Lecture 13, Jun 17, 2010

Note Title 16/06/2010

Last time:

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

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

$$Q^{(1)}(N_{\vec{q}}) = 1 - H_{\vec{q}}$$, achieved by non degenerate stabilizer code (via a randomized argument)

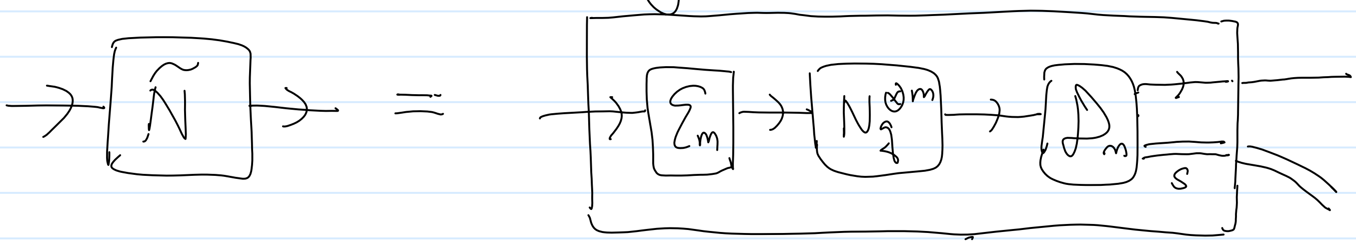
Note no nondegenerate code can beat the above rate since to identify the errors, the syndrome takes $nH_{\vec{q}}$ bits to describe, By Holevo's bdd, it takes $nH_{\vec{q}}$ qubits to extract that info, which has to be indep of the actual quantum data.

$\therefore$ Superadditivity of $Q^{(1)}(N_{\vec{q}})$ requires degenerate codes.

Focus on N_q now:

When $q \geq q_c = 0.1893$, $Q^{(1)}(N_q) = 0$ & quantum data rate $= 0$ using nondegenerate codes.

Idea: Consider a small degenerate code with block length m.
The encoding & decoding induce a new channel



which is a distribution of channels N_q^s & receiver knows which.

Hope: average N_q^s is better than N_q.

☆ It takes m uses of N_q to make 1 $\tilde{N}$!, comm rate $\sim \frac{1}{m}$.

But for q s.t. $Q^{(1)}(N_q) = 0$, any nonzero rate of $\tilde{N}$ gives a strict improvement.

eg Take $q = 0.1894 \underset{\neq}{>} q'$.

$m=5$, $\mathcal{E}_m$ takes $\alpha|0\rangle+\beta|1\rangle$ to $\alpha|0\rangle^{\otimes 5} + \beta|1\rangle^{\otimes 5}$.

Intuition to try this code: single qubit Z errors are degenerate.

The stabilizers for this code: $ZZIII$
$ZIZII$
$ZIIZI$
$ZIIIZ$

The syndrome is a 4-bit string saying if the 2^{nd}, 3^{rd}, 4th, 5th qubits have been flipped relative to the first.

$\therefore$ 16 syndromes (for a total of $4^5 = 1024$ errors).

(5 too small for typicality to help).

each w/ 64 possible errors causing it

Z Z I I I
Z I Z I I
Z I I Z I
Z I I I Z

e.g. if s = ++++, we make no correction and decode.

The actual error can be:
I I I I I, XXXXX, Z I I I I, I Z I I I, I I Z I I, I I I Z I, I I I I Z, + what they generate multiplicatively.
i.e: 32 possible errors with only I/Z, 32 possible errors with only X/Y.

(1) I I I I I and any even weight Z error gives a logical I.
(2) any odd weight Z error gives a logical Z.
(3) any X/Y type error with even weight #Y's gives a logical X.
(4) any X/Y type error with odd weight #Y's gives a logical Y.

