-2^{-n\delta_n}\right)\rho + \left(2^{-n\delta_n} + \delta_n\right)\rho'$$

∴ Very high worse case fidelity & syndrome is unique

∴ code is mostly nondegenerate.

The proof of the claim relies on some background on

- stabilizer code
- counting Pauli matrices with prescribed commutation & anticommutation relations using a fixed list of Pauli matrices

These are described in detail with egs in Appendices 1 & 2.

Pf (claim):

$$\mathop{\text{Prob}}_{C} \mathop{\text{Prob}}_{i} \left(\exists E_j \text{ s.t. } \bar{E}_i, \bar{E}_j \text{ have same syndrome} \right)$$

$$= \mathop{\text{Prob}}_{i} \mathop{\text{Prob}}_{C} \left(\exists E_j \text{ s.t. } \bar{E}_i, \bar{E}_j \text{ have same syndrome} \right)$$

Consider an arbitrary pair of $\bar{E}_i, \bar{E}_j$ for $i \neq j$ (all we need is $\bar{E}_i^{+} \bar{E}_j \neq I$).

Using appendix 1, for a stabilizer code with stabilizer generators $S_1, S_2, \ldots, S_{n-k}$

E_i, E_j have same syndrome iff $\forall l \underbrace{[E_i^\dagger E_j, S_l] = 0}_{E_i^\dagger E_j \in N(S) \text{ normalizer of } S}$

If we pick m independent Pauli matrices on n qubits there are 2^{2n-m} Pauli matrices having a prescribed comm / anti relation with them.

Idea: fix $\bar{E}_i^{\dagger}\bar{E}_j \neq I$.

① We pick $S_1 \cdots S_{n-k}$ at random & count how # ways to do it.

② Repeat but impose also each S_ℓ commutes w/ $E_i^{\dagger}E_j$.

$$\therefore \text{Prob}\left[\bar{E}_i^{\dagger}\bar{E}_j \in N(S)\right] = \frac{\#\textcircled{2}}{\#\textcircled{1}}$$

#① : $2^{2n}-1$ choices for S_1 ($S_1 \neq I$)

$2^{2n}/2 - 2$ choices for S_2 (Only $2^n/2$ Pauli's commute with S_1 and take out I, S_1)

$2^{2n}/2^2 - 2^2$ - - - S_3 ($2^n/2^2$ Pauli's commute with both S_1, S_2, take out $I^{\otimes n}$)

⋮

$2^{2n}/2^{n-k-1} - 2^{n-k-1}$ - - - S_{n-k}

#② : $2^{2n-1} - 1$ - - - for S_1

$2^{2n-1}/2 - 2$ for S_2

$\vdots$

$2^{2n-1}/2^{n-k-1} - 2^{n-k-1}$ for S_{n-k}

$$\frac{\#\textcircled{2}}{\#\textcircled{1}} = \frac{2^{2n-1}-1}{2^{2n}-1} \times \cdots \times \frac{2^{2n-1}/2^{n-k-1} - 2^{n-k-1}}{2^{2n}/2^{n-k-1} - 2^{n-k-1}}$$

$$\leq \left(\frac{1}{2}\right)^{(n-k)}$$

$$\underset{C}{\mathrm{Prob}}\ \underset{i}{\mathrm{Prob}}\left(\exists E_j \text{ s.t. } \bar{E}_i, \bar{E}_j \text{ have same syndrome} \right)$$

$$= \underset{i}{\mathrm{Prob}}\ \underbrace{\underset{C}{\mathrm{Prob}}\left(\exists \bar{E}_j \text{ s.t. } \bar{E}_i, \bar{E}_j \text{ have same syndrome} \right)}$$

$$\leq \underset{i}{\mathrm{Prob}}\ \left(\# \bar{E}_j\text{'s} \right) 2^{-(n-k)}$$

$$= 2^{n(H(\vec{p}) + \epsilon_n)}\ 2^{-(n-k)} \qquad \text{as claimed.}$$

Appendix 1 on stabilizer codes:

A quantum code is a subspace of the ambient space.

A stabilizer code specifies this subspace as follows:

$S_1, S_2, \ldots, S_\ell, \ldots S_{n-k}$ are commuting Pauli matrices so that none is the product of a subset of the others.

They generate the stabilizer S multiplicatively:

$$S = \{ M = S_1^{e_1} \cdot S_2^{e_2} \cdots S_{n-k}^{e_{n-k}} : e_i \in \{0,1\}\}$$

($e_i = 1$ means S_i is a factor of M).

