# Moderate deviation analysis for c-q channels (and hypothesis testing)

# Christopher T. Chubb

physics.usyd.edu.au/~cchubb/

Centre for Engineered Quantum Systems University of Sydney





# Hao-Chung Cheng

Centre for Quantum Software and Information University of Technology Sydney



QIP 2018 QuTech, TU Delft

US

Refined small-deviation analysis:

• "Moderate deviation analysis for classical communication over quantum channels", Christopher T. Chubb, Vincent Y.F. Tan, and Marco Tomamichel, Communications in Mathematical Physics (2017) 355: 1283, arXiv:1701.03114.

Refined large-deviation analysis:

- "Moderate Deviation Analysis for Classical-Quantum Channels and Quantum Hypothesis Testing", **Hao-Chung Cheng** and Min-Hsiu Hsieh, IEEE Transactions on Information Theory (to appear), arXiv:1701.03195.
- "Quantum Sphere-Packing Bounds with Polynomial Prefactors", Hao-Chung Cheng, Min-Hsiu Hsieh, and Marco Tomamichel, arXiv:1704.05703.

- Number of channel uses
- Amount of information transmitted
- Error probability





- Number of channel uses
- Amount of information transmitted
- Error probability





- Number of channel uses
- Amount of information transmitted
- Error probability





- Number of channel uses
- Amount of information transmitted
- Error probability





- Number of channel uses
- Amount of information transmitted
- Error probability



- Number of channel uses
- Amount of information transmitted
- Error probability



- Number of channel uses
- Amount of information transmitted
- Error probability

If we have access to a quantum channel, then quantum encoding/decoding can allow us to transmit more information with less error than classical encoding/decoding.

A simple example is a bit-flip channel

$$\mathcal{E}(\rho) = p X \rho X + (1-p)\rho.$$

Classically: Either we send many noisy bits, or fewer encoded bits.

Quantumly: Simply transmit our bits noiselessly in the X basis  $\{|+\rangle, |-\rangle\}$ .

We are going to consider coding of classical-quantum channels.

For c-q channel W, a  $(n, R, \epsilon)$ -code is an encoder E and decoding POVM  $\{D_i\}$  such that

$$\frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}\mathsf{Tr}\left[\mathcal{W}^{\otimes n}\left(\otimes_{i=1}^{n}E_{i}(m)\right)D_{m}\right]\geq1-\epsilon$$

We will be concerned with the trade-off between the <u>block-length</u> n, the <u>rate</u> R, and the <u>error probability</u>  $\epsilon$ . We define the optimal rate/error probability as

$$R^*(\mathcal{W}; n, \epsilon) := \max \{ R \mid \exists (n, R, \epsilon) \text{-code} \}, \\ \epsilon^*(\mathcal{W}; n, R) := \min \{ \epsilon \mid \exists (n, R, \epsilon) \text{-code} \}.$$

For a constant error probability  $\epsilon$ , the Strong Converse Theorem tells us the rate approaches a constant known as the <u>capacity</u>

$$\lim_{n\to\infty} R^*(\mathcal{W}; n, \epsilon) = C(\mathcal{W}).$$

Equivalently this means that the error probability must to go 0 to 1 either side of the capacity

$$\lim_{n\to\infty} \epsilon^*(\mathcal{W}; n, R) = \begin{cases} 0 & : R < C(\mathcal{W}) \\ 1 & : R > C(\mathcal{W}) \end{cases}$$

This tells us we can have either  $R \rightarrow C \text{ OR } \epsilon \rightarrow 0$ .

How fast are these convergences? Can we do both?

For a constant error probability  $\epsilon$ , the Strong Converse Theorem tells us the rate approaches a constant known as the <u>capacity</u>

$$\lim_{n\to\infty} R^*(\mathcal{W}; n, \epsilon) = C(\mathcal{W}).$$

Equivalently this means that the error probability must to go 0 to 1 either side of the capacity

$$\lim_{n\to\infty} \epsilon^*(\mathcal{W}; n, R) = \begin{cases} 0 & : R < C(\mathcal{W}) \\ 1 & : R > C(\mathcal{W}) \end{cases}$$

This tells us we can have either  $R \rightarrow C \text{ OR } \epsilon \rightarrow 0$ .

How fast are these convergences? Can we do both?















#### Moderate deviations





#### Woderate deviation (This work)

For any  $\{a_n\}$  such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$  we have  $R^*(n, \epsilon_n) = C - \sqrt{2V}a_n + o(a_n)$  for  $\epsilon_n = e^{-na_n^2}$ , or equivalently

 $\ln \epsilon^*(n, R_n) = -\frac{na_n^2}{2V} + o(na_n^2) \quad \text{for} \quad R_n = -\frac{na_n^2}{2V} + o(na_n^2)$ 

#### Moderate deviations



#### Moderate deviation (This work)

For any  $\{a_n\}$  such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$  we have  $R^*(n, \epsilon_n) = C - \sqrt{2V}a_n + o(a_n)$  for  $\epsilon_n = e^{-na_n^2}$ , or equivalently

$$\operatorname{n} \epsilon^*(n, R_n) = -\frac{na_n^2}{2V} + o(na_n^2) \quad \text{for} \quad R_n = C - a_n.$$

