CO781 / QIC890 Lec 19, Nov 17, 2016

Non additivity of $Q^{(1)}(N)$ & degenerate QECCs.

- qubit depolarizing channels
- rocket channel
- super-activation ?

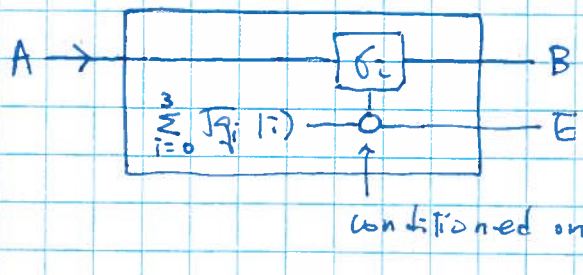
+ Assisted & private capacities of a quantum channel

- Consider the random Pauli channel:

$$\mathcal{N}_{\vec{q}}(\rho) = q_0 \rho + q_1 X\rho X + q_2 Y\rho Y + q_3 Z\rho Z$$

where $0 \le q_i$, $\sum_{i=0}^{3} q_i = 1$ & WLOG $q_0 \ge q_1 \ge q_2 \ge q_3$.

- One possible isometric extension for $\mathcal{N}_{\vec{q}}$:



- Not degradable if $q_2 > 0$ (at least 3 Kraus terms)

Many ways to see this:

(a) End of notes for lec 18, characterization of degradable channels with qubit outputs:

Cubitt, Ruskai, (G) Smith 0802.1360

$\forall \mathcal{N}: B(\mathbb{C}^d) \to B(\mathbb{C}^2)$

$\mathcal{N}$ degradable $\Rightarrow$ rank $(I \otimes \mathcal{N}(|\Phi_d\rangle\langle\Phi_d|)) \le 2$ & $d \le 3$.

(b) 1510.01366 L. Datrous:

If $q_2 > 0$ then $Q^{(1)}(\mathcal{N}_{\vec{q}}^{c}) > 0$,

So $\mathcal{N}_{\vec{q}}$ couldn't be degradable.

- Based on extensive numerics & continuity of $I_c(R \rangle B)$ as a function of $|\Psi\rangle$, we "know":

$$Q^{(1)}(\mathcal{N}_{\vec{p}}) := \max_{|\Psi\rangle_{RA}} I_c(R\rangle B)_{\mathcal{I}\otimes\mathcal{N}_{\vec{p}}(|\Psi\rangle\langle\Psi|)}$$

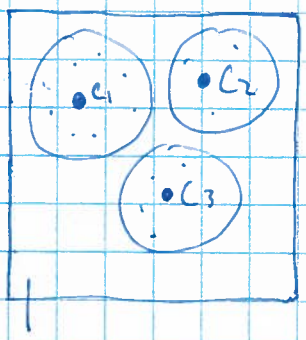
$$= \max\{1 - H(\vec{p}), 0\}$$

with optimal input $|\Psi\rangle_{RA} = \begin{cases} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & \text{if } 1 - H(\vec{p}) \geq 0 \\ |00\rangle & \text{otherwise.} \end{cases}$

* No analytic proof as of this lecture

- A simple random stabilizer code achieves the rate $Q^{(1)}(\mathcal{N}_{\vec{p}})$ in a non degenerate manner. (Detail: see Dec 12, 2012 p20-42).

Classical ECC

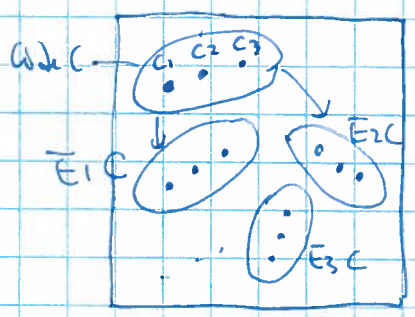


Ambient space
All possible input strings

Codewords: subset

Correctible errors take each C_i to a sphere of outputs. If error spheres don't overlap, decode by measuring "which sphere".

