Quantum Achievability Proof via Collision Relative Entropy

Salman Beigi

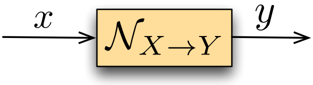
Institute for Research in Fundamental Sciences (IPM)
Tehran, Iran

Setemper 8, 2014

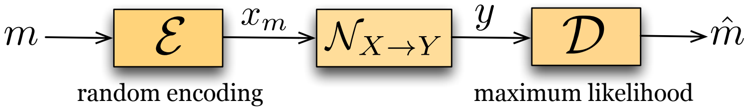
Based on a joint work with Amin Gohari

arXiv:1312.3822

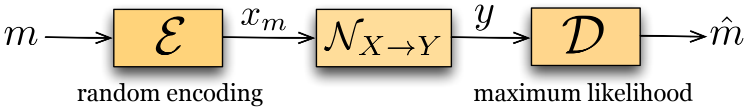
Technique of Yassaee et al (ISIT 2013)



Technique of Yassaee et al (ISIT 2013)

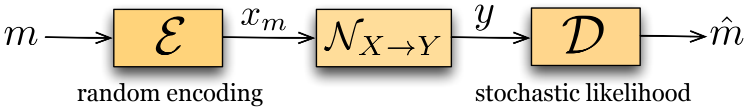


Technique of Yassaee et al (ISIT 2013)



- Random encoding:
  - choose some p_X
  - pick i.i.d samples $\mathrm{x}_1, \ldots, \mathrm{x}_M$

Technique of Yassaee et al (ISIT 2013)



- Random encoding:
  - choose some p_X
  - pick i.i.d samples $\mathrm{x}_1, \ldots, \mathrm{x}_M$
- Stochastic likelihood decoder
  - sample from $p(m|y)$

$$p(m, y) = \frac{1}{M} p(y|\mathrm{x}_m) \qquad \Rightarrow \qquad p(m|y) = \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{m'})}$$

Technique of Yassaee et al (ISIT 2013)

Random codebook: $\mathcal{C} = \{\mathrm{x}_1, \ldots, \mathrm{x}_M\}$

$$\mathbb{E}_{\mathcal{C}} \Pr[\mathrm{succ}] \quad = \quad \mathbb{E}_{\mathcal{C}} \sum_{m,y} \frac{1}{M} p(y|\mathrm{x}_m) \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{\bar{m}})}$$

Technique of Yassaee et al (ISIT 2013)

Random codebook: $\mathcal{C} = \{\mathrm{x}_1, \ldots, \mathrm{x}_M\}$

$$\begin{aligned} \mathbb{E}_{\mathcal{C}} \Pr[\text{succ}] &= \mathbb{E}_{\mathcal{C}} \sum_{m,y} \frac{1}{M} p(y|\mathrm{x}_m) \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{\bar{m}})} \\ &= \mathbb{E}_{\mathcal{C}} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\sum_{m'} p(y|\mathrm{x}_{m'})} \end{aligned}$$

Technique of Yassaee et al (ISIT 2013)

Random codebook: $\mathcal{C} = \{\mathrm{x}_1, \ldots, \mathrm{x}_M\}$

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}} \Pr[\mathrm{succ}] &= \mathbb{E}_{\mathcal{C}} \sum_{m,y} \frac{1}{M} p(y|\mathrm{x}_m) \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{\bar{m}})} \\
&= \mathbb{E}_{\mathcal{C}} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\sum_{m'} p(y|\mathrm{x}_{m'})} \\
&\overset{\text{(Jensen)}}{\geq} \mathbb{E}_{\mathrm{x}_1} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\mathbb{E}_{\mathcal{C}\setminus \mathrm{x}_1} \sum_{m'} p(y|\mathrm{x}_{m'})}
\end{aligned}$$

Technique of Yassaee et al (ISIT 2013)

