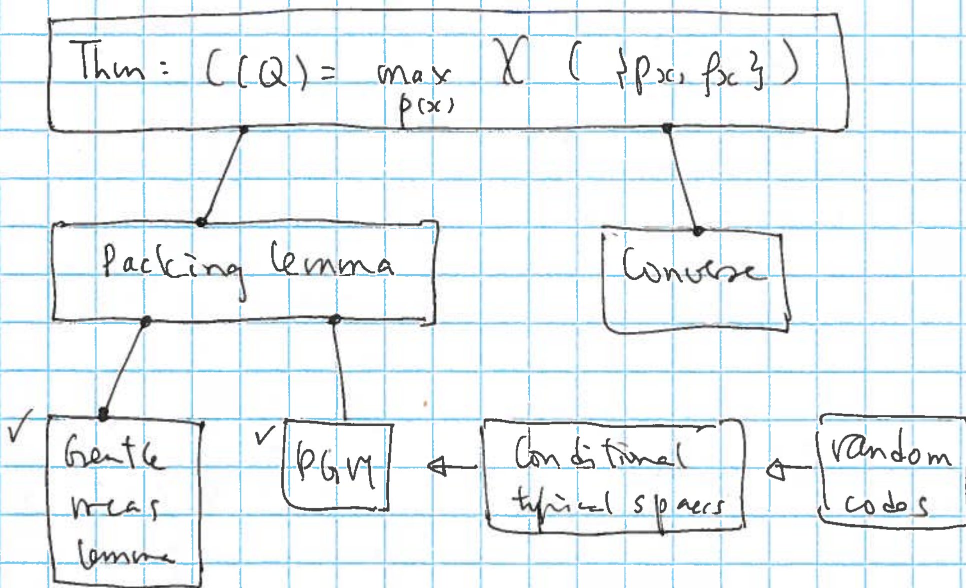
Last time: lec 10

Oct 11

Q-box: $\xrightarrow{x} \boxed{Q} \rightarrow \rho^x$



- Def: Let $S = \{\rho_1, \rho_2, \dots, \rho_k\}$

  Let $d_e(S) := \min_{\text{meas}} \mathbb{E}_i \Pr(\text{outcome} \neq i \mid \text{state} = \rho_i)$

  "distinguishability error of S"

  $\min_{\text{meas}}$ avg error

NB: specific measurements give upper bounds of $d_e(S)$.

③ The packing lemma.

Let $p(x)$ be a prob dist^n, ς_x be states, $\varsigma = \sum_x p_x \varsigma_x$.

If projectors Π, Π_x exist s.t. $\forall x$:

① $\mathrm{Tr}(\varsigma_x \Pi) \geq 1-\eta$ (or $1-\eta_1$)

② $\mathrm{Tr}(\varsigma_x \Pi_x) \geq 1-\eta$ (or $1-\eta_2$)

③ $\mathrm{Tr}(\Pi_x) \leq d_1$

④ $\Pi \varsigma \Pi \leq \frac{\Pi}{d_0}$

Then $S = \{\gamma_1, \dots, \gamma_k\}$ formed by drawing each γ_i iid from $\{p(x), \varsigma_x\}$ with $k = \frac{d_0}{d_1} \cdot f$ has

$\mathbb{E}_S d_e(S) \leq 2(\eta + \sqrt{3\eta}) + 4f$ (or $2(\eta_2 + \sqrt{3\eta_1}) + 4f$).

NB ① only needs to hold for most x.

Interpreting the packing lemma:

Conditions ② & ③ ensure each ρ_x lives in some d_1-dim space (up to approx).

Condition ① says all ρ_x live in a common space (defined by Π).

Condition ④: $\because \operatorname{tr}(\rho_x \Pi) \geq 1-\eta$

$$\therefore \Pi \rho_x \Pi \approx \rho_x \quad \text{GML}$$

$$\Pi \rho \Pi \approx \rho$$

$$\Pi \rho \Pi \leq \frac{\Pi}{d_0}$$

$\lambda_{max}(\rho) \lesssim \frac{1}{d_0}$

max eigval.

Controls how distinguishable the ρ_x's are.

Intuitively: $\rho = \sum_x p(x) \rho_x$

If ρ_x more distinguishable, $\lambda_{max}(\rho)$ is smaller, d_0 larger.

[Think of $\lambda_{max}(|\psi\rangle\langle\psi| + |\phi\rangle\langle\phi|)$.]

The packing lemma says:

If we're to communicate using a Q-box emitting $\{\rho_x\}$

then a random code S with $K = \frac{d_0}{d_1} f$ messages succeeds whp.

wrt choice of S

a fraction of being fully packed

d_1 dim each.

