Lecture 3

Quantum Comm. over Q. Channels

How much quantum data can we send reliably using a quantum channel?

When sending classical data, we quantified performance w/ success probability. Here we use a different measure called <u>fidelity</u>

For pure states, fidelity is

$$F(\psi, \phi) = |\langle\psi|\phi\rangle|^2$$

probability that one state can "fake" being another

$F=1$ iff states are the same

$F=0$ iff states are orthogonal.

Fidelity for mixed states ρ & σ is defined as the maximum overlap wrt all purifications $|\psi^\rho\rangle$ & $|\psi^\sigma\rangle$:

$$F(\rho, \sigma) = \max_{|\psi^\rho\rangle, |\psi^\sigma\rangle} |\langle\psi^\rho|\psi^\sigma\rangle|^2$$

can show that

$$F(\rho, \sigma) = \| \sqrt{\rho} \sqrt{\sigma} \|_1^2$$

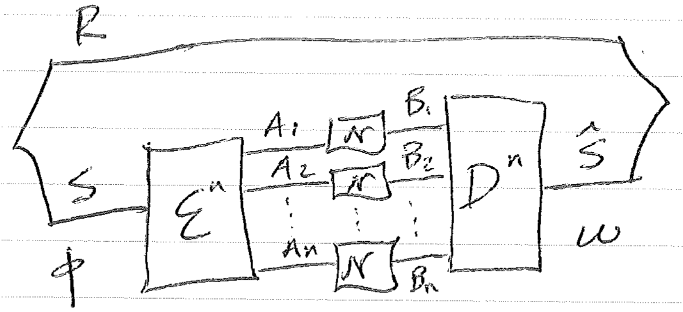
where $\|A\|_1 = \mathrm{Tr}\{\sqrt{A^\dagger A}\}$

fidelity between a pure state ϕ & mixed state ρ is

$$F(\phi, \rho) = \langle\phi|\rho|\phi\rangle$$

---

now we define an (n, Q, ε) protocol for a quantum channel. Again consists of an encoding $\mathcal{E}^n$ & decoding $\mathcal{D}^n$ where



ϕ_{RS} is some pure state &

$$\omega_{R\hat{S}} = D_{B^n \to \hat{S}}\left(\mathcal{N}^{\otimes n}\left(\mathcal{E}_{S \to A^n}\left(\phi_{RS}\right)\right)\right)$$

demand that

$$F(\phi_{RS}, \omega_{R\hat{S}}) = \langle \phi|_{RS}\, \omega_{R\hat{S}}\, |\phi\rangle_{RS} \geq 1 - \varepsilon$$

$\forall$ states ϕ_{RS} in a subspace S of fixed dimension

rate $Q = \frac{1}{n} \log_2 |S|$

---

rate Q is achievable if $\forall \varepsilon > 0$ & sufficiently large n, $\exists$ an (n, Q, ε) protocol.

---

quantum capacity of $\mathcal{N}$ = supremum of all achievable rates $= Q(\mathcal{N})$

First, let's get an upper bound on quantum capacity. To do so, we can suppose that sender & receiver are using the channel to generate maximal entanglement

$$|\Phi\rangle_{R\hat{S}} = \frac{1}{\sqrt{d}} \sum_i |i\rangle_R |i\rangle_{\hat{S}}$$

w/ an (n, Q, ε) protocol.

We will use a quantity called coherent information.

Given a bipartite state ρ_{AB}

$$I(A\rangle B)_\rho = H(B)_\rho - H(AB)_\rho$$

coherent information obeys a data processing inequality:

$$I(A\rangle B_1)_\sigma \geq I(A\rangle B_2)_\tau$$

where $\tau_{AB_2} = (id_A \otimes N_{B_1 \to B_2})(\sigma_{AB_1})$

follows from monotonicity of relative entropy.

coherent information of max. entangled state

$$I(R \rangle \hat{S})_{\Phi} = \log d$$

signature of entanglement.

So this is our first step:

$$\log |\hat{S}| = I(R \rangle \hat{S})_{\Phi}$$

$$\leq I(R \rangle \hat{S})_{\omega} + f(n, \varepsilon)$$

$f(n,\varepsilon)$ is a function such that

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} f(n, \varepsilon) \equiv 0$$

this follows from assumption of an (n, Q, ε) protocol & continuity of entropy.

