Optimal Adaptive Strategies for Sequential Quantum Hypothesis Testing

Yonglong Li
School of Mathematics and Statistics
Xi'an JiaoTong University
E-mail: liyonglong@xjtu.edu.cn.

August 9, 2024

Outline

- Setup
  - Background
  - Quantum Hypothesis Testing: Literature Review
  - Sequential Quantum Hypothesis Testing (SQHT)
- Main Results
  - Error Exponent Pairs for SQHT
  - Numerical Examples
- Proof of the Main Results

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.
- $\{X_k\}_{k=1}^{\infty}$ are i.i.d. random variables distributed according to P.

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.
- $\{X_k\}_{k=1}^{\infty}$ are i.i.d. random variables distributed according to P.
- A sequence of decision functions d_k taking values in $\{0, 1, *\}$.

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.
- $\{X_k\}_{k=1}^{\infty}$ are i.i.d. random variables distributed according to P.
- A sequence of decision functions d_k taking values in $\{0, 1, *\}$.
- T is the first time k that $d_k \neq *$.

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.
- $\{X_k\}_{k=1}^{\infty}$ are i.i.d. random variables distributed according to P.
- A sequence of decision functions d_k taking values in $\{0, 1, *\}$.
- T is the first time k that $d_k \neq *$.
- d_T is a $\{0, 1\}$-valued function and $d_T = i$ means H_i is the underlying hypothesis.

Classical Sequential Hypothesis Testing

- Binary hypothesis testing: $H_0 : P = P_0$ and $H_1 : P = P_1$, where P_0 and P_1 are probability distributions defined on the same alphabet $\mathcal{X}$.
- $\{X_k\}_{k=1}^{\infty}$ are i.i.d. random variables distributed according to P.
- A sequence of decision functions d_k taking values in $\{0, 1, *\}$.
- T is the first time k that $d_k \neq *$.
- d_T is a $\{0, 1\}$-valued function and $d_T = i$ means H_i is the underlying hypothesis.
- $\alpha = P_0(d_T = 1) \quad \text{and} \quad \beta = P_1(d_T = 0)$.

Classical Sequential Hypothesis Testing

Error Exponents

Given a sequence of SHTs $\{\{(d_{n,k}, T_n)\}_{k=1}^{\infty}\}_{n=1}^{\infty}$ satisfying the constraint

$$\max_{i=0,1} \mathbf{E}_i[T_n] \leq n,$$

the *error exponents* (E_0, E_1) defined as

$$E_0 = \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_n} \quad \text{and} \quad E_1 = \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n}.$$

In 1948, Wald and Wolfowitz showed that $E_0 \leq D(P_1 \| P_0)$ and $E_1 \leq D(P_0 \| P_1)$ and the error exponent can be achieved by a sequence of SPRTs.

Setup

- $\mathbb{C}^d$: d-dimensional complex Euclidean space;
- Quantum state ρ over $\mathbb{C}^d$: a $d \times d$ positive-semidefinite matrix with trace value 1.
- A positive operator-valued measure (POVM) $m = \{m(x) : x \in \mathcal{X}\}$ with outcomes in $\mathcal{X}$: $m(x)$ is a $d \times d$ positive-semidefinite matrix such that $\sum_{x \in \mathcal{X}} m(x) = I_d$.
- A projector-valued measure $m = \{m(x) : x \in \mathcal{X}\}$ with outcomes in $\mathcal{X}$: m is a POVM with the additional condition that $m(x)^2 = m(x)$.
- The probability of obtaining outcome x when m is applied to the underlying state ρ:

$$P_{\rho,m}(X = x) = \mathrm{Tr}[\rho m(x)].$$

Setup

Quantum Divergence

For a $d \times d$ Hermitian matrix A, let $\sum_{i=1}^{d} \lambda_i P_i$ be the spectral decomposition of A. We define $\log A \triangleq \sum_{i=1}^{d} \log \lambda_i P_i$.
For a $d \times d$ Hermitian matrix A, the *support* of A is defined as the subspace generated by the eigenvectors corresponding to non-0 eigenvalues.

Definition 1 (Quantum Relative Entropy)

Let ρ_0 and ρ_1 be two quantum states with the same support. The quantum relative entropy between two quantum states ρ_0 and ρ_1 is defined as

$$D(\rho_0 \| \rho_1) = \mathrm{Tr}[\rho_0(\log \rho_0 - \log \rho_1)].$$

Measured Relative Entropy

The measured relative entropy is defined as

$$D_{\mathcal{M}}(\rho_0 \| \rho_1) := \sup_{m} D(P_{\rho_0,m} \| P_{\rho_1,m}), \tag{1}$$

where the supremum runs over all rank-1 PVMs comprised of d projectors.

Theorem 2 (Berta, Fawzi, Tomamichel (2017))

For two states ρ_0 and ρ_1 with full support, we have

$$D_{\mathcal{M}}(\rho_0 \| \rho_1) = \sup_{\mathcal{X}} \sup_{m \in \mathcal{M}_{\mathcal{X}}} D(P_{\rho_0,m} \| P_{\rho_1,m}) \tag{2}$$