Pr(s=++++) = prob of no X/Y + prob of no I/Z = (1-2q/3)^5 + (2q/3)^5 = 0.50924

(n-C-k) := (n-choose-k)

Pr(1) = (1-q)^5 + (5-C-2) (1-q)^3 * (q/3)^2 + (5-C-4) (1-q)^1 * (q/3)^4 = 0.37127
Pr(2) = (5-C-1) (1-q)^4 * (q/3) + (5-C-3) (1-q)^2 * (q/3)^3 + (q/3)^5 = 0.13794
Pr(3) = (2q/3)^5 [1 + (5-C-2) + (5-C-4)] = 0.000016
Pr(4) = (2q/3)^5 [(5-C-1) + (5-C-3) + (5-C-5)] = 0.000016

The decoded channel is a random Pauli channel with

qx = qy = 0.000016/0.50924 = 0.0000315

qz = 0.27088, qi = 0.72906 H(q) = 0.84373 < 1.

e.g. if s = -+++, mostly likely error IXIII. Bob reverts it and decodes.

Z Z I I I
Z I Z I I
Z I I Z I
Z I I I Z

The set of possible errors is IXIII * set of errors giving the ++++ syndrome.

(1) IXIII * (I I I I I and any even weight Z error) gives a logical I.
(2) IXIII * (any odd weight Z error) gives a logical Z.
(3) IXIII * (any X/Y type error with even weight #Y's) gives a logical X.
(4) IXIII * (any X/Y type error with odd weight #Y's) gives a logical Y.

(1): IXIII * (IIIII, ZZIII, IZZII, IZIZI, IZIIZ, 6 cases of 2 Z's not on 2nd qubit,
ZIZZZ, 4 cases of 4Z's one of which is on 2nd qubit)
(2): IXIII * (IZIII, 4 cases of 1Z's not on 2nd qubit, 6 cases of 3Z's involving 2nd qubit,
4 cases of 3Z's not involing 2nd qubit, ZZZZZ)
(3): IXIII * (XXXXX,6 cases of 3X's and 2Y's with X on 2nd qubit, 4 cases with Y on 2nd qubit
YXYYY, 4 cases of 1X not on 2nd qubit)
(4): IXIII * (XYXXX, 4 cases of 1Y not on 2nd qubit,
6 cases of 2X's & 3Y's with Y on 2nd qubit, 4 cases with X on 2nd qubit, YYYYY)

Pr(s=+-++) = 0.0738

Pr(1) = pr(1error) + 4 * pr(2errors) + 6 * pr(3errors) + pr(5errors) + 4 * pr(4errors) = 0.0368
Pr(2) = pr(1error) + 4 * pr(2errors) + 6 * pr(3errors) + 4 * pr(4errors) + pr(5errors) = 0.0368
Pr(3) = pr(4errors) + 6 * pr(4errors) + 4 * pr(5errors) + pr(4errors) + 4 * pr(5errors) = 0.00011
Pr(4) = pr(5errors) + 4 * pr(4errors) + 6 * pr(5errors) + 4 * pr(4errors) + pr(5errors) = 0.00011

The decoded channel is a random Pauli channel with

$q_i = q_z = 0.0368/0.0738 = 0.4985$

$q_x = q_y = 0.00011/0.0738 = 0.0015$ $\qquad H(q) = 1.0295 > 1.$

By symmetry, the 5 syndromes -+++, +-++, ++-+, +++-, ---- are similar to the above.

Repeating for all 16 syndromes ...

The average H(q) over all syndromes

$= 0.50924 * 0.84373 + 0.0738 * 1.0295 * 5 + \ldots \approx \boxed{1 - 0.001}$ (rough estimate)

The same code results in average $\boxed{H(q) < 1}$ up until q = 0.1904.

Reference: Shor-Smolin 9604006.

or the expanded DiVincenzo Shor Smolin 9706061.

Idea: a random stabilizer code can now be used on $\tilde{N}$

Note a subtlety — we calculate the average entropy for the decoded syndrome-labeled N_q^s's, but only Bob knows the syndrome.