Next step:

$$I(R \rangle \hat{S})_{\omega} \leq I(R \rangle B^n)$$

quantum data processing

Finally: optimize over all inputs to get an info. quantity which depends only on channel

$$I(R \rangle B^n) \leq I_c(\mathcal{N}^{\otimes n})$$

where $I_c(\mathcal{N}) = \max_{\phi_{RA'}} I(R\rangle B)_\rho$

$$\rho_{RB} = \mathcal{N}_{A\to B}(\phi_{RA})$$

Put it all together to get

$$\log|\hat{S}| \leq I_c(\mathcal{N}^{\otimes n}) + f(n,\varepsilon)$$

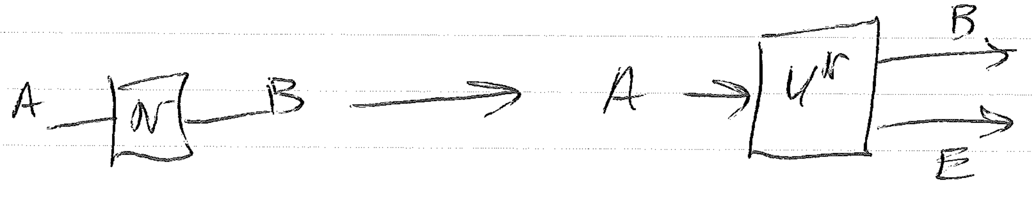
$$\Rightarrow \quad Q = \frac{1}{n}\log|\hat{S}| \leq \frac{1}{n} I_c(\mathcal{N}^{\otimes n}) + \frac{1}{n} f(n,\varepsilon)$$

Take limit as $n \to \infty$ & $\varepsilon \to 0$ to find that

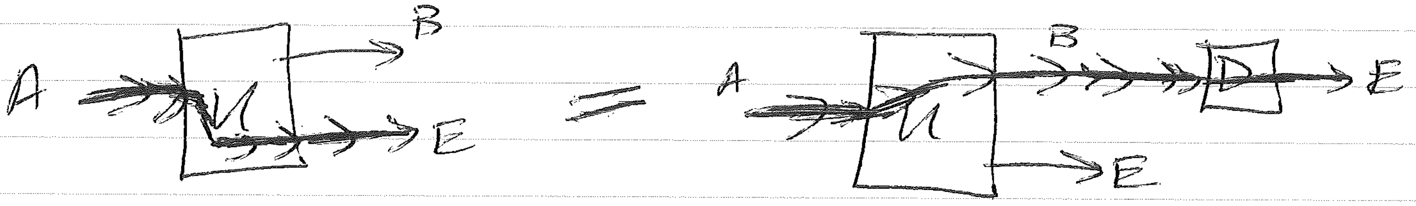
$$Q \leq \underbrace{\lim_{n\to\infty} \frac{1}{n} I_c(\mathcal{N}^{\otimes n})}$$

so this is an upper bound on quantum capacity.

Certain channels are "degradable", meaning that the receiver can always simulate the channel to the environment



For degradable channels, $\exists$ degrading CPTP map $\mathcal{D}_{B\to E'}$ such that



For such channels, one can show that

$$I_c(\mathcal{N}^{\otimes n}) = n\, I_c(\mathcal{N}) \quad \text{\& thus}$$

$$\lim_{n\to\infty} \frac{1}{n} I_c(\mathcal{N}^{\otimes n}) = \underset{\substack{\uparrow \\ \text{can compute this!}}}{I_c(\mathcal{N})}$$

An example of a degradable channel is the qubit dephasing channel:

$$\rho \to (1-p)\rho + p Z \rho Z$$

where Z is Pauli Z.

upper bound is equal to $1 - h_2(p)$ in this case. We will now show that this is achievable using the theory of stabilizer codes

Brief review of stabilizer codes:

Let G'^n denote the Pauli group:

$$G'^n \equiv \{\pm 1, \pm i\} \otimes \{\underbrace{I, X, Y, Z}_{\text{single-qubit Paulis}}\}^{\otimes n}$$

Let $G^n = G'^n / \{\pm 1, \pm i\}$

"phase-free" Pauli group

it has 4^n elements

Let S be an abelian subgroup of G^n

S has size 2^{n-k} for some k such that $0 \leq k \leq n$

S is generated by a set of size $n-k$

$$S = \langle S_1, \ldots, S_{n-k} \rangle$$

A state $|\psi\rangle$ is stabilized by S if

$$S|\psi\rangle = |\psi\rangle \quad \forall\, S \in S$$

- 2^k subspace stabilized by $\mathcal{S}$ is "codespace"
  $[n,k]$ stabilizer code encodes k logical qubits into n physical qubits.