and the supremum is achieved at some PVM m^* with $|\mathcal{X}| = d$.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.
- Make a quantum measurement $\{\Lambda_n, I_n - \Lambda_n\}$ with outcome $\{0, 1\}$ to figure out the underlying states.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.
- Make a quantum measurement $\{\Lambda_n, I_n - \Lambda_n\}$ with outcome $\{0, 1\}$ to figure out the underlying states.
- If the outcome is 0, guess the state $\rho_0^{\otimes n}$; otherwise guess the state $\rho_1^{\otimes n}$.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.
- Make a quantum measurement $\{\Lambda_n, I_n - \Lambda_n\}$ with outcome $\{0, 1\}$ to figure out the underlying states.
- If the outcome is 0, guess the state $\rho_0^{\otimes n}$; otherwise guess the state $\rho_1^{\otimes n}$.
- Probability of type I-error: $\alpha_n := \mathrm{Tr}[\rho_0^{\otimes n}(I_n - \Lambda_n)]$.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.
- Make a quantum measurement $\{\Lambda_n, I_n - \Lambda_n\}$ with outcome $\{0, 1\}$ to figure out the underlying states.
- If the outcome is 0, guess the state $\rho_0^{\otimes n}$; otherwise guess the state $\rho_1^{\otimes n}$.
- Probability of type I-error: $\alpha_n := \mathrm{Tr}[\rho_0^{\otimes n}(I_n - \Lambda_n)]$.
- Probability of type II-error: $\beta_n := \mathrm{Tr}[\rho_1^{\otimes n}\Lambda_n]$.

Quantum Hypothesis Testing

- The quantum system is prepared in one of the two states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$.
- Make a quantum measurement $\{\Lambda_n, I_n - \Lambda_n\}$ with outcome $\{0, 1\}$ to figure out the underlying states.
- If the outcome is 0, guess the state $\rho_0^{\otimes n}$; otherwise guess the state $\rho_1^{\otimes n}$.
- Probability of type I-error: $\alpha_n := \mathrm{Tr}[\rho_0^{\otimes n}(I_n - \Lambda_n)]$.
- Probability of type II-error: $\beta_n := \mathrm{Tr}[\rho_1^{\otimes n}\Lambda_n]$.

Quantum Hypothesis Testing: Known Results

Quantum Stein's Lemma [Hiai and Petz (1991), Ogawa and Hayashi (2004)]

For any $\varepsilon > 0$, let $\beta_n(\varepsilon) \triangleq \inf\{\beta_n : (\Lambda_n, I_n - \Lambda_n)\,\text{such that}\,\alpha_n \leq \varepsilon\}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n(\varepsilon)} = D(\rho_0 \| \rho_1).$$

Quantum Hypothesis Testing: Known Results

Quantum Stein's Lemma [Hiai and Petz (1991), Ogawa and Hayashi (2004)]

For any $\varepsilon > 0$, let $\beta_n(\varepsilon) \triangleq \inf\{\beta_n : (\Lambda_n, I_n - \Lambda_n) \text{ such that } \alpha_n \leq \varepsilon\}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n(\varepsilon)} = D(\rho_0 \| \rho_1).$$

Quantum Chernoeff exponent [Audenaert et al. (2007), Nussbaum and Azkoła (2009)]

Let $C_n = \inf\{\alpha_n + \beta_n : (\Lambda_n, I_n - \Lambda_n)\}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{C_n} = C(\rho_0, \rho_1) = -\log \sup_{0\leq s\leq 1} \mathrm{Tr}[\rho_0^s \rho_1^{1-s}].$$

Quantum Hypothesis Testing: Known Results

Quantum Stein's Lemma [Hiai and Petz (1991), Ogawa and Hayashi (2004)]

For any $\varepsilon > 0$, let $\beta_n(\varepsilon) \triangleq \inf\{\beta_n : (\Lambda_n, I_n - \Lambda_n) \text{ such that } \alpha_n \leq \varepsilon\}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n(\varepsilon)} = D(\rho_0 \| \rho_1).$$

Quantum Chernoeff exponent [Audenaert et al. (2007), Nussbaum and Azkoła (2009)]

Let $C_n = \inf\{\alpha_n + \beta_n : (\Lambda_n, I_n - \Lambda_n)\}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{C_n} = C(\rho_0, \rho_1) = -\log \sup_{0\leq s\leq 1} \mathrm{Tr}[\rho_0^s \rho_1^{1-s}].$$

Quantum Hypothesis Testing: Known Results

Quantum Hoeffding's Bound [Hayashi and Nagaoka (2003), Ogawa and Hayashi (2004), Nagaoka (2006)]

Let

$$\mathcal{R} := \left\{ (R_0, R_1) : \exists\ (\Lambda_n, I_n - \Lambda_n) \text{ such that } \begin{array}{l} R_0 \le \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_n}, \\ R_1 \le \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n}. \end{array} \right\}$$

Then

$$\mathcal{R} = \bigcup_{0 \le r \le D(\rho_1\|\rho_0)} \left\{ (R_0, R_1) : \begin{array}{c} R_0 \le r, \\ R_1 \le \sup_{0\le s\le 1} \frac{-sr - \log \operatorname{Tr}[\rho_0^{1-s}\rho_1^s]}{1-s} \end{array} \right\}.$$

Sequential Quantum Hypothesis Testing: Problem Set-Up

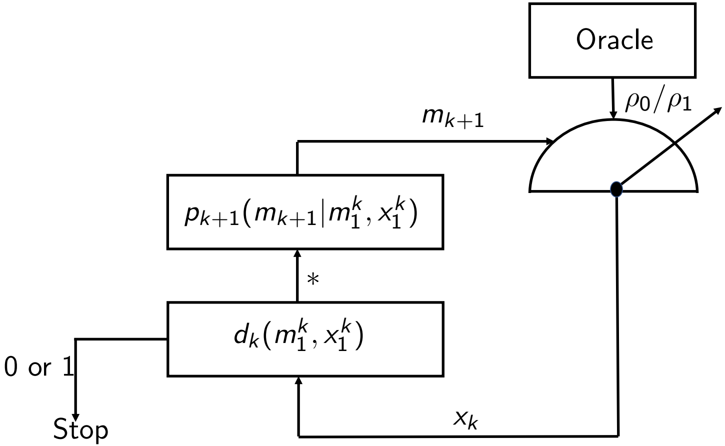

Figure: The structure of a general adaptive sequential hypothesis testing protocol.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Sequential Quantum Hypothesis Test