#### Moderate deviations

What if we want  $R \rightarrow C$  AND  $\epsilon \rightarrow 0$ ? 1 - $\epsilon$ 0 R Moderate deviation (This work) For any  $\{a_n\}$  such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$  we have  $R^*(n,\epsilon_n) = C - \sqrt{2V}a_n + o(a_n)$  for  $\epsilon_n = e^{-na_n^2}$ , or equivalently  $\ln \epsilon^*(n, R_n) = -\frac{na_n^2}{2M} + o(na_n^2) \quad \text{for} \quad R_n = C - a_n.$ 

# Concentration inequalities

Take 
$$\{X_i\}$$
 iid with  $\mathbb{E}[X_i] = 0$  and  $\operatorname{Var}[X_i] =: V$ , and  $\bar{X}_n := \frac{1}{n} \sum_{i=1}^n X_i$ .

Asymptotic (Law of large numbers)

$$\lim_{n\to\infty} \Pr\left[\bar{X}_n \ge t\right] = \begin{cases} 1 & t < 0, \\ 0 & t > 0. \end{cases}$$

Small deviation (Berry-Esseen)Large deviation (Cramér)
$$\Pr\left[\bar{X}_n \ge \frac{\epsilon}{\sqrt{n}}\right] = Q\left(\frac{\epsilon}{\sqrt{V}}\right) + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right) \quad \epsilon \in (0,1)$$
 $\ln \Pr\left[\bar{X}_n \ge t\right] = -n \cdot I(t) + o(n) \quad t \ge 0$ 

Moderate deviation

For any 
$$\{a_n\}$$
 such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$ 

$$\ln \Pr\left[\bar{X}_n \ge a_n\right] = -\frac{na_n^2}{2V} + o(na_n^2)$$

# Concentration inequalities

Take 
$$\{X_i\}$$
 iid with  $\mathbb{E}[X_i] = 0$  and  $\operatorname{Var}[X_i] =: V$ , and  $\bar{X}_n := \frac{1}{n} \sum_{i=1}^n X_i$ .

Asymptotic (Law of large numbers)

$$\lim_{n\to\infty} \Pr\left[\bar{X}_n \ge t\right] = \begin{cases} 1 & t < 0, \\ 0 & t > 0. \end{cases}$$

Small deviation (Berry-Esseen)Large deviation (Cramér)
$$\Pr\left[\bar{X}_n \ge \frac{\epsilon}{\sqrt{n}}\right] = Q\left(\frac{\epsilon}{\sqrt{V}}\right) + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right) \quad \epsilon \in (0,1)$$
 $\ln \Pr\left[\bar{X}_n \ge t\right] = -n \cdot l(t) + o(n) \quad t \ge 0$ 

Moderate deviation

For any 
$$\{a_n\}$$
 such that  $a_n o 0$  and  $\sqrt{n}a_n o \infty$ 

$$\operatorname{n}\operatorname{Pr}\left[\bar{X}_n \ge a_n\right] = -\frac{na_n^2}{2V} + o(na_n^2)$$

# Concentration inequalities

Take 
$$\{X_i\}$$
 iid with  $\mathbb{E}[X_i] = 0$  and  $\operatorname{Var}[X_i] =: V$ , and  $\bar{X}_n := \frac{1}{n} \sum_{i=1}^n X_i$ .

Asymptotic (Law of large numbers)

$$\lim_{n\to\infty} \Pr\left[\bar{X}_n \ge t\right] = \begin{cases} 1 & t < 0, \\ 0 & t > 0. \end{cases}$$

Small deviation (Berry-Esseen)Large deviation (Cramér)
$$\Pr\left[\bar{X}_n \ge \frac{\epsilon}{\sqrt{n}}\right] = Q\left(\frac{\epsilon}{\sqrt{V}}\right) + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right) \quad \epsilon \in (0,1)$$
 $\ln \Pr\left[\bar{X}_n \ge t\right] = -n \cdot I(t) + o(n) \quad t \ge 0$ 

Moderate deviation

For any 
$$\{a_n\}$$
 such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$ 

$$\ln \Pr\left[\bar{X}_n \ge a_n\right] = -\frac{na_n^2}{2V} + o(na_n^2).$$

# Hypothesis testing

We want to test between two hypotheses,  $\rho$  and  $\sigma$ . For a binary POVM  $\{A, I - A\}$ , we define the type-I and type-II errors as

$$\alpha(A; \rho, \sigma) := \operatorname{Tr}(I - A)\rho, \qquad \beta(A; \rho, \sigma) := \operatorname{Tr} A\sigma,$$

and the  $\epsilon$ -hypothesis-testing divergence

$$D_h^{\epsilon}(\rho \| \sigma) := -\log \min_{0 \le A \le I} \left\{ \beta(A; \rho, \sigma) \, | \, \alpha(A; \rho, \sigma) \le \epsilon \right\}.$$

If we now consider testing between  $ho^{\otimes n}$  and  $\sigma^{\otimes n}$ , then the asymptotic behaviour is given by Quantum Stein's Lemma.

