Multiparty Quantum State Discrimination

by

Tianyi Peng

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

Master of Science in Aeronautics and Astronautics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2020

Signature redacted

Author ....
Department of Aeronautics and Astronautics
January 30, 2020

Signature redacted

Certified by..............................
Moe Z. Win
Professor
Thesis Supervisor

Signature redacted

Accepted by ....
Sertac Karaman
Associate Professor, Aeronautics and Astronautics
Chair, Graduate Program Committee

Multiparty Quantum State Discrimination

by

Tianyi Peng

Submitted to the Department of Aeronautics and Astronautics
on January 30, 2020, in partial fulfillment of the
requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

We consider the problem of identifying an unknown multiparty quantum state using local operations and classical communication (LOCC). In particular, we consider a class of protocols that utilize a sequence of LOCC, referred to as LOCC protocols. We derive the necessary and sufficient conditions for optimal LOCC protocol that maximizes the probability of correct identification (PCI) and provide an algorithm to determine the maximal PCI. Moreover, we develop a protocol based on the alternating optimization approach and demonstrate its near-optimal performance. The numerical results suggest that the LOCC protocols can be desirable alternatives to traditional discrimination approaches that require measuring the entire state of a quantum system.

Thesis Supervisor: Moe Z. Win
Title: Professor

Acknowledgments

I would like to express my deepest gratitude to my advisor Professor Moe Win for his mentorship and guidance throughout the years. From him, I have learnt how to think rigorously, review the literature thoroughly, and develop the skills for solving complex problems. Professor Win has always been a good mentor and friend, from whom I have gained precious advice for both research and life.

I am greatly thankful to Wenhan Dai for his tremendous advice and mentorship on research and life since the first day I met him.

I am also grateful to my friends, colleagues, mentors, and staff - Andrea Conti, Xiaodi Wu, Aram Harrow, Liangzhong Ruan, Zehao Yu, Stefano Guerrini, Florian Meyer, Zhenyu Liu, Augustin (Alex) Saucan, Fan Jiang, Rico Mendrzik, Xinzhe Fu, Bai Liu, Beth Marois - for their support and advice.

I am indebted to my family and my girlfriend Xueyue for their love, encouragement, and persistent support in everything I do. This thesis is dedicated to them!

I acknowledge the support from the Office of Naval Research.

Contents

List of Figures

Chapter 1

Introduction

Introduction— Quantum State Discrimination (QSD) is a fundamental problem [1, 2, 3, 4, 5] in quantum information science. The problem is to identify an unknown quantum state among an ensemble of states and has a wide range of applications including quantum communication [6, 7, 8, 9, 10, 11], quantum computation [12, 13, 14], and quantum metrology [15, 16, 17]. Traditional QSD that requires measuring the entire state of a quantum system [18, 19, 20, 21] are unamenable for implementation with the noisy intermediate-scale quantum (NISQ) technology [22]. To address this issue, we can store the quantum state on multiple devices (e.g., an N-party state can be shared among N devices, and each device holds one part of the state), and then design distributed protocols that utilize local operations and classical communication (LOCC). These protocols, referred to as LOCC protocols, are amenable to implementation and their effectiveness has been demonstrated in various quantum information processing tasks [23, 24, 25, 26].

This Letter considers the task of multiparty QSD, i.e., QSD that involves multiple devices (parties) and utilizes LOCC protocols. Suppose with a probability p_k, the multiple parties in the system share a state Ξ_k for some $k \in \mathcal{K}_K = \{1, 2, \ldots, K\}$. The objective is to maximize the probability of correct identification (PCI) of the unknown state over the set of LOCC protocols. The difficulty in the maximization lies in the LOCC constraints. The mathematical characterization of LOCC protocols, compared to that of traditional approaches, is more complicated [27, 28, 29, 30], making the optimization problem challenging.

Special scenarios for multiparty QSD have been investigated in [31, 32, 33, 34, 35]. Some studies focus on $K = 2$ [31, 32, 33]. For example, when $K = 2$ and the two states to be discriminated are multi-copy mixed states, an algorithm has been proposed to find an upper bound on the performance of LOCC protocols [33]. When the LOCC protocol is restricted to have one-way classical communication, the necessary and sufficient conditions of the optimal protocols has been determined in [34, 35]. The above studies either consider a specific value of K, a particular type of states, or a special class of LOCC protocols. However, little is known about how to design the LOCC protocols (both one-way and two-way) for multiparty QSD with arbitrary K.

The fundamental questions related to multiparty QSD are (i) how to formulate the optimization of LOCC protocols; (ii) how to characterize the structure of the optimal solution. The answers to these questions provide insights into the design of cooperation strategies among multiple quantum devices. The goal of this Letter is to establish a framework for designing LOCC protocols for multiparty QSD.

In this Letter, we formulate an optimization problem based on the LOCC tree and provide two algorithms to solve the optimization problem. In particular, we determine the necessary and sufficient conditions for optimal LOCC protocols, based on which we provide an algorithm to determine the maximum PCI. We represent LOCC protocols using a set of positive operators that have a tree structure (LOCC tree) instead of using the conventional Kraus representation. We show that the optimization problem reduces to an semidefinite programming (SDP) problem when the local measurements are fixed for all parties except one, based on which we design an algorithm to develop LOCC protocols based on the alternating optimization approach and demonstrate its near-optimal performance.

Notation: In this Letter, we use $\mathcal{L}(\mathcal{H})$ to denote the set of Hermitian operators on the Hilbert space $\mathcal{H}$, $\mathcal{L}^+(\mathcal{H})$ to denote the set of positive semidefinite operators on the Hilbert space $\mathcal{H}$, $I_{\mathcal{H}}$ to denote the identity operator on the Hilbert space $\mathcal{H}$, and $\mathcal{K}_N$ to denote the set $\{1, 2, \ldots, N\}$.

Chapter 2

Preliminaries

2.1 Multiparty QSD

A multiparty QSD consists of three aspects: a collection of parties, an ensemble of states, and a communication sequence.

- Collection of parties: consider N parties described by $1, 2, \dots, N$. Let $\mathcal{H}_n$ denote the Hilbert space corresponding to the quantum system of n-th party.

- Ensemble of states: an ensemble of states is denoted by $\{\Xi_k \mid k \in \mathcal{K}_K\}$. The N parties share a state Ξ_k with the probability p_k.

- Communication sequence: a communication sequence is a sequence denoted by $\boldsymbol{s} = (s_1, s_2, \dots, s_r)$, where the i-th element $s_i \in \mathcal{K}_N$. Once a sequence is given, the parties can send classical messages according to the order of the sequence, i.e., $s_1 \to s_2 \to \dots \to s_r$.

2.2 LOCC Protocol and LOCC Tree

With these three aspects above, an LOCC protocol can be described as the following process consisting of r steps:

- In the i-th step ($i \in \mathcal{K}_r$), the party s_i performs a measurement on its part of the state based on the outcomes of measurements performed by $s_1, s_2, \dots, s_{i-1}$.

- In the r-th step, if the outcome of the measurement is k, the state is determined to be Ξ_k.

Without loss of generality, we assume $\boldsymbol{s}$ covers each party at least once. As a special case, we call $\boldsymbol{s}$ one-way if $\boldsymbol{s} = (1, 2, \ldots, N)$. In this case, the LOCC protocols are referred to as one-way protocols.

Let $b(i) = \max\{j \mid j < i, s_j = s_i\}$ denote the step before i, in which party s_i performs a measurement (if no such j exists, set $b(i) = 0$). Let m_i denote the number of possible outcomes of the i-th step measurement. Specifically, we set $m_i = \dim^2 \mathcal{H}_{s_i}$ for $i \in \mathcal{K}_{r-1}$ and $m_r = K$.[1] Let $z_i \in \mathcal{K}_{m_i}$ denote the outcome of the i-th step measurement. Let $\boldsymbol{z}_i = [z_1, z_2, \ldots, z_i]$ and $\boldsymbol{z} = \boldsymbol{z}_r$. Denote by $\mathcal{Z} = \{\boldsymbol{z} | z_i \in \mathcal{K}_{m_i} \text{ with } i \in \mathcal{K}_r\}$ the set of all possible measurement outcomes of the protocol. The set of measurement operators of an LOCC protocol is denoted by $\mathcal{M} = \{\boldsymbol{M}_{\boldsymbol{z}_i} \mid i \in \mathcal{K}_r, z_j \in \mathcal{K}_{m_j} \text{ for } j \leqslant i\}$, where $\boldsymbol{M}_{\boldsymbol{z}_i}$ is an operator associated with the outcome $\boldsymbol{z}_i$. In particular, the $\boldsymbol{M}_{\boldsymbol{z}_i}$ is a positive semidefinite operator on $\mathcal{H}_{s_i}$:

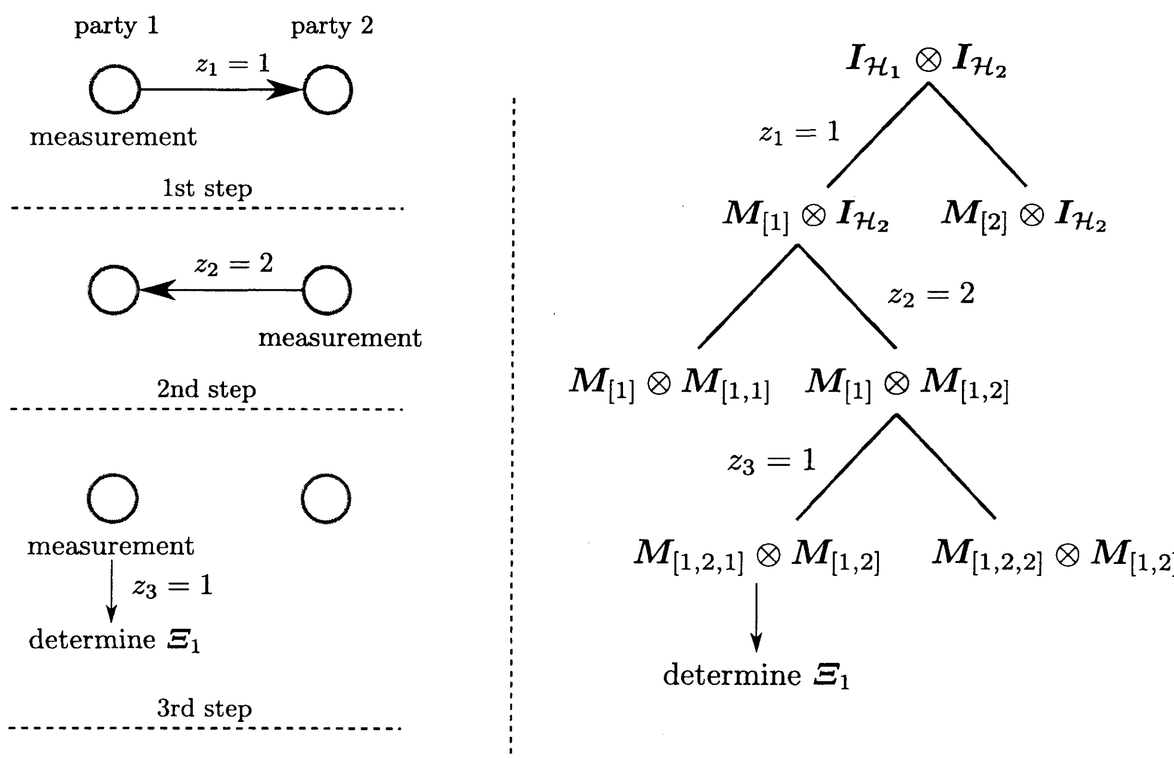
$$\boldsymbol{M}_{\boldsymbol{z}_i} \in \mathcal{L}^+(\mathcal{H}_{s_i}). \tag{2.1}$$

Furthermore, for fixed i and $\boldsymbol{z}_{i-1}$, the summation of $\boldsymbol{M}_{\boldsymbol{z}_i}$ ($z_i \in \mathcal{K}_{m_i}$) has the following constraint:

$$\sum_{z_i=1}^{m_i} \boldsymbol{M}_{\boldsymbol{z}_i} = \begin{cases} \boldsymbol{M}_{\boldsymbol{z}_{b(i)}} & b(i) \neq 0 \\ I_{\mathcal{H}_{s_i}} & b(i) = 0. \end{cases} \tag{2.2}$$

Figure 2-1 describes a simple example of an LOCC protocol with $\boldsymbol{s} = (1, 2, 1)$ for which $b(1) = 0, b(2) = 0, b(3) = 1$. Therefore, we have the constraints for the LOCC protocol: $\boldsymbol{M}_{[1]} + \boldsymbol{M}_{[2]} = I_{\mathcal{H}_1}$, $\boldsymbol{M}_{[1,1]} + \boldsymbol{M}_{[1,2]} = I_{\mathcal{H}_2}$, $\boldsymbol{M}_{[1,2,1]} + \boldsymbol{M}_{[1,2,2]} = \boldsymbol{M}_{[1]}$. One can interpret $\boldsymbol{M}_{\boldsymbol{z}_i}$ as the positive-operator valued measure (POVM) element on the party s_i associated with the outcomes $\boldsymbol{z}_i$ [39]. We use a tree to represent an LOCC protocol

[1] Although m_i can be arbitrarily large or even infinite, it has been shown that there exists an LOCC protocol that achieves the maximal PCI with $m_i = \dim^2 \mathcal{H}_{n_i}$ for $i \in \mathcal{K}_{r-1}$ and $m_r = K$ [37, 38].