Random codebook: $\mathcal{C} = \{\mathrm{x}_1, \ldots, \mathrm{x}_M\}$

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}} \Pr[\mathrm{succ}] &= \mathbb{E}_{\mathcal{C}} \sum_{m,y} \frac{1}{M} p(y|\mathrm{x}_m) \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{\bar{m}})} \\
&= \mathbb{E}_{\mathcal{C}} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\sum_{m'} p(y|\mathrm{x}_{m'})} \\
&\overset{\text{(Jensen)}}{\geq} \mathbb{E}_{\mathrm{x}_1} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\mathbb{E}_{\mathcal{C}\setminus \mathrm{x}_1} \sum_{m'} p(y|\mathrm{x}_{m'})} \\
&= \mathbb{E}_{\mathrm{x}_1} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{p(y|\mathrm{x}_1) + (M-1)p(y)}
\end{aligned}$$

Technique of Yassaee et al (ISIT 2013)

Random codebook: $\mathcal{C} = \{\mathrm{x}_1, \ldots, \mathrm{x}_M\}$

$$
\begin{aligned}
\mathbb{E}_{\mathcal{C}} \Pr[\text{succ}] &= \mathbb{E}_{\mathcal{C}} \sum_{m,y} \frac{1}{M} p(y|\mathrm{x}_m) \frac{p(y|\mathrm{x}_m)}{\sum_{m'} p(y|\mathrm{x}_{\bar{m}})} \\
&= \mathbb{E}_{\mathcal{C}} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\sum_{m'} p(y|\mathrm{x}_{m'})} \\
&\overset{\text{(Jensen)}}{\geq} \mathbb{E}_{\mathrm{x}_1} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{\mathbb{E}_{\mathcal{C}\backslash \mathrm{x}_1} \sum_{m'} p(y|\mathrm{x}_{m'})} \\
&= \mathbb{E}_{\mathrm{x}_1} \sum_{y} p(y|\mathrm{x}_1) \frac{p(y|\mathrm{x}_1)}{p(y|\mathrm{x}_1) + (M-1)p(y)} \\
&= \mathbb{E}_{\mathrm{xy}} \frac{p(\mathrm{y}|\mathrm{x})}{p(\mathrm{y}|\mathrm{x}) + (M-1)p(\mathrm{y})} \\
&= \mathbb{E}_{\mathrm{xy}} \frac{1}{1 + (M-1)\frac{p(\mathrm{y})}{p(\mathrm{y}|\mathrm{x})}}
\end{aligned}
$$

Plan for the talk

Better understanding and quantum generalization of

- Stochastic likelihood decoder
- convexity $\Rightarrow$ Jensen's inequality
- Asymptotic analysis of the result

Pretty good measurement

- Pretty good measure for signal states $\{\rho_1, \ldots, \rho_M\}$

$$E_m = \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}} \rho_m \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}}$$

Pretty good measurement

- Pretty good measure for signal states $\{\rho_1, \ldots, \rho_M\}$

$$E_m = \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}} \rho_m \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}}$$

- If the signal states are $\rho_m \sim p(y|\mathrm{x}_m)$ then

$$E_m \sim \frac{p(y|\mathrm{x}_m)}{\sum_i p(y|\mathrm{x}_i)}$$

Pretty good measurement

- Pretty good measure for signal states $\{\rho_1, \ldots, \rho_M\}$

$$E_m = \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}} \rho_m \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}}$$

- If the signal states are $\rho_m \sim p(y|x_m)$ then

$$E_m \sim \frac{p(y|x_m)}{\sum_i p(y|x_i)}$$

- The probability of successful decoding

$$\Pr[\text{succ}] = \frac{1}{M} \sum_m \operatorname{tr}\Big[\rho_m \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}} \rho_m \Big(\sum_i \rho_i\Big)^{-\frac{1}{2}}\Big]$$

Collision relative entropy

$$D_2(\rho\|\sigma) = \log \operatorname{tr}[\rho\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}]$$

Collision relative entropy

$$D_2(\rho\|\sigma) = \log \operatorname{tr}[\rho\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}]$$

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \operatorname{tr}\left[\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right]$$

Collision relative entropy

$$D_2(\rho\|\sigma) = \log \operatorname{tr}[\rho\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}]$$

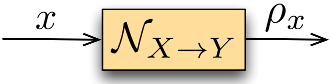
$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha - 1} \log \operatorname{tr}\left[\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha}\right]$$