Asymptotics (Hiai and Petz 1991, Ogawa and Nagaoka 1999) For any  $\epsilon \in (0, 1)$  $\lim_{n \to \infty} \frac{1}{n} D_h^{\epsilon}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma).$ 

# Hypothesis testing

We want to test between two hypotheses,  $\rho$  and  $\sigma$ . For a binary POVM  $\{A, I - A\}$ , we define the type-I and type-II errors as

$$\alpha(A; \rho, \sigma) := \operatorname{Tr}(I - A)\rho, \qquad \beta(A; \rho, \sigma) := \operatorname{Tr} A\sigma,$$

and the  $\epsilon$ -hypothesis-testing divergence

$$D_h^{\epsilon}(\rho \| \sigma) := -\log \min_{0 \le A \le I} \left\{ \beta(A; \rho, \sigma) \, | \, \alpha(A; \rho, \sigma) \le \epsilon \right\}.$$

If we now consider testing between  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$ , then the asymptotic behaviour is given by Quantum Stein's Lemma.

Asymptotics (Hiai and Petz 1991, Ogawa and Nagaoka 1999) For any  $\epsilon \in (0, 1)$  $\lim_{n \to \infty} \frac{1}{n} D_h^{\epsilon}(\rho^{\otimes n} || \sigma^{\otimes n}) = D(\rho || \sigma).$  Small deviation (Tomamichel and Hayashi 2013, Li 2014)

$$\frac{1}{n}D_h^{\epsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma) + \sqrt{\frac{V(\rho\|\sigma)}{n}}\Phi^{-1}(\epsilon) + \mathcal{O}\left(\frac{\log n}{n}\right) \quad \text{for} \quad \epsilon \in (0,1).$$

Large deviation (Hayashi 2006, Nagaoka 2006)

$$\ln \epsilon_n = -n \cdot E(R) + o(n) \quad \text{for} \quad \frac{1}{n} D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = R < D(\rho \| \sigma).$$

#### Moderate deviation (This work)

For any 
$$\{a_n\}$$
 such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$  and  $\epsilon_n := e^{-na_n^2}$ ,  
$$\frac{1}{n}D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma) - \sqrt{2V(\rho \| \sigma)}a_n + o(a_n).$$

Small deviation (Tomamichel and Hayashi 2013, Li 2014)

$$\frac{1}{n}D_h^{\epsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma) + \sqrt{\frac{V(\rho\|\sigma)}{n}}\Phi^{-1}(\epsilon) + \mathcal{O}\left(\frac{\log n}{n}\right) \quad \text{for} \quad \epsilon \in (0,1).$$

Large deviation (Hayashi 2006, Nagaoka 2006)

$$\ln \epsilon_n = -n \cdot E(R) + o(n) \quad \text{for} \quad \frac{1}{n} D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = R < D(\rho \| \sigma).$$

Moderate deviation (This work)

For any 
$$\{a_n\}$$
 such that  $a_n \to 0$  and  $\sqrt{n}a_n \to \infty$  and  $\epsilon_n := e^{-na_n^2}$ ,  
 $\frac{1}{n}D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma) - \sqrt{2V(\rho \| \sigma)}a_n + o(a_n).$ 

# Bounding the rate

For this we can use the one shot bounds

$$R^{*}(1,\epsilon) \geq \sup_{P_{X}} D_{h}^{\epsilon/2}(\pi_{XY} \| \pi_{X} \otimes \pi_{Y}) - \mathcal{O}(1), \qquad (\text{Wang and Renner 2012})$$
$$R^{*}(1,\epsilon) \leq \inf_{\sigma} \sup_{\rho \in \text{Im}(\mathcal{W})} D_{h}^{2\epsilon}(\rho \| \sigma) + \mathcal{O}(1), \qquad (\text{Tomamichel and Tan 2015})$$

where 
$$\pi_{XY} = \sum_{x} P_X(x) |x\rangle \langle x|_X \otimes \rho_Y^{(x)}$$
.

This give *n*-shot bounds

$$R^*(n,\epsilon_n) \ge \sup_{P_{X^n}} \frac{1}{n} D_h^{\epsilon_n/2}(\pi_{X^nY^n} \| \pi_{X^n} \otimes \pi_{Y^n}) - \mathcal{O}(1/n)$$
$$R^*(n,\epsilon_n) \le \inf_{\sigma^n} \sup_{\rho^n \in \operatorname{Im}(\mathcal{W}^{\otimes n})} \frac{1}{n} D_h^{2\epsilon_n}(\rho^n \| \sigma^n) + \mathcal{O}(1/n).$$

This now reduces the problem of proving a moderate deviation bound for channels to hypothesis testing.

# Bounding the rate

For this we can use the one shot bounds

$$\begin{aligned} R^*(1,\epsilon) &\geq \sup_{P_X} D_h^{\epsilon/2}(\pi_{XY} \| \pi_X \otimes \pi_Y) - \mathcal{O}(1), \qquad \text{(Wang and Renner 2012)} \\ R^*(1,\epsilon) &\leq \inf_{\sigma} \sup_{\rho \in \operatorname{Im}(\mathcal{W})} D_h^{2\epsilon}(\rho \| \sigma) + \mathcal{O}(1), \qquad \text{(Tomamichel and Tan 2015)} \end{aligned}$$

where  $\pi_{XY} = \sum_{x} P_X(x) |x\rangle \langle x|_X \otimes \rho_Y^{(x)}$ .