- decoding operation is to measure the $n-k$ stabilizer generators, process this "syndrome", & perform recovery.
- there are methods for encoding (algorithm is analogous to Gaussian elimination.)

What are logical operations on encoded quantum data?

Given by the normalizer, defined as

$$N(\mathcal{S}) = \{ U \in U(2^n) : U \mathcal{S} U^\dagger = \mathcal{S} \}$$

Any $U \in N(\mathcal{S})$ does not take $|\psi\rangle$ in codespace outside of it. Consider that for $U \in N(\mathcal{S})$

$$S U|\psi\rangle = U U^\dagger S U|\psi\rangle = U S_U |\psi\rangle = U|\psi\rangle$$

where $S_U = U^\dagger S U$ & $S_U \in \mathcal{S}$ from normalizer def.

So $U|\psi\rangle$ is in codespace if $U \in N(\mathcal{S})$

Also $\mathcal{S} \subseteq N(\mathcal{S})$ b/c $\forall S_1, S_2 \in \mathcal{S}$

$$S_1 S_2 S_1^\dagger = S_2 S_1 S_1^\dagger = S_2$$

In QEC, we would like to correct a fixed set of errors $\mathcal{E} \subseteq G^n$.

Might not be able to correct all of the errors in a set $\mathcal{E}$ if $\exists$ a pair $E_1, E_2 \in \mathcal{E}$ such that

$$E_1^\dagger E_2 \in N(\mathcal{S})$$

To see this, consider $\forall S \in \mathcal{S}$

$$E_1^\dagger E_2 S = (-1)^{g(S,E_1)+g(S,E_2)} S E_1^\dagger E_2$$

where $g(P,Q)$ is defined by $PQ = (-1)^{g(P,Q)} QP$ $\forall P, Q \in G^n$.

The above then implies

$$(E_1^\dagger E_2) S (E_1^\dagger E_2)^\dagger = (-1)^{g(S,E_1)+g(S,E_2)} S$$

Since we assumed that

$$E_1^\dagger E_2 \in N(S)$$

it must be the case that

$$g(S, E_1) = g(S, E_2) \quad \forall S \in S$$

That is, when Bob measures stabilizer generators when E_1 or E_2 occurs, he gets the same syndrome & cannot distinguish the errors. This is not a problem if $E_1^\dagger E_2 \in S$ because in that case, we have

$$E_1 |\psi\rangle = E_2 |\psi\rangle \quad \forall |\psi\rangle \text{ in codespace}$$

can then do either $E_1^\dagger$ or $E_2^\dagger$ to correct.

But there is a problem if

$$E_1^\dagger E_2 \in N(S) / S$$

So error correcting conditions are that

$\mathcal{E}$ is a correctable set of errors

if $\forall E_1, E_2 \in \mathcal{E}$ we have that

$$E_1^\dagger E_2 \notin N(\mathcal{S}) / \mathcal{S}$$

simple way to satisfy this is to have

$$E_1^\dagger E_2 \notin N(\mathcal{S})$$

so that each error has a unique syndrome. (called non-degenerate code)

Now use this theory to show how to achieve the "hashing bound" for a Pauli channel.

Pauli channel is

$$\rho \to p_I \rho + p_X X \rho X + p_Y Y \rho Y + p_Z Z \rho Z$$

define $\bar{p} = [p_I, p_X, p_Y, p_Z]$ & $H(\bar{p})$ is Shannon entropy of $\bar{p}$.

Can show that the rate $1 - H(\bar{p})$ is achievable.

use the method of random stabilizer coding to correct only the "typical error" set.

define this as

$$T_\delta^{\bar{p}^n} \equiv \left\{ a^n : \left| -\frac{1}{n}\left[\log \Pr\{E_{a^n}\}\right] - H(\bar{p}) \right| \leq \delta \right\}$$

where a^n is a sequence of classical letters corresponding to a Pauli error

$$E_{a^n} = E_{a_1} \otimes \cdots \otimes E_{a_n}$$

w/ $E_{a_i} \in \{I, X, Y, Z\}$.