Müller-Lennert et al, arXiv:1306.3142
Wilde, Winter, Yang, arXiv:1306.1586

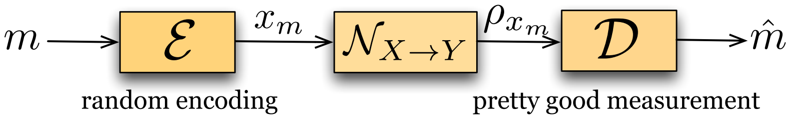
Frank, Lieb, arXiv:1306.5358
SB, arXiv:1306.5920

- (Positivity) $D_2(\rho\|\sigma) \geq 0$.
- (Data processing) $D_2(\rho\|\sigma) \geq D_2(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$.
- (Joint convexity) $\exp D_2(\cdot\|\cdot)$ is jointly convex

Classical-Quantum channels

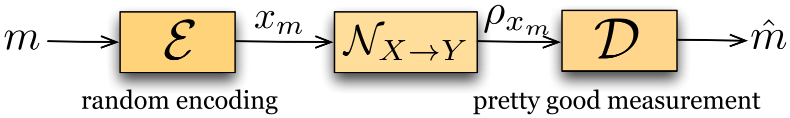


Classical-Quantum channels



- input distribution $p(x)$
- pick random codebook $\mathrm{x}_1, \ldots, \mathrm{x}_M$
- pretty good measurement at the decoder

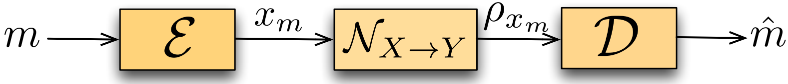
Classical-Quantum channels



- input distribution $p(x)$
- pick random codebook $\mathrm{x}_1, \ldots, \mathrm{x}_M$
- pretty good measurement at the decoder

$$\sigma_{UXY} = \frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m| \otimes |\mathrm{x}_m\rangle\langle \mathrm{x}_m| \otimes \rho_{\mathrm{x}_m},$$

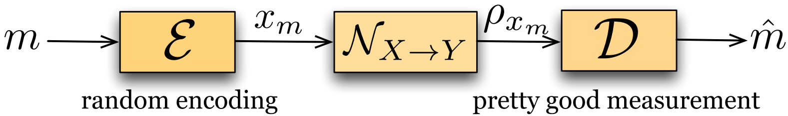
c-q channel coding



$$\sigma_{UXB} = \sum_{m=1}^{M} \frac{1}{M} |m\rangle\langle m| \otimes |\mathrm{x}_m\rangle\langle \mathrm{x}_m| \otimes \rho_{\mathrm{x}_m},$$

$$\Pr[\mathrm{succ}] \quad = \quad \frac{1}{M} \sum_{m=1}^{M} \mathrm{tr}\left[\rho_{\mathrm{x}_m} \left(\sum_i \rho_{\mathrm{x}_i} \right)^{-1/2} \rho_{\mathrm{x}_m} \left(\sum_i \rho_{\mathrm{x}_i} \right)^{-1/2} \right]$$

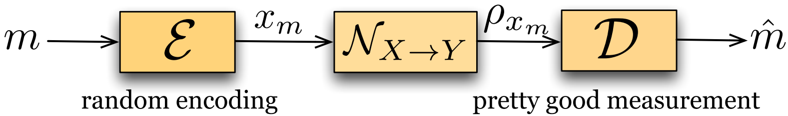
c-q channel coding



$$\sigma_{UXB} = \sum_{m=1}^{M} \frac{1}{M} |m\rangle\langle m| \otimes |\mathrm{x}_m\rangle\langle \mathrm{x}_m| \otimes \rho_{\mathrm{x}_m},$$

$$\begin{aligned} \Pr[\mathrm{succ}] &= \frac{1}{M} \sum_{m=1}^{M} \mathrm{tr}\left[\rho_{\mathrm{x}_m} \Big(\sum_i \rho_{\mathrm{x}_i}\Big)^{-1/2} \rho_{\mathrm{x}_m} \Big(\sum_i \rho_{\mathrm{x}_i}\Big)^{-1/2}\right] \\ &= \frac{1}{M} \exp D_2(\sigma_{UXY} \| \sigma_{UX} \otimes \sigma_Y) \end{aligned}$$