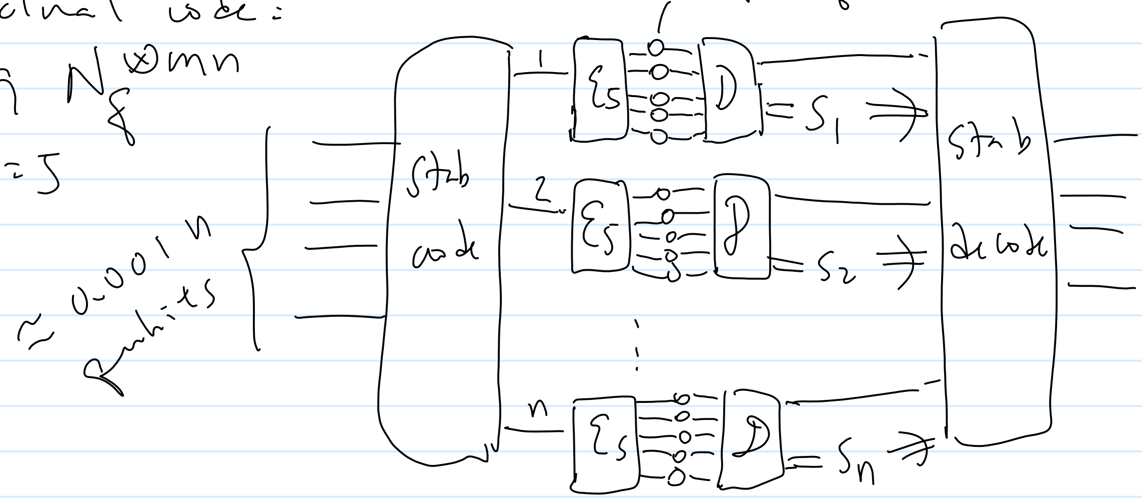
Luckily, Alice need not know the syndrome of each 5-qubit block. The random stabilizer code works as long as

$$\#\text{errors to be distinguished} \times 2^{-\text{"}n-k\text{"}} \ll 1$$

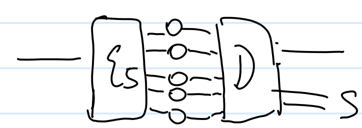
$\therefore$ The average $(1-H(\vec{q}))$ for the decoded 5-qubit code blocks is an appropriate value for $\frac{k}{n}$!

The actual code: using $N_q \otimes mn$ for $m=5$

N_q for $q = 0.1894$



The $m=5$ code



is often called the inner code.

Note that if $\rho_{RB} = \sum_s \rho_{s\,RB_1} \otimes |s\rangle\langle s|_{B_2}\, p_s$

then $I(R\rangle B)_{\rho_{RB}} = (S_B - S_{RB})_{\rho_{RB}}$

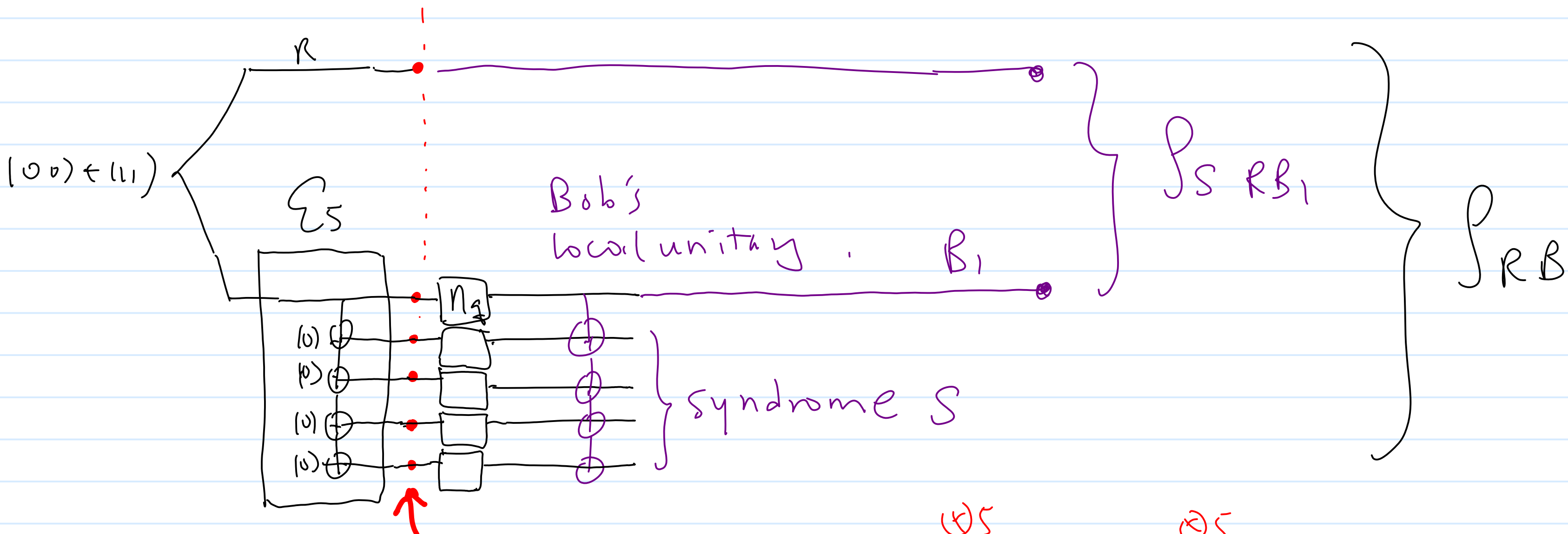
$$= \left[H(p_s) + \sum_s (S_{B_1})_{\rho_{s\,RB_1}} p_s \right] - \left[H(p_s) + \sum_s (S_{RB_1})_{\rho_{s\,RB_1}} p_s \right]$$