This give *n*-shot bounds

$$R^*(n,\epsilon_n) \geq \sup_{P_{X^n}} \frac{1}{n} D_h^{\epsilon_n/2}(\pi_{X^nY^n} \| \pi_{X^n} \otimes \pi_{Y^n}) - \mathcal{O}(1/n)$$
  
$$R^*(n,\epsilon_n) \leq \inf_{\sigma^n} \sup_{\rho^n \in \operatorname{Im}(\mathcal{W}^{\otimes n})} \frac{1}{n} D_h^{2\epsilon_n}(\rho^n \| \sigma^n) + \mathcal{O}(1/n).$$

This now reduces the problem of proving a moderate deviation bound for channels to hypothesis testing.

# Bounding the rate

For this we can use the one shot bounds

$$\begin{aligned} R^*(1,\epsilon) &\geq \sup_{P_X} D_h^{\epsilon/2}(\pi_{XY} \| \pi_X \otimes \pi_Y) - \mathcal{O}(1), \qquad \text{(Wang and Renner 2012)} \\ R^*(1,\epsilon) &\leq \inf_{\sigma} \sup_{\rho \in \operatorname{Im}(\mathcal{W})} D_h^{2\epsilon}(\rho \| \sigma) + \mathcal{O}(1), \qquad \text{(Tomamichel and Tan 2015)} \end{aligned}$$

where  $\pi_{XY} = \sum_{x} P_X(x) |x\rangle \langle x|_X \otimes \rho_Y^{(x)}$ .

This give *n*-shot bounds

$$R^*(n,\epsilon_n) \geq \sup_{P_{X^n}} \frac{1}{n} D_h^{\epsilon_n/2}(\pi_{X^nY^n} \| \pi_{X^n} \otimes \pi_{Y^n}) - \mathcal{O}(1/n),$$
  
$$R^*(n,\epsilon_n) \leq \inf_{\sigma^n} \sup_{\rho^n \in \operatorname{Im}(\mathcal{W}^{\otimes n})} \frac{1}{n} D_h^{2\epsilon_n}(\rho^n \| \sigma^n) + \mathcal{O}(1/n).$$

This now reduces the problem of proving a moderate deviation bound for channels to hypothesis testing.

## Reducing hyp. testing to concentration inequalities

To give a moderate deviation analysis of the HTD, we will use concentration bounds. First we see it is related to tail bounds of the Nussbaum-Szkoła distributions<sup>1</sup>

$$P^{
ho,\sigma}(a,b):=r_a|\langle \phi_a|\psi_b
angle|^2 \quad ext{and} \quad Q^{
ho,\sigma}(a,b):=s_b|\langle \phi_a|\psi_b
angle|^2,$$

where we have eigendecomposed our states  $\rho := \sum_{a} r_{a} |\phi_{a}\rangle \langle \phi_{a}|$  and  $\sigma := \sum_{b} s_{b} |\psi_{b}\rangle \langle \psi_{b}|$ . These reproduce the first two moments of our states 1

$$D\left(P^{
ho,\sigma}\|Q^{
ho,\sigma}
ight)=D(
ho\|\sigma)\qquad ext{and}\qquad V\left(P^{
ho,\sigma}\|Q^{
ho,\sigma}
ight)=V(
ho\|\sigma).$$

$$\frac{1}{n} D_h^{\epsilon_n} \left( \rho^{\otimes n} \big\| \sigma^{\otimes n} \right) \ge \sup \left\{ R \left| \Pr\left[ \sum_{i=1}^n Z_i \right] \le \epsilon_n / 2 \right\} - \mathcal{O}(\log 1 / \epsilon_n), \\ \frac{1}{n} D_h^{\epsilon_n} \left( \rho^{\otimes n} \big\| \sigma^{\otimes n} \right) \le \sup \left\{ R \left| \Pr\left[ \sum_{i=1}^n Z_i \right] \le 2\epsilon_n \right\} + \mathcal{O}(\log 1 / \epsilon_n). \right.$$

<sup>1</sup>Nussbaum and Szkoła 2009

## Reducing hyp. testing to concentration inequalities

To give a moderate deviation analysis of the HTD, we will use concentration bounds. First we see it is related to tail bounds of the <u>Nussbaum-Szkoła</u> distributions<sup>1</sup>

$$\mathcal{P}^{
ho,\sigma}(a,b):=r_a|\langle \phi_a|\psi_b
angle|^2 \quad ext{and} \quad Q^{
ho,\sigma}(a,b):=s_b|\langle \phi_a|\psi_b
angle|^2,$$

where we have eigendecomposed our states  $\rho := \sum_{a} r_{a} |\phi_{a}\rangle\langle\phi_{a}|$  and  $\sigma := \sum_{b} s_{b} |\psi_{b}\rangle\langle\psi_{b}|$ . These reproduce the first two moments of our states  $D(P^{\rho,\sigma} ||Q^{\rho,\sigma}) = D(\rho ||\sigma)$  and  $V(P^{\rho,\sigma} ||Q^{\rho,\sigma}) = V(\rho ||\sigma)$ .