c-q channel coding



$$\sigma_{UXB} = \sum_{m=1}^{M} \frac{1}{M} |m\rangle\langle m| \otimes |\mathrm{x}_m\rangle\langle \mathrm{x}_m| \otimes \rho_{\mathrm{x}_m},$$

$$\begin{aligned}
\Pr[\text{succ}] &= \frac{1}{M}\sum_{m=1}^{M} \operatorname{tr}\left[\rho_{\mathrm{x}_m}\Big(\sum_i \rho_{\mathrm{x}_i}\Big)^{-1/2}\rho_{\mathrm{x}_m}\Big(\sum_i \rho_{\mathrm{x}_i}\Big)^{-1/2}\right] \\
&= \frac{1}{M}\exp D_2(\sigma_{UXY} \| \sigma_{UX} \otimes \sigma_Y) \\
&\geq \frac{1}{M}\exp D_2(\sigma_{XY} \| \sigma_X \otimes \sigma_Y)
\end{aligned}$$

Error analysis

Use the joint convexity of $\exp D_2(\cdot\|\cdot)$

$$\begin{aligned}\mathbb{E}_{\mathcal{C}}\Pr[\text{succ}] &\geq \frac{1}{M}\mathbb{E}_{\mathcal{C}}\exp D_2(\sigma_{XY}\|\sigma_X\otimes\sigma_Y)\\ &\geq \frac{1}{M}\exp D_2(\mathbb{E}_{\mathcal{C}}\,\sigma_{XY}\|\mathbb{E}_{\mathcal{C}}\,\sigma_X\otimes\sigma_Y)\end{aligned}$$

Error analysis

Use the joint convexity of $\exp D_2(\cdot\|\cdot)$

$$
\begin{aligned}
\mathbb{E}_{\mathcal{C}}\Pr[\text{succ}] &\geq \frac{1}{M}\mathbb{E}_{\mathcal{C}} \exp D_2(\sigma_{XY}\|\sigma_X \otimes \sigma_Y) \\
&\geq \frac{1}{M} \exp D_2(\mathbb{E}_{\mathcal{C}}\, \sigma_{XY}\|\mathbb{E}_{\mathcal{C}}\, \sigma_X \otimes \sigma_Y) \\
&= M^{-1} \exp D_2 \left(\rho_{XY}\Big\| \frac{1}{M}\rho_{XY} + (1 - \frac{1}{M})\rho_X \otimes \rho_Y\right),
\end{aligned}
$$

$$
\boxed{\rho_{XY} = \textstyle\sum_x p(x)|x\rangle\langle x| \otimes \rho_x}
$$

Information spectrum relative entropy

- $\Pi_{U\geq 0}$: projection on eigenspaces with non-negative eigenvalues
- $\Pi_{U\geq V} := \Pi_{U-V\geq 0}$

Information spectrum relative entropy

- $\Pi_{U\geq 0}$: projection on eigenspaces with non-negative eigenvalues
- $\Pi_{U\geq V} := \Pi_{U-V\geq 0}$

$$D_s^{\epsilon}(\rho\|\sigma) := \sup\left\{R \middle| \operatorname{tr}\left(\rho\Pi_{\rho\leq 2^R\sigma}\right) \leq \epsilon\right\}.$$

Information spectrum relative entropy

- $\Pi_{U\geq 0}$: projection on eigenspaces with non-negative eigenvalues
- $\Pi_{U\geq V} := \Pi_{U-V\geq 0}$

$$D_s^\epsilon(\rho\|\sigma) := \sup\left\{R \middle| \operatorname{tr}\left(\rho\Pi_{\rho\leq 2^R\sigma}\right) \leq \epsilon\right\}.$$

$$D_s^\epsilon(p\|q) = \sup\left\{R \middle| \sum_{x:\, p(x)\leq 2^R q(x)} p(x) \leq \epsilon\right\}$$

Information spectrum relative entropy

- $\Pi_{U\geq 0}$: projection on eigenspaces with non-negative eigenvalues
- $\Pi_{U\geq V} := \Pi_{U-V\geq 0}$

$$D_s^\epsilon(\rho\|\sigma) := \sup\left\{R \middle| \operatorname{tr}\left(\rho\Pi_{\rho\leq 2^R\sigma}\right) \leq \epsilon\right\}.$$

$$D_s^\epsilon(p\|q) = \sup\left\{R \middle| \sum_{x:\, p(x)\leq 2^R q(x)} p(x) \leq \epsilon\right\}$$