Alternative view



Correctible errors
$E_1, E_2, \ldots$
take C to non overlapping images

So we can find out <u>what error</u> and invert it.

"syndrome"

QECC

Same as

C: Subspace

Except it is possible
$E_iC = E_jC$ for $i \neq j$

If so, the code is "degenerate".

Eg. 9bit Shor code

$$|0\rangle_L = \frac{1}{2^{3/2}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$$

$$|1\rangle_L = \frac{1}{2^{3/2}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$$

Correct up to 1 Pauli error in 9 qubits.

But Z_1, Z_2, Z_3 act identically on the code!

So no need to distinguish between them.

Stabilizer code: (see Ink's talk in QIC 710)

- Let $G_1, \ldots G_{n-k}$ be $n-k$ independent (none is a product of a subset of the others) mutually commuting n-qubit Pauli operators.
- Each G_i has eigenvalues $+1, -1$.
- The simultaneous $+1$ eigenspace of $G_1 \cdots G_{n-k}$ is called the stabilizer code generated by $G_1 \ldots G_{n-k}$. [C]
- The code has 2^k dims so we encode k qubits in n.
- After a Pauli error E, if $|\psi\rangle \in C$

then $G_i(E|\psi\rangle) = \pm E G_i|\psi\rangle = \pm(E|\psi\rangle)$

$+$ if E, G_i commute
$-$ " " anticommute

- So meas $G_1 \ldots G_{n-k}$ gives $n-k$ "parity check bits" concerning whether the error com/anti with them.

eg. 9 bit Shor code, $n=9$, $K>8$

$G_1 = XXX\ XXX\ III$ ← matching ± signs in blocks 1,2
$G_2 = III\ XXX\ XXX$ ← " " " 2,3

$G_3 = ZZI\ III\ III$ ← qubits 1,2 in each parity
$G_4 = IZZ\ III\ III$ " " 2,3 " "
(Note $G_3 \cdot G_4$ not an independent generator)

G_5 ⊥ ZZI III ⊥
G_6 ⊥ IZZ ⊥

G_7 ⊥ ⊥ ZZI
G_8 ⊥ ⊥ IZZ

eg Y_4 gives a syndrome: − − + + − + + +

Z_1 : − + + + + + + + } degenerate.
Z_2 : same as above
Z_3 : − − − − − − − }

Back to $N_{\vec{q}}^{\otimes n}$:

Each $N_{\vec{q}}$ is associated with a draw from I, X, Y, Z w.p. q_0, q_1, q_2, q_3.

$N_{\vec{q}}^{\otimes n}$ is n iid draws.

There are 4^n outcomes, corresponding to the 4^n Kraus ops.

Let T = set of typical outcomes, $|T| \approx 2^{n(H(\vec{q})+\delta)}$.

$$\therefore N_{\vec{q}}^{\otimes n}(\rho) = \sum_{E \in T} E \rho E^\dagger p_E + \varepsilon_n \Lambda(\rho)$$

Vanishes ↓ $= \dfrac{\sum_{E \in T} E \rho E^\dagger p_E}{\sum_{E \in T} p_E}$ (TCP map)

Lemma:

Let C be a random stabilizer code with $n-k$ generators

Then $\Pr_{C} \Pr_{E \in T} \left(\exists F \in T \text{ s.t. } E, F \text{ have same syndromes} \right)$

$$\leq \underbrace{2^{n(H(\vec{p})+\delta n)}}_{\text{union bdd over } F} \cdot \underbrace{2^{-(n-k)}}_{\Pr_C(EF \neq I \text{ com with all generators for a fixed } EF)}$$

E if both com or both anti com with G
$\Leftrightarrow$ EF com with G

- Given the Lemma, $\exists$ code C_0 s.t.

$$\Pr_{E \in T} \left[\exists F \in T \text{ s.t. } E, F \text{ have same syndromes} \right)$$

$$\leq 2^{n(H(\vec{p})+\delta n)} \cdot 2^{-(n-k)} = \epsilon_n'$$

- For $k \leq n(1 - H(\vec{p}) - \delta n)$, $\epsilon_n' \to 0$.
- With prob $\geq 1 - \epsilon_n - \epsilon_n'$, error E has unique syndrome and can be identified & inverted (all E are unitary here).