$$= \sum_s p_s \, I(R\rangle B_1)_{\rho_{s\,RB_1}}$$

• An alternative interpretation of the Shor–Smolin code:

For N_q w/ $q = 0.1894$ & $Q^{(1)}(N_q) = 0$

the Shor–Smolin code is a description of an input $|\psi\rangle_{RA}$ into $N_q^{\otimes 5}$ that lower bound $Q^{(5)}(N_q)$ as follows:



A particular input to $N_q^{\otimes 5}$, which is $|0\rangle_R |0\rangle^{\otimes 5} + |1\rangle_R |1\rangle^{\otimes 5}$

and $Q^{(5)}(N_f) = \frac{1}{5} Q^{(1)}(N_f^{\otimes 5})$

$$\geq \frac{1}{5} I_c(R\rangle B)_{\rho_{RB}} = \frac{1}{5}\sum_s p_s \, I_c(R\rangle B)_{\rho_{sRB}},$$

$$= \frac{1}{5}\sum_s p_s \left[1 - H(\vec{\xi}_s)\right] > 0.0002$$

but $Q^{(1)}(N_f) = 0$ $\therefore$ $Q^{(1)}(N)$ not additivity

- We can also use any of our favorite random code for $N_f^{\otimes 5}$ based on the above lower bdd on $Q^{(1)}(N_f^{\otimes 5})$

Further thoughts :

- for N_q with $q \geq 0.1893$

* for the most likely syndrome $++++$ (prob ≈ 0.51)