Theorem

For every $0 < \epsilon, \lambda < 1$ and density matrices ρ, σ we have

$$\exp D_2(\rho\|\lambda\rho + (1-\lambda)\sigma) \geq (1-\epsilon)\left[\lambda + (1-\lambda)\exp\left(-D_s^\epsilon(\rho\|\sigma)\right)\right]^{-1}$$

A one-shot achievable bound

$$\mathbb{E}_{\mathcal{C}} \Pr[\text{succ}] \geq M^{-1} \exp D_2 \left(\rho_{XY} \middle\| \frac{1}{M} \rho_{XY} + (1 - \frac{1}{M}) \rho_X \otimes \rho_Y \right)$$
$$\geq (1-\epsilon) \left[1 + (M-1) \exp \left(-D_s^{\epsilon}(\rho_{XY} \| \rho_X \otimes \rho_Y) \right) \right]^{-1}$$

Theorem

$M^*(1, \epsilon)$: maximum number of messages with error $\leq \epsilon$

$$M^*(1, \epsilon) \geq \max_{p(x),\, 0<\delta<\epsilon} \left\lfloor \frac{\epsilon - \delta}{1 - \epsilon} \exp \left(D_s^{\delta}(\rho_{XY} \| \rho_X \otimes \rho_Y) \right) + 1 \right\rfloor$$

Asymptotic analysis

- Relative entropy: $D(\sigma\|\rho) := \mathrm{tr}(\sigma(\log\sigma - \log\rho))$.
- Information variance or the relative entropy variance

$$V(\rho\|\sigma) := \mathrm{tr}\big(\rho(\log\rho - \log\sigma - D(\rho\|\sigma))^2\big).$$

Theorem [Tomamichel & Hayashi '12]

For fixed $0 < \epsilon < 1$ and δ proportional to $1/\sqrt{n}$ we have

$$D_s^{\epsilon\pm\delta}(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\,\Phi^{-1}(\epsilon) + O(\log n),$$

$\Phi(u) := \int_{-\infty}^{u} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}t^2}\mathrm{d}t$, and $\Phi^{-1}(\epsilon) = \sup\{u|\,\Phi(u) \le \epsilon\}$.

Asymptotic analysis

Theorem

For $0 < \epsilon < 1/2$ we have

$$\log M^*(n,\epsilon) \geq nC + \sqrt{nV}\Phi^{-1}(\epsilon) + O(\log n),$$

where C is the channel capacity

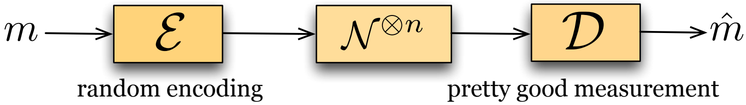
$$C := \max_{p(x)} I(X;Y)$$

and V is the channel dispersion

$$V = \min_{p(x)\in \operatorname{argmax} I(X;Y)} V(\rho_{XB}\|\rho_X \otimes \rho_B)$$

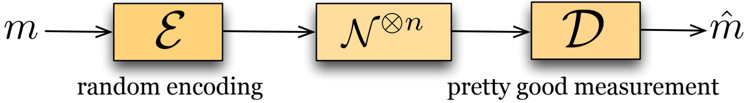
[Tan & Tomamichel '13]: this achievable bound is tight

Summary



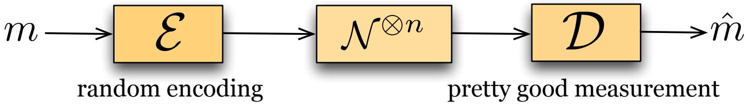
- Write probability of successful decoding in terms of collision relative entropy

Summary



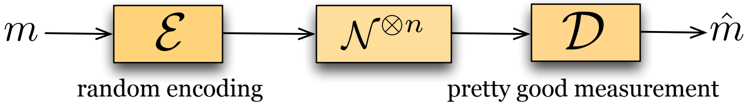
- Write probability of successful decoding in terms of collision relative entropy
- Use joint convexity of collision relative entropy