[$X_1, X_2, \ldots, X_k$ iid $\sim p(x)$]

Pf: let $\gamma_i = \rho_{X_i}$

Define a "PGM" (based on $\Pi\, \Pi_{X_i} \Pi$):

[Note PGM can be defined on any set of positive semi definite matrices.]

$$\Lambda_i = \Pi\, \Pi_{X_i}\, \Pi, \quad \Lambda = \sum_{i=1}^{k} \Lambda_i$$

$$M_i = \Lambda^{-\frac{1}{2}} \Lambda_i \Lambda^{-\frac{1}{2}}, \quad M_{k+1} = I - \sum_{i=1}^{k} M_i$$

(*) Then $d_e(S) \leq \frac{1}{k} \sum_i \mathrm{Tr}\, \gamma_i (I - M_i)$ ← error of PGM.

Trick: $I - M_i = I - \Lambda^{-\frac{1}{2}} \Lambda_i \Lambda^{-\frac{1}{2}}$

unwraps the $\Lambda^{-\frac{1}{2}}$ layers.

$$= I - \Big(\Lambda_i + \sum_{j \neq i} \Lambda_j\Big)^{-\frac{1}{2}} \Lambda_i \Big(\Lambda_i + \sum_{j\neq i} \Lambda_j\Big)^{-\frac{1}{2}}$$

$$\leq 2(I - \Lambda_i) + 4 \sum_{j \neq i} \Lambda_j$$

op ineq $I - (X+Y)^{-\frac{1}{2}} X (X+Y)^{-\frac{1}{2}} \leq 2(I - X) + 4Y$

$\because \gamma_i \geq 0$,

$$(*): d_e(S) \leq \frac{1}{k} \sum_i \mathrm{Tr}\, \gamma_i \Big[2(I - \Lambda_i) + 4 \sum_{j\neq i} \Lambda_j\Big]$$

$$= \frac{2}{k} \sum_i \underbrace{\Big[\mathrm{Tr}\, \gamma_i (I - \Lambda_i)\Big]}_{\parallel} + \frac{4}{k} \sum_i \underbrace{\Big[\sum_{j \neq i} \mathrm{Tr}\, \gamma_i \Lambda_j\Big]}$$

$1 - \mathrm{Tr}(\rho_{X_i} \Pi\, \Pi_{X_i} \Pi)$

$= 1 - \mathrm{Tr}(\Pi \rho_{X_i} \Pi \cdot \Pi_{X_i})$

If $\| A - B \|_{tr} \leq \delta$ then $\forall\, 0 \leq P \leq I$, $|\mathrm{Tr}\, P(A-B)| \leq 2\delta$

$\leq 1 - \mathrm{Tr}(\rho_{X_i} \Pi_{X_i}) + 2\sqrt{3\eta}$

Here $A = \Pi \rho_{X_i} \Pi$, $B = \rho_{X_i}$, $\delta = \sqrt{3\eta}$ by Gentle meas lemma & ①.

$\overset{②}{\leq} \eta + 2\sqrt{3\eta}$

$\mathop{\mathbb{E}}_S \sum_{j \neq i} \mathrm{Tr}\, \gamma_i \Lambda_j$ (γ_i, Λ_j indep)

$$= \sum_{j \neq i} \mathrm{Tr}\Big(\mathop{\mathbb{E}}_S \rho_{X_i}\Big) \cdot \Pi \Big(\mathop{\mathbb{E}}_S \Pi_{X_j}\Big) \Pi$$

$$\leq \sum_j \mathrm{Tr}\, \rho \cdot \Pi \Big(\mathop{\mathbb{E}}_S \Pi_{X_j}\Big) \Pi$$

$$\overset{③}{\leq} \sum_j \mathrm{Tr} \Big(\frac{\Pi}{d_0}\Big) \mathop{\mathbb{E}}_S \Pi_{X_j}$$

$\Pi \leq I$

$$\overset{④}{\leq} \mathop{\mathbb{E}}_S \sum_j \frac{d_1}{d_0} = k \cdot \frac{d_1}{d_0} \leq f.$$

$\mathrm{rank}(\Pi_{X_j}) \leq d_1$

Need $\mathop{\mathbb{E}}_S$

Note $\frac{2}{k} \sum_i \ldots$, so if a fraction $\geq 1-g$ satisfies condition ①, $\eta + 2\sqrt{3\eta} \to g + \eta + 2\sqrt{3\eta}$.