(a) LOCC protocol

(b) LOCC tree

Figure 2-1: A three-step LOCC protocol and the corresponding LOCC tree.

since a sequence of measurement outcomes can be represented by a path in a tree.[2] In particular, the nodes and the branches of the tree corresponds to the measurement operators $\boldsymbol{M}_{\boldsymbol{z}_i}$ and measurement outcomes $\boldsymbol{z}_i$, respectively (see Figure 2-1).

2.3 Problem Formulation

Let $l(s) = \max\{j \mid s_j = s\}$ denote the last measurement step performed by party s. The joint POVM element associated with the outcomes $\boldsymbol{z}$ of the N-party measurement on the whole system is $\otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}}$. Hence, the conditional probability of obtaining $\boldsymbol{z}$ when $\boldsymbol{\Xi}_k$ is shared, is $\mathrm{tr}\left\{(\otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}})\boldsymbol{\Xi}_k\right\}$. Since the protocol determines the state to be $\boldsymbol{\Xi}_{z_r}$ where z_r is the outcome of the last step, the probability that a LOCC protocol $\mathcal{M}$ correctly identifies the unknown quantum state is $\sum_{\boldsymbol{z}\in\mathcal{Z}} p_{z_r}\, \mathrm{tr}\left\{(\otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}})\boldsymbol{\Xi}_{z_r}\right\}$.

The problem of maximizing the PCI for multiparty QSD can be formalized as the following optimization problem:[3]

$$\begin{aligned} \mathscr{P}: \quad & \underset{\mathcal{M}}{\text{maximize}} \quad \sum_{\boldsymbol{z}\in\mathcal{Z}} p_{z_r}\, \mathrm{tr}\left\{(\otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}})\boldsymbol{\Xi}_{z_r}\right\} \\ & \text{subject to} \quad \text{constraints (2.1) and (2.2).} \end{aligned} \tag{2.3}$$

Let $\mathcal{M}^*$ and λ^* respectively denote the optimal solution and the optimal value of $\mathscr{P}$.

[2]This can be regarded as a new application of the LOCC tree, which were used for checking the implementability of LOCC [40, 39].

[3]Here, we assume the communication sequence is predetermined in the optimization problem. Another layer of optimization can be added for optimizing the communication sequence, which is out of the scope of this Letter.

Chapter 3

Necessary and Sufficient Conditions for Optimal Protocols

In this section, we consider an auxiliary problem $\mathscr{P}_{\mathrm{aux}}$ corresponding to $\mathscr{P}$ in order to provide the necessary and sufficient conditions for an LOCC protocol $\mathcal{M}^*$ to be an optimal solution of $\mathscr{P}$.

3.1 Auxiliary Optimization Problem

Before giving the $\mathscr{P}_{\mathrm{aux}}$, we first consider the following optimization problem $\mathscr{P}_{\boldsymbol{H}}$ for some positive semi-definite operator $\boldsymbol{H}$ on $\mathcal{H}_{s_1}$:

$$\mathscr{P}_{\boldsymbol{H}}: \underset{\mathcal{M}}{\text{maximize}} \quad \sum_{z \in \mathcal{Z}, z_1 = 1} p_{z_r} \operatorname{tr}\left\{(\otimes_{n=1}^{N} \boldsymbol{M}_{z_{l(n)}}) \boldsymbol{\Xi}_{z_r}\right\}$$

$$\text{subject to constraints (2.1) and (2.2)}$$

$$\boldsymbol{M}_{[1]} = \boldsymbol{H} \tag{3.1}$$

Let $\mathcal{M}^*_{\boldsymbol{H}}$ and $\lambda^*_{\boldsymbol{H}}$ respectively denote the optimal solution and the optimal value of $\mathscr{P}_{\boldsymbol{H}}$. The solution to the problem $\mathscr{P}_{\boldsymbol{H}}$ corresponds to the optimal protocol design described by the path in the LOCC tree with $z_1 = 1$ and $\boldsymbol{M}_{[1]} = \boldsymbol{H}$. Note that $\lambda^*_{\boldsymbol{H}}$ does not change if we replace $z_1 = 1, \boldsymbol{M}_{[1]} = \boldsymbol{H}$ by $z_1 = c, \boldsymbol{M}_{[c]} = \boldsymbol{H}$ for any $c \in \mathcal{K}_{m_1}$.

Furthermore, an optimal solution $\mathcal{M}^*$ for $\mathscr{P}$ is also an optimal solution for $\mathscr{P}_{\boldsymbol{H}}$ with $z_1 = c$ and $\boldsymbol{H} = \boldsymbol{M}^*_{[c]}$ for any $c \in \mathcal{K}_{m_1}$. Therefore

$$\lambda^* = \sum_{z_1 \in \mathcal{K}_{m_1}} \lambda^*_{\boldsymbol{M}^*_{[z_1]}}. \tag{3.2}$$

The auxiliary problem $\mathscr{P}_{\text{aux}}$ is given by:

$$\begin{aligned}\mathscr{P}_{\text{aux}}: \ & \text{minimize} \quad \operatorname{tr}\{\boldsymbol{X}\} \\ & \text{subject to } \boldsymbol{X} \in \mathcal{L}^+(\mathcal{H}_{s_1}) \\ & \qquad\qquad \operatorname{tr}\{\boldsymbol{X}\boldsymbol{G}\} \geqslant \lambda^*_{\boldsymbol{G}}, \ \forall \boldsymbol{G} \in \mathcal{F}\end{aligned} \tag{3.3}$$

where $\lambda^*_{\boldsymbol{G}}$ is the optimal value of $\mathscr{P}_{\boldsymbol{G}}$ and $\mathcal{F} = \{\boldsymbol{G} \mid 0 \preccurlyeq \boldsymbol{G} \preccurlyeq \boldsymbol{I}_{\mathcal{H}_{s_1}}\}$. Let $\boldsymbol{X}^*$ and μ^* respectively denote the optimal solution and optimal value of $\mathscr{P}_{\text{aux}}$. It is easy to verify that

$$\begin{aligned}\mu^* &= \operatorname{tr}\{\boldsymbol{X}^*\} \\ &= \operatorname{tr}\left\{\boldsymbol{X}^* \left(\sum_{z_1=1}^{m_1} \boldsymbol{M}^*_{[z_1]}\right)\right\} \\ &\geqslant \sum_{z_1=1}^{m_1} \lambda^*_{\boldsymbol{M}^*_{[z_1]}} \\ &= \lambda^*.\end{aligned} \tag{3.4}$$

The second equality is due to (2.2) and the last equality is due to (3.2).

For an LOCC protocol $\mathcal{M}$, let $\boldsymbol{N}_k$ denote the induced POVM element that determines the state to be $\boldsymbol{\Xi}_k$: $\boldsymbol{N}_k = \sum_{\boldsymbol{z}, z_r = k} \otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}}$. Let $\boldsymbol{\Gamma}(\mathcal{M})$ be the operator denoted by

$$\boldsymbol{\Gamma}(\mathcal{M}) = \sum_{k=1}^{K} p_k \frac{1}{2}(\boldsymbol{N}_k \boldsymbol{\Xi}_k + \boldsymbol{\Xi}_k \boldsymbol{N}_k).$$

Note that $\operatorname{tr}\{\boldsymbol{\Gamma}(\mathcal{M})\}$ equals the PCI of the protocol. Denote $\boldsymbol{\Gamma}_s(\mathcal{M})$ by taking the partial trace of $\boldsymbol{\Gamma}(\mathcal{M})$ over the Hilbert space of the whole system except $\mathcal{H}_s$, i.e.,

$$\boldsymbol{\Gamma}_s(\mathcal{M}) = \mathrm{tr}_{\otimes_{m\in\mathcal{K}_N\setminus\{s\}}\mathcal{H}_m}\{\boldsymbol{\Gamma}(\mathcal{M})\}.$$

3.2 Necessary and Sufficient Conditions

The necessary and sufficient conditions for optimality of an LOCC protocol are given in the following theorem:

Theorem 1. *Consider the optimization problem $\mathscr{P}$ and $\mathscr{P}_{\mathrm{aux}}$ given by (2.3) and (3.3) respectively. The following holds: $\mathcal{M}^*$ is an optimal solution of $\mathscr{P}$ if and only if $\boldsymbol{\Gamma}_{s_1}(\mathcal{M}^*)$ is a feasible solution of $\mathscr{P}_{\mathrm{aux}}$.*

Based on the Theorem 1, we also have the following corollary:

Corollary 1. *The optimal values of the optimization problem $\mathscr{P}$ and $\mathscr{P}_{\mathrm{aux}}$ given by (2.3) and (3.3), satisfy $\lambda^* = \mu^*$.*

Theorem 1 characterizes the structure of optimal LOCC protocols. The zero-gap between $\mathscr{P}$ and $\mathscr{P}_{\mathrm{aux}}$ shown in Corollary 1 inspires the design of algorithms for determining λ^*, which will be explained later.

Chapter 4

Algorithm Design

We next provide two algorithms, namely Sequence Recursive (SR) algorithm and Alternating Optimization (AO) algorithm. The SR algorithm determines the optimal value λ^* of $\mathscr{P}$ based on recursively solving a series of optimization problems. The AO algorithm can provide a near-optimal LOCC protocol for a given multiparty QSD based on alternating optimization.

4.1 Sequence Recursive Algorithm

The SR algorithm consists of the following two procedures:

- Approximation: formulate an optimization problem $\tilde{\mathscr{P}}_{\text{aux}}$, with optimal value $\tilde{\mu}$ that approximates μ^*.
- Sequence Length Reduction: solving $\tilde{\mathscr{P}}_{\text{aux}}$ by solving several optimization problems: each corresponds to a multiparty QSD with a strictly shorter communication sequence.

The approximation procedure and sequence length reduction procedure can be done recursively.

In the approximation procedure, we aim to formulate an optimization problem that approximates $\mathscr{P}_{\text{aux}}$. In particular, we first find a finite set to approximate $\mathcal{F}$

using epsilon-nets [41, 42]. For arbitrary small δ, we can find a finite set $\mathcal{G}_\delta$ such that $\forall \boldsymbol{G} \in \mathcal{F}$,

$$\|\boldsymbol{G}_i - \boldsymbol{G}\| < \delta \qquad \text{for some } \boldsymbol{G}_i \in \mathcal{G}_\delta.$$

Then, we can formulate an approximation problem $\tilde{\mathscr{P}}_{\text{aux}}$ of $\mathscr{P}_{\text{aux}}$:

$$\begin{aligned}\tilde{\mathscr{P}}_{\text{aux}}: \ & \text{minimize} \quad \operatorname{tr}\{\boldsymbol{X}\} \\ & \text{subject to } \ \boldsymbol{X} \in \mathcal{L}^+(\mathcal{H}_{s_1}) \\ & \qquad\qquad \operatorname{tr}\{\boldsymbol{X}\boldsymbol{G}_i\} \geqslant \lambda^*_{\boldsymbol{G}_i}, \forall \boldsymbol{G}_i \in \mathcal{G}_\delta.\end{aligned}$$

Note that the problem $\tilde{\mathscr{P}}_{\text{aux}}$ can be solved by SDP if $\lambda^*_{\boldsymbol{G}_i}$'s are known.

In the sequence length reduction procedure, we determine $\lambda^*_{\boldsymbol{G}_i}$ by solving the optimization problem $\mathscr{P}_{\boldsymbol{G}_i}$ for every $\boldsymbol{G}_i \in \mathcal{G}_\delta$. In fact, with $\mathscr{P}_{\boldsymbol{G}_i}$, one can formulate a new optimization problem that corresponds to a multiparty QSD with a communication sequence $\mathring{\boldsymbol{s}} = (s_2, s_3, \ldots, s_r)$ and an ensemble of states $\{\mathring{\boldsymbol{\Xi}}_k\}$ where each $\mathring{\boldsymbol{\Xi}}_k$ is shared with probability $\mathring{p}_k$. Here, $\{\mathring{\boldsymbol{\Xi}}_k\}$ can be seen as the posterior ensemble conditioned on the outcome z_1 with the POVM element $\boldsymbol{G}_i$. In particular, if the shared state is $\boldsymbol{\Xi}_k$, then the posterior state $\mathring{\boldsymbol{\Xi}}_k$ can be determined by:[1]

$$\mathring{\boldsymbol{\Xi}}_k = \frac{\sqrt{\breve{\boldsymbol{G}}_i}\boldsymbol{\Xi}_k\sqrt{\breve{\boldsymbol{G}}_i}}{\operatorname{tr}\left\{\boldsymbol{\Xi}_k\breve{\boldsymbol{G}}_i\right\}}$$

where $\breve{\boldsymbol{G}}_i = \otimes_{s \in \mathcal{K}_N \setminus \{s_1\}} \boldsymbol{I}_{\mathcal{H}_s} \otimes \boldsymbol{G}_i$. Furthermore, the posterior probability $\mathring{p}_k$ can be determined by:

$$\mathring{p}_k = p_k \operatorname{tr}\left\{\boldsymbol{\Xi}_k\breve{\boldsymbol{G}}_i\right\} \Big/ \sum_{\check{k} \in \mathcal{K}_K} p_{\check{k}} \operatorname{tr}\left\{\boldsymbol{\Xi}_{\check{k}}\breve{\boldsymbol{G}}_i\right\}.$$

[1] Any operator $\boldsymbol{H}$ such that $\boldsymbol{H}^\dagger\boldsymbol{H} = \boldsymbol{G}_i$ can be used as the Kraus operator for implementing the POVM element $\boldsymbol{G}_i$. Here we choose $\boldsymbol{H} = \sqrt{\boldsymbol{G}_i}$.