Summary



- Write probability of successful decoding in terms of collision relative entropy
- Use joint convexity of collision relative entropy
- Lower bound collision relative entropy with information spectrum relative entropy

Summary



- Write probability of successful decoding in terms of collision relative entropy
- Use joint convexity of collision relative entropy
- Lower bound collision relative entropy with information spectrum relative entropy
- Compute the asymptotics of information spectrum relative entropy

$$\log M^*(n,\epsilon) \geq nC + \sqrt{nV}\Phi^{-1}(\epsilon) + O(\log n)$$

Hypothesis testing

- Given either ρ or σ
- Want to decide which one
- Apply POVM measurement $\{F_\rho, F_\sigma\}$

Hypothesis testing

- Given either ρ or σ
- Want to decide which one
- Apply POVM measurement $\{F_\rho, F_\sigma\}$
- $\Pr[\text{type I error}] = \Pr[\text{error} \,|\rho] = \mathrm{tr}(\rho F_\sigma)$
  $\Pr[\text{type II error}] = \Pr[\text{error} \,|\sigma] = \mathrm{tr}(\sigma F_\rho)$

Hypothesis testing

- Given either ρ or σ
- Want to decide which one
- Apply POVM measurement $\{F_\rho, F_\sigma\}$
- $\Pr[\text{type I error}] = \Pr[\text{error}\,|\rho] = \operatorname{tr}(\rho F_\sigma)$
  $\Pr[\text{type II error}] = \Pr[\text{error}\,|\sigma] = \operatorname{tr}(\sigma F_\rho)$

$$\beta_\epsilon(\rho\|\sigma) = \min_{\Pr[\text{type I error}] \le \epsilon} \Pr[\text{type II error}]$$

Hypothesis testing

- Given either ρ or σ
- Want to decide which one
- Apply POVM measurement $\{F_\rho, F_\sigma\}$
- $\Pr[\text{type I error}] = \Pr[\text{error} \,|\rho] = \mathrm{tr}(\rho F_\sigma)$
  $\Pr[\text{type II error}] = \Pr[\text{error} \,|\sigma] = \mathrm{tr}(\sigma F_\rho)$

$$\beta_\epsilon(\rho\|\sigma) = \min_{\Pr[\text{type I error}] \le \epsilon} \Pr[\text{type II error}]$$

- Pick some M and define

$$F_\rho = (\rho + M\sigma)^{-1/2}\rho(\rho + M\sigma)^{-1/2}$$

$$F_\sigma = (M^{-1}\rho + \sigma)^{-1/2}\sigma(M^{-1}\rho + \sigma)^{-1/2}$$

A one-shot hypothesis testing

$$\begin{aligned} 1 - \Pr[\text{type I error}] &= \exp D_2(\rho || \rho + M\sigma) \\ &\geq (1-\epsilon)\left[1 + M \exp\big(-D_s^{\epsilon}(\rho\|\sigma)\big)\right]^{-1} \end{aligned}$$

A one-shot hypothesis testing

$$
\begin{aligned}
1 - \Pr[\text{type I error}] &= \exp D_2(\rho || \rho + M\sigma) \\
&\geq (1-\epsilon)\left[1 + M \exp\left(-D_s^{\epsilon}(\rho\|\sigma)\right)\right]^{-1}
\end{aligned}
$$

$$
\begin{aligned}
1 - \Pr[\text{type II error}] &= \exp D_2(\sigma \| M^{-1}\rho + \sigma) \\
&\geq (1 + M^{-1})^{-1},
\end{aligned}
$$

A one-shot hypothesis testing

$$\begin{aligned} 1 - \Pr[\text{type I error}] &= \exp D_2(\rho||\rho + M\sigma) \\ &\geq (1-\epsilon)\left[1 + M\exp\left(-D_s^\epsilon(\rho\|\sigma)\right)\right]^{-1} \end{aligned}$$

$$\begin{aligned} 1 - \Pr[\text{type II error}] &= \exp D_2(\sigma\|M^{-1}\rho + \sigma) \\ &\geq (1 + M^{-1})^{-1}, \end{aligned}$$

Theorem

$$-\log \beta_{2\epsilon}(\rho\|\sigma) \geq D_s^\epsilon(\rho\|\sigma) + \log \epsilon.$$