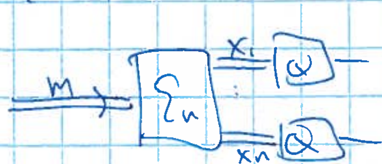
Now back to : $C(Q) = \max_{p(x)} \chi(\{p(x), \rho_x\})$

for Q box $\xrightarrow{x} \boxed{Q} \xrightarrow{\rho_x}$

① Direct coding thm. Given Q box, any dist^n $p(x)$

Consider (M, n) code :

Alice



- A random code is generated as follows : (& told to Alice & Bob)

$$C_1 = x_{11}\ x_{12} \cdots x_{1n}$$
$$C_2 = x_{21}\ x_{22} \cdots x_{2n}$$
$$\vdots$$
$$C_M = x_{M1}\ x_{M2} \cdots x_{Mn}$$

where each x_{ij} drawn iid $\sim p(x)$, and reject C_i's if not strongly typical

- For message i, Alice inputs $x_{i1}, x_{i2} \ldots x_{in}$ into the n uses of Q.

- Bob receives $\gamma_i = \rho_{x_{i1}} \otimes \rho_{x_{i2}} \otimes \cdots \otimes \rho_{x_{in}}$

Want to bound $\mathbb{E}_S\, d_e(S)$ for $S = \{\gamma_1, \gamma_2, \ldots \gamma_M\}$

each γ_i drawn iid from :

$$\{ \underbrace{\rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n}}_{\xi_C} : C = x_1 \ldots x_n \in A_{n,\varepsilon} \}$$

strongly typical

To apply the packing lemma, need to find $\bar{\Pi}$, $\bar{\Pi}_C$, d_0, d_1, η, + & "g".

Strongly typical sequence:

X r.v $\sim p(x)$

$C = x_1 x_2 \dots x_n \in A_{n,\varepsilon}$

ε-strongly typical

If empirical distribution in C, $q(x)$, is ε close to $p(x)$.

eg. $\Omega = \{1, 2, 3, 4\}$, $p(a) = \frac{a}{10}$, $n = 20$.

$C = 33344 \quad 21322 \quad 24343 \quad 42443$

$q(1) = 1/20$ $\qquad$ $p(1) = 1/10$

$q(2) = 5/20$ $\qquad$ $p(2) = 2/10$

$q(3) = 7/20$ $\qquad$ $\vdots$

$q(4) = 7/20$

$$\sum_x |p(x) - q(x)|$$

$$\|p - q\|_1 = \left|\frac{1}{20} - \frac{1}{10}\right| + \left|\frac{5}{20} - \frac{2}{10}\right| + \left|\frac{7}{20} - \frac{3}{10}\right| + \left|\frac{7}{20} - \frac{4}{10}\right|$$

$$= 0.2.$$

$\therefore C \in A_{20, 0.2}$.

NB. $A_{n,\varepsilon}$ is a high prob set.

Proof sketch: want $\sum_x |q(x) - p(x)| \le \varepsilon$

suffices to have $|q(x) - p(x)| \le \frac{\varepsilon}{|\Omega|}$ $\quad \forall x$.

$\Pr(\text{not}) \underset{\text{union bd}}{\le} |\Omega| \Pr\left(|q(x) - p(x)| > \frac{\varepsilon}{|\Omega|}\right)$ small.

Suppose $C = x_1 x_2 \ldots x_n \in A_{n,\varepsilon}$

$$\xi_C = \rho_{x_1} \otimes \cdots \otimes \rho_{x_n}.$$

Up to reordering the n systems,

$$\xi_C = \bigotimes_{x \in \Omega} \rho_x^{\otimes n f(x)}$$ ← look at each $\rho_x^{\otimes n f(x)}$ $\forall x$

By QAEP, $\forall \delta > 0$, $\forall \varepsilon_1 > 0$, $\exists n_0$ $\forall n f(x) \geq n_0$

Discussion for Schumacher compression

$\exists \Pi_x$ (projector) s.t.

- $\mathrm{tr}\left(\Pi_x \, \rho_x^{\otimes n f(x)} \right) \geq 1 - \delta$
- $\dim \Pi_x \leq 2^{n f(x) (S(\rho_x) + \varepsilon_1)}$

Given C, let $\Pi_C = \bigotimes_{x \in \Omega} \Pi_x$ ← acting on the correct systems.