$\forall \varepsilon > 0$ + sufficiently large n, we have that

$$\sum_{a^n \in T_\delta^{\bar{p}^n}} \Pr\{E_{a^n}\} \geq 1 - \varepsilon$$

From stabilizer error correction conditions, we know for a given code $\mathcal{S}$ that $\{E_{a^n} : a^n \in T_\delta^{\bar{p}^n}\}$ is correctable if

$$E_{a^n}^\dagger E_{b^n} \notin N(\mathcal{S}) / \mathcal{S}$$

$$\forall\ E_{a^n}, E_{b^n} \text{ w/ } a^n, b^n \in T_\delta^{\bar{p}^n}$$

Pick a stabilizer code @ random.

How to do so? Fix $Z_1, \ldots, Z_{n-k}$ + perform a "Clifford" unitary uniformly @ random. (Clifford unitary takes Pauli group to Pauli group under unitary conjugation).

Analyze expectation of the error probability

$$\mathbb{E}_S\{p_e\} = \mathbb{E}_S\left\{\sum_{a^n} \Pr\{E_{a^n}\}\, \mathcal{I}(E_{a^n} \text{ is uncorrectable using } S)\right\}$$

$$\leq \mathbb{E}_S\left\{\sum_{a^n \in T_\delta^{p^n}} \Pr\{E_{a^n}\}\, \mathcal{I}(E_{a^n} \text{ is uncorrectable using } S)\right\} + \varepsilon$$

atypical errors have negligible probability mass.

Now commute $\mathbb{E}_S$ w/ sum

$$= \sum_{a^n \in T_\delta^{p^n}} \Pr\{E_{a^n}\}\, \mathbb{E}_S\{\mathcal{I}(\text{ " })\}$$

$$= \sum_{a^n \in T_\delta^{p^n}} \Pr\{E_{a^n}\}\, \cancel{\mathbb{E}}\, \underbrace{\Pr_S\{E_{a^n} \text{ is uncorrectable using } S\}}_{\text{focus on this term}}$$

$$\Pr_{S}\left\{E_{a^n} \text{ is uncorrectable using } S'\right\}$$

$$= \Pr_{S}\left\{\exists E_{b^n} : b^n \in T_\delta^{\bar{p}^n}, b^n \neq a^n, E_{a^n}^\dagger E_{b^n} \in N(S) / S\right\}$$

$$\leq \Pr_{S}\left\{\exists E_{b^n} : b^n \in T_\delta^{\bar{p}^n}, b^n \neq a^n, E_{a^n}^\dagger E_{b^n} \in N(S)\right\}$$

follows b/c $N(S)$ is larger than $N(S) / S$

$$\leq \sum_{b^n \in T_\delta^{\bar{p}^n}, b^n \neq a^n} \Pr_{S}\left\{E_{a^n}^\dagger E_{b^n} \in N(S)\right\}$$

What is

$$\Pr_{S}\left\{E_{a^n}^\dagger E_{b^n} \in N(S)\right\} \quad ? \quad \text{w/ } b^n \neq a^n$$

code chosen uniformly @ random

total # of non-identity operators for n qubits $= 2^{2n} - 1$

total # of non-identity operators in $N(S) = 2^{n+k} - 1$

(i.e. S has size 2^{n-k} + then 2^{2k} logical operators)

$$\Rightarrow \Pr_{S}\left\{E_{a^n}^\dagger E_{b^n} \in N(S)\right\} \leq \frac{2^{n+k} - 1}{2^{2n} - 1} \leq 2^{-(n-k)}$$

$$\Rightarrow \sum'_{b^n \in T^{\bar{p}^n}_\delta,\, b^n \neq a^n} \Pr_{S} \left\{ E^\dagger_{a^n} E_{b^n} \in N(S) \right\}$$

$$\leq \sum'_{b^n \in T^{\bar{p}^n}_\delta,\, b^n \neq a^n} 2^{-(n-k)}$$

$$\leq 2^{n[H(\bar{p})+\delta]}\, 2^{-(n-k)}$$

size of typical set

$\Rightarrow$ overall bound is

$$\sum_{a^n \in T^{\bar{p}^n}_\delta} \Pr\{E_{a^n}\}\, 2^{n[H(\bar{p})+\delta]}\, 2^{-(n-k)} + \varepsilon$$

$$\leq 2^{-n\left[1 - H(\bar{p}) - \delta - \frac{k}{n}\right]} + \varepsilon$$

Pick $\frac{k}{n} = 1 - H(\bar{p}) - 2\delta$

$$\Rightarrow \quad \leq 2^{-n\delta} + \varepsilon$$

which can be made to go to zero as $n \to \infty$

can conclude existence of codes for which this is true.

for dephasing channel, this gives achievable rate of $1 - H_2(p_Z)$