A one-shot hypothesis testing

$$\begin{aligned} 1 - \Pr[\text{type I error}] &= \exp D_2(\rho\|\rho + M\sigma) \\ &\geq (1-\epsilon)\left[1 + M\exp\left(-D_s^{\epsilon}(\rho\|\sigma)\right)\right]^{-1} \end{aligned}$$

$$\begin{aligned} 1 - \Pr[\text{type II error}] &= \exp D_2(\sigma\|M^{-1}\rho + \sigma) \\ &\geq (1 + M^{-1})^{-1}, \end{aligned}$$

Theorem

$$-\log \beta_{2\epsilon}(\rho\|\sigma) \geq D_s^{\epsilon}(\rho\|\sigma) + \log \epsilon.$$

Corollary

$$-\log \beta_{\epsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\epsilon) + o(n).$$

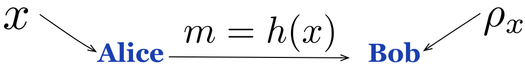
This upper bound is tight [Tomamichel & Hayashi '12, Li '12]

Source compression with side information

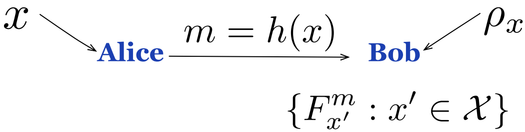
x → **Alice**

Bob ← ρ_x

Source compression with side information

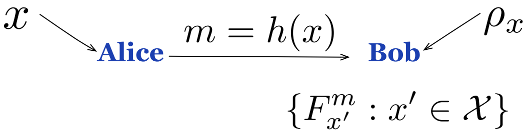


Source compression with side information



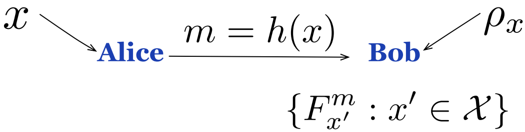
- $\rho_{XY} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x$

Source compression with side information



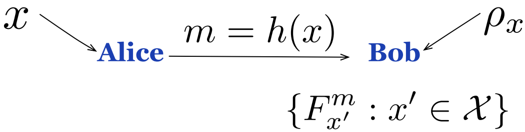
- $\rho_{XY} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x$
- $\Pr[\text{succ}] = \sum_{x,m} p_X(x) \mathbf{1}_{\{m=h(x)\}} \text{tr}(\rho_x F_x^m)$

Source compression with side information



- $\rho_{XY} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x$
- $\Pr[\text{succ}] = \sum_{x,m} p_X(x) \mathbf{1}_{\{m=h(x)\}} \text{tr}(\rho_x F_x^m)$
- pick a random $\mathtt{h} : \mathcal{X} \to \{1, \ldots, M\}$

Source compression with side information



- $\rho_{XY} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x$
- $\Pr[\text{succ}] = \sum_{x,m} p_X(x) \mathbf{1}_{\{m=h(x)\}} \operatorname{tr}(\rho_x F^m_x)$
- pick a random $\mathtt{h} : \mathcal{X} \to \{1, \ldots, M\}$
- Let $\{F^m_x : x \in \mathcal{X}\}$ be the pretty good measurement for

$$\{p(x)\rho_x | \, x \in \mathcal{X}, \mathtt{h}(x) = m\}$$

Source compression with side information

$$\sigma_{XB} = \sum_x p(x) \mathbf{1}_{\{\mathtt{h}(x)=1\}} |x\rangle\langle x| \otimes \rho_x,$$
$$\tau_{XB} = \left(\sum_x \mathbf{1}_{\{\mathtt{h}(x)=1\}} |x\rangle\langle x| \right) \otimes \left(\sum_{x'} p(x') \mathbf{1}_{\{\mathtt{h}(x')=1\}} \rho_{x'} \right).$$

$$\mathbb{E}_{\mathtt{h}} \Pr[\text{succ}] = M \mathbb{E}_{\mathtt{h}} \exp D_2(\sigma_{XB} \| \tau_{XB})$$