$\therefore r = \frac{k}{n} = 1 - H(\vec{p})$ achievable as $n \to \infty$.

- Note: for non degenerate code, $r = 1 - H(\vec{p})$ optimal by the Quantum Hamming Bound:

$$\#\text{Errors} \times \text{Code dim} \leq \text{dim of output space}$$

$$2^{H(\vec{p})n} \times 2^{k} \leq 2^{n}$$

$$\frac{k}{n} \leq 1 - H(\vec{p})$$

Pf (lemma):

$$\Pr_{C}\ \Pr_{E \in T}\ (\exists f \in T,\ E \neq F,\ E, f \text{ have same syndromes})$$

$$= \Pr_{E \in T}\ \Pr_{C}\ (\exists f \in T,\ E \neq F,\ E, f \text{ have same syndromes})$$

- Note E, F have same syndromes

  $\Leftrightarrow$ $\forall\ i = 1, 2, \ldots, n-k$, E, F both commute with G_i

  or E, F both anti-commute with G_i

  $\Leftrightarrow$ $\forall\ i = 1, 2, \ldots, n-k$, EF commute with G_i

- So, fix $EF \neq I$.

  ① Count # of ways to pick $G_1, G_2, \ldots, G_{n-k}$

  ② Repeat ① imposing also each G_i commute with EF.

- # ①: $2^{2n}-1$ choices for G_1 $(G_1 \neq I)$

  $\frac{2^{2n}}{2} - 2$ ---- G_2 ($2^{2n}/2$ Paulis commute with G_1, take out I, G_1.)

  $\frac{2^{2n}}{2^2} - 2^2$ ---- G_3 ($2^{2n}/2^2$ Paulis commute with G_1, G_2, take out $\langle G_1, G_2 \rangle$)

  $\vdots$

  $\frac{2^{2n}}{2^{n-k-1}} - 2^{n-k-1}$ ---- G_{n-k}

  ↑ See Appendix 2 lec 12, 2010 last 5 pages.

- $\#(\Sigma) = \frac{2^{2n}}{2} - 1$ choices for G_1 ($G_1 \neq I$, G_1 commute with EF)

$\frac{2^{2n}}{2^2} - 2$ ... G_2 ($G_2 \notin \langle G_1 \rangle$, G_2 com G_1, EF)

$\vdots$

$\frac{2^{2n}}{2^{n-k}} - 2^{n-k-1}$ ... G_{n-k}.

- $\Pr_C$ (EF commute with all $G_1 \cdots G_{n-k}$)

$= \frac{\#(\Sigma)}{\#(U)} = \frac{\frac{2^{2n}}{2} - 1}{2^{2n} - 1} \times \frac{\frac{2^{2n}}{2^2} - 2}{\frac{2^{2n}}{2} - 2} \times \cdots \times \frac{\frac{2^{2n}}{2^{n-k}} - 2^{n-k-1}}{\frac{2^{2n}}{2^{n-k-1}} - 2^{n-k-1}}$

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

- $\Pr_{E \in T} \Pr_C$ ($\exists F \in T$, $E \neq F$, EF commutes with $G_1 \cdots G_{n-k}$)

$\leq \Pr_{E \in T}$ [($\#F \in T$) $\times$ (for fixed F, $\Pr$ EF commutes with $G_1 \cdots G_{n-k}$)]

Union over F

$\leq \Pr_{E \in T} 2^{n(H(\vec{p}_E) + \delta n)} \times 2^{(n-k)} \leq 2^{n(H(\vec{p}_F) + \delta n)} \cdot 2^{(n-k)}$.