Specifically for iid  $Z_i = \log P^{
ho,\sigma}/Q^{
ho,\sigma}$  and  $(a_i,b_i) \sim P^{
ho,\sigma}$ , then<sup>2</sup>

$$\frac{1}{n} D_h^{\epsilon_n} \left( \rho^{\otimes n} \big\| \sigma^{\otimes n} \right) \ge \sup \left\{ R \left| \Pr\left[ \sum_{i=1}^n Z_i \right] \le \epsilon_n / 2 \right\} - \mathcal{O}(\log 1 / \epsilon_n), \\ \frac{1}{n} D_h^{\epsilon_n} \left( \rho^{\otimes n} \big\| \sigma^{\otimes n} \right) \le \sup \left\{ R \left| \Pr\left[ \sum_{i=1}^n Z_i \right] \le 2\epsilon_n \right\} + \mathcal{O}(\log 1 / \epsilon_n). \right.$$

<sup>1</sup>Nussbaum and Szkoła 2009. <sup>2</sup>Tomamichel and Hayashi 2013

# Different regimes






















# From large deviation regime



Is the reliable communication possible as rate approaches capacity?

# From large deviation regime

Is the reliable communication possible as rate approaches capacity?

• Let 
$$R_n = \mathsf{C} - a_n$$
, where 
$$\begin{cases} (i) \lim_{n \to \infty} a_n = 0 \\ (ii) \lim_{n \to \infty} \sqrt{n} a_n = \infty \end{cases}$$

### From large deviation regime

Is the reliable communication possible as rate approaches capacity?

• Let 
$$R_n = \mathsf{C} - a_n$$
, where 
$$\begin{cases} (i) \lim_{n \to \infty} a_n = 0 \\ (ii) \lim_{n \to \infty} \sqrt{n} a_n = \infty \end{cases}$$

$$\epsilon^*(n, R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\} \to 0$$

$$R^*(n, \epsilon_n) = \mathsf{C} - \sqrt{2\mathsf{V}}a_n + o(a_n)$$
$$\epsilon_n = \exp\{-na_n^2\}$$

Channel coding

$$\epsilon^*(n, R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}$$
$$R_n = \mathsf{C} - a_n$$

$$R^{*}(n, \epsilon_{n}) = C - \sqrt{2V}a_{n} + o(a_{n})$$

$$\epsilon_{n} = \exp\{-na_{n}^{2}\}$$
Channel coding
$$R_{n} = C - a_{n}$$

$$R_{n} = C - a_{n}$$

$$R_{n} = C - a_{n}$$

$$\frac{1}{n}\log\beta_{n}^{*} \rightarrow D - \sqrt{2V}a_{n},$$

$$\alpha_{n} \le \exp\{-na_{n}^{2}\}$$
Hypothesis testing
$$\alpha_{n} \le \exp\{-n[D - a_{n}]\}$$



#### Moderate deviations for hypothesis testing

• Type-I, -II errors:  $\alpha_n := \operatorname{Tr} \left[ (\mathbbm{1} - A_n) \rho^{\otimes n} \right]$  $\beta_n := \operatorname{Tr} \left[ A_n \sigma^{\otimes n} \right]$ 

• Given 
$$\beta_n \leq \exp\{-nR\}$$

Quantum Stein's lemma (Hiai and Petz 1991, Ogawa and Nagaoka 1999)

$$\alpha_n^* \to \begin{cases} 0, & R < D(\rho \| \sigma) \\ 1, & R > D(\rho \| \sigma) \end{cases}$$

#### Moderate deviations for hypothesis testing

• Type-I, -II errors:  $\alpha_n := \operatorname{Tr} \left[ (\mathbbm{1} - A_n) \rho^{\otimes n} \right]$  $\beta_n := \operatorname{Tr} \left[ A_n \sigma^{\otimes n} \right]$ 

• Given 
$$\beta_n \leq \exp\{-nR\}$$

Quantum Stein's lemma (Hiai and Petz 1991, Ogawa and Nagaoka 1999)

$$\alpha_n^* \to \begin{cases} 0, & R < D(\rho \| \sigma) \\ 1, & R > D(\rho \| \sigma) \end{cases}$$

• Question:  $\alpha_n^* \to 0$ ? given  $\beta_n \le \exp\{-n[D(\rho \| \sigma) - a_n]\}$ 

#### Moderate deviations for hypothesis testing

• Type-I, -II errors: 
$$\alpha_n := \operatorname{Tr} \left[ (\mathbbm{1} - A_n) \rho^{\otimes n} \right]$$
  
 $\beta_n := \operatorname{Tr} \left[ A_n \sigma^{\otimes n} \right]$ 

• Given 
$$\beta_n \leq \exp\{-nR\}$$

Quantum Stein's lemma (Hiai and Petz 1991, Ogawa and Nagaoka 1999)

$$\alpha_n^* \to \begin{cases} 0, & R < D(\rho \| \sigma) \\ 1, & R > D(\rho \| \sigma) \end{cases}$$

• Question:  $\alpha_n^* \to 0$ ? given  $\beta_n \le \exp\{-n[D(\rho \| \sigma) - a_n]\}$ 