A sequential quantum hypothesis test (SQHT) $\mathcal{S} = \left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}\right)$, in its most general form, is given by (see also Figure 1):

- a finite set of measurement outcomes, $\mathcal{X}$;

Sequential Quantum Hypothesis Testing: Problem Set-Up

Sequential Quantum Hypothesis Test

A sequential quantum hypothesis test (SQHT) $\mathcal{S} = \left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}\right)$, in its most general form, is given by (see also Figure 1):

- a finite set of measurement outcomes, $\mathcal{X}$;
- a sequence of (conditional) probability distributions to determine the next measurement, $p_k(m_k | x_1^{k-1}, m_1^{k-1})$ for every $k \in \mathbb{N}$;

Sequential Quantum Hypothesis Testing: Problem Set-Up

Sequential Quantum Hypothesis Test

A sequential quantum hypothesis test (SQHT) $\mathcal{S} = \left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}\right)$, in its most general form, is given by (see also Figure 1):

- a finite set of measurement outcomes, $\mathcal{X}$;
- a sequence of (conditional) probability distributions to determine the next measurement, $p_k(m_k|x_1^{k-1}, m_1^{k-1})$ for every $k \in \mathbb{N}$;
- a sequence of $\{0, 1, *\}$-valued decision functions $d_k(x_1^k, m_1^k)$, for every $k \in \mathbb{N}$.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Sequential Quantum Hypothesis Test

A sequential quantum hypothesis test (SQHT) $\mathcal{S} = \left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}\right)$, in its most general form, is given by (see also Figure 1):

- a finite set of measurement outcomes, $\mathcal{X}$;
- a sequence of (conditional) probability distributions to determine the next measurement, $p_k(m_k|x_1^{k-1}, m_1^{k-1})$ for every $k \in \mathbb{N}$;
- a sequence of $\{0, 1, *\}$-valued decision functions $d_k(x_1^k, m_1^k)$, for every $k \in \mathbb{N}$.

Let T be the first time that $d_k \neq *$. Thus the number of samples of the underlying state ρ used during the test is T.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Sequential Quantum Probability Ratio Tests (SQPRTs)

For $k \geq 1$, let p_k be the probability density function according to which the experimenter chooses POVM M_k at time k. Let

$$S_k := \log \frac{\mathbb{P}_0(X_1^k, M_1^k)}{\mathbb{P}_1(X_1^k, M_1^k)}. \tag{3}$$

Additionally, let A and B be two fixed positive real numbers. The decision function d_k at time k is defined as follows

$$d_k(X_1^k, M_1^k) = \begin{cases} 0 & S_k \geq B \\ 1 & S_k \leq -A \\ * & \text{otherwise.} \end{cases} \tag{4}$$

Let $T = \inf\{k \geq 1 : S_k \notin (-A, B)\}$. We say $\left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}, T\right)$ is an *SQPRT* with parameters A and B.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Adaptive Versus Non-adaptive Strategies

- In an adaptive QSHT S, the measurement m_{k+1} depends on m_1^k and x_1^k.
- In an non-adaptive QSHT S, the measurement m_{k+1} does not depends on m_1^k and x_1^k.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Consider sequences of QSHT $\mathcal{S}_n$, indexed by $n \in \mathbb{N}$. We use $\mathbb{P}_{n,i}$ and $\mathbf{E}_{n,i}[\cdot]$ to denote the probability measure and the expectation induced by the QSHT $\mathcal{S}_n$ and the underlying state ρ_i.

Two Types of Errors

- Type I-error: $\alpha_n := \mathbb{P}_{n,0}(d_{T_n} = 1)$.
- Type II-error: $\beta_n := \mathbb{P}_{n,1}(d_{T_n} = 0)$.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Consider sequences of QSHT $\mathcal{S}_n$, indexed by $n \in \mathbb{N}$. We use $\mathbb{P}_{n,i}$ and $\mathbf{E}_{n,i}[\cdot]$ to denote the probability measure and the expectation induced by the QSHT $\mathcal{S}_n$ and the underlying state ρ_i.

Two Types of Errors

- Type I-error: $\alpha_n := \mathbb{P}_{n,0}(d_{T_n} = 1)$.
- Type II-error: $\beta_n := \mathbb{P}_{n,1}(d_{T_n} = 0)$.

Constraints on the Sample Size

- The first type of constraint is the expectation constraint:

$$\max_{i \in \{0,1\}} \mathbf{E}_{n,i}[T_n] \leq n. \tag{5}$$

- The second type of constraint is the probabilistic constraint

$$\max_{i \in \{0,1\}} \mathbb{P}_{n,i}(T_n > n) < \varepsilon. \tag{6}$$

Sequential Quantum Hypothesis Testing: Problem Set-Up

Achievable Error Exponent Pairs

A pair $(R_0, R_1) \in \mathbb{R}_+^2$ is said to be *an achievable error exponent pair under the expectation constraint* if there exists a sequence of QSHTs $\{\mathcal{S}_n\}_{n\in\mathbb{N}}$ such that

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_n} \geq R_0, \text{ and } \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n} \geq R_1, \quad \text{and} \tag{7}$$

$$\limsup_{n\to\infty} \left(\max_{i\in\{0,1\}} \mathbf{E}_{n,i}[T_n] - n \right) \leq 0. \tag{8}$$

Similarly, for $0 < \varepsilon < 1$, a pair $(R_0, R_1) \in \mathbb{R}_+^2$ is said to be *an ε-achievable error exponent pair under the probabilistic constraint* if there exists a sequence of QSHTs $\{\mathcal{S}_n\}_{n\in\mathbb{N}}$ such that (7) hold and (instead of(8)),

$$\limsup_{n\to\infty} \max_{i\in\{0,1\}} \mathbb{P}_{n,i}(T_n > n) < \varepsilon. \tag{9}$$