Source compression with side information

$$\sigma_{XB} = \sum_x p(x)\mathbf{1}_{\{\mathtt{h}(x)=1\}}|x\rangle\langle x| \otimes \rho_x,$$
$$\tau_{XB} = \Big(\sum_x \mathbf{1}_{\{\mathtt{h}(x)=1\}}|x\rangle\langle x|\Big) \otimes \Big(\sum_{x'} p(x')\mathbf{1}_{\{\mathtt{h}(x')=1\}}\rho_{x'}\Big).$$

$$\mathbb{E}_{\mathtt{h}}\Pr[\text{succ}] = M\mathbb{E}_{\mathtt{h}} \exp D_2(\sigma_{XB}\|\tau_{XB})$$

Theorem

There exists some $h : \mathcal{X} \to \{1, \ldots, M\}$ s.t.

$$\Pr[\text{succ}] \geq \exp D_2\left(\rho_{XB}\Big\|\big(1 - \frac{1}{M}\big)\rho_{XB} + \frac{1}{M}I_X \otimes \rho_B\right)$$
$$\geq \frac{1-\epsilon}{1 + M^{-1}\exp\big(-D_s^{\epsilon}(\rho_{XB}\|I_X \otimes \rho_B)\big)}$$

Source compression with side information

$$\sigma_{XB} = \sum_x p(x)\mathbf{1}_{\{\mathtt{h}(x)=1\}}|x\rangle\langle x| \otimes \rho_x,$$
$$\tau_{XB} = \Big(\sum_x \mathbf{1}_{\{\mathtt{h}(x)=1\}}|x\rangle\langle x|\Big) \otimes \Big(\sum_{x'} p(x')\mathbf{1}_{\{\mathtt{h}(x')=1\}}\rho_{x'}\Big).$$

$$\mathbb{E}_{\mathtt{h}}\Pr[\mathrm{succ}] = M\mathbb{E}_{\mathtt{h}} \exp D_2(\sigma_{XB}\|\tau_{XB})$$

Theorem

There exists some $h : \mathcal{X} \to \{1, \ldots, M\}$ s.t.

$$\Pr[\mathrm{succ}] \geq \exp D_2\left(\rho_{XB}\Big\|(1-\frac{1}{M})\rho_{XB} + \frac{1}{M}I_X \otimes \rho_B\right)$$
$$\geq \frac{1-\epsilon}{1 + M^{-1}\exp\big(-D_s^\epsilon(\rho_{XB}\|I_X \otimes \rho_B)\big)}$$

This also gives a second order asymptotics which again is tight [Tomamichel & Hayashi '12]

Our contribution

- Reformulation of the technique of Yassaee et al (2013)
- Stochastic likelihood = pretty good measurement
- Collision relative entropy: $D_2(\cdot\|\cdot)$
- Information spectrum relative entropy: $D_s^\epsilon(\cdot\|\cdot)$
    - c-q channel coding
    - quantum hypothesis testing
    - source compression of quantum side information

Our contribution

- Reformulation of the technique of Yassaee et al (2013)
- Stochastic likelihood = pretty good measurement
- Collision relative entropy: $D_2(\cdot\|\cdot)$
- Information spectrum relative entropy: $D_s^\epsilon(\cdot\|\cdot)$
    - c-q channel coding
    - quantum hypothesis testing
    - source compression of quantum side information
- We avoided Hayashi-Nagaoka operator inequality

What else?

- Quantum capacity: achievability of coherent information?

What else?

- Quantum capacity: achievability of coherent information?
- Entanglement-assisted capacity [Datta, Tomamichel, Wilde '14]

What else?

- Quantum capacity: achievability of coherent information?
- Entanglement-assisted capacity [Datta, Tomamichel, Wilde '14]
- Yassaee et al apply this method to
  - Gelfand-Pinsker (coding over a state-dependent channel)
  - Broadcast channel (Marton bound)
  - Multiple access channel (MAC)

What else?

- Quantum capacity: achievability of coherent information?
- Entanglement-assisted capacity [Datta, Tomamichel, Wilde '14]
- Yassaee et al apply this method to
  - Gelfand-Pinsker (coding over a state-dependent channel)
  - Broadcast channel (Marton bound)
  - Multiple access channel (MAC)
- Need more convexity properties in the quantum case
  - Yassaee et al use the joint convexity of $(x, y) \mapsto \frac{1}{xy}$

Thanks for your attention!