S is a commutative group with 2^{n-k} elements.

eg1, $n=5$, $k=1$

$S_1 = X Z Z X 1$

$S_2 = 1 X Z Z X$

$S_3 = X 1 X Z Z$

$S_4 = Z X 1 X Z$

Note that $ZZX1X = S_1 S_2 S_3 S_4$ can already be generated by the existing ones. Adding it to the list does not give a new S.

eg2. $n=3$, $k=1$,

$S_1 = ZZ1$

$S_2 = Z1Z$

$S = \{1, S_1, S_2, S_1 S_2\} = \{111, ZZ1, Z1Z, 1ZZ\}$

The code is the simultaneously +1 eigenspace of every element of S

but it suffices to say it is the simultaneous +1 eigenspace of the generators $S_1 \dots S_{n-k}$.

Dim of the code $= 2^n / 2^{n-k} = 2^k$

So this code encodes k qubits in n.

Let $\Pi_C =$ projector onto the code space

Say, some Pauli error E_i occurs to an encoded state & we measure $S_1, S_2, \ldots S_{n-k}$.

What do we get? (BTW, each S_ℓ only has eigvals ± 1).

$$S_\ell E_i \Pi_c = \begin{cases} +1 \quad E_i S_\ell \Pi_c = E_i \Pi_c & \text{if } E_i S_\ell = S_\ell E_i \\ -1 \quad E_i S_\ell \Pi_c = -E_i \Pi_c & \underbrace{\text{otherwise} \quad .}_{\text{2 Pauli matrices either commutes or anti comm}} \end{cases}$$

∴ $E_i \Pi_c$ is a $\pm$ eigenspace of S_ℓ if S_ℓ, E_i $\substack{\text{commut} \\ \text{anti com}}$

∴ Measuring $S_1 \ldots S_{n-k}$, get string of ± 1's s.t.

a "−" occurs on the lth position iff $\{S_l, E_i\} = 0$.

This $(n-k)$-bit string is called the syndrome of E_i.

$\therefore$ 2 errors E_i, E_j have same syndromes

iff $\forall l$ they both commute with S_l
or they both anticommute with it

iff $E_i^\dagger E_j = E_i E_j$ commute with every S_l.

If so, $E_i^\dagger E_j \in N(S)$ (normalizer of S, happens to be the group of Pauli's commuting with all of S).

$\star$ $N(S) / S$ = encoded Pauli's on code space.

eg1. $S_1 = X Z Z X 1$

$S_2 = 1 X Z Z X$

$S_3 = X 1 X Z Z$

$S_4 = Z X 1 X Z$

anti comm

$N(S)/S$ generated by $XXXXX \leftarrow$ encoded X

$ZZZZZ \leftarrow$ - - - Z

Note both commute with all of $S_1 \cdots S_4$ but neither is generated by them.

Let $E_1 = Y1111$ then measuring $S_1\ S_2\ S_3\ S_4$ gives $-\ +\ -\ -$.

Exercise: Check that all 15 single qubit Pauli errors have a diff syndrome.

eg. $E_2 = 11X11$ has syndrome $--++$.

But $E_3 = ZXXXX$ has syndrome $-+--$ same as E_1

Note $E_1^\dagger E_3 = (Y1111)(ZXXXX) = XXXXX$

$\in N(S)$.

$\underline{\text{eg 2}} \rightarrow$ $S_1 = ZZ1$

$S_2 = 1ZZ$

$E_1 = Z11$, $E_2 = 1Z1$, $E_3 = 11Z$ all have same syndrome as III.

$N(S)$ generated by ZZZ & XXX.

Appendix 2:

There are 2^{2n} Pauli's on n qubits.

Let P_1 P_2 $\cdots$ P_m be m independent Pauli's.

How many of the 2^{2n} Pauli's have a prescribed comm/anticomm relation with each P_i's?

Ans: $2^{2n}/2^m$

Idea: express X as 10

Z as 01

Y as 11

every Pauli P expressed as 2n bit string. S_P

$$[P, Q] = 0 \iff S_P \cdot S_Q = 0$$

$$\{P, Q\} = 1 \iff S_P \cdot S_Q = 1$$

where the $S_P \cdot S_Q = \left(S_{P1} S_{Q1} + S_{P2} S_{Q2} + \ldots + S_{P2n} S_{Q2n} \right) \bmod 2$

∴ Comm / anti comm relation w/ m Pauli's are m linear constraints on the binary space of $2n$, each reducing the space to half the original size.

eg. $n=2$ There're 8 Pauli's commuting with
$X1$ (1 or X on first qubit,
anything on 2nd qubit).

What about comm w/ $X1$
& anti comm w/ ZZ ?

	✓	✓	×	×
Out of	1X	1Y	1Z	11
Out of	XX	XY	XZ	X1
	×	×	✓	✓

Instead # = 4 = 16/4.