  the decoded channel has $q_z = 0.27$, $q_x \simeq q_y \simeq 10^{-5}$

* for the 2nd most likely syndromes $----$ or $-+++$, $+-++$, $++-+$, $+++-$

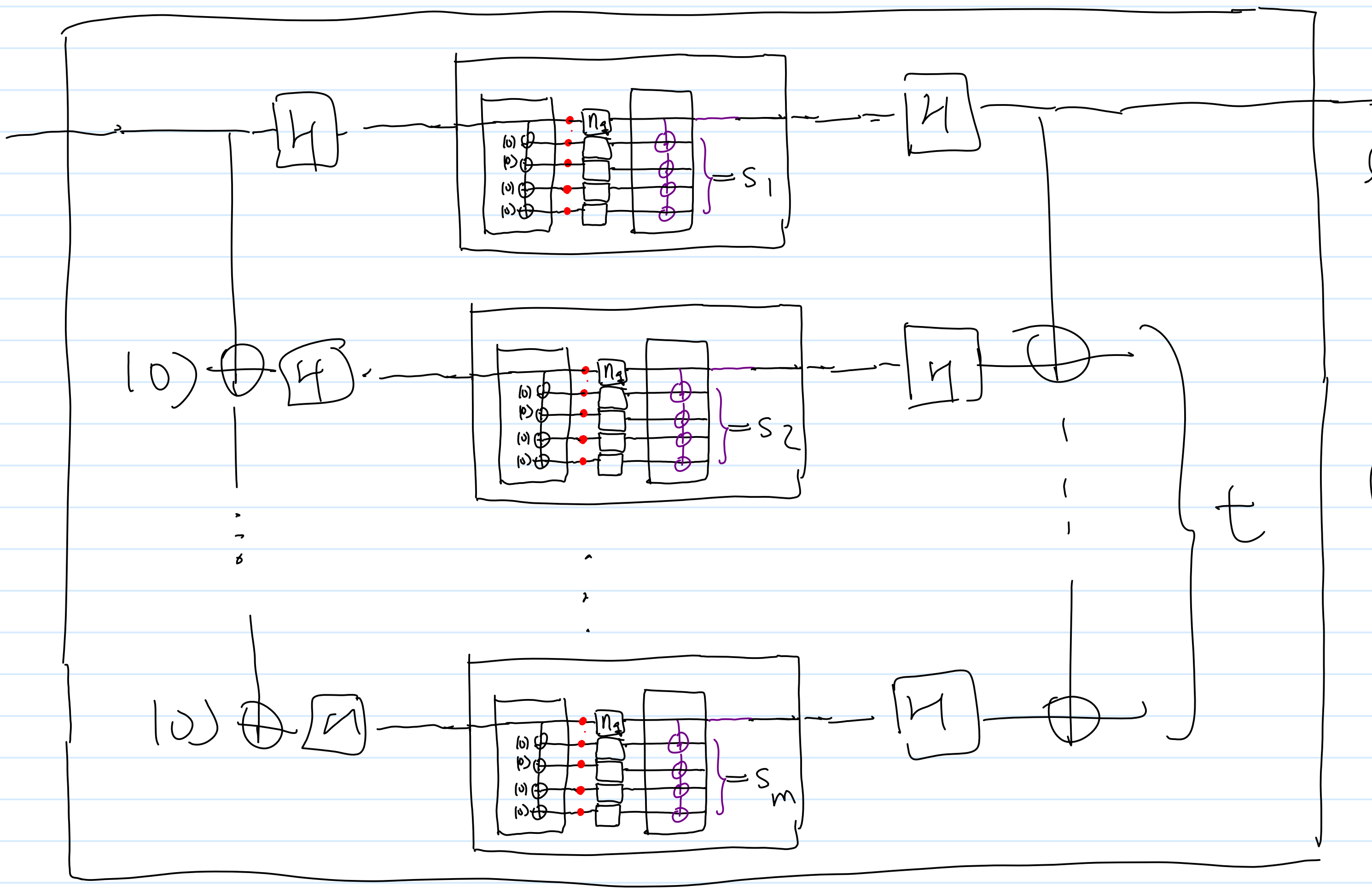
  (combined prob ≈ 0.37)

  the decoded channel has $q_z = 0.4985$, $q_x = q_y \approx 10^{-3}$

The rep code is very good to catch X errors but makes the phase error much worse (any 1 in 5 qubit have Z error results in encoded Z error).

Instead of random code — much better to concatenate a rep code in the $|\pm\rangle$ basis (Smith-Smolin 0604107)

ie



eg $m=16$

$Q^{(80)}(N_g)>0$

for $g<0.19088$

(0.1904 before).