Answer: 
$$\alpha_n^* = \exp\left\{-\frac{na_n^2}{2V(\rho\|\sigma)} + o(na_n^2)\right\} \to 0$$

• Quantum Hoeffding bound (  $\beta_n \leq \exp\{-nR\}$  )

$$\alpha_n^* = \exp\{-n\mathsf{E}(R) + o(n)\}$$

$$\sup_{0 < \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{\alpha}(\rho \| \sigma) - R \right)$$

Achievability (Audenaert et al. 2007, Hayashi 2007, Audenaert, Nussbaum, Szkola, Verstraete 2008)

$$\alpha_n^* \leq \exp\{-n\mathsf{E}(R)\}$$

• Quantum Hoeffding bound (  $\beta_n \leq \exp\{-nR\}$  )

$$\alpha_n^* = \exp\{-n\mathsf{E}(R) + o(n)\}$$

$$\sup_{0 < \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{\alpha}(\rho \| \sigma) - R \right)$$

$$\left(\begin{array}{c} \frac{\mathsf{E}(D(\rho \| \sigma) - a_n)}{a_n^2} \to \frac{1}{2V(\rho \| \sigma)} \end{array}\right)$$

Achievability (Audenaert et al. 2007, Hayashi 2007, Audenaert, Nussbaum, Szkola, Verstraete 2008)

$$\alpha_n^* \le \exp\{-n\mathsf{E}(R)\} \qquad \Rightarrow \alpha_n^* \le \exp\left\{-\frac{na_n^2}{2V(\rho\|\sigma)} + o(na_n^2)\right\}$$

• Quantum Hoeffding bound (  $\beta_n \leq \exp\{-nR\}$  )

$$\alpha_n^* = \exp\{-n\mathsf{E}(R) + o(n)\}$$

$$\sup_{0 < \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{\alpha}(\rho \| \sigma) - R \right)$$

$$\boxed{\frac{\mathsf{E}(D(\rho \| \sigma) - a_n)}{a_n^2} \to \frac{1}{2V(\rho \| \sigma)}}$$

 $\alpha_n^* \ge \exp\{-n\mathsf{E}(R) + O(\sqrt{n})\}$ 

• Quantum Hoeffding bound (  $\beta_n \leq \exp\{-nR\}$  )

$$\alpha_n^* = \exp\{-n\mathsf{E}(R) + o(n)\}$$

$$\sup_{0 < \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{\alpha}(\rho \| \sigma) - R \right)$$

$$\boxed{ \frac{\mathsf{E}(D(\rho \| \sigma) - a_n)}{a_n^2} \to \frac{1}{2V(\rho \| \sigma)} }$$

• Quantum Hoeffding bound (  $\beta_n \leq \exp\{-nR\}$  )

$$\alpha_n^* = \exp\{-n\mathsf{E}(R) + o(n)\}$$

$$\sup_{0 < \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{\alpha}(\rho \| \sigma) - R \right)$$

$$\boxed{ \frac{\mathsf{E}(D(\rho \| \sigma) - a_n)}{a_n^2} \to \frac{1}{2V(\rho \| \sigma)} }$$

Converse (Nagaoka 2006)

Moderate deviations

## Channel coding

• Goal: for  $R_n = \mathsf{C} - a_n$ ,

$$\Rightarrow \epsilon^*(n, R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}$$
  
Information variance  
$$\mathsf{V} := \sup_{\rho_X: I(X:B)_\rho = \mathsf{C}} V(\rho_{XB} \| \rho_X \otimes \rho_B)$$

- Challenges:
  - The optimal error exponent is still open
  - Need a tight finite blocklength analysis for the optimal error probability

## Achievability

• Hayashi 2007:  $\epsilon^*(n, R) \le 4 \exp\left\{-n \mathsf{E}_{\mathbf{r}}^{\downarrow}(R)\right\}$ 

$$\max_{\frac{1}{2} \le \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{2 - \frac{1}{\alpha}}(\rho_{XB} \| \rho_X \otimes \rho_B) - R \right)$$

#### Achievability

• Hayashi 2007:  $\epsilon^*(n, R) \le 4 \exp\left\{-n\mathsf{E}^{\downarrow}_{\mathbf{r}}(R)\right\}$ 

$$\max_{\frac{1}{2} \le \alpha \le 1} \frac{1 - \alpha}{\alpha} \left( D_{2 - \frac{1}{\alpha}}(\rho_{XB} \| \rho_X \otimes \rho_B) - R \right)$$

• Asymptotic expansion:

$$\frac{\mathsf{E}_{\mathrm{r}}^{\downarrow}(\mathsf{C}-a_n)}{a_n^2} \to \frac{1}{2\mathsf{V}}$$

$$\epsilon^*(n, \mathbf{R}_n) \le \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}$$

• Winter 1999:

$$\lim_{n \to \infty} -\frac{1}{n} \log \epsilon^*(n, R) \le \widetilde{\mathsf{E}}_{\mathrm{sp}}(R) := \max_{\rho_X} \min_{\sigma_X B : \sigma_X = \rho_X} \left\{ D(\sigma_{XB} \| \rho_{XB}) : \mathsf{I}(X : B)_{\sigma} \le R \right\}$$

Dalai 2013:

$$\lim_{n \to \infty} -\frac{1}{n} \log \epsilon^*(n, R) \le \mathsf{E}_{\mathrm{sp}}(R) := \max_{\rho_X} \sup_{0 < \alpha \le 1} \min_{\sigma_B} \frac{1 - \alpha}{\alpha} \left( D_\alpha(\rho_{XB} \| \rho_X \otimes \sigma_B) - R \right)$$

- Questions:
  - What is the right exponent?
  - Finite blocklength bound with tight prefactor?