One can check that the maximum PCI $\mathring{\lambda}$ of this new optimization problem is

$$\mathring{\lambda} = \frac{\lambda^*_{G_i}}{\sum_{k' \in \mathcal{K}_K} p_{k'} \operatorname{tr}\left\{ \Xi_{k'} \breve{G}_i \right\}}.$$

In this way, we transform $\mathscr{P}$ into new optimization problems that correspond to multiparty QSD with strictly shorter communication sequences. If we recursively perform the approximation and sequence length reduction procedures[2], we will end up with QSD problems that have only one party in the system and can be solved easily. This algorithm is referred to as the SR algorithm, for which the following result holds

Theorem 2. *There exists an algorithm to approximate the optimal value λ^* of the problem $\mathscr{P}$ within precision ϵ and time complexity $\left(\frac{Dr}{\epsilon}\right)^{O(D^2 r)}$, where $D = \max_n \dim \mathcal{H}_n$ and r is the length of the communication sequence.*

A stronger result holds if the communication path $\mathcal{S}$ is one-way, as given by the following theorem

Theorem 3. *If $\mathcal{S}$ is one-way, there exists an algorithm to approximate the optimal value λ^* of the problem $\mathscr{P}$ within precision ϵ and time complexity $\left(\frac{Dr}{\epsilon}\right)^{O(Dr)}$, where $D = \max_n \dim \mathcal{H}_n$ and r is the length of the communication sequence.*

The SR algorithm provides a way to approximate the maximum PCI for a multiparty QSD. However, the complexity of the algorithm increases with the dimension of the system. This can be alleviated by using alternating optimization techniques as described in the following.

4.2 Alternating Optimization Algorithm

The optimization problem $\mathscr{P}$ has semidefinite constraints, but the objective function is non-convex over the matrix variables. The non-convexity of the objective function

[2] If there is one party that is not covered by the communication sequence, we remove the party from the system.

brings difficulties for solving $\mathscr{P}$. To address the non-convexity, we use the alternating optimization technique that has been widely used for solving non-convex optimization problems [43]. This technique consists of three aspects:

- Partitioning: partition the set of variables involved in the problem.
- Solving: solve the problem for variables in a part of the partition while fixing the other variables.
- Alternating: solve the original problem by alternating among parts of the partition.

In the partitioning procedure, we split the set of variables $\mathcal{M}$ in $\mathscr{P}$ as follows

$$\mathcal{M} = \mathcal{M}_1 \bigcup \mathcal{M}_2 \bigcup \ldots \bigcup \mathcal{M}_N$$

where $\mathcal{M}_s = \{\boldsymbol{M}_{\boldsymbol{z}_i} \in \mathcal{M} \mid s_i = s, \forall i \in \mathcal{K}_r\}$ denote the variables associated with the steps related to party s. Let $\mathcal{M}_s^{\mathrm{c}} = \mathcal{M} \setminus \mathcal{M}_s$. If $\mathcal{M}_s^{\mathrm{c}}$ is fixed, then the objective function of $\mathscr{P}$ degenerates to a linear function over the variables in $\mathcal{M}_s$:

$$\sum_{\boldsymbol{z} \in \mathcal{Z}} p_{\boldsymbol{z}_r} \operatorname{tr}\left\{ \boldsymbol{M}_{\boldsymbol{z}_{l(s)}} \bigotimes \left(\bigotimes_{n \in \mathcal{K}_N \setminus \{s\}} \boldsymbol{M}_{\boldsymbol{z}_{l(n)}} \right) \boldsymbol{\Xi}_{\boldsymbol{z}_r} \right\}$$

where $\boldsymbol{M}_{\boldsymbol{z}_{l(s)}} \in \mathcal{M}_s$ and $\boldsymbol{M}_{\boldsymbol{z}_{l(n)}} \in \mathcal{M}_s^{\mathrm{c}}$ for every $n \in \mathcal{K}_N \setminus \{s\}$.

In the procedure for solving over parts of the partition, $\mathcal{M}_s^{\mathrm{c}}$ is fixed in which case, $\mathscr{P}$ degenerates to an SDP problem and can be efficiently solved by SDP optimization packages [44, 45]. Then, $\mathcal{M}_s$ is replaced by the solution of the corresponding SDP problem. In the alternating procedure, we solve the problem with different s and iteratively updating the variables. Note that the PCI is upper bounded by 1 and it increases with each iteration. Therefore, the iterating procedure is guaranteed to converge. The effectiveness and the near-optimal performance of the algorithms are showing in the following.

Chapter 5

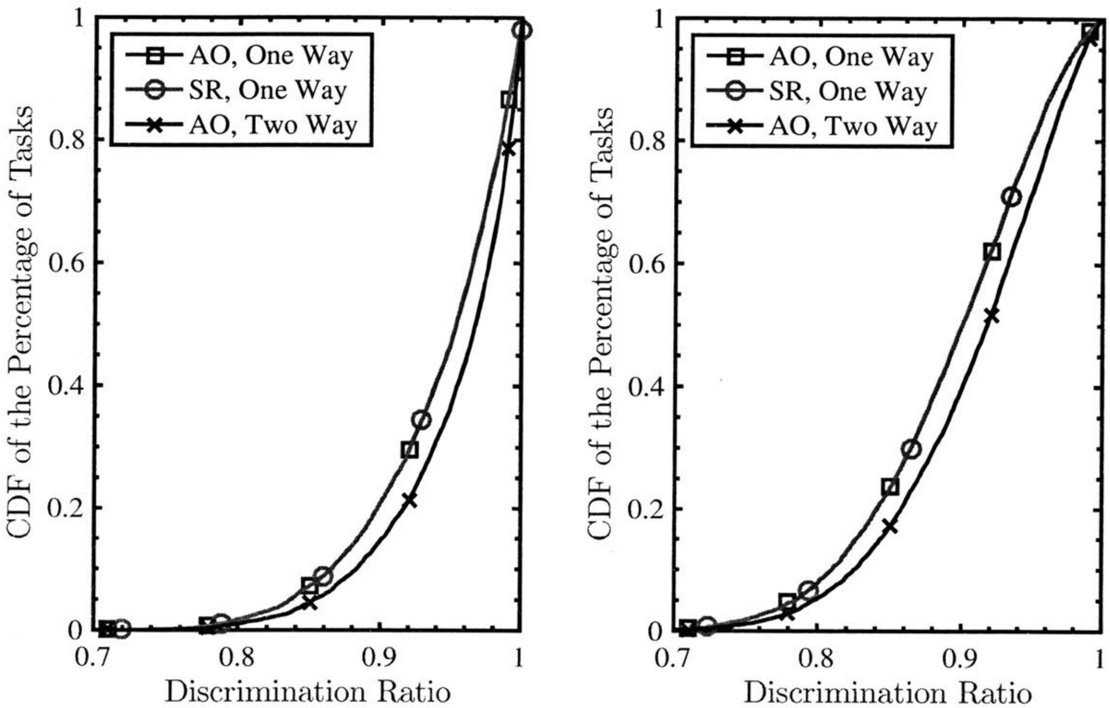
Numerical Results

We evaluate the performance of the AO algorithm in various scenarios.[1] For a fixed multiparty QSD, let η denote the ratio between $p_{\rm LOCC}$ and $p_{\rm opt}$, where $p_{\rm LOCC}$ is the PCI that is achieved by some LOCC protocol or determined by the SR algorithm, $p_{\rm opt}$ is the PCI achieved by the optimal protocols that can globally measure the entire state of the system. We refer to η as the discrimination ratio.

We first consider two parties where $\mathcal{H}_1, \mathcal{H}_2$ are two-dimensional. For the ensemble of states $\{\Xi_k\}$, let Ξ_k be a pure state drawn uniformly from the real unit vector space, and let $p_k = 1/K$ for $k \in \mathcal{K}_K$. We consider two communication sequences $\boldsymbol{s}_{\rm one} = \{1, 2\}$ and $\boldsymbol{s}_{\rm two} = \{1, 2, 1\}$, which correspond to one-way and two-way communication, respectively. We quantify the performance of the SR algorithm and AO algorithm in the following scenarios: (1) the AO algorithm with $\boldsymbol{s}_{\rm one}$; (2) the SR algorithm with $\boldsymbol{s}_{\rm one}$; and (3) the AO algorithm with $\boldsymbol{s}_{\rm two}$. Figure 5-1 shows the empirical CDF of the discrimination ratio for the three scenarios above.[2] First, the AO algorithm and the SR algorithm provide almost the same performance for the one-way scenario. For example, the median of discrimination ratio with $\boldsymbol{s}_{\rm one}$ and $K = 3$ for the AO algorithm is 0.9532, whereas it is 0.9534 for the SR algorithm. This demonstrates the near optimality of the AO algorithm. Second, there exists a gap between one-way

[1] In the implementation of the AO algorithm, the iteration is stopped when the increment improvement in the PCI is smaller than a predetermined threshold.

[2] Here, we use the SR algorithm to provide a tight upper bound on the PCI of the multiparty QSD.



(a) $K = 3$ (b) $K = 4$

Figure 5-1: The CDF of the discrimination ratio for two parties.

and two-way protocols. In the literature, such a gap is demonstrated only for a few special examples [36]. Results in Figure 5-1 show that the existence of the gap is a common phenomenon.

We then consider three parties where $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ are D-dimensional. For the ensemble of states $\{\Xi_k\}$, let $\Xi_k = \hat{\Xi}_k \otimes \hat{\Xi}_k \otimes \hat{\Xi}_k$ be a three-copy state where $\hat{\Xi}_k$ is a D-dimensional pure state drawn uniformly from the corresponding Hilbert space, and let $p_k = 1/K$ for $k \in \mathcal{K}_K$. Here, each party holds one copy $\hat{\Xi}_k$. Consider that the communication sequence $\boldsymbol{s}$ is one-way: $\boldsymbol{s} = \{1, 2, 3\}$. This scenario corresponds to designing one-way protocols for multiparty QSD with multi-copy states, which has applications such as quantum receiver design [46, 9, 47]. The myopic algorithm is commonly used in this scenario [46, 48, 49]. In each step of the protocol provided by the myopic algorithm, the corresponding party performs measurements for maximizing the immediate PCI, ignoring the impact of the current measurements for the future steps. We consider $K = 10$ and evaluate the performance of the AO algorithm and the myopic algorithm. Figure 5-2 shows the empirical CDF of the discrimination ratio for two algorithms. First, the AO algorithm achieves high discrimination ratios. For example, the median of the discrimination ratio is 0.9464 for $D = 2$ and 0.9325 for $D = 5$, respectively. It is known that when $K = 2$, the LOCC protocol can achieve the same performance as the optimal protocols that can perform global operations [49]. Here we demonstrate the desirable performance of LOCC protocols for random selecting states and large K. This result suggests the effectiveness of AO algorithm, especially when global operations are infeasible. Second, the AO algorithm improves the performance significantly compared to the myopic algorithm. For example, when $D = 2$, the median of the discrimination ratio is 0.8753 for the myopic algorithm, whereas it is 0.9464 for the AO algorithm. This leads to an improvement of 8.12%. This is because the AO algorithm accounts for both the current measurements and future measurements for the optimization, whereas the myopic algorithm ignores the future ones.

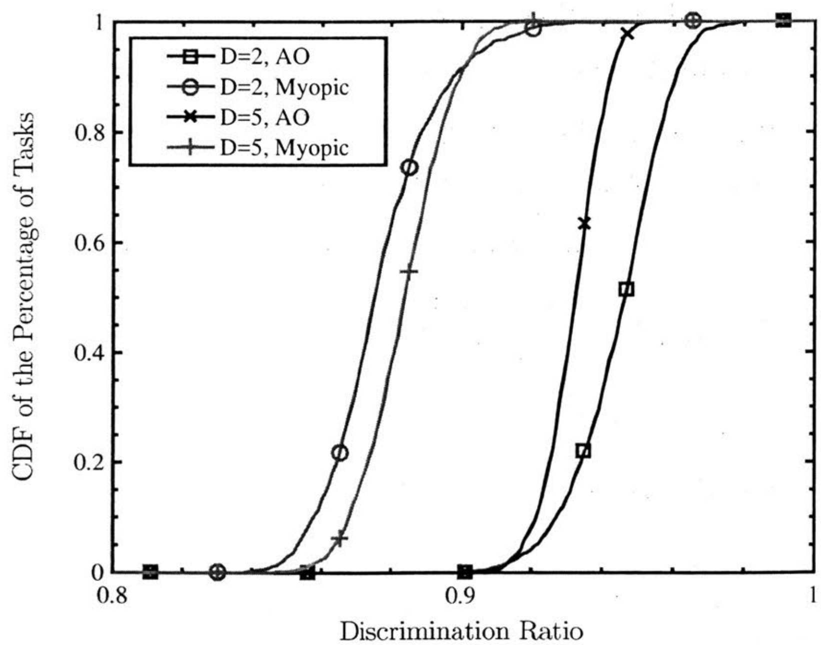


Figure 5-2: The CDF of the discrimination ratio for three parties with $K = 10$ and one-way protocols.