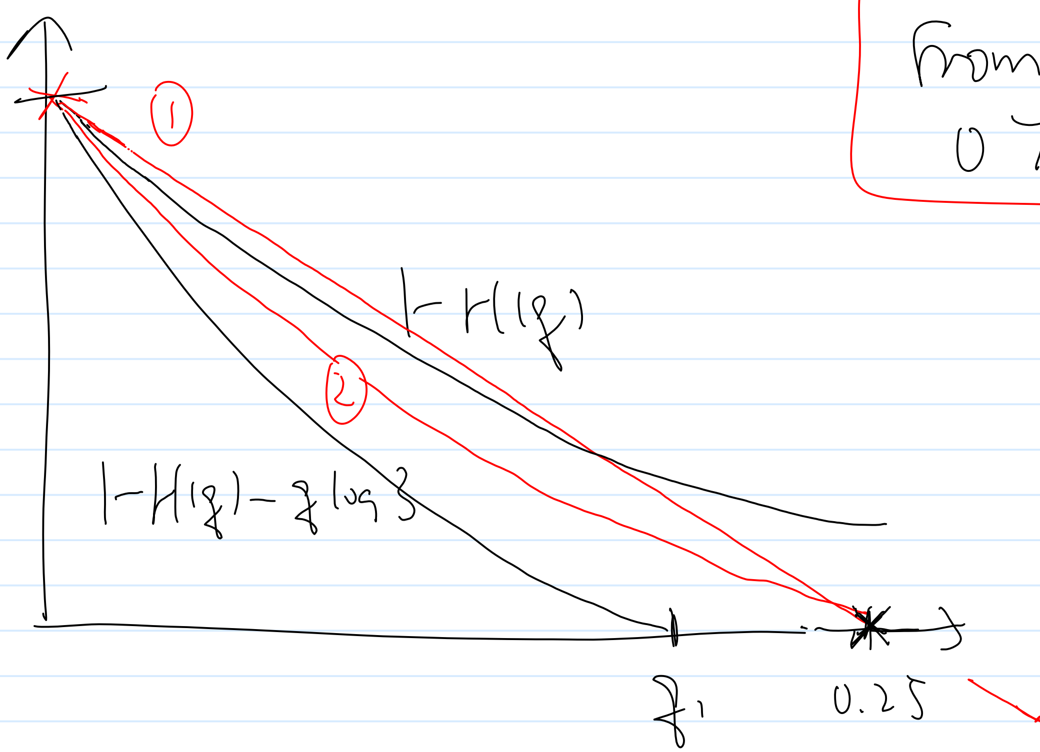
Many other random Pauli channels with $H(\vec{p}) > 1$
also have $Q^{(m)}(N_{\vec{p}}) > 0$ by using one inner
repetition code, followed by another rep code
in the conjugate basis (& alternate for a while).

Other inner codes were studied numerically in 0708.1597
(Fern & Whaley).

④ Upper bounds on $Q(N)$.

(i) N_q antidegradable when $q = \frac{1}{4}$ (9705038)

(ii) $Q(N_q) \le 1 - H(q)$ (Rains 0008047 (or 5.7))



From Smith-Smolin
0712.2471

Ideas:

Thm 1

Given N, if $\boxed{\exists\, S, T \text{ s.t. } N = S \circ T \quad -\boxed{N}- = -\boxed{S}-\boxed{T}-}$ & $\boxed{Q(T) = Q^{(1)}(T)}$

then $Q(N) \leq Q^{(1)}(T)$

Terminology: T is called an additive extension of N

If T is degradable, it's called a degradable extension of N, in which case private capacity $\leq Q^{(1)}(T)$ also.

Reason for $Q(N) \le Q^{(1)}(T)$

$Q(T)^{(1)} = Q(T)$ by hypothesis

$$= \sup_n \frac{1}{n} \max_{|\psi\rangle} I(R\rangle B^{\otimes n})_{I \otimes T^{\otimes n}(|\psi\rangle\langle\psi|)}$$

$$\ge \sup_n \frac{1}{n} I(R\rangle B^{\otimes n})_{I \otimes T^{\otimes n}} \underbrace{(|\psi^*\rangle\langle\psi^*|)}_{\text{op for } Q(N)}$$