Special case of random Pauli channel:

Depolarizing channel:

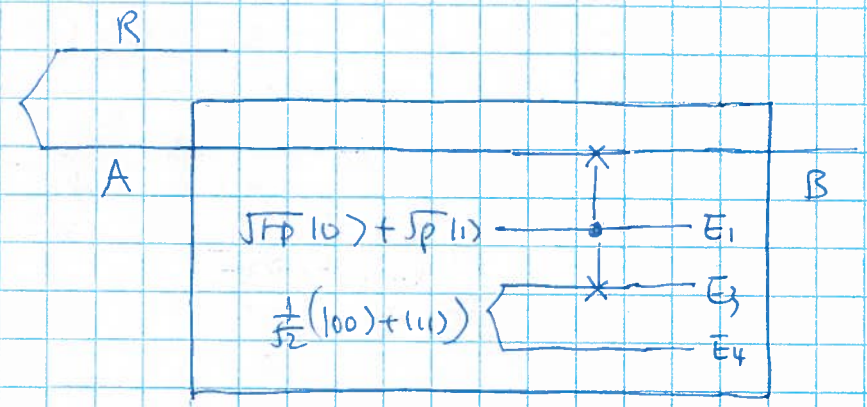
$$N_q(\rho) = (1-q)\rho + \frac{q}{3}\left[X\rho X + Y\rho Y + Z\rho Z\right] \qquad \left(q_0 = 1-q,\ q_1 = q_2 = q_3 = \tfrac{q}{3}\right)$$

$$= \left(1 - \tfrac{4}{3}q\right)\rho + 4\tfrac{q}{3}\underbrace{\left[\rho + X\rho X + Y\rho Y + Z\rho Z\right]\tfrac{1}{4}}_{\frac{I}{2}\ \text{for all}\ \rho}$$

$$= (1-p)\rho + p\,\frac{I}{2} \qquad \text{where } p = \tfrac{4}{3}q,$$

so $q_0 = 1 - \frac{3}{4}p$, $q_1 = q_2 = q_3 = \frac{p}{4}$

Alternative isometric extension:



NB: Replacing $\left(\sqrt{1-p}\,|0\rangle + \sqrt{p}\,|1\rangle\right)_{E_1}$ by $\left(\sqrt{1-p}\,|00\rangle + \sqrt{p}\,|11\rangle\right)_{E_1E_2}$ and giving E_2 to B turns N_p to erasure channel. E_p.

N_p (Bob has no info about whether error occurs)

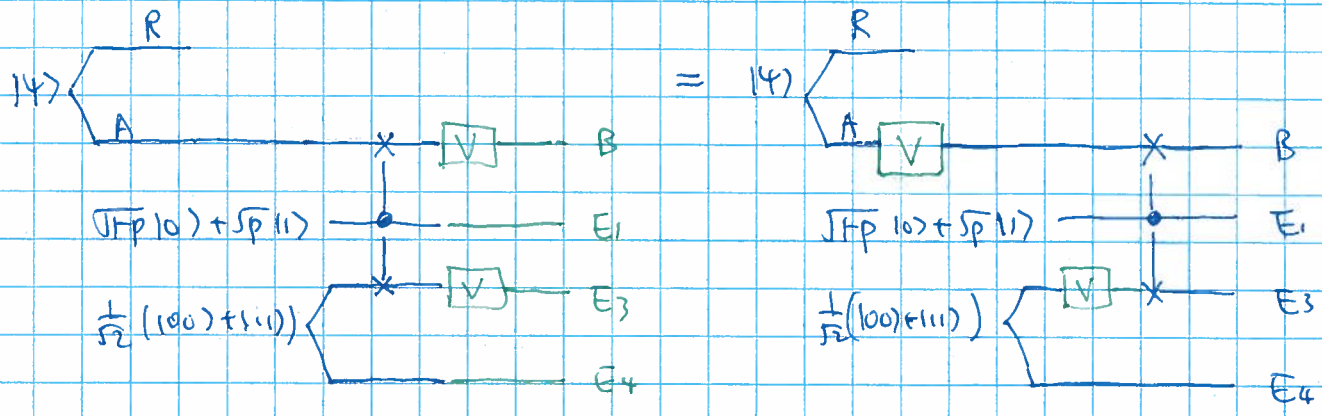
E_p (Bob & Eve each knows if error occurs)

N_p^c (Eve has all info about whether error occurs).