Sequential Quantum Hypothesis Testing: Problem Set-Up

Error Exponent Regions

- $\mathcal{A}_{\mathrm{E}}$ is the closure of the set of all achievable error exponent pairs under the expectation constraint using adaptive strategies.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Error Exponent Regions

- $\mathcal{A}_{\mathrm{E}}$ is the closure of the set of all achievable error exponent pairs under the expectation constraint using adaptive strategies.
- $\mathcal{A}_{\mathrm{P}}(\varepsilon)$ is the closure of the set of all ε-achievable error exponent pairs under the probabilistic constraint using adaptive strategies.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Error Exponent Regions

- $\mathcal{A}_{\mathrm{E}}$ is the closure of the set of all achievable error exponent pairs under the expectation constraint using adaptive strategies.
- $\mathcal{A}_{\mathrm{P}}(\varepsilon)$ is the closure of the set of all ε-achievable error exponent pairs under the probabilistic constraint using adaptive strategies.
- $\mathcal{R}_{\mathrm{E}}$ is the closure of the set of achievable error exponent pairs under the expectation constraint using non-adaptive strategies.

Sequential Quantum Hypothesis Testing: Problem Set-Up

Error Exponent Regions

- $\mathcal{A}_{\mathrm{E}}$ is the closure of the set of all achievable error exponent pairs under the expectation constraint using adaptive strategies.
- $\mathcal{A}_{\mathrm{P}}(\varepsilon)$ is the closure of the set of all ε-achievable error exponent pairs under the probabilistic constraint using adaptive strategies.
- $\mathcal{R}_{\mathrm{E}}$ is the closure of the set of achievable error exponent pairs under the expectation constraint using non-adaptive strategies.
- $\mathcal{R}_{\mathrm{P}}(\varepsilon)$ is the closure of the set of achievable error exponent pairs under the probabilistic constraint using non-adaptive strategies.

Sequential Quantum Hypothesis Testing: Literature Review

- Slussarenko et al. (2017, PRL) first applied sequential strategy to discriminate two quantum states.
- Martínez-Vargas et al. (2021, PRL) proposed the problem of sequential quantum hypothesis testing and showed the following.
  - For vanishing error probabilities α and β,

$$\mathbf{E}_0[T] = \frac{1+o(1)}{D(P_{\rho_0,m} \| P_{\rho_1,m})} \log \frac{1}{\beta},$$
$$\mathbf{E}_1[T] = \frac{1+o(1)}{D(P_{\rho_1,m} \| P_{\rho_0,m})} \log \frac{1}{\alpha}.$$

  - For vanishing error probabilities α and β,

$$\mathbf{E}_0[T] \geq \frac{1+o(1)}{D(\rho_0 \| \rho_1)} \log \frac{1}{\beta},$$
$$\mathbf{E}_1[T] \geq \frac{1+o(1)}{D(\rho_1 \| \rho_0)} \log \frac{1}{\alpha}.$$

Main Results for Adaptive Strategies

Theorem 3

Let ρ_0 and ρ_1 be two quantum states with full support. Then for any $0 < \varepsilon < 1$,

$$\mathcal{A}_{\mathrm{P}}(\varepsilon) = \mathcal{A}_{\mathrm{E}} = \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leq D_{\mathcal{M}}(\rho_1 \| \rho_0) \\ R_1 \leq D_{\mathcal{M}}(\rho_0 \| \rho_1) \end{array} \right\}. \tag{10}$$

Comparison with the result in Martínez-Vargas et al. (2021, PRL)

For vanishing error probabilities α and β,

$$\mathbf{E}_0[T] = \frac{1 + o(1)}{D_{\mathcal{M}}(\rho_1 \| \rho_0)} \log \frac{1}{\beta},$$
$$\mathbf{E}_1[T] = \frac{1 + o(1)}{D_{\mathcal{M}}(\rho_0 \| \rho_1)} \log \frac{1}{\alpha}.$$

Main Results for Adaptive Strategies

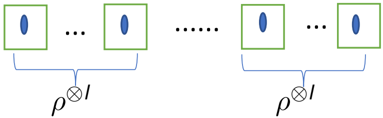

Figure: Multiple copies

Main Results for Adaptive Strategies

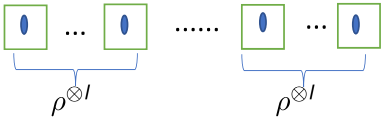

Figure: Multiple copies

Consider the binary quantum hypothesis test,

$$H_0^{(l)} : \rho^{\otimes l} = \rho_0^{\otimes l} \qquad H_1^{(l)} : \rho^{\otimes l} = \rho_1^{\otimes l}. \tag{11}$$

Define the achievable regions of the error exponent pairs $\mathcal{A}_{\mathrm{E}}^{(l)}$ and $\mathcal{A}_{\mathrm{P}}^{(l)}(\varepsilon)$. Similar to Theorems 3, we have

$$\mathcal{A}_{\mathrm{E}}^{(l)} = \mathcal{A}_{\mathrm{P}}^{(l)}(\varepsilon) = \left\{ (R_0, R_1) : \begin{array}{c} R_0 \le \frac{1}{l} D_{\mathcal{M}}(\rho_1^{\otimes l} \| \rho_0^{\otimes l}) \\ R_1 \le \frac{1}{l} D_{\mathcal{M}}(\rho_0^{\otimes l} \| \rho_1^{\otimes l}) \end{array} \right\}. \tag{12}$$

Main Results for Non-Adaptive Strategies: Ultimate Quantum Limit

Hiai and Petz, 1991

Let ρ_0 and ρ_1 be two quantum states with full support. Then

$$\lim_{l\to\infty} \frac{D_{\mathcal{M}}(\rho_1^{\otimes l}\|\rho_0^{\otimes l})}{l} = D(\rho_1\|\rho_0). \tag{13}$$

We now characterize the ultimate quantum limit of achievable error exponent pairs using sequential adaptive testing strategies.