Operating on $B^{\otimes n}$ by $S^{\otimes n}$

cannot increase $I_c(R\rangle B^{\otimes n})$

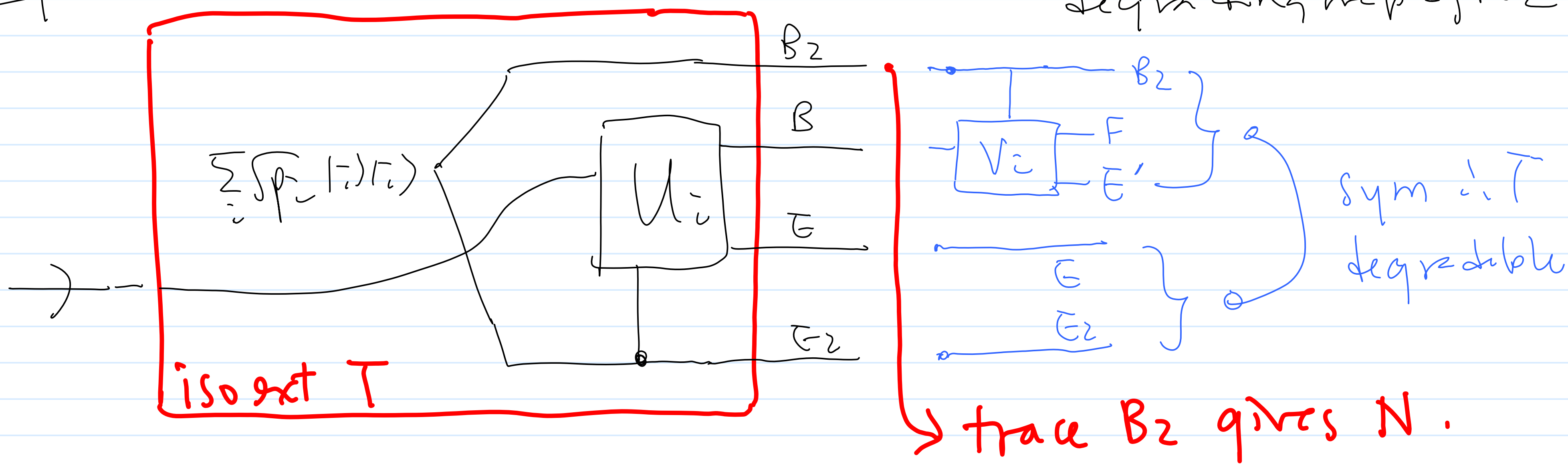
$$\ge \sup_n \frac{1}{n} I(R\rangle B^{\otimes n})_{I \otimes \underbrace{(S \circ T)}_{N}^{\otimes n}(|\psi^*\rangle\langle\psi^*|)} = Q(N)$$

Thm 2 If $N = \sum_i p_i N_i$, each N_i degradable

then $T = \sum_i p_i N_i \otimes |i\rangle\langle i|$ is a deg ext of N

& $Q(N) \leq \sum_i p_i Q^{(1)}(N_i)$

Pf: Let U_i be the iso ext of N_i, V_i be that of the degrading map of N_i



$$Q^{(1)}(T) = \max_{|\psi\rangle_{RA}} I_c(R \rangle B_2 B)_{I\otimes T(|\psi\rangle\langle\psi|_{RA})}$$

$$I \otimes T(|\psi\rangle\langle\psi|_{RA}) = \sum_i p_i \underbrace{(I \otimes N_i)(|\psi\rangle\langle\psi|)_{RB}}_{\rho_{i\,RB}} \otimes |i\rangle\langle i|_{B_2}$$

$$\therefore\ I_c(R \rangle B_2 B)_{I\otimes T(|\psi\rangle\langle\psi|)} = \sum_i p_i I_c(R \rangle B)_{I\otimes N_i(|\psi\rangle\langle\psi|)}$$

$$\leq \sum_i p_i Q^{(1)}(N_i)$$

eg. $N(\rho) = 0.8\,\rho + 0.15\, X\rho X$
$\quad + 0.04\, Y\rho Y + 0.01\, Z\rho Z$

$$N(\rho) = \frac{3}{5}\left(\frac{3}{4}\rho + \frac{1}{4}X\rho X\right) + \frac{1}{5}\left(\frac{4}{5}\rho + \frac{1}{5}Y\rho Y\right) + \frac{1}{5}\left(\frac{19}{20}\rho + \frac{1}{20}Z\rho Z\right)$$