Classical approach (Altug, Wagner 2014)

$$\epsilon^*(n, R_n) \ge \exp\left\{-n\widetilde{\mathsf{E}}_{\mathrm{sp}}(R) + o(na_n^2)\right\}$$

Classical approach (Altug, Wagner 2014)

$$\epsilon^*(n, R_n) \ge \exp\left\{-n\widetilde{\mathsf{E}}_{\mathrm{sp}}(R) + o(na_n^2)\right\}$$

• Asymptotic expansion:

$$\frac{\widetilde{\mathsf{E}}_{\rm sp}(\mathsf{C}-a_n)}{a_n^2} \to \frac{1}{2\widetilde{\mathsf{V}}}$$

Classical approach (Altug, Wagner 2014)

$$\epsilon^*(n, R_n) \ge \exp\left\{-n\widetilde{\mathsf{E}}_{\mathrm{sp}}(R) + o(na_n^2)\right\}$$

$$V(\rho \| \sigma) := \operatorname{Tr} \left[ \rho (\log \rho - \log \sigma)^2 \right] - D(\rho \| \sigma)^2 \quad \text{[Li12, Tomamichel, Hayashi12]}$$
$$\widetilde{V}(\rho \| \sigma) := \int_0^1 \mathrm{d}t \operatorname{Tr} \left[ \rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma) \right] - D(\rho \| \sigma)^2$$

• Asymptotic expansion:

$$\frac{\widetilde{\mathsf{E}}_{\rm sp}(\mathsf{C}-a_n)}{a_n^2} \to \frac{1}{2\widetilde{\mathsf{V}}} \ge \frac{1}{2\mathsf{V}}$$

Classical approach (Altug, Wagner 2014)

$$\epsilon^*(n, R_n) \ge \exp\left\{-n\widetilde{\mathsf{E}}_{\mathrm{sp}}(R) + o(na_n^2)\right\}$$

$$V(\rho \| \sigma) := \operatorname{Tr} \left[ \rho(\log \rho - \log \sigma)^2 \right] - D(\rho \| \sigma)^2 \quad \text{[Li12, Tomamichel, Hayashi12]}$$
$$\widetilde{V}(\rho \| \sigma) := \int_0^1 \mathrm{d}t \operatorname{Tr} \left[ \rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma) \right] - D(\rho \| \sigma)^2$$

- Asymptotic expansion:  $\frac{\widetilde{\mathsf{E}}_{\mathrm{sp}}(\mathsf{C}-a_n)}{a_n^2} \to \frac{1}{2\widetilde{\mathsf{V}}} \ge \frac{1}{2\mathsf{V}}$
- Result: a tight sphere-packing bound

Dalai: 
$$\exp\{O(\sqrt{n})\}$$

$$\epsilon^*(n, R) \ge \frac{A}{(1 - \alpha^*)\sqrt{n}} \exp\{-n\mathsf{E}_{\mathrm{sp}}(R)\}$$

[arXiv:1704.05703]

Classical approach (Altug, Wagner 2014)

$$\epsilon^*(n, R_n) \ge \exp\left\{-n\widetilde{\mathsf{E}}_{\mathrm{sp}}(R) + o(na_n^2)\right\}$$

$$V(\rho \| \sigma) := \operatorname{Tr} \left[ \rho(\log \rho - \log \sigma)^2 \right] - D(\rho \| \sigma)^2 \quad \text{[Li12, Tomamichel, Hayashi12]}$$
$$\widetilde{V}(\rho \| \sigma) := \int_0^1 \mathrm{d}t \operatorname{Tr} \left[ \rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma) \right] - D(\rho \| \sigma)^2$$

- Asymptotic expansion:  $\frac{\widetilde{\mathsf{E}}_{\mathrm{sp}}(\mathsf{C}-a_n)}{a_n^2} \to \frac{1}{2\widetilde{\mathsf{V}}} \ge \frac{1}{2\mathsf{V}}$
- Result: a tight sphere-packing bound

Dalai: 
$$\exp\{O(\sqrt{n})\}$$

$$\epsilon^*(n, R) \ge \frac{A}{(1 - \alpha^*)\sqrt{n}} \exp\{-n\mathsf{E}_{\mathrm{sp}}(R)\}$$

[arXiv:1704.05703]

$$\epsilon^*(n, R_n) \ge \exp\left\{-rac{na_n^2}{2\mathsf{V}} + o(na_n^2)
ight\}$$

# Conclusions

- We study the fundamental trade-off between error, rate, and blocklength
  - How fast are the convergences  $R \to C$  or  $\epsilon \to 0$  as  $n \to \infty$ ?