Theorem 4

Let ρ_0 and ρ_1 be two quantum states with full support. Then for any $0 < \varepsilon < 1$,

$$\bigcup_{l=1}^{\infty} \mathcal{A}_{\mathrm{E}}^{(l)} = \bigcup_{l=1}^{\infty} \mathcal{A}_{\mathrm{P}}^{(l)}(\varepsilon) = \left\{ (R_0, R_1) : \begin{array}{l} R_0 \le D(\rho_1\|\rho_0) \\ R_1 \le D(\rho_0\|\rho_1) \end{array} \right\}. \tag{14}$$

Quantum Hypothesis Testing: Known Results

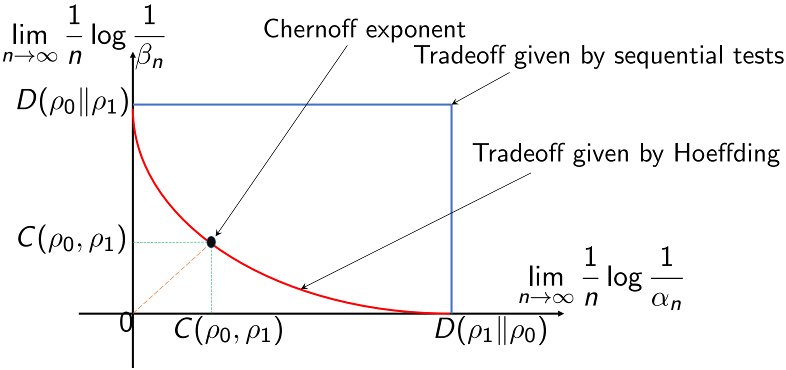

Figure: Schematic of the optimal trade-off between the exponential decay rates for the error of the first and second kind

Main Results for Non-Adaptive Strategies

Theorem 5

Let ρ_0 and ρ_1 be two quantum states with full support. Then for any $0 < \varepsilon < 1$,

$$\mathcal{R}_{\mathrm{E}} = \mathcal{R}_{\mathrm{P}}(\varepsilon) = \overline{\mathrm{Conv}(\mathcal{C})}, \tag{15}$$

where

$$\mathcal{C} = \bigcup_{\mathcal{X}} \bigcup_{m \in \mathcal{M}_{\mathcal{X}}} \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leq D(P_{\rho_1,m} \| P_{\rho_0,m}) \\ R_1 \leq D(P_{\rho_0,m} \| P_{\rho_1,m}) \end{array} \right\}, \tag{16}$$

and $\mathcal{X}$ runs over all finite sets and $\mathcal{M}_{\mathcal{X}}$ is the set of POVMs with support $\mathcal{X}$.

Main Results for Non-Adaptive Strategies

Corollary 6

Let ρ_0 and ρ_1 be two quantum states with full support and let

$$\mathcal{C}^{(l)} = \bigcup_{\mathcal{X}} \bigcup_{m \in \mathcal{M}_{\mathcal{X}}^{(l)}} \left\{ (R_0, R_1) : \begin{array}{c} R_0 \leq \frac{1}{l} D(P_{\rho_1,m} \| P_{0,m}) \\ R_1 \leq \frac{1}{l} D(P_{\rho_0,m} \| P_{1,m}) \end{array} \right\}. \quad (17)$$

Then for any $0 < \varepsilon < 1$, we have

$$\mathcal{R}_{\mathrm{E}}^{(l)} = \mathcal{R}_{\mathrm{P}}^{(l)}(\varepsilon) = \overline{\mathrm{Conv}(\mathcal{C}^{(l)})}, \quad (18)$$

and

$$\bigcup_{l=1}^{\infty} \mathcal{R}_{\mathrm{E}}^{(l)} = \bigcup_{l=1}^{\infty} \mathcal{R}_{\mathrm{P}}^{(l)}(\varepsilon). \quad (19)$$

Numerical Example

Let $\rho_0 = r_0 |\psi_0\rangle \langle\psi_0| + (1 - r_0)\frac{I}{2}$ and $\rho_1 = r_1 |\psi_1\rangle \langle\psi_1| + (1 - r_1)\frac{I}{2}$, where $|\psi_i\rangle = \cos\frac{\theta}{4} |0\rangle + (-1)^i \sin\frac{\theta}{4} |1\rangle$, $0 \le \theta \le \pi$, and $0 \le r_i \le 1$, $|0\rangle = (1, 0)^\top$, $|1\rangle = (0, 1)^\top$, I is the 2×2 identity matrix. For ρ_0 and ρ_1 with parameters (r_0, r_1, θ), we define the sum rate of error exponent pairs as follows:

$$f(r_0, r_1, \theta) := D_{\mathcal{M}}(\rho_1 \| \rho_0) + D_{\mathcal{M}}(\rho_0 \| \rho_1) \tag{20}$$

and

$$g(r_0, r_1, \theta) := \sup_{\mathcal{X}} \sup_{m \in \mathcal{M}_{\mathcal{X}}} D(P_{\rho_0,m} \| P_{\rho_1,m}) + D(P_{\rho_1,m} \| P_{\rho_0,m}). \tag{21}$$

Numerical Example

Let $[d^2] = \{1, 2, \dots, d^2\}$ and let
$\mathcal{M}^{(1)}_{[d^2]} = \{m \in \mathcal{M}_{[d^2]} : m(x) \text{ is of rank one for all } x \in [d^2]\}$.