Then $\mathrm{tr}[\Pi_C \cdot \xi_C] \geq (1-\delta)^{|\Omega|}$ ← ② packing lemma sets η_2

$$\dim \Pi_C \leq 2^{\sum_x n f(x) (S(\rho_x) + \varepsilon_1)}$$

$$= 2^{n \left[\sum_x f(x) S(\rho_x) + \varepsilon_1 \right]}$$

③ sets d_1

$$\leq 2^{n \left[\sum_x p(x) S(\rho_x) + \sum_x |f(x) - p(x)| \cdot S(\rho_x) + \varepsilon_1 \right]}$$

$$\leq 2^{n \left[\sum_x p(x) S(\rho_x) + \varepsilon \cdot \log(d) + \varepsilon_1 \right]}$$

dim of ρ_x, const

e.g. $C = 33344 \quad 21322 \quad 24343 \quad 42443$

$\gamma_C = \rho_3 \otimes \rho_3 \otimes \rho_3 \otimes \rho_4 \otimes \rho_4 \otimes \cdots \quad \otimes \rho_4 \otimes \rho_4 \otimes \rho_3$

$x = 1$, Π_1 acts on sys 7.

$x = 2$, Π_2 acts on sys 6, 9, 10, 11, 17

$x = 3$, Π_3 acts on sys 1, 2, 3, 8, 13, 15, 20

$x = 4$, Π_4 acts on sys 4, 5, 12, 14, 16, 18, 19.

For conditions (1) & (4) :

let $\rho = \sum_x p(x)\, \rho_x$

Π = projector onto n, ε_2 typical space of $\rho^{\otimes n}$

s.t. $\operatorname{tr}(\Pi \rho^{\otimes n}) \geq 1 - \delta_2$.

By QAEP: $\Pi \rho^{\otimes n} \Pi \leq 2^{-n[S(\rho) - \varepsilon_2]} \Pi$

But we want $\Pi \varsigma \Pi \leq \frac{\Pi}{d_0}$ where $\varsigma = \mathop{\mathbb{E}}_{C} \varsigma_C$

Condition (4).

$\varsigma_C = \rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n}$.

drawn iid $\sim p(x)$

reject if $C \notin A_{n,\varepsilon}$.

In fact $\rho^{\otimes n} = \sum_{\text{all } \vec{c}} p(\vec{c})\, \rho_{\vec{c}} = \sum_{\vec{c} \in A_{n,\varepsilon}} p(\vec{c})\, \rho_{\vec{c}} + \sum_{\vec{c} \notin A_{n,\varepsilon}} p(\vec{c})\, \rho_{\vec{c}}$

$= \underbrace{pr(\vec{c} \in A_{n,\varepsilon})}_{1-\delta_3} \cdot \underbrace{\varsigma}_{(\text{trace } 1)} + \underbrace{pr(\vec{c} \notin A_{n,\varepsilon})}_{\text{let this be } \delta_3} \cdot \underbrace{\varsigma'}_{\text{some density matrix}}$.

$\therefore (1-\delta_3)\, \Pi \varsigma \Pi + \delta_3\, \Pi \varsigma' \Pi \leq 2^{-n[S(\rho) - \varepsilon_2]}\, \Pi$

$$\Pi \varsigma \Pi \leq \frac{2^{-n[S(\rho) - \varepsilon_2]}}{1-\delta_3}\, \Pi$$

$\therefore d_0 \geq (1-\delta_3)\, 2^{n[S(\rho) - \varepsilon_2]}$.

finally for condition ①:

$$\mathrm{tr}(\rho^{\otimes n}\Pi) = \sum_{\vec{c}\in A_{n,\varepsilon}} p(\vec{c})\,\mathrm{tr}(\rho_{\vec{c}}\Pi) + \underbrace{\sum_{\vec{c}\notin A_{n,\varepsilon}} p(\vec{c})\,\mathrm{tr}(\rho_{\vec{c}}\Pi)}_{\leq \delta_3} \geq 1-\delta_2$$

$$\sum_{\vec{c}\in A_{n,\varepsilon}} \underbrace{p(\vec{c})}_{\approx \text{same}}\,\mathrm{tr}(\rho_{\vec{c}}\Pi) \geq 1-\delta_2-\delta_3 .$$

$$\frac{1}{|A_{n,\varepsilon}|}\sum_{\vec{c}\in A_{n,\varepsilon}} \mathrm{tr}(\rho_{\vec{c}}\Pi) \gtrsim \frac{1-\delta_2-\delta_3}{1-\delta_2} \simeq 1-\delta_3-\delta_3\delta_2 + 3^{\text{rd}}\text{ order terms}$$

$$:= 1-\delta_4$$

Let $G = \{\vec{c}\in A_{n,\varepsilon},\ \mathrm{tr}(\rho_{\vec{c}}\Pi) \geq 1-\sqrt{\delta_4}\}$

Let $g = 1 - \frac{|G|}{|A_{n,\varepsilon}|}$.