## Conclusions

- We study the fundamental trade-off between error, rate, and blocklength
  - ▶ How fast are the convergences  $R \to C$  or  $\epsilon \to 0$  as  $n \to \infty$  ?

$$\begin{cases} R^*(n,\epsilon_n) = \mathsf{C} - \sqrt{2\mathsf{V}}a_n + o(a_n), & \epsilon_n = \exp\{-na_n^2\} \\ \epsilon^*(n,R_n) = \exp\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\}, & R_n = \mathsf{C} - a_n \end{cases}$$





### Conclusions

- We study the fundamental trade-off between error, rate, and blocklength
  - ▶ How fast are the convergences  $R \to C$  or  $\epsilon \to 0$  as  $n \to \infty$  ?

$$\begin{cases} R^*(n,\epsilon_n) = \mathsf{C} - \sqrt{2\mathsf{V}}a_n + o(a_n), & \epsilon_n = \exp\{-na_n^2\} \\ \epsilon^*(n,R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}, & R_n = \mathsf{C} - a_n \end{cases}$$

Moderate deviations for hypothesis testing

$$\begin{cases} \frac{1}{n} D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma) - \sqrt{2V(\rho \| \sigma)} a_n + o(a_n), \quad \epsilon_n := \exp\{-na_n^2\} \\ \frac{1}{n} D_h^{\exp\{-nR_n\}}(\rho^{\otimes n} \| \sigma^{\otimes n}) = \frac{a_n^2}{V(\rho \| \sigma)} + o(a_n^2), \quad R_n := D(\rho \| \sigma) - a_n \end{cases}$$
## Conclusions

- We study the fundamental trade-off between error, rate, and blocklength
  - ▶ How fast are the convergences  $R \to C$  or  $\epsilon \to 0$  as  $n \to \infty$  ?

$$\begin{cases} R^*(n,\epsilon_n) = \mathsf{C} - \sqrt{2\mathsf{V}}a_n + o(a_n), & \epsilon_n = \exp\{-na_n^2\} \\ \epsilon^*(n,R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}, & R_n = \mathsf{C} - a_n \end{cases}$$

Moderate deviations for hypothesis testing

$$\begin{cases} \frac{1}{n} D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma) - \sqrt{2V(\rho \| \sigma)} a_n + o(a_n), \quad \epsilon_n := \exp\{-na_n^2\} \\ \frac{1}{n} D_h^{\exp\{-nR_n\}}(\rho^{\otimes n} \| \sigma^{\otimes n}) = \frac{a_n^2}{V(\rho \| \sigma)} + o(a_n^2), \quad R_n := D(\rho \| \sigma) - a_n \end{cases}$$

Extension to image-additive channels – What about other channels (entanglementbreaking) or capacities (entanglement-assisted)?

## Conclusions

- We study the fundamental trade-off between error, rate, and blocklength
  - ▶ How fast are the convergences  $R \to C$  or  $\epsilon \to 0$  as  $n \to \infty$  ?

$$\begin{cases} R^*(n,\epsilon_n) = \mathsf{C} - \sqrt{2\mathsf{V}}a_n + o(a_n), & \epsilon_n = \exp\{-na_n^2\} \\ \epsilon^*(n,R_n) = \exp\left\{-\frac{na_n^2}{2\mathsf{V}} + o(na_n^2)\right\}, & R_n = \mathsf{C} - a_n \end{cases}$$

Moderate deviations for hypothesis testing

$$\begin{cases} \frac{1}{n} D_h^{\epsilon_n}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma) - \sqrt{2V(\rho \| \sigma)} a_n + o(a_n), \quad \epsilon_n := \exp\{-na_n^2\} \\ \frac{1}{n} D_h^{\exp\{-nR_n\}}(\rho^{\otimes n} \| \sigma^{\otimes n}) = \frac{a_n^2}{V(\rho \| \sigma)} + o(a_n^2), \quad R_n := D(\rho \| \sigma) - a_n \end{cases}$$

- Extension to image-additive channels What about other channels (entanglementbreaking) or capacities (entanglement-assisted)?
- Other applications private communications, classical data compression with quantum side information, etc.

## Different concentration regimes

Regimes	Channel Coding	Concentration
Small deviation	$\epsilon^*\left(n,C-\frac{A}{\sqrt{n}}\right)\sim \Phi\left(\frac{A}{\sqrt{V}}\right)$	$\Pr\left[\bar{X}_n \ge \frac{1}{\sqrt{n}}t\right] \sim 1 - Q\left(\frac{x}{\sqrt{V}}\right)$
Moderate deviation	$\epsilon^*(n, C - a_n) = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$	$\Pr\left[\bar{X}_n \ge a_n t\right] = e^{-\frac{na_n^2}{2V}x + o(na_n^2)}$
Large deviation	$\epsilon^*(n,R) = \mathrm{e}^{-nE(R) + o(n)}$	$\Pr\left[\bar{X}_n \ge t\right] = e^{-nI(x) + o(n)}$
Second-order AnalysisError Exponent AnalysisInterplay between $R$ and $n$ Interplay between $\varepsilon$ and $n$		
	given a fixed <i>ɛ</i> [Small deviation]	given a fixed <i>R</i> [Large deviation]

Hao-Chung Cheng

Moderate deviations