Theorem 7

Let ρ_0 and ρ_1 be two quantum states with full support. Then

$$\overline{\mathrm{Conv}(\mathcal{C})} = \overline{\mathrm{Conv}(\mathcal{C}^{(1)})} \tag{22}$$

where

$$\mathcal{C}^{(1)} = \bigcup_{m \in \mathcal{M}^{(1)}_{[d^2]}} \left\{ (R_0, R_1) : \begin{array}{l} R_0 \le D(P_{\rho_1,m} \| P_{\rho_0,m}) \\ R_1 \le D(P_{\rho_0,m} \| P_{\rho_1,m}) \end{array} \right\}. \tag{23}$$

Numerical Example

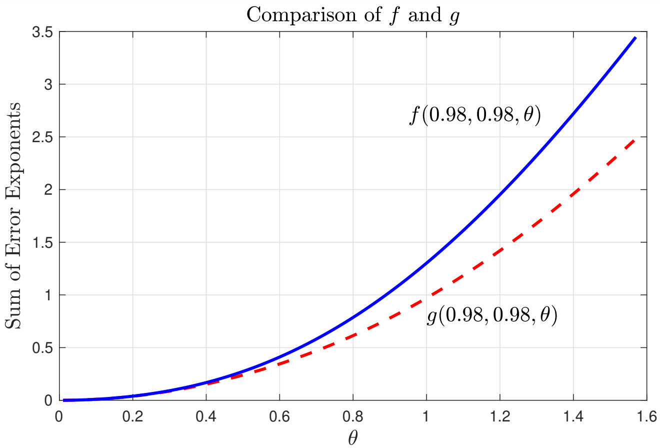

Figure: Maxima of the sum rate of error exponent pairs with adaptive or non-adaptive measurement strategies for $r_1 = r_2 = 0.98$ and $\theta \in (0, \frac{\pi}{2})$. The gap is most pronounced for large values of θ.

Numerical Example

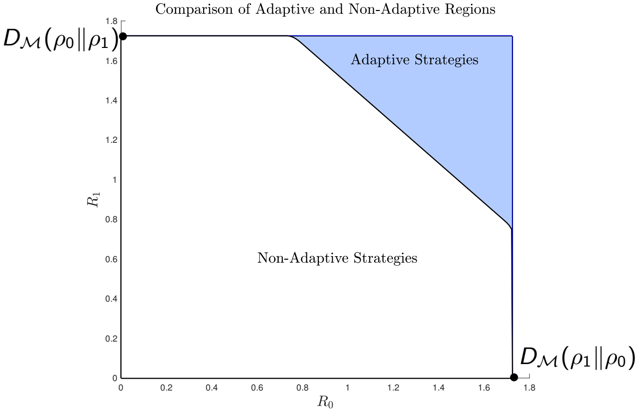

Figure: Achievable regions of error exponent pairs with adaptive or non-adaptive measurement strategies for when $(r_1, r_2, \theta) = (0.98, 0.98, 1.57)$. Note that the region for adaptive strategies is the entire rectangle including the region for non-adaptive strategies.

Numerical Example

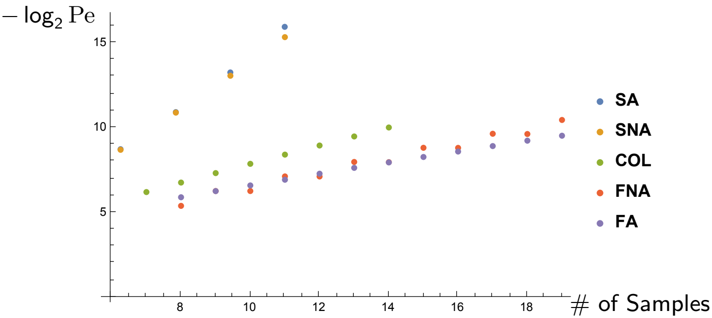

Figure: Error probabilities for different tests when $(r_1, r_2, \theta) = (0.9, 0.9, \frac{\pi}{2})$.

Proof of Achievability Part Theorem 3

Main Idea: Construct an appropriate sequence of SQPRTs.

SQPRTs

Let $\mathcal{X} = \{1, 2, \ldots, d\}$. Let $m_0^* = \{m_0^*(x)\}_{x \in \mathcal{X}}$ and $m_1^* = \{m_1^*(x)\}_{x \in \mathcal{X}}$ be the projective-valued measurements that achieve the suprema in the definitions of $D_{\mathcal{M}}(\rho_0 \| \rho_1)$ and $D_{\mathcal{M}}(\rho_1 \| \rho_0)$, respectively. Recall that $Z_j = \log \operatorname{Tr}\left[\rho_0 M_j(X_j)\right] - \log \operatorname{Tr}\left[\rho_1 M_j(X_j)\right]$ and $S_k = \sum_{j=1}^{k} Z_j$.