Chapter 6

Conclusion

This Letter derives necessary and sufficient conditions for optimality of LOCC protocols for distributed multiparty QSD. We utilize the tree to characterize LOCC protocols in the optimization problem, facilitating the use of alternating optimization and SDP. We develop the SR and AO algorithm to solve the optimization problem. Furthermore, the numerical simulation shows that there exists a gap between one-way and two-way protocols for the ensemble of states that are randomly generated; such phenomenon has been observed only for special states [36]. The numerical results also suggest that LOCC protocols can be a desirable alternative to traditional discrimination approaches that require measuring the entire state of a quantum system. This work paves the way to cooperation of spatially separated quantum devices.

Appendix A

Appendices

A.1 Proof of Theorem 1

Proof. For simplification, we use $\boldsymbol{\Gamma}^*$ to represent $\boldsymbol{\Gamma}_{s_1}(\mathcal{M}^*)$ if there is no ambiguity. We will prove the theorem by proving the following conditions:

- Sufficient Condition: if $\boldsymbol{\Gamma}^*$ is a feasible solution of $\mathscr{P}_{\text{aux}}$, $\mathcal{M}^*$ is an optimal solution of $\mathscr{P}$.
- Necessary Condition: if $\mathcal{M}^*$ is an optimal solution of $\mathscr{P}$, $\boldsymbol{\Gamma}^*$ is a feasible solution of $\mathscr{P}_{\text{aux}}$.

Sufficient Condition: Recall that λ^* is the optimal value of $\mathscr{P}$, μ^* is the optimal value of $\mathscr{P}_{\text{aux}}$, and $\mu^* \geqslant \lambda^*$ by (3.4). Since $\boldsymbol{\Gamma}^*$ is a feasible solution of $\mathscr{P}_{\text{aux}}$ and $\mathcal{M}^*$ is a feasible solution of $\mathscr{P}$, we have

$$\text{tr}\{\boldsymbol{\Gamma}^*\} \geqslant \mu^* \geqslant \lambda^* \geqslant f(\mathcal{M}^*) \tag{A.1}$$

where $f(\mathcal{M}^*)$ denote the PCI of $\mathcal{M}^*$.

Combining (A.1) and the fact that $\text{tr}\{\boldsymbol{\Gamma}^*\} = \text{tr}\{\boldsymbol{\Gamma}(\mathcal{M}^*)\} = f(\mathcal{M}^*)$ by the property of partial trace and the definition of $\boldsymbol{\Gamma}(\mathcal{M}^*)$, we have

$$\text{tr}\{\boldsymbol{\Gamma}^*\} = \mu^* = \lambda^* = f(\mathcal{M}^*). \tag{A.2}$$

Therefore, $\mathcal{M}^*$ is an optimal solution of $\mathscr{P}$ and $\boldsymbol{\Gamma}^*$ is an optimal solution of $\mathscr{P}_{\text{aux}}$.

Necessary Condition: To show that $\boldsymbol{\Gamma}^*$ is a feasible solution of $\mathscr{P}_{\text{aux}}$, we need to prove that

$$\boldsymbol{\Gamma}^* \in \mathcal{L}^+(\mathcal{H}_{s_1}) \tag{A.3}$$

$$\operatorname{tr}\{\boldsymbol{\Gamma}^* \boldsymbol{G}\} \geqslant \lambda^*_{\boldsymbol{G}},\ \forall \boldsymbol{G} \in \mathcal{F} \tag{A.4}$$

Note that $\boldsymbol{\Gamma}^*$ is obtained by taking the partial trace of $\boldsymbol{\Gamma}(\mathcal{M}^*)$, which is a Hermitian operator. Hence $\boldsymbol{\Gamma}^*$ is also a Hermitian operator, i.e., $\boldsymbol{\Gamma}^* \in \mathcal{L}(\mathcal{H}_{s_1})$. If (A.4) holds, (A.3) will also hold given $\lambda^*_{\boldsymbol{G}} \geqslant 0$ and $\boldsymbol{\Gamma}^* \in \mathcal{L}(\mathcal{H}_{s_1})$. Note that $\lambda^*_{\boldsymbol{G}} \geqslant 0$ by the definition, therefore it is sufficient to prove (A.4).

We will prove (A.4) by contradiction. Suppose there exists some $0 \preccurlyeq \boldsymbol{G} \preccurlyeq \boldsymbol{I}_{\mathcal{H}_{s_1}}$ such that

$$\operatorname{tr}\{\boldsymbol{\Gamma}^* \boldsymbol{G}\} < \lambda^*_{\boldsymbol{G}}.$$

We then construct an LOCC protocol $\tilde{\mathcal{M}}$ that can achieve a higher PCI than $\mathcal{M}^*$, which gives the contradiction. The proof goes through three steps:

- Step 1: construction of $\tilde{\mathcal{M}}$.
- Step 2: show that $\tilde{\mathcal{M}}$ is a feasible solution of $\mathscr{P}$.
- Step 3: show that the PCI of $\tilde{\mathcal{M}}$ is higher than that of $\mathcal{M}^*$.

Step 1: Recall the number of outcomes for the i-th measurement in $\mathcal{M}^*$ is m_i. Denote the number of outcomes for the i-th measurement in $\tilde{\mathcal{M}}$ by $\tilde{m}_i$. Let $\tilde{m}_1 = m_1 + 2$ and $\tilde{m}_i = m_i, \forall i \in \{2, 3, \ldots, r\}$. Therefore, the first measurement of $\tilde{\mathcal{M}}$ has two more outcomes than $\mathcal{M}^*$. Let $\boldsymbol{z}_{x:y} = [z_x, z_{x+1}, \ldots, z_y]$.

Let the operators in $\mathcal{M}^*$ be $\boldsymbol{M}^*_{\boldsymbol{z}_{1:i}}$:

$$\mathcal{M}^* = \{\boldsymbol{M}^*_{\boldsymbol{z}_{1:i}} \mid i \in \mathcal{K}_r, z_j \in \mathcal{K}_{m_j} \text{ for } j \leqslant i\}.$$

Let the operators in $\tilde{\mathcal{M}}$ be $\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:i}}$:

$$\tilde{\mathcal{M}} = \{\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:i}} \mid i \in \mathcal{K}_r, z_j \in \mathcal{K}_{\tilde{m}_j} \text{ for } j \leqslant i\}.$$

The operators $\tilde{\boldsymbol{M}}_{[z_1]}$ associated with the first measurement in $\tilde{\mathcal{M}}^*$ is constructed as follows:

$$\begin{aligned}
\tilde{\boldsymbol{M}}_{[c]} &= (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G})\boldsymbol{M}^*_{[c]}(\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}), \forall c \in \mathcal{K}_{m_1} \\
\tilde{\boldsymbol{M}}_{[m_1+1]} &= (2\epsilon - \epsilon^2)\boldsymbol{G}, \\
\tilde{\boldsymbol{M}}_{[m_1+2]} &= \epsilon^2(\boldsymbol{G} - \boldsymbol{G}^2).
\end{aligned}$$

where $0 < \epsilon < 1$.

Next, we construct $\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:i}}$ for $i \geqslant 2$. Consider $\boldsymbol{z}_{1:i}$ with $z_1 \in \mathcal{K}_{m_1}$ and $2 \leqslant i \leqslant r$, let

$$\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:i}} = \begin{cases} \boldsymbol{M}^*_{\boldsymbol{z}_{1:i}} & s_i \neq s_1 \\ (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G})\boldsymbol{M}^*_{\boldsymbol{z}_{1:i}}(\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) & s_i = s_1. \end{cases}$$

Consider $\boldsymbol{z}_{1:i}$ with $z_1 = m_1 + 1$ and $2 \leqslant i \leqslant r$. Let $\mathring{\mathcal{M}} = \{\mathring{\boldsymbol{M}}_{\boldsymbol{z}_{[1,2:i]}} \mid i \in \mathcal{K}_r, z_j \in \mathcal{K}_{\tilde{m}_j} \text{ for } j \leqslant i\}$ be the set of optimal solution for the problem $\mathscr{P}_{\boldsymbol{G}}$. Then let

$$\tilde{\boldsymbol{M}}_{[m_1+1,\boldsymbol{z}_{2:i}]} = \begin{cases} \mathring{\boldsymbol{M}}_{[1,\boldsymbol{z}_{2:i}]} & s_i \neq s_1 \\ (2\epsilon - \epsilon^2)\mathring{\boldsymbol{M}}_{[1,\boldsymbol{z}_{2:i}]} & s_i = s_1. \end{cases}$$

Consider $\boldsymbol{z}_{1:i}$ with $z_1 = m_1 + 2$ and $2 \leqslant i \leqslant r$. An arbitrary feasible solution is assigned to $\tilde{\boldsymbol{M}}_{[m_1+2,\boldsymbol{z}_{2:i}]}$.

Step 2: We will show that $\tilde{\boldsymbol{M}}_{[z_1]}, z_1 \in \mathcal{K}_{\tilde{m}_1}$ satisfy the constraints (2.1) and (2.2) and the others of $\tilde{\mathcal{M}} = \{\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:i}}\}$ can verified directly.

Note that $\boldsymbol{G} - \boldsymbol{G}^2 \succcurlyeq 0$ since $\boldsymbol{I}_{\mathcal{H}_{s_1}} \succcurlyeq \boldsymbol{G} \succcurlyeq 0$. Hence $\tilde{\boldsymbol{M}}_{[z_1]}$ is a positive semidefinite operator for all $z_1 \in \mathcal{K}_{\tilde{m}_1}$. Furthermore, since $\sum_{z_1=1}^{m_1} \boldsymbol{M}^*_{[z_1]} = \boldsymbol{I}_{\mathcal{H}_{s_1}}$, we have

$$\begin{aligned}
\sum_{z_1=1}^{m_1+2} \tilde{\boldsymbol{M}}_{[z_1]} &= \sum_{z_1=1}^{m_1} (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \boldsymbol{M}^*_{[c]} (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \\
&\quad + \tilde{\boldsymbol{M}}_{[m_1+1]} + \tilde{\boldsymbol{M}}_{[m_1+2]} \\
&= (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \left(\sum_{z_1=1}^{m_1} \boldsymbol{M}^*_{[c]} \right) (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \\
&\quad + \tilde{\boldsymbol{M}}_{[m_1+1]} + \tilde{\boldsymbol{M}}_{[m_1+2]} \\
&= (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G})(\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \\
&\quad + \tilde{\boldsymbol{M}}_{[m_1+1]} + \tilde{\boldsymbol{M}}_{[m_1+2]} \\
&= (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G})(\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \\
&\quad + (2\epsilon - \epsilon^2)\boldsymbol{G} + \epsilon^2 (\boldsymbol{G} - \boldsymbol{G}^2) \\
&= \boldsymbol{I}_{\mathcal{H}_{s_1}}.
\end{aligned}$$

Hence $\tilde{\boldsymbol{M}}_{[z_1]}$ satisfy the constraints (2.1) and (2.2).