Due to the symmetry of N_q, we can evaluate $Q^{(1)}(N_q)$ and the optimal state.

First we show that optimal input on A is diagonal WLOG.

Pf #1: $\forall |\psi\rangle_{RA}$, $\forall V \in \mathbb{U}(2)$, the following holds:



Isometric extension of N_q acting on $|\psi\rangle_{RA}$

local unitaries keeping $I_c(R\rangle B)$ invariant

$V \otimes V$ commutes with SWAP and with I on $B E_3$.

Also V on E_3 = V^T on E_4 so it does not affect the channel nor $I_c(R\rangle B)$.

So $I_c(R\rangle B)_{I \otimes N_q(|\psi\rangle\langle\psi|)}$ is inv under the unitary V acting on A.

So $|\psi\rangle_{RA} = \sqrt{1-\alpha}\,|00\rangle + \sqrt{\alpha}\,|11\rangle$ WLOG.

Pf #2: (more like Pf #1 in equations)

Let $|\psi\rangle_{RA} = \sqrt{1-\alpha}\,|0\rangle_R|e_0\rangle_A + \sqrt{\alpha}\,|1\rangle_R|e_1\rangle_A$

where $\{|e_0\rangle, |e_1\rangle\}$ is a basis for A.

$$|\psi\rangle\langle\psi|_{RA} = (1-\alpha)\,|0\rangle\langle 0| \otimes |e_0\rangle\langle e_0| + \alpha\,|1\rangle\langle 1| \otimes |e_1\rangle\langle e_1|$$
$$+ \sqrt{1-\alpha}\sqrt{\alpha}\left(|0\rangle\langle 1| \otimes |e_0\rangle\langle e_1| + |1\rangle\langle 0| \otimes |e_1\rangle\langle e_0|\right)$$

$$\rho_{RB} = I \otimes N_f(|\psi\rangle\langle\psi|)$$
$$= (1-p)\left[(1-\alpha)\,|0\rangle\langle 0| \otimes |e_0\rangle\langle e_0| + \alpha\,|1\rangle\langle 1| \otimes |e_1\rangle\langle e_1| + \sqrt{1-\alpha}\sqrt{\alpha}\,(|0\rangle\langle 1| \otimes |e_0\rangle\langle e_1| + |1\rangle\langle 0| \otimes |e_1\rangle\langle e_0|)\right]$$
$$+ p\left[(1-\alpha)\,|0\rangle\langle 0| + \alpha\,|1\rangle\langle 1|\right] \otimes \frac{I}{2}$$

(which is $|e_0\rangle\langle e_0| + |e_1\rangle\langle e_1|$)

So, $I \otimes N_f(I \otimes V|\psi\rangle\langle\psi|I \otimes V^\dagger)$

$= (I \otimes V)\; I \otimes N_f(|\psi\rangle\langle\psi|)\; (I \otimes V^\dagger)$

So $I_c(R\rangle B)_{I \otimes N_f(|\psi\rangle\langle\psi|)}$ inv under V acting on A.

Together, $I_c(R\rangle B)$ unchanged by any V acting on A.

So, choose V to turn the Schmidt basis of $|\psi\rangle_{RA}$ to be the computation basis on A.