Adaptive Strategies

For $k \geq 1$, the adaptive strategies are defined as follows

$$p_k(m_0^* | x_1^{k-1}, m_1^{k-1}) = \begin{cases} \frac{1}{2} & \text{if } k = 1 \\ 1 & \text{if } k \geq 2 \text{ and } S_{k-1} \geq 0, \end{cases} \quad \text{and} \qquad (24)$$

$$p_k(m_1^* | x_1^{k-1}, m_1^{k-1}) = \begin{cases} \frac{1}{2} & \text{if } k = 1 \\ 1 & \text{if } k \geq 2 \text{ and } S_{k-1} < 0. \end{cases} \qquad (25)$$

Proof of Achievability Part Theorem 3

SQPRTs

For any fixed $0 < \tau < \min\{D_{\mathcal{M}}(\rho_1\|\rho_0), D_{\mathcal{M}}(\rho_0\|\rho_1)\}$, let

$$A_n := n(D_{\mathcal{M}}(\rho_1\|\rho_0) - \tau) \quad \text{and} \quad B_n := n(D_{\mathcal{M}}(\rho_0\|\rho_1) - \tau). \tag{26}$$

Let $T_n = \inf\{k \geq 1 : S_k \notin (-A_n, B_n)\}$ and that

$$d_{n,k}(X_1^k, M_1^k) = \begin{cases} 0 & S_k \geq B_n \\ 1 & S_k \leq -A_n \\ * & \text{otherwise.} \end{cases} \tag{27}$$

We will show that this sequence of SQPRTs $\mathcal{S}_n = \left(\mathcal{X}, \{p_k, d_{n,k}\}_{k=1}^{\infty}, T_n\right)$ with parameters A_n and B_n achieves $(D_{\mathcal{M}}(\rho_1\|\rho_0), D_{\mathcal{M}}(\rho_0\|\rho_1))$.

Proof of Achievability Part Theorem 3

Bounds on the Error Probabilities

$$\begin{aligned}\alpha_n &= \mathbb{P}_0(d_{T_n} = 1)\\ &= \mathbf{E}_0[\chi_{\{S_{T_n} \leq -A_n\}}]\\ &= \mathbf{E}_1[e^{S_{T_n}} \chi_{\{S_{T_n} \leq -A_n\}}]\\ &\leq e^{-A_n}.\end{aligned}$$

Similarly, $\beta_n \leq e^{-B_n}$.

Proof of Achievability Part Theorem 3

Verification of the Expectation Constraints for the Tests S_n

Let $\hat{T}_n = \inf\{k : S_k \geq B_n\}$. Then $T_n \leq \hat{T}_n$ and

$$S_{\hat{T}_n} \leq S_{\hat{T}_n - 1} + Z_n \leq B_n + C.$$

$$\begin{aligned}
\mathbf{E}_0[T_n] &\leq \mathbf{E}_0[\hat{T}_n] \\
&= \frac{-\mathbf{E}_0[S_{\hat{T}_n} - \hat{T}_n D_{\mathcal{M}}(\rho_0\|\rho_1)] + \mathbf{E}_0[S_{\hat{T}_n}]}{D_{\mathcal{M}}(\rho_0\|\rho_1)} \\
&\leq \frac{-\mathbf{E}_0[S_{\hat{T}_n} - \hat{T}_n D_{\mathcal{M}}(\rho_0\|\rho_1)] + B_n + C}{D_{\mathcal{M}}(\rho_0\|\rho_1)} \\
&\leq \frac{C_1 + B_n + C}{D_{\mathcal{M}}(\rho_0\|\rho_1)} = n - \frac{n\tau - C_1 - C}{D_{\mathcal{M}}(\rho_0\|\rho_1)}.
\end{aligned}$$

Proof of Converse Part of Theorem 3

The following lemma provides lower bounds on the error probabilities for a general SQHT $\left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}, T\right)$.

Lemma 8

For any SQHT $\left(\mathcal{X}, \{p_k, d_k\}_{k=1}^{\infty}, T\right)$ *with adaptive strategies such that*

$$\max_{i=0,1} \mathbf{E}_i[T] < \infty, \tag{28}$$

the following inequalities hold,

$$\log \frac{1}{\beta} \leq \frac{\mathbf{E}_0[T] D_{\mathcal{M}}(\rho_0 \| \rho_1) + 1}{1-\alpha} \quad \textit{and} \tag{29}$$

$$\log \frac{1}{\alpha} \leq \frac{\mathbf{E}_0[T] D_{\mathcal{M}}(\rho_0 \| \rho_1) + 1}{1-\beta}. \tag{30}$$

Proof of Converse Part of Theorem 3

Let $\{\mathcal{S}_n\}_{n=1}^{\infty}$ be a sequence of SQHTs with adaptive strategies such that $\alpha_n \to 0$ and $\beta_n \to 0$ and the sequence $\{T_n\}_{n=1}^{\infty}$ satisfies the expectation constraint (8). Then from (29) and (30) in Lemma 8, we have that

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_n} \leq \limsup_{n\to\infty} \frac{\mathbf{E}_{n,0}[T_n] D_{\mathcal{M}}(\rho_0\|\rho_1) + 1}{n(1-\alpha_n)} \leq D_{\mathcal{M}}(\rho_0\|\rho_1). \tag{31}$$

and

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\alpha_n} \leq \limsup_{n\to\infty} \frac{\mathbf{E}_{n,1}[T_n] D_{\mathcal{M}}(\rho_1\|\rho_0) + 1}{n(1-\beta_n)} \leq D_{\mathcal{M}}(\rho_1\|\rho_0). \tag{32}$$

Conclusion: any achievable error exponent pair (R_0, R_1) is such that $R_0 \leq D_{\mathcal{M}}(\rho_1\|\rho_0)$ and $R_1 \leq D_{\mathcal{M}}(\rho_0\|\rho_1)$.

Proof of Converse Part of Theorem 3

Proof of Lemma 8

- Let $\mathbb{P}_i$ be the probability measure on $(\Omega, \mathcal{F})$ when the underlying state is ρ_i.
- Let $\mathcal{F}_T$ be the sub-σ-algebra generated by T and let $\mathbb{P}_{i,T}$ be the restriction of $\mathbb{P}_i$ to the σ-algebra $\mathcal{F}_T$.

Then

$$\exp(S_T) = \frac{\mathrm{d}\mathbb{P}_{0,T}}{\mathrm{d}\mathbb{P}_{1,T}} \text{ and } \mathbf{E}_0[S_T] = D(\mathbb{P}_{0,T} \| \mathbb{P}_{1,T}).$$

We define a stochastic kernel V with input alphabet Ω (with elements ω) and output alphabet $\{0, 1\}$ as follows:

$$V(0|\omega) := \begin{cases} 1 & \text{if } d_T(\omega) = 0 \\ 0 & \text{if } d_T(\omega) = 1 \end{cases}. \tag{33}$$

Proof of Converse Part of Theorem 3

Let $D(a\|b) = a\log\frac{a}{b} + (1-a)\log\frac{1-a}{1-b}$ for any $0 \le a, b \le 1$.

Proof of Lemma 8

Using the data processing inequality to the classical relative entropy when $\left(\mathbb{P}_{0,T}, \mathbb{P}_{1,T}\right)$ is processed via the stochastic kernel V, we obtain,

$$\begin{aligned} D(\alpha\|1-\beta) &= D\big(\mathbb{P}_0(d_T = 1)\|\mathbb{P}_1(d_T = 1)\big) \\ &\le D(\mathbb{P}_{0,T}\|\mathbb{P}_{1,T}) = \mathbf{E}_0[S_T], \end{aligned} \tag{34}$$

which implies that

$$\log\frac{1}{\beta} \le \frac{D(\alpha\|1-\beta)+1}{1-\alpha} \le \frac{\mathbf{E}_0[S_T]+1}{1-\alpha}. \tag{35}$$

Proof of Converse Part of Theorem 3

Proof of Lemma 8

Key Fact: $\{S_k - kD_{\mathcal{M}}(\rho_0\|\rho_1)\}_{k=1}^{\infty}$ is a supermartingale.
Applying Optional Stopping Theorem to the supermartingale $\{S_k - kD_{\mathcal{M}}(\rho_0\|\rho_1)\}_{k=1}^{\infty}$ and the stopping time T, we obtain

$$\mathbf{E}_0[S_T - TD_{\mathcal{M}}(\rho_0\|\rho_1)] \leq \mathbf{E}_0[S_1 - D_{\mathcal{M}}(\rho_0\|\rho_1)] \leq 0. \tag{36}$$

Combining (35) and (36), we obtain

$$\log\frac{1}{\beta} \leq \frac{\mathbf{E}_0[S_T]+1}{1-\alpha} \leq \frac{\mathbf{E}_0[T]D_{\mathcal{M}}(\rho_0\|\rho_1)+1}{1-\alpha}. \tag{37}$$

Similarly, we have that

$$\log\frac{1}{\alpha} \leq \frac{\mathbf{E}_0[T]D_{\mathcal{M}}(\rho_0\|\rho_1)+1}{1-\beta}. \tag{38}$$

Proof of Converse Part of Theorem 4

Lemma 9

For any $0 \le \Lambda_n \le I_n$, *we have that*
$\mathrm{Tr}[\rho_0^{\otimes n}\Lambda_n] - \gamma\,\mathrm{Tr}[\rho_1^{\otimes n}\Lambda_n] \le \mathrm{Tr}[\rho_0^{\otimes n}\{\rho_0^{\otimes n} \ge \gamma\rho_1^{\otimes n}\}]$.

Note that

$$P_0(T_n > k) = 1 - P_0(T_n \le n)$$

$$= 1 - \sum_{j=1}^{k} \big(P_0(T_n = j, d_n = 0) + P_0(T_n = j, d_n = 1)\big).$$

Let $\tilde{\alpha}_k$ and $\tilde{\beta}_k$ be the type-I and type-II error probabilities of the test: H_0 is true if and only if $\{T_n \le k, \delta_n = 0\}$ holds.

Proof of Converse Part of Theorem 4

Then we have that $\tilde{\beta}_k \leq \beta_n$ and

$$\tilde{\alpha}_k = P_0(T_n > k) + \sum_{j=1}^{k} P_0(T_n = j, d_n = 1)$$

$$\tilde{\beta}_k = \sum_{j=1}^{k} P_0(T_n = j, d_n = 0).$$

Hence

$$\begin{aligned} P_0(T_n > k) &= \tilde{\alpha}_k - \sum_{j=1}^{k} P_0(T_n = j, d_n = 1) \geq \tilde{\alpha}_k - \alpha_n \\ &\geq 1 - \gamma_n \tilde{\beta}_k - \mathrm{Tr}[\rho_0^{\otimes k}\{\rho_0^{\otimes k} \geq \gamma_n \rho_1^{\otimes k}\}] - \alpha_n \\ &= \mathrm{Tr}[\rho_0^{\otimes k}\{\rho_0^{\otimes k} \leq \gamma_n \rho_1^{\otimes k}\}] - \gamma_n \beta_n - \alpha_n. \qquad (39) \end{aligned}$$

Proof of Converse Part of Theorem 4

Let

$$k_n = \frac{1}{D(\rho_0\|\rho_1) + \tau} \log \frac{1}{\beta_n} \quad \text{and} \quad \gamma_n = e^{k_n(D(\rho_0\|\rho_1)+\tau_1)} \tag{40}$$

with $\tau_1 > \tau > 0$. Then we have that

$$\begin{aligned} n \geq \mathbf{E}_0[T_n] &\geq P_0(T_n > k_n)k_n \\ &\geq (\mathrm{Tr}[\rho_0^{\otimes k_n}\{\rho_0^{\otimes k_n} \leq \gamma_n \rho_1^{\otimes k_n}\}] - \gamma_n\beta_n - \alpha_n)k_n \\ &\sim (1 - \beta_n^{\frac{\tau_1-\tau}{D(\rho_0\|\rho_1)+\tau}} - \alpha_n)\frac{1}{D(\rho_0\|\rho_1)+\tau}\log\frac{1}{\beta_n}. \end{aligned} \tag{41}$$

Thanks for Your Attention!