Step 3: Let the PCI of the protocol $\tilde{\mathcal{M}}$ be $f(\tilde{\mathcal{M}})$. Ignoring the PCI when $z_1 = m_1 + 2$, we have

$$\begin{aligned}
&f(\tilde{\mathcal{M}}) \\
&\geqslant \sum_{z_1 \in \mathcal{K}_{m_1}, \boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\Big\{ (\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{z_r} \Big\} \\
&\quad + \sum_{z_1 = m_1+1, \boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\Big\{ (\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{z_r} \Big\}.
\end{aligned}$$

For $z_1 \in \mathcal{K}_{m_1}$, recall that $\boldsymbol{N}_k = \sum_{\boldsymbol{z}_{1:(r-1)}, z_r = k} \otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{1:l(n)}}$. Let $\mathcal{H}_{\overline{n}}$ be

$$\mathcal{H}_{\overline{n}} = \bigotimes_{m \in \mathcal{K}_N \setminus \{n\}} \mathcal{H}_m.$$

Denote $\tilde{\boldsymbol{N}}_k$ by [1]

$$\begin{aligned}\tilde{\boldsymbol{N}}_k &= \sum_{z_1 \in \mathcal{K}_{m_1}, \boldsymbol{z}_{2:(r-1)}, z_r = k} \otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}} \\ &= \left((\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}} \right) \boldsymbol{N}_k \left((\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}} \right).\end{aligned}$$

Then

$$\begin{aligned}&\sum_{z_1 \in \mathcal{K}_{m_1}, \boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\left\{ (\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{z_r} \right\} \\ &= \sum_{k=1}^{K} p_k \operatorname{tr}\left\{ \tilde{\boldsymbol{N}}_k \boldsymbol{\Xi}_k \right\} \\ &= \sum_{k=1}^{K} p_k \operatorname{tr}\{ \boldsymbol{N}_k \boldsymbol{\Xi}_k \} + O(\epsilon^2) \\ &\qquad - \epsilon \operatorname{tr}\left\{ \left(\boldsymbol{G} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}} \right) \sum_{k=1}^{K} p_k \boldsymbol{N}_k \boldsymbol{\Xi}_k \right\} \\ &\qquad - \epsilon \operatorname{tr}\left\{ \left(\boldsymbol{G} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}} \right) \sum_{k=1}^{K} p_k \boldsymbol{\Xi}_k \boldsymbol{N}_k \right\} \\ &= \sum_{k=1}^{K} p_k \operatorname{tr}\{ \boldsymbol{N}_k \boldsymbol{\Xi}_k \} + O(\epsilon^2) - 2\epsilon \operatorname{tr}\{ \boldsymbol{\Gamma}^* \boldsymbol{G} \}.\end{aligned}$$

For $z_1 = m_1 + 1$, note that

$$\begin{aligned}&\sum_{z_1 = m_1 + 1, \boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\left\{ (\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{z_r} \right\} \\ &= (2\epsilon - \epsilon^2) \sum_{z_1 = m_1 + 1, \boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\left\{ (\otimes_{n=1}^{N} \mathring{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{z_r} \right\} \\ &= (2\epsilon - \epsilon^2) \lambda_{\boldsymbol{G}}^*.\end{aligned}$$

[1] Here, we use $(\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}$ to represent $\boldsymbol{A} \otimes (\boldsymbol{I}_{\mathcal{H}_{s_1}} - \epsilon \boldsymbol{G}) \otimes \boldsymbol{B}$, where $\boldsymbol{A} = \boldsymbol{I}_{\mathcal{H}_1} \otimes \ldots \otimes \boldsymbol{I}_{\mathcal{H}_{s_1 - 1}}$, $\boldsymbol{B} = \boldsymbol{I}_{\mathcal{H}_{s_1+1}} \otimes \ldots \otimes \boldsymbol{I}_{\mathcal{H}_N}$.

Therefore,

$$
\begin{aligned}
& f(\tilde{\mathcal{M}}) \\
& \geqslant \sum_{z_1 \in \mathcal{K}_{m_1}, \boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\Big\{(\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{\boldsymbol{z}_r}\Big\} \\
& \quad + \sum_{z_1 = m_1+1, \boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\Big\{(\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{1:l(n)}}) \boldsymbol{\Xi}_{\boldsymbol{z}_r}\Big\} \\
& = \sum_{k=1}^{K} p_k \operatorname{tr}\{\boldsymbol{N}_k \boldsymbol{\Xi}_k\} + O(\epsilon^2) - 2\epsilon \operatorname{tr}\{\boldsymbol{\Gamma}^* \boldsymbol{G}\} \\
& \quad + (2\epsilon - \epsilon^2)\lambda_{\boldsymbol{G}}^* \\
& = \sum_{k=1}^{K} p_k \operatorname{tr}\{\boldsymbol{N}_k \boldsymbol{\Xi}_k\} + 2\epsilon(\lambda_{\boldsymbol{G}}^* - \operatorname{tr}\{\boldsymbol{\Gamma}^* \boldsymbol{G}\}) + O(\epsilon^2).
\end{aligned}
$$

Note that $\sum_{k=1}^{K} p_k \operatorname{tr}\{\boldsymbol{N}_k \boldsymbol{\Xi}_k\}$ is the PCI of $\mathcal{M}^*$, and $\lambda_{\boldsymbol{G}}^* \geqslant \operatorname{tr}\{\boldsymbol{\Gamma}^* \boldsymbol{G}\}$. Hence, there exists $\epsilon > 0$, such that $\tilde{\mathcal{M}}$ can achieve a higher PCI than $\mathcal{M}^*$, which contradicts with the assumption that $\mathcal{M}^*$ is the optimal protocol. This proves that $\boldsymbol{\Gamma}^*$ is indeed a feasible solution of $\mathscr{P}_{\text{aux}}$. □

Proof of Corollary 1: As proven in (A.2), the optimal solution $\mathcal{M}^*$ and the corresponding operator $\boldsymbol{\Gamma}^*$ satisfy $\operatorname{tr}\{\boldsymbol{\Gamma}^*\} = \mu^* = \lambda^* = f(\mathcal{M}^*)$. This means that the optimal value of $\mathscr{P}$ is equal to the optimal value of $\mathscr{P}_{\text{aux}}$.

A.2 Proof of Theorem 2

Proof. Consider the optimization problem $\mathscr{P}_{\text{aux}}$ defined in (3.3) of the main paper. Recall that the communication sequence is $\boldsymbol{s}$. The length of $\boldsymbol{s}$ is r. We rewrite $\mathscr{P}_{\text{aux}}$ in the following form:

$$
\begin{aligned}
\mathscr{P}_{\text{aux}}: \ & \text{minimize} \quad \operatorname{tr}\{\boldsymbol{X}\} \\
& \text{subject to } \boldsymbol{X} \in \mathcal{L}^+(\mathcal{H}_{s_1}) \\
& \qquad\qquad \operatorname{tr}\{\boldsymbol{X}\boldsymbol{G}^2\} \geqslant \lambda_{\boldsymbol{G}^2}^*, \ \forall \boldsymbol{G} \in \mathcal{W}
\end{aligned}
$$

where $\mathcal{W} = \{\boldsymbol{G} \mid \boldsymbol{G} \succcurlyeq 0, \|\boldsymbol{G}\|_{\mathrm{F}} = 1\}$ ($\|\cdot\|_{\mathrm{F}}$ is the Frobenius norm). The new form is equivalent to the original form since $\boldsymbol{G} \in \mathcal{F}$ iff $\boldsymbol{G}^2 \in \mathcal{F}$ and $\mathrm{tr}\{\boldsymbol{X}\boldsymbol{G}^2\} \geqslant \lambda^*_{\boldsymbol{G}^2}$ is equivalent to $\mathrm{tr}\{\boldsymbol{X}\boldsymbol{G}^2 \cdot c\} \geqslant \lambda^*_{\boldsymbol{G}^2 \cdot c}$ for any positive number $c > 0$. Let μ^* be the optimal value of $\mathscr{P}_{\mathrm{aux}}$. We aim to develop the SR algorithm that approximates μ^*, i.e., the optimal value λ^* of the problem $\mathscr{P}$, within precision ϵ and time complexity $\left(\frac{\tilde{D}r}{\epsilon}\right)^{O(\tilde{D}^2 r)}$, where $\tilde{D} = \max_n \dim \mathcal{H}_n$. In particular, the proof goes through three steps:

- Step 1: development of the SR algorithm.
- Step 2: characterization of the approximation error for the algorithm.
- Step 3: characterization of the time complexity for the algorithm.

Step 1: We firstly provide a lemma for constructing the epsilon-net of $\mathcal{W}$.

Lemma 1. *In a D-dimensional Hilbert space $\mathcal{H}$, let $\mathcal{W} = \{\boldsymbol{H} \mid \boldsymbol{H} \succcurlyeq 0, \|\boldsymbol{H}\|_{\mathrm{F}} = 1\}$. There exists a set $\mathcal{W}_\delta = \{\boldsymbol{H}_i \in \mathcal{W}, i \in \mathcal{K}_M\}$ with*

$$M \leqslant \left(\frac{3}{\delta}\right)^{2D^2}$$

such that for any $\boldsymbol{H} \in \mathcal{W}$, there exists a $\boldsymbol{H}_i \in \mathcal{W}_\delta$ where $\|\boldsymbol{H} - \boldsymbol{H}_i\|_{\mathrm{F}} \leqslant \delta \leqslant 1$.

Proof. Let $\mathcal{W}_\delta = \{\boldsymbol{H}_i \in \mathcal{W}, i \in \mathcal{K}_M\}$ be the maximal subset of $\mathcal{W}$ such that

$$\forall i, j \in \mathcal{K}_M, \|\boldsymbol{H}_i - \boldsymbol{H}_j\|_{\mathrm{F}} \geqslant \delta.$$

It is easy to see that for any $\boldsymbol{H} \in \mathcal{W}$, there exists a $\boldsymbol{H}_i \in \mathcal{W}_\delta$ such that $\|\boldsymbol{H} - \boldsymbol{H}_i\|_{\mathrm{F}} \leqslant \delta$. Otherwise a new element can be added into $\mathcal{W}_\delta$. As a subspace of $\mathbb{R}^{2D^2}$, each ball centered at $\boldsymbol{H}_i$ with $\delta/2$ radius are disjointed and contained in the ball centered at zero point with $1 + \delta/2$ radius. Therefore,

$$M \leqslant \frac{(1+\delta/2)^{2D^2}}{(\delta/2)^{2D^2}} \leqslant \left(\frac{3}{\delta}\right)^{2D^2}.$$

□

Let the dimension of $\mathcal{H}_{s_1}$ be D. By Lemma 1, we can find a set $\mathcal{W}_\delta = \{\boldsymbol{G}_i \in \mathcal{W}, i \in \mathcal{K}_M\}$ where $M \leqslant \left(\frac{3}{\delta}\right)^{2D^2}$ such that for any $\boldsymbol{G} \in \mathcal{W}$, there exists a $\boldsymbol{G}_i \in \mathcal{W}_\delta$ where $\|\boldsymbol{G} - \boldsymbol{G}_i\|_\mathrm{F} \leqslant \delta$. Then consider the following optimization problem:

$$\begin{aligned} \tilde{\mathscr{P}}_\mathrm{aux}: \ \text{minimize} \quad & \mathrm{tr}\{\boldsymbol{X}\} \\ \text{subject to} \quad & \boldsymbol{X} \in \mathcal{L}^+(\mathcal{H}_{s_1}) \\ & \mathrm{tr}\{\boldsymbol{X}\boldsymbol{G}_i^2\} \geqslant \lambda^*_{\boldsymbol{G}_i^2}, \forall \boldsymbol{G}_i \in \mathcal{W}_\delta. \end{aligned}$$

The optimization value of $\tilde{\mathscr{P}}_\mathrm{aux}$ can be viewed as a good approximation of μ^*. Recall that $\lambda^*_{\boldsymbol{G}_i^2}$ for each $\boldsymbol{G}_i \in \mathcal{W}_\delta$ can be obtained by solving an optimization problem that corresponds to a multiparty QSD with a shorter communication sequence $\mathring{\boldsymbol{s}}$. Let $\mathring{\lambda}$ denote the maximum PCI for this new multiparty QSD. We have

$$\lambda^*_{\boldsymbol{G}_i^2} = \mathring{\lambda} \cdot q_i$$

where

$$\begin{aligned} q_i &:= \sum_{k=1}^{K} p_k \, \mathrm{tr}\{(\boldsymbol{G}_i \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}) \, \boldsymbol{\Xi}_k \, (\boldsymbol{G}_i \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}})\} \\ &= \mathrm{tr}\left\{\boldsymbol{G}_i \, \mathrm{tr}_{\mathcal{H}_{\bar{s}_1}}\left(\sum_{k=1}^{K} p_k \boldsymbol{\Xi}_k\right) \boldsymbol{G}_i\right\} \\ &= \mathrm{tr}\left\{\boldsymbol{G}_i^2 \, \mathrm{tr}_{\mathcal{H}_{\bar{s}_1}}\left(\sum_{k=1}^{K} p_k \boldsymbol{\Xi}_k\right)\right\}. \end{aligned}$$

Assume we can obtain an estimator $\hat{\mathring{\lambda}}$ for $\mathring{\lambda}$, let $\hat{\lambda}_{\boldsymbol{G}_i^2} = \hat{\mathring{\lambda}} q_i$. Consider the following optimization problem that replaces $\lambda^*_{\boldsymbol{G}_i^2}$ in $\tilde{\mathscr{P}}_\mathrm{aux}$ by $\hat{\lambda}_{\boldsymbol{G}_i^2}$,

$$\begin{aligned} \tilde{\tilde{\mathscr{P}}}_\mathrm{aux}: \ \text{minimize} \quad & \mathrm{tr}\{\boldsymbol{X}\} \\ \text{subject to} \quad & \boldsymbol{X} \in \mathcal{L}^+(\mathcal{H}_{s_1}) \\ & \mathrm{tr}\{\boldsymbol{X}\boldsymbol{G}_i^2\} \geqslant \hat{\lambda}_{\boldsymbol{G}_i^2}, \forall \boldsymbol{G}_i \in \mathcal{W}_\delta. \end{aligned}$$

We can solve $\tilde{\tilde{\mathscr{P}}}_{\text{aux}}$, which can be regarded as an approximation of $\mathscr{P}$, by SDP. Therefore, based on the estimator for the maximal PCI of a multiparty QSD with $(r-1)$-step communication sequence, we provide an estimator for λ^* that corresponds to the maximal PCI of an r-step multiparty QSD. Note that this can be done recursively. We will end up with QSD problems that have only one party in the system that can be solved easily. This algorithm is called SR algorithm.