$\therefore$ WLOG, $|\psi\rangle_{RA} = \sqrt{1-\alpha}\,|00\rangle + \sqrt{\alpha}\,|11\rangle$

$$\rho_B = \begin{bmatrix} 1-\alpha & 0 \\ 0 & \alpha \end{bmatrix}(1-p) + \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} p$$

$$\rho_{RB} = \begin{bmatrix} 1-\alpha & 0 & 0 & \sqrt{1-\alpha}\sqrt{\alpha} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{1-\alpha}\sqrt{\alpha} & 0 & 0 & \alpha \end{bmatrix}_{RA}(1-p) + \begin{bmatrix} 1-\alpha & 0 \\ 0 & \alpha \end{bmatrix}_R \otimes \frac{I}{2}_B \; p.$$

$$I_c(R\rangle B)_{I\otimes N_q(|+\rangle\langle+|)} = S(\rho_B) - S(\rho_{RB}).$$

If $H(\vec{q}) \le 1$, then above maximized by $\alpha = \frac{1}{2}$,

$H\left(1-q, \frac{q}{3}, \frac{q}{3}, \frac{q}{3}\right)$

$|\psi\rangle_{RA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$S(\rho_B) = 1$

$S(\rho_{RB}) = H(\vec{q})$ (ρ_{RB} = mixture of 4 Bell states with weight $1-q, \frac{q}{3}, \frac{q}{3}, \frac{q}{3}$).

$Q^{(1)}(N_{\vec{q}}) = 1 - H(\vec{q})$.

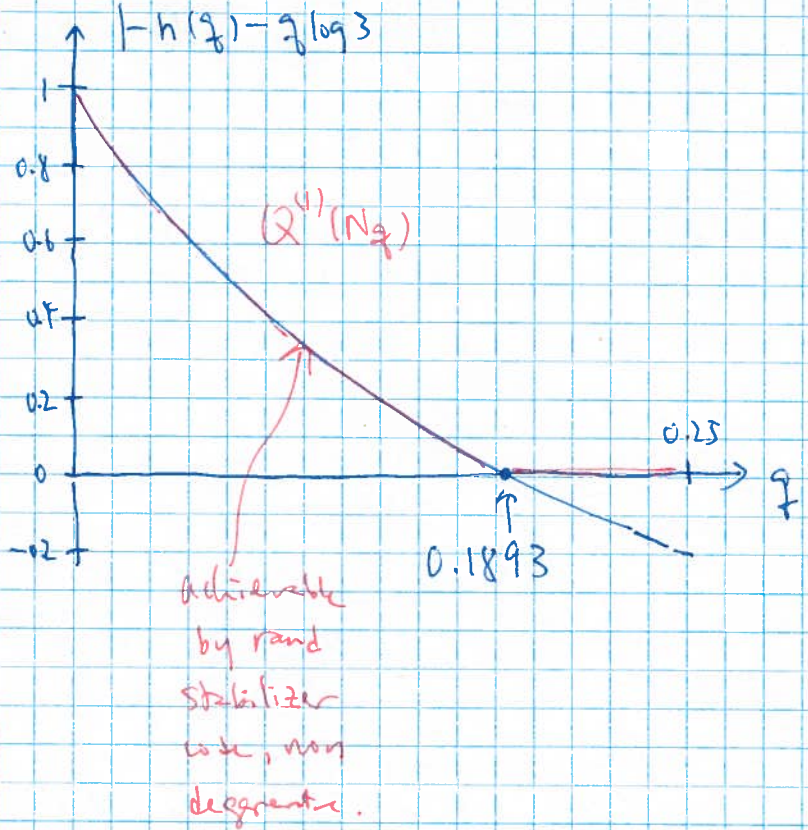
$= -(1-q)\log(1-q) - q\log\frac{q}{3}$

$= h(q) + q\log 3.$

$= 1 - h(q) - q\log 3.$

If $H(\vec{q}) > 1$, then max by $\alpha = 1$.

$Q^{(1)}(N_{\vec{q}}) = 0.$


$1-h(q)-q\log 3$
1
0.8
0.6
0.4
0.2
0
-0.2
$(Q^{(1)}(N_q))$
0.125
q
0.1893
achievable by rand stabilizer code, non degenerate.