Then $(1-g)\cdot 1 + g\cdot(1-\sqrt{\delta_4}) \geq 1-\delta_4$

$$\sqrt{\delta_4} \geq g$$

(Note general technique to bound the bad fraction given the ave.).

$\therefore$ for $\underset{g}{g} \leq \sqrt{\delta_4}$, $(1-g)$ fraction of ρ_c has $\mathrm{tr}(\rho_c\Pi) \geq \underset{\eta_1}{1-\sqrt{\delta_4}}$

Now applying the packing lemma with:

$\rho_C = \rho_{x_1} \otimes \rho_{x_2} \cdots \otimes \rho_{x_n}$ for $C = x_1 \ldots x_n \in A_{n,\varepsilon}$, $\left[\begin{array}{c} \text{prob}(C \in A_{n,\varepsilon}) \\ \shortparallel \\ 1-\delta_3 \end{array}\right]$

$$p(C) = \frac{1}{(1-\delta_3)} \times p(x_1) \cdots p(x_n).$$

$\Pi = \varepsilon_2$-typical space of $\rho^{\otimes n}$, $\rho = \sum_x p(x) \rho_x$.

$\Pi_C = \bigotimes_{x \in \Omega} \varepsilon_1$-typical space of $\rho_x^{\otimes n_{p(x)}}$

$n_{p(x)} = n_C$

$$d_1 = 2^{n\left[\sum_x p(x) S(\rho_x) + \varepsilon \cdot \underbrace{\log d}_{\text{dim of } \rho_x} + \varepsilon_1\right]}.$$

$$d_0 \geq (1-\delta_3)\, 2^{n[S(\rho) - \varepsilon_2]}$$

$g \leq \sqrt{\delta_4}$, $\delta_4 \doteq (d_2+1)\delta_3$

$\eta_1 = \sqrt{\delta_4}$

$\eta_2 = 1-(1-\delta)^{|\Omega|}$

$$\text{for } M = \frac{d_0}{d_1} f \doteq (1-\delta_3)\, 2^{n\left[S(\rho) - \varepsilon_2 - \sum_x p(x) S(\rho_x) - \varepsilon \log d - \varepsilon_1\right]} \cdot f$$
$$= 2^{n[\chi(\{p_x, \rho_x\}) - \varepsilon']}$$

$$\mathbb{E}_S\, d_e(S) \leq 2(g + \eta_2 + 2\sqrt{3\eta_1}) + 4f \qquad \square$$

Now follow same procedure as in Shannon's noisy coding thm:

① $\exists$ a code $\tilde{S}_n$ with $d_e(S) \leq$ vanishing function of n.

② Keep the better half of the code words in $\tilde{S}_n$ to bound the worst case error.

Converse:

Consider the state $\displaystyle\sum_{x_1 x_2 \ldots x_n} \underset{\text{arbitrary, } \frac{1}{n} \text{ if } x_1 \cdots x_n \text{ is a code word, 0 otherwise}}{p(x_1 x_2 \ldots x_n)} \underbrace{|x_1 \ldots x_n\rangle\langle x_1 \ldots x_n|}_{\text{Sys } X_1 X_2 \ldots X_n} \otimes \underbrace{\rho_{x_1} \otimes \ldots \otimes \rho_{x_n}}_{B_1 B_2 \ldots B_n}$

Then $nR \leq I_{acc}\left(\{p(x_1 x_2 \ldots x_n), \rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n}\}\right)$

$$\leq \chi\left(\{p(x_1 x_2 \ldots x_n), \rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n}\}\right)$$

$$= I(X_1 X_2 \ldots X_n : B_1 \ldots B_n)$$

Conditioning on classical sys is OK

$$= S(B_1 B_2 \ldots B_n) - S(B_1 B_2 \ldots B_n | X_1 X_2 \ldots X_n)$$

$$\overset{SA}{\leq} \sum_{i=1}^{n} S(B_i) - \sum_{x_1 \ldots x_n} p(x_1 x_2 \ldots x_n)\, S(\rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n}).$$

product state

$$= \sum_{i=1}^{n} S(B_i) - \sum_{x_1 \ldots x_n} p(x_1 x_2 \ldots x_n) \sum_{i=1}^{n} S(\rho_{x_i})$$

marginal

$$= \sum_{i=1}^{n} S(B_i) - \sum_{i=1}^{n} p(x_i)\, S(\rho_{x_i})$$

$$\leq \underbrace{\sum_{i=1}^{n} I(X_i : B_i)}_{\substack{\text{1-shot Holevo info} \\ \text{for some } p(x_i)}} \leq n \max_{p(x)} \chi\left(\{p(x), \rho_x\}\right).$$