Step 2: Next, by induction, we will provide an error analysis for $\tilde{\tilde{\mathscr{P}}}_{\text{aux}}$ to quantify the approximation of $\mathscr{P}$ when $\delta = \epsilon/4D$. Let the optimal value of $\tilde{\tilde{\mathscr{P}}}_{\text{aux}}$ be $\hat{\lambda}^*$ and the optimal solution of $\tilde{\tilde{\mathscr{P}}}_{\text{aux}}$ be $\boldsymbol{X}^*$, respectively.

Assume we can obtain the estimator $\hat{\mathring{\lambda}}$ for the maximal PCI $\mathring{\lambda}$ of any $(r-1)$-step multiparty QSD such that

$$\mathring{\lambda} - (r-1)\epsilon \leqslant \hat{\mathring{\lambda}} \leqslant \mathring{\lambda}.$$

We aim to show

$$\lambda^* - r\epsilon \leqslant \hat{\lambda}^* \leqslant \lambda^* \tag{A.5}$$

where λ^* is the optimal value of $\mathscr{P}$.

Firstly, the feasible solution set of $\tilde{\tilde{\mathscr{P}}}_{\text{aux}}$ contains the feasible solution set of $\mathscr{P}_{\text{aux}}$ since $\hat{\mathring{\lambda}} \leqslant \mathring{\lambda}$ and thereby $\hat{\lambda}^*_{\boldsymbol{G}_i^2} \leqslant \lambda^*_{\boldsymbol{G}_i^2}$. Hence,

$$\hat{\lambda}^* \leqslant \mu^* = \lambda^*.$$

where μ^* is the optimal solution of $\mathscr{P}_{\text{aux}}$.

Next, we show that

$$\lambda^* = \mu^* \leqslant \min\{\hat{\lambda}^* + r\epsilon, 1\}.$$

Note that $\lambda^* \leqslant 1$ since the physical meaning of λ^* is the maximum PCI. Hence, we focus on the scenario $\hat{\lambda}^* + r\epsilon \leqslant 1$.

Let

$$\boldsymbol{X}^{**} := \boldsymbol{X}^{*} + (r-1)\epsilon\,\mathrm{tr}_{\mathcal{H}_{\bar{s}_1}}\left(\sum_{k=1}^{K} p_k \boldsymbol{\Xi}_k\right) + \frac{\epsilon}{D}\boldsymbol{I}_{\mathcal{H}_{s_1}}.$$

Note that $\mathrm{tr}\{\boldsymbol{X}^{**}\} = \hat{\lambda}^* + r\epsilon$. If $\boldsymbol{X}^{**}$ is a feasible solution of $\mathscr{P}_{\mathrm{aux}}$, then $\mu^* \leqslant \hat{\lambda}^* + r\epsilon$ gives the desired result.

In order to show that $\boldsymbol{X}^{**}$ is a feasible solution of $\mathscr{P}_{\mathrm{aux}}$, we first present the following lemma, where the proof will be given in the next section.

Lemma 2. *In a D-dimensional Hilbert space, let* $\boldsymbol{H}, \tilde{\boldsymbol{H}} \succcurlyeq 0, \|\boldsymbol{H}\|_{\mathrm{F}} = 1, \|\tilde{\boldsymbol{H}}\|_{\mathrm{F}} = 1$ *and* $\|\tilde{\boldsymbol{H}} - \boldsymbol{H}\|_{\mathrm{F}} \leqslant \epsilon$. *Consider the optimization problem* $\mathscr{P}$ *and* $\mathscr{P}_{\boldsymbol{H}}$ *given by (2.3) and (3.1) respectively. Let* $\lambda^*_{\boldsymbol{H}}$ *be the optimal value of* $\mathscr{P}_{\boldsymbol{H}}$. *For any operator* $\boldsymbol{X}$ *such that* $\boldsymbol{X} \succcurlyeq 0, \mathrm{tr}\{\boldsymbol{X}\} \leqslant 1$, *the following inequality holds:*

$$\mathrm{tr}\left\{\boldsymbol{X}\tilde{\boldsymbol{H}}^2\right\} - \lambda^*_{\tilde{\boldsymbol{H}}^2} \geqslant \mathrm{tr}\left\{\boldsymbol{X}\boldsymbol{H}^2\right\} - \lambda^*_{\boldsymbol{H}^2} - 4\epsilon.$$

By Lemma 1, for any $\boldsymbol{G} \in \mathcal{W}$, there exists $\boldsymbol{G}_i \in \mathcal{W}_{\frac{\epsilon}{4D}}$ such that $\|\boldsymbol{G} - \boldsymbol{G}_i\|_{\mathrm{F}} \leqslant \epsilon/(4D)$. Note that $\boldsymbol{G}, \boldsymbol{G}_i \succcurlyeq 0, \|\boldsymbol{G}\|_{\mathrm{F}} = \|\boldsymbol{G}_i\|_{\mathrm{F}} = 1$, and $\mathrm{tr}\{\boldsymbol{X}^{**}\} = \hat{\lambda}^* + r\epsilon \leqslant 1$. Moreover, $\boldsymbol{X}^{**} \in \mathcal{L}^+(\mathcal{H}_{s_1})$ since

$$\boldsymbol{X}^{*}, \mathrm{tr}_{\mathcal{H}_{\bar{s}_1}}\left(\sum_{k=1}^{K} p_k \boldsymbol{\Xi}_k\right), \boldsymbol{I}_{\mathcal{H}_{s_1}} \in \mathcal{L}^+(\mathcal{H}_{s_1}).$$

Then, by Lemma 2,

$$\begin{aligned}\operatorname{tr}\{\boldsymbol{X}^{**}\boldsymbol{G}^2\} - \lambda^*_{\boldsymbol{G}^2} &\geqslant \operatorname{tr}\{\boldsymbol{X}^{**}\boldsymbol{G}_i^2\} - \lambda^*_{\boldsymbol{G}_i^2} - 4\frac{\epsilon}{4D} \\ &\geqslant \operatorname{tr}\{\boldsymbol{X}^{**}\boldsymbol{G}_i^2\} \\ &\quad - \hat{\lambda}_{\boldsymbol{G}_i^2} - (r-1)\epsilon q_i - \frac{\epsilon}{D} \\ &= \operatorname{tr}\{\boldsymbol{X}^{*}\boldsymbol{G}_i^2\} + (r-1)\epsilon q_i \\ &\quad + \frac{\epsilon}{D}\operatorname{tr}\{\boldsymbol{G}_i^2\} \\ &\quad - \hat{\lambda}_{\boldsymbol{G}_i^2} - (r-1)\epsilon q_i - \frac{\epsilon}{D} \\ &= \operatorname{tr}\{\boldsymbol{X}^{*}\boldsymbol{G}_i^2\} - \hat{\lambda}_{\boldsymbol{G}_i^2} \\ &\geqslant 0.\end{aligned}$$

Here, we use the fact that $q_i = \operatorname{tr}\left\{\boldsymbol{G}_i^2 \operatorname{tr}_{\mathcal{H}_{\bar{s}_1}}\left(\sum_{k=1}^K p_k \boldsymbol{\Xi}_k\right)\right\}$, $\lambda^*_{\boldsymbol{G}_i^2} \leqslant \hat{\lambda}_{\boldsymbol{G}_i^2} + (r-1)\epsilon q_i$, $\operatorname{tr}\{\boldsymbol{G}_i^2\} = \|\boldsymbol{G}_i\|_{\mathrm{F}}^2 = 1$, and $\operatorname{tr}\{\boldsymbol{X}^*\boldsymbol{G}_i^2\} \geqslant \hat{\lambda}_{\boldsymbol{G}_i^2}$. Therefore, $\boldsymbol{X}^{**}$ is a feasible solution of $\mathscr{P}_{\text{aux}}$, and

$$\lambda^* = \mu^* \leqslant \operatorname{tr}\{\boldsymbol{X}^{**}\} = \hat{\lambda}^* + r\epsilon.$$

Note that this procedure can be done inductively. We can conclude that, when $\delta = \epsilon/4D$, (A.5) provides a performance guarantee of the SR algorithm.

Step 3: Next, we consider the time complexity of the whole algorithm. For solving an r-step multiparty QSD optimization problem, we need to

- solve $|\mathcal{W}_\delta|$ $(r-1)$-step multiparty QSD optimization problems.
- solve an SDP problem with $|\mathcal{W}_\delta|$ constraints.

Let $T(r)$ be the time complexity of solving an r-step multiparty QSD. Let $S(|\mathcal{W}_\delta|)$ be the time complexity of solving an SDP problem with $|\mathcal{W}_\delta|$ constraints. Then

$$T(r) = |\mathcal{W}_\delta| T(r-1) + S(|\mathcal{W}_\delta|).$$

Note that $S(|\mathcal{W}_\delta|)$ is a polynomial function of $|\mathcal{W}_\delta|$ and $T(r)$ can be calculated recursively. Let $\tilde{D} = \max_n \dim \mathcal{H}_n$ and $\delta = \epsilon/4\tilde{D}$. Then $|\mathcal{W}_\delta| \leqslant \left(\frac{12\tilde{D}}{\epsilon}\right)^{2\tilde{D}^2}$ by Lemma 1. We can obtain that $T(r) = \left(\frac{\tilde{D}}{\epsilon}\right)^{O(\tilde{D}^2 r)}$. Note that the precision of the r-step multiparty QSD optimization problem is $r\epsilon$. Hence, for achieving an precision ϵ', the total time complexity is $\left(\frac{\tilde{D}r}{\epsilon'}\right)^{O(\tilde{D}^2 r)}$, which completes the proof.[2]

□

A.3 Proof of Lemma 2

Proof. Let

$$a := \mathrm{tr}\left\{\tilde{\boldsymbol{H}}\boldsymbol{X}\tilde{\boldsymbol{H}}\right\} - \lambda^*_{\tilde{\boldsymbol{H}}^2},$$
$$b := \mathrm{tr}\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H}\} - \lambda^*_{\boldsymbol{H}^2}.$$

Denote $\boldsymbol{\Delta} = \boldsymbol{H} - \tilde{\boldsymbol{H}}$. We have $\|\boldsymbol{\Delta}\|_2 \leqslant \|\boldsymbol{\Delta}\|_{\mathrm{F}} \leqslant \epsilon$ ($\|\cdot\|_2$ is the spectral norm). Recall that the optimization for $\lambda^*_{\boldsymbol{H}^2}$ can be formulated as an optimization problem that corresponds to a multiparty QSD with the communication sequence $\mathring{\boldsymbol{s}} = (s_2, s_3, \ldots, s_r)$. In particular, one can verify that $\lambda^*_{\boldsymbol{H}^2}$ is equal to the optimal value of the following optimization problem:

$$\mathring{\mathscr{P}}_{\boldsymbol{H}^2} : \ \underset{\mathcal{M}}{\text{maximize}} \ \sum_{\boldsymbol{z}_{2:r}} p_{z_r} \,\mathrm{tr}\left\{(\otimes_{n=1}^N \boldsymbol{M}_{\boldsymbol{z}_{2:l(n)}})\mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H})\right\}$$
$$\text{subject to} \ \text{constraints (2.1) and (2.2)}$$

where $\mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H}) = \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_{z_r} \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)$ and $\mathcal{M} = \{\boldsymbol{M}_{\boldsymbol{z}_{2:i}}\}$ is an LOCC protocol associated with $\mathring{\boldsymbol{s}}$.

Let $\tilde{\mathcal{M}} = \{\tilde{\boldsymbol{M}}_{\boldsymbol{z}_{2:i}}\}$ be the optimal solution for $\mathring{\mathscr{P}}_{\tilde{\boldsymbol{H}}^2}$. Let

$$\tilde{\boldsymbol{N}}_k = \sum_{\boldsymbol{z}_{2:(r-1)}, z_r = k} \otimes_{n=1}^N \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{2:l(n)}}.$$

[2]Here we do not count the time complexity for constructing the set $\mathcal{W}_\delta$ since it is independent from the input and can be obtained offline.

Note that

$$
\begin{aligned}
\lambda^*_{\boldsymbol{H}^2} &= \max_{\mathcal{M}} \sum_{\boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\Big\{(\otimes_{n=1}^{N} \boldsymbol{M}_{\boldsymbol{z}_{2:l(n)}}) \mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H})\Big\} \\
&\geqslant \sum_{\boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\Big\{(\otimes_{n=1}^{N} \tilde{\boldsymbol{M}}_{\boldsymbol{z}_{2:l(n)}}) \mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H})\Big\} \\
&= \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H})\Big\}.
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
b &= \operatorname{tr}\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H}\} - \lambda^*_{\boldsymbol{H}^2} \\
&\leqslant \operatorname{tr}\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H}\} - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \mathring{\boldsymbol{\Xi}}_{z_r}(\boldsymbol{H})\Big\} \\
&= \operatorname{tr}\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H}\} \\
&\quad - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\}.
\end{aligned}
$$

Note that

$$
\lambda^*_{\tilde{\boldsymbol{H}}^2} = \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\}.
$$

Hence,

$$
\begin{aligned}
b &\leqslant \operatorname{tr}\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H}\} \\
&\quad - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\} \\
&= \operatorname{tr}\Big\{\tilde{\boldsymbol{H}}\boldsymbol{X}\tilde{\boldsymbol{H}}\Big\} - \lambda^*_{\tilde{\boldsymbol{H}}^2} \\
&\quad + \operatorname{tr}\Big\{\boldsymbol{H}\boldsymbol{X}\boldsymbol{H} - \tilde{\boldsymbol{H}}\boldsymbol{X}\tilde{\boldsymbol{H}}\Big\} \\
&\quad + \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\} \\
&\quad - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\} \\
&= a + \operatorname{tr}\Big\{\boldsymbol{\Delta}\boldsymbol{X}\boldsymbol{H} + \tilde{\boldsymbol{H}}\boldsymbol{X}\boldsymbol{\Delta}\Big\} \\
&\quad - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\boldsymbol{\Delta} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\} \\
&\quad - \sum_{k=1}^{K} p_k \operatorname{tr}\Big\{\tilde{\boldsymbol{N}}_k \left(\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right) \boldsymbol{\Xi}_k \left(\boldsymbol{\Delta} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right)\Big\}.
\end{aligned}
$$

Note that for arbitrary $\boldsymbol{A} \succcurlyeq 0$, where $\boldsymbol{A}$ has the eigen-decomposition $\boldsymbol{A} = \sum_i \lambda_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$, we have $|\operatorname{tr}\{\boldsymbol{A}\boldsymbol{B}\}| \leqslant \operatorname{tr}\{\boldsymbol{A}\}\|\boldsymbol{B}\|_2$ due to the follows:

$$
\begin{aligned}
|\operatorname{tr}\{\boldsymbol{A}\boldsymbol{B}\}| &= |\sum_i \lambda_i \left\langle\phi_i\right| \boldsymbol{B} \left|\phi_i\right\rangle| \\
&\leqslant \sum_i \lambda_i |\left\langle\phi_i\right| \boldsymbol{B} \left|\phi_i\right\rangle| \\
&\leqslant \sum_i \lambda_i \|\boldsymbol{B}\|_2 \\
&= \operatorname{tr}\{\boldsymbol{A}\}\|\boldsymbol{B}\|_2.
\end{aligned} \tag{A.6}
$$

Based on (A.6) and $\boldsymbol{X} \succcurlyeq 0, \boldsymbol{\Xi}_k \succcurlyeq 0, \|\boldsymbol{AB}\|_2 \leqslant \|\boldsymbol{A}\|_2\|\boldsymbol{B}\|_2$, we have

$$\begin{aligned} b \leqslant a &+ \operatorname{tr}\{\boldsymbol{X}\}(\|\boldsymbol{\Delta}\|_2\|\boldsymbol{H}\|_2 + \|\boldsymbol{\Delta}\|_2\left\|\tilde{\boldsymbol{H}}\right\|_2) \\ &+ \sum_{k=1}^{K} p_k \operatorname{tr}\{\boldsymbol{\Xi}_k\}\|\boldsymbol{H} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\|_2\|\boldsymbol{\Delta} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\|_2\left\|\tilde{\boldsymbol{N}}_k\right\|_2 \\ &+ \sum_{k=1}^{K} p_k \operatorname{tr}\{\boldsymbol{\Xi}_k\}\left\|\tilde{\boldsymbol{H}} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\right\|_2\|\boldsymbol{\Delta} \otimes \boldsymbol{I}_{\mathcal{H}_{\bar{s}_1}}\|_2\left\|\tilde{\boldsymbol{N}}_k\right\|_2. \end{aligned}$$

Note the fact that $\sum_{k=1}^{K} p_k = 1, \operatorname{tr}\{\boldsymbol{\Xi}_k\} = 1, \left\|\tilde{\boldsymbol{N}}_k\right\|_2 \leqslant 1, \operatorname{tr}\{\boldsymbol{X}\} \leqslant 1, \|\boldsymbol{A} \otimes \boldsymbol{I}\|_2 = \|\boldsymbol{A}\|_2$, then

$$b \leqslant a + 2\|\boldsymbol{\Delta}\|_2\|\boldsymbol{H}\|_2 + 2\|\boldsymbol{\Delta}\|_2\left\|\tilde{\boldsymbol{H}}\right\|_2.$$

Since $\|\boldsymbol{H}\|_2 \leqslant \|\boldsymbol{H}\|_{\mathrm{F}} = 1, \left\|\tilde{\boldsymbol{H}}\right\|_2 \leqslant \left\|\tilde{\boldsymbol{H}}\right\|_{\mathrm{F}} = 1$, we complete the proof:

$$a \geqslant b - 4\|\boldsymbol{\Delta}\|_2 \geqslant b - 4\epsilon.$$

□

A.4 Proof of Theorem 3

Proof. The algorithm for the multiparty QSD where $\boldsymbol{s}$ is one-way is similar to the algorithm constructed in the Theorem 2 with a slight modification. We will conduct the proof by the following three steps:

- Step 1: characterization of the properties for the multiparty QSD when $\boldsymbol{s}$ is one-way.
- Step 2: development of the modified algorithm.
- Step 3: characterization of the approximation error and time complexity for the modified algorithm.

Step 1: Recall that $\lambda^*_{\boldsymbol{H}}$ is the optimal value of the optimization problem $\mathscr{P}_{\boldsymbol{H}}$. When $\boldsymbol{s}$ is one-way, we claim the following convexity of $\lambda^*_{\boldsymbol{H}}$: for any $\boldsymbol{H}_1, \boldsymbol{H}_2 \succcurlyeq 0$ and $l_1, l_2 \geqslant 0$,

$$\lambda^*_{l_1 \cdot \boldsymbol{H}_1 + l_2 \cdot \boldsymbol{H}_2} \leqslant l_1 \cdot \lambda^*_{\boldsymbol{H}_1} + l_2 \cdot \lambda^*_{\boldsymbol{H}_2}.$$

To prove the claim, we firstly show that

$$\lambda^*_{\boldsymbol{H}_1 + \boldsymbol{H}_2} \leqslant \lambda^*_{\boldsymbol{H}_1} + \lambda^*_{\boldsymbol{H}_2}$$

for any $\boldsymbol{H}_1, \boldsymbol{H}_2 \succcurlyeq 0$. To see this, let $\mathcal{M}^* = \{\boldsymbol{M}^*_{[1]}\} \cup \{\boldsymbol{M}^*_{[1,\boldsymbol{z}_{2:i}]} \mid 2 \leqslant i \leqslant r\}$ be the optimal solution of $\mathscr{P}_{\boldsymbol{H}_1+\boldsymbol{H}_2}$. Note that $\boldsymbol{M}^*_{[1]} = \boldsymbol{H}_1 + \boldsymbol{H}_2$ due to the constraints of $\mathscr{P}_{\boldsymbol{H}_1+\boldsymbol{H}_2}$. When $\boldsymbol{s}$ is one-way, $\{\boldsymbol{M}^*_{[1,\boldsymbol{z}_{2:i}]} \mid 2 \leqslant i \leqslant r\}$ corresponds to measurements performed by the parties excluding P_1. Therefore, by replacing $\boldsymbol{M}^*_{[1]} = \boldsymbol{H}_1 + \boldsymbol{H}_2$ by $\boldsymbol{M}^{(1)}_{[1]} = \boldsymbol{H}_1$, we can obtain a feasible solution $\mathcal{M}^{(1)}$ for $\mathscr{P}_{\boldsymbol{H}_1}$:

$$\mathcal{M}^{(1)} = \{\boldsymbol{M}^{(1)}_{[1]}\} \cup \{\boldsymbol{M}^*_{[1,\boldsymbol{z}_{2:i}]} \mid 2 \leqslant i \leqslant r\}.$$

Similarly, we also can obtain a feasible solution $\mathcal{M}^{(2)}$ of $\mathscr{P}_{\boldsymbol{H}_2}$ by replacing $\boldsymbol{M}^*_{[1]} = \boldsymbol{H}_1 + \boldsymbol{H}_2$ by $\boldsymbol{M}^{(2)}_{[1]} = \boldsymbol{H}_2$:

$$\mathcal{M}^{(2)} = \{\boldsymbol{M}^{(2)}_{[1]}\} \cup \{\boldsymbol{M}^*_{[1,\boldsymbol{z}_{2:i}]} \mid 2 \leqslant i \leqslant r\}.$$

Recall that the objective function of $\mathscr{P}_{\boldsymbol{H}}$ has the following form:

$$f(\mathcal{M}) := \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\Big\{(\otimes_{n=1}^N \boldsymbol{M}_{\boldsymbol{z}_{1:l(n)}})\boldsymbol{\Xi}_{z_r}\Big\}.$$

where $\mathcal{M} = \{\boldsymbol{M}_{\boldsymbol{z}_{1:i}} \mid i \in \mathcal{K}_r\}$. When $\boldsymbol{s}$ is one-way, this objective function can be simplified to

$$f(\mathcal{M}) = \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{z_r} \operatorname{tr}\{(\otimes_{n=1}^N \boldsymbol{M}_{\boldsymbol{z}_{1:n}})\boldsymbol{\Xi}_{z_r}\}.$$

Hence, we have

$$
\begin{aligned}
f(\mathcal{M}^*) &= \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\left\{(\otimes_{n=1}^{N}\boldsymbol{M}^*_{\boldsymbol{z}_{1:n}})\boldsymbol{\Xi}_{\boldsymbol{z}_r}\right\} \\
&= \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\left\{((\boldsymbol{H}_1+\boldsymbol{H}_2)\otimes\otimes_{n=2}^{N}\boldsymbol{M}^*_{\boldsymbol{z}_{1:n}})\boldsymbol{\Xi}_{\boldsymbol{z}_r}\right\} \\
&= \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\left\{(\boldsymbol{H}_1\otimes\otimes_{n=2}^{N}\boldsymbol{M}^*_{\boldsymbol{z}_{1:n}})\boldsymbol{\Xi}_{\boldsymbol{z}_r}\right\} \\
&\quad + \sum_{z_1=1,\boldsymbol{z}_{2:r}} p_{\boldsymbol{z}_r} \operatorname{tr}\left\{(\boldsymbol{H}_2\otimes\otimes_{n=2}^{N}\boldsymbol{M}^*_{\boldsymbol{z}_{1:n}})\boldsymbol{\Xi}_{\boldsymbol{z}_r}\right\} \\
&= f(\mathcal{M}^{(1)}) + f(\mathcal{M}^{(2)}).
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\lambda^*_{\boldsymbol{H}_1+\boldsymbol{H}_2} &= f(\mathcal{M}^*) \\
&= f(\mathcal{M}^{(1)}) + f(\mathcal{M}^{(2)}) \\
&\leqslant \lambda^*_{\boldsymbol{H}_1} + \lambda^*_{\boldsymbol{H}_2}.
\end{aligned}
$$

Note that $\lambda^*_{c\cdot\boldsymbol{H}} = c\cdot\lambda^*_{\boldsymbol{H}}$ for any non-negative number c, therefore we can obtain the convexity of $\lambda^*_{\boldsymbol{H}}$ and finish the proof of the claim.

Recall that the optimization problem $\mathscr{P}_{\text{aux}}$ that needs to be solved has the following form:

$$
\begin{aligned}
\mathscr{P}_{\text{aux}}:\ \ &\text{minimize}\ \ \operatorname{tr}\{\boldsymbol{X}\} \\
&\text{subject to}\ \boldsymbol{X}\in\mathcal{L}^+(\mathcal{H}_{s_1}) \\
&\qquad\qquad \operatorname{tr}\{\boldsymbol{X}\boldsymbol{G}\}\geqslant\lambda^*_{\boldsymbol{G}},\ \forall\boldsymbol{G}\in\mathcal{F}
\end{aligned}
$$

where $\mathcal{F} = \{\boldsymbol{H}\mid \boldsymbol{I}_{\mathcal{H}_{s_1}}\succcurlyeq\boldsymbol{H}\succcurlyeq 0\}$. When $\boldsymbol{s}$ is one-way, $\mathscr{P}_{\text{aux}}$ is equivalent to the following optimization problem

$$\begin{aligned}\mathscr{P}_{\text{aux}}^{\text{one-way}}: \text{ minimize } & \operatorname{tr}\{\boldsymbol{X}\} \\ \text{subject to } & \boldsymbol{X} \in \mathcal{L}^{+}(\mathcal{H}_{s_1}) \\ & \langle\phi| \boldsymbol{X} |\phi\rangle \geqslant \lambda^{*}_{|\phi\rangle\langle\phi|}, \ \forall |\phi\rangle \in \mathcal{H}_{s_1}.\end{aligned}$$

The equivalence is due to the convexity of $\lambda^{*}_{\boldsymbol{H}}$. In particular, for any $\boldsymbol{G} \in \mathcal{F}$, we can find the spectral decomposition of $\boldsymbol{G}$: $\boldsymbol{G} = \sum_i l_i |\phi_i\rangle\langle\phi_i|, l_i \geqslant 0$. Then,

$$\begin{aligned}\operatorname{tr}\{\boldsymbol{X}\boldsymbol{G}\} &= \sum_i l_i \langle\phi_i| \boldsymbol{X} |\phi_i\rangle \\ &\geqslant \sum_i l_i \lambda^{*}_{|\phi_i\rangle\langle\phi_i|} \\ &\geqslant \lambda^{*}_{\sum_i l_i |\phi_i\rangle\langle\phi_i|} \\ &\geqslant \lambda^{*}_{\boldsymbol{G}}.\end{aligned}$$

Hence, it suffices to consider $\mathscr{P}_{\text{aux}}^{\text{one-way}}$, whose constraints are corresponding to vectors.

Step 2: To solve $\mathscr{P}_{\text{aux}}^{\text{one-way}}$, we construct a recursive algorithm that is similar as the algorithm in the proof of Theorem 2 excepts a modification of $\mathcal{W}$ and its cover $\mathcal{W}_\delta$. Recall that $\mathcal{W} = \{\boldsymbol{H} \mid \boldsymbol{H} \succcurlyeq 0, \|\boldsymbol{H}\|_{\text{F}} = 1\}$. Let $\mathcal{W}^{\text{one-way}} = \{|\phi\rangle\langle\phi|\}$ be the substitute of $\mathcal{W}$ in the one-way scenario. Note that $\mathcal{W}^{\text{one-way}}$ is a subset of $\mathcal{W}$ with rank-1 matrices. To construct the epsilon-net for $\mathcal{W}^{\text{one-way}}$, we present the following lemma:

Lemma 3. *In a D-dimensional Hilbert space $\mathcal{H}$, let $\mathcal{W} = \{|\phi\rangle\langle\phi| \mid |\phi\rangle \in \mathcal{H}\}$. There exists a set $\mathcal{W}_\delta = \{|\psi_i\rangle\langle\psi_i|, i \in \mathcal{K}_M\}$ with*

$$M \leqslant \left(\frac{5}{\sqrt{2}\delta}\right)^{2D}$$

such that for any $|\phi\rangle\langle\phi| \in \mathcal{W}$, there exists a $|\psi_i\rangle\langle\psi_i| \in \mathcal{W}_\delta$ where $\||\phi\rangle\langle\phi| - |\psi_i\rangle\langle\psi_i|\|_{\text{F}} \leqslant \delta$.

Proof. Let $\phi = |\phi\rangle\langle\phi|, \psi = |\psi\rangle\langle\psi|$, we have

$$\begin{aligned}
\|\phi - \psi\|_{\mathrm{F}} &= \sqrt{\mathrm{tr}\{(\phi - \psi)(\phi - \psi)\}} \\
&= \sqrt{2 - 2|\langle\psi|\phi\rangle|^2} \\
&\leqslant 2\sqrt{1 - |\langle\psi|\phi\rangle|} \\
&\leqslant 2\sqrt{1 - \mathrm{Re}\,\langle\psi|\phi\rangle} \\
&= \sqrt{2}\||\phi\rangle - |\psi\rangle\|_2
\end{aligned}$$

Hence, the Frobenius norm is bounded by the vector norm with a factor $\sqrt{2}$.

Based on the Lemma 4 of [41], we can find a cover $\mathcal{W}_\delta$ with $|\mathcal{W}_\delta| \leqslant (\frac{5}{\delta'})^{2D}$ such that for any $\phi \in \mathcal{W}$, there exists $\psi \in \mathcal{W}_\delta$ such that

$$\||\phi\rangle - |\psi\rangle\|_2 \leqslant \delta'/2.$$

Therefore, we can obtain the desired $\mathcal{W}_\delta$ by letting $\delta' = \sqrt{2}\delta$. In this case,

$$\|\phi - \psi\|_{\mathrm{F}} \leqslant \sqrt{2}\||\phi\rangle - |\psi\rangle\|_2 \leqslant \delta.$$

□

Then, based on Lemma 3, we can find $\mathcal{W}_\delta^{\text{one-way}} = \{\boldsymbol{G}_i \in \mathcal{W}^{\text{one-way}}, i \in \mathcal{K}_M\}$ such that for any $|\phi\rangle \in \mathcal{H}_{s_1}$, there exists $|\phi_i\rangle \in \mathcal{W}_\delta^{\text{one-way}}$ where $\|\phi - \phi_i\|_{\mathrm{F}} \leqslant \delta$. Then, based on the similar recursive procedures in the Step 1 of Theorem 2 with a replacement of $\mathcal{W}$ and $\mathcal{W}_\delta$ by $\mathcal{W}^{\text{one-way}}$ and $\mathcal{W}_\delta^{\text{one-way}}$ respectively, we obtain an algorithm to solve the multiparty QSD when $\boldsymbol{s}$ is one-way.

Step 3: Let $\tilde{D} = \max_n \dim \mathcal{H}_n$ and $\delta = \epsilon/4\tilde{D}$, similarly as Theorem 2, an estimator for λ^* within the error $r\epsilon$ can be obtained.

To analyze the complexity of this algorithm, let $T^{\text{one-way}}(r)$ be the time complexity of solving an multiparty QSD when s is one-way. Note that

$$T^{\text{one-way}}(r) = |\mathcal{W}_\delta^{\text{one-way}}| T^{\text{one-way}}(r-1) + S(|\mathcal{W}_\delta^{\text{one-way}}|)$$

where $S(|\mathcal{W}_\delta^{\text{one-way}}|)$ is the time complexity of solving an SDP problem with $|\mathcal{W}_\delta^{\text{one-way}}|$ constraints. Note that $|\mathcal{W}_\delta^{\text{one-way}}| \leqslant \left(\frac{20\tilde{D}}{\sqrt{2}\epsilon}\right)^{2\tilde{D}}$. One can conclude that $T^{\text{one-way}}(r) = \left(\frac{\tilde{D}}{\epsilon}\right)^{O(\tilde{D}r)}$. To achieve an precision ϵ' in solving the one-way multiparty QSD, the total time complexity is $\left(\frac{\tilde{D}r}{\epsilon'}\right)^{O(\tilde{D}r)}$, which reduces the exponential factor from $D^2 r$ to Dr compared to two-way scenarios. □

Bibliography

[1] A. S. Holevo, "Statistical decision theory for quantum systems," *Journal of multivariate analysis*, vol. 3, no. 4, pp. 337–394, 1973.

[2] C. W. Helstrom, J. W. Liu, and J. P. Gordon, "Quantum-mechanical communication theory," *Proceedings of the IEEE*, vol. 58, no. 10, pp. 1578–1598, 1970.

[3] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 125–134, Mar. 1975.

[4] S. M. Barnett and S. Croke, "Quantum state discrimination," *Advances in Optics and Photonics*, vol. 1, no. 2, pp. 238–278, 2009.

[5] J. Bae and L.-C. Kwek, "Quantum state discrimination and its applications," *Journal of Physics A: Mathematical and Theoretical*, vol. 48, no. 8, p. 083001, 2015.

[6] S. J. Dolinar, "An optimum receiver for the binary coherent state quantum channel," *Research Laboratory of Electronics, MIT, Quarterly Progress Report*, vol. 11, pp. 115–120, 1973.

[7] R. S. Bondurant, "Near-quantum optimum receivers for the phase-quadrature coherent-state channel," *Optics letters*, vol. 18, no. 22, pp. 1896–1898, 1993.

[8] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Structured near-optimal channel-adapted quantum error correction," *Phys. Rev. A*, vol. 77, no. 1, p. 012320, Jan. 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.77.012320

[9] F. Becerra, J. Fan, G. Baumgartner, J. Goldhar, J. Kosloski, and A. Migdall, "Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination," *Nature Photonics*, vol. 7, no. 2, p. 147, 2013.

[10] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Optimum quantum error recovery using semidefinite programming," *Phys. Rev. A*, vol. 75, no. 1, p. 012338, Jan. 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.75.012338

[11] ——, "Channel-adapted quantum error correction for the amplitude damping channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5705–5718, Dec. 2008.

[12] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, "Quantum computation with optical coherent states," *Physical Review A*, vol. 68, no. 4, p. 042319, 2003.

[13] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *SIAM Journal on Computing*, vol. 35, no. 1, pp. 170–188, 2005.

[14] D. Bacon, A. M. Childs, and W. van Dam, "From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups," in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*. IEEE, 2005, pp. 469–478.

[15] M. G. Paris, "Quantum estimation for quantum technology," *International Journal of Quantum Information*, vol. 7, no. supp01, pp. 125–137, 2009.

[16] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nature photonics*, vol. 5, no. 4, p. 222, 2011.

[17] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum mixed-state discrimination for noisy entanglement-enhanced sensing," *Phys. Rev. Lett.*, vol. 118, no. 4, p. 040801, Jan. 2017.

[18] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation," *International Journal of Theoretical Physics*, vol. 36, no. 6, pp. 1269–1288, 1997.

[19] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Designing optimal quantum detectors via semidefinite programming," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1007–1012, 2003.

[20] M. Osaki, M. Ban, and O. Hirota, "Derivation and physical interpretation of the optimum detection operators for coherent-state signals," *Physical Review A*, vol. 54, no. 2, p. 1691, 1996.

[21] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 858–872, 2001.

[22] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[23] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, "Optimal local implementation of nonlocal quantum gates," *Phys. Rev. A*, vol. 62, no. 5, p. 052317, Oct. 2000.

[24] H. J. Kimble, "The quantum Internet," *Nature*, vol. 453, no. 7198, p. 1023, 2008.

[25] L. Ruan, W. Dai, and M. Z. Win, "Adaptive recurrence quantum entanglement distillation for two-Kraus-operator channels," *Phys. Rev. A*, vol. 97, no. 5, p. 052332, May 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.052332

[26] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, no. 6760, pp. 390–393, Nov. 1999.

[27] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum nonlocality without entanglement," *Phys. Rev. A*, vol. 59, no. 2, p. 1070, 1999.

[28] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, "Everything you always wanted to know about LOCC (but were afraid to ask)," *Communications in Mathematical Physics*, vol. 328, no. 1, pp. 303–326, 2014.

[29] E. Chitambar, "Local quantum transformations requiring infinite rounds of classical communication," *Physical review letters*, vol. 107, no. 19, p. 190502, 2011.

[30] S. M. Cohen, "Structure of local quantum operations and classical communication: Finite versus infinite rounds," *Phys. Rev. A*, vol. 91, no. 4, p. 042106, 2015.

[31] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, "Optimal local discrimination of two multipartite pure states," *Physics Letters A*, vol. 288, no. 2, pp. 62–68, 2001.

[32] B. Higgins, B. Booth, A. Doherty, S. Bartlett, H. Wiseman, and G. Pryde, "Mixed state discrimination using optimal control," *Phys. Rev. Lett.*, vol. 103, no. 22, p. 220503, 2009.

[33] J. Calsamiglia, J. de Vicente, R. Muñoz-Tapia, and E. Bagan, "Local discrimination of mixed states," *Phys. Rev. Lett.*, vol. 105, no. 8, p. 080504, 2010.

[34] S. Croke, S. M. Barnett, and G. Weir, "Optimal sequential measurements for bipartite state discrimination," *Phys. Rev. A*, vol. 95, no. 5, p. 052308, May 2017.

[35] K. Nakahira, K. Kato, and T. S. Usuda, "Optimal discrimination of optical coherent states cannot always be realized by interfering with coherent light, photon counting, and feedback," *Phys. Rev. A*, vol. 97, no. 2, p. 022320, 2018.

[36] E. Chitambar and M.-H. Hsieh, "Revisiting the optimal detection of quantum information," *Physical Review A*, vol. 88, no. 2, p. 020302, 2013.

[37] D. Leung, A. Winter, and N. Yu, "LOCC protocols with bounded width per round optimize convex functions," *arXiv preprint arXiv:1904.10985*, 2019.

[38] S. M. Cohen, "Strong bounds on required resources for quantum channels by local operations and classical communication," *arXiv preprint arXiv:1904.10980*, 2019.

[39] ——, "Local quantum protocols for separable measurements with many parties," *Physical Review A*, vol. 87, no. 5, p. 052135, 2013.

[40] ——, "When a quantum measurement can be implemented locally, and when it cannot," *Physical Review A*, vol. 84, no. 5, p. 052322, 2011.

[41] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, "Remote preparation of quantum states," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 56–74, Jan. 2005.

[42] Y. Shi and X. Wu, "Epsilon-net method for optimizations over separable states," *Theoretical Computer Science*, vol. 598, pp. 51–63, 2015.

[43] J. C. Bezdek and R. J. Hathaway, "Convergence of alternating optimization," *Neural, Parallel & Scientific Computations*, vol. 11, no. 4, pp. 351–368, 2003.

[44] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences. Springer-Verlag Limited, 2008, pp. 95–110, http://stanford.edu/ boyd/graph_dcp.html.

[45] ——, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[46] S. Dolinar Jr, "A near-optimum receiver structure for the detection of m-ary optical ppm signals," *The Telecommunications and Data Acquisition Progress Report*, vol. 42, no. 72, 1982.

[47] F. Becerra, J. Fan, and A. Migdall, "Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states," *Nature communications*, vol. 4, p. 2028, 2013.

[48] A. Acín, E. Bagan, M. Baig, L. Masanes, and R. Munoz-Tapia, "Multiple-copy two-state discrimination with individual measurements," *Physical Review A*, vol. 71, no. 3, p. 032338, 2005.

[49] A. Assalini, N. Dalla Pozza, and G. Pierobon, "Revisiting the dolinar receiver through multiple-copy state discrimination theory," *Physical Review A*, vol. 84, no. 2, p. 022342, 2011.