$H(\frac{1}{4}) = 0.8113$, $H(\frac{1}{5}) = 0.7219$, $H(\frac{1}{39}) = 0.2864$

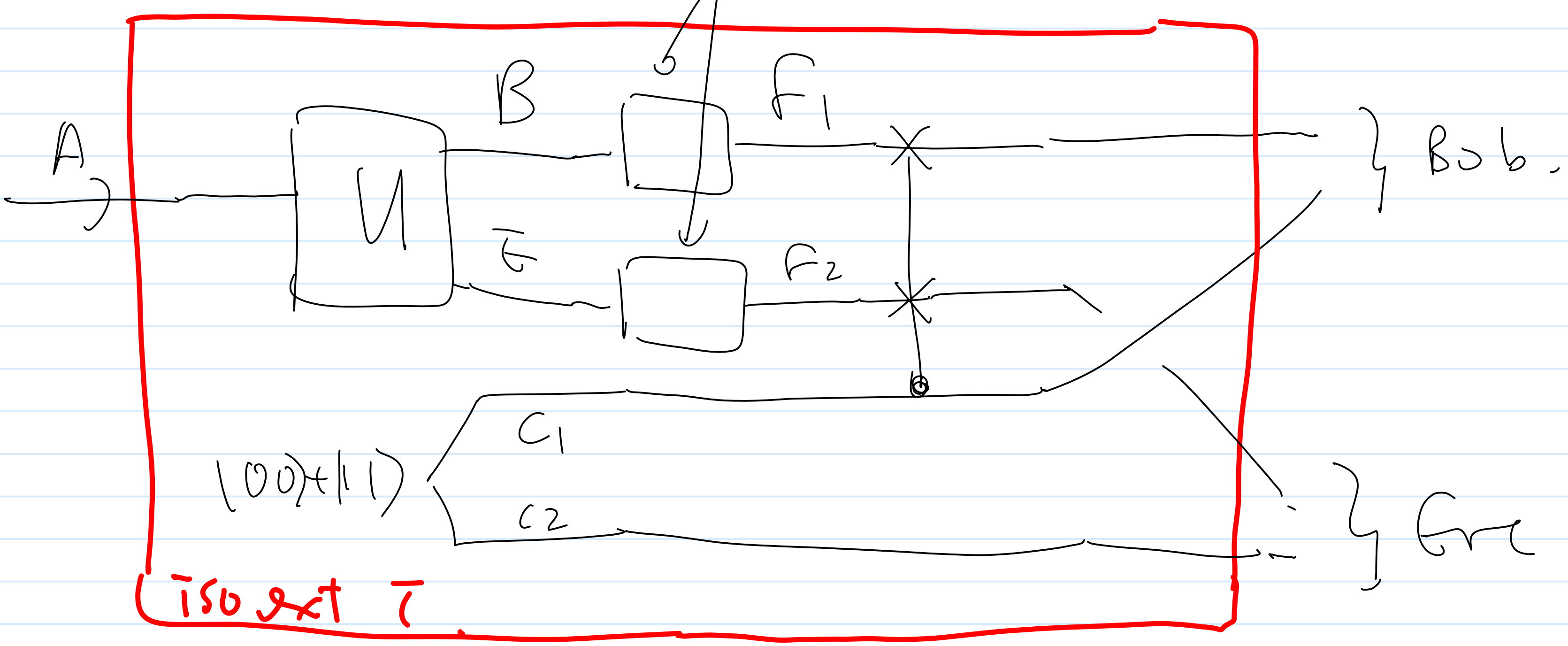
$$Q(N) \leq 0.6(1-0.8113) + 0.2\times(1-0.7219) + 0.2(0.2864)$$
$$= 0.3116.$$

$$Q^{(1)}(N) = 1 - H(\vec{p}) = 0.0797.$$

Thm 3 If N antidegradable, it has an antidegrable & degradable extension T

Pf let U be the iso extension for N

embed into $d = \max(d_B, d_E)$ dims



T clearly sym w.r.t. Bob & Eve.

T is an extension of N:

Def S in which Bob use C_1 to "control degrade" F_1. i.e. if $C_1 = 0$, do nothing, if $C_1 = 1$, $F_1 = E$ & D is applied (D degrades N^c to N). Then discard C_1.

Now Bob is left with output of N.

Thm 4 If $\mathcal{T}_0$ deg ext of $\mathcal{N}_0$

$\mathcal{T}_1$ " " " $\mathcal{N}_1$

then $\mathcal{T} = p\,\mathcal{T}_0 \otimes |0\rangle\langle 0| + (1-p)\,\mathcal{T}_1 \otimes |1\rangle\langle 1|$

is a deg ext of $\mathcal{N} = p\,\mathcal{N}_0 + (1-p)\,\mathcal{N}_1$

& $Q^{(1)}(\mathcal{T}) \leq p\, Q^{(1)}(\mathcal{T}_0) + (1-p)\, Q^{(1)}(\mathcal{T}_1)$