

Lower bounds on error probability of quantum channel discrimination by the Bures angle and the trace distance

Ryo Ito¹ and Ryuhei Mori²

¹Tokyo Institute of Technology, ²Nagoya University

Sept. 7, 2023

Quantum channel discrimination problem

Definition (Quantum channel discrimination problem)

For fixed finite set of quantum channels $\{\Phi_1, \Phi_2, \dots, \Phi_k\}$ and a probability distribution $(p_i)_{i=1,2,\dots,k}$,

Input: An oracle $\mathcal{O} = \Phi_i$ for $i \in \{1, 2, \dots, k\}$ drawn w.p. p_i

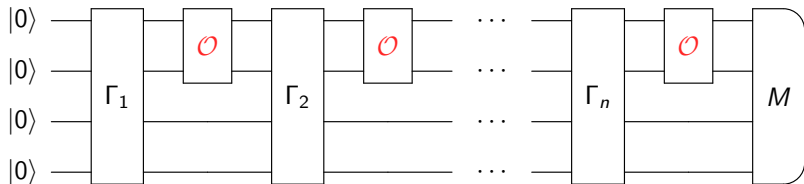
Output: $i \in \{1, 2, \dots, k\}$ satisfying $\mathcal{O} = \Phi_i$

- ▶ A fundamental problem in quantum information science

Algorithm for quantum channel discrimination problem

General algorithm calling the oracle n times.

- ▶ $\mathcal{O} \in \{\Phi_1, \dots, \Phi_k\}$
- ▶ $\Gamma_1, \dots, \Gamma_n$: Quantum channels
- ▶ M : Measurement



Discrimination of quantum states

Definition (Quantum state discrimination problem)

For fixed finite set of quantum states $\{\rho_1, \rho_2, \dots, \rho_k\}$ and a probability distribution $(p_i)_{i=1,2,\dots,k}$,

Input: A quantum state $\rho = \rho_i$ for $i \in \{1, 2, \dots, k\}$ drawn w.p. p_i

Output: $i \in \{1, 2, \dots, k\}$ satisfying $\rho = \rho_i$

Theorem (Holevo–Helstrom theorem)

[Helstrom 1967], [Holevo 1972]

The largest success probability of discrimination of two quantum states is

$$\frac{1 + \|\rho_1 \rho_1 - \rho_2 \rho_2\|_1}{2}.$$

For more than two quantum states, the largest success probability is a solution of semidefinite programming (SDP).

Discrimination of two quantum channels

Theorem (Discrimination of two quantum channels)

The largest success probability of discrimination of *two* quantum channels with a *single* query is

$$p_{\text{succ}} = \frac{1 + \|\rho_1 \Phi_1 - \rho_2 \Phi_2\|_{\diamond}}{2}$$

where

$$\|\Gamma_A\|_{\diamond} := \max_{\rho_{AR}} \|(\Gamma_A \otimes \text{Id}_R)(\rho_{AR})\|_1.$$

Corollary (Discrimination by non-adaptive algorithms)

The largest success probability of discrimination of *two* quantum channels with *n non-adaptive (parallel)* queries is

$$p_{\text{succ}} = \frac{1 + \|\rho_1 \Phi_1^{\otimes n} - \rho_2 \Phi_2^{\otimes n}\|_{\diamond}}{2}.$$

Previous qualitative result

- ▶ There are two quantum channels that cannot be distinguished exactly by any non-adaptive algorithm, but **can be distinguished exactly** by an adaptive algorithm with two queries [Harrow, Hassidim, Leung, Watrous, 2010].
- ▶ For any two quantum channels, either of the followings is true [Yu and Zhou 2021]
 - ▶ The quantum channels can be distinguished **exactly** by finite queries.
 - ▶ The error probability of quantum channel discrimination decays **exponentially** in the number of queries.

Previous result and our result

# of channels	2	≥ 2
QUD	[Kawachi, Kawano, Le Gall, Tamaki 2019]	Grover search $\ell = 1$ [Zalka 1999]
QCD	Port-based teleportation [Pirandola, Laurenza, Lupo, Pereira, 2019] [This work]	[Zhuang, Pirandola, 2020]
QCGD		[This work]

Discrimination of two quantum channels

Quantum channel discrimination of $\Phi_A^{(1)}$ and $\Phi_A^{(2)}$.

$$\begin{aligned}\rho_1 &= \Phi_A^{(1)} \Gamma_{AR}^{(n)} \Phi_A^{(1)} \Gamma_{AR}^{(n-1)} \cdots \Phi_A^{(1)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \\ \rho_2 &= \Phi_A^{(2)} \Gamma_{AR}^{(n)} \Phi_A^{(2)} \Gamma_{AR}^{(n-1)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|\end{aligned}$$

From Holevo–Helstrom theorem,

$$\frac{1 - \frac{1}{2} \|\rho_1 - \rho_2\|_1}{2}.$$

Hybrid argument

$$\rho^{(0)} = \Phi_A^{(1)} \Gamma_{AR}^{(n)} \Phi_A^{(1)} \Gamma_{AR}^{(n-1)} \dots \Phi_A^{(1)} \Gamma_{AR}^{(2)} \Phi_A^{(1)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|$$

$$\rho^{(1)} = \Phi_A^{(1)} \Gamma_{AR}^{(n)} \Phi_A^{(1)} \Gamma_{AR}^{(n-1)} \dots \Phi_A^{(1)} \Gamma_{AR}^{(2)} \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|$$

$$\rho^{(2)} = \Phi_A^{(1)} \Gamma_{AR}^{(n)} \Phi_A^{(1)} \Gamma_{AR}^{(n-1)} \dots \Phi_A^{(2)} \Gamma_{AR}^{(2)} \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|$$

⋮

$$\rho^{(n)} = \Phi_A^{(2)} \Gamma_{AR}^{(n)} \Phi_A^{(2)} \Gamma_{AR}^{(n-1)} \dots \Phi_A^{(2)} \Gamma_{AR}^{(2)} \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|$$

$$\begin{aligned} \|\rho_1 - \rho_2\|_1 &= \|\rho^{(0)} - \rho^{(n)}\|_1 \\ &= \|\rho^{(0)} - \rho^{(1)} + \rho^{(1)} - \dots - \rho^{(n-1)} + \rho^{(n-1)} - \rho^{(n)}\|_1 \\ &\leq \sum_{i=0}^{n-1} \|\rho^{(i)} - \rho^{(i+1)}\|_1 \end{aligned}$$

Upper bound for the single step

$$\begin{aligned}
 \|\rho^{(i)} - \rho^{(i+1)}\|_1 &= \left\| \Phi_A^{(1)} \Gamma_{AR}^{(n)} \cdots \Phi_A^{(1)} \Gamma_{AR}^{(i+1)} \Phi_A^{(2)} \Gamma_{AR}^{(i)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right. \\
 &\quad \left. - \Phi_A^{(1)} \Gamma_{AR}^{(n)} \cdots \Phi_A^{(1)} \Gamma_{AR}^{(i+2)} \Phi_A^{(2)} \Gamma_{AR}^{(i+1)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right\|_1 \\
 &\leq \left\| \Phi_A^{(1)} \Gamma_{AR}^{(i+1)} \Phi_A^{(2)} \Gamma_{AR}^{(i)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right. \\
 &\quad \left. - \Phi_A^{(2)} \Gamma_{AR}^{(i+1)} \Phi_A^{(2)} \Gamma_{AR}^{(i)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right\|_1 \\
 &\leq \max_{\rho_{AR}} \left\| \Phi_A^{(1)}(\rho_{AR}) - \Phi_A^{(2)}(\rho_{AR}) \right\|_1 \\
 &= \left\| \Phi_A^{(1)} - \Phi_A^{(2)} \right\|_{\diamond}
 \end{aligned}$$

A simple lower bound of the error probability

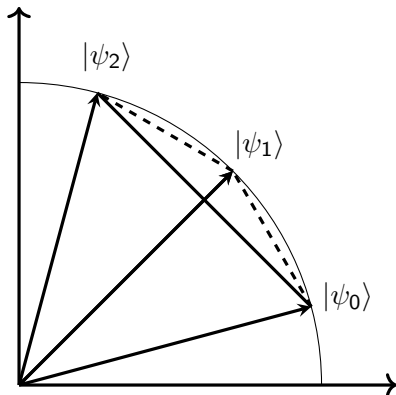
Lemma (A simple lower bound)

The quantum channel discrimination of $\Phi^{(1)}$, $\Phi^{(2)}$

$$p_{\text{err}}(n) \geq \frac{1 - \frac{n}{2} \left\| \Phi_A^{(1)} - \Phi_A^{(2)} \right\|_{\diamond}}{2}$$

Triangle inequalities are not tight

For pure states with two real state vectors $|\psi_0\rangle$ and $|\psi_2\rangle$, the trace distance is equal to the **Euclidean distance** up to a constant factor.



Obviously, $\| |\psi_0\rangle - |\psi_2\rangle \|_2 < \| |\psi_0\rangle - |\psi_1\rangle \|_2 + \| |\psi_1\rangle - |\psi_2\rangle \|_2$.

Bures angle

- ▶ The fidelity: $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$.
- ▶ The **Bures angle**: $A(\rho, \sigma) := \arccos F(\rho, \sigma)$.

Lemma

$$\|p\rho - (1-p)\sigma\|_1 \leq \sqrt{1 - 4p(1-p)F(\rho, \sigma)^2}$$

The equality is satisfied if ρ and σ are pure states.

From the triangle inequality of the Bures angle

$$A(\rho^{(0)}, \rho^{(n)}) \leq \sum_{i=0}^{n-1} A(\rho^{(i)}, \rho^{(i+1)})$$

Upper bound for the single step

$$\begin{aligned} A(\rho^{(i)}, \rho^{(i+1)}) &= A\left(\Phi_A^{(1)} \Gamma_{AR}^{(n)} \cdots \Phi_A^{(1)} \Gamma_{AR}^{(i+1)} \Phi_A^{(2)} \Gamma_{AR}^{(i)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|, \right. \\ &\quad \left. \Phi_A^{(1)} \Gamma_{AR}^{(n)} \cdots \Phi_A^{(1)} \Gamma_{AR}^{(i+2)} \Phi_A^{(2)} \Gamma_{AR}^{(i+1)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right) \\ &\leq A\left(\Phi_A^{(1)} \Gamma_{AR}^{(i+1)} \Phi_A^{(2)} \Gamma_{AR}^{(i)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n|, \right. \\ &\quad \left. \Phi_A^{(2)} \Gamma_{AR}^{(i+1)} \cdots \Phi_A^{(2)} \Gamma_{AR}^{(1)} |0^n\rangle \langle 0^n| \right) \\ &\leq \max_{\rho_{AR}} A\left(\Phi_A^{(1)}(\rho_{AR}), \Phi_A^{(2)}(\rho_{AR})\right) \\ &= \arccos \min_{\rho_{AR}} F\left(\Phi_A^{(1)}(\rho_{AR}), \Phi_A^{(2)}(\rho_{AR})\right). \end{aligned}$$

The minimum of the fidelity can be evaluated by SDP.

Our result using the Bures angle

Theorem ([Ito and Mori 2021])

$$p_{\text{err}}(n) \geq \frac{1}{2} \left(1 - \sqrt{1 - 4p_1 p_2 \cos^2(n\tau)} \right)$$

where

$$\tau := \arccos \min_{\rho_{AR}} F \left(\Phi_A^{(1)}(\rho_{AR}), \Phi_A^{(2)}(\rho_{AR}) \right).$$

Corollary (Discrimination of two amplitude damping channels)

For the discrimination of two amplitude damping channels with parameters r_1 and r_2 ,

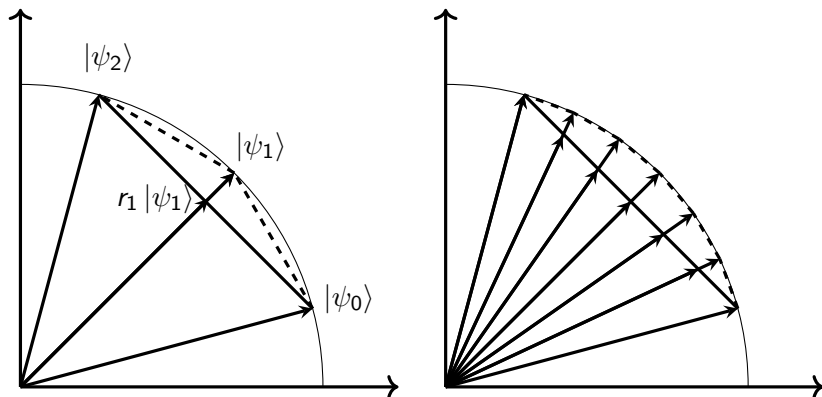
$$p_{\text{err}}(n) \geq \frac{1}{2} \left(1 - \sqrt{1 - 4p_1 p_2 \cos^2(n\Delta)} \right)$$

where $\Delta := \arccos(\sqrt{r_1 r_2} + \sqrt{(1-r_1)(1-r_2)})$.

Especially, when $p_1 = p_2 = 1/2$,

$$p_{\text{err}}(n) \geq \frac{1}{2} (1 - \sin(n\Delta)).$$

Improvement of the triangle inequality



Let $k \in \{0, 1, \dots, n\}$, $\alpha \in (0, 1]$, $\beta \in (0, 1]$ satisfying $\alpha^k = \beta^{n-k}$.

The weights are chosen as
 $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^k = \beta^{n-k}, \beta^{n-k-1}, \dots, \beta, 1$.

Our result using the trace distance with the weights

Theorem

Let $k \in \{0, 1, \dots, n\}$ be an integer. Let α and β be non-negative real numbers that satisfy $p_1 \alpha^k = p_2 \beta^{n-k}$. Let τ_{\diamond}^1 and τ_{\diamond}^2 be

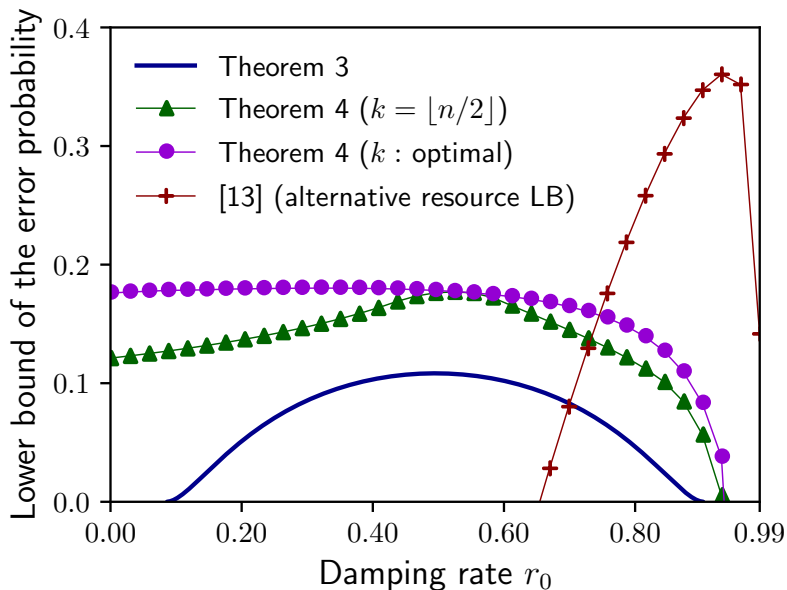
$$\tau_{\diamond}^1 := \max_{\rho_{AR}} \left\| \left(\Phi_A^{(1)} - \alpha \Phi_A^{(2)} \right) (\rho_{AR}) \right\|_1,$$
$$\tau_{\diamond}^2 := \max_{\rho_{AR}} \left\| \left(\beta \Phi_A^{(1)} - \Phi_A^{(2)} \right) (\rho_{AR}) \right\|_1.$$

The following then holds:

$$p_{\text{err}}(n) \geq \frac{1}{2} \left[1 - p_1 \left(\sum_{i=0}^{k-1} \alpha^i \right) \tau_{\diamond}^1 - p_2 \left(\sum_{i=0}^{n-k-1} \beta^i \right) \tau_{\diamond}^2 \right],$$

for arbitrary α , β and k .

Numerical results



Quantum channel group discrimination

Quantum channel **group** discrimination:

Problem to find a **group** including the channel (group may intersect).

We also derive lower bounds of the error probability for the quantum channel **group** discrimination problem using the **Bures angle** and the **trace distance with weight**.

The lower bound using Bures angle proves the **optimality of Grover's search** (This was proven for the case with exactly one marked element by [Zalka 1999]).

The lower bound using the trace distance with weight is numerically better than previously known lower